

PRÉ-REQUISITOS · IMPLANTAÇÃO

# Pré-requisitos: Implantação da plataforma GitLab™ em servidores Linux

Documento enviado após a escolha do serviço PS-IMP-01: o que o cliente provisiona, as credenciais que entrega à Pointer, as informações a enviar e o checklist de prontidão.

CÓDIGO

PR-IMP-01

TIPO

Pré-requisitos

VERSÃO

1.2

DATA

1 de outubro de 2026

O3S Consultoria e Tecnologia da Informação Ltda.  
contato@pointertech.digital · +55 (61) 99874-4648 · pointertech.digital

GITLAB is a trademark of GitLab Inc. in the United States and other countries and regions.



GitLab  
Select  
Partner

PRÉ-REQUISITOS · PR-IMP-01 · OFERTA PS-IMP-01

## Pré-requisitos: Implantação da plataforma GitLab em servidores Linux

Este documento é enviado depois que o cliente escolhe o serviço **PS-IMP-01 — Implantação da plataforma GitLab em servidores Linux**. É dirigido às equipes de infraestrutura, rede e segurança do cliente e reúne:

1. a infraestrutura que o cliente provisiona, por arquitetura de referência, ou, quando o pipeline cria a infraestrutura na AWS ou no Azure, a conta, a identidade e as cotas que o cliente fornece;
2. as credenciais que o cliente entrega à Pointer e a forma de entrega;
3. o formulário com as informações não secretas do ambiente;
4. o checklist de prontidão, com o que é conferido automaticamente pelo pipeline e o que é conferido na reunião de prontidão.

Os recursos opcionais (balanceador do cliente, Container Registry, GitLab Geo, frota de runners do cliente, agentes GitLab para Kubernetes e Grafana gerenciado, este sob consulta) têm seções próprias e só se aplicam quando contratados.

As especificações de hardware seguem as arquiteturas de referência GitLab (documentação oficial consultada em 29/09/2026). O prazo de devolução do formulário e do checklist é definido na reunião de kick-off. A implantação só começa depois de uma verificação prévia (preflight) sem erros contra as VMs reais.

### Conteúdo

Infraestrutura que o cliente provisiona

Máquinas virtuais por arquitetura de referência

Sistemas operacionais aceitos

Portas padrão dos componentes (tabela oficial do Linux package)

Balanceadores (HAProxy do GET)

Acesso de rede de saída

Infraestrutura criada pelo pipeline (AWS ou Azure)

Balanceador do cliente (no lugar do HAProxy do GET)

GitLab Geo (dois sites)

Frota de runners do cliente

---

Agentes GitLab para Kubernetes

---

Monitoramento: Prometheus e Grafana gerenciado (sob consulta)

---

Entrega das credenciais

---

Como a Pointer usa essas informações

---

Critérios de aceite

---

Credenciais que o cliente entrega à Pointer

---

Informações a enviar

---

Checklist de prontidão

---

## 1. Infraestrutura que o cliente provisiona

| Item                        | Especificação                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Obrigatório |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| Máquinas virtuais por papel | Quantidade, vCPU e memória por papel conforme a arquitetura de referência escolhida (tabela <i>Máquinas virtuais por arquitetura de referência</i> ). Um endereço por VM, alcançável pelo runner; cada papel em VM dedicada (o mesmo endereço em dois papéis é recusado pela validação). Na infraestrutura criada pelo pipeline, as VMs e os endereços vêm do estado do Terraform (seção <i>Infraestrutura criada pelo pipeline</i> ). O preflight compara cada VM com a arquitetura: abaixo de 90% de vCPU ou de memória, erro; vCPU abaixo de 100% ou memória abaixo de 97%, alerta. A documentação GitLab orienta evitar instâncias <i>burstable</i> (desempenho inconsistente). | Sim         |
| Sistema operacional         | Versão da matriz do pipeline (tabela <i>Sistemas operacionais aceitos</i> ): suportados Ubuntu 22.04 e 24.04, Debian 12 e 13, Red Hat Enterprise Linux 9 e 10 e Amazon Linux 2023. Instalação limpa do sistema operacional, sem instalação GitLab prévia (o GET exige instalação limpa; o preflight emite alerta quando encontra instância GitLab instalada). <b>python3</b> instalado em todas as VMs.                                                                                                                                                                                                                                                                             | Sim         |
| Arquitetura de CPU          | x86_64 ou aarch64. Em aarch64 o preflight emite alerta (a documentação GitLab registra <i>known issues</i> em ARM); Oracle Linux e SLES só têm pacote para x86_64 (erro em aarch64).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Sim         |

| Item                         | Especificação                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Obrigatório             |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Usuário de implantação       | Um usuário SSH presente em todas as VMs, com sudo sem senha (os playbooks do GET executam com escalonamento de privilégio), autenticado pela chave entregue à Pointer. Porta SSH (padrão 22) acessível a partir do runner. VM inacessível ou coleta de fatos com falha: erro no preflight. Na infraestrutura criada pelo pipeline, a chave pública é gravada nas VMs pelo pipeline: na AWS, com o usuário da imagem usada pelo módulo do GET; no Azure, com o usuário de administração informado no formulário.                                                                                                                                                                                                                                                                                                                                             | Sim                     |
| Disco                        | Volume de <code>/var/opt/gitlab</code> montado antes da implantação: o GET não configura discos de dados em servidores próprios. Documentação GitLab: nós de aplicação (GitLab Rails, Sidekiq) com no mínimo 40 GB (pacote de cerca de 2,5 GB, sistema operacional, logs e temporários); Gitaly com no mínimo a soma de todos os repositórios, em disco local e dedicado por nó (a documentação orienta SSD para o Gitaly, processo intensivo em I/O, e não suporta NFS nem sistemas de arquivos em nuvem para repositórios); PostgreSQL com 5 a 10 GB (GitLab Ultimate: pelo menos 12 GB). A documentação orienta evitar discos <i>burstable</i> e sistemas de arquivos em rede (NFS, Amazon EFS, Azure Files). Preflight: menos de 10 GB livres no volume de <code>/var/opt/gitlab</code> , erro; menos de 40 GB, alerta (limiar operacional da Pointer). | Sim                     |
| Memória e swap               | A documentação GitLab orienta desabilitar o swap sempre que possível ou provisionar memória para que a instância não use swap.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Não                     |
| Sincronismo de horário (NTP) | Todas as VMs sincronizadas por NTP; o preflight confere o sincronismo e emite alerta quando não há. Por padrão, os nós Gitaly e Praefect consultam pool.ntp.org nas verificações de sincronização de horário (documentação GitLab); sem acesso a pool.ntp.org, informe o servidor NTP interno no formulário.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Sim                     |
| Latência entre nós           | Menor que 5 ms entre os nós, exigência da documentação GitLab para a replicação síncrona. Uma instância não pode abranger várias regiões geográficas; ao distribuir entre zonas ou data centers, a documentação orienta número ímpar de zonas na mesma região.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Condicional: 3k ou mais |
| DNS                          | Registro DNS do host da URL externa apontando para a VM única (1k) ou para o balanceador externo (HAProxy do GET ou balanceador do cliente, 2k ou mais), resolvível nas VMs GitLab Rails e do balanceador externo: o preflight emite alerta quando não resolve, e erro com Let's Encrypt. GitLab Pages: registro DNS wildcard do domínio do Pages. Container Registry: registro do nome do registry para o mesmo ponto de entrada. A gestão do servidor DNS fica fora do escopo do GET, e o pipeline não cria registros DNS, inclusive na infraestrutura criada por ele.                                                                                                                                                                                                                                                                                    | Sim                     |

| Item                  | Especificação                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Obrigatório                                  |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Certificado TLS       | Certificado do host externo e chave privada em PEM, com os certificados intermediários da cadeia no mesmo arquivo do certificado; SAN obrigatório (CN sozinho é obsoleto), cobrindo o host externo e os hostnames adicionais usados (documentação do GET), inclusive o nome do Container Registry quando habilitado. GitLab Pages com HTTPS: certificado wildcard do domínio do Pages. Com autoridade certificadora não pública, a cadeia da AC emissora é entregue para que os nós confiem na URL externa (sem balanceador interno, o Gitaly chama a API interna pela URL externa). Alternativa ao certificado do cliente: Let's Encrypt, com e-mail de registro.                    | Condicional: certificado do cliente (padrão) |
| Object storage        | Serviço com API S3-compatível (endpoint, região, endereçamento <i>path style</i> quando o serviço exigir e credenciais de acesso), com os buckets criados antes da implantação. Obrigatório a partir de 2k e para GitLab Pages em mais de um nó; opcional em 1k. Entre os serviços testados pela GitLab está o Amazon S3 (Object Lock não suportado); outras soluções S3-compatíveis, como Ceph RGW ou appliances on-premises, são documentadas pela comunidade, e o suporte da GitLab pode não conseguir ajudar em serviços fora do conjunto testado. Os objetos do object storage não entram no backup da plataforma GitLab: a cópia desses dados usa o backup do próprio provedor. | Condicional: 2k ou mais                      |
| Buckets               | Nomes exatos, com o prefixo definido no formulário (padrão <b>gitlab</b> ): <b>&lt;prefixo&gt;-artifacts</b> , <b>&lt;prefixo&gt;-dependency-proxy</b> , <b>&lt;prefixo&gt;-lfs</b> , <b>&lt;prefixo&gt;-packages</b> , <b>&lt;prefixo&gt;-terraform-state</b> , <b>&lt;prefixo&gt;-uploads</b> , <b>&lt;prefixo&gt;-pages</b> , <b>&lt;prefixo&gt;-mr-diffs</b> , <b>&lt;prefixo&gt;-ci-secure-files</b> , <b>&lt;prefixo&gt;-backups</b> e, com Container Registry, <b>&lt;prefixo&gt;-registry</b> . A lista gerada para o ambiente consta do as-built. Na infraestrutura criada pelo pipeline na AWS, os buckets são criados pelo pipeline (padrão).                              | Condicional: object storage                  |
| VMs dos balanceadores | VMs para o HAProxy instalado pelo GET: balanceador externo a partir de 2k e balanceador interno a partir de 3k (tabela por arquitetura). O GET instala o Docker Engine nessas VMs e executa a imagem do HAProxy obtida do Docker Hub. Com o balanceador do cliente no lugar do HAProxy externo, não há VM de balanceador externo (seção <i>Balanceador do cliente</i> ).                                                                                                                                                                                                                                                                                                              | Condicional: 2k ou mais, com HAProxy do GET  |
| VMs OpenSearch        | Somente com busca avançada no modo de nós: no mínimo 1 VM (abaixo de 3, o pipeline emite alerta). A arquitetura de referência não fixa especificação para a busca (depende dos dados) e o preflight não confere vCPU e memória dessas VMs. O GET instala o Docker Engine nessas VMs.                                                                                                                                                                                                                                                                                                                                                                                                  | Condicional: busca avançada em VMs           |

