AvantScan

Documentação de uso da ferramenta AvantScan

Introdução ao módulo AvantScan

AvantScan é o módulo do AvantData que executa varreduras de vulnerabilidades. A ideia é processar os dados encontrados e gerar informação, melhorando o conhecimento da equipe de segurança sobre a infraestrutura monitorada.

O AvantScan age indexando todas as vulnerabilidades encontradas no AvantData, correlacionando com fontes de inteligência externas ou ainda com outras entradas de dados, criando um CMDB (Banco de dados de Gerenciamento de Configuração) dos ativos encontrados e possibilitando fazer a gestão das vulnerabilidades dentro da solução, incluindo o tratamento e a mitigação de riscos. Para isso, é possível configurar varreduras autenticadas ou não autenticadas, que vão alimentar os dashboards de gerenciamento de vulnerabilidades.

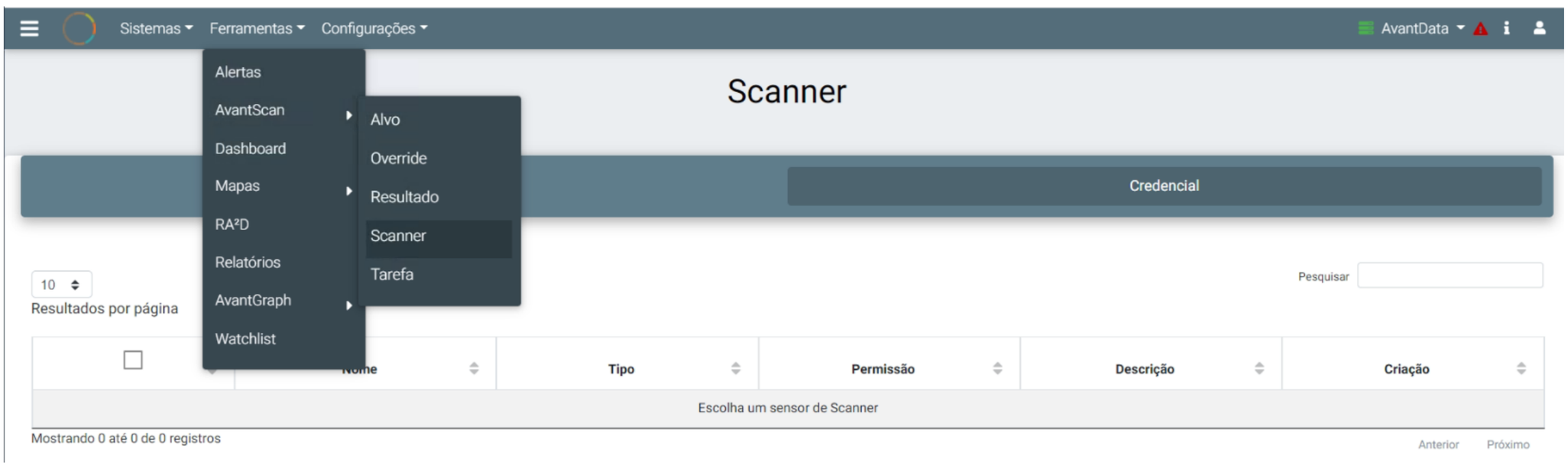
Documentação – AvantScan

Para executar uma varredura, antes, é preciso decidir se a varredura será autenticada ou não. A varredura autenticada consegue logar nas máquinas e ter acesso a mais informações, checando bibliotecas e softwares instalados quanto a vulnerabilidades conhecidas, independente de serviços abertos.

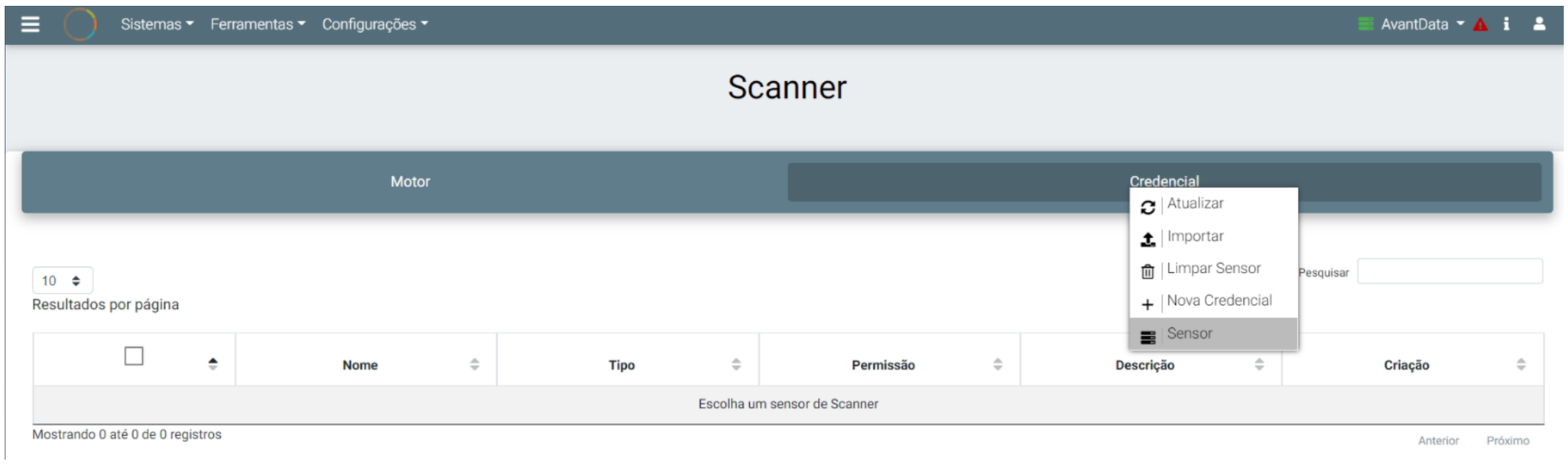
Segue abaixo os passos para configurar uma varredura autenticada no AvantScan:

Passo 1: Selecione o SENSOR.

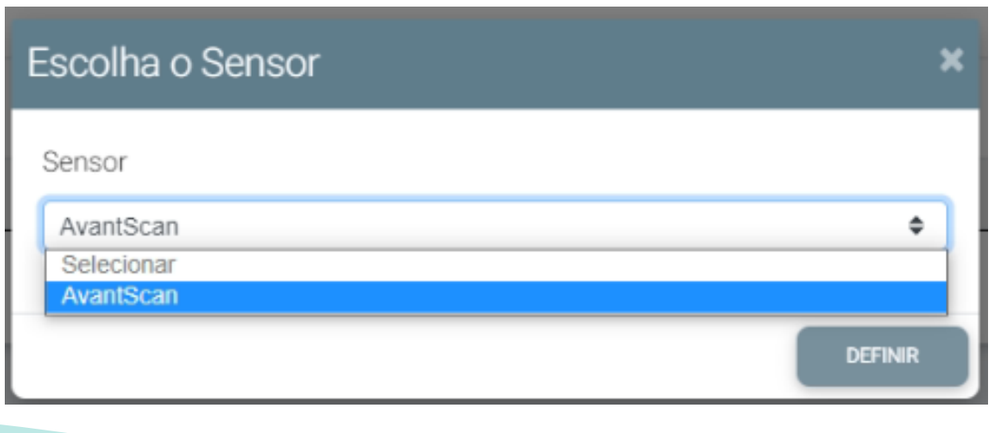
Clique em Ferramentas > AvantScan > Scanner > Credencial.



Clique com o botão direito em Credencial e depois em Sensor.



Escolha o Sensor.

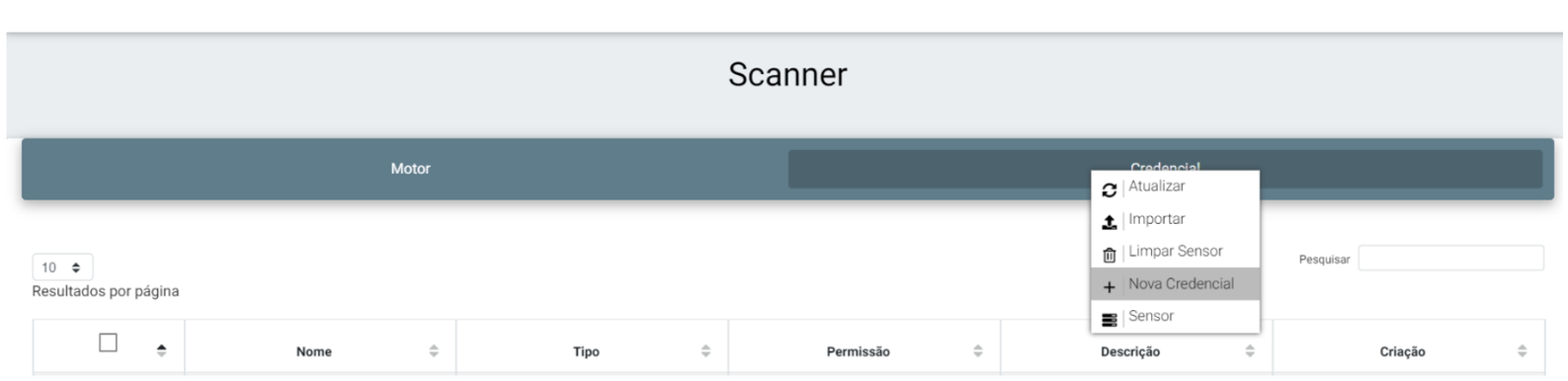


Documentação – AvantScan

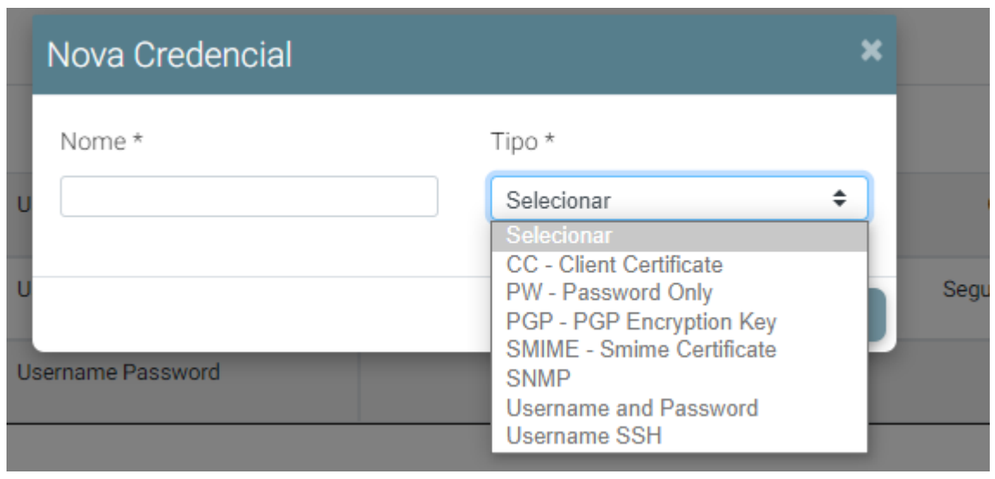
Passo 2: Criar a CREDENCIAL.

