1. OBJETIVO

Este documento tem como objetivo auxiliar no procedimento de configuração de ambientes específicos para Windows Server (AD e DC), para permitir coleta de logs para o ISH Vision via HTTP.

1. AVISO LEGAL

Esta Instrução de Trabalho trata-se de um guia passo-a-passo para configurações dos serviços de Gerenciamento Remoto e Controladores de Domínio do Microsoft Windows e portanto seu objetivo principal é servir de orientação em procedimentos e poderá ser adaptado e/ou alterado de acordo com cada cenário específico da empresa.

Muitos dos nomes de empresas e serviços referidos neste documento são marcas registradas de propriedade de seus respectivos proprietários. Todas elas são reconhecidas mediante esta declaração.

1. RECOMENDAÇÕES GERAIS

Cada empresa possui um ambiente próprio com suas políticas e procedimentos pré-estabelecidos. Assim, a ISH Tecnologia recomenda fortemente a revisão dos procedimentos aqui exemplicados em formato de guia, com o objetivo de resguardar cada servidor e/ou ambiente testado e adequar sempre que necessário, algum dos passos estabelecidos.

Como referência completa, recomenda-se a leitura do guia oficial da RSA (anexo 02) em paralelo a esta instrução de trabalho.

Cabe ressaltar que cada corporação estabelece suas próprias políticas de segurança, incluindo mas não limitando-se, os processos de resgate de configurações em caso de falhas, tais como *Backup* dos Serviços de *Active Diretory*, haja vista que um plano de *recovery* é muito particular de cada administrador. Portanto, sempre realize esta cópia de segurança antes da realização de qualquer procedimento de configuração e/ou alteração dos seus serviços.

1. ANEXOS

Os seguintes arquivos devem ser disponibilizados em anexo a este guia/procedimento:

|  |  |  |
| --- | --- | --- |
| Item | Tipo | Título |
| 01 | Script Powershell | winrmconfig.ps1 |
| 02 | Arquivo PDF | WinRM Configuration Guide |

1. SUMÁRIO EXECUTIVO

Este documento fornece informações para configurar os serviços *Windows WinRM* (Gerenciamento Remoto do Windows) e *Active Directory Domain Controller* (Controlador de Domínio) para permitir que o *RSA NetWitness* colete *logs* de eventos de segurança de máquinas Microsoft Windows. Neste documento, a palavra *"Collector"* refere-se ao *RSA NetWitness Log Collector* ou ao *Virtual Log Collector*. A palavra *"Channel"* refere-se a um *log* de eventos do Windows, por exemplo, *Security*, *System*, *Forwarded Event*, ou *DNS*.

Este guia também documenta os requisitos e permissões para coletar eventos e *SIDs* (*Security Identifiers* exibidos nos eventos que podem ser traduzidos para nomes de usuários e grupos pelo *RSA NetWitness*) de um sistema usando uma conta não administrativa.

A *RSA* recomenda o uso de uma conta de *non-administrative* para o *collection user*. Você pode executar as etapas para criar essas permissões manualmente em cada sistema de destino ou usar uma GPO ou utilizar um *script* do *PowerShell* fornecido pela *RSA* para realizar essas tarefas manualmente em cada *Domain Controller* ou como um *script* de *logon* por meio de uma GPO para aplicar a mesma configuração em um grande número de sistemas.

* 1. Uso do *script winrmconfig*

Nota: A RSA recomenda que você teste o script primeiro, executando-o manualmente em uma máquina de teste ou cenário de homologação em para observar as saídas de sua execução, antes de executá-lo em seu ambiente de produção.

O arquivo ***winrmconfig*** trata-se de um *script* desenvolvido para ser executado via *PowerShell*. Pode ser utilizado para os seguintes procedimentos:

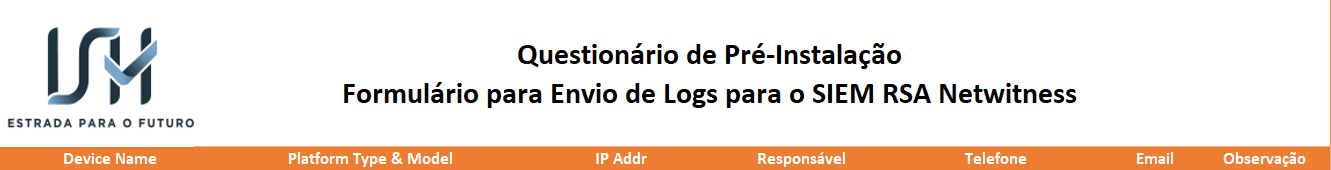
* *Troubleshoot* com o modo de relatório.
* Automatizar as etapas para criar um *WinRM Listener* (HTTP/HTTPS) que aceite solicitações de um *collector*, como ferramenta de configuração;
* Habilitar o acesso ao *log* de segurança, criar permissões de usuário para acessar remotamente o *WMI* e acessar o *plug-in WinRM WMI*;
* Utilizar o *script* via GPO para vários sistemas.

Para download do arquivo ***script winrmconfig***, acesse o link na página oficial da *RSA*: <https://community.rsa.com/docs/DOC-58018>. Alternativamente, o mesmo arquivo estará sendo entregue como um anexo a este manual.

Neste guia, a utilização deste *script* destina-se única e exclusivamente para habilitar um ***WinRM Listener* com protocolo HTTP** necessário para conclusão dos procedimentos de configuração de coleta de *logs* através do WinRM do *Active Directory* para o *RSA NetWitness*.

