# Arquitetura

Modelos de arquitetura do CtrlStation

- Arquitetura SaaS - Cloud
- Arquitetura On-Premises
- Instalação OnPremises - Checklist Hardening

# Arquitetura SaaS - Cloud

# CtrlStation - Ambiente SaaS

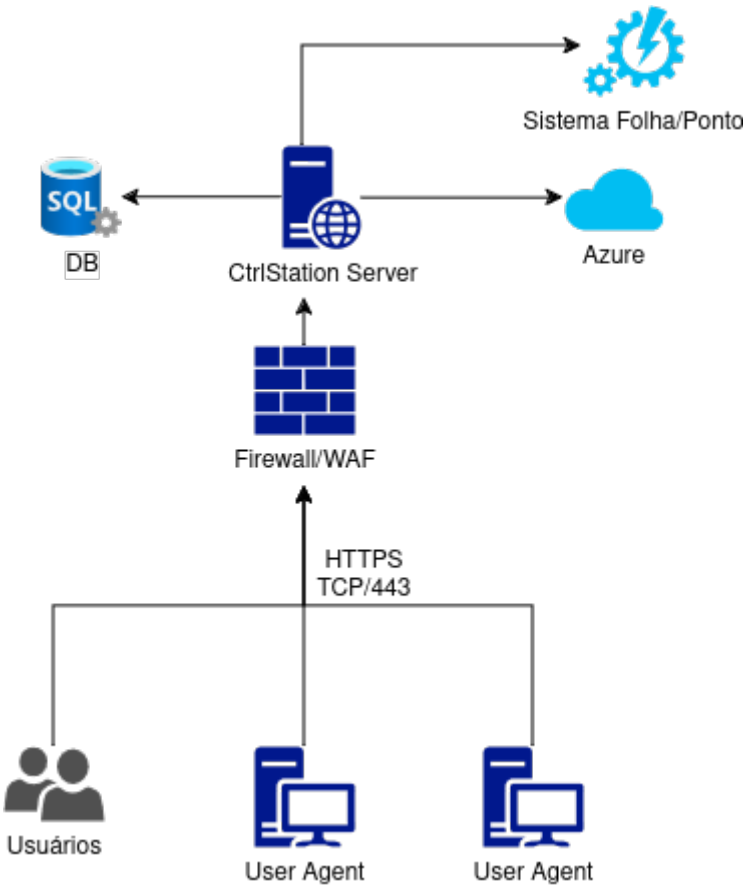
No modelo SaaS o CtrlStation é executado dentro do ambiente *cloud* da LAB3, utilizando o provedor de infraestrutura *Azure*. Cada cliente tem um ambiente dedicado à sua aplicação, com isolamento de dados e aplicação.

# Arquitetura de Rede

A aplicação tem uma arquitetura simples, sendo composta por um servidor de aplicação e uma base de dados SQL, todos gerenciados pela LAB3 em ambiente isolado. Toda comunicação com a aplicação é feita somente via HTTPS na porta 443. Não há nenhuma outra entrada de comunicação por outras portas.

Se houver integrações com outros sistemas (folha/ponto/RH)  ou com o Azure, a comunicação é feita à partir do servidor de aplicação utiliza as portas especificadas na integração.

Um diagrama simplificado de rede pode ser visualizado abaixo.



# Integrações e VPN

Caso haja necessidade de integração com sistema que seja interno ao cliente, é possível estabelecer uma VPN  ponto-a-ponto para efetuar o acesso. A VPN é estabelecida diretamente à partir do servidor de aplicação com o cliente.

# Redundância e Disponibilidade

O ambiente trabalha em modo ativo-ativo, com servidores de aplicação em dois sites distintos e o serviço de banco de dados gerenciado com replicação ativo-passivo, com fallback automático.

# Segurança de Dados

Todos os dados são criptografados em repouso. Arquivos de backup são criptografados com chaves gerenciadas pela LAB3, podendo também ser oferecido ao cliente a opção de gestão da chave de backup. Os backups são feitos diariamente.

