



Banco Safra S.A.

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

Cliente: Banco Safra
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), focando na configuração de horários de logon permitidos. 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 com base em definições fornecidas via JSON.
- Converte automaticamente fusos horários para garantir que os horários definidos sejam aplicados corretamente.
- 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.

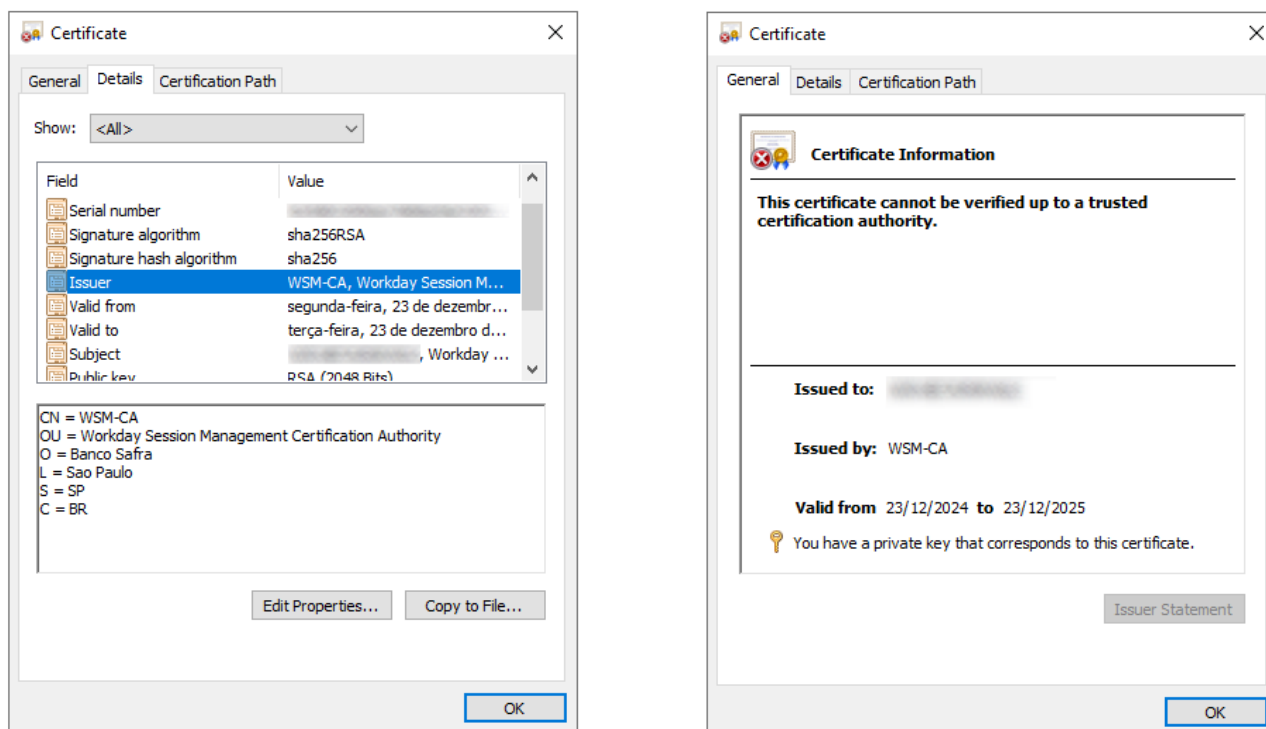
Processo de certificação

O primeiro passo após o início do serviço é o processo de certificação, em que é gerado um par de chave público-privada e é criado um CSR (Certificate Signing Request). O CSR é um pedido de assinatura que é enviado ao Session Server para que a Autoridade Certificadora 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, que contém jornada de horas e dados do usuário. 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

Inicialmente é realizado o processo de certificação descrito anteriormente. 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 com base no JSON fornecido.
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.
- 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

