



TECNOLOGIA

Banco Safra S.A.

WSM Windows Agent

***Definição do módulo Aplicação WSM responsável
pelo controle de jornada e notificação das máquinas***

Cliente: Banco Safra
Projeto: Controle de jornadas - Workday Session Management
Documento: Documentação
Versão: 1.0
Data: 26/12/2024
Autor: Gabriel Silva Ribeiro

Índice

Introdução.....	3
Visão de Negócio.....	3
Windows Desktop Agent.....	3
Componentes do agente.....	4
Logs e chaves.....	4
Startup.....	4
Funcionamento do agente.....	4
Windows Session Service.....	5
Componentes do serviço.....	6
Logs.....	6
Chaves.....	6
Certificados.....	6
Endereços.....	6
Funcionamento do serviço.....	7
Eventos.....	7
Heartbeat.....	7
Vigilância.....	7
Implementação.....	8
Configuração TXT Record no DNS.....	8
Windows AD.....	8
Instalação dos módulos.....	10
Desinstalação dos módulos.....	11

Introdução

Este documento tem como objetivo apresentar o desenho proposto para implantação do *Windows Session Service* e *Desktop Agent*, responsáveis pela atualização de horário de jornada de trabalho dos usuários nas respectivas estações, gerenciamento e vigilância de sessões ativas, assim como, apresentar notificações e interações ao usuário final.

Visão de Negócio

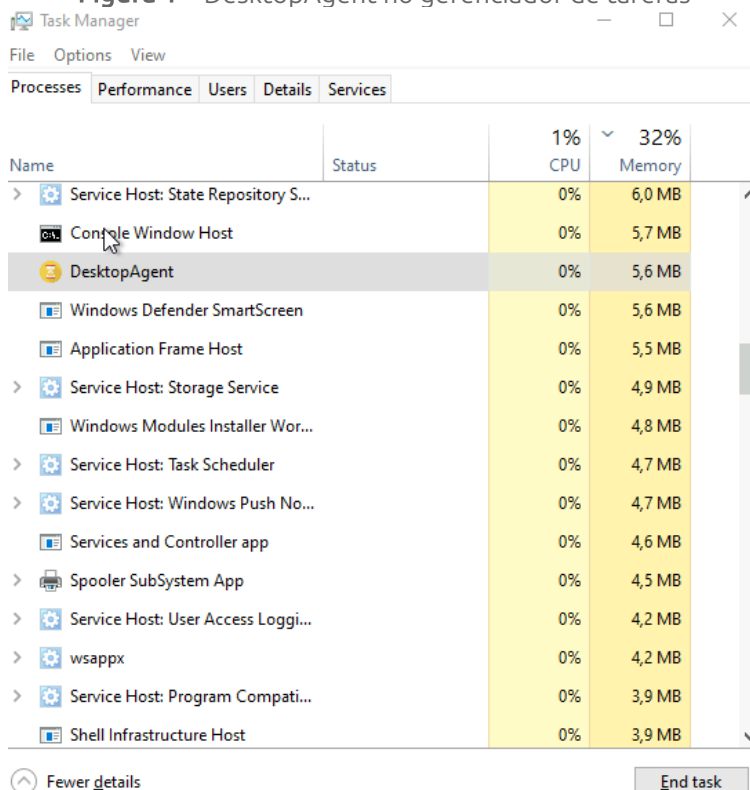
Este componente auxilia o gerenciamento dos horários de trabalho do ponto de vista da aplicação WSM .

Este componente deverá se comunicar com o “*WSM Router*” para gerenciar os *status* das sessões ativas, atualizar o banco de dados e receber comandos via ZeroMQ.

Windows Desktop Agent

O Windows Desktop Agent é uma aplicação rodando no *background* do sistema operacional para cada usuário, iniciando automaticamente ao realizar o login na estação de trabalho. Essa aplicação é responsável por notificar o usuário sobre as alterações realizadas na sua jornada de trabalho, receber mensagens personalizadas, identificar uma violação de horário e notificar antes de desconectar, assim como, criar interações (*pop-ups*) de aceite para o usuário.

