ZABBIX

Desenvolvido por Diego Cavalcante - 10/02/2017
E-mail: diego@suportecavalcante.com.br
Telegram: @diego_cavalcante
Descrição: Monitoramento Windows RDP - Terminal Server
S.O: Windows
Linguagem: Powershell

Caso você tenha um servidor Windows RDP “Terminal Server”, o monitoramento consiste em coletar estatísticas de conexões dos usuários.

° ITENS

° Total de usuários ativos
° Total de usuários inativos
° Nome dos usuários ativos
° Nome dos usuários inativos
° Endereço IP remoto dos usuários ativos
° Hostname do dispositivo remoto dos usuários ativos
° Serviço Terminal Service
° Serviço Terminal Service Licence
° Status da porta RDP

° TRIGGERS

° Numero de Usuários Conectados
° Numero de Usuários Desconectados
° Status da Porta RDP
° Status do Serviço Remote Desktop Licencing
° Status do Serviço Remote Desktop Services

° GRÁFICOS

° Estatísticas de Conexões

1º PREPARANDO HOST:

O monitoramento em si, necessita que alguns ajustes sejam realizados no host antes da coleta de dados. Como exemplo em meu ambiente existem alguns diretórios padrão que utilizo para Scripts e UserParameters.

Scripts: c:\zabbix\monitoramento\scripts\
UserParameters: c:\zabbix\monitoramento\userparameters\

OBS: Ajuste de acordo com o seu ambiente, dentro do zabbix_agentd.conf do Host, ajuste o parâmetro: Include= e aponte para o diretório onde irá conter seus arquivos .conf com os UserParameters.

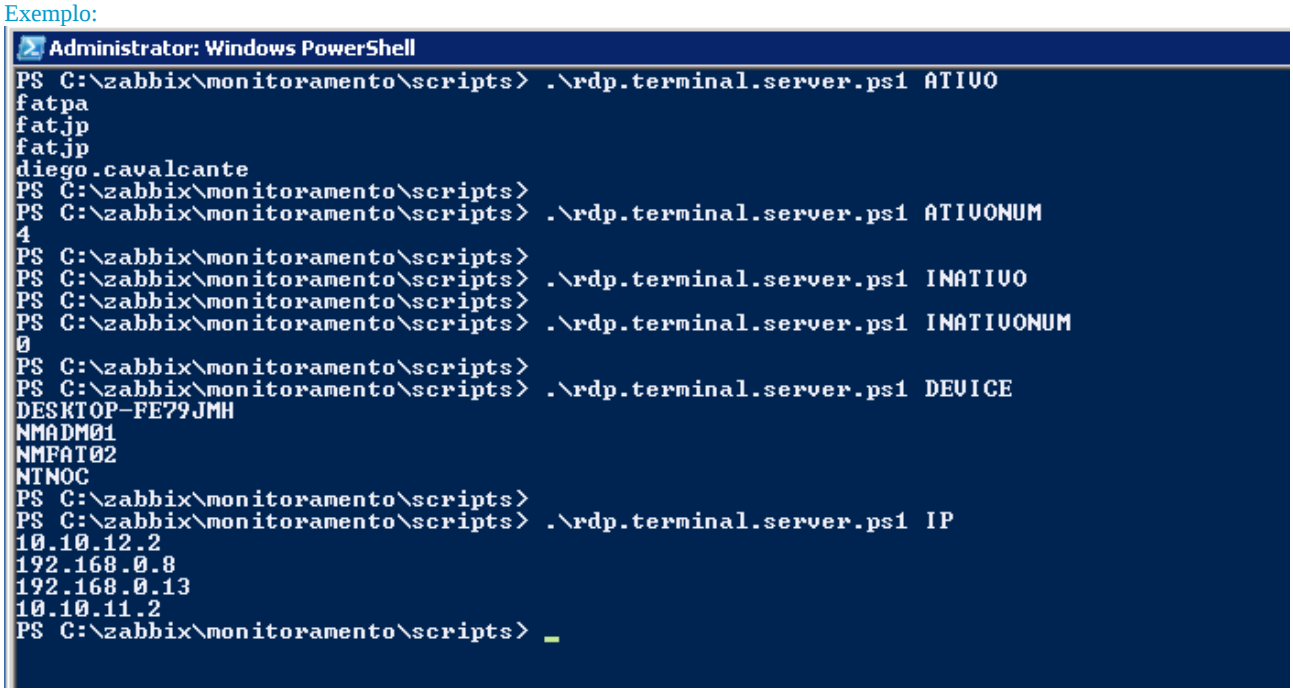
2º REQUERIMENTOS INICIAIS:

° Abra o Powershell como Administrador e execute o comando Set-ExecutionPolicy Unrestricted e confirme.
° Caso já tenha feito o procedimento acima no Host, desconsidere e pule para o próximo requerimento.
° Coloque rdp.terminal.server.ps1 no diretório de sua escolha.
° Coloque rdp.terminal.server.conf no diretório de sua escolha.
° Instale o Módulo rdp.terminal.server.msi
° Após a instalação, copie a pasta C:\Users\SeuUsuario\Documents\WindowsPowerShell\modules\PSTerminalServices\
° Cole a pasta PSTerminalServices em C:\Windows\System32\WindowsPowerShell\v1.0\Modules\
° Reinicie o Zabbix Agent no Host.

3º FEITO OS PASSOS ACIMA, VAMOS AOS TESTES:

° Abra o powershell e navegue até a pasta do script e teste com os comandos disponíveis abaixo:
° .\rdp.terminal.server.ps1 ATIVO (Retorna o nome dos usuários ativos)
° .\rdp.terminal.server.ps1 ATIVONUM (Retorna o numero total de usuários ativos)
° .\rdp.terminal.server.ps1 IP (Retorna o IP dos usuários ativos)
° .\rdp.terminal.server.ps1 DEVICE (Retorna o nome do dispositivo dos usuários ativos)
° .\rdp.terminal.server.ps1 INATIVO (Retorna o nome dos usuários inativos)
° .\rdp.terminal.server.ps1 INATIVONUM (Retorna o numero total de usuários inativos)

Exemplo:



OBS: Caso algum erro apareça ao executar os comandos, reveja todos os passos anteriores.

4º MACROS DO HOST:

O template utiliza macros apartadas, e deverá ser cadastrada no Host monitorado.

{$RDPPORTA} = Porta que o servidor RDP está escutando, padrão 3389.
{$RDPA} = Usado na trigger, ex: 5 caso queira que alarme se existirem mais de 5 usuários ativos conectados.
{$RDPI} = Usado na trigger, ex: 5 caso queira que alarme se existirem mais de 5 usuários inativos conectados.

5º TEMPLATE:

º Importe o Template - Windows Terminal Server RDP.xml em seu Zabbix Frontend.
º Cadastre as Macros acima no Host.
º Associe o Template ao Host monitorado e aguarde a coleta.
° Ajuste os intervalos de coleta, período de retenção de History e Trend dos itens de acordo com seu ambiente.

OBS: Caso os dados não sejam coletados, use e abuse do zabbix_get para validar a coleta dos dados.