# Controle de Acesso

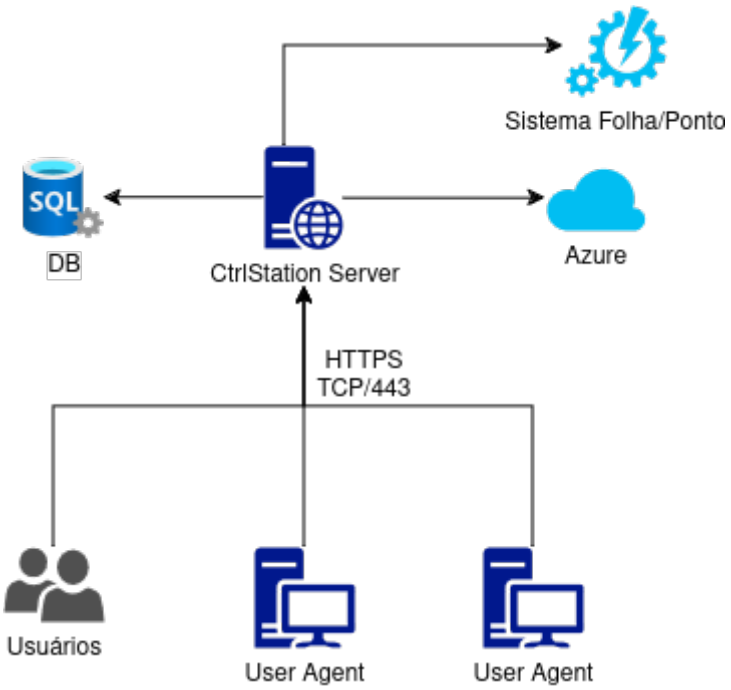
Todo o acesso à aplicação está sujeito ao controle de acesso e política de segurança da LAB3. O acesso por funcionários da LAB3 é restrito após a entrada em produção.

# Arquitetura On-Premises

# Ambiente On-Premises

## Arquitetura

A arquitetura do CtrlStation é simples e envolve apenas o servidor de aplicação e banco de dados. Se houver integração com Azure ou outros sistemas, é necessário analisar para cada um o funcionamento. A estrutura simplificada de rede pode ser visualizada abaixo:




A porta 443 do CtrlStation precisa ser acessível pelas máquinas que serão controladas, então é necessário que o cliente efetue a configuração de um domínio DNS e configure um NAT ou balanceador de carga para a conectividade.

## Pré-Requisitos

Para execução on-premises do CtrlStation é necessário um servidor Windows e uma base de dados SQL Server, seguindo os requisitos a seguir.

### Servidor

- Processador 2Ghz 4 core
- Memória 4 GB RAM

● Espaço em Disco Livre: 20Gb

**Sistema Operacional**

● Windows Server 2016
● Windows Server 2019
● Windows Server 2022

**Software**

Os seguintes pacotes devem estar instalados:
● .NET Extensibility 4.6.2 ou superior
● ASP .NET 4.6.2 ou superior
● ISAPI Extensions
● ISAPI Filters
● .NET Framework 4.6.2 ou superior
● IIS 6.0 ou superior

## Banco de Dados

O Banco de Dados pode ser instalado no mesmo servidor da aplicação, ou utilizado um externo. O sistema de banco de dados deve ser:

- SQL Server 2016 ou superior

A modalidade *Express* do SQL Server pode ser utilizada para clientes com poucas licenças, dado o limite de armazenamento imposto por esta versão.

# Alta Disponibilidade

Caso deseje alta disponibilidade, podeser duplicado o servidor de aplicação e o banco de dados precisa ser configurado com replicação. Estas configurações devem ser feitas pelo cliente. Também é necessário alterar a arquitetura de rede para incluir um balanceador de carga.

# Backup

No modelo *on-premises* os backups são de responsabilidade do cliente, devendo ser feito o **backup da base de dados** e também do diretório:

- C:\inetpub\wwwroot\ctrl-station

É recomendado o backup diário.

# Instalação OnPremises - Checklist Hardening

## Hardening Servidor On-Premises

Para instalações on-premises, recomendamos o *hardening* dos servidores Windows de acordo com as melhores práticas. O checklist sugerido está a seguir:

Com certeza! Aqui está o checklist de endurecimento (hardening) do IIS e Windows Server traduzido e adaptado para o português técnico utilizado no Brasil.

---

### 1. Sistema Operacional e Servidor

- [ ] **Instalar Apenas o Mínimo Necessário:** Certifique-se de que apenas a função "Web Server (IIS)" e os módulos necessários do ASP.NET estejam instalados. Remova todas as funções não relacionadas
- [ ] **Desativar Protocolos Desnecessários:** Desative protocolos antigos e vulneráveis, como o **SMBv1** , para evitar ataques de movimentação lateral na rede.
- [ ] **Manter o Sistema Atualizado:** Imponha a aplicação automática de patches de segurança para o Windows OS e o .NET Framework utilizando o WSUS ou o Windows Update.

