


IT-PRO-012 Rev.00	CONFIGURAÇÃO DO WINRM PARA PERMITIR A COLETA DE LOGS VIA HTTP PARA O ISH VISION	
Classificação Restrito		

1 OBJETIVO

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

2 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.

3 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 exemplificados 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 Directory*, 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.

IT-PRO-012 Rev.00	CONFIGURAÇÃO DO WINRM PARA PERMITIR A COLETA DE LOGS VIA HTTP PARA O ISH VISION	
Classificação Restrito		

4 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

5 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.

IT-PRO-012 Rev.00	CONFIGURAÇÃO DO WINRM PARA PERMITIR A COLETA DE LOGS VIA HTTP PARA O ISH VISION	
Classificação Restrito		

5.1 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.

6 TAREFAS

6.1 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).

IT-PRO-012 Rev.00	CONFIGURAÇÃO DO WINRM PARA PERMITIR A COLETA DE LOGS VIA HTTP PARA O ISH VISION	
Classificação Restrito		



Questionário de Pré-Instalação Formulário para Envio de Logs para o SIEM RSA Netwitness

Device Name	Platform Type & Model	IP Addr	Responsável	Telefone	Email	Observação
-------------	-----------------------	---------	-------------	----------	-------	------------

6.2 Liberação de porta e endereço IP para *Log Decoder*

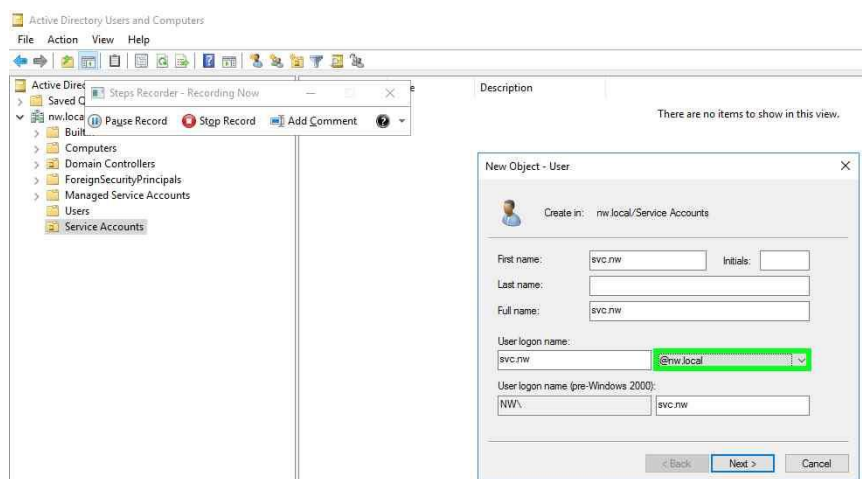
O *RSA NetWitness* utiliza uma porta específica para coleta de *logs* via protocolo HTTP. Desta forma, será necessário garantir que o servidor tenha a porta **5985** aberta para entrada de origem do endereço **IP do Log Decoder**.

Passo 1 - Liberar acesso externo de origem via **IP do Log Decoder** para a porta **TCP 5985** (HTTP).

