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.

Revisão #1
Criado 18 maio 2026 19:26:30 por Felipe Weckx
Atualizado: 18 maio 2026 19:30:01 por Felipe Weckx