



***Workday Session Management Connector AD  
Definição do serviço Windows responsável  
pela atualização do Active Directory***

**Projeto:** Workday Session Management  
**Documento:** Documentação  
**Versão:** 1.0  
**Data:** 26/12/2024  
**Autor:** Nikolas Machado Corrêa

## Introdução

O WSM Connector AD é um serviço desenvolvido em .NET que automatiza a integração e a administração de usuários no Active Directory (AD). Este serviço é projetado para funcionar como um Serviço do Windows, garantindo uma execução contínua em segundo plano, com suporte a logs detalhados e segurança aprimorada.

## Visão de Negócio

Este serviço resolve a necessidade de configurar e monitorar horários de trabalho dos colaboradores, garantindo conformidade com políticas de segurança e controle de acesso. Tem como funções:

- Automatizar a definição de horários permitidos de logon para cada usuário.
- Fornecer integração com o AD para gerenciar permissões.
- Melhorar a segurança, limitando acessos fora dos horários autorizados.

## Definição do serviço

O **WSM Connector AD** é uma aplicação que:

- Atualiza horários de logon de usuários no Active Directory.
- Atualiza status do usuário: habilitado/desabilitado.
- Desbloqueia senha em caso de bloqueio por múltiplas tentativas.
- Registra logs detalhados no Visualizador de Eventos do Windows, permitindo auditoria e monitoramento.

O serviço é configurado para iniciar automaticamente como um Serviço do Windows, com suporte a execução contínua.

# Arquitetura e Estrutura do Projeto

## Principais Componentes

1. **Controller/Program.cs:** Ponto de entrada da aplicação, configurando o serviço para ser executado como um Serviço do Windows.
2. **ActiveDirectory/AdManager.cs:** Classe principal responsável por interagir com o Active Directory, incluindo:
  1. Conexão ao AD.
  2. Busca de usuários.
  3. Atualização de horários de logon.
3. **Utils/:** Conjunto de classes utilitárias que incluem:
  1. Criptografia.
  2. Gerenciamento de logs.
  3. Recuperação de parâmetros de instalação.

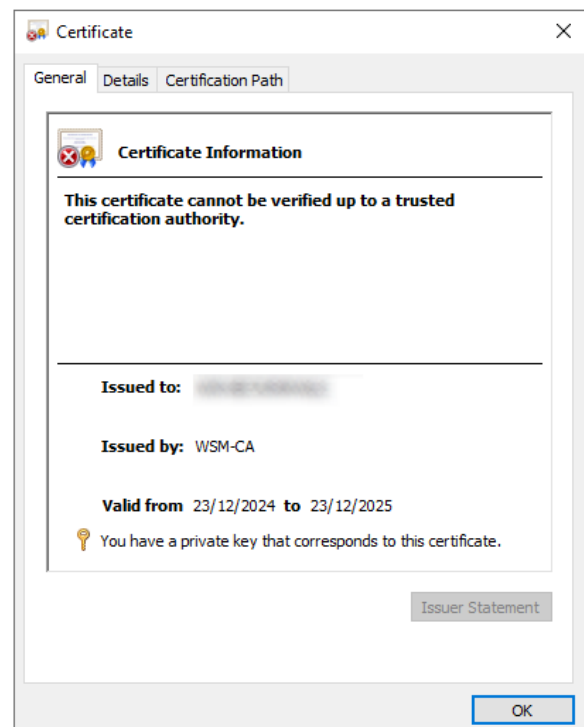
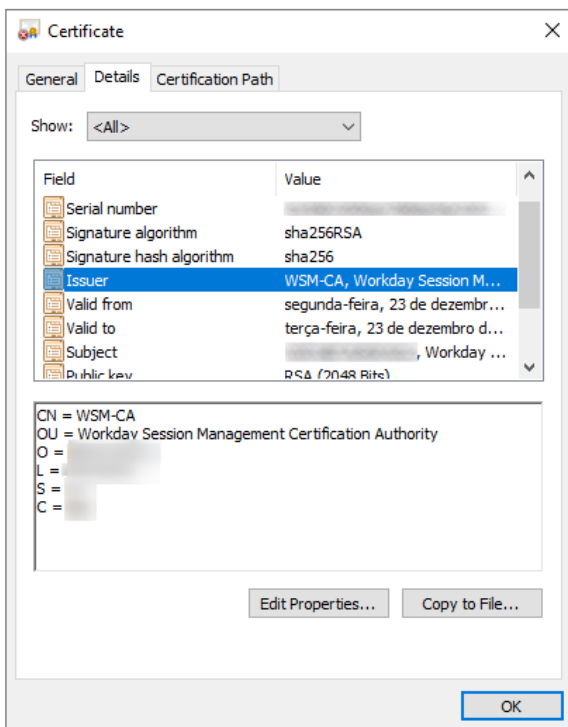
## Processo de certificação

