

Descrição: Descreve como instalar, a partir de um arquivo o Snare em máquinas Windows, para que seja possível direcionarmos os logs do eventviewer do Windows para o OpMon(OpLogs).

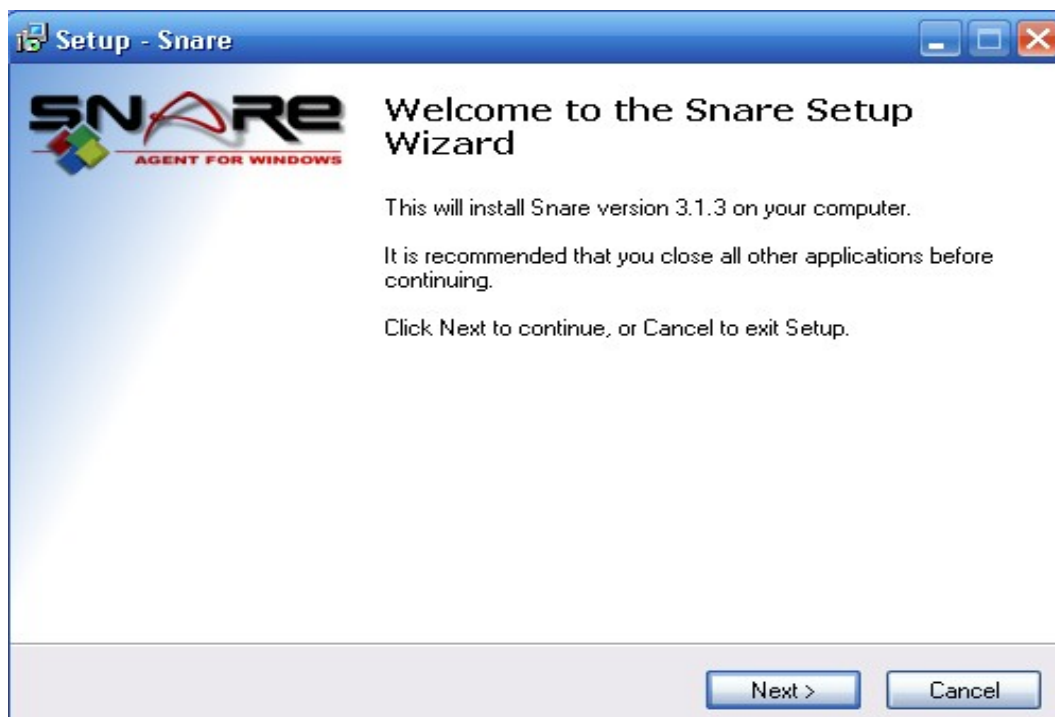
AVISO: Em caso de problemas em qualquer passo do procedimento, enviar o conteúdo da tela para a OpServices pelo email (suporte@opservices.com.br).

A instalação é composta por 1 arquivo:
SnareSetup-3.1.3-MultiArch.exe

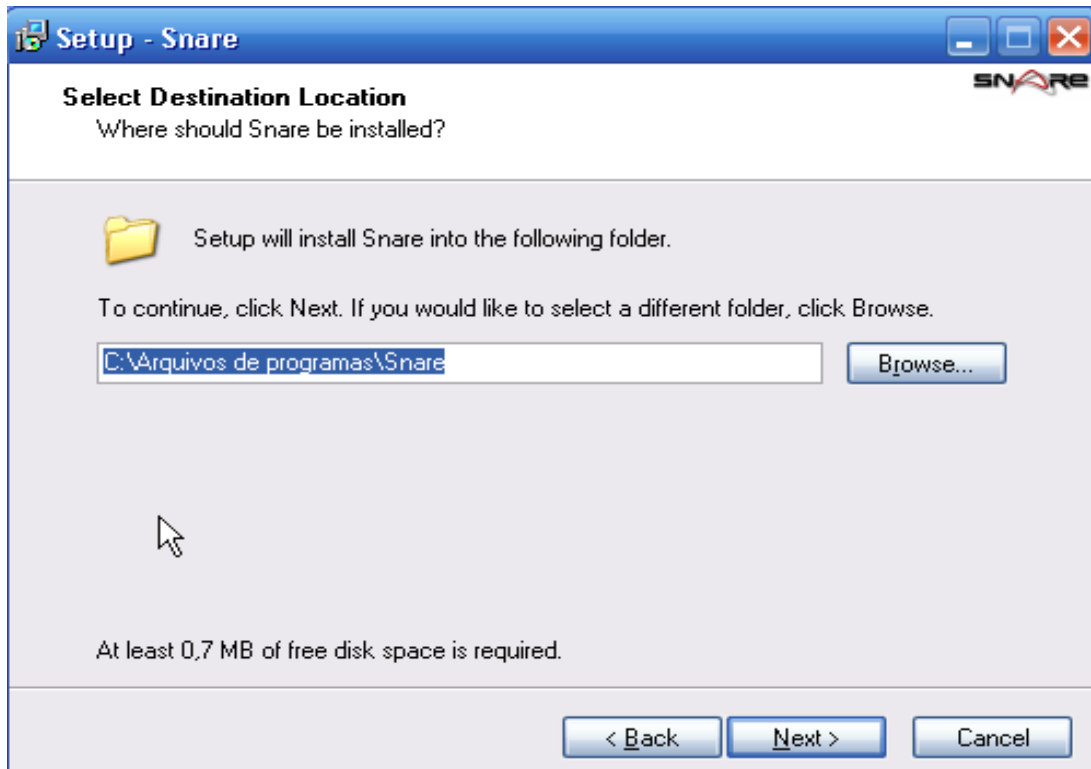
Observação: Os valores em vermelho podem alterar, dependendo do sistema alvo e da geração do pacote, além disso podem existir algumas dependências que deverão ser satisfeitas para o completo funcionamento dos plugins.