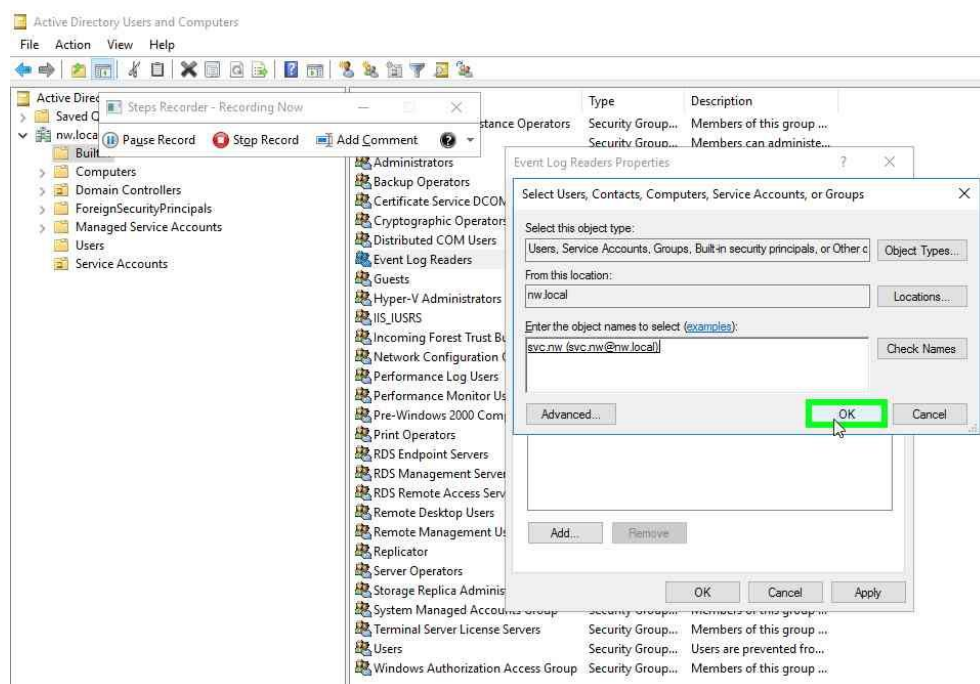
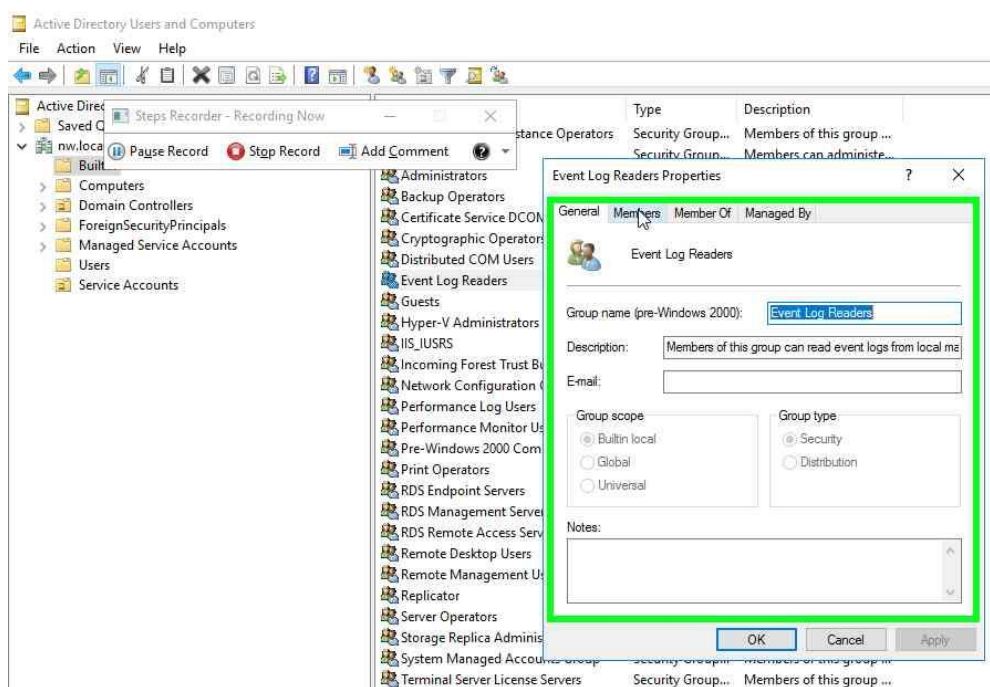
Este passo pode variar de acordo com as tecnologias utilizadas no ambiente. Por exemplo, caso tenha algum antivírus agindo como um *firewall*, essa liberação deverá ser executada no mesmo. Paralelamente deverá ser permitido a comunicação para essa Porta e IP de origem oriundo do *RSA NetWitness* no *Firewall* de Borda caso o tenha.