| Item                      | Especificação                                                                                                                                                                                                                                                                                                                                 | Obrigatório                     |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| VM do runner              | Linux com Docker Engine, 2 vCPU, 4 GB de memória e 40 GB de disco (a imagem do pipeline ocupa cerca de 6 GB). Somente conexões de saída, nenhuma porta de entrada; acesso SSH a todas as VMs e HTTPS à URL externa. Com proxy corporativo, o proxy é configurado no serviço do runner.                                                        | Sim                             |
| Acesso de rede de saída   | Conforme a tabela <i>Acesso de rede de saída</i> : runner para gitlab.com e registry.gitlab.com; VMs para packages.gitlab.com e para os repositórios do sistema operacional; VMs de balanceador e OpenSearch para o Docker Hub. Instalação sem acesso à internet: roadmap.                                                                    | Sim                             |
| Portas entre os nós       | Regras de firewall entre as VMs e dos balanceadores, a partir da tabela oficial de portas do Linux package e da tabela de balanceadores deste documento.                                                                                                                                                                                      | Condicional: 2k ou mais         |
| Serviços do cliente       | LDAP ou Active Directory, SMTP e cluster de busca externo, quando habilitados, alcançáveis a partir das VMs GitLab Rails e Sidekiq nas portas informadas no formulário.                                                                                                                                                                       | Condicional: recurso habilitado |
| Container Registry        | Nome do registry (por exemplo <code>registry.&lt;domínio&gt;</code> , coberto pelo certificado) ou porta própria no mesmo host (somente nó único ou balanceador do cliente encaminhando a porta), registro DNS para o mesmo ponto de entrada e bucket <code>&lt;prefixo&gt;-registry</code> no object storage (obrigatório em mais de um nó). | Condicional: Container Registry |
| Segundo site (GitLab Geo) | Segundo ambiente com os mesmos requisitos deste documento para a arquitetura escolhida, a mesma versão GitLab, object storage nos dois sites ou em nenhum, rede entre os sites e acesso do runner às VMs dos dois sites com a mesma chave SSH (seção <i>GitLab Geo</i> ).                                                                     | Condicional: GitLab Geo         |
| Licença                   | Assinatura GitLab Premium ou GitLab Ultimate: activation code (ativação online) ou arquivo de licença (instalação offline). O GET exige Premium ou superior; a edição Community Edition é recusada pela validação, e a ausência de licença gera alerta. Com GitLab Geo, a licença fica só no site primário.                                   | Sim                             |

## 2. Máquinas virtuais por arquitetura de referência

| Papel                                  | 1k                 | 2k                  | 3k                  | 5k                  | 10k                 | 25k                 | 50k                   |
|----------------------------------------|--------------------|---------------------|---------------------|---------------------|---------------------|---------------------|-----------------------|
| Instância única (todos os componentes) | 1 × 8 vCPU / 16 GB | —                   | —                   | —                   | —                   | —                   | —                     |
| Balanceador externo (HAProxy)          | —                  | 1 × 4 vCPU / 3,6 GB | 1 × 4 vCPU / 3,6 GB | 1 × 4 vCPU / 3,6 GB | 1 × 4 vCPU / 3,6 GB | 1 × 8 vCPU / 7,2 GB | 1 × 16 vCPU / 14,4 GB |
| Consul                                 | —                  | —                   | 3 × 2 vCPU / 1,8 GB | 3 × 2 vCPU / 1,8 GB | 3 × 2 vCPU / 1,8 GB | 3 × 2 vCPU / 1,8 GB | 3 × 2 vCPU / 1,8 GB   |

| Papel                                              | 1k                          | 2k                               | 3k                                | 5k                                 | 10k                                | 25k                                | 50k                                  |
|----------------------------------------------------|-----------------------------|----------------------------------|-----------------------------------|------------------------------------|------------------------------------|------------------------------------|--------------------------------------|
| PostgreSQL                                         | —                           | 1 × 2 vCPU<br>/ 7,5 GB           | 3 × 2 vCPU<br>/ 7,5 GB            | 3 × 4 vCPU<br>/ 15 GB              | 3 × 8 vCPU<br>/ 30 GB              | 3 × 16 vCPU<br>/ 60 GB             | 3 × 32 vCPU<br>/ 120 GB              |
| PgBouncer                                          | —                           | —                                | 3 × 2 vCPU<br>/ 1,8 GB            | 3 × 2 vCPU<br>/ 1,8 GB             | 3 × 2 vCPU<br>/ 1,8 GB             | 3 × 2 vCPU<br>/ 1,8 GB             | 3 × 2 vCPU /<br>1,8 GB               |
| Balanceador interno<br>(HAProxy)                   | —                           | —                                | 1 × 4 vCPU /<br>3,6 GB            | 1 × 4 vCPU /<br>3,6 GB             | 1 × 4 vCPU /<br>3,6 GB             | 1 × 8 vCPU /<br>7,2 GB             | 1 × 16 vCPU /<br>14,4 GB             |
| Redis (com Sentinel a<br>partir de 3k)             | —                           | 1 × 1 vCPU /<br>3,75 GB          | 3 × 2 vCPU<br>/ 7,5 GB            | 3 × 2 vCPU<br>/ 7,5 GB             | —                                  | —                                  | —                                    |
| Redis cache                                        | —                           | —                                | —                                 | —                                  | 3 × 4 vCPU<br>/ 15 GB              | 3 × 4 vCPU<br>/ 15 GB              | 3 × 4 vCPU /<br>15 GB                |
| Redis persistente                                  | —                           | —                                | —                                 | —                                  | 3 × 4 vCPU<br>/ 15 GB              | 3 × 4 vCPU<br>/ 15 GB              | 3 × 4 vCPU /<br>15 GB                |
| Gitaly                                             | —                           | 1 × 4 vCPU<br>/ 15 GB            | 3 × 4 vCPU<br>/ 15 GB             | 3 × 8 vCPU<br>/ 30 GB              | 3 × 16 vCPU<br>/ 60 GB             | 3 × 32 vCPU<br>/ 120 GB            | 3 × 64 vCPU<br>/ 240 GB              |
| Praefect (somente<br>Gitaly Cluster)               | —                           | —                                | 3 × 2 vCPU<br>/ 1,8 GB            | 3 × 2 vCPU<br>/ 1,8 GB             | 3 × 2 vCPU<br>/ 1,8 GB             | 3 × 4 vCPU<br>/ 3,6 GB             | 3 × 4 vCPU /<br>3,6 GB               |
| PostgreSQL do Praefect<br>(somente Gitaly Cluster) | —                           | —                                | 1 × 2 vCPU /<br>1,8 GB            | 1 × 2 vCPU /<br>1,8 GB             | 1 × 2 vCPU /<br>1,8 GB             | 1 × 2 vCPU /<br>1,8 GB             | 1 × 2 vCPU /<br>1,8 GB               |
| Sidekiq                                            | —                           | 1 × 4 vCPU<br>/ 15 GB            | 2 × 4 vCPU<br>/ 15 GB             | 2 × 4 vCPU<br>/ 15 GB              | 4 × 4 vCPU<br>/ 15 GB              | 4 × 4 vCPU<br>/ 15 GB              | 4 × 4 vCPU /<br>15 GB                |
| GitLab Rails                                       | —                           | 2 × 8 vCPU<br>/ 7,2 GB           | 3 × 8 vCPU<br>/ 7,2 GB            | 3 × 16 vCPU<br>/ 14,4 GB           | 3 × 32 vCPU<br>/ 28,8 GB           | 5 × 32 vCPU<br>/ 28,8 GB           | 12 × 32<br>vCPU / 28,8<br>GB         |
| Monitoramento                                      | —                           | 1 × 2 vCPU<br>/ 1,8 GB           | 1 × 2 vCPU /<br>1,8 GB            | 1 × 2 vCPU /<br>1,8 GB             | 1 × 4 vCPU /<br>3,6 GB             | 1 × 4 vCPU /<br>3,6 GB             | 1 × 4 vCPU /<br>3,6 GB               |
| Total com Gitaly Cluster                           | 1 VM · 8<br>vCPU · 16<br>GB | 8 VMs · 33<br>vCPU ·<br>61,05 GB | 27 VMs · 86<br>vCPU ·<br>168,6 GB | 27 VMs · 128<br>vCPU ·<br>257,7 GB | 32 VMs ·<br>240 vCPU ·<br>535,2 GB | 34 VMs ·<br>390 vCPU ·<br>875,4 GB | 41 VMs · 774<br>vCPU ·<br>1.631,4 GB |
| Total com Gitaly<br>Sharded                        | —                           | —                                | 23 VMs · 78<br>vCPU · 161,4<br>GB | 23 VMs ·<br>120 vCPU ·<br>250,5 GB | 28 VMs ·<br>232 vCPU ·<br>528 GB   | 30 VMs ·<br>376 vCPU ·<br>862,8 GB | 37 VMs ·<br>760 vCPU ·<br>1.618,8 GB |

- Formato: quantidade de VMs × vCPU / memória por VM. Fonte: arquiteturas de referência GitLab (documentação oficial, consultada em 29/09/2026). Os totais são a soma de quantidade × especificação de cada papel (aritmética).
- Gitaly Sharded (3k ou mais) usa as mesmas especificações de Gitaly e dispensa as VMs de Praefect e de PostgreSQL do Praefect. A documentação GitLab registra o PostgreSQL do Praefect como 1 ou mais nós; o pipeline aceita no mínimo 1.
- O pipeline aceita mais VMs de GitLab Rails, Sidekiq e Gitaly que a arquitetura, com alerta; nos demais papéis, a quantidade precisa ser exatamente a da arquitetura.
- Os tipos de máquina citados como exemplo na documentação GitLab não são obrigatórios; outros tipos que atendam aos requisitos, inclusive ARM, são aceitos pela documentação.
- Com monorepos grandes (vários gigabytes), a documentação GitLab informa que as especificações de Gitaly e GitLab Rails podem precisar de aumento.

- Busca avançada no modo de nós: VMs OpenSearch adicionais, fora desta tabela (ver *Infraestrutura que o cliente provisiona*).
- Com o balanceador do cliente no lugar do HAProxy externo, a VM do balanceador externo sai da arquitetura; com balanceador interno do cliente (sob consulta), também a do balanceador interno.
- As mesmas quantidades valem para a infraestrutura criada pelo pipeline, que escolhe para cada papel o menor tipo da sua lista que atende vCPU e memória (AWS: c7i, m7i, r7i; Azure: Fsv2, Dasv5, Easv5), salvo tipo definido no formulário.

