

PRÉ-REQUISITOS · AVALIAÇÃO

Pré-requisitos: Levantamento da plataforma

Documento enviado após a escolha do serviço PS-AVA-02: o que o cliente provisiona, as credenciais que entrega à Pointer, as informações a enviar e o checklist de prontidão.

CÓDIGO

PR-AVA-02

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-AVA-02 · OFERTA PS-AVA-02

Pré-requisitos: Levantamento da plataforma

Este documento é enviado depois da escolha da oferta PS-AVA-02. Ele lista o que o cliente provisiona em cada plataforma de origem, as credenciais somente leitura, as informações que devolve à Pointer e o checklist de prontidão conferido antes da primeira coleta. O prazo de devolução é definido no kick-off. Nenhum valor de credencial é enviado com o formulário.

Conteúdo

O que o cliente provisiona

Regras para as credenciais

O que é coletado

Credenciais que o cliente entrega à Pointer

Informações a enviar

Checklist de prontidão

1. O que o cliente provisiona

Item	Especificação	Obrigatório
Conta dedicada por origem	Conta de serviço ou usuário dedicado ao levantamento em cada plataforma de origem, com a permissão de leitura descrita em Credenciais.	Sim
Credencial somente leitura por origem	Token ou chave de acesso da conta dedicada, conforme a origem (seção Credenciais).	Sim
Acesso de rede à API da origem	Origem acessível pela internet: coleta pelos runners da instância, sem ação do cliente. Origem só na rede interna: máquina na rede do cliente com acesso HTTPS à API da origem, para o runner do projeto do engajamento (executor Docker ou Kubernetes) ou para a coleta externa.	Condicional: origem sem acesso pela internet
Certificado da CA interna	Certificado (PEM) da autoridade certificadora corporativa que emitiu o certificado HTTPS da origem, disponível na máquina da coleta.	Condicional: origem com certificado de CA interna
Proxy de saída	Endereço do proxy HTTPS e exceções, quando a saída da máquina da coleta passa por proxy.	Condicional: rede com proxy

Item	Especificação	Obrigatório
Revogação no encerramento	Revogação das credenciais pelo cliente ao fim do engajamento.	Sim

- Quando a coleta roda num runner na rede do cliente, esse runner também precisa de saída HTTPS para o GitLab.com, onde fica o projeto do engajamento, e para o registry.gitlab.com, de onde vem a imagem da coleta.

2. Regras para as credenciais

- Credencial somente leitura, de conta de serviço ou de usuário dedicado ao levantamento.
- O valor é cadastrado somente como variável de CI/CD do projeto do engajamento, com as opções Protected e Masked and hidden. O arquivo de configuração do levantamento guarda apenas o nome da variável, nunca o valor.
- O valor nunca é enviado por e-mail, chat, issue ou arquivo. Se isso ocorrer, a credencial é revogada e outra é emitida.
- Validade até o encerramento do engajamento; no encerramento, o agendamento da coleta é removido e o cliente revoga a credencial.
- Os coletores só fazem consultas (GET e HEAD; POST apenas em APIs de consulta, como a WQL do Azure DevOps e a API do AWS CodeCommit) e nunca registram a credencial em URL, mensagem de erro ou log.

3. O que é coletado

Inventário, volumes, atividade e contagens por projeto ou repositório, para as métricas e para o dimensionamento da migração. Usuários entram só em contagens: nomes, e-mails e usernames não são gravados, e namespaces pessoais são mascarados no que é publicado. Quando a API da origem nega um campo à credencial, a coleta segue, registra um aviso e deixa o campo em branco. A coleta de cada origem é independente das demais.

4. 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
Personal access token da origem GitLab	Coleta das origens GitLab (GitLab.com ou GitLab self-managed).	Escopo <code>read_api</code> . Escopo de coleta instância: usuário administrador (usuários, runners e configurações da instância e todos os projetos). Escopo grupo ou projeto: papel Reporter ou superior; com Maintainer, a coleta também conta variáveis de CI/CD, webhooks, espelhos, agendamentos de pipeline e tokens de trigger (sem ele, esses campos ficam em branco). Conta de serviço (GitLab Premium ou Ultimate) ou usuário dedicado.	Token (uma linha) Até o encerramento do engajamento; revogado pelo cliente no encerramento.	Condicional: origem GitLab
Token do GitHub	Coleta das origens GitHub.com ou GitHub Enterprise Server.	Leitura das organizações e repositórios do escopo. <code>read:org</code> para agrupar os repositórios por time (sem ele, agrupamento só por organização); <code>read:packages</code> para contar pacotes (sem ele, pacotes não contados). Campos que exigem permissão de administrador do repositório ficam em branco sem ela. GitHub Enterprise Server com escopo instância: token de administrador (todas as organizações).	Token (uma linha) Até o encerramento do engajamento; revogado pelo cliente no encerramento.	Condicional: origem GitHub
Personal access token do Azure DevOps	Coleta das origens Azure DevOps Services ou Azure DevOps Server.	Leitura de código e de build nos projetos do escopo; leitura de work items para as contagens por consulta WQL; Member Entitlement Management para contar os usuários da organização (sem ele, usuários não contados). Políticas de branch negadas ficam em branco.	Token (uma linha) Até o encerramento do engajamento; revogado pelo cliente no encerramento.	Condicional: origem Azure DevOps

