

The graphic features a dark blue background with a pattern of glowing, curved lines of dots in shades of blue and purple, creating a sense of motion and data flow. The text is centered and uses a clean, sans-serif font. The word 'ZABBIX' is highlighted in a red box, while the rest of the text is white. The year ''26' is positioned to the right of 'ZABBIX'.

**ZABBIX** '26

CONFERENCE

LATIN AMERICA



**Denison Soares**  
Especialista Zabbix

Graduado em Redes de Computadores pela Faculdade Ipiranga (2011) e especialista pela UFPA (2013), atua com redes e monitoramento desde 2013, com experiência em ambientes corporativos. Trabalhou na SEFA/PA, no Banco do Estado do Pará e, desde 2017, no Tribunal de Justiça do Pará. Também atua como consultor em Zabbix e Grafana na Master Support.



**Davison Logan**  
Engenheiro de IA

Especialista em Inteligência Artificial, M/L e soluções GenAI na AWS, atua no desenvolvimento de arquiteturas escaláveis e aplicações inteligentes voltadas para automação, análise de dados e observabilidade. Possui experiência em Python e Golang, atuando na construção de APIs, sistemas orientados a eventos e soluções distribuídas em ambientes AWS. Atualmente atua como Engenheiro de Inteligência Artificial (AI Cloud), integrando IA generativa e automação em soluções de monitoramento inteligente.



**Enne Rebeca Freitas**

Analista de Observabilidade

Profissional certificada ZCP e ZCS, e AWS. Atua como Analista de Observabilidade na Master Support, com foco em monitoramento, análise de dados e confiabilidade de sistemas.

É Graduada em Redes de Computadores - IFAP (2017), Especialista em Governança em TI (2020) e Mestre em Ciência da Informação - UFPA (2025).

**ZABBIX** '26

CONFERENCE

LATIN AMERICA



---

**Denison Soares**

Especialista Zabbix

---

**Davison Logan**

Engenheiro de IA

---

**Enne Rebeca Freitas**

Analista de Observabilidade

### ► Concepção e Objetivo do Projeto

- Crescimento da operação em nuvem (AWS)
- Falta de padronização no NOC
- Ambientes distribuídos e complexos
- Dependência de análise manual
- Dificuldade no repasse de turno

# DEFINIÇÕES INICIAIS

## ORIGEM

- ▶ Criação de um **NOC Centralizado**
- ▶ Foco em clientes na **Amazon Web Services (AWS)**
- ▶ Cenário de migração (**On-Premises** → **Cloud**)
- ▶ Necessidade de:
  - Automação
  - Inteligência operacional
  - Redução de MTTR

# DEFINIÇÕES INICIAIS

## OBJETIVO

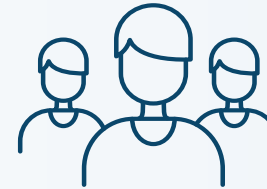
- ▶ Criar o **Zabbix Cortex**
- ▶ Plataforma inteligente baseada no **Zabbix**
- ▶ Integrar
  - Monitoramento
  - Dados históricos
  - Inteligência Artificial
- ▶ Evoluir de:
  - Monitoramento reativo → preditivo e automatizado