6.3 Criação de Usuário para Coleta de Logs

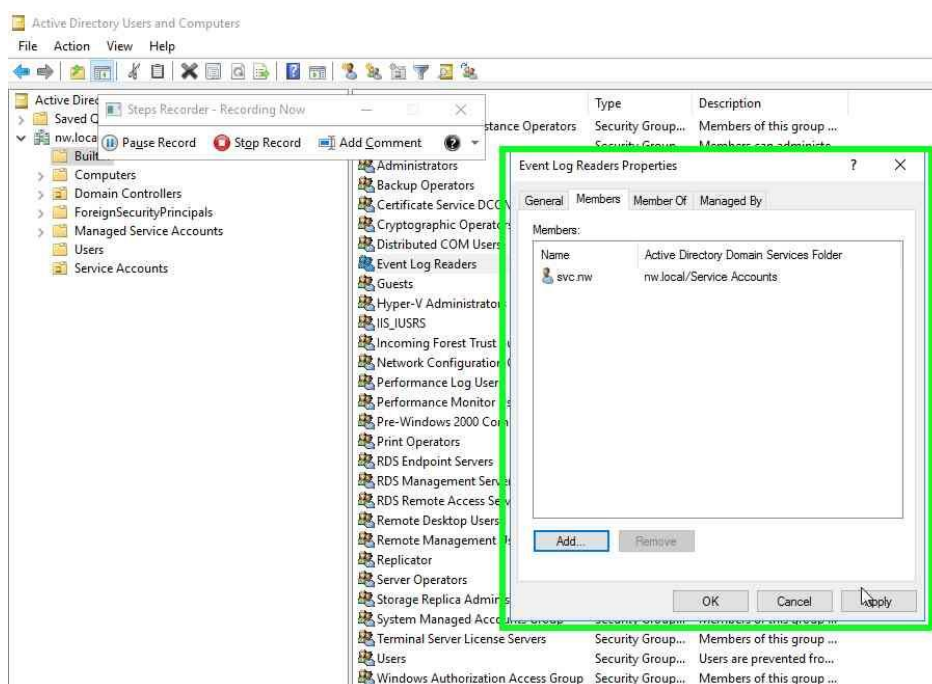
Passo 1 - Na **Unidade Organizacional** desejada, **crie uma conta de usuário** que funcionará como uma conta de serviço (*Service Accounts*).



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**.



IT-PRO-012 Rev.00	CONFIGURAÇÃO DO WINRM PARA PERMITIR A COLETA DE LOGS VIA HTTP PARA O ISH VISION	
Classificação Restrito		



6.4. 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).

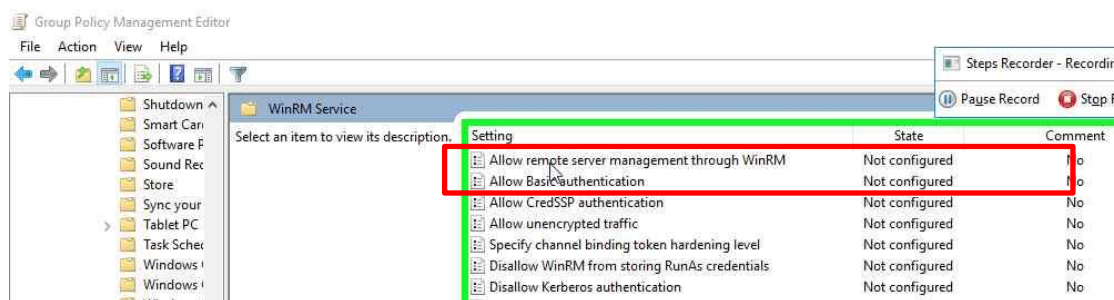
Passo 1 - Na política **Default Domain Controller Policy** acessar o **WinRM Service**:


Computer Configuration >> Policies >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service