1. Procedimentos para compilação

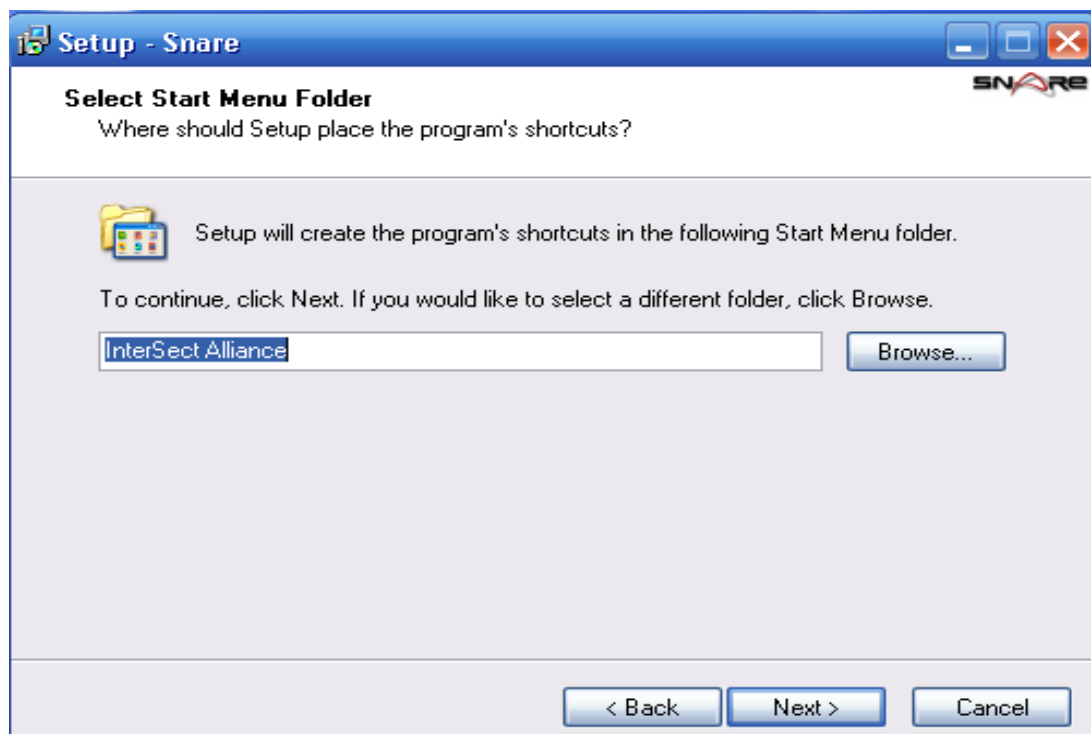
- a) Logar como “Administrador” no servidor alvo.
- b) Execute o arquivo SnareSetup-3.1.3-MultiArch.exe, e clique em “Next” conforme mostra a figura abaixo.



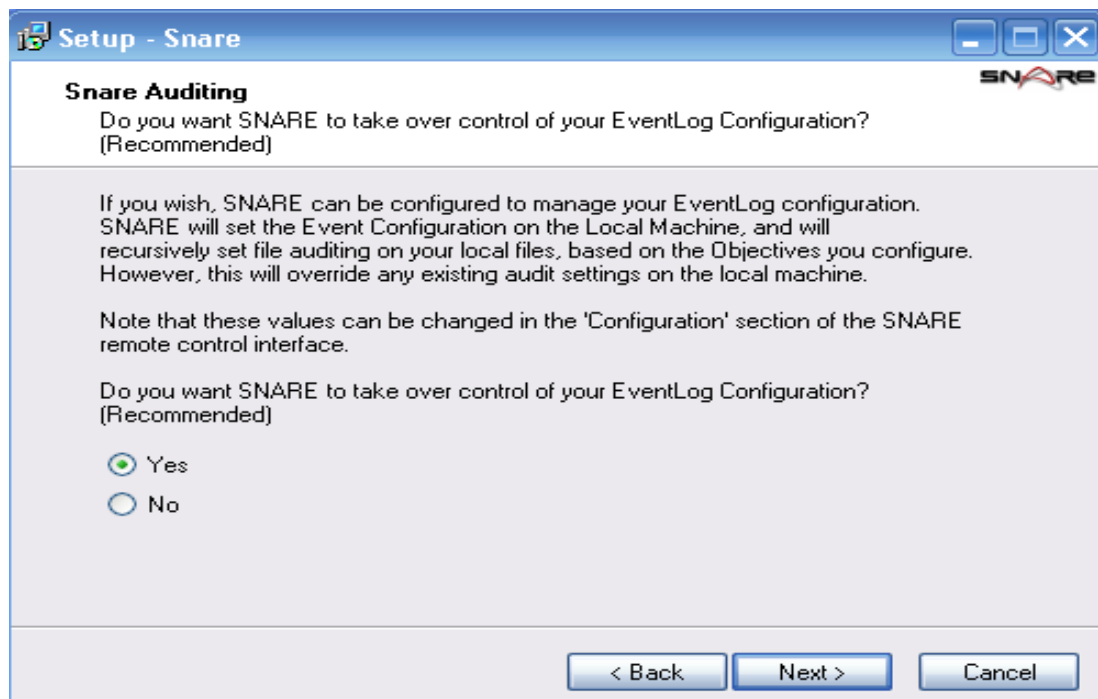
c) Selecione o diretório da instalação, conforme mostra na figura abaixo.



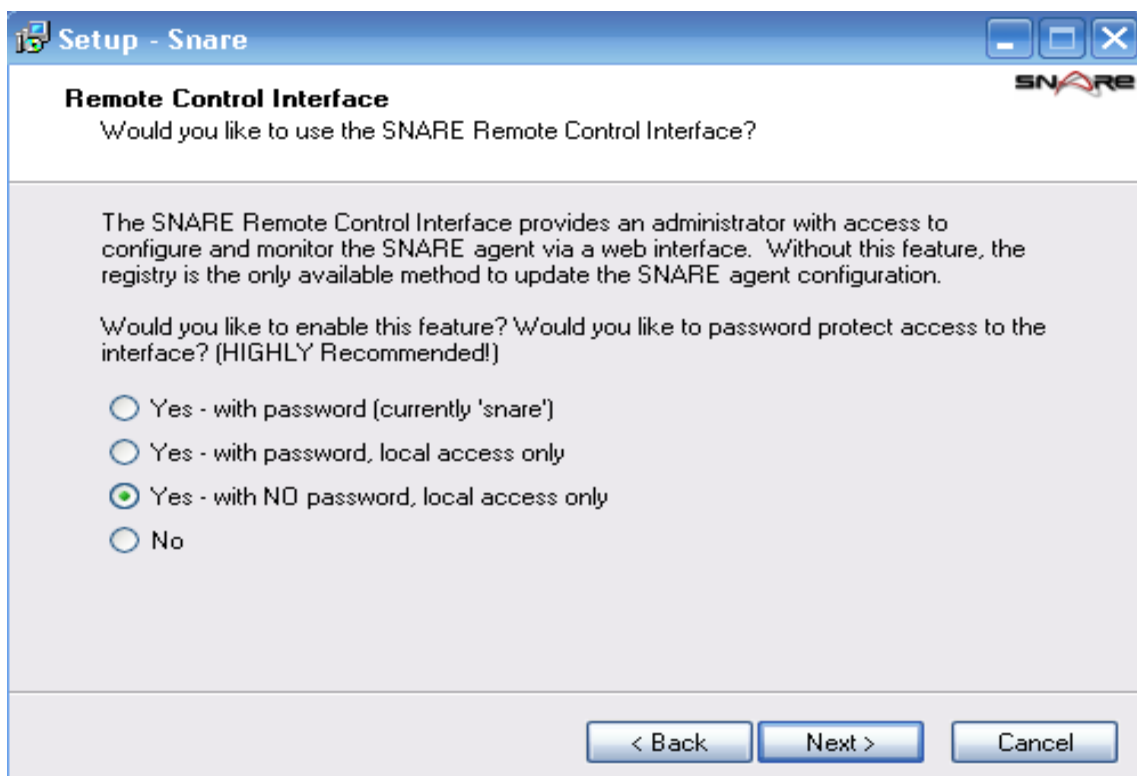
d) Selecione o diretório da instalação, conforme mostra na figura abaixo.



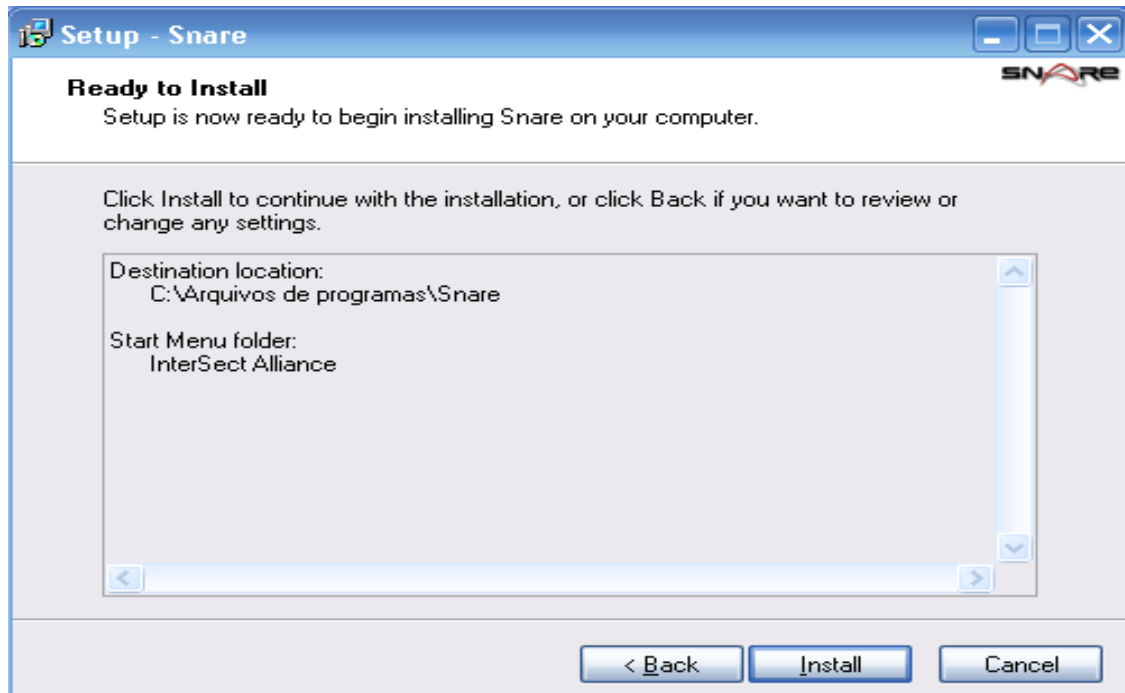
e) Selecione a opção 'Yes' e clique em 'Next' na tela abaixo.



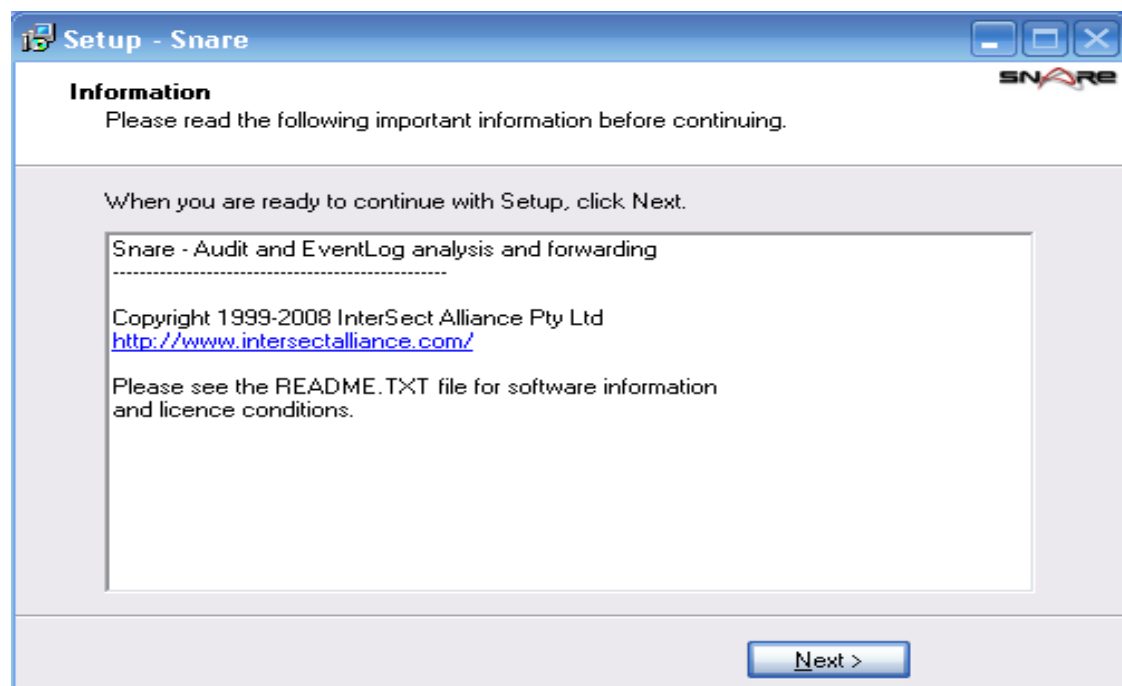
f) Selecione a opção da imagem abaixo e clique em 'Next'.



g) No passo abaixo basta clicar em 'Install'.



h) Abaixo clique em 'Next'.



i) Clique em 'Finish' para finalizar a instalação.



j) Através de seu navegador padrão acesse a página '<http://localhost:6161>' para configurar as opções de envio de logs. As configurações devem ser realizadas conforme as imagens abaixo:

Menu 'Network Configuration'

Menu 'Objectives Configuration'

SNARE Filtering Objectives Configuration

The following filtering objectives of the SNARE unit are active:

Action Required	Criticality	Event ID Include/Exclude	Event ID Match	User Include/Exclude	User Match	General Match	Return	Event Src
<input type="button" value="Delete"/> <input type="button" value="Modify"/>	Critical	Include	Process_Events	Include	*	cmd.exe	Failure Error Warning	Application
<input type="button" value="Delete"/> <input type="button" value="Modify"/>	Critical	Include	User_Group_Management_Events	Include	*	*	Failure Error Warning	Security
<input type="button" value="Delete"/> <input type="button" value="Modify"/>	Critical	Include	Reboot_Events	Include	*		Failure	System
<input type="button" value="Delete"/> <input type="button" value="Modify"/>	Critical	Include	Security_Policy_Events	Include	*		Failure Error Warning	Security
<input type="button" value="Delete"/> <input type="button" value="Modify"/>	Critical	Include	*	Include	*		Failure Error Warning	System Application

Select this button to add a new objective.

Latest Events

Network Configuration

Remote Control
Configuration

Objectives
Configuration

View Audit Service
Status

Apply the Latest Audit
Configuration

Local Users
Domain Users
Local Group Members
Domain Group Members
Registry Dump

k) Clique na opção mostrada na imagem abaixo para aplicar as configurações realizadas.

The screenshot shows the 'SNARE for Windows' status page. At the top left is the 'INTERSECT ALLIANCE' logo. The top right features a red banner with the text 'SNARE for Windows'. The main heading is 'SNARE Version 3.1.3 Status Page'. Below this, a green message states 'Snare for Windows is currently active.' A copyright notice at the bottom reads '(c) Intersect Alliance Pty Ltd 1999-2007. This site is powered by SNARE for Windows.' On the left side, there is a red sidebar menu with the following items: 'Latest Events', 'Network Configuration', 'Remote Control Configuration', 'Objectives Configuration', 'View Audit Service Status', 'Apply the Latest Audit Configuration' (with a mouse cursor over it), 'Local Users', 'Domain Users', 'Local Group Members', 'Domain Group Members', and 'Registry Dump'.

Após a conclusão do procedimento, informar a OpServices através do email suporte@opservices.com.br para que possa ser feito os testes necessários e a configuração dos itens a serem monitorados no referido servidor.