### 3. Sistemas operacionais aceitos

| Sistema operacional                     | Situação no pipeline                                                | Fim de vida do sistema operacional           | Última versão GitLab proposta (documentação GitLab) |
|-----------------------------------------|---------------------------------------------------------------------|----------------------------------------------|-----------------------------------------------------|
| Ubuntu 22.04                            | Suportado                                                           | abril de 2027                                | 19.11.0                                             |
| Ubuntu 24.04                            | Suportado                                                           | abril de 2029                                | 21.11.0                                             |
| Ubuntu 26.04                            | Best effort (Linux package desde 19.3.0; fora da lista do GET 3.11) | abril de 2031                                | 23.11.0                                             |
| Ubuntu 20.04                            | Bloqueado                                                           | —                                            | 18.11 (versão final publicada)                      |
| Debian 11                               | Aceito com alerta                                                   | agosto de 2026                               | 19.3.0                                              |
| Debian 12                               | Suportado                                                           | junho de 2028                                | 19.3.0 (ver nota)                                   |
| Debian 13                               | Suportado                                                           | junho de 2030                                | 23.1.0                                              |
| Red Hat Enterprise Linux 9              | Suportado                                                           | maio de 2032                                 | 25.0.0                                              |
| Red Hat Enterprise Linux 10             | Suportado                                                           | maio de 2035                                 | 28.0.0                                              |
| Red Hat Enterprise Linux 8              | Best effort (deprecated no GET)                                     | maio de 2029                                 | 22.0.0                                              |
| Amazon Linux 2023                       | Suportado                                                           | junho de 2029                                | 22.1.0                                              |
| Amazon Linux 2                          | Bloqueado                                                           | junho de 2026                                | 19.1.0                                              |
| AlmaLinux 8, 9 e 10                     | Best effort (fora da lista do GET)                                  | março de 2029, maio de 2032 e maio de 2035   | 21.10.0, 25.0.0 e 28.0.0                            |
| Oracle Linux 8, 9 e 10 (somente x86_64) | Best effort (fora da lista do GET)                                  | julho de 2029, junho de 2032 e junho de 2035 | 22.2.0, 25.1.0 e 28.1.0                             |

| Sistema operacional                                    | Situação no pipeline               | Fim de vida do sistema operacional | Última versão GitLab proposta (documentação GitLab) |
|--------------------------------------------------------|------------------------------------|------------------------------------|-----------------------------------------------------|
| SLES 12 e 15, openSUSE Leap 15                         | Bloqueado (o GET não suporta SUSE) | —                                  | —                                                   |
| Outras distribuições (por exemplo Rocky Linux, CentOS) | Bloqueado                          | —                                  | —                                                   |

- *Suportado*: suportado pelo Linux package e pelo GET 3.11.0. *Best effort*: suportado pelo Linux package, fora da lista do GET; o preflight registra erro, ou alerta quando a exceção é liberada e registrada no engajamento. *Bloqueado*: erro no preflight.
- Debian 11: o fim de vida do sistema operacional (agosto de 2026) já passou; o pipeline aceita a versão com alerta. A tabela oficial informa 19.3.0 como última versão GitLab proposta para Debian 11 e também para Debian 12; em 29/09/2026 o repositório oficial publica pacotes 19.4.1 para as duas versões.
- O preflight cruza a versão GitLab pedida com a última versão proposta para o sistema operacional (coluna da direita): acima dela, erro (alerta com a exceção de best effort registrada no engajamento); na mesma versão major, alerta. Com GitLab 19.4 ou superior, Debian 11 e Debian 12 reprovam no preflight.
- Segundo a documentação GitLab, os pacotes são publicados até o fim de vida do sistema operacional, e a GitLab busca avisar com pelo menos 6 meses de antecedência antes de descontinuar uma versão.

## 4. Portas padrão dos componentes (tabela oficial do Linux package)

| Componente                | Porta padrão                       | Observação                                                                            |
|---------------------------|------------------------------------|---------------------------------------------------------------------------------------|
| GitLab Rails (NGINX)      | 80 ou 443                          | Entrada HTTP/HTTPS da instância                                                       |
| GitLab Shell (SSH do Git) | 22                                 | Com o HAProxy do GET, a entrada SSH do Git no balanceador externo usa 2222 por padrão |
| PostgreSQL                | 5432                               | Socket local por padrão; porta quando o PostgreSQL fica em VM separada                |
| PgBouncer                 | 6432                               | Desligado por padrão; usado a partir de 3k                                            |
| Patroni                   | 8008                               | Desligado por padrão; usado a partir de 3k                                            |
| Consul                    | 8300, 8301 (TCP e UDP), 8500, 8600 | Desligado por padrão; usado a partir de 3k                                            |
| Redis                     | 6379                               | Socket local por padrão; porta quando o Redis fica em VM separada                     |
| Redis Sentinel            | 26379                              | Desligado por padrão; usado a partir de 3k                                            |

| Componente                       | Porta padrão            | Observação                                                         |
|----------------------------------|-------------------------|--------------------------------------------------------------------|
| Gitaly                           | 8075 (9999 com TLS)     | Socket local por padrão; porta quando o Gitaly fica em VM separada |
| Praefect                         | 2305 (3305 com TLS)     | Desligado por padrão; usado com Gitaly Cluster                     |
| Puma                             | 8080                    | Socket local por padrão                                            |
| GitLab Workhorse                 | 8181                    | Socket local por padrão                                            |
| GitLab KAS                       | 8150                    | Ligado por padrão                                                  |
| Prometheus                       | 9090                    | Ligado por padrão                                                  |
| Node exporter                    | 9100                    | Ligado por padrão                                                  |
| Redis exporter                   | 9121                    | Ligado por padrão                                                  |
| PostgreSQL exporter              | 9187                    | Ligado por padrão                                                  |
| PgBouncer exporter               | 9188                    | Desligado por padrão                                               |
| GitLab Exporter                  | 9168                    | Ligado por padrão                                                  |
| Sidekiq exporter e health check  | 8082 e 8092             | Ligados por padrão                                                 |
| Gitaly exporter                  | 9236                    | Ligado por padrão                                                  |
| GitLab Workhorse exporter        | 9229                    | Ligado por padrão                                                  |
| NGINX status                     | 8060                    | Ligado por padrão                                                  |
| GitLab Pages                     | 80 ou 443               | Quando habilitado                                                  |
| Busca (Elasticsearch/OpenSearch) | 9200                    | Quando habilitada                                                  |
| LDAP                             | Conforme a configuração | Padrão do pipeline: 636                                            |
| SMTP                             | 465 na tabela oficial   | Na prática, a porta do servidor SMTP informada no formulário       |

- Tabela oficial de portas padrão do Linux package (documentação GitLab). A tabela não informa direção nem protocolo de transporte, exceto Consul 8301 (TCP e UDP), e o Consul pode usar outras portas quando funcionalidades adicionais são habilitadas.
- Na arquitetura 1k (nó único), PostgreSQL, Redis, Puma, GitLab Workhorse e Gitaly usam socket local por padrão; a VM expõe HTTPS (443) e o SSH do Git (22).
- O pipeline Pointer não tem matriz própria de portas entre nós: as regras de origem e destino entre as VMs são levantadas no discovery com a equipe de rede do cliente, a partir desta tabela.

- Portas usadas pela configuração do pipeline, além da tabela: TCP 8155 entre os nós GitLab Rails (API privada do KAS, com 2 ou mais nós); 9090 do Prometheus no nó de monitoramento, consultada pela verificação pós-implantação; 9252 nos managers da frota de runners (métricas sem autenticação, restringir por firewall).

## 5. Balanceadores (HAProxy do GET)

| Balanceador                          | Porta de entrada | Destino                       | Observação                                                                                       |
|--------------------------------------|------------------|-------------------------------|--------------------------------------------------------------------------------------------------|
| Externo (2k ou mais)                 | 443              | VMs GitLab Rails              | TCP ou HTTPS, conforme a documentação GitLab de balanceadores                                    |
| Externo (2k ou mais)                 | 80               | VMs GitLab Rails              | HTTP                                                                                             |
| Externo (2k ou mais)                 | 2222             | VMs GitLab Rails (SSH do Git) | Porta padrão do GET com HAProxy, para não conflitar com o SSH do sistema (22) usado pelo Ansible |
| Interno (3k ou mais)                 | 6432             | VMs PgBouncer                 | Balanceamento interno para o PgBouncer                                                           |
| Interno (3k ou mais, Gitaly Cluster) | 2305             | VMs Praefect                  | Balanceamento interno para o Praefect                                                            |

- Fontes: documentação GitLab de balanceadores e da arquitetura de referência 3k, e documentação do GET (porta 2222).
- Para usar a porta 22 no SSH do Git em ambiente com HAProxy, a documentação do GET prevê um balanceador externo separado. Com o balanceador do cliente no lugar do HAProxy, ver a seção *Balanceador do cliente*.

## 6. Acesso de rede de saída

| Origem       | Destino                                              | Porta           | Finalidade                                                                        |
|--------------|------------------------------------------------------|-----------------|-----------------------------------------------------------------------------------|
| VM do runner | gitlab.com, registry.gitlab.com, *.gitlab-static.net | 443 (HTTPS)     | Comunicação com o projeto do engajamento e download das imagens do pipeline       |
| VM do runner | *.storage.googleapis.com                             | 443 (HTTPS)     | Download de imagens de registry.gitlab.com, conforme a documentação do GitLab.com |
| VM do runner | Todas as VMs do inventário                           | SSH (padrão 22) | Coleta de fatos, execução do GET, verificação e rotinas de dia 2                  |
| VM do runner | URL externa da instância                             | 443 (HTTPS)     | Health check do GET e verificação pós-implantação                                 |

| Origem                                                                                                | Destino                                                                                                                        | Porta                        | Finalidade                                                                                                            |
|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Todas as VMs                                                                                          | packages.gitlab.com                                                                                                            | 443 (HTTPS)                  | Linux package e chave GPG do repositório oficial                                                                      |
| Todas as VMs                                                                                          | Repositórios de pacotes do sistema operacional                                                                                 | Conforme o repositório       | Pacotes instalados pelo GET (por exemplo curl, ca-certificates, tzdata)                                               |
| VMs de balanceador e OpenSearch                                                                       | Docker Hub (docker.io)                                                                                                         | 443 (HTTPS)                  | Imagem do HAProxy executada pelo GET; o GET também instala o Docker Engine nessas VMs                                 |
| VMs Gitaly e Praefect                                                                                 | pool.ntp.org ou servidor NTP interno                                                                                           | —                            | Verificação de sincronização de horário                                                                               |
| Runner do provisionamento (runners hospedados do GitLab.com, padrão, ou runner indicado pelo cliente) | API da AWS ou do Azure; API do projeto do engajamento no GitLab.com (estado do Terraform); registro dos providers do Terraform | 443 (HTTPS)                  | Plano, aplicação e destruição da infraestrutura criada pelo pipeline                                                  |
| Managers da frota de runners                                                                          | URL externa da instância; packages.gitlab.com; repositórios do sistema operacional                                             | 443 (HTTPS)                  | Registro e comunicação com a instância; pacote gitlab-runner; Docker Engine do sistema operacional (executor Docker)  |
| Manager do docker-autoscaler (AWS)                                                                    | API da AWS (Auto Scaling e EC2) e SSH até as instâncias do grupo                                                               | 443 (HTTPS); 22              | Plugin fleeting: escala o Auto Scaling Group e conecta às instâncias; credenciais pelo perfil de instância do manager |
| Agente GitLab para Kubernetes (clusters do cliente)                                                   | URL externa da instância, caminho <code>/-/kubernetes-agent/</code>                                                            | 443 (WebSocket seguro)       | Conexão do agente ao KAS pelo balanceador da instância                                                                |
| Runner do engajamento (agentes)                                                                       | API server de cada cluster com agente; charts.gitlab.io                                                                        | Porta da API do cluster; 443 | Instalação do agente pelo Helm                                                                                        |

- A documentação do GitLab.com lista, para liberação em firewall, [gitlab.com](https://gitlab.com), [gitlab-static.net](https://gitlab-static.net), [gitlab.io](https://gitlab.io) e [gitlab.net](https://gitlab.net), e, para download de imagens de registry.gitlab.com, [storage.googleapis.com](https://storage.googleapis.com) e [cdn.registry.gitlab-static.net](https://cdn.registry.gitlab-static.net).
- Proxy corporativo: configurado no serviço do runner e no executor Docker (HTTPS\_PROXY e NO\_PROXY); o GET aceita proxy por variáveis de ambiente nas VMs.