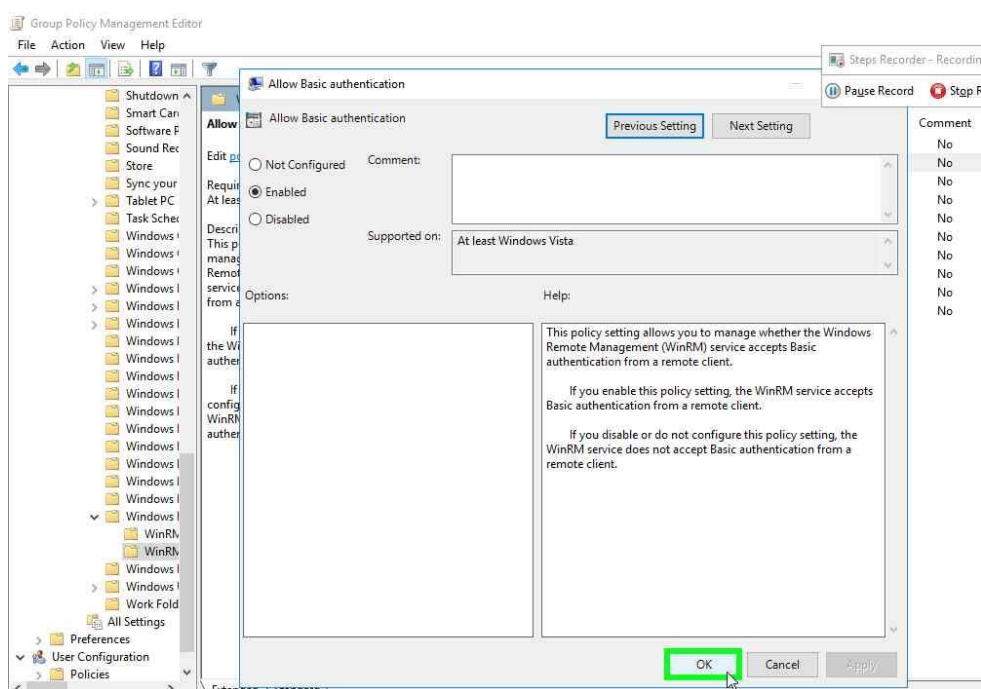
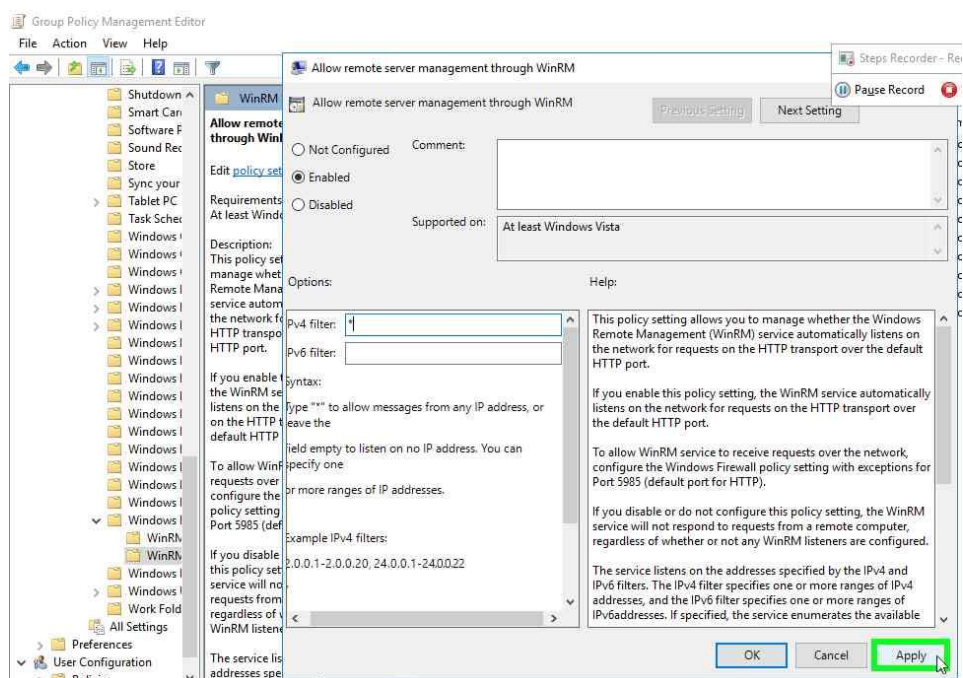
Passo 2 - Habilitar as seguintes configurações:

Allow remote server management through WinRM – **Enabled**;

Allow Basic Authentication – **Enabled**.