Credencial	Finalidade	Permissões	Formato e validade	Obrigatório
API token da conta Atlassian (Bitbucket Cloud)	Coleta das origens Bitbucket Cloud.	Leitura do workspace, dos projetos e dos repositórios do escopo, com autenticação básica pelo e-mail da conta Atlassian e o API token. Variáveis do Bitbucket Pipelines e webhooks exigem permissão de administrador do repositório; sem ela, ficam em branco.	Dois valores: e-mail da conta Atlassian e API token Até o encerramento do engajamento; revogado pelo cliente no encerramento.	Condicional: origem Bitbucket Cloud
Token HTTP de acesso do Bitbucket Server/Data Center	Coleta das origens Bitbucket Server/Data Center (sob consulta: escopo e condições definidos em proposta específica, com execução piloto).	Leitura dos projetos e repositórios do escopo (autenticação Bearer). Usuários contados pela API administrativa quando o token tem acesso a ela; sem acesso, pela lista de usuários visível ao token. Restrições de branch e webhooks negados ficam em branco.	Token (uma linha) Até o encerramento do engajamento; revogado pelo cliente no encerramento.	Condicional: origem Bitbucket Server/Data Center
Chave de acesso de usuário IAM (AWS CodeCommit)	Coleta das origens AWS CodeCommit.	Ações <code>codecommit:List*</code> , <code>codecommit:Get*</code> e <code>codecommit:BatchGet*</code> na região do escopo. Session token opcional.	Dois valores: access key ID e secret access key (e session token, quando usado) Até o encerramento do engajamento; revogada pelo cliente no encerramento.	Condicional: origem AWS CodeCommit

5. 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.

Origens (uma linha por origem)

Informação	Exemplo	Obrigatório	Observação
Tipo da origem	GitLab self-managed	Sim	GitLab, GitHub, Bitbucket Cloud, Bitbucket Server/Data Center, Azure DevOps ou AWS CodeCommit.
URL	https://gitlab.cliente.gov.br	Condicional: GitLab, GitHub Enterprise Server, Bitbucket Server/Data Center e Azure DevOps	Azure DevOps: https://dev.azure.com/ ou /.
Escopo da coleta	Instância	Sim	GitLab: instância, grupo ou projeto. GitHub: organização, usuário, repositório ou instância (Enterprise Server). Bitbucket Cloud: workspace, projeto ou repositório. Bitbucket Server/Data Center: instância, projeto ou repositório. Azure DevOps: organização, projeto ou repositório. AWS CodeCommit: região ou repositório.
Caminho	ti/sistemas	Condicional: escopos grupo, projeto, repositório, usuário, workspace e organização (exceto organização do Azure DevOps)	Grupo, organização, workspace, projeto ou repositório a coletar.
Região	sa-east-1	Condicional: AWS CodeCommit	
Exclusões	ti/arquivo-morto	Não	Caminhos fora do levantamento.
Janela das métricas (dias)	90	Não	Padrão: 90 dias.
Acesso de rede	Só na rede interna	Sim	Acessível pela internet ou só na rede interna; define runner da instância, runner na rede do cliente ou coleta externa.
CA interna e proxy	CA corporativa; proxy.cliente.gov.br:3128	Condicional: CA interna ou proxy	

Informação	Exemplo	Obrigatório	Observação
Responsável pela origem	Nome, cargo, e-mail	Sim	Quem emite e revoga a credencial.

Migração pretendida (para o modelo de esforço)

Informação	Exemplo	Obrigatório	Observação
Destino	GitLab self-managed	Não	GitLab self-managed, GitLab.com ou GitLab Dedicated. Padrão: GitLab self-managed.
Método (origem GitLab)	Direct Transfer	Não	Direct Transfer ou exportação e importação por arquivo. Padrão: Direct Transfer.
Provisionamento de usuários no destino	LDAP/SSO	Não	LDAP/SSO, criação pela migração ou cadastro manual.

Fases e coleta agendada

Informação	Exemplo	Obrigatório	Observação
Data de referência da fase inicial	2026-11-10	Não	Padrão: encerramento da rodada inicial do Teste de Maturidade.
Data de referência da fase final	2026-12-08	Não	Padrão: encerramento da rodada final; com a rodada em andamento, a coleta mais recente.
Periodicidade e data final da coleta agendada	Semanal, até 2026-12-08	Não	A série histórica e o comparativo por fase usam as coletas agendadas.

6. 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.

☐ Item	Verificado por
☐ Conta de serviço ou usuário dedicado criado em cada origem, com a permissão de leitura da seção Credenciais.	Cliente
☐ Credencial cadastrada como variável protegida e mascarada no projeto do engajamento, sem envio por e-mail, chat, issue ou arquivo.	Reunião de prontidão
☐ Configuração do levantamento validada pelo pipeline do engajamento.	Preflight automático
☐ Forma de acesso à origem definida e disponível: runner da instância, runner na rede do cliente ou máquina para a coleta externa.	Reunião de prontidão
☐ Certificado da CA interna e proxy informados, quando existirem.	Cliente
☐ Data de revogação das credenciais e de remoção do agendamento combinada.	Reunião de prontidão

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

PR-AVA-02 · 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.