- Por padrão, o GET configura atualizações automáticas de segurança do sistema operacional nas VMs (unattended-upgrades ou dnf-automatic), sem reinicialização automática.
- O runner não recebe conexões: nenhuma porta de entrada é aberta na VM do runner.

## 7. Infraestrutura criada pelo pipeline (AWS ou Azure)

| Item                             | Especificação                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Obrigatório                                      |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| Conta e identidade na AWS        | Usuário ou role IAM dedicado ao engajamento, com access key cadastrada como variável protegida com escopo do ambiente, e permissão para criar os recursos do módulo AWS do GitLab Environment Toolkit na conta: VMs, rede (quando criada), grupos de segurança, roles IAM e buckets (quando criados). O módulo consulta a chave KMS gerenciada <code>alias/aws/s3</code> : a identidade precisa de leitura dessa chave. Políticas da organização (SCP do AWS Organizations) aplicadas à conta não podem negar essas ações. A lista exata de permissões é conferida no Assessment com a documentação do GET (a Pointer não publica política mínima). Revogada no encerramento. | Condicional: infraestrutura criada na AWS        |
| Assinatura e identidade no Azure | Service principal com permissão no resource group existente informado no formulário, cadastrado como variáveis protegidas com escopo do ambiente. O pipeline não registra resource providers: os usados pelo módulo precisam estar registrados na assinatura. Azure Policy do resource group que limite tipos de recurso ou SKUs precisa permitir os usados pelo módulo (VMs dos tipos escolhidos, rede virtual, NAT gateway, IPs públicos Standard, grupos de segurança e Application Security Groups). Revogado no encerramento.                                                                                                                                            | Condicional: infraestrutura criada no Azure      |
| Região e cotas                   | Região definida no formulário (por exemplo <code>sa-east-1</code> ou <code>brazilsouth</code> ), com cotas da conta suficientes para os recursos da arquitetura: vCPU das famílias de instância escolhidas, endereços IP públicos e balanceadores. Na AWS, com rede nova e subnets privadas, o módulo do GET cria um NAT gateway com um Elastic IP para cada par de subnets pública e privada; a cota padrão de Elastic IPs da região limita quantos ambientes cabem na mesma conta.                                                                                                                                                                                          | Condicional: infraestrutura criada pelo pipeline |
| Rede na AWS                      | Rede nova (CIDR /24 ou maior, do qual o pipeline deriva as subnets; 1 a 6 subnets públicas e até o mesmo número de subnets privadas) ou VPC e subnets existentes. CIDRs com acesso às VMs (rede interna e a do runner; <code>0.0.0.0/0</code> gera alerta). Com subnets privadas, grupo de segurança de acesso para o runner do engajamento e, com GitLab Geo, para o outro site.                                                                                                                                                                                                                                                                                             | Condicional: infraestrutura criada na AWS        |
| Rede no Azure                    | Resource group existente; faixa da rede virtual e da subnet (opcional) e IP público nas VMs (padrão: sim).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Condicional: infraestrutura criada no Azure      |

| Item                               | Especificação                                                                                                                                                                                                                                                         | Obrigatório                                      |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| Tipos de instância e disco         | Menor tipo da lista do pipeline que atende vCPU e memória do papel (AWS: c7i, m7i, r7i; Azure: Fsv2, Dasv5, Easv5) ou tipo definido no formulário por papel; disco de 100 GB por VM (padrão; mínimo 30, abaixo de 100 gera alerta).                                   | Não                                              |
| Object storage                     | AWS: buckets criados pelo pipeline (padrão) ou existentes. Azure: serviço S3-compatível existente (os containers Blob criados pelo módulo do GET não são S3-compatíveis, e a validação recusa essa combinação).                                                       | Condicional: 2k ou mais, ou object storage em 1k |
| Tags                               | Tags de custo e governança exigidas pelo cliente, aplicadas a todos os recursos criados, somadas às tags da plataforma ( <b>gerenciado-por</b> e <b>ps-ambiente</b> ).                                                                                                | Não                                              |
| Runner com rota para a rede criada | O Terraform roda em runners hospedados do GitLab.com (padrão; usa só a API da nuvem) ou em runner indicado pelo cliente. A implantação roda no runner do engajamento, instalado na rede criada ou com rota até os endereços internos dela.                            | Condicional: infraestrutura criada pelo pipeline |
| DNS, certificados e balanceador    | Continuam com o cliente: o pipeline não cria registros DNS, certificados nem o balanceador do cliente.                                                                                                                                                                | Condicional: infraestrutura criada pelo pipeline |
| Estado do Terraform e destruição   | Estado no GitLab-managed Terraform state do projeto do engajamento, com trava durante cada execução; transferência ao cliente definida no encerramento. A destruição só é executada com decisão registrada por merge request; bucket com objetos impede a destruição. | Condicional: infraestrutura criada pelo pipeline |

- Com infraestrutura criada pelo pipeline, as VMs de *Máquinas virtuais por arquitetura de referência* não são provisionadas pelo cliente.
- Criação de infraestrutura no Google Cloud: sob consulta. VMs existentes no Google Cloud entram como infraestrutura existente, com os requisitos das demais seções.

## 8. Balanceador do cliente (no lugar do HAProxy do GET)

| Item | Especificação                                                                                                                                                                                                                                                        | Obrigatório                         |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| Modo | Balanceador externo do cliente em TLS passthrough: encaminha TCP 443 (HTTPS) e a porta do SSH do Git aos nós GitLab Rails, sem terminar TLS; o NGINX de cada nó serve HTTPS com o certificado do cliente. Exige certificado do cliente e 2 ou mais nós GitLab Rails. | Condicional: balanceador do cliente |

| Item                 | Especificação                                                                                                                                                                                                                                                    | Obrigatório                         |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| Health check         | Configurado pelo cliente. A documentação GitLab orienta usar o readiness check ( <code>/-/readiness</code> ) como health check do balanceador; a allowlist de monitoramento dos nós precisa incluir o balanceador (o GET usa <code>0.0.0.0/0</code> por padrão). | Condicional: balanceador do cliente |
| WebSocket            | Segundo a documentação GitLab, o balanceador precisa suportar WebSocket; em TLS passthrough (TCP), o tráfego chega aos nós sem alteração.                                                                                                                        | Condicional: balanceador do cliente |
| CIDRs do balanceador | CIDRs de origem do balanceador, configurados como confiáveis no NGINX dos nós GitLab Rails para o endereço real do usuário; sem eles, a validação emite alerta.                                                                                                  | Condicional: balanceador do cliente |
| DNS                  | URL externa, nome do Container Registry (quando habilitado) e domínio wildcard do GitLab Pages (quando habilitado) apontando para o balanceador; com GitLab Pages em HTTPS, os nós GitLab Rails atendem o domínio do Pages na 443 com o certificado wildcard.    | Condicional: balanceador do cliente |
| Verificação          | O pipeline não configura nem verifica o balanceador; a verificação pós-implantação testa a página de login pela URL externa e o roteamento do domínio do Pages nos nós.                                                                                          | —                                   |

- Sob consulta: TLS terminado no balanceador do cliente (nós GitLab Rails em HTTP) e balanceador interno do cliente no lugar do HAProxy interno (3k ou mais).
- Sem balanceador interno, o Gitaly chama a API interna pela URL externa: com autoridade certificadora não pública, a cadeia da AC emissora é entregue (credencial *Cadeia da autoridade certificadora da URL externa*).

## 9. GitLab Geo (dois sites)

- Dois ambientes no mesmo projeto do engajamento, um primário e um secundário, cada um com a sua arquitetura, a mesma versão GitLab e prefixos de nomes diferentes.
- Licença GitLab Premium ou GitLab Ultimate no site primário; o secundário usa a licença do primário.
- Object storage nos dois sites ou em nenhum.
- Rede entre os sites para a replicação do banco e dos repositórios e para o acesso HTTPS do secundário à URL do primário; com autoridade certificadora não pública, a cadeia da AC do primário é instalada pelo pipeline nos nós do secundário.
- Runner do engajamento com acesso por SSH às VMs dos dois sites, com a mesma chave.
- Senha do PostgreSQL com o mesmo valor nos dois sites (o GET a usa também como senha do usuário de replicação), inclusive em 1k.
- O pipeline configura a replicação a partir do site primário; failover e acompanhamento da replicação não são automatizados nesta versão. GitLab Geo em Kubernetes: sob consulta.

## 10. Frota de runners do cliente

| Item                                   | Especificação                                                                                                                                                                                                                                                                                                                                       | Obrigatório                           |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| Modalidades disponíveis                | VMs Linux com executor Docker (uma ou mais VMs; Docker Engine do sistema operacional instalado pelo pipeline em Debian e Ubuntu, existente nas demais distribuições); docker-autoscaler na AWS (um manager e Auto Scaling Group existente e dedicado); Kubernetes pelo chart oficial gitlab-runner (cluster existente ou EKS criado pelo pipeline). | Condicional: frota contratada         |
| Sob consulta                           | Executor shell (jobs direto no host, sem isolamento; a validação emite alerta) e docker-autoscaler no Azure (VM Scale Set).                                                                                                                                                                                                                         | —                                     |
| Token de API                           | Token de acesso com escopos <code>create_runner</code> e <code>manage_runner</code> ; de administrador da instância para runners de instância ou de Owner do grupo para runners de grupo. Os runners são criados na instância pela API e registrados com o token devolvido, que não vai para artefato nem log.                                      | Condicional: frota contratada         |
| VMs dos managers                       | Sistema operacional Linux com acesso por SSH e sudo sem senha a partir do runner do engajamento, com o usuário de implantação; saída para a URL da instância, packages.gitlab.com e os repositórios do sistema operacional.                                                                                                                         | Condicional: VMs ou docker-autoscaler |
| Auto Scaling Group (docker-autoscaler) | Grupo existente e dedicado à frota; imagem das instâncias com o Docker Engine pronto ou comando de prontidão informado (por exemplo <code>cloud-init status --wait</code> ); credenciais da AWS pelo perfil de instância do manager (o pipeline não grava credenciais de nuvem).                                                                    | Condicional: docker-autoscaler        |
| Cluster (Kubernetes)                   | Kubeconfig com permissão para criar o namespace (padrão <code>gitlab-runner</code> ), Secrets e o release Helm; no EKS criado pelo pipeline, o acesso vem do estado do Terraform. Nós com acesso à URL da instância.                                                                                                                                | Condicional: Kubernetes               |
| Governança                             | Por runner: escopo (instância, grupo ou projeto) e alvo, tags, execução sem tag, proteção, bloqueio (projeto), timeout máximo, concorrência, imagem padrão e modo privilegiado (alerta). Métricas na porta 9252, sem autenticação (restringir por firewall).                                                                                        | Condicional: frota contratada         |
| CA da instância                        | Com autoridade certificadora não pública, a cadeia da AC da URL da instância, instalada nos managers e no namespace do runner.                                                                                                                                                                                                                      | Condicional: AC não pública           |