# DEFINIÇÕES INICIAIS

## PÚBLICOS

### ► Analista de NOC

- Turnos de 6h
- Necessidade de contexto rápido
- Redução de esforço manual



**Analistas  
do NOC**

### ► Gestor de Área

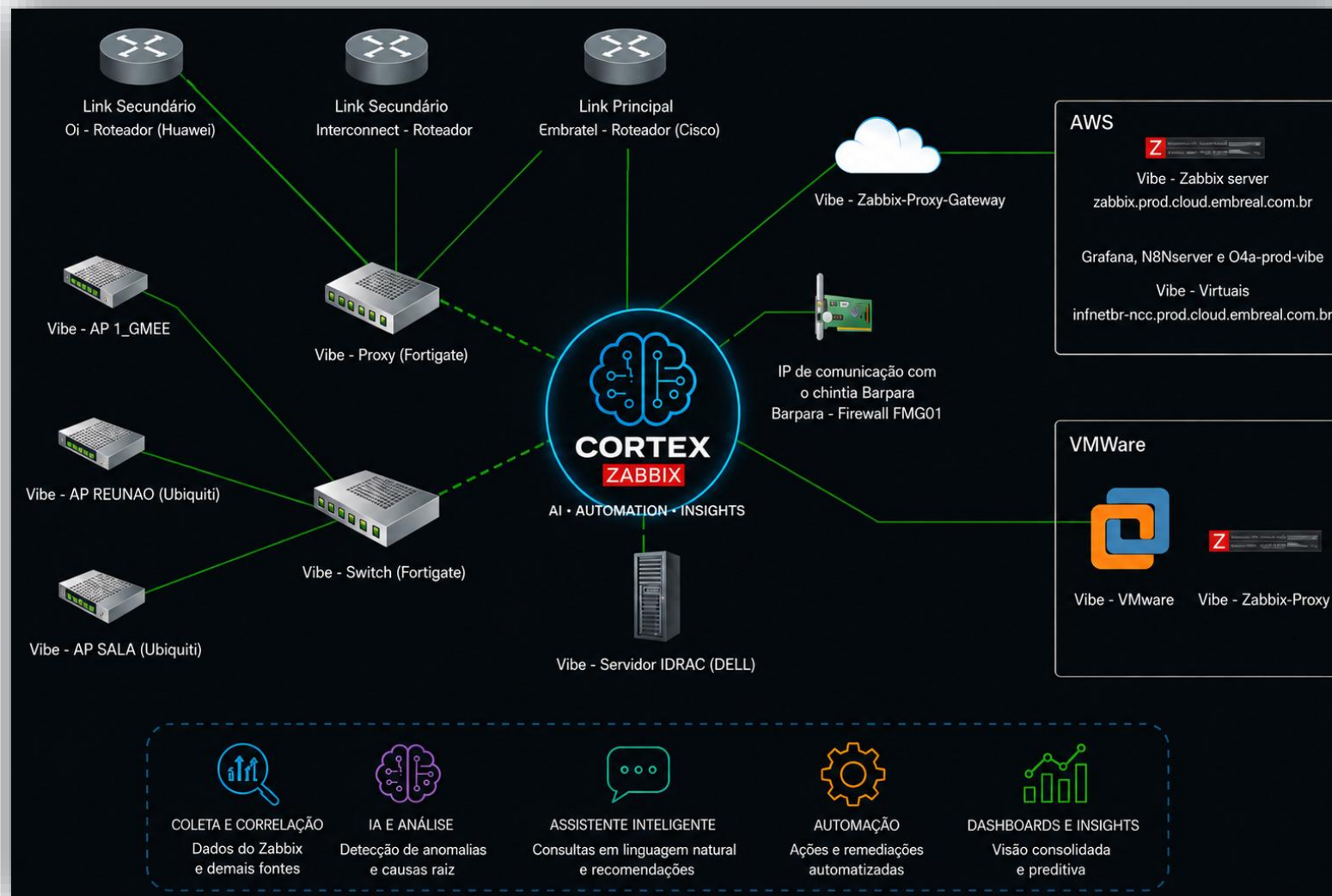
- Visão consolidada
- Indicadores de disponibilidade
- Tomada de decisão estratégica