1. PROCEDIMENTOS
   1. Servidores de AD que terão *logs* coletados

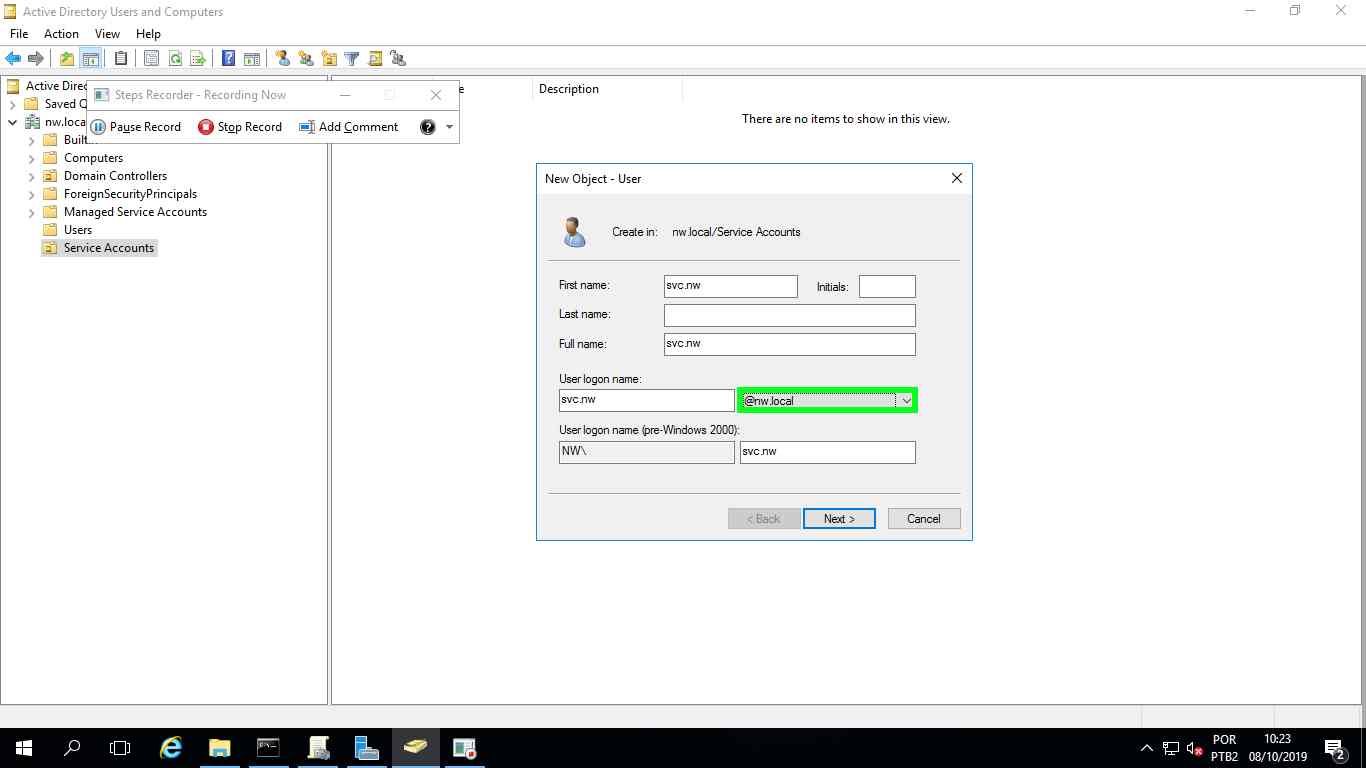
* **Passo 1** – Informar para a ISH Tecnologia, por meio do preenchimento do arquivo em planilha eletrônica (*PIQ\_NOMECLIENTE.xlsx*) todos os endereços IP dos ADs que terão seus *logs* de segurança coletados.
  + Acesse a planilha “*Logs*” dentro deste arquivo eletrônico e preencha corretamente as colunas: ***Device Name*** (*Hostname*), ***Platform Type & Model*** (Serviço/Produto), ***IP Address***, **Responsável** (Responsável Técnico pelo ativo), **Telefone** (Forma de contato), **Observações** (quando aplicável).