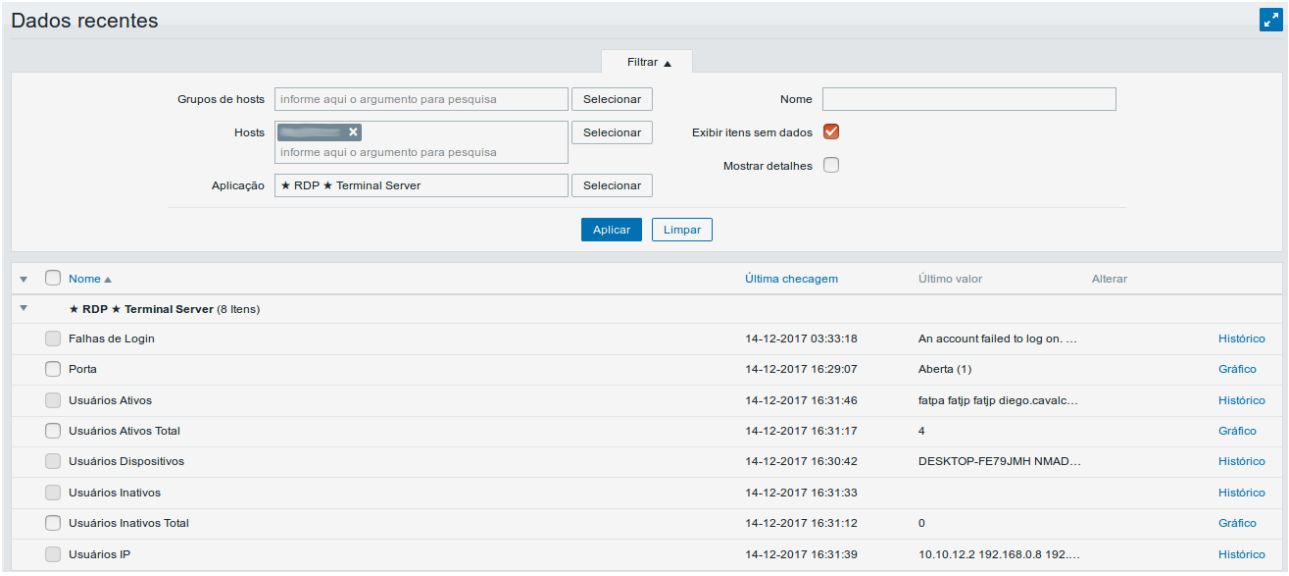
6º MAPEAMENTO DE VALORES:

NOME: ★ STATUS ★ Check Porta
0 = Inacessível
1 = Aberta

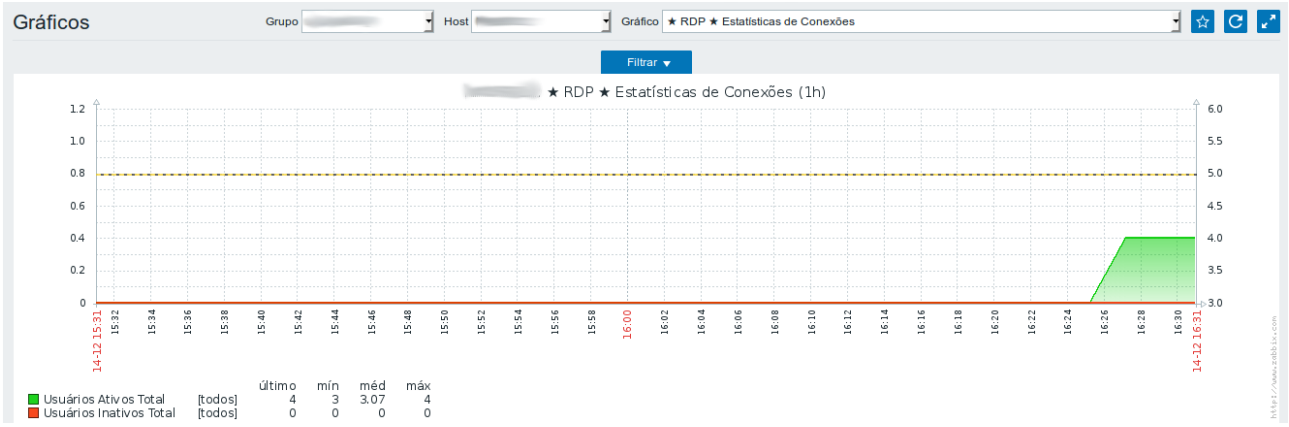
NOME: ★ STATUS ★ Serviço
0 = Iniciado
1 = Pausado
2 = Iniciar Pendente
3 = Pausa Pendente
4 = Continuar Pendente
5 = Parar Pendente
6 = Parado
7 = Desconhecido
255 = Desconhecido

6º DADOS COLETADOS E GRÁFICOS:

Dados Recentes:



Gráficos:



FIM.