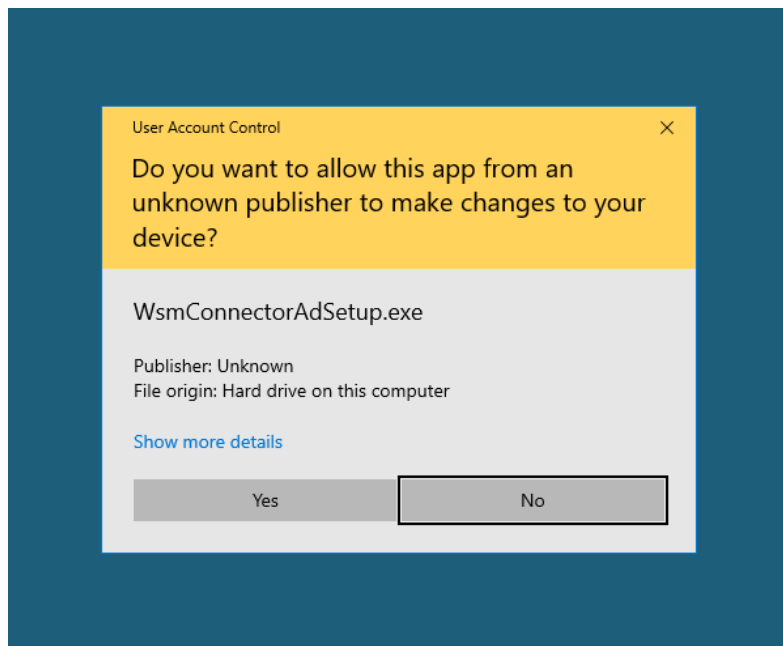
Os horários de trabalho permitidos são recebidos de forma encriptada pelo Session Server em uma string JSON no seguinte formato:

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

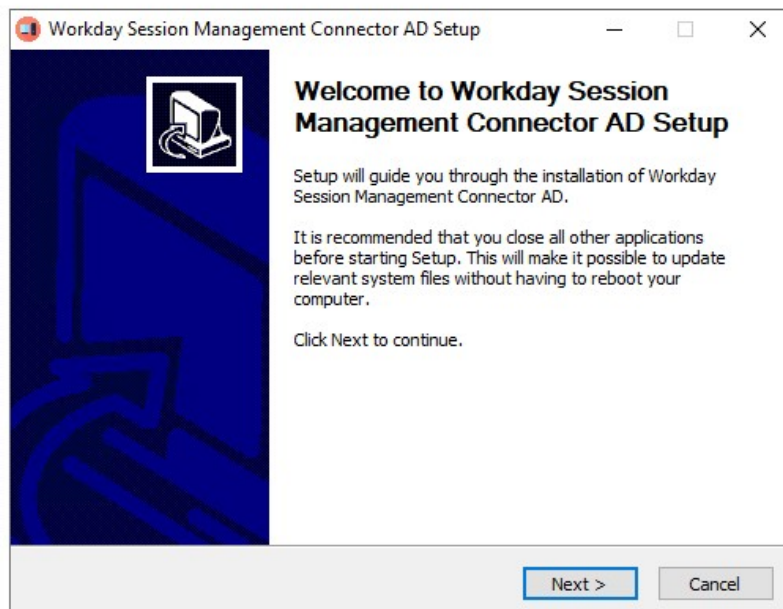
Em que *uid* representa o usuário cadastrado no AD e os valores representam minutos após a meia-noite. Exemplo: 480 (minutos após a meia-noite) equivale às 8h da manhã.

Como executar o instalador

1. Autorize a instalação com privilégios administrativos



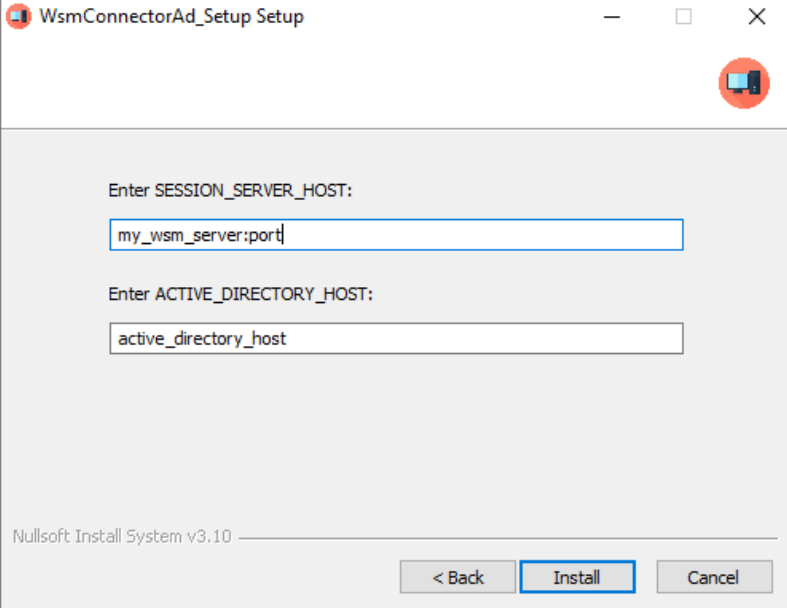
2. Página inicial do instalador:



3. Configuração dos parâmetros:

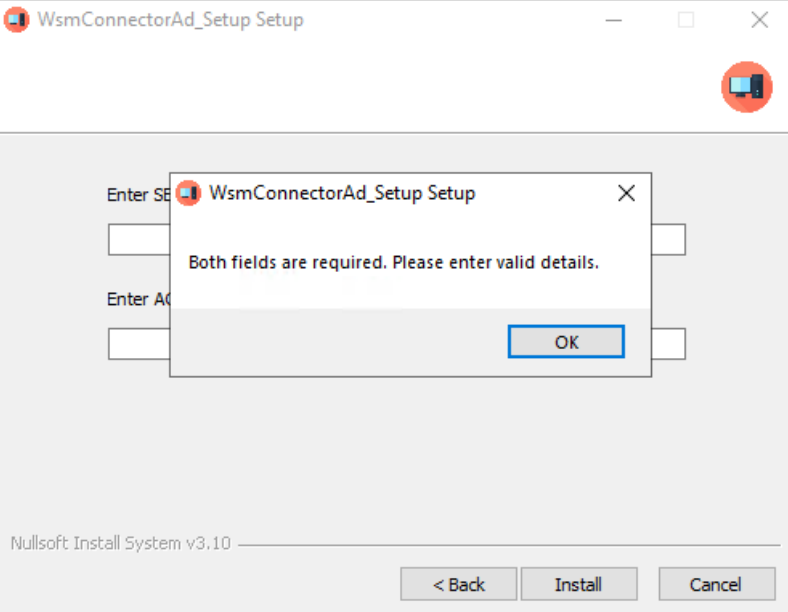
- O instalador requer dois parâmetros:

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', and 'Cancel'. The 'Install' button is highlighted with a blue border. The window title bar shows 'WsmConnectorAd_Setup Setup' and standard Windows window controls. A small icon of a computer with a red circle is in the top right corner.

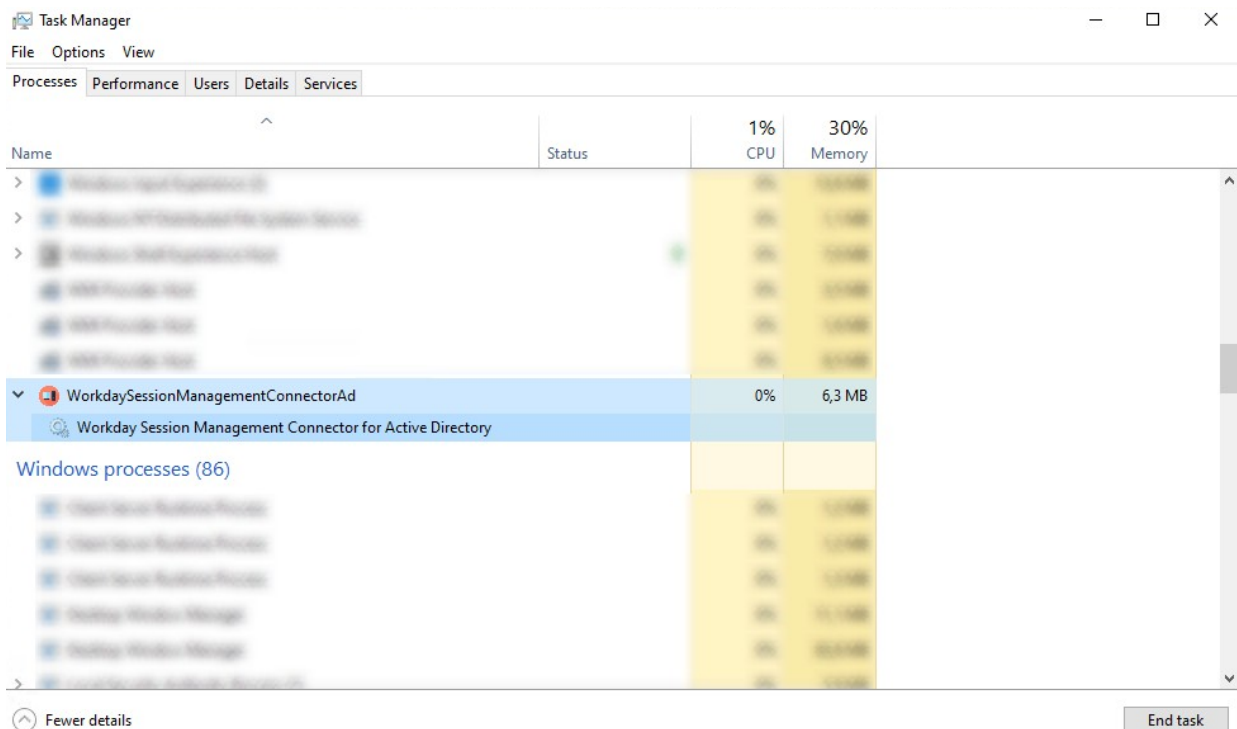
- Os dois campos são obrigatórios



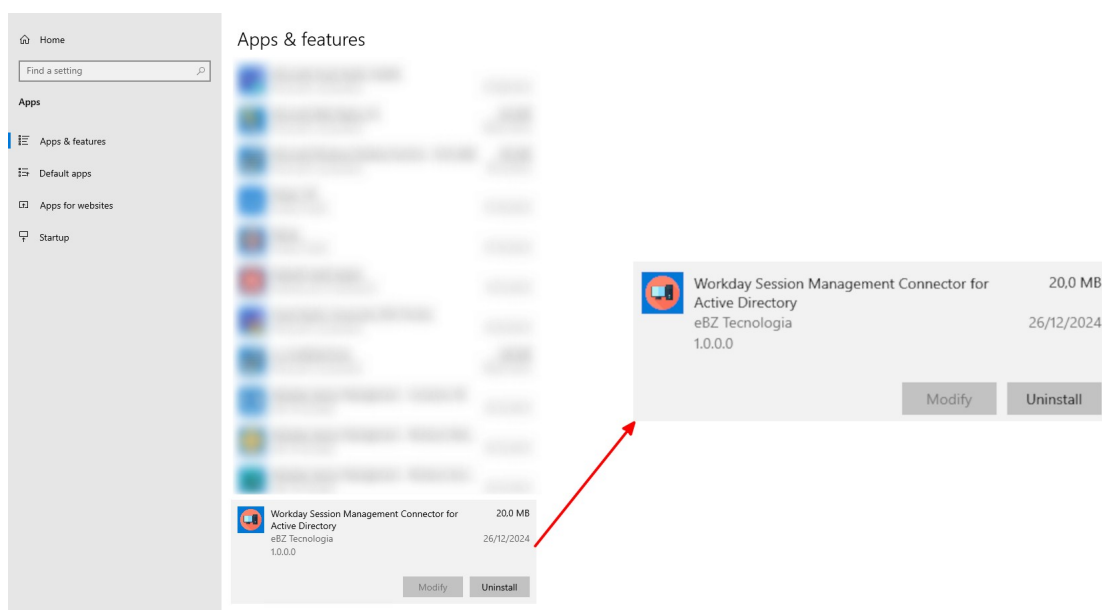
The screenshot shows the 'WsmConnectorAd_Setup Setup' window with an error dialog box overlaid. The dialog box has the title 'WsmConnectorAd_Setup Setup' and a close button. The message inside says 'Both fields are required. Please enter valid details.' with an 'OK' button. The background window shows the same input fields as before, but they are partially obscured by the dialog box. The 'Install' button is still highlighted. The window title bar and icons are the same as in the previous screenshot.

Verificando a instalação

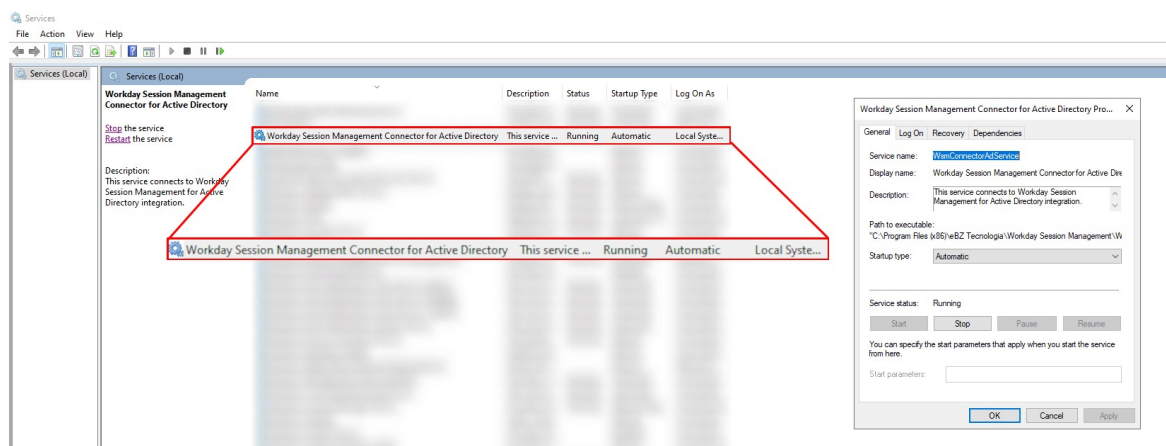
1. Abra o Task Manager (Gerenciador de Tarefas) do Windows e procure por WorkdaySessionManagementConnectorAd.



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

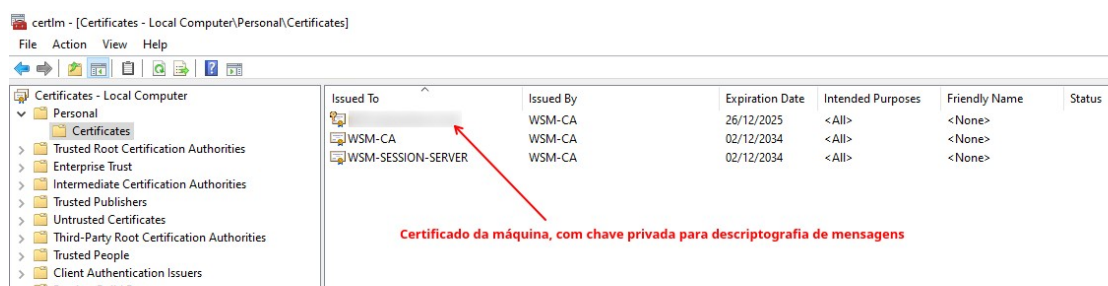


3. Verifique o status do serviço na aplicação “Serviços”, que pode ser iniciada através do menu inicial ou utilizando o comando Win + R, digitando “services.msc” e pressionando OK.



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. Os dois primeiros são buscados no Session Server e o terceiro é gerado pela Autoridade Certificadora (CA) configurada no Session Server.

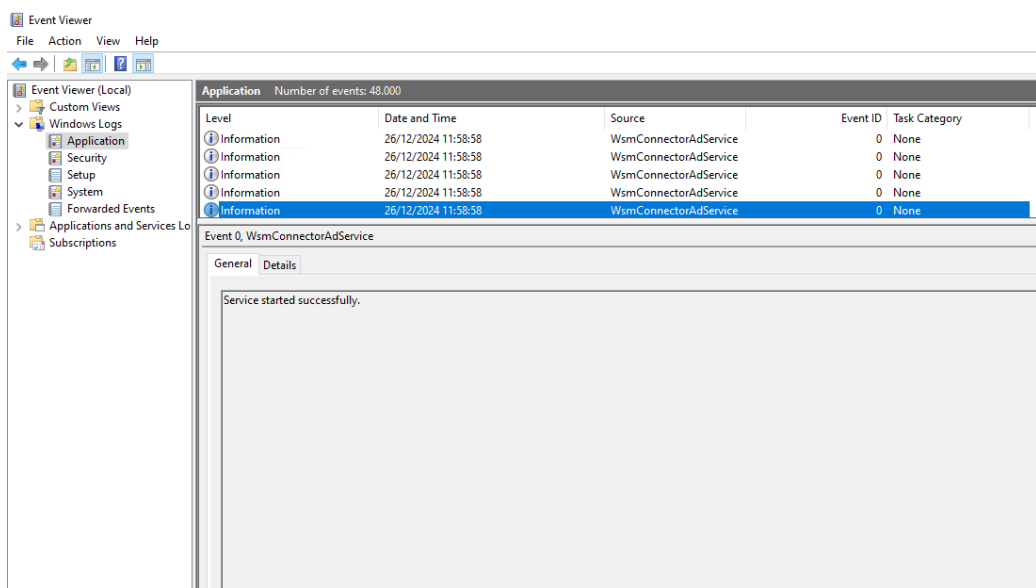
Para verificar se a instalação dos certificados ocorreu corretamente, abra a Certificate Store do Windows, buscando por “Manage computer certificates” ou utilizando o comando Win+R, digitando ‘**certmgr.msc**’ (sem aspas) e pressionando OK. Os certificados devem estar no caminho *Personal > Certificates*.



As chaves do certificado da máquina são geradas localmente e é criado um CSR (*Certificate Signing Request*), que é enviado à autoridade certificadora. A CA, por sua vez, assina este certificado e o devolve à máquina que realizou a solicitação de assinatura. 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.

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