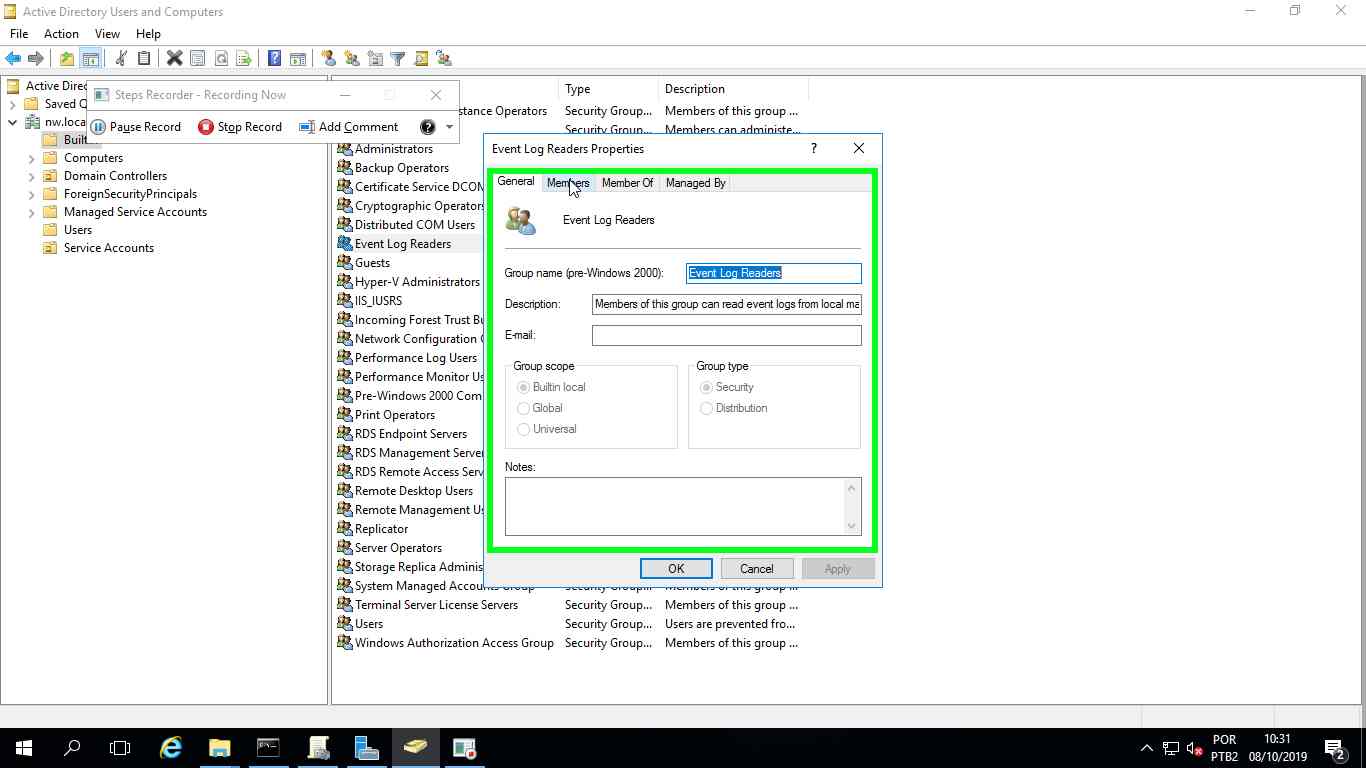
* 1. Liberação de porta e endereço IP para *Log Decoder*

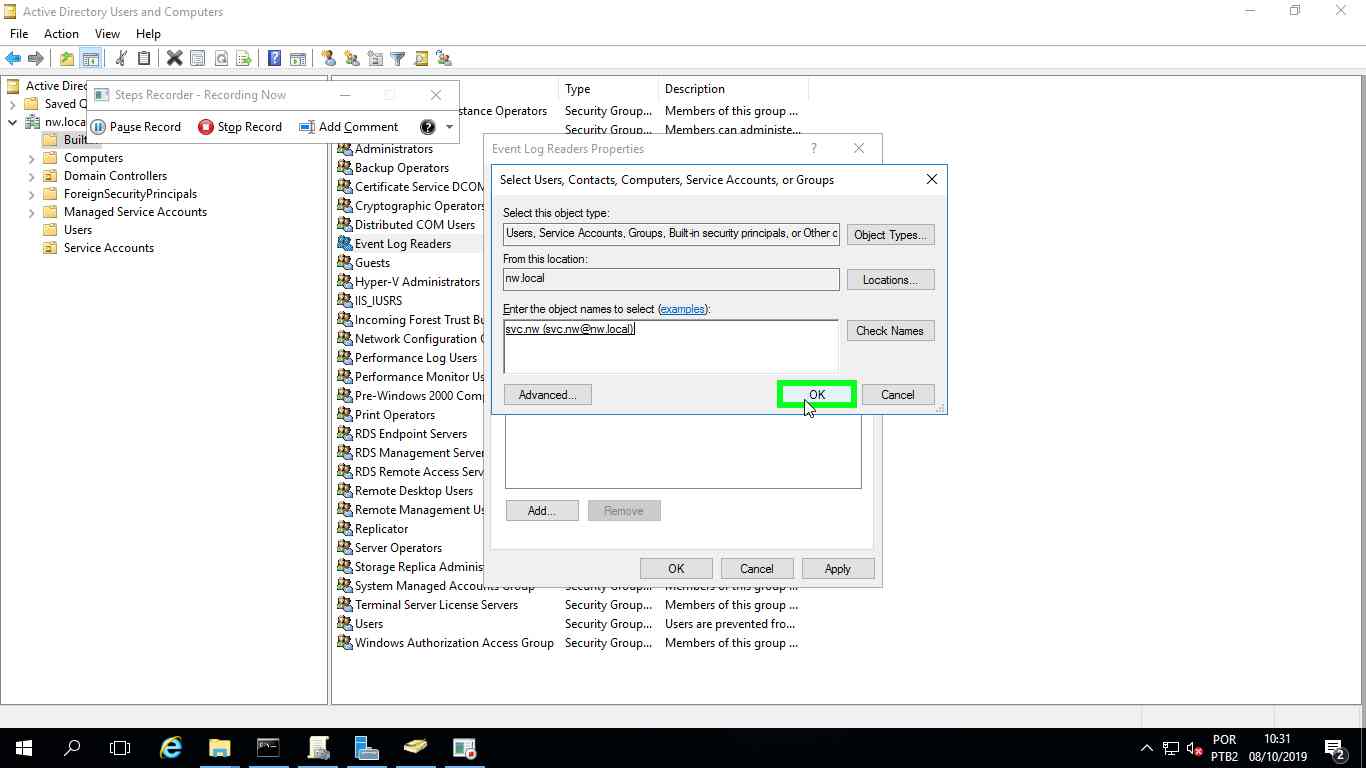
O *RSA NetWitness* utiliza uma porta específica para coleta de *logs* via protocolo HTTP. Desta forma, será necessário garantir que o servidor tenha a porta **5985** aberta para entrada de origem do endereço **IP do *Log Decoder***.

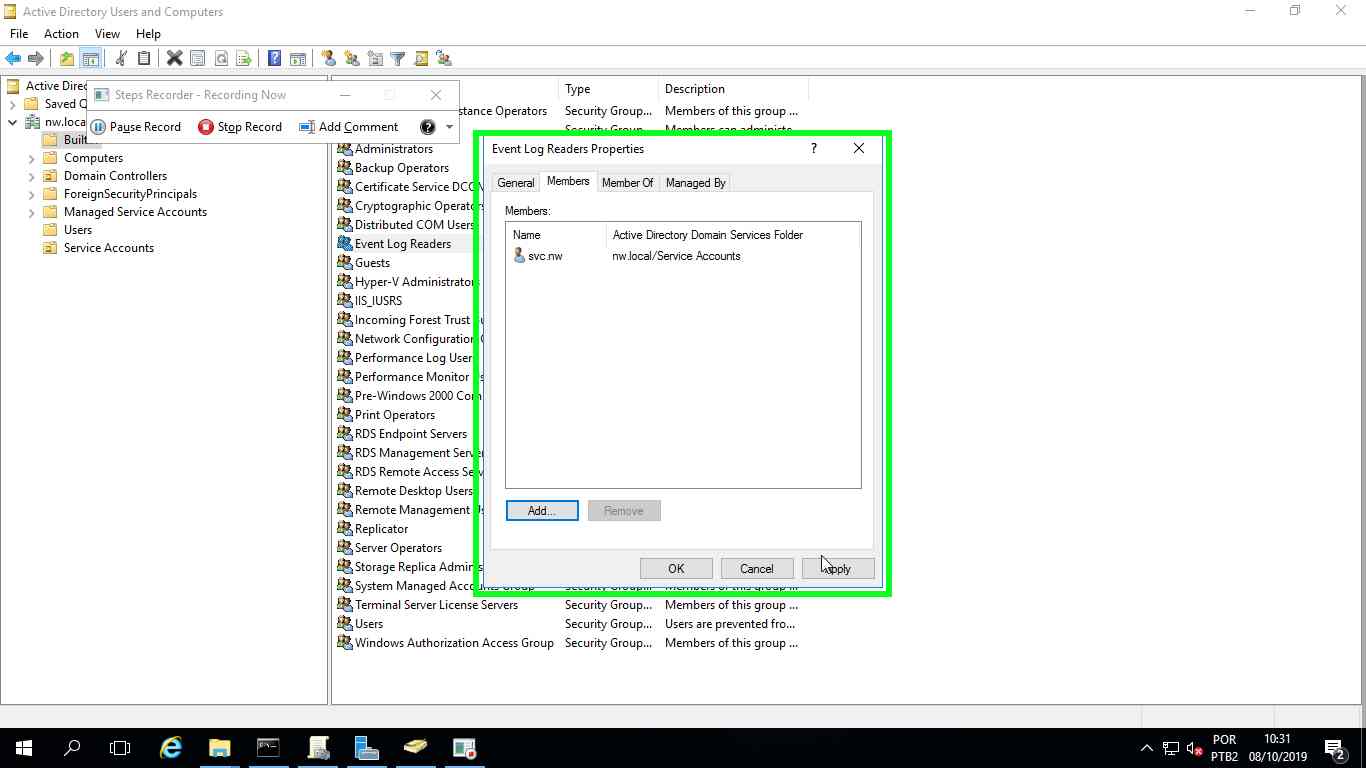
* **Passo 1** - Liberar acesso externo de origem via **IP** **do *Log Decoder*** para a **porta TCP** **5985** (HTTP).
  + Este passo pode variar de acordo com as tecnologias utilizadas no ambiente. Por exemplo, caso tenha algum antivírus agindo como um *firewall*, essa liberação deverá ser executada no mesmo. Paralelamente deverá ser permitido a comunicação para essa Porta e IP de origem oriundo do *RSA NetWitness* no *Firewall* de Borda caso o tenha.
  1. Criação de Usuário para Coleta de *Logs*
* **Passo 1** - Na **Unidade Organizacional** desejada, **crie uma conta de usuário** que funcionará como uma conta de serviço *(Service Accounts)*.



* **Passo 2** - Conforme solicitado no guia oficial da *RSA* (anexo 02, página 07), é necessário **adicionar** esse **usuário** criado ao **Builtin>>Grupo *Event Log Readers***.



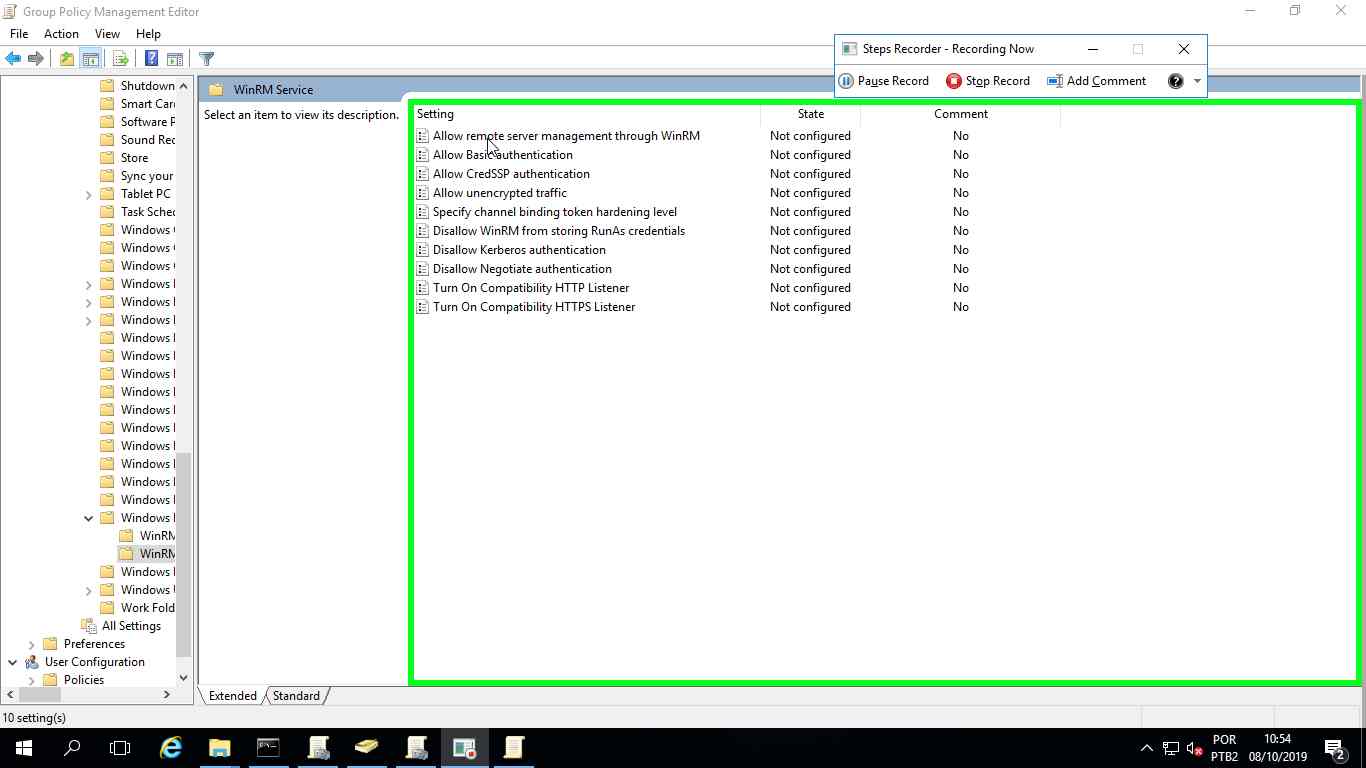


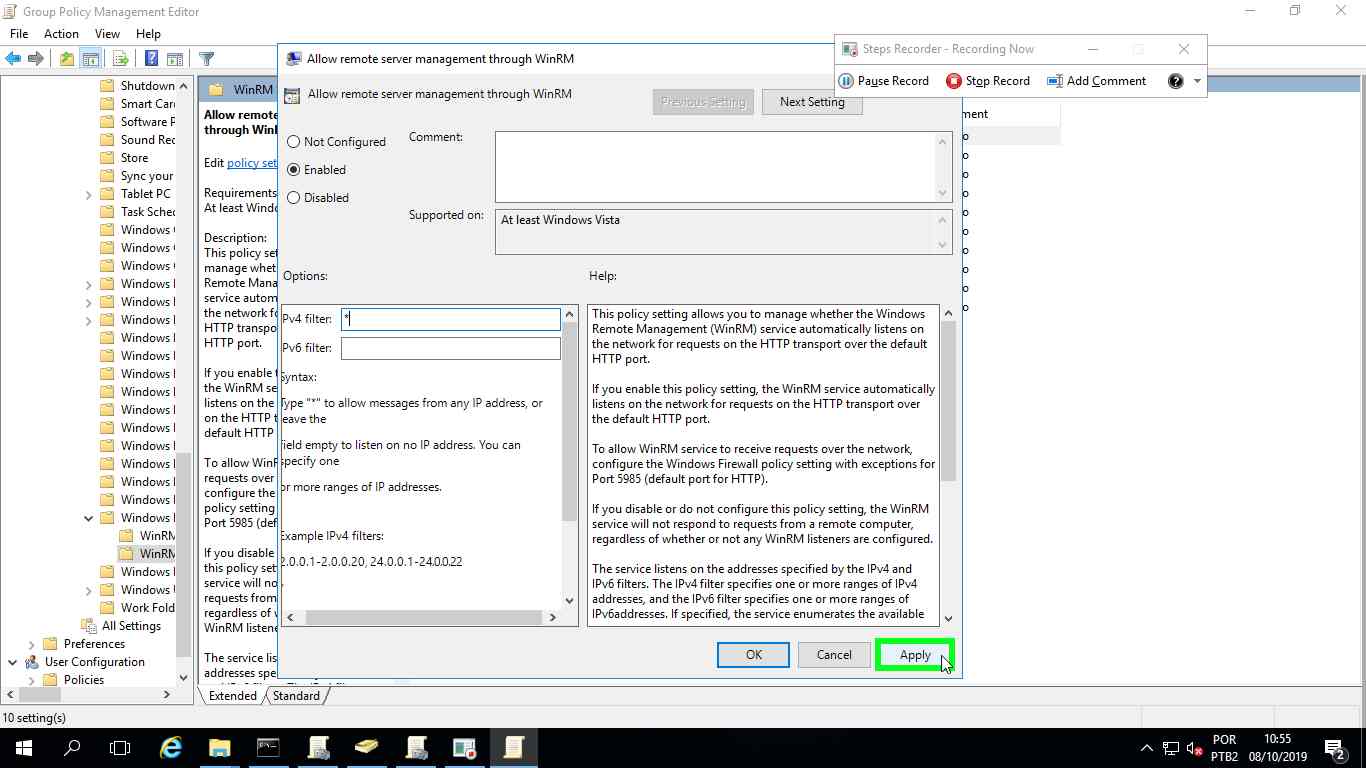


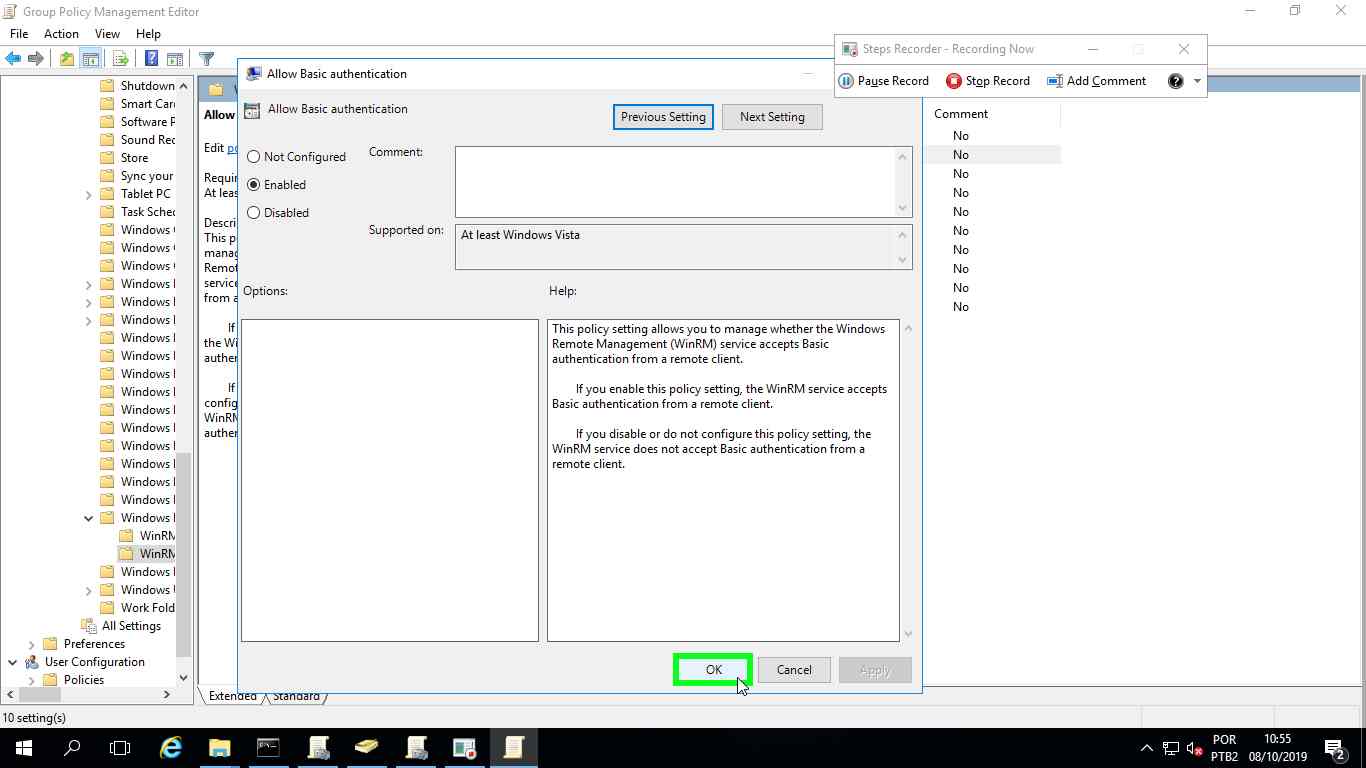
* 1. Criação de GPO para WinRM nos *Domain Controllers*

Nesta etapa, recomenda-se criar uma política específica para as configurações do WinRM em todos os *Domain Controllers* (Controladores de Domínio).

* **Passo 1** - Na política *Default Domain Controller Policy* **acessar o** **WinRM Service**:
  + *Computer Configuration >> Polices >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service*
* **Passo 2** - Habilitar as seguintes configurações:
  + ***Allow remote server management through WinRM - Enabled***
  + ***Allow Basic Authentication - Enabled***



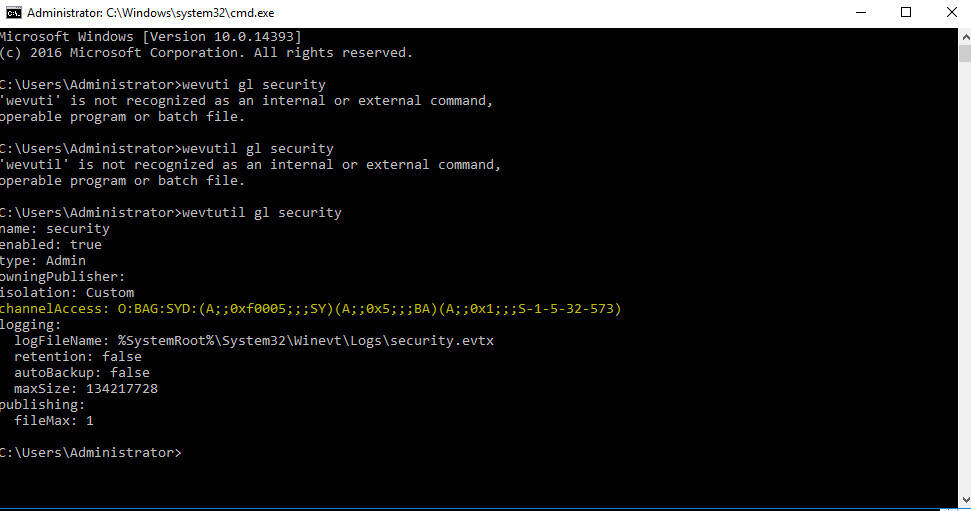




* 1. Configuração do *Listener* HTTP

Após configurar a GPO, você deve configurar o *WinRM* para escutar via HTTP.

* **Passo 1** – Utilize o comando abaixo para verifique o estado atual do *listener*
  + winrm e winrm/config/listener
* **Passo alternativo** – Se verificar que o HTTP não está habilitado, execute o comando abaixo
  + winrm quickconfig -transport:http
  + repita o passo 1 e confirme se o HTTP está habilitado
* **Passo 2** - Para validar o certificado que está sendo utilizado no *listener* WinRM, utilize o comando abaixo:
  + winrm enumerate winrm/config/listener
  + observe que ele retorna algo semelhante ao passo 1
* **Passo 3** - Após verificar que o *WinRM* está escutando HTTP, obtenha o ***securechannel*** (mesmo que ***chanellAcess***) do *event log* utilizando o comando abaixo:
  + wevtutil gl security

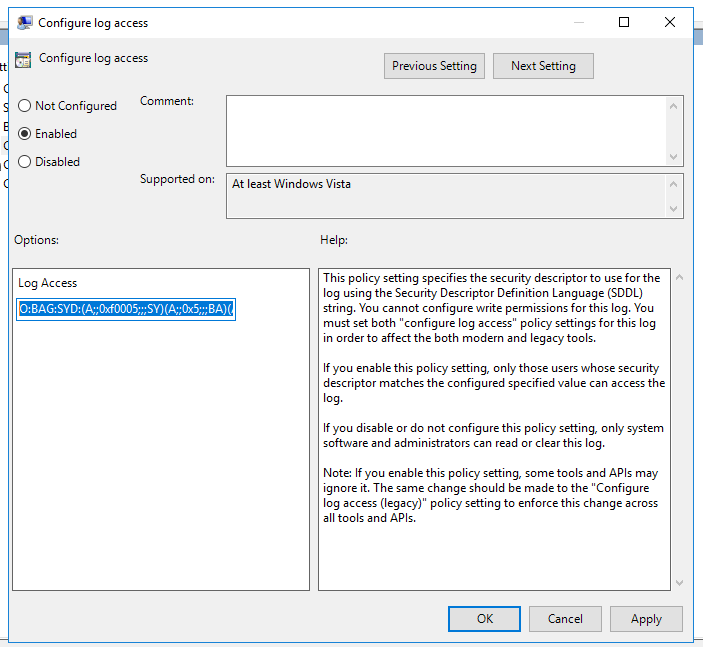


* **Passo 4** - Copiar o número do ***ChannelAccess***
  + Este código corresponde ao tipo de *log* que será encaminhado, no caso, os *logs* de segurança.
  + O código é padrão e é necessário executar o comando apenas em um *Domain Controller* para obtê-lo.
  1. Permissões de acesso aos *logs*

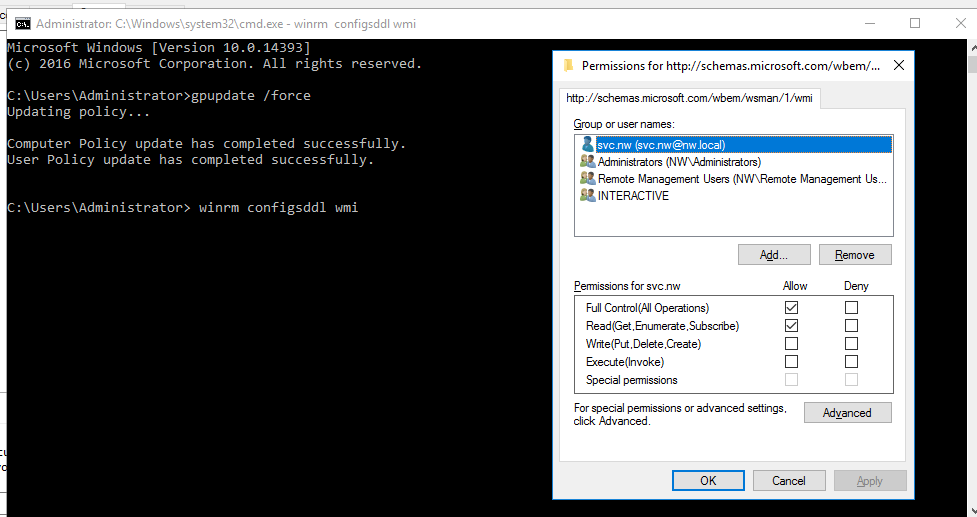
Nota: Este procedimento deve ser realizado em todos os *Domain Controllers* que forem configurados

* **Passo 1** - Na política *Default Domain Controller Policy* habilite as seguintes configurações:
  + *Computer Configuration >> Polices >> Administrative Templates >> Windows Components >>Event Log Service >> Security*
  + ***Configure Log Access – Enabled***
  + No campo ***LogAccess*** inserir o **valor do *channelAccess***copiado anteriormente*.*