Após o início do serviço ocorre o processo de certificação, em que é gerado um par de chave público-privada e é criado um pedido de assinatura ou CSR (Certificate Signing Request). O CSR é enviado ao Session Server para que a Autoridade Certificadora (CA) configurada no servidor assine e retorne o certificado da máquina onde foi instalado o serviço.

Este processo tem como finalidade garantir que as mensagens trocadas entre o serviço e o servidor WSM sejam encriptadas e que somente o destinatário consiga acessá-las. Ao todo são instalados 3 certificados: **WSM\_SESSION\_SERVER**, **WSM\_CA** e **certificado local da máquina**.

- **WSM\_CA:** certificado auto-assinado pela CA que estabelece a sua identidade.
- **WSM\_SESSION\_SERVER:** certificado do Session Server de onde é extraída a chave pública para encriptar as mensagens destinadas ao servidor. Dessa forma, somente ele consegue decriptá-las.
- **Certificado local:** identificado pelo FQDN da máquina, possui chave privada usada para decriptar mensagens do Session Server. As mensagens enviadas pelo servidor são encriptadas com a chave pública deste certificado local, isto é, somente o serviço Windows consegue decriptá-las com sua chave privada. **Nenhuma chave privada é armazenada fora da máquina local.**

Exemplos de certificados instalados na máquina. Na imagem da esquerda, é possível observar detalhes do certificado como o campo *Issuer*, que representa a Autoridade certificadora que o assinou. Na imagem da direita, o campo *Issued by* e a informação de que está armazenada localmente uma chave privada.



## Fluxo de Funcionamento

Caso não seja possível estabelecer comunicação com o session server, o serviço não funcionará corretamente e não poderá receber mensagens. Neste caso, precisa ser reiniciado pelo *services.msc*. Após garantir que todos os certificados estão instalados localmente e que há comunicação com o servidor, o serviço segue o seguinte fluxo de funcionamento:

1. O serviço recebe uma mensagem JSON encriptada e utiliza seu certificado local para decriptá-la.
2. Com a mensagem decriptada, interpreta o JSON com os horários de trabalho permitidos do usuário.
3. Conecta-se ao Active Directory utilizando credenciais e domínio configurados.
4. Atualiza os horários de logon do usuário, habilita/desabilita conta e/ou desbloqueia a senha, com base nos parâmetros fornecidos via JSON.
5. Registra logs detalhados de todas as operações, incluindo sucessos e erros.
6. Envia uma resposta encriptada com a chave pública do servidor indicando o status da operação.

# Guia de Instalação

## Pré-requisitos

- Sistema operacional Windows com Active Directory configurado.
- .NET 8.0 ou superior.
- Porta 44901 liberada para comunicação com servidor (Session Service).
- Ferramenta NSIS (Nullsoft Scriptable Install System) para gerar o instalador.

## Passos para Instalar

### 1. Clone o repositório:

- `git clone <repository-url>`

### 2. Restaure os pacotes NuGet:

- `dotnet restore`

### 3. Faça o build da solução:

- `dotnet build`

### 4. Publique a aplicação:

- `dotnet publish -c Release`

### 5. Instalação e execução do serviço Windows:

A instalação é feita usando NSIS (Nullsoft Scriptable Install System). Para gerar um novo instalador, é necessário ter o NSIS instalado e executar o arquivo de script *.nsi* fornecido: *WsmConnectorAdInstallerScript.nsi*. **Se já houver um instalador gerado, basta executar diretamente o arquivo WsmConnectorAdSetup.exe.**

## Uso

Os horários de trabalho permitidos são recebidos de forma encriptada pelo Session Server em uma string JSON no seguinte formato:

```
{
  "uid": "jdoe",
  "allowed_work_hours": {
    "MONDAY": [{ "start": 480, "end": 1020 }],
    "TUESDAY": [{ "start": 480, "end": 1020 }]
  },
  "enable": true,
  "unlock": true
}
```