**Gestor de Área**

# Arquitetura da Solução

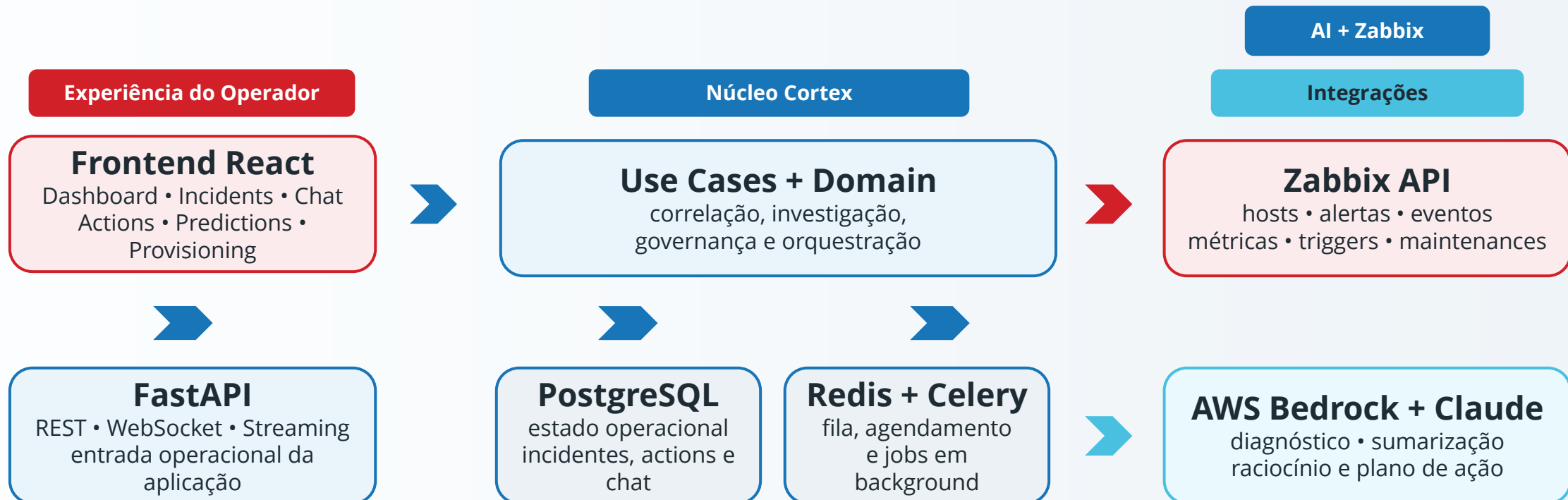
## ZABBIX + CÓRTEX



# Arquitetura da Solução

## Componentes

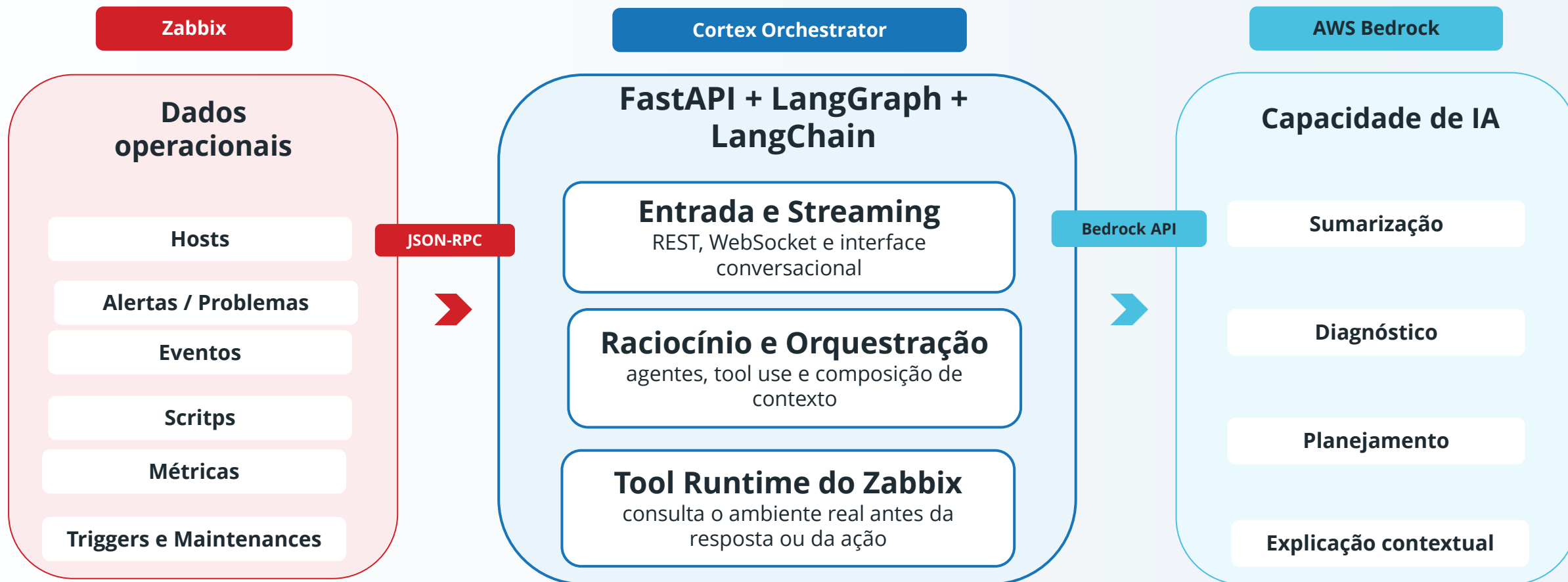
- ▶ Componentes que conectam operação, automação e inteligência



# Arquitetura da Solução

## Integração AI + Zabbix

- ▶ A IA raciocina com Claude, mas se ancora no dado real capturado do Zabbix



O diferencial não é apenas responder com IA; é responder com IA baseada em dados vivos do Zabbix.