### 2. Segurança de Rede e Criptografia do IIS (Camada de Transporte)

- [ ] **Desativar TLS/SSL Legados:** Desative o SSL 2.0, SSL 3.0, TLS 1.0 e TLS 1.1 através do Registro do Windows (Registry). Force o uso exclusivo de **TLS 1.2 e TLS 1.3**.
- [ ] **Restringir Ciphers (Algoritmos de Criptografia):** Desative ciphers fracos (como RC4, Triple DES/3DES) e algoritmos de hash antigos (MD5, SHA-1). Priorize ciphers com *Perfect Forward Secrecy* (PFS).
- [ ] **Forçar HTTPS:** Configure o *binding* do site para a porta 443 com um certificado TLS válido e confiável. Configure um redirecionamento automático de HTTP (porta 80) para HTTPS (porta 443).

### 3. Isolamento do Application Pool (Pool de Aplicativos) do IIS

- [ ] **Identidades Únicas para o AppPool:** Nunca execute os Pools de Aplicativos sob contas de altos privilégios como `LocalSystem` , `Administrator` ou `NetworkService` . Crie uma identidade dedicada do tipo **ApplicationPoolIdentity** ou uma Conta de Serviço Gerenciada (MSA) para a sua aplicação ASP.NET.
- [ ] **Habilitar Restrições do Modelo de Processo:** Certifique-se de que as propriedades `Idle Time-out` (Tempo de Limite de Inatividade) e `Regular Time Interval` (Reciclagem Regular) estejam configuradas para evitar vazamentos de memória ou exposição prolongada caso um processo seja comprometido.
- [ ] **Carregar Perfil do Usuário:** Defina `Load User Profile = True` nas configurações do AppPool para que as chaves criptográficas e arquivos temporários fiquem isolados no espaço de usuário daquela identidade específica.

### 4. Permissões de Sistema de Arquivos e Pastas

- [ ] **Controle de Acesso à Raiz da Web:** Restrinja as permissões no diretório físico do site (geralmente `C:\inetpub\wwwroot\ctrl-station` ).

    - *Administrators / SYSTEM:* Controle Total (Full Control).
    - *Identidade do App Pool (`IIS_IUSRS`):* Ler & Executar, Listar Conteúdo da Pasta e Leitura. **Não conceda permissão de Gravação (Write)**, a menos que seja estritamente necessário para uma pasta de uploads específica.
- [ ] **Proteger o `web.config`:** Garanta que o arquivo `web.config` não possa ser lido por usuários anônimos da web. Ele deve ter suas seções criptografadas caso contenha strings de conexão com o banco de dados ou credenciais sensíveis.

# 5. Redução da Superfície de Ataque e Cabeçalhos HTTP (Headers)

- [ ] **Remover Banners do Servidor:** Oculte os cabeçalhos que dizem exatamente qual software e versão você está rodando para dificultar a vida de atacantes.
    - Remover `Server: Microsoft-IIS/10.0` (Pode ser feito via módulo URL Rewrite ou diretamente no `web.config`).
    - Remover `X-Powered-By: ASP.NET` (Remova através do Gerenciador do IIS $\rightarrow$ Cabeçalhos de Resposta HTTP).
    - Remover `X-AspNet-Version` (Configure `<httpRuntime enableVersionHeader="false" />` no seu `web.config`).
- [ ] **Injetar Cabeçalhos de Segurança:** Configure explicitamente os seguintes cabeçalhos de resposta HTTP no IIS:
    - `Strict-Transport-Security (HSTS)` (Força o uso de HTTPS no navegador do usuário).
    - `X-Frame-Options: SAMEORIGIN` (Previne ataques de Clickjacking).
    - `X-Content-Type-Options: nosniff` (Prevines ataques de exploração de MIME-sniffing).
    - `Content-Security-Policy (CSP)` (Restringe de onde os scripts, imagens e recursos podem ser carregados).

# 6. Logs e Auditoria

- [ ] **Habilitar Log Avançado no IIS:** Configure o log do IIS para capturar campos cruciais de auditoria, incluindo: IP do Cliente, User Agent, URI Stem (página acessada), Status HTTP e Bytes Enviados/Recebidos.
- [ ] **Centralização de Logs:** Certifique-se de que os logs do IIS e os Logs de Eventos de Segurança do Windows (Event Viewer) sejam enviados para um armazenamento centralizado do tipo *write-once* (apenas escrita) ou para um sistema **SIEM** (Gerenciamento de Eventos e Informações de Segurança), impedindo que um invasor apague os rastros.