## Descrição dos parâmetros

Parâmetro	Tipo	Descrição
<code>uid</code>	string	O nome de usuário (nome da conta SAM) do usuário no Active Directory. Exemplo: "jdoe".
<code>allowed_work_hours</code>	object	Um dicionário que define as janelas de tempo de login por dia da semana. As chaves são os nomes dos dias em maiúsculas (ex.: "MONDAY"). Os valores são arrays com intervalos de tempo em minutos desde a meia-noite.
<code>start</code>	int	Hora de início em minutos após a meia-noite. Exemplo: 480 = 08:00 da manhã.
<code>end</code>	int	Hora de término em minutos após a meia-noite. Exemplo: 1020 = 17:00 (5 da tarde).
<code>enable</code>	bool	Ativa ou desativa a conta. true ativa a conta, false a desativa.
<code>unlock</code>	bool	Se for true, a conta será desbloqueada caso esteja bloqueada devido a tentativas de login malsucedidas.

### ***Permissões Necessárias no Active Directory***

O usuário de domínio que executa o serviço deve ter permissão para gerenciar contas de usuário.

#### **Permissões mínimas exigidas:**

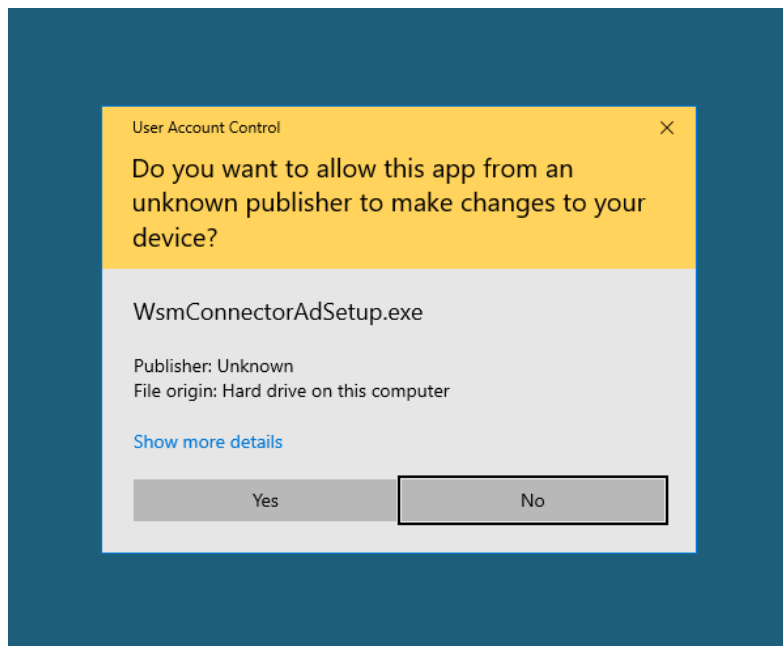
Operação	Permissão necessária no AD
Atualizar horário de logon	Permissão de escrita no atributo <code>logonHours</code>
Ativar/Desativar conta	Permissão de escrita no atributo <code>userAccountControl</code>
Desbloquear conta	Redefinir o atributo <code>lockoutTime</code> ou usar o controle de desbloqueio

### ***Delegar permissões via "Usuários e Computadores do Active Directory":***

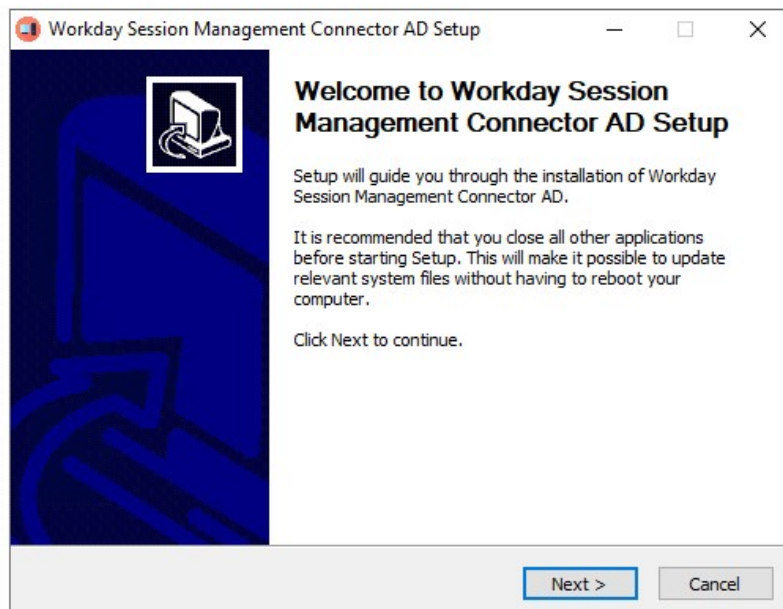
1. Clique com o botão direito na OU (Unidade Organizacional) desejada → Delegar Controle
2. Selecione o usuário ou a conta de serviço
3. Escolha "Criar uma tarefa personalizada para delegar"
4. Selecione Objetos de usuário
5. Atribua as permissões necessárias