# Arquitetura da Solução

## Funcionamento

- Do evento monitorado até a ação governada e validada

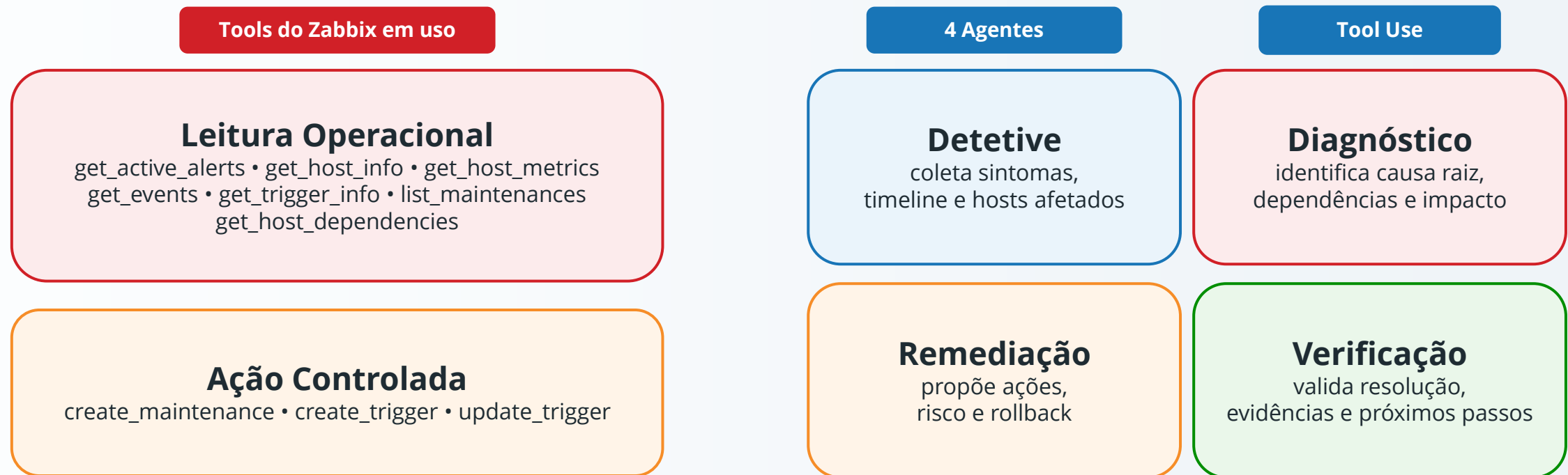


A IA entra no meio do fluxo operacional, não fora dele: ela investiga, sugere e valida em cima do Zabbix.

# Arquitetura da Solução

## Tools e Agentes

- Tool use conectado ao monitoramento real e agentes especializados por etapa



Resultado: IA conectada ao dado real do Zabbix, com aprovação humana nas ações críticas.

# FUNCIONALIDADES

## PAINEL

- Painel**
- Alertas
- Incidentes
- Ações
- Chat IA
- Previsões
- Provisionamento
- Documentação
- Knowledge Base
- Dependências
- Configurações

### Quick Actions AI Powered

- Listar manutenções
- Manutenção 1h
- Manutenção custom
- Criar trigger
- Atualizar trigger

Desabilitar trigger

### Saúde do Ambiente

**30**  
Critical Stable

Fatores-chave

Alertas ativos:	57	Incidentes abertos:	1
Ações pendentes:	0	Previsões críticas:	0

Recomendações da IA

- Address 7 disaster-level alert(s) immediately
- Review 7 high-severity alert(s)
- Investigate 1 critical incident(s)

### Resumo de Alertas

**57**  
Alertas totais [Ver todos](#)

<b>57</b> Ativos	<b>0</b> Reconhecidos
<b>0</b> Suprimidos	<b>0</b> Resolvidos

Por severidade

High: 7	Disaster: 7	Average: 10
Information: 10	Warning: 23	

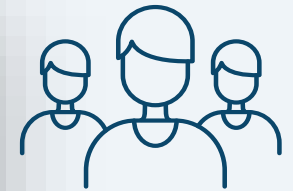
### Feed Tempo Real Conectado

WebSocket conectado — ouvindo eventos desde há menos de um minuto

MONITORANDO

- Alertas criados / suprimidos
- Tempestade de alertas
- Regras de correlação
- Incidentes criados / atualizados
- Investigação IA (despacho / conclusão)
- Ações propostas / executadas
- Previsões de violação

Aguardando eventos de correlação, alertas e incidentes...



Analistas  
do NOC

# FUNCIONALIDADES

## ALERTAS



Painel
<b>Alertas</b>
Incidentes
Ações
Chat IA
Previsões
Provisionamento
Documentação
Knowledge Base
Dependências
Configurações
Usuários
Auditoria

### Alertas

Monitore e gerencie alertas do Zabbix

Sincronizar do Zabbix Atualizar

Total **110** Ativos **110** Reconhecidos **0** Suprimidos **0** Resolvidos **0**

Filtros:  Todas as... Todos os status

Severidade	Host	Trigger	Status	Horário	Ações
information	Unknown	0526-000646: Monitoramento - Alerta / Infraes...	active	about 3 hours ago	<input checked="" type="checkbox"/> Reconhecer
high	Vibe - n8n-server	N8N: Falha no Workflow - Erro no fluxo: Bot Tea...	active	about 3 hours ago	<input checked="" type="checkbox"/> Reconhecer
information	Unknown	0526-000643: Sistemas e Aplicativos - Zabbix ...	active	about 4 hours ago	<input checked="" type="checkbox"/> Reconhecer
information	Vibe - DeskManager API	0426-001157: Administrativo - Pagamentos - S...	active	about 8 hours ago	<input checked="" type="checkbox"/> Reconhecer
information	Vibe - DeskManager API	0426-000907: Infraestrutura - Microsoft Intune...	active	about 8 hours ago	<input checked="" type="checkbox"/> Reconhecer
information	Vibe - DeskManager API	0426-000727: Sistemas e Aplicativos - Desk M...	active	about 8 hours ago	<input checked="" type="checkbox"/> Reconhecer
warning	Unknown	RotinaComFalha: VIBE_LJ.J_MSG_LOJA_PEDID...	active	about 9 hours ago	<input checked="" type="checkbox"/> Reconhecer