## 11. Agentes GitLab para Kubernetes

| Item                  | Especificação                                                                                                                                                                                                                                                          | Obrigatório                      |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| KAS na instância      | Habilitado por padrão; publicado pela URL externa ( <code>/-/kubernetes-agent/</code> ). Com 2 ou mais nós GitLab Rails, TCP 8155 liberada entre eles.                                                                                                                 | Condicional: agentes contratados |
| Token de API          | Token de acesso com escopo <code>api</code> de usuário Maintainer dos projetos de configuração dos agentes; o grupo desses projetos precisa existir (o projeto é criado quando não existe).                                                                            | Condicional: agentes contratados |
| Acesso a cada cluster | Kubeconfig com permissão para criar o namespace do agente, o Secret do token e o release Helm, inclusive as permissões de escopo de cluster que o chart cria para o agente (padrão do chart: cluster-admin, com alerta da validação; ClusterRole do cliente opcional). | Condicional: agentes contratados |
| Rede                  | Agente com saída para a URL externa da instância na 443 (WebSocket seguro); nós do cluster com acesso ao registry da imagem do agente; runner do engajamento com acesso ao API server do cluster e a charts.gitlab.io.                                                 | Condicional: agentes contratados |
| Acesso de CI/CD       | Grupos e projetos autorizados a usar o cluster nos pipelines e modo de acesso (com as permissões do agente ou por impersonação do job de CI/CD).                                                                                                                       | Condicional: agentes contratados |
| CA da instância       | Com autoridade certificadora não pública, a cadeia da AC da URL externa, para o agente confiar no KAS.                                                                                                                                                                 | Condicional: AC não pública      |

## 12. Monitoramento: Prometheus e Grafana gerenciado (sob consulta)

| Item                                           | Especificação                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Obrigatório                     |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| Prometheus                                     | Do Linux package, no nó de monitoramento da arquitetura (2k ou mais), com retenção definida no formulário (padrão 30 dias); coleta dos exporters dos nós nas portas da tabela oficial. A verificação pós-implantação consulta o Prometheus (9090) no nó de monitoramento. A arquitetura 1k não tem nó de monitoramento.                                                                                                                                                                        | Condicional: 2k ou mais         |
| Grafana gerenciado pela Pointer (sob consulta) | Grafana OSS em versão fixa no nó de monitoramento (2k ou mais), com o Prometheus da instância como fonte de dados: host próprio (por exemplo <code>grafana.&lt;domínio&gt;</code> ) com registro DNS para o nó de monitoramento, certificado e chave desse host, porta da URL (padrão 443) liberada para os usuários, saída do nó de monitoramento para <code>apt.grafana.com</code> ou <code>rpm.grafana.com</code> e, para os dashboards da GitLab, do runner para <code>gitlab.com</code> . | Condicional: Grafana contratado |

| Item                                                | Especificação                                                                                                                                                                                                                                                                                                                                                                                                            | Obrigatório                                          |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| Login pela instância GitLab (Grafana, sob consulta) | Aplicação OAuth criada na instância pela Pointer (redirect <code>https://&lt;host do Grafana&gt;/login/gitlab</code> ; escopos <code>openid</code> , <code>email</code> e <code>profile</code> ) e grupos da instância com acesso e com papel de administrador ou editor no Grafana. Em instância nova, o login pela instância GitLab é habilitado numa segunda execução da implantação, depois da criação da aplicação. | Condicional: Grafana com login pela instância GitLab |

## 13. Entrega das credenciais

As credenciais listadas neste documento são cadastradas como **variáveis de CI/CD protegidas** no projeto do engajamento, com escopo restrito ao ambiente (por exemplo `producao`), e do tipo arquivo para chaves, certificados e arquivo de licença. Os valores **nunca são enviados por e-mail, chat, issue ou arquivo**; um valor exposto em qualquer desses canais é revogado e substituído. A forma de cadastro de cada valor é combinada no kick-off. No encerramento do engajamento, as variáveis são revogadas.

Restrição da plataforma GitLab para o mascaramento de variáveis (documentação oficial de variáveis de CI/CD): só pode ser mascarado um valor em uma única linha, sem espaços e com 8 ou mais caracteres, e a opção de ocultar o valor (*hidden*) só pode ser definida na criação da variável. Conteúdos de várias linhas (chave SSH, certificados, chaves PEM, arquivo de licença) não atendem a essa condição: para eles, a proteção é a variável protegida, com escopo do ambiente, do tipo arquivo. Senhas e tokens em uma linha devem atender à condição para serem mascarados.

O pipeline recusa valores que contenham a sequência `#[` e valida, antes de cada execução, se todas as variáveis exigidas existem e se as do tipo arquivo foram cadastradas como arquivo. Os arquivos gerados pelo pipeline nunca contêm credenciais: os valores são lidos das variáveis somente durante a execução, no runner da rede do cliente, e o as-built registra apenas os nomes.

As credenciais de nuvem (AWS ou Azure) e os tokens de API da frota de runners e dos agentes seguem a mesma regra: variáveis protegidas com escopo do ambiente (ou do ambiente do componente da frota e dos agentes), revogadas no encerramento. A falta delas aparece na execução do Terraform ou do componente correspondente. O estado do Terraform usa a credencial do próprio job no projeto do engajamento, sem variável adicional.

## 14. Como a Pointer usa essas informações

As informações do formulário se tornam a **configuração do engajamento**, versionada no repositório do projeto do engajamento e alterada somente por merge request revisado por outro consultor. Credenciais não entram nesse repositório.

A cada alteração, o pipeline **valida a configuração automaticamente**, em runner hospedado, sem credenciais e sem acesso à rede do cliente: arquitetura e papéis, quantidade de VMs por papel, versão e edição, URL externa, TLS, object storage e recursos opcionais. A mesma etapa gera os arquivos do GitLab Environment Toolkit e a lista exata das credenciais exigidas para essa configuração.

Antes de qualquer alteração no ambiente, a **verificação prévia (preflight)** roda contra as VMs reais, a partir do runner na rede do cliente, em modo somente leitura: coleta sistema operacional, CPU, memória, discos, horário e DNS de cada VM e compara com a arquitetura de referência e com a matriz de sistemas operacionais. O relatório por servidor, com erros e alertas, fica anexado ao pipeline. A implantação repete essa verificação e não começa se houver qualquer erro; alertas aceitos são registrados no registro de decisões do engajamento. Cada implantação exige aprovação de uma pessoa diferente de quem a executa, e só uma execução por ambiente acontece de cada vez.

Quando o pipeline cria a infraestrutura, a mesma configuração gera o módulo Terraform em runner hospedado, sem credenciais; o plano, com o resumo das ações, é revisado antes da aplicação, que exige a mesma aprovação. Os endereços internos de cada papel são lidos do estado do Terraform por todos os jobs seguintes.

## 15. Critérios de aceite

- Todas as checagens obrigatórias da verificação pós-implantação com resultado OK.
- Acesso pela URL externa com certificado válido.
- Login LDAP e envio de e-mail de teste validados com o cliente, quando habilitados.
- Backup agendado executado ao menos uma vez com sucesso, quando habilitado.
- Runners da frota online na instância e agentes GitLab para Kubernetes conectados, quando contratados.

## 16. Credenciais que o cliente entrega à Pointer

Nenhum valor secreto é enviado por e-mail, chat, issue ou arquivo. Cada credencial é cadastrada como variável de CI/CD protegida no projeto do engajamento, com escopo do ambiente, e revogada no encerramento.

| Credencial                                             | Finalidade                                                                                                                 | Permissões                                                                                                     | Formato e validade                                                                                                                                        | Obrigatório                                                                |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| <b>Chave SSH do usuário de implantação</b>             | Acesso do runner às VMs para a verificação prévia, a execução do GET, a verificação pós-implantação e as rotinas de dia 2. | Usuário presente em todas as VMs, com sudo sem senha; a chave pública correspondente autorizada nesse usuário. | Chave privada OpenSSH (arquivo)<br>Até o encerramento do engajamento, quando a variável é revogada.                                                       | Sim                                                                        |
| <b>Certificado TLS e chave privada do host externo</b> | Entrada HTTPS da instância pela URL externa.                                                                               | Certificado com SAN do host externo e dos hostnames adicionais usados.                                         | Dois arquivos PEM: certificado com os intermediários da cadeia e chave privada<br>Validade do certificado emitido; a variável é revogada no encerramento. | Condicional: certificado do cliente (padrão; dispensado com Let's Encrypt) |
| <b>Activation code ou arquivo de licença</b>           | Ativação da assinatura GitLab Premium ou GitLab Ultimate na instância.                                                     | Assinatura ativa no portal de clientes da GitLab (Customers Portal).                                           | Activation code (texto em uma linha) ou arquivo <code>.gitlab-license</code><br>Vigência da assinatura; a variável é revogada no encerramento.            | Sim                                                                        |
| <b>Access key e secret key do object storage</b>       | Gravação e leitura dos objetos e dos backups nos buckets do ambiente.                                                      | Acesso aos buckets listados neste documento.                                                                   | Dois valores de texto em uma linha<br>Continuam em uso pela instância entregue; a variável do projeto do engajamento é revogada no encerramento.          | Condicional: object storage (obrigatório a partir de 2k)                   |

| Credencial                                                  | Finalidade                                                                   | Permissões                                                                         | Formato e validade                                                                                                            | Obrigatório                                     |
|-------------------------------------------------------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| <b>Certificado wildcard e chave privada do GitLab Pages</b> | HTTPS dos sites publicados pelo GitLab Pages.                                | Certificado wildcard do domínio do Pages.                                          | Dois arquivos PEM: certificado e chave privada<br><br>Validade do certificado emitido; a variável é revogada no encerramento. | Condicional: GitLab Pages com HTTPS             |
| <b>Senha da conta de bind LDAP</b>                          | Consulta ao diretório para autenticação dos usuários.                        | Conta de bind (DN) informada no formulário.                                        | Texto em uma linha<br><br>Continua em uso pela instância entregue; a variável é revogada no encerramento.                     | Condicional: LDAP com conta de bind             |
| <b>Senha do usuário SMTP</b>                                | Envio de e-mails da instância.                                               | Usuário SMTP informado no formulário, autorizado a enviar pelo remetente definido. | Texto em uma linha<br><br>Continua em uso pela instância entregue; a variável é revogada no encerramento.                     | Condicional: SMTP com autenticação              |
| <b>Senha do cluster de busca externo</b>                    | Conexão da busca avançada ao cluster Elasticsearch ou OpenSearch do cliente. | Usuário informado no formulário.                                                   | Texto em uma linha<br><br>Continua em uso pela instância entregue; a variável é revogada no encerramento.                     | Condicional: busca avançada externa com usuário |

| Credencial                                                       | Finalidade                                                                                                                                                                                                                                                                            | Permissões                                     | Formato e validade                                                                                                                                                                                            | Obrigatório                                                               |
|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| <b>Senha inicial do usuário root</b>                             | Primeiro acesso administrativo à instância. Definida no kick-off (cliente ou Pointer) e cadastrada como variável protegida.                                                                                                                                                           | Administrador da instância GitLab.             | Texto em uma linha; para mascaramento, sem espaços e com 8 ou mais caracteres; sem a sequência <b>#f</b><br><br>Trocada na entrega (pendência registrada no as-built); a variável é revogada no encerramento. | Sim                                                                       |
| <b>Senhas e token internos (2k ou mais)</b>                      | Senha do usuário gitlab no PostgreSQL, senha do Redis e token de autenticação do Gitaly. Definidos no kick-off (cliente ou Pointer) e cadastrados como variáveis protegidas. Com GitLab Geo, a senha do PostgreSQL é também a senha de replicação e tem o mesmo valor nos dois sites. | Uso interno entre os componentes da instância. | Texto em uma linha; para mascaramento, sem espaços e com 8 ou mais caracteres; sem a sequência <b>#f</b><br><br>Continuam em uso pela instância entregue; as variáveis são revogadas no encerramento.         | Condicional: 2k ou mais; com GitLab Geo, senha do PostgreSQL também em 1k |
| <b>Senhas do PostgreSQL em alta disponibilidade (3k ou mais)</b> | Senha da API REST do Patroni, senha do usuário do Consul no PostgreSQL e senha do PgBouncer. Definidas no kick-off (cliente ou Pointer) e cadastradas como variáveis protegidas.                                                                                                      | Uso interno entre os componentes da instância. | Texto em uma linha; para mascaramento, sem espaços e com 8 ou mais caracteres; sem a sequência <b>#f</b><br><br>Continuam em uso pela instância entregue; as variáveis são revogadas no encerramento.         | Condicional: 3k ou mais                                                   |

| Credencial                                                                                                                                                      | Finalidade                                                                                                                                                                             | Permissões                                                                                                                                                               | Formato e validade                                                                                                                                                                                        | Obrigatório                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| <b>Tokens e senha do Gitaly Cluster (3k ou mais)</b>                                                                                                            | Token externo e token interno do Praefect e senha do banco do Praefect. Definidos no kick-off (cliente ou Pointer) e cadastrados como variáveis protegidas.                            | Uso interno entre os componentes da instância.                                                                                                                           | Texto em uma linha; para mascaramento, sem espaços e com 8 ou mais caracteres; sem a sequência <code>#f</code> .<br>Continuam em uso pela instância entregue; as variáveis são revogadas no encerramento. | Condicional: 3k ou mais com Gitaly Cluster        |
| <b>Cadeia da autoridade certificadora da URL externa</b>                                                                                                        | Confiança dos nós com Linux package, dos runners da frota, dos agentes e do site secundário GitLab Geo na URL externa, quando o certificado não é de autoridade certificadora pública. | Cadeia pública da AC emissora (não é segredo); cadastrada como variável do tipo arquivo com escopo do ambiente.                                                          | Arquivo PEM<br>Validade da AC; a variável é revogada no encerramento.                                                                                                                                     | Condicional: autoridade certificadora não pública |
| <b>Credencial da conta AWS ( <code>AWS_ACCESS_KEY_ID</code> e <code>AWS_SECRET_ACCESS_KEY</code> )</b>                                                          | Plano, aplicação e destruição da infraestrutura criada pelo pipeline na AWS.                                                                                                           | Identidade IAM dedicada ao engajamento, com permissão para criar os recursos do GitLab Environment Toolkit na conta (seção <i>Infraestrutura criada pelo pipeline</i> ). | Dois valores de texto em uma linha<br>Até o encerramento; revogada pelo cliente.                                                                                                                          | Condicional: infraestrutura criada na AWS         |
| <b>Service principal do Azure ( <code>ARM_CLIENT_ID</code>, <code>ARM_CLIENT_SECRET</code>, <code>ARM_TENANT_ID</code> e <code>ARM_SUBSCRIPTION_ID</code> )</b> | Plano, aplicação e destruição da infraestrutura criada pelo pipeline no Azure.                                                                                                         | Permissão no resource group informado no formulário.                                                                                                                     | Quatro valores de texto em uma linha<br>Até o encerramento; revogado pelo cliente.                                                                                                                        | Condicional: infraestrutura criada no Azure       |
| <b>Token de API da frota de runners ( <code>PS_RUNNER_TOKEN_API</code> )</b>                                                                                    | Criação, consulta, recriação e remoção dos runners da frota na instância.                                                                                                              | Escopos <code>create_runner</code> e <code>manage_runner</code> ; usuário administrador (runners de instância) ou Owner do grupo (runners de grupo).                     | Texto em uma linha<br>Até o encerramento; revogado pelo cliente.                                                                                                                                          | Condicional: frota de runners                     |

| Credencial                                                               | Finalidade                                                                                       | Permissões                                                                                                                                                             | Formato e validade                                                                                                        | Obrigatório                                    |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| <b>Chave SSH dos managers da frota</b>                                   | Instalação e configuração do GitLab Runner nas VMs da frota (VMs e docker-autoscaler).           | Usuário de implantação com sudo sem senha nas VMs dos managers.                                                                                                        | Chave privada OpenSSH (arquivo)<br>Até o encerramento do engajamento, quando a variável é revogada.                       | Condicional: frota em VMs ou docker-autoscaler |
| <b>Kubeconfig dos clusters da frota e dos agentes</b>                    | Instalação do chart do GitLab Runner e do agente GitLab para Kubernetes nos clusters do cliente. | Conta de serviço dedicada, com permissão para criar namespace, Secrets e o release Helm (seções <i>Frota de runners do cliente e Agentes GitLab para Kubernetes</i> ). | Arquivo kubeconfig<br>Até o encerramento; revogado com o administrador do cluster.                                        | Condicional: frota em Kubernetes ou agentes    |
| <b>Token de API dos agentes ( PS_AGENTES_TOKEN_API )</b>                 | Projeto de configuração, config.yaml, registro, tokens e consulta das conexões dos agentes.      | Escopo <code>api</code> ; usuário Maintainer dos projetos de configuração dos agentes.                                                                                 | Texto em uma linha<br>Até o encerramento; revogado pelo cliente.                                                          | Condicional: agentes GitLab para Kubernetes    |
| <b>Certificado TLS e chave privada do host do Grafana (sob consulta)</b> | HTTPS do Grafana gerenciado pela Pointer.                                                        | Certificado com SAN do host do Grafana.                                                                                                                                | Dois arquivos PEM: certificado e chave privada<br>Validade do certificado emitido; a variável é revogada no encerramento. | Condicional: Grafana gerenciado (sob consulta) |

## 17. Informações a enviar

Informações sem sigilo, devolvidas pelo cliente antes da reunião de prontidão. Os campos marcados como obrigatórios são conferidos pela validação automática do pipeline.

### Identificação e contatos

| Informação                            | Exemplo       | Obrigatório | Observação |
|---------------------------------------|---------------|-------------|------------|
| <b>Denominação oficial do cliente</b> | Órgão Exemplo | Sim         |            |

| Informação                                     | Exemplo                | Obrigatório | Observação                                                                                               |
|------------------------------------------------|------------------------|-------------|----------------------------------------------------------------------------------------------------------|
| Sigla do cliente                               | exemplo                | Sim         | Minúsculas, números e hífen; até 40 caracteres.                                                          |
| Número do contrato, pedido ou ordem de serviço | Contrato 12/2026       | Não         |                                                                                                          |
| Nome do ambiente                               | producao               | Sim         | Minúsculas, números e hífen (por exemplo homologacao, producao). Cada ambiente tem configuração própria. |
| Patrocinador                                   | Nome, cargo, e-mail    | Sim         | Decisões de escopo, prioridade e aceite.                                                                 |
| Ponto focal técnico                            | Nome, e-mail, telefone | Sim         | Pré-requisitos, acessos, janelas de mudança e validação funcional.                                       |
| Contatos de infraestrutura, rede e segurança   | Nome e e-mail por área | Sim         | VMs, DNS, certificados, firewall e contas de serviço.                                                    |
| Aprovador das execuções em produção            | Nome e e-mail          | Sim         | No projeto do engajamento, cada implantação é aprovada por pessoa diferente de quem executa.             |
| Janela de manutenção                           | Sábados, 22h às 2h     | Sim         |                                                                                                          |

## Plataforma GitLab

| Informação             | Exemplo                       | Obrigatório | Observação                                                                                                                                          |
|------------------------|-------------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Versão GitLab          | 19.4.1                        | Sim         | Versão exata no formato X.Y.Z, 16.0.0 ou superior; acima da última versão proposta para o sistema operacional escolhido, o preflight registra erro. |
| Edição                 | Enterprise Edition            | Não         | Enterprise Edition (padrão) ou FIPS. Community Edition não é aceita.                                                                                |
| URL externa            | https://gitlab.cliente.gov.br | Sim         | https:// seguido do host, sem caminho.                                                                                                              |
| Forma de licenciamento | Activation code               | Não         | Activation code (padrão; ativação online) ou arquivo de licença (offline).                                                                          |
| Porta SSH do Git       | 2222                          | Não         | Padrão do GET: 22 em nó único e 2222 com o HAProxy (2k ou mais).                                                                                    |

## Dimensionamento e arquitetura

| Informação                                        | Exemplo                     | Obrigatório | Observação |
|---------------------------------------------------|-----------------------------|-------------|------------|
| Número de usuários atual e projeção de 1 a 3 anos | 1.800 hoje; 3.000 em 2 anos | Sim         |            |

| Informação                                           | Exemplo                                                 | Obrigatório                             | Observação                                                                                                                |
|------------------------------------------------------|---------------------------------------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Carga medida (RPS)                                   | Relatório do GitLab Performance Tool ou análise de logs | Condicional: instância GitLab existente |                                                                                                                           |
| Uso intenso de monorepos, CI/CD, pacotes ou registry | Monorepo de 8 GB; 500 pipelines por dia                 | Sim                                     |                                                                                                                           |
| Necessidade de alta disponibilidade                  | Sim                                                     | Sim                                     | A documentação GitLab associa alta disponibilidade às arquiteturas a partir de 3.000 usuários.                            |
| Arquitetura de referência                            | 3k                                                      | Sim                                     | 1k, 2k, 3k, 5k, 10k, 25k ou 50k; definida no Assessment.                                                                  |
| Modo do Gitaly                                       | Gitaly Cluster                                          | Condicional: 3k ou mais                 | Gitaly Cluster com Praefect (padrão) ou Gitaly Sharded.                                                                   |
| Prefixo de nomes                                     | gitlab                                                  | Não                                     | Prefixo dos nomes de servidor no inventário e dos buckets; padrão gitlab. Com GitLab Geo, prefixo diferente em cada site. |
| Forma da infraestrutura                              | Criada pelo pipeline na AWS                             | Sim                                     | VMs existentes ou criadas pelo pipeline na AWS ou no Azure (Google Cloud: sob consulta).                                  |

## Servidores e acesso

| Informação                                     | Exemplo                                                      | Obrigatório                                | Observação                                                                                      |
|------------------------------------------------|--------------------------------------------------------------|--------------------------------------------|-------------------------------------------------------------------------------------------------|
| Endereço de cada VM, por papel                 | GitLab Rails: 10.0.9.1, 10.0.9.2, 10.0.9.3                   | Sim                                        | IP ou hostname alcançável pelo runner, para todos os papéis da arquitetura; um endereço por VM. |
| Sistema operacional e versão de cada VM        | Ubuntu 24.04                                                 | Sim                                        | Conforme a tabela de sistemas operacionais aceitos.                                             |
| Usuário SSH de implantação                     | ubuntu                                                       | Sim                                        | Mesmo usuário em todas as VMs, com sudo sem senha.                                              |
| Porta SSH das VMs                              | 22                                                           | Não                                        | Padrão 22.                                                                                      |
| Servidor NTP interno                           | ntp.cliente.gov.br                                           | Condicional: VMs sem acesso a pool.ntp.org | Usado nas verificações de horário do Gitaly e do Praefect.                                      |
| Faixa de IPs e regras de firewall entre as VMs | 10.0.0.0/24                                                  | Condicional: 2k ou mais                    | A partir das tabelas de portas e de balanceadores.                                              |
| Latência medida entre as VMs                   | < 1 ms                                                       | Condicional: 3k ou mais                    | Exigência da documentação GitLab: menor que 5 ms.                                               |
| Proxy de saída                                 | http://proxy.cliente.gov.br:3128; exceções: *.cliente.gov.br | Condicional: saída por proxy               | Configurado no runner e, quando necessário, nas VMs.                                            |

| Informação   | Exemplo                                          | Obrigatório | Observação |
|--------------|--------------------------------------------------|-------------|------------|
| VM do runner | 10.0.0.50, Ubuntu 24.04, Docker Engine instalado | Sim         |            |

## Infraestrutura criada pelo pipeline

| Informação                                        | Exemplo                                                 | Obrigatório                                      | Observação                                                                                                       |
|---------------------------------------------------|---------------------------------------------------------|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Provedor e região                                 | AWS, sa-east-1                                          | Condicional: infraestrutura criada pelo pipeline | AWS ou Azure.                                                                                                    |
| Conta AWS ou assinatura e resource group do Azure | Conta 1234...; resource group rg-gitlab                 | Condicional: infraestrutura criada pelo pipeline | No Azure, resource group existente.                                                                              |
| Rede                                              | Rede nova 10.44.0.0/16, 2 subnets públicas e 2 privadas | Condicional: infraestrutura criada pelo pipeline | AWS: rede nova (CIDR) ou VPC e subnets existentes; Azure: faixa da rede virtual e da subnet (opcional).          |
| CIDRs com acesso às VMs                           | 10.0.0.0/8                                              | Condicional: infraestrutura criada pelo pipeline | Rede interna e a do runner do engajamento.                                                                       |
| Grupos de segurança de acesso (AWS)               | sg-0abc...                                              | Condicional: subnets privadas                    | Entrada do runner do engajamento e, com GitLab Geo, do outro site.                                               |
| Tipos de instância por papel                      | GitLab Rails: m7i.2xlarge                               | Não                                              | Padrão: menor tipo da lista do pipeline que atende a arquitetura.                                                |
| Disco por VM (GB)                                 | 100                                                     | Não                                              | Padrão 100; mínimo 30.                                                                                           |
| Criação dos buckets pelo pipeline                 | Sim                                                     | Não                                              | AWS: padrão sim. Azure: não (object storage S3-compatível existente).                                            |
| Tags de custo e governança                        | centro-de-custo: TI-123                                 | Não                                              | Aplicadas a todos os recursos criados.                                                                           |
| Destino da infraestrutura no encerramento         | Entregue ao cliente                                     | Sim                                              | Entregue ao cliente (transferência do estado do Terraform) ou destruída por decisão registrada em merge request. |

## Balanceador do cliente

| Informação                     | Exemplo                | Obrigatório                         | Observação                                                            |
|--------------------------------|------------------------|-------------------------------------|-----------------------------------------------------------------------|
| Balanceador externo            | Balanceador do cliente | Condicional: 2k ou mais             | HAProxy do GET (padrão) ou balanceador do cliente em TLS passthrough. |
| CIDRs de origem do balanceador | 10.0.0.0/24            | Condicional: balanceador do cliente | Configurados como confiáveis nos nós GitLab Rails.                    |

| Informação          | Exemplo      | Obrigatório                               | Observação                                                    |
|---------------------|--------------|-------------------------------------------|---------------------------------------------------------------|
| Portas encaminhadas | TCP 443 e 22 | Condicional:<br>balanceador<br>do cliente | HTTPS e SSH do Git aos nós GitLab Rails,<br>sem terminar TLS. |

## TLS e DNS

| Informação                                       | Exemplo                                              | Obrigatório                               | Observação                                                    |
|--------------------------------------------------|------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|
| Origem do certificado                            | Certificado do cliente                               | Não                                       | Certificado do cliente (padrão) ou Let's Encrypt.             |
| Autoridade certificadora, SANs e validade        | AC interna;<br>gitlab.cliente.gov.br;<br>até 10/2027 | Condicional:<br>certificado do<br>cliente | SAN obrigatório.                                              |
| E-mail de registro do Let's Encrypt              | infra@cliente.gov.br                                 | Condicional:<br>Let's Encrypt             |                                                               |
| Registros DNS da URL externa (interno e externo) | gitlab.cliente.gov.br<br>→ 10.0.0.5                  | Sim                                       | Apontando para a VM única (1k) ou para o balanceador externo. |

## Object storage

| Informação                      | Exemplo                             | Obrigatório                    | Observação                                                                          |
|---------------------------------|-------------------------------------|--------------------------------|-------------------------------------------------------------------------------------|
| Serviço S3-compatível           | Ceph RGW                            | Condicional: 2k<br>ou mais     | Opcional em 1k.                                                                     |
| Endpoint                        | https://s3.cliente.gov.br           | Condicional:<br>object storage | URL do serviço.                                                                     |
| Região                          | us-east-1                           | Condicional:<br>object storage | Valor aceito pelo serviço.                                                          |
| Endereçamento path style        | Sim                                 | Não                            | Bucket no caminho da URL; o pipeline usa path style quando o campo não é informado. |
| Prefixo dos buckets             | gitlab                              | Não                            | Padrão: prefixo de nomes.                                                           |
| Confirmação dos buckets criados | 10 buckets criados em<br>15/10/2026 | Condicional:<br>object storage | Nomes exatos conforme a tabela de infraestrutura.                                   |

## Recursos opcionais

| Informação           | Exemplo                            | Obrigatório | Observação                                                  |
|----------------------|------------------------------------|-------------|-------------------------------------------------------------|
| GitLab Pages         | Sim; https://pages.cliente.gov.br  | Não         | URL raiz com DNS wildcard; com HTTPS, certificado wildcard. |
| Busca avançada: modo | VMs OpenSearch instaladas pelo GET | Não         | VMs OpenSearch pelo GET ou cluster externo do cliente.      |
|                      |                                    |             |                                                             |

| Informação                                        | Exemplo                                            | Obrigatório                | Observação                                                                                                                                      |
|---------------------------------------------------|----------------------------------------------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Busca avançada: endereços das VMs OpenSearch      | 10.0.11.1, 10.0.11.2, 10.0.11.3                    | Condicional: busca em VMs  | Mínimo 1; abaixo de 3, alerta.                                                                                                                  |
| Busca avançada: URLs e usuário do cluster externo | https://opensearch.cliente.gov.br:9200; gitlab     | Condicional: busca externa | A senha é entregue como credencial.                                                                                                             |
| Escopos da busca global                           | Código, commits e wiki ligados; usuários desligado | Não                        | Código, commits, wiki, itens de trabalho, merge requests, usuários, grupos e títulos de snippets; código, commits e wiki exigem busca avançada. |
| Container Registry                                | https://registry.cliente.gov.br                    | Não                        | Subdomínio coberto pelo certificado ou porta própria (nó único ou balanceador do cliente).                                                      |
| Servidor do agente GitLab para Kubernetes (KAS)   | Habilitado                                         | Não                        | Padrão: habilitado.                                                                                                                             |

## GitLab Geo

| Informação                                    | Exemplo                          | Obrigatório             | Observação                            |
|-----------------------------------------------|----------------------------------|-------------------------|---------------------------------------|
| Papel deste ambiente e ambiente do outro site | Primário; par: producao-rj       | Condicional: GitLab Geo | Um primário e um secundário.          |
| Identificador e nome do site                  | sp; São Paulo                    | Condicional: GitLab Geo | Identificador diferente em cada site. |
| URL interna do site                           | https://gitlab-sp.cliente.gov.br | Não                     | Padrão: URL externa do site.          |

## Frota de runners do cliente

| Informação                                       | Exemplo                                                                       | Obrigatório                      | Observação                                                                                                                                                                                   |
|--------------------------------------------------|-------------------------------------------------------------------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Runners da frota                                 | docker-geral: VMs 10.0.20.1 e 10.0.20.2; escopo instância; tags docker, linux | Condicional: frota contratada    | Por runner: nome, modalidade (VM, docker-autoscaler na AWS ou Kubernetes), escopo e alvo, tags, execução sem tag, proteção, timeout máximo, concorrência, imagem padrão e modo privilegiado. |
| Auto Scaling Group e limites (docker-autoscaler) | asg-runners; até 10 instâncias; 1 job por instância; cloud-init status --wait | Condicional: docker-autoscaler   | Grupo existente e dedicado; comando de prontidão quando a imagem não sobe com o Docker Engine pronto.                                                                                        |
| Cluster, contexto e namespace (Kubernetes)       | cliente-prd; gitlab-runner                                                    | Condicional: frota em Kubernetes | Ou o ambiente com EKS criado pelo pipeline.                                                                                                                                                  |

| Informação              | Exemplo | Obrigatório | Observação                         |
|-------------------------|---------|-------------|------------------------------------|
| Versão do GitLab Runner | 19.4.1  | Não         | Versão fixa do pacote ou do chart. |

## Agentes GitLab para Kubernetes

| Informação      | Exemplo                                                                         | Obrigatório                            | Observação                                                                                               |
|-----------------|---------------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------------------------------------------------------------|
| Agentes         | producao: projeto<br>plataforma/kubernetes-<br>agentes; contexto<br>cliente-prd | Condicional:<br>agentes<br>contratados | Por agente: nome, projeto de<br>configuração, cluster e contexto,<br>namespace e ClusterRole (opcional). |
| Acesso de CI/CD | Grupo apps; projeto<br>plataforma/infra;<br>impersonação do job                 | Condicional:<br>agentes<br>contratados | Grupos e projetos autorizados e modo de<br>acesso.                                                       |

## LDAP / Active Directory

| Informação                          | Exemplo                                                | Obrigatório          | Observação                                                                                 |
|-------------------------------------|--------------------------------------------------------|----------------------|--------------------------------------------------------------------------------------------|
| Habilitar LDAP                      | Sim                                                    | Não                  |                                                                                            |
| Rótulo exibido na tela de login     | AD Cliente                                             | Condicional:<br>LDAP |                                                                                            |
| Servidor                            | ldap.cliente.gov.br                                    | Condicional:<br>LDAP |                                                                                            |
| Porta                               | 636                                                    | Não                  | Padrão 636.                                                                                |
| Criptografia                        | simple_tls                                             | Não                  | simple_tls (padrão), start_tls ou plain; plain gera alerta (credenciais sem criptografia). |
| Verificar o certificado do servidor | Sim                                                    | Não                  | Padrão: sim.                                                                               |
| Servidor Active Directory           | Sim                                                    | Não                  | Padrão: sim.                                                                               |
| Base DN de usuários                 | OU=Usuarios,DC=cliente,DC=gov,DC=br                    | Condicional:<br>LDAP |                                                                                            |
| Atributo de login                   | sAMAccountName                                         | Condicional:<br>LDAP |                                                                                            |
| Conta de bind (DN)                  | CN=svc-gitlab,OU=Servicos,DC=cliente,DC=gov,DC=br      | Não                  | A senha é entregue como credencial.                                                        |
| Filtro de usuários                  | (memberOf=CN=GitLab,OU=Grupos,DC=cliente,DC=gov,DC=br) | Não                  |                                                                                            |

| Informação                                | Exemplo                                          | Obrigatório | Observação                    |
|-------------------------------------------|--------------------------------------------------|-------------|-------------------------------|
| Base de grupos e grupo de administradores | OU=Grupos,DC=cliente,DC=gov,DC=br; GitLab-Admins | Não         | Sincronização de grupos LDAP. |

## SMTP

| Informação                      | Exemplo                     | Obrigatório          | Observação                          |
|---------------------------------|-----------------------------|----------------------|-------------------------------------|
| Habilitar SMTP                  | Sim                         | Não                  |                                     |
| Servidor e porta                | smtp.cliente.gov.br;<br>587 | Condicional:<br>SMTP |                                     |
| TLS                             | starttls                    | Não                  | starttls (padrão), tls ou nenhum.   |
| Usuário                         | gitlab@cliente.gov.br       | Não                  | A senha é entregue como credencial. |
| Domínio                         | cliente.gov.br              | Não                  |                                     |
| Remetente                       | gitlab@cliente.gov.br       | Condicional:<br>SMTP |                                     |
| Endereço de resposta (reply-to) | noreply@cliente.gov.br      | Não                  |                                     |

## Backup e operação

| Informação                                                                          | Exemplo                                             | Obrigatório                        | Observação                                                                                                    |
|-------------------------------------------------------------------------------------|-----------------------------------------------------|------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Backup agendado                                                                     | Sim                                                 | Não                                | Padrão: habilitado.                                                                                           |
| Horário do backup                                                                   | Diário às 02:00                                     | Não                                | Formato cron de 5 campos; padrão diário às 02:00.                                                             |
| Retenção dos backups locais, em dias                                                | 7                                                   | Não                                | Padrão 7.                                                                                                     |
| RTO e RPO                                                                           | RT0 8 h; RPO 24 h                                   | Sim                                |                                                                                                               |
| Destino externo dos backups                                                         | Bucket de backups replicado em outro site           | Sim                                | Com object storage, os backups vão para o bucket de backups.                                                  |
| Política de atualização de versão                                                   | Trimestral, em janela de manutenção                 | Sim                                |                                                                                                               |
| Monitoramento corporativo existente                                                 | Zabbix                                              | Não                                | O Prometheus instalado pelo GET é o monitoramento incluído; o Grafana gerenciado pela Pointer é sob consulta. |
| Retenção do Prometheus, em dias                                                     | 30                                                  | Não                                | Padrão 30 (2k ou mais).                                                                                       |
| Grafana gerenciado (sob consulta): host, grupos com acesso e grupos administradores | https://grafana.cliente.gov.br;<br>infra; infra/sre | Condicional:<br>Grafana contratado | Host com DNS para o nó de monitoramento e certificado próprio.                                                |

| Informação                       | Exemplo                                                     | Obrigatório | Observação |
|----------------------------------|-------------------------------------------------------------|-------------|------------|
| Requisitos regulatórios de dados | Logs de pipeline e artefatos somente em território nacional | Sim         |            |

## 18. Checklist de prontidão

Itens conferidos antes da execução. "Preflight automático" indica verificação feita pelo pipeline contra o ambiente real; os demais são conferidos na reunião de prontidão ou pelo cliente.

| <input type="checkbox"/> | Item                                                                                                                                                                                                                                                  | Verificado por       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <input type="checkbox"/> | Todas as credenciais exigidas cadastradas como variáveis protegidas do ambiente, com o tipo correto (arquivo para chaves, certificados e licença). Falta ou tipo incorreto: erro.                                                                     | Preflight automático |
| <input type="checkbox"/> | Cada VM acessível por SSH a partir do runner, com o usuário de implantação, sudo sem senha e <code>python3</code> . VM inacessível ou sem fatos coletados: erro.                                                                                      | Preflight automático |
| <input type="checkbox"/> | Sistema operacional de cada VM na matriz: suportado; best effort gera erro, ou alerta com exceção registrada; bloqueado gera erro; Debian 11 gera alerta. Versão GitLab acima da última proposta para o sistema operacional: erro.                    | Preflight automático |
| <input type="checkbox"/> | CPU x86_64 ou aarch64 (aarch64: alerta; Oracle Linux em aarch64: erro).                                                                                                                                                                               | Preflight automático |
| <input type="checkbox"/> | vCPU e memória de cada VM de acordo com o papel: abaixo de 90% da arquitetura, erro; vCPU abaixo de 100% ou memória abaixo de 97%, alerta.                                                                                                            | Preflight automático |
| <input type="checkbox"/> | Pelo menos 40 GB livres no volume de <code>/var/opt/gitlab</code> em cada VM (menos de 10 GB: erro; menos de 40 GB: alerta).                                                                                                                          | Preflight automático |
| <input type="checkbox"/> | Relógio sincronizado por NTP em todas as VMs (sem sincronismo: alerta).                                                                                                                                                                               | Preflight automático |
| <input type="checkbox"/> | Host da URL externa resolvido por DNS nas VMs GitLab Rails e do balanceador externo (falha: alerta; erro com Let's Encrypt).                                                                                                                          | Preflight automático |
| <input type="checkbox"/> | VMs sem instalação GitLab prévia (instalação encontrada: alerta).                                                                                                                                                                                     | Preflight automático |
| <input type="checkbox"/> | Quantidade de VMs por papel igual à arquitetura escolhida, uma VM por papel, conferida também pela validação automática da configuração.                                                                                                              | Reunião de prontidão |
| <input type="checkbox"/> | Volume de <code>/var/opt/gitlab</code> montado em cada VM e, nos nós GitLab, disco local e dedicado com capacidade para a soma dos repositórios.                                                                                                      | Cliente              |
| <input type="checkbox"/> | Latência entre as VMs menor que 5 ms (3k ou mais).                                                                                                                                                                                                    | Cliente              |
| <input type="checkbox"/> | Regras de firewall entre as VMs e dos balanceadores liberadas conforme as tabelas de portas (2k ou mais).                                                                                                                                             | Reunião de prontidão |
| <input type="checkbox"/> | Saída liberada: runner para gitlab.com, registry.gitlab.com, <i>gitlab-static.net</i> e <i>storage.googleapis.com</i> ; VMs para <i>packages.gitlab.com</i> e repositórios do sistema operacional; VMs de balanceador e OpenSearch para o Docker Hub. | Reunião de prontidão |
| <input type="checkbox"/> | VM do runner com Docker Engine, 2 vCPU, 4 GB e 40 GB; runner registrado no projeto do engajamento e online.                                                                                                                                           | Reunião de prontidão |
| <input type="checkbox"/> | Certificado TLS com SAN do host externo, cadeia de intermediários e chave correspondente; certificado wildcard do Pages, quando habilitado.                                                                                                           | Reunião de prontidão |

| <input type="checkbox"/> | Item                                                                                                                                                                                                                           | Verificado por       |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <input type="checkbox"/> | Registro DNS da URL externa criado nos DNS interno e externo; DNS wildcard do Pages, quando habilitado.                                                                                                                        | Cliente              |
| <input type="checkbox"/> | Object storage com os buckets criados com os nomes exatos e credenciais com acesso a eles (2k ou mais, ou quando habilitado em 1k).                                                                                            | Reunião de prontidão |
| <input type="checkbox"/> | LDAP, SMTP e cluster de busca externo alcançáveis a partir das VMs GitLab Rails e Sidekiq, com as contas informadas.                                                                                                           | Reunião de prontidão |
| <input type="checkbox"/> | Assinatura GitLab Premium ou GitLab Ultimate ativa, com activation code ou arquivo de licença disponível.                                                                                                                      | Cliente              |
| <input type="checkbox"/> | Infraestrutura criada pelo pipeline: credencial de nuvem cadastrada no ambiente, permissões da identidade e políticas da organização conferidas, cotas da região suficientes e plano do Terraform revisado antes da aplicação. | Reunião de prontidão |
| <input type="checkbox"/> | Infraestrutura criada pelo pipeline: runner do engajamento com rota para os endereços internos da rede criada.                                                                                                                 | Reunião de prontidão |
| <input type="checkbox"/> | Balanceador do cliente: TCP 443 e porta do SSH do Git encaminhados em passthrough aos nós GitLab Rails, health check configurado e registros DNS da URL externa, do registry e do Pages apontando para ele.                    | Cliente              |
| <input type="checkbox"/> | Container Registry: nome coberto pelo certificado, registro DNS criado e bucket do registry disponível.                                                                                                                        | Reunião de prontidão |
| <input type="checkbox"/> | GitLab Geo: dois ambientes com a mesma versão GitLab, prefixos diferentes, licença só no primário, senha do PostgreSQL igual nos dois sites e rede entre os sites liberada.                                                    | Reunião de prontidão |
| <input type="checkbox"/> | Frota de runners: token de API com os escopos exigidos, VMs, Auto Scaling Group ou cluster disponíveis e configuração da frota validada pelo pipeline.                                                                         | Reunião de prontidão |
| <input type="checkbox"/> | Agentes GitLab para Kubernetes: token de API, grupo dos projetos de configuração existente, acesso a cada cluster e saída dos clusters para a URL externa na 443.                                                              | Reunião de prontidão |
| <input type="checkbox"/> | Aprovador das execuções, janela de manutenção e contatos definidos.                                                                                                                                                            | Reunião de prontidão |

O3S Consultoria e Tecnologia da Informação Ltda. · contato@pointertech.digital · +55 (61) 99874-4648 ·  
pointertech.digital

PR-IMP-01 · versão 1.2 · 1 de outubro de 2026. GITLAB is a trademark of GitLab Inc. in the United States and other countries and regions. A Pointer é parceira GitLab Select.