Figura 1 – DesktopAgent no gerenciador de tarefas



The image shows a screenshot of the Windows Task Manager application. The 'Performance' tab is selected, displaying a list of running processes. The 'DesktopAgent' process is highlighted. The table below represents the data shown in the screenshot.

Name	Status	1% CPU	32% Memory
Service Host: State Repository S...		0%	6,0 MB
Control Window Host		0%	5,7 MB
DesktopAgent		0%	5,6 MB
Windows Defender SmartScreen		0%	5,6 MB
Application Frame Host		0%	5,5 MB
Service Host: Storage Service		0%	4,9 MB
Windows Modules Installer Wor...		0%	4,8 MB
Service Host: Task Scheduler		0%	4,7 MB
Service Host: Windows Push No...		0%	4,7 MB
Services and Controller app		0%	4,6 MB
Spooler SubSystem App		0%	4,5 MB
Service Host: User Access Loggi...		0%	4,2 MB
wsappx		0%	4,2 MB
Service Host: Program Compati...		0%	3,9 MB
Shell Infrastructure Host		0%	3,9 MB

Componentes do agente

Após a instalação do Windows Desktop Agent, alguns componentes serão criados e instalados nos seus respectivos diretórios padrões. A aplicação e suas dependências ficarão em:

C:\Program Files (x86)\eBZ Tecnologia\Workday Session Management\WSM Desktop Agent

Logs e chaves

O agente também possui um arquivo de log, que irá registrar as mensagens recebidas pelo usuário e as respostas do mesmo para eventos de interação. Este arquivo de log compartilhará o diretório com as chaves pública e privada do agente (utilizadas para estabelecer comunicação segura com o serviço windows), o par de chaves é gerado durante a primeira inicialização da aplicação.

C:\Users\<usuario>\AppData\Roaming\eBZ Tecnologia\Workday Session Management

Startup

Por fim, a instalação do agente gera um atalho no diretório *startup* do windows, responsável por garantir que a aplicação seja iniciada durante o *login* do usuário. Remover este atalho significa que o usuário não mais receberá notificações das ações do serviço.

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

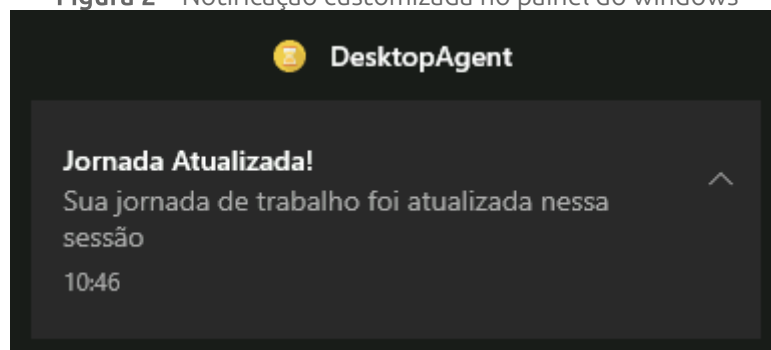
Funcionamento do agente

A aplicação recebe mensagens de outro componente do sistema (referenciado aqui como serviço windows) através de um JSON criptografado, interpreta a mensagem e realiza uma das respectivas ações:

- Interact: Apresenta um painel de opções para o usuário, acompanhado de mensagem e título;
- Lock: Notificação padrão de que a sessão será trancada;
- Logoff: Notificação padrão de que a sessão encerrará em 10 segundos;
- Notify: Notificação customizada para apresentar ao usuário.