IT-PRO-012 Rev.00	CONFIGURAÇÃO DO WINRM PARA PERMITIR A COLETA DE LOGS VIA HTTP PARA O ISH VISION	
Classificação Restrito		



6.5. Configuração do *Listener* HTTP

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

IT-PRO-012 Rev.00	CONFIGURAÇÃO DO WINRM PARA PERMITIR A COLETA DE LOGS VIA HTTP PARA O ISH VISION	
Classificação Restrito		

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 **chanellAccess**) do *event log* utilizando o comando abaixo:

wevtutil gl security


```
C:\Users\Administrator>wevtutil gl security
'wevtutil' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>wevtutil gl security
name: security
enabled: true
type: Admin
owningPublisher:
isolation: Custom
channelAccess: 0:BAG:SYD:(A;;;0xf0005;;;SY)(A;;;0x5;;;BA)(A;;;0x1;;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\security.evtx
  retention: false
  autoBackup: false
  maxSize: 134217728
publishing:
  fileMax: 1
```

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.

IT-PRO-012 Rev.00	CONFIGURAÇÃO DO WINRM PARA PERMITIR A COLETA DE LOGS VIA HTTP PARA O ISH VISION	
Classificação Restrito		

6.6. Permissões de acesso aos logs

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

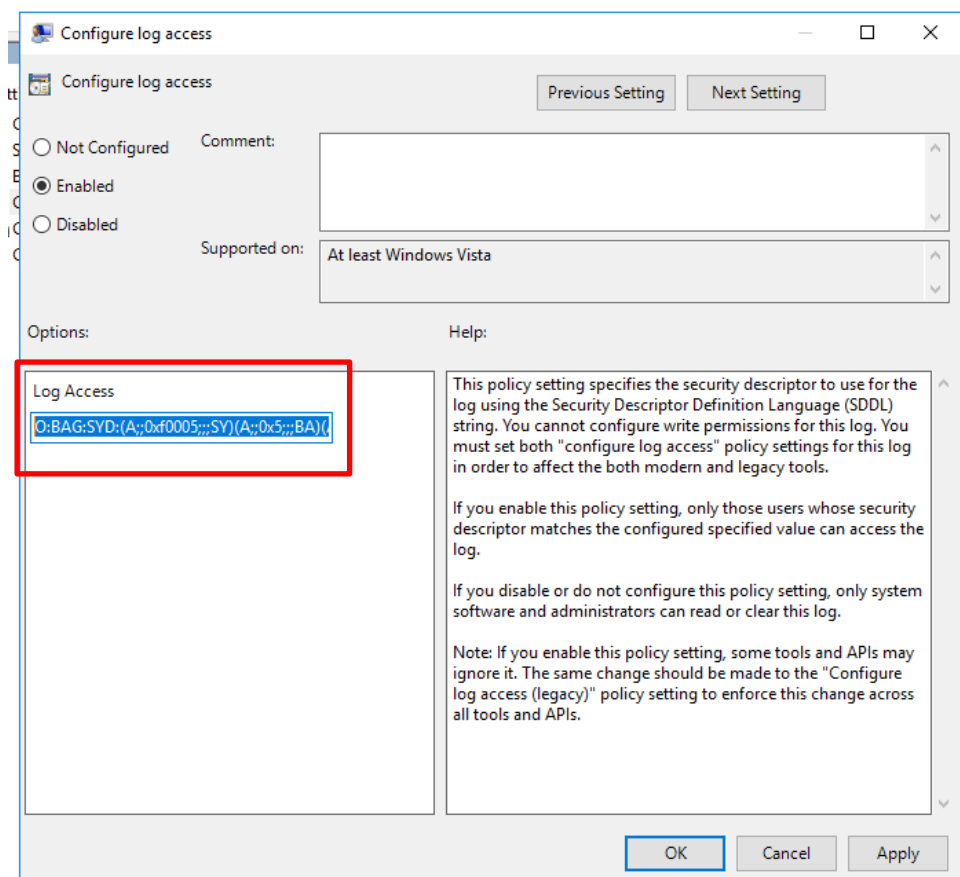
Passo 1 - Na política *Default Domain Controller Policy* habilite as seguintes configurações:

Computer Configuration >> Policies >> Administrative Templates >> Windows Components >> Event Log Service >> Security;

Configure Log Access – **Enabled**;

No campo **LogAccess** inserir o **valor do channelAccess** copiado anteriormente.