## Como executar o instalador

1. Autorize a instalação com privilégios administrativos

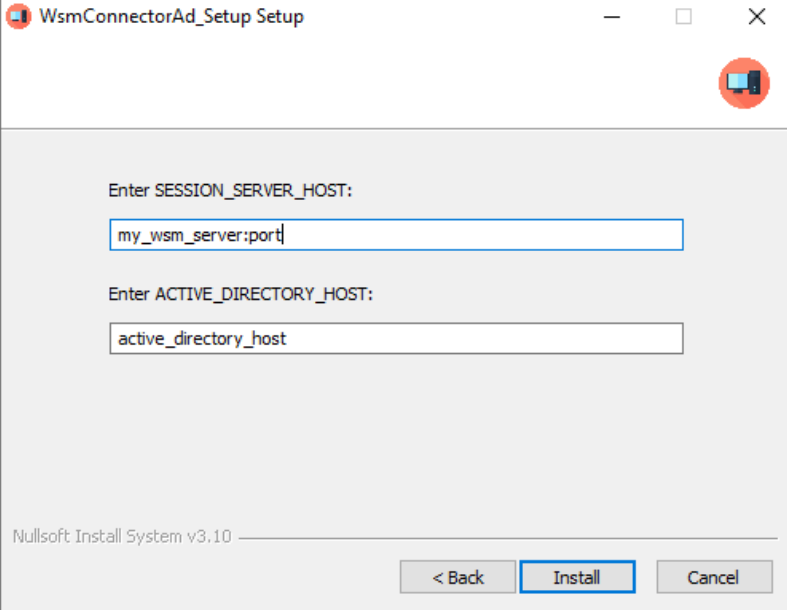


2. Página inicial do instalador:



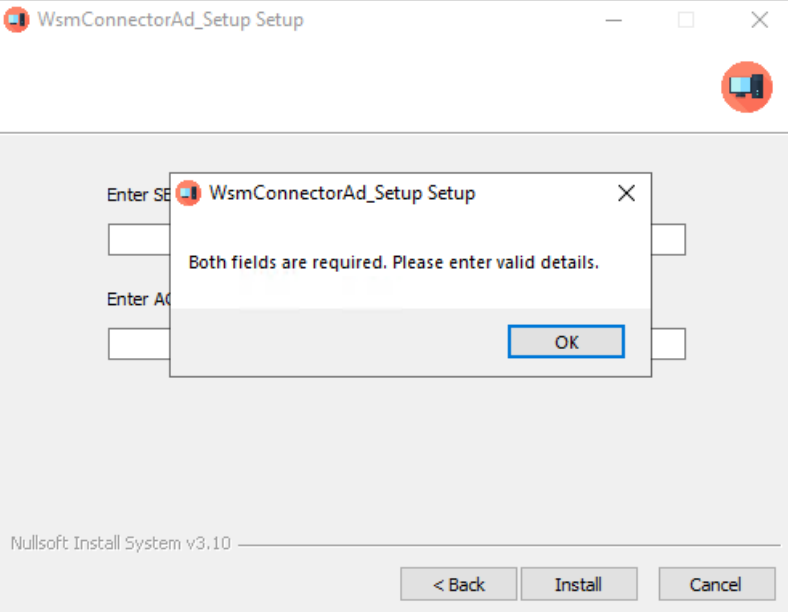
3. Configuração dos parâmetros:

- O instalador requer dois parâmetros:
  1. **SESSION\_SERVER\_HOST:** servidor onde está instalado o módulo Session Server e porta
  2. **ACTIVE\_DIRECTORY\_HOST:** endereço do Active Directory (mesma máquina onde está sendo instalado o serviço)



The screenshot shows the 'WsmConnectorAd\_Setup Setup' window. It has two input fields. The first is labeled 'Enter SESSION\_SERVER\_HOST:' and contains the text 'my\_wsm\_server:port'. The second is labeled 'Enter ACTIVE\_DIRECTORY\_HOST:' and contains the text 'active\_directory\_host'. At the bottom, there are three buttons: '< Back', 'Install' (highlighted with a blue border), and 'Cancel'. The footer text reads 'Nullsoft Install System v3.10'.

- Os dois campos são obrigatórios

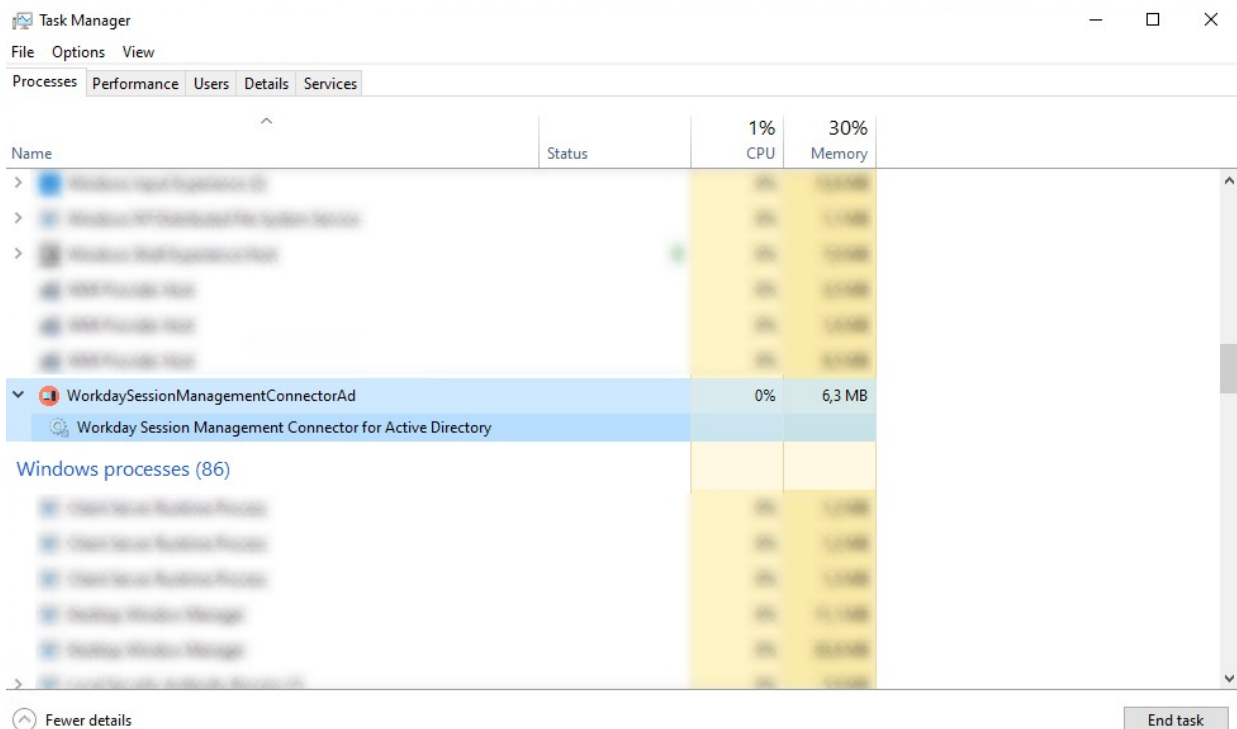


The screenshot shows the same 'WsmConnectorAd\_Setup Setup' window, but with an error dialog box overlaid. The dialog box has the title 'WsmConnectorAd\_Setup Setup' and the message 'Both fields are required. Please enter valid details.' with an 'OK' button. The background window's input fields and buttons are partially visible behind the dialog.

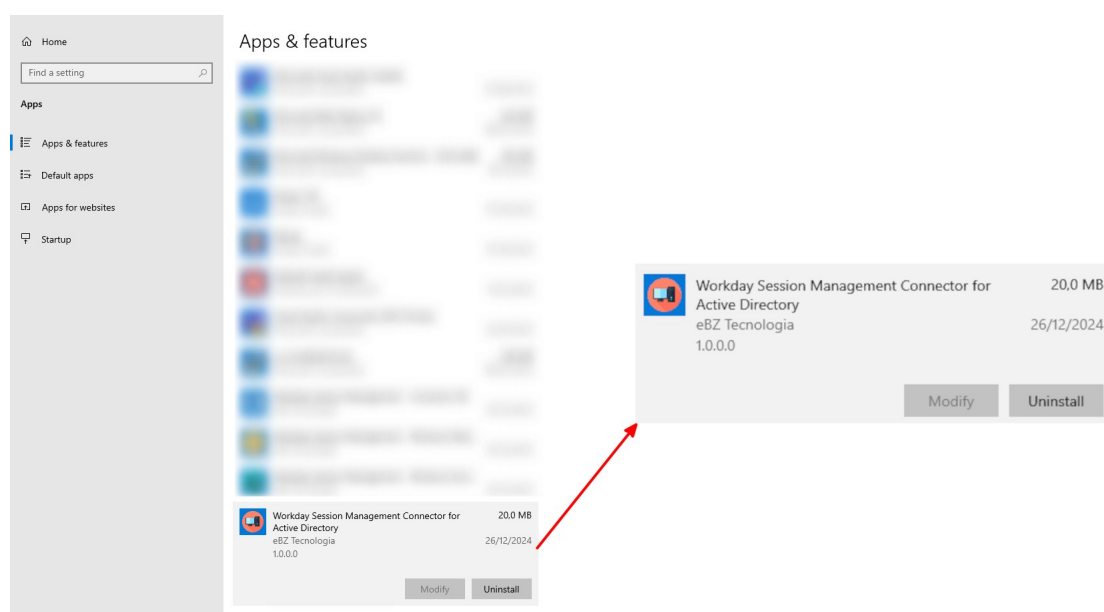


## Verificando a instalação

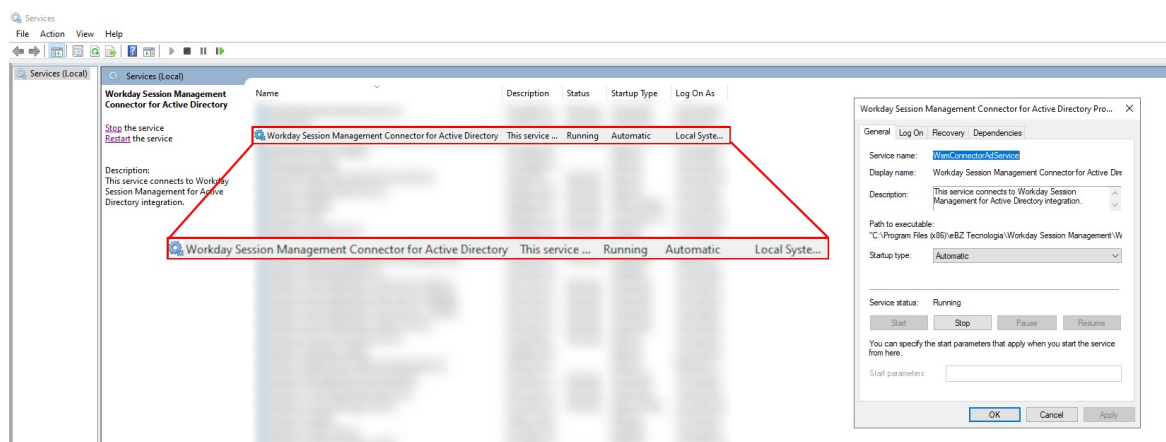
1. Abra o Task Manager (Gerenciador de Tarefas) do Windows e procure por WorkdaySessionManagementConnectorAd.



2. A aplicação também deve aparecer nos aplicativos instalados. No menu inicial, busque por “Apps & Features” ou “aplicativos instalados”.



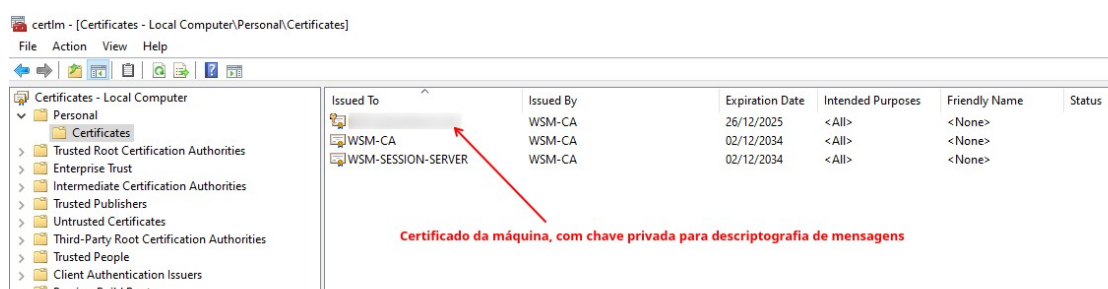
3. Verifique o status do serviço na aplicação “Serviços”, que pode ser iniciada através do menu inicial ou utilizando o comando Win + R, digitando “services.msc” e pressionando OK. Na aba “Log On” deve ser configurado o usuário com permissões para modificar o AD.



4. Verifique se os certificados foram instalados corretamente. O serviço deve carregar 3 certificados: **WSM\_SESSION\_SERVER**, **WSM\_CA** e o certificado com o **FQDN** da máquina onde foi instalado.

Para verificar se a instalação dos certificados ocorreu corretamente, abra a Certificate Store do Windows, buscando por “Manage computer certificates” ou utilizando o comando Win+R, digitando ‘**certmgr.msc**’ (sem aspas) e pressionando OK.

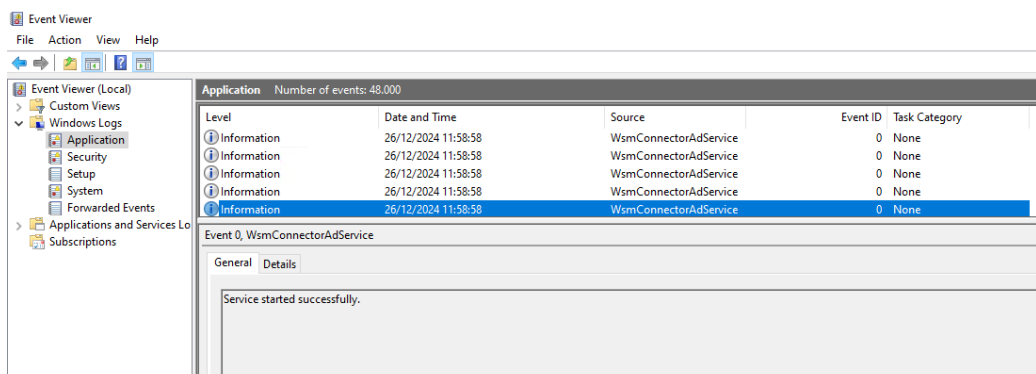
Os certificados devem estar no caminho *Personal > Certificates*.



As chaves do certificado da máquina são geradas localmente. Nenhuma chave privada é armazenada fora da máquina que a criou. As chaves são utilizadas para a troca segura de mensagens entre o serviço e o Session Server, como descritas anteriormente.

5. Caso não estejam armazenados os três certificados, ocorreu um erro de comunicação com o servidor que os envia. Os erros podem ser observados no Visualizador de Eventos do Windows, que é aberto buscando por “Visualizador de

Eventos” ou “Event Viewer” no menu inicial. Para visualizar os *logs*, navegue até *Windows Logs > Application*.



Para resolver possíveis erros, basta navegar até a aplicação **Serviços** (Win+R > *services.msc* > OK), localizar o serviço pelo nome Workday Session Management Connector for Active Directory, selecioná-lo e clicar em “Restart”.

## Desinstalação

Para desinstalar o componente, basta navegar até Aplicativos ou “Apps & features” do Windows, localizar o software “Workday Session Management Connector for Active Directory” e desinstalá-lo.

## Erros e Soluções

- **Erro de Conexão com o AD:**
  - Certificar-se de que as credenciais e o domínio estão corretos.
  - Verificar se o servidor do AD está acessível.
- **Usuário Não Encontrado:**
  - Garantir que o usuário existe no domínio configurado.
- **Horários Inválidos:**
  - Verificar o formato do JSON e certificar-se de que os horários estão corretos.
- **Falta de permissões:**
  - Verificar liberações de firewall para a porta 44901
  - Verificar permissões do usuário configurado para efetuar operações no AD

Logs detalhados de erros podem ser encontrados no Visualizador de Eventos do Windows.