Toda mensagem recebida fora deste escopo é imprimida no log como um erro, inclusive erros de conexão com o endereço e porta. O Agente aguarda por mensagens vindas do serviço windows no seguinte endereço: **tcp://localhost:12345**

Figura 2 – Notificação customizada no painel do windows



Windows Session Service

O Windows Session Service (também chamado de *Session Service* ou apenas serviço windows) é um serviço windows rodando no *background* do sistema operacional com privilégios de administrador, possui apenas uma instância e gerencia todos os usuários ativos, iniciando automaticamente com o *boot* da estação de trabalho. Esse serviço possui muitas responsabilidades, entre elas estão:

- ◆ Leitura e envio de eventos de *Logon/Logoff* e *Lock/Unlock* para o *WSM Router*;
- ◆ Controle de sessões ativas;
- ◆ Recebimento de ações do *WSM Router*;
- ◆ Registro e controle dos horários de trabalho das sessões ativas;
- ◆ Vigilância de atuação dos usuários;
- ◆ Desconexão de usuário em atuação indevida;
- ◆ Log de atividades das sessões.

Figura 3 – SessionService no gerenciador de tarefas e serviços

Windows Connection Manager	Makes auto...	Running	Automatic (T...	Local Service
Windows Defender Advanced Threat Protection Service	Windows D...		Manual	Local Syste...
Windows Defender Firewall	Windows D...	Running	Automatic	Local Service
Windows Encryption Provider Host Service	Windows E...		Manual (Trig...	Local Service
Windows Error Reporting Service	Allows error...		Manual (Trig...	Local Syste...
Windows Event Collector	This service ...		Manual	Network S...
Windows Event Log	This service ...	Running	Automatic	Local Service
Windows Font Cache Service	Optimizes p...	Running	Automatic	Local Service
Windows Image Acquisition (WIA)	Provides im...		Manual	Local Service
Windows Insider Service	Provides inf...		Disabled	Local Syste...
Windows Installer	Adds, modi...		Manual	Local Syste...
Windows License Manager Service	Provides inf...	Running	Manual (Trig...	Local Service
Windows Licensing Monitoring Service	This service ...	Running	Automatic	Local Syste...
Windows Management Instrumentation	Provides a c...	Running	Automatic	Local Syste...
Windows Media Player Network Sharing Service	Shares Win...		Manual	Network S...
Windows Modules Installer	Enables inst...		Manual	Local Syste...
Windows Push Notifications System Service	This service ...	Running	Automatic	Local Syste...
Windows Push Notifications User Service_2d53bed	This service ...	Running	Automatic	Local Syste...
Windows Push Notifications User Service_4b0a7	This service ...	Running	Automatic	Local Syste...
Windows PushToInstall Service	Provides inf...		Disabled	Local Syste...
Windows Remote Management (WS-Management)	Windows R...	Running	Automatic	Network S...
Windows Search	Provides co...		Disabled	Local Syste...
Windows Security Service	Windows Se...	Running	Manual	Local Syste...
Windows Time	Maintains d...		Manual (Trig...	Local Service
Windows Update	Enables the ...		Manual (Trig...	Local Syste...
Windows Update Medic Service	Enables rem...		Manual	Local Syste...
WinHTTP Web Proxy Auto-Discovery Service	WinHTTP i...	Running	Manual	Local Service
Wired AutoConfig	The Wired A...		Manual	Local Syste...
WMI Performance Adapter	Provides pe...		Manual	Local Syste...
Workday Session Management Connector for Active Dir...	This service ...		Disabled	Local Syste...
Workstation	Creates and...	Running	Automatic	Network S...
WSM-Windows-Service		Running	Automatic	Local Syste...

Task Manager			
File Options View			
Processes Performance Users Details Services			
		7%	37%
		CPU	Memory
Name	Status		
ServiceHub.IndexingService.exe		0%	41,5 MB
ServiceHub.VSDetouredHost.exe		0%	41,0 MB
MSBuild.exe		0%	32,8 MB
Microsoft.ServiceHub.Controller		0%	31,6 MB
ServiceHub.ThreadedWaitDialog...		0%	30,0 MB
Start (2)		0%	29,1 MB
Windows PowerShell		0%	24,8 MB
Service Host: Windows Event Log		0%	23,6 MB
SessionService		0%	23,2 MB
Settings		0%	22,9 MB
Task Manager		0%	19,7 MB
Desktop Window Manager		0%	19,2 MB
ServiceHub.TestWindowStoreH...		0%	18,9 MB
Service Host: UtcSvc		0%	16,1 MB
Runtime Broker (3)		0%	15,1 MB
Fewer details		End task	

Componentes do serviço

Após a instalação do Windows Session Service, alguns componentes serão criados e instalados nos seus respectivos diretórios padrões. A aplicação e suas dependências ficarão em:

C:\Program Files (x86)\eBZ Tecnologia\Workday Session Management\WSM-Windows-Service

Logs

O serviço possui um arquivo de log, que irá registrar as mensagens recebidas do *WSM-Router*, erros, ações realizadas e *status* do serviço como *uptime* e endereços.

C:\Program Files (x86)\eBZ Tecnologia\Workday Session Management

Chaves

Durante a inicialização, o serviço irá gerar (caso não exista) um par de chaves para realizar a comunicação local e criptografada com o agente, o arquivo **publisher_communication.key** é público e deve permanecer com permissões amplas de leitura para que o agente possa autoconfigurar-se, já o arquivo **publisher_secret.key** deve permanecer privado e acessível apenas para a administração. O par de chaves deve estar em:

C:\Program Files (x86)\eBZ Tecnologia\Workday Session Management

Certificados

A primeira comunicação com o *WSM-Router* estabelece as chaves a serem utilizadas e gera os certificados necessários para que essa comunicação passe a ser criptografada daqui para frente, utilizando um sistema robusto. Após certificação com a Certificate Authority, três certificados serão armazenados no *windows certificate manager* para a máquina atual:

Figura 4 – Certificados visualizados no mmc

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
CA_IDMEXT	CA_IDMEXT	17/08/2034	<All>	<None>		
localhost	localhost	06/08/2029	Server Authenticati...	IIS Express Develop...		
midpoint:win-be7ur9nv6ls	CA_IDMEXT	16/12/2025	<All>	<None>		
MIDPOINT_IDMEXT	CA_IDMEXT	29/08/2025	<All>	<None>		
WIN-BE7UR9NV6LS	WSM-CA	23/12/2025	<All>	<None>		
WSM-CA	WSM-CA	02/12/2034	<All>	<None>		
WSM-SESSION-SERVER	WSM-CA	02/12/2034	<All>	<None>		

Endereços

O serviço se configura automaticamente (endereço e porta) ao consultar o *TXT Record* do domínio, para isso, é necessário especificar no TXT da seguinte forma:

wsm_session_servers=<IP/FQDN>:<porta>, <IP/FQDN>:<porta>

Exemplo:

wsm_session_servers=wsm_session_servers=wsmserver1.example.com:51555,wsmserver2.example.com:51555

Funcionamento do serviço

O serviço ao inicializar pela primeira vez, gera um par de chaves para a criptografia *CURVE*, usada na comunicação segura com os agentes, em seguida, checa a existência dos certificados que, caso não existam, são requisitados para CA, a fim de estabelecer o padrão de criptografia e comunicação segura com o *WSM Router*. O serviço lê do *TXT Record* o endereço do *router* para realizar seus processos, em caso de falha ou não existência, estabelecerá conexão com o endereço **tcp://localhost:5555**. Sem um endereço válido para a CA e *Router*, o serviço deverá ser reiniciado para funcionar adequadamente.

O *Session Server* recebe os *payloads* criptografados e encripta seus próprios antes de enviar ao *Router*.

Após descriptografar, o serviço interpreta a mensagem e realiza uma das respectivas ações:

- Interact: Formata o payload para o agente e envia as informações de interação;
- Lock: Envia notificação padrão de lock para o agente e bloqueia a sessão alvo;
- Logoff: Envia notificação padrão de que a sessão encerrará em 10 segundos para o agente, deslogando o usuário na sequência;
- Notify: Formata o payload para o agente e envia as informações de notificação;
- Ping: Retorna para o *Router* as informações de instalação do client e seu *uptime*;
- UpdateHours: Atualiza os horários de trabalho permitidos para o alvo especificado.

Toda mensagem recebida fora deste escopo é imprimida no log como um erro, inclusive erros de conexão com o endereço e porta.

Eventos

É feito o monitoramento do *event viewer* do windows com o objetivo de identificar eventos de *lock/unlock* e *logon/logoff*. Após a identificação, o serviço atualiza sua lista de sessões ativas de usuários e notifica o servidor de sessões para manter o banco atualizado. O servidor, por sua vez, retorna uma resposta apropriada ao evento disparado, seja uma mensagem de conformidade ou uma ação de *logoff* (caso um usuário não permitido realize o *login*).

Heartbeat

A cada trinta minutos, o serviço notifica o servidor, enviando suas informações de instalação e seu *uptime*, isso serve para mostrar que o serviço ainda está ativo e capaz de se comunicar.

Vigilância

O Serviço verifica periodicamente a lista de sessões ativas para certificar-se de que estes usuários podem estar acessando a máquina em dado momento, em caso de não conformidade, tais sessões são desconectadas.

Implementação

Esta seção tem como objetivo demonstrar o passo-a-passo para implementar este módulo do Workday Session Management.

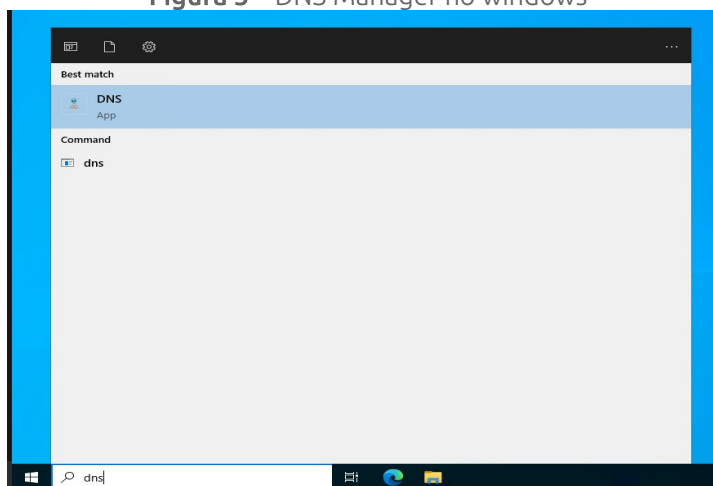
Configuração TXT Record no DNS

Este passo pode variar de acordo com o gerenciador de DNS utilizado, o procedimento aqui documentado diz respeito ao gerenciamento de DNS via Windows AD.

Windows AD

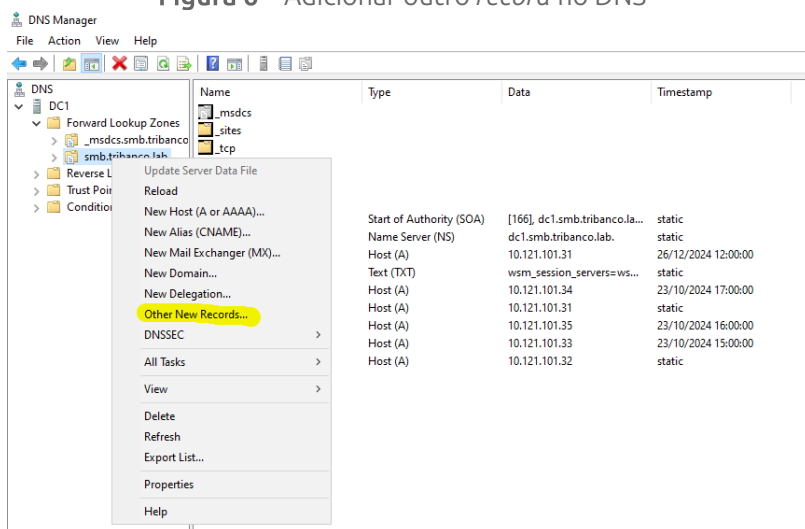
1. Abra o gerenciador de DNS:

Figura 5 – DNS Manager no windows



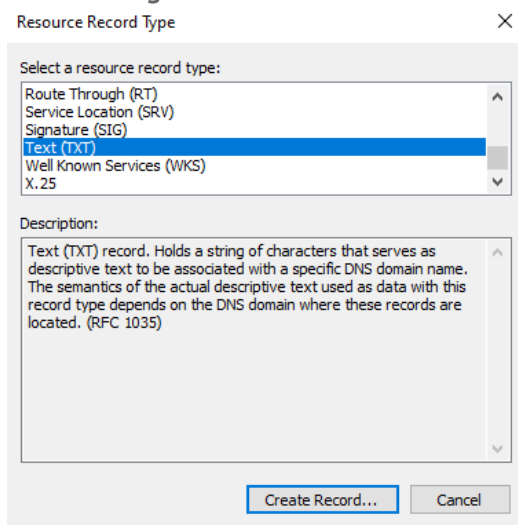
2. No *DNS Manager*, expandir o nome da máquina e ir para *Forward Lookup Zone*, botão direito no dns e *clique em Other New Records...*

Figura 6 – Adicionar outro record no DNS



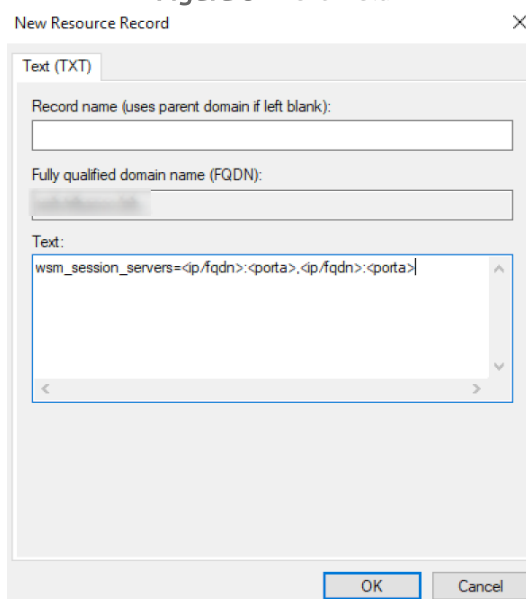
3. Selecione o tipo como *Text* e crie o *Record*

Figura 7 – Text Record



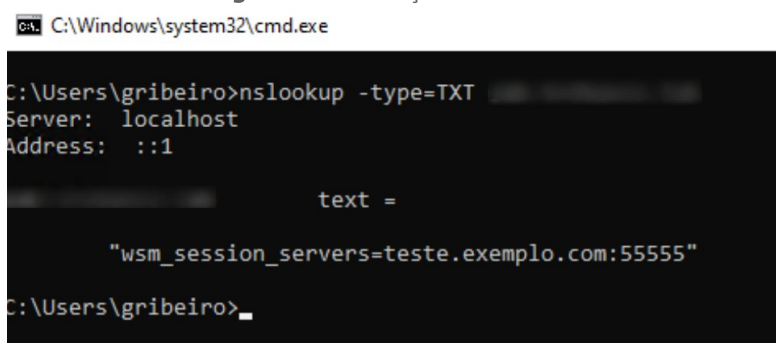
4. Preencha o campo *text* com o padrão informado na documentação, substituindo os campos <ip/fqdn> e <porta> pelos valores corretos e clique em OK

Figura 8 – Text Field



5. (opcional) Valide utilizando o seguinte comando no cmd: **nslookup -type=TXT <DOMAIN>**

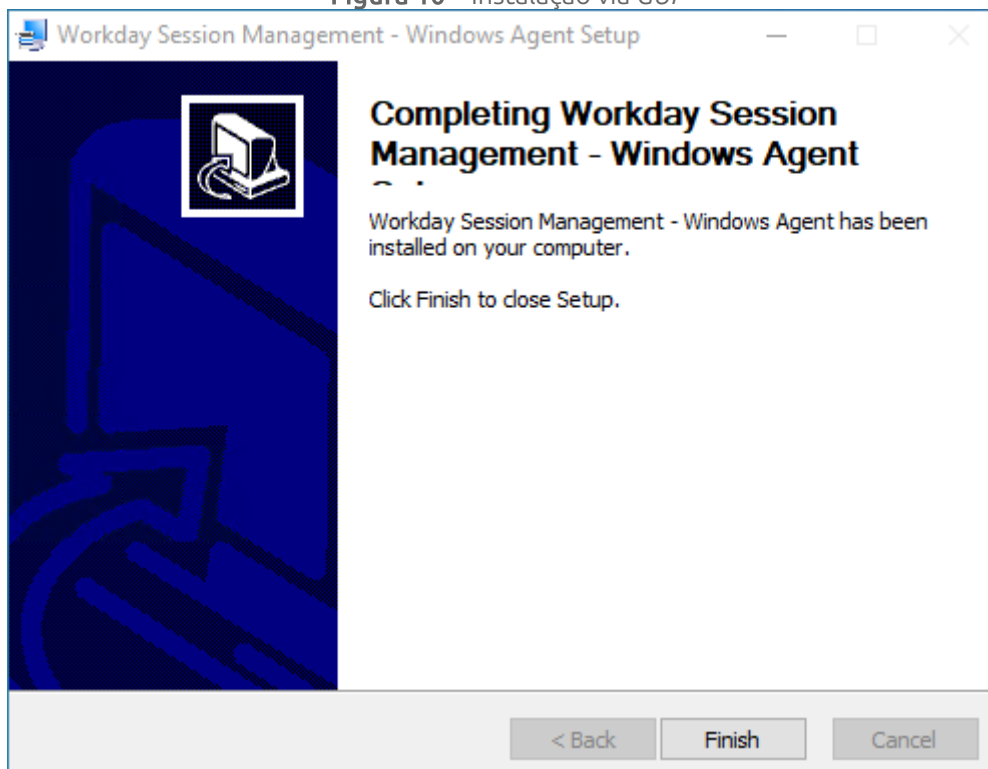
Figura 9 – Validação no CMD



Instalação dos módulos

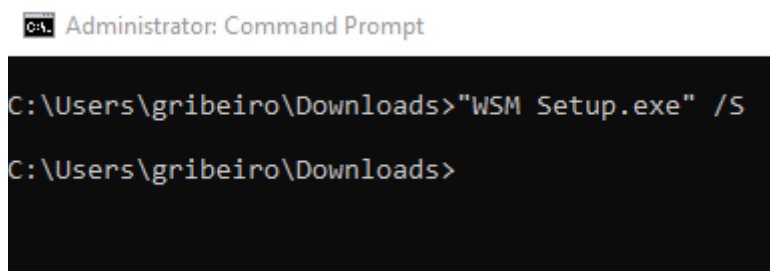
Ambos os módulos são instalados com a execução do instalador **WSM Setup** (é possível instalar os componentes individualmente com os instaladores **WSM Desktop Agent Setup** e **WSM Service Setup**), incluindo o *runtime .NET* necessário para o funcionamento das aplicações. É possível instalar tudo seguindo as instruções via interface gráfica ou, alternativamente, em modo silencioso pelo prompt de comando:

Figura 10 – Instalação via GUI



Utilizando o cmd (como administrador), é necessário navegar até o diretório onde está localizado o instalador e executar a seguinte linha de comando: **"WSM Setup.exe" /S**

Figura 11 – Instalação via CMD



Desinstalação dos módulos

Os módulos devem ser desinstalados individualmente, é possível desinstalar tanto através das configurações do windows → Apps, quanto pelo executável de desinstalação (chamado de Uninstall.exe) contido no diretório de cada aplicação.

Figura 12 – Desinstalação via configurações do windows
Apps & features

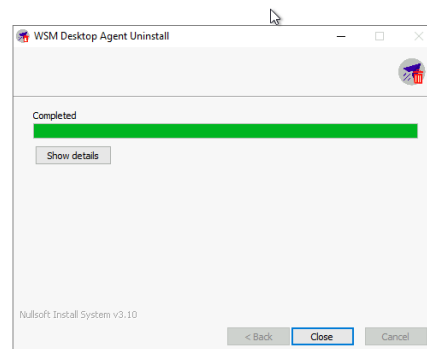
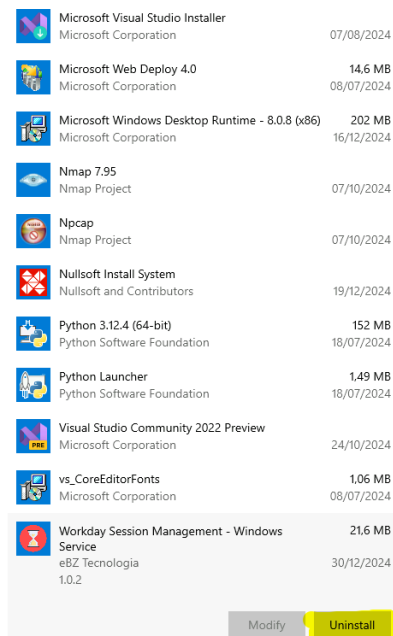
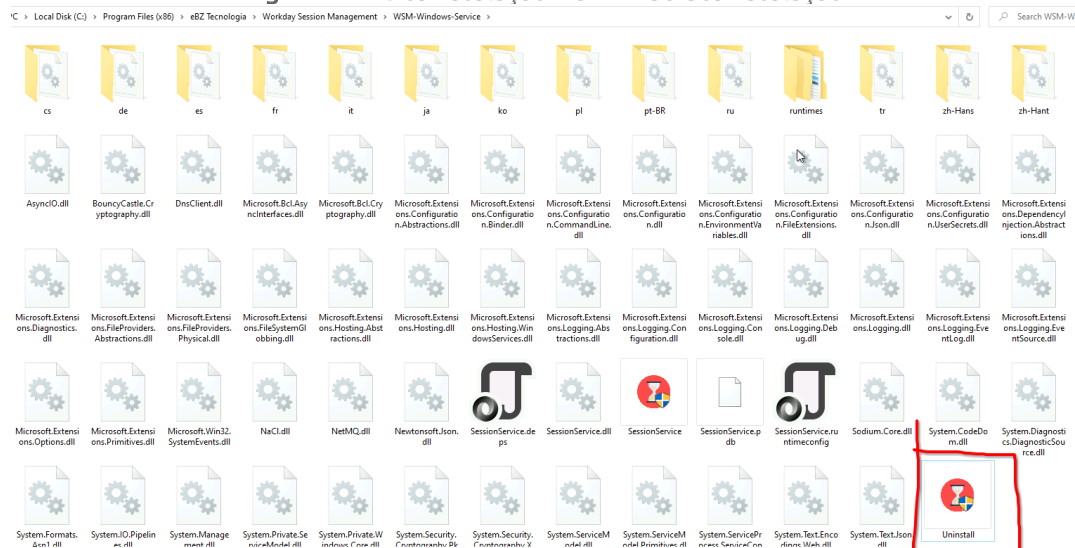


Figura 13 – Desinstalação via EXE de desinstalação



É possível realizar a desinstalação dos componentes através do prompt de comando em modo silencioso, utilizando o mesmo procedimento de instalação e apenas substituindo pelo comando: **"Uninstall.exe" /S**