Setting	State	Comment
Control the location of the log file	Not configured	No
Specify the maximum log file size (KB)	Not configured	No
Back up log automatically when full	Not configured	No
Configure log access	Enabled	No
Control Event Log behavior when the log file reaches its ma...	Not configured	No



Configure log access

Previous Setting Next Setting

☐ Not Configured
☒ Enabled
☐ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Log Access

O:BAG:SYD:(A;;0x0005;;;SY)(A;;0x5;;;BA)

Help:


This policy setting specifies the security descriptor to use for the log using the Security Descriptor Definition Language (SDDL) string. You cannot configure write permissions for this log. You must set both "configure log access" policy settings for this log in order to affect the both modern and legacy tools.

If you enable this policy setting, only those users whose security descriptor matches the configured specified value can access the log.

If you disable or do not configure this policy setting, only system software and administrators can read or clear this log.

Note: If you enable this policy setting, some tools and APIs may ignore it. The same change should be made to the "Configure log access (legacy)" policy setting to enforce this change across all tools and APIs.

OK Cancel Apply

IT-PRO-012 Rev.00	CONFIGURAÇÃO DO WINRM PARA PERMITIR A COLETA DE LOGS VIA HTTP PARA O ISH VISION	
Classificação Restrito		

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:

channelAccess: 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

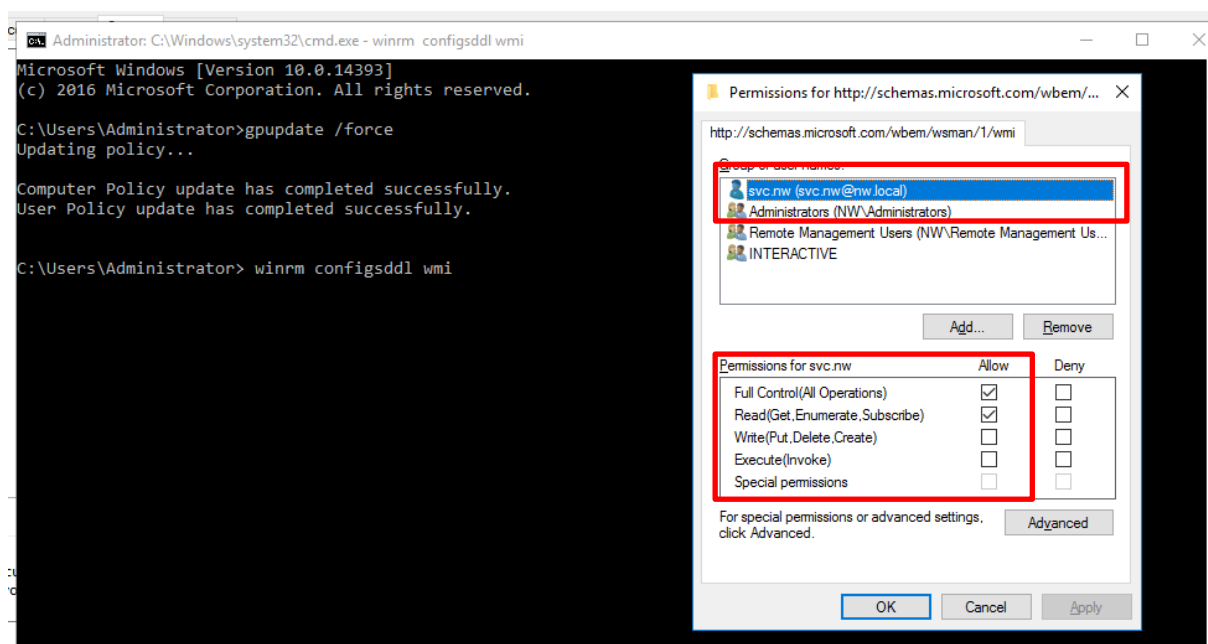
Para confirmar se as políticas foram aplicadas, execute o comando abaixo, como administrador e confirme cada política que foi alterada.


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.