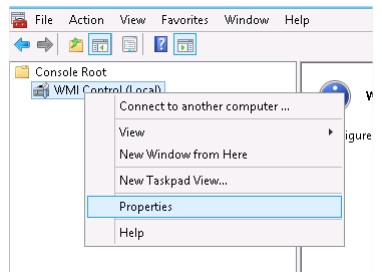


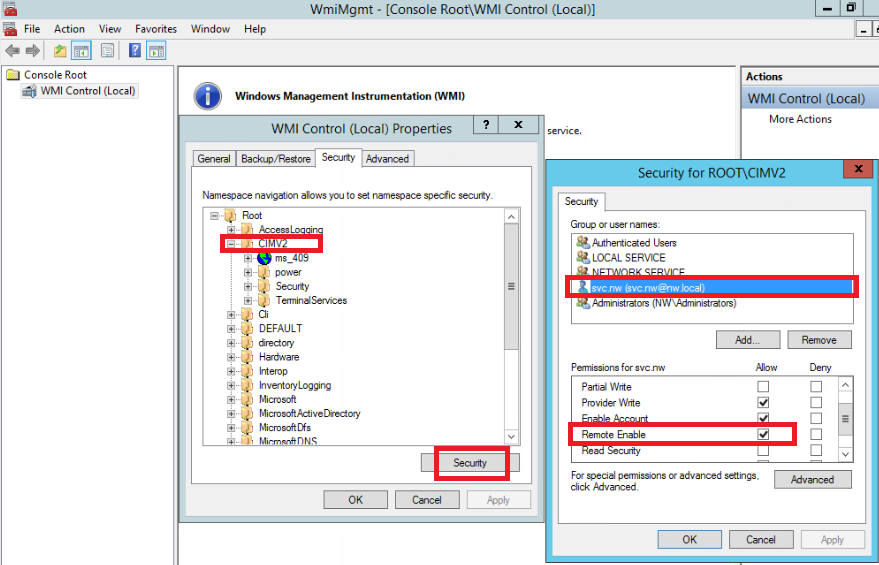


* + É importante nesta etapa, sempre adicionar ao final do channelAccess o seguinte valor: **(A;;0x1;;;S-1-5-20)**
  + Deverá ficar algo semelhante ao código abaixo:
    - *channelAcess*: **O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)**
    - *Log security*: **(A;;0x1;;;S-1-5-20)**
    - Valor final: **O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20)**
* **Passo 2** – Forçar a atualização das políticas:
  + gpupdate /force
* Para confirmar se as políticas foram aplicadas, execute o comando abaixo, como administrador e confirme cada política que foi alterada.
  + rsop.msc
* **Passo 3** - Após validar que a configuração do *log* foi aplicada, execute o comando abaixo:
  + winrm configsddl wmi
  + na janela que é aberta dê **permissão *Full Control*** e ***Read*** para a conta de serviço que foi criada na seção 6.3 deste guia.



* 1. Permissões para o WMI
* **Passo 1** – Execute do comando abaixo (via “Executar”, CMD ou Powershell) para alterar as permissões do WMI:
  + WMIMgmt.msc

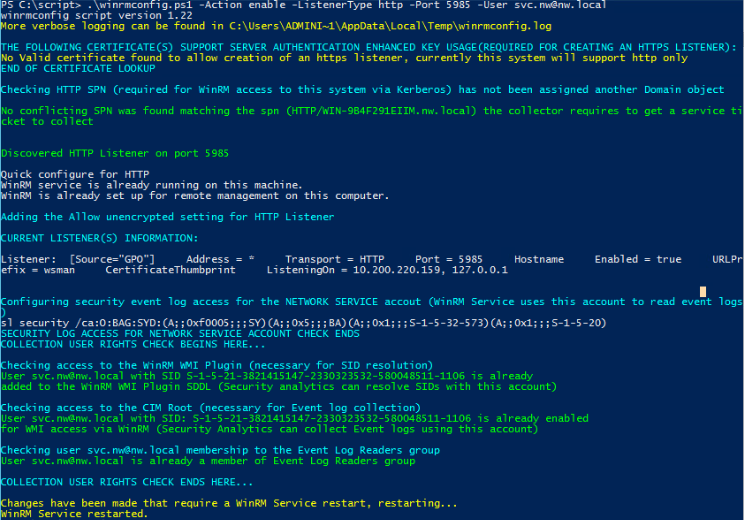




* + Em propriedades do ***WMI Control***, clique na aba “***Security***”, selecione ***CIMV2*** e clique no botão “***Security***”.
  + Na janela que se abre, selecione o object name “***Authenticated Users***” (recomenda-se fortemente que esta configuração seja apenas para a conta de serviço criada na seção 6.3 deste guia) e habilite o “***Remote Enable***” (selecione ***Allow***).
  1. *Linkar* *Listener* e ao Usuário

Nota: Este procedimento deve ser realizado em todos os *Domain Controllers* que forem configurados

* **Passo 1** – Abra o *Powershell* com usuário Administrador, acesse o diretório onde você salvou o ***script winrmconfig.ps1*** e execute o comando abaixo:
  + .\winrmconfig.ps1 -Action enable -ListenerType http -Port 5985 -User user@domain
  + Informe o usuário criado na seção 6.3 deste guia.



* + É interessante realizar um double-check dos listeners atuais para HTTP e verificar se o ThumbPrint é o mesmo informado no comando anterior.
  + Para isso, basta executar o comando abaixo e verificar a saída:
  + winrm e winrm/config/listener

1. REFERÊNCIAS

**RSA** Link. **Configure Windows Collection**. 2019. Disponível em: <https://community.rsa.com/docs/DOC-58163> Acesso ago 2019.

**RSA** Link. **Script WinRMConfig**. 2019. Disponível em: <https://community.rsa.com/docs/DOC-58018> Acesso ago 2021.

**RSA** Link. **Microsoft WinRM Configuration and Troubleshooting**. 2019. Disponível em: <https://community.rsa.com/docs/DOC-58164> Acesso ago 2021.