# FUNCIONALIDADES

## PREDIÇÃO



Gestor de Área



Analistas do NOC

- Painel
- Alertas
- Incidentes
- Ações
- Chat IA
- Previsões**
- Provisionamento
- Documentação
- Knowledge Base
- Dependências

### Previsões

Análise preditiva com IA e simulação de falhas

Atualizar

Análise Proativa

Gerar Previsões

Simular Falha

#### Insights Proativos IA

##### Falhas críticas em múltiplos

Identificado cluster de 8 alertas de falhas em sistemas externos (DESKMANAGER, F... de validação de dados, conflitos de c...

RH Cloud

Criar incidente para investigar pr... dados nas integrações. Verificar...

##### Workflow N8N com falha c

Falha no workflow 'Bot Teams - Dispa... indisponíveis do nó 'Final - enviar só... fluxo que pode impactar notificações automáticas críticas:

Vibe - n8n-server

Revisar configuração do workflow N8N, verificar mapeamento de dados entre nós e testar fluxo completo. Considerar implementar fallback para...

#### Problemas Recorrentes de Dados Incompletos n... medium

Múltiplos colaboradores com centros de custo incompletos e benefícios sem folha inicial preenchida, além de pagamentos não conciliados. Isso indica possível problema sistemático no processo de cadastro ou migração de...

RH Cloud

Revisar processo de cadastro de colaboradores, implementar validações obrigatórias nos formulários e executar auditoria complet...

esgotamento que pode impactar novos usuários ou renovações.

Vibe - Licenças (Microsoft)

Planejar aquisição de licenças adicionais imediatamente. Revisar usuários inativos para liberação de licenças e implementar monitoramento proativo ...

dependência comum ou problema sistêmico que pode afetar processamento batch.

Control-M server (IN01)

Analisar logs dos jobs falhados, verificar dependências e recursos compartilhados. Implementar retry automático e notificação para falhas...

ativos → 0 previsões críticas → 50 não correlacionados

##### com múltiplas falhas de conectividade high

as em componentes críticos: API MSTRacker-vm Hom Banpará indisponível há 10 dias, e impressora HP sem as. Padrão sugere problema de rede ou infraestrutura.

Vibe Crédito Banpará Vibe - Impressora (HP)

de rede, switches e firewall. Testar conectividade entre alidar configurações de roteamento.

##### m falhas recorrentes medium

om\_erro\_os' e 'Job\_com\_erro') falharam as 'Ended Not OK' no mesmo horário (03:20), sugerindo problema sistêmico que pode afetar processamento batch.

# FUNCIONALIDADES

## CHAT IA



Gestor de  
Área



Analistas  
do NOC

- Painel
- Alertas
- Incidentes
- Ações
- Chat IA
- Previsões
- Provisionamento
- Documentação
- Knowledge Base
- Dependências
- Configurações

**Liste todos os alertas ativos** Renomear ⚡ Pode executar ações

Alimentado por Claude AI • Streaming

**Liste todos os alertas ativos**  
about 1 month ago

Vou listar todos os alertas ativos do Zabbix para você.## Alertas Ativos no Zabbix

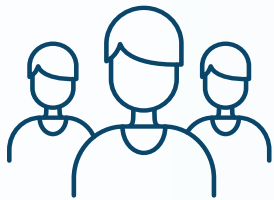
Total: 57 alertas ativos

**Resumo por Severidade:**

- Disaster (7 alertas): Problemas críticos que precisam de atenção imediata
- High (7 alertas): Problemas de alta prioridade
- Average (10 alertas): Problemas de prioridade média
- Warning (23 alertas): Avisos que precisam de monitoramento
- Information (10 alertas): Alertas informativos

# FUNCIONALIDADES

## CHAT IA



Analistas  
do NOC

- Painel
- Alertas
- Incidentes
- Ações
- Chat IA**
- Previsões
- Provisionamento
- Documentação
- Knowledge Base
- Dependências
- Configurações

Novo chat Renomear  
Alimentado por Claude AI • Streaming ↳ Pode executar ações

Quais alertas surgiram nas últimas 24h  
in less than a minute

Vou analisar especificamente os novos alertas que surgiram nas últimas 24 horas:## 🔥 **Novos Alertas Surgidos nas Últimas 24h**

Total: 74 novos alertas

**Distribuição por Severidade:**

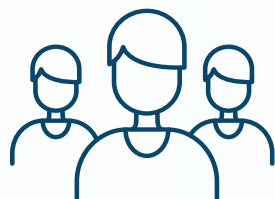
- Disaster (5): 13 alertas
- High (4): 4 alertas
- Average (3): 5 alertas
- Warning (2): 14 alertas
- Information (1): 38 alertas

**Alertas Críticos (Disaster/High):**

- Disaster (13 alertas):**
  - FTP Chubb Indisponível (2 ocorrências) - 23:01 e 07:56
  - TESTE Apache Services Down (11 ocorrências) - Múltiplas falhas entre 17:46-19:26
- High (4 alertas):**
  - N8N Workflow Failures (2x) - Bot Teams com falhas de autenticação - 13:59 e 14:22

# FUNCIONALIDADES

## CHAT IA



Analistas  
do NOC

- Painel
- Alertas
- Incidentes
- Ações
- Chat IA**
- Previsões
- Provisionamento
- Documentação
- Knowledge Base
- Dependências
- Configurações

Novo chat Renomear

Alimentado por Claude AI • Streaming

Pode executar ações

Em qual horário do dia há maior incidência de alertas e quais alertas?  
in less than a minute

Baseado na análise dos 140 eventos das últimas 24 horas, aqui está a distribuição temporal dos alertas:

**🕒 Horários de Maior Incidência de Alertas**

🔥 **Pico Principal: 00:00 - 04:00 (Madrugada)**  
25 eventos - 18% do total

Alertas predominantes:

- 00:01-00:08: 6 novos chamados DeskManager (Inventário/Infraestrutura)
- 01:20-01:36: Reinicializações MSSQL Chubb + Interface VPN instável
- 03:01-04:05: Pico crítico - Control-M Enel Chubb failures + APIs indisponíveis

🔥 **Segundo Pico: 18:00 - 20:00 (Final da Tarde)**  
22 eventos - 16% do total

Alertas predominantes:

- 18:00-18:26: Múltiplas falhas Apache/Docker em ambiente teste
- 18:05-18:20: 4 chamados SAQ (Reenvio de webhook)
- 19:26-19:58: Serviços críticos: Apache, RDP Banpará, Firewall

🟡 **Terceiro Pico: 11:00 - 13:00 (Meio-dia)**  
15 eventos - 11% do total

# FUNCIONALIDADES

## RELATÓRIOS



- Painel
- Alertas
- Incidentes
- Ações
- Chat IA**
- Previsões
- Provisionamento
- Documentação
- Knowledge Base
- Dependências
- Configurações

Novo chat Renomear

Alimentado por Claude AI • Streaming

Qual foi a disponibilidade do sistema Fedz na última semana?

Novo chat Renomear

Alimentado por Claude AI • Streaming

✔ Sistema operacional - Não há alertas ativos no momento

Análise de Eventos (Últimos 7 dias)

Com base nos eventos registrados, identifiquei 6 eventos relacionados ao "Http Response - Feedz":

Incidentes identificados:

- 29/04 às 07:05 - Problema (severidade: disaster) → Resolvido imediatamente
- 29/04 às 07:08 - Problema (severidade: disaster) → Resolvido às 07:12 (4 minutos de downtime)
- 29/04 às 08:06 - Problema (severidade: disaster) → Resolvido às 08:18 (12 minutos de downtime)

Cálculo de Disponibilidade

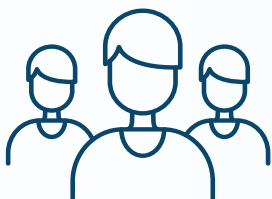
- Total de downtime identificado: ~16 minutos na última semana
- Período analisado: 168 horas (7 dias)
- Disponibilidade estimada: ~99.98%

# FUNCIONALIDADES

## RELATÓRIOS




Gestor de  
Área




Analistas  
do NOC

 Painel

 Alertas

 Incidentes

 Ações

 Chat IA

 Previsões


 Provisionamento



 Documentação


 Knowledge Base

 Dependências

 Configurações


 Novo chat Renomear



 Alimentado por Claude AI  Streaming

 Pode executar ações

Quais foram os incidentes mais graves que ocorreram na semana corrente?

less than a minute ago

 Novo chat Renomear

 Alimentado por Claude AI  Streaming

less than a minute ago

Vou consultar os alertas e eventos mais graves da semana atual para identificar os incidentes críticos. Agora vou consultar os eventos recentes para ter uma visão temporal dos incidentes da semana: Baseado na análise dos alertas ativos e eventos recentes, aqui estão os incidentes mais graves da semana corrente:

### Incidentes Críticos (Disaster - Nível 5)

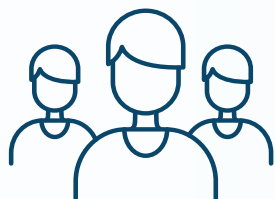
- 1. FTP Chubb Indisponível**
  - Host: Chubb - Links de API
  - Início: 29/04/2026 às 23:01
  - Status: Ativo, não reconhecido
  - Impacto: Sistema de transferência de arquivos crítico fora do ar
- 2. DeskManager Indisponível**
  - Host: DeskManager
  - Início: 22/04/2026 às 19:00
  - Status: Ativo há 8 dias, não reconhecido
  - Impacto: Sistema de gestão de chamados completamente fora
- 3. Múltiplas Falhas em Ambiente de Teste**
  - Host: TESTE MSMonitor / TESTE MSMonitor Frontend
  - Início: 29/04/2026 (múltiplos eventos)
  - Detalhes: Apache services down, endpoints indisponíveis
  - Status: Eventos recorrentes ao longo do dia

# FUNCIONALIDADES

## RELATÓRIOS



Gestor de  
Área



Analistas  
do NOC

- Painel
- Alertas
- Incidentes
- Ações
- Chat IA**
- Previsões
- Provisionamento
- Documentação
- Knowledge Base
- Dependências
- Configurações

Novo chat Renomear

Alimentado por Claude AI • Streaming

↳ Pode executar ações

Quais foram os incidentes mais recorrentes dos últimos 07 dias? fazer uma lista decrescente do mais recorrente pro menos recorrente com o TOP10

less than a minute ago

Novo chat Renomear

Alimentado por Claude AI • Streaming

Vou analisar os eventos dos últimos 7 dias para identificar os incidentes mais recorrentes. Primeiro, vou buscar todos os eventos do período. Com base nos eventos dos últimos 7 dias, vou analisar e contar os incidentes mais recorrentes. Analisando os 542 eventos de problema, posso identificar padrões pelos nomes dos eventos.

**TOP 10 - Incidentes Mais Recorrentes dos Últimos 7 Dias**

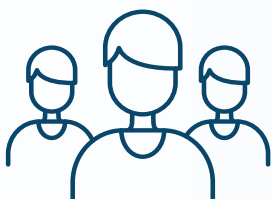
- ENEL API Adesão(Subscription) CE Indisponível
  - Ocorrências: 96
  - Host: Chubb - Links de API
  - Severidade: Warning (2)
  - Padrão: Ocorre aproximadamente de hora em hora
- Chamados DeskManager (diversos tipos)
  - Ocorrências: 85+
  - Host: Vibe - DeskManager API / Unknown
  - Severidade: Information (1)
  - Tipos: Monitoramento, SAQ, Equipamentos, Administrativo, etc.
- SD-WAN/FortiGate Intrusões Detectadas
  - Ocorrências: 70+
  - Host: Vibe - Proxy [Fortigate]
  - Severidade: High (4)
  - Padrão: Múltiplas interfaces (wan1, wan2, internal2)

# FUNCIONALIDADES

## PREDIÇÃO



Gestor de  
Área



Analistas  
do NOC

- Painel
- Alertas
- Incidentes
- Ações
- Chat IA
- Previsões
- Provisionamento
- Documentação
- Knowledge Base
- Dependências
- Configurações

Novo chat Renomear

Alimentado por Claude AI • Streaming

↳ Pode executar ações

Qual sistema tem maior risco de falha?  
less than a minute ago

Novo chat Renomear

Alimentado por Claude AI • Streaming

Vou analisar os alertas ativos para identificar qual sistema apresenta maior risco de falha. Deixe-me buscar informações mais detalhadas sobre os alertas críticos. Agora vou analisar os eventos recentes para entender a frequência de problemas por sistema. Agora vou analisar especificamente alguns dos sistemas com mais problemas críticos: Vou verificar as métricas atuais dos sistemas mais críticos: ## Análise de Risco de Falha dos Sistemas

Com base na análise dos alertas ativos e eventos recentes, identifiquei os sistemas com maior risco de falha:

- Alto Risco**
- 1. DeskManager (grupovibe.desk.ms)
  - Status: Sistema INDISPONÍVEL (alerta disaster ativo há 7 dias)
  - Impacto: Sistema de service desk principal - afeta abertura e gestão de chamados
  - Evidência: Status = 1 (down) desde 22/04
- 2. Vibe - n8n-server (Automação)
  - Status: Falhas recorrentes em workflows críticos
  - Problemas: Erro de autenticação e integração com Teams
  - Frequência: 2 falhas nas últimas 24h
  - Impacto: Automações e notificações comprometidas
- 3. TESTE - MSMonitor Frontend
  - Status: Endpoint indisponível (disaster)
  - Problema: Sistema de monitoramento auxiliar fora do ar há 7 dias

⚠ Risco Médio-Alto

# MELHORIAS OBTIDAS

## CORTEX

### ▶ Analista de NOC



**Analistas  
do NOC**

- Repasses Turnos mais Ágeis (75% mais ágeis)
- Sugestão de Solução reduziu em 50% o RTT

### ▶ Gestor de Área



**Gestor de  
Área**

- Redução no tempo necessários para confeccionar os relatórios mensais de medição por cliente (40% mais ágeis)
- Insights sobre a carga de trabalho em cada turno (Possibilitar adequação de reforço em horários de pico)

# SIMULAÇÃO

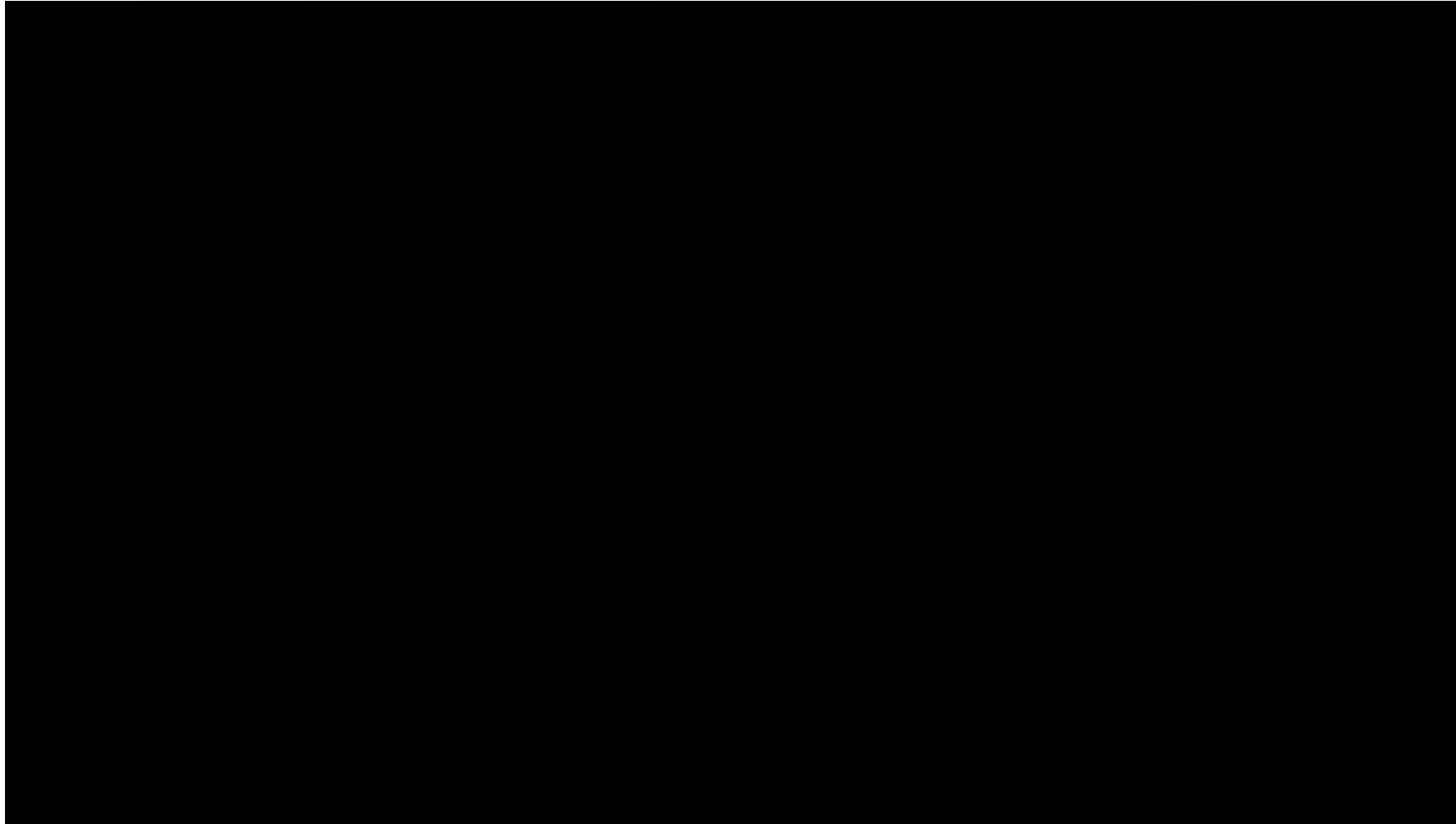
## ESTEIRA CORTEX

---

ZABBIX '26

CONFERENCE

LATIN AMERICA





Obrigado!