Obs: O cadastro de credenciais só é utilizado para varreduras autenticadas, caso não seja essa a intenção pule para o próximo passo.

Com o sensor definido, clique com o botão direito novamente em Credencial e no menu de contexto clique em Nova Credencial.



Na modal que irá aparecer, escolha o nome e o tipo da credencial.



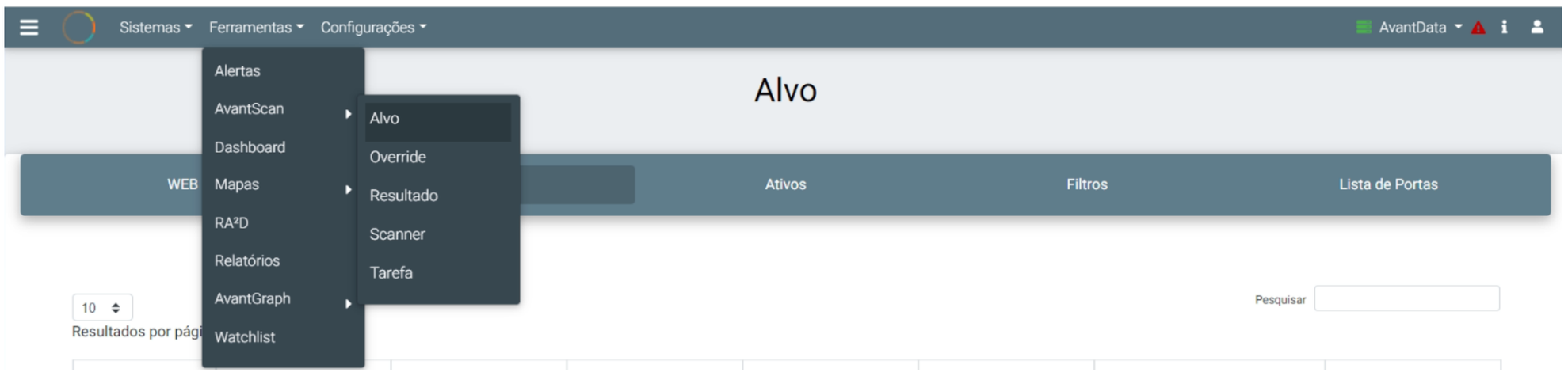
Obs: Use "**Username and Password**" para configurar a autenticação em máquinas Windows ou compartilhamentos SMB.

Documentação – AvantScan

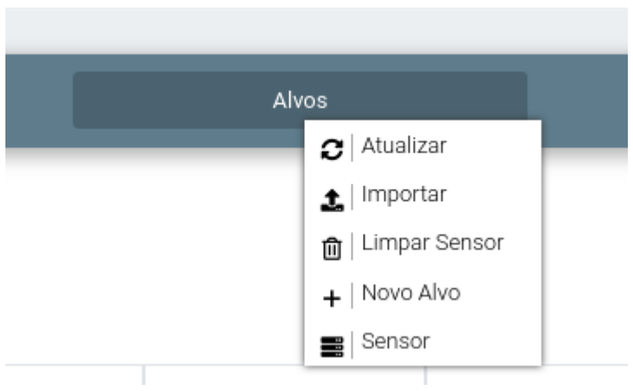
Obs: O Modo Inseguro definido para "Verdadeiro", significa que a credencial pode ser usada em protocolos que não exigem tráfego seguro, como FTP ou Telnet. Ao definir "Verdadeiro", o AvantScan tenta usar a autenticação de forma segura, caso a aplicação não suporte, ele usará o modo inseguro.

Passo 3: Criar o ALVO.

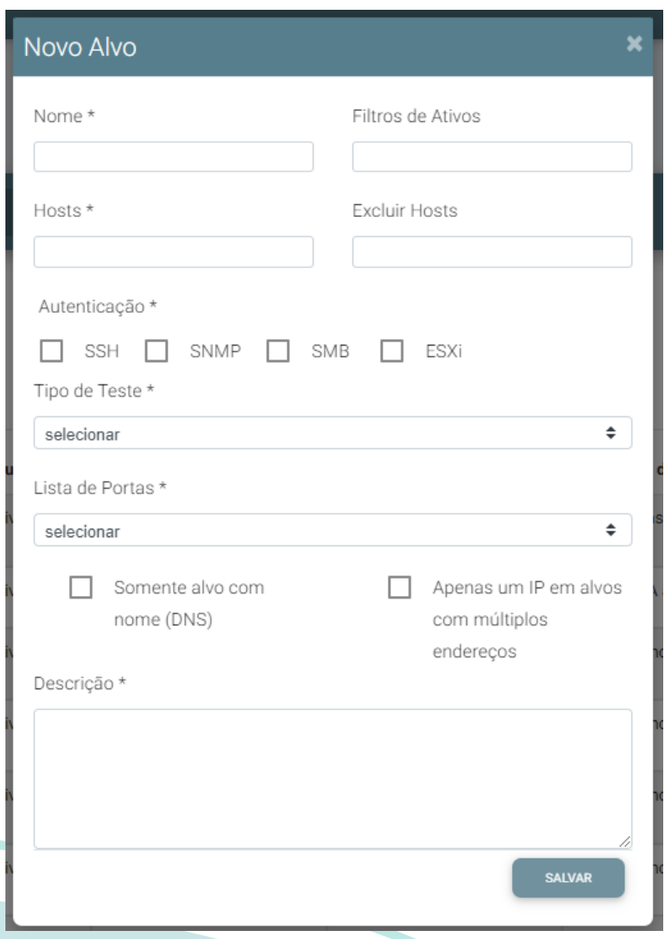
Clique em Ferramentas > AvantScan > Alvo.



Clique com o botão direito em Alvos, e em Novo Alvo.



Cadastre o novo alvo.



Documentação – AvantScan

Nome: é como o Alvo será identificado no AvantData

Hosts: são um ou mais endereços IPs de dispositivos ou redes que serão varridas. Separe múltiplos endereços por vírgula.(Aceita notação CIDR ex: 192.0.2.0/24)

Filtros de Ativos: Filtros que podem ser aplicados para selecionar apenas um ou mais ativos que devem ser contemplados na varredura.

Exemplos de filtros que podem ser feitos:

Targets	Targets with a specific UUID	uuid	UUID	
	Targets with a specific name	name	String	
	Targets with a specific comment	comment	String	
	Targets with a specific creation time	created	Date and time in ISO 8601 format	Example: "2011-11-08T19:57:06+02:00"
	Targets with a specific modification time	modified	Date and time in ISO 8601 format	Example: "2011-11-08T19:57:06+02:00"
	Targets with a specific owner	owner	String	
	Targets with a specific host	hosts	String	
	Targets with a specific excluded host	exclude_hosts	String	
	Targets with a specific number of IP addresses	ips	Positive integer	
	Targets with a specific port list	port_list	String	
	Targets with a specific SSH credential	ssh_credentials	String	
	Targets with a specific SMB credential	smb_credentials	String	
	Targets with a specific ESXi credential	esxi_credentials	String	
	Targets with a specific SNMP credential	snmp_credentials	String	

"Excluir Hosts" (esse campo aceita notação CIDR): Excluir um endereço de host ou de rede da varredura, como uma exceção da rede ou endereços definido em "Hosts"

Autenticação: Caso tenha credencial criada, selecionar qual o tipo e selecionar a credencial cadastrada.

Tipo do teste: O tipo de teste define o teste que deve ser feito antes de varrer um host para saber se ele é um IP ativo dentro dos hosts informados.

Lista de Portas: A lista de portas define as portas que serão varridas para identificação dos serviços, CPEs e vulnerabilidades. É possível criar uma lista de portas customizadas em Ferramentas > AvantScan > Alvo > LIsta de Portas

Somente alvo com nome (DNS): Ao marcar esta opção, a varredura vai varrer apenas os hosts encontrados que tenha nome registrado no DNS.

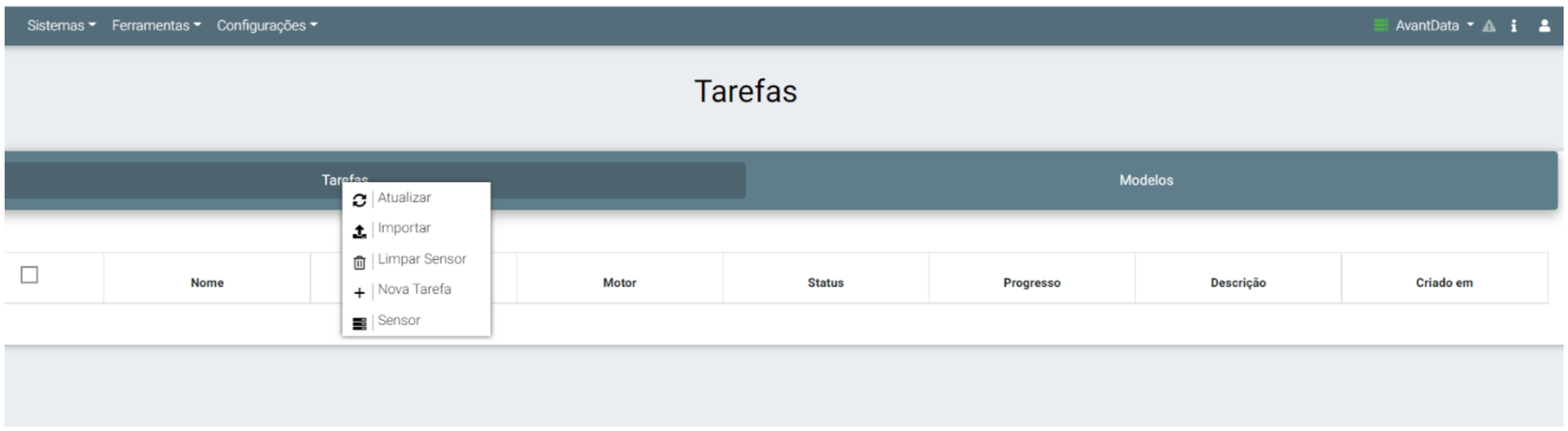
Apenas um IP em alvos com múltiplos endereços: Ao marcar esta opção, quando a varredura descobrir um host com mais de um endereço IP, ela vai varrer apenas o primeiro IP encontrado.

Passo 4: Criar uma nova TAREFA.

Para criar uma tarefa clique em Ferramentas > AvantScan > Tarefa.

Documentação – AvantScan

Clique com o botão direito em Tarefas e selecione Nova Tarefa.



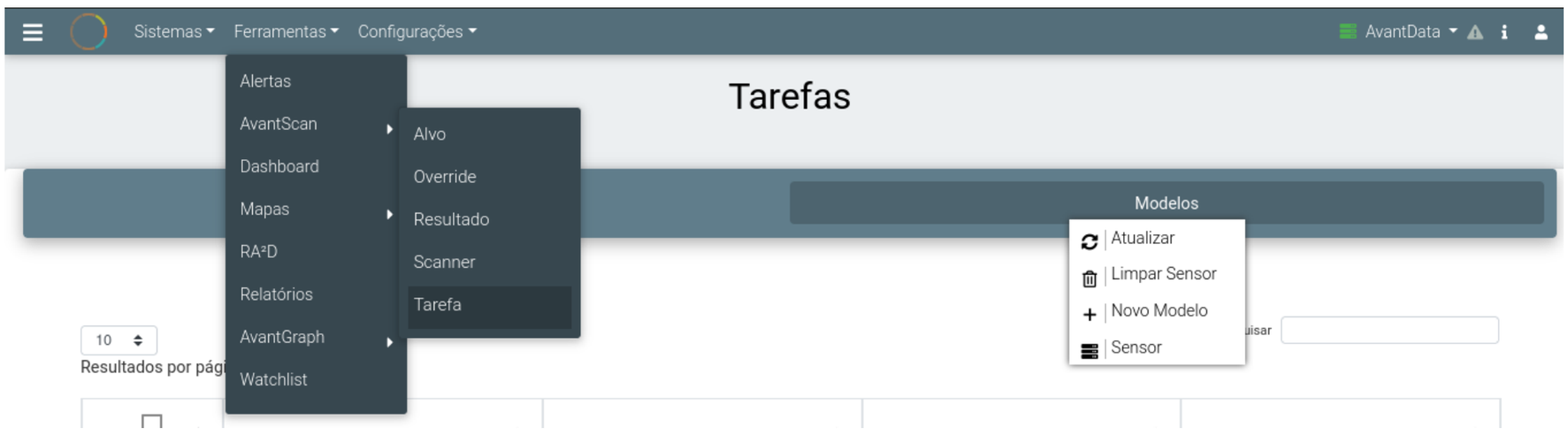
Na modal a seguir insira as informações necessárias:.

Nova Tarefa: nome para a tarefa que está sendo criada.

Motor: é o motor que realizará a varredura. É possível cadastrar outros motores para a varredura, mas na grande maioria das vezes o OpenVas é o motor que utilizaremos dentro do AvantScan.

Alvo: selecionar o alvo que foi criado no Passo 3.

Modelo: o modelo define o escopo da varredura e pode ser personalizado conforme a necessidade.

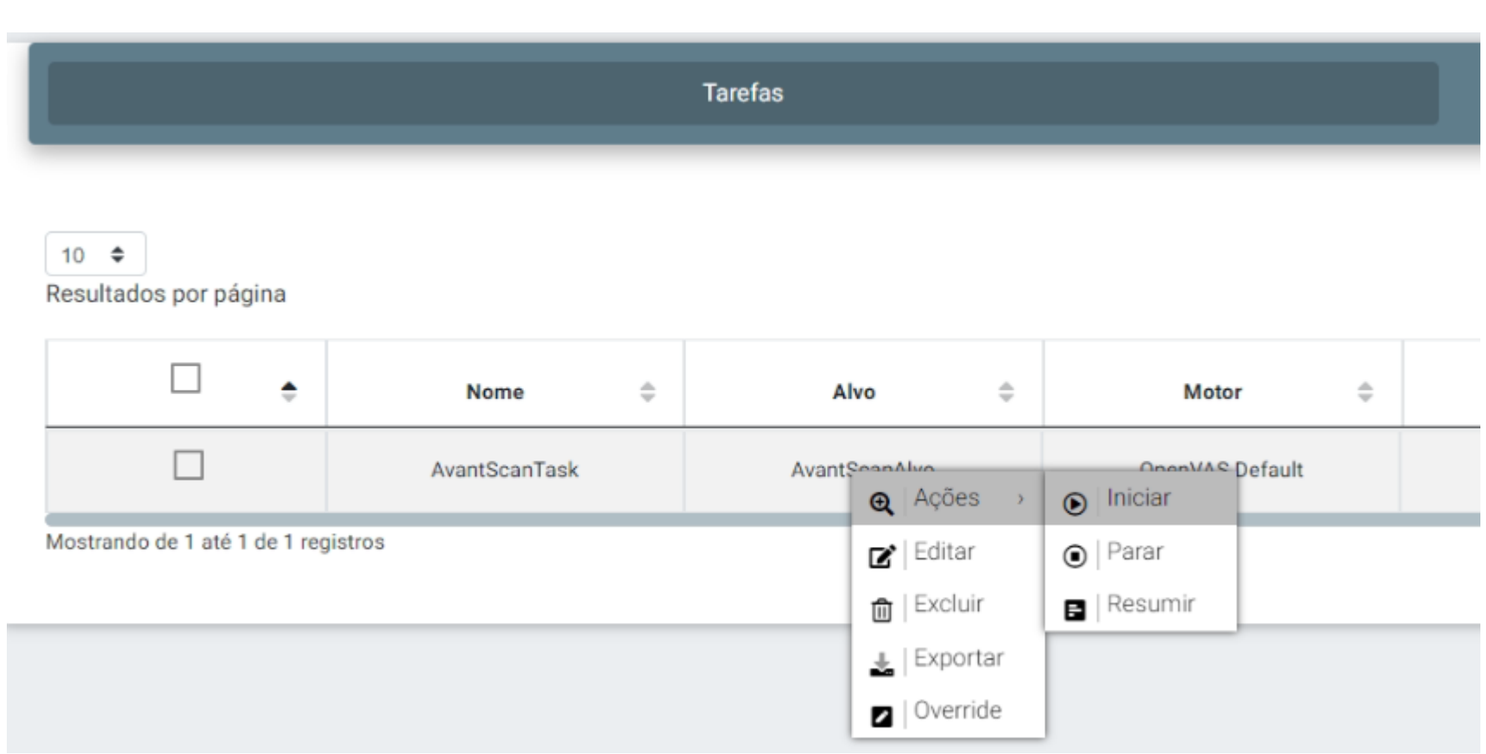


Documentação – AvantScan

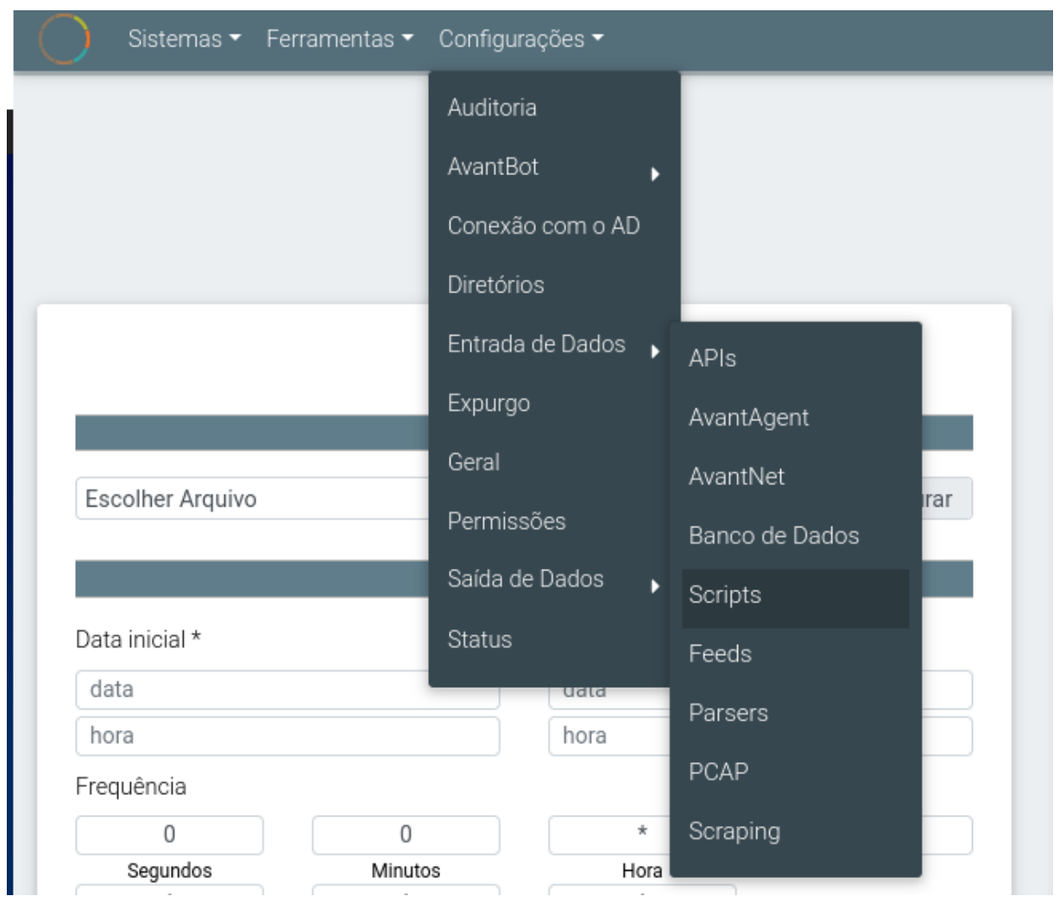
Passo 5 : Iniciar a VARREDURA.

A varredura pode ser iniciada de duas formas: manual ou agendada.

Para iniciar a varredura manual basta clicar com o botão direito na tarefa que foi criada no passo anterior e clicar em Ações › Iniciar

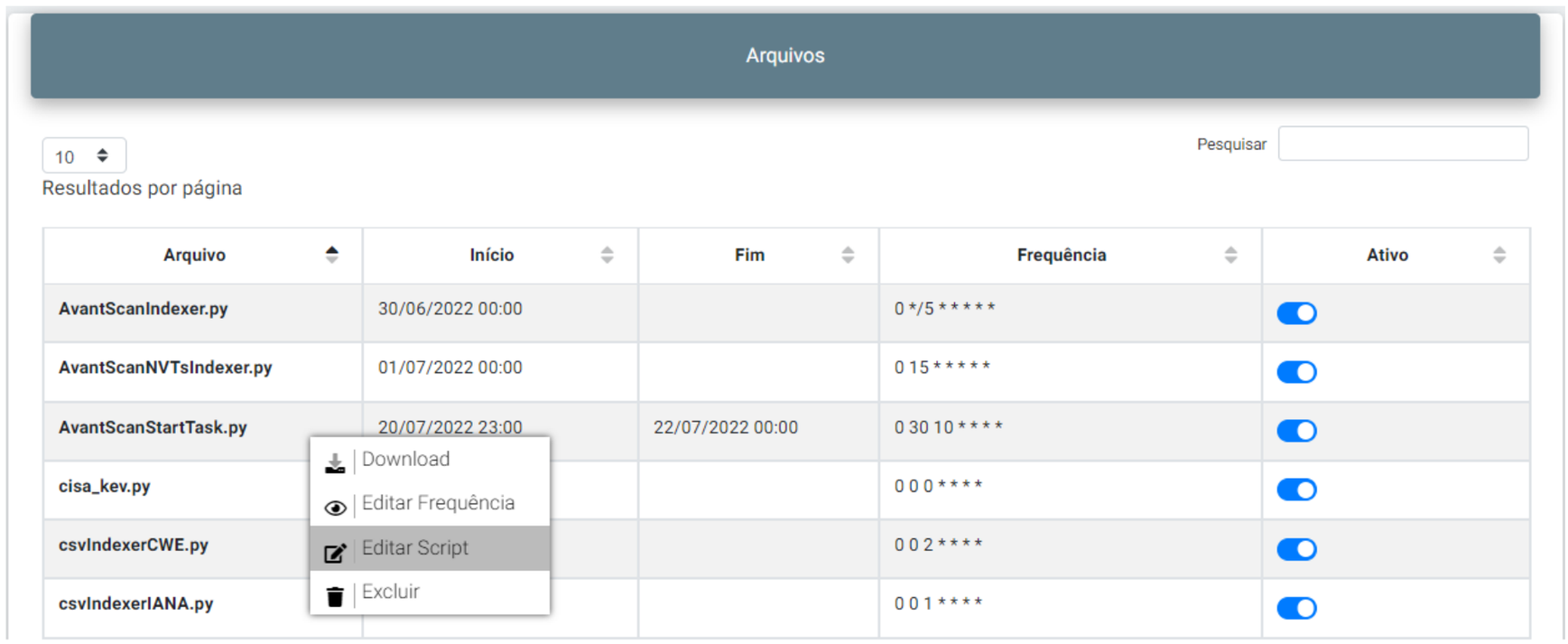


A varredura agendada é realizada por meio de um script chamado ‘‘AvantScanStartTask.py’’, que fica localizado no caminho: Configurações › Entrada de Dados › Scripts.

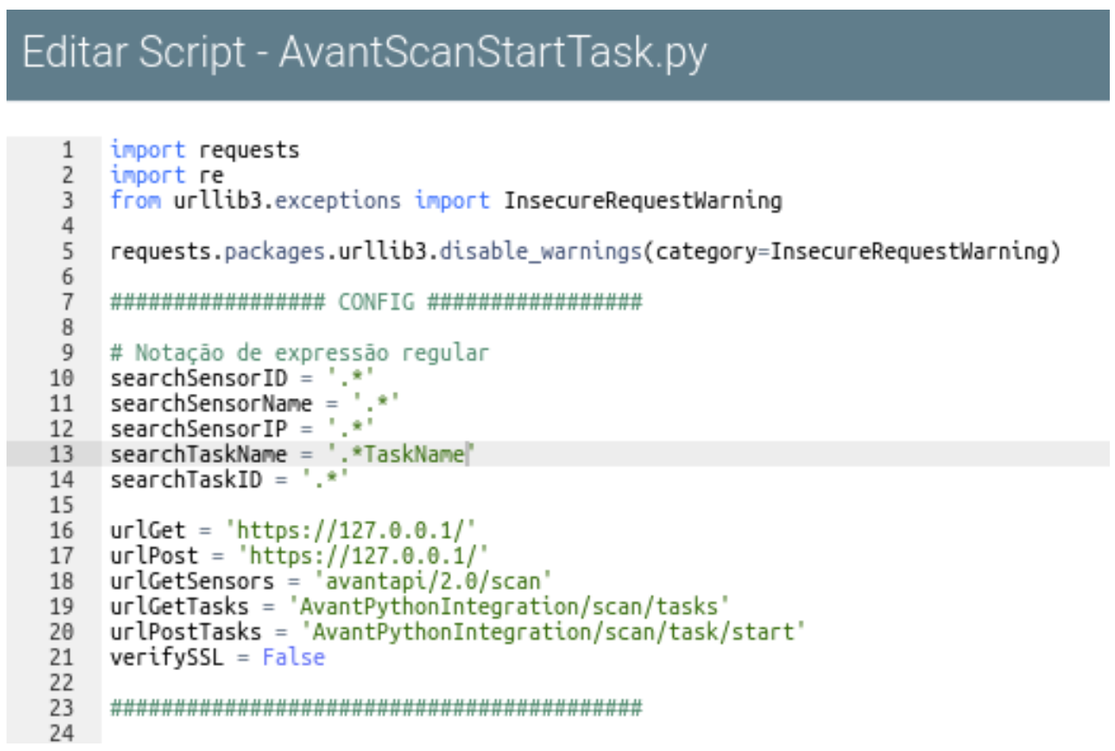


Documentação – AvantScan

É preciso clicar com o botão direito no script e em seguida clicar em Editar Script.

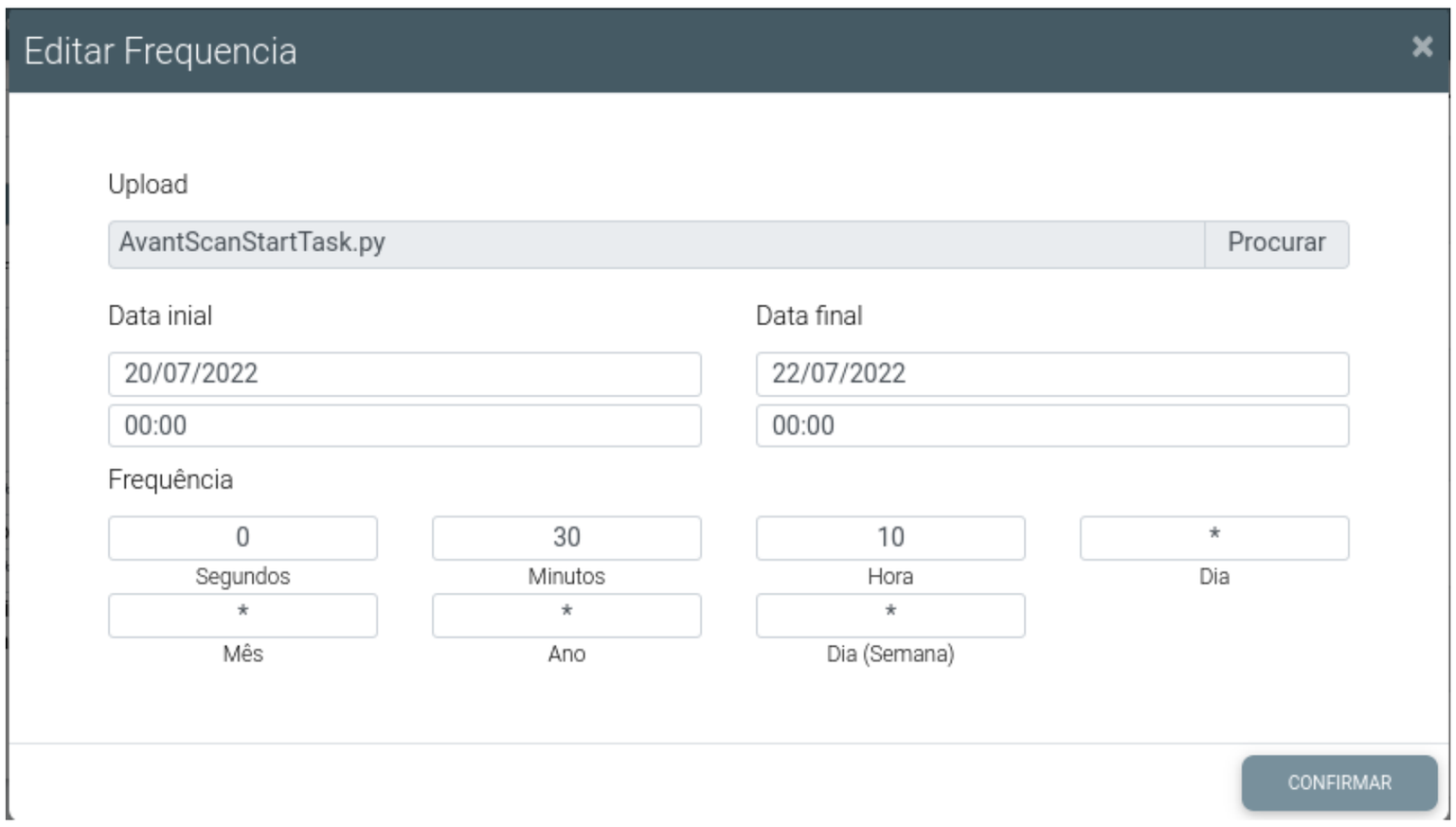


Uma nova modal será aberta onde é necessário editar o script. Coloque o nome da tarefa que foi criada no campo "searchTaskName".



O próximo passo é editar o agendamento da tarefa, que pode ser executada uma única vez ou repetida periodicamente. Usamos o formato de crontab estendido, onde é possível definir uma data/hora inicial e final para as repetições, além de definir exatamente a hora ou segundo em que a tarefa deve ser iniciada. .

Documentação – AvantScan



No exemplo acima, a tarefa será executada, todos os dias às 10:30:00 entre os dias 20/07/2022 e 22/07/2022.
Uma frequência é composta por 7 campos. Os campos podem conter qualquer um dos valores permitidos, juntamente com várias combinações dos caracteres especiais permitidos para esse campo.

Os campos são:

Nome do Campo	Obrigatoriedade	Valores Permitidos	Caracteres Especiais Permitidos
Segundos	SIM	0-59	, - * /
Minutos	SIM	0-59	, - * /
Horas	SIM	0-23	, - * /
Dia do mês	SIM	1-31	, - * ? / LW
Mês	SIM	1-12 ou JAN-DEC	, - * /
Dia da semana	SIM	1-7 ou SUN -SAT	, - * ? / L #
Ano	NÃO	vazio, 1970-2099	, - * /