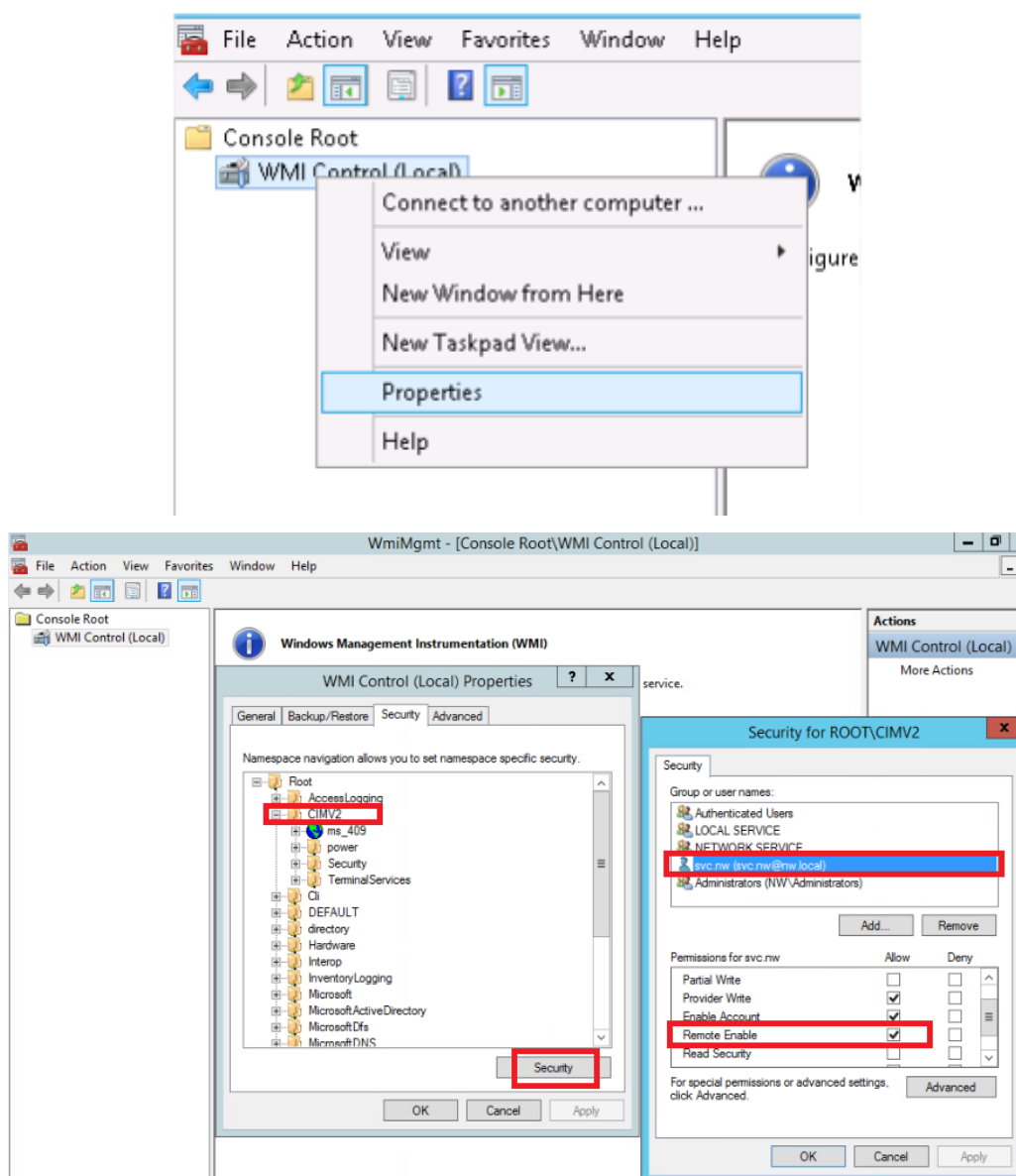


IT-PRO-012 Rev.00	CONFIGURAÇÃO DO WINRM PARA PERMITIR A COLETA DE LOGS VIA HTTP PARA O ISH VISION	
Classificação Restrito		

6.7. 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**).

IT-PRO-012 Rev.00	CONFIGURAÇÃO DO WINRM PARA PERMITIR A COLETA DE LOGS VIA HTTP PARA O ISH VISION	
Classificação Restrito		

6.8. 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.

```
PS C:\script> .\winrmconfig.ps1 -Action enable -ListenerType http -Port 5985 -User svc.nw@nw.local
winrmconfig script version 1.22
More verbose logging can be found in C:\Users\ADMINI~1\AppData\Local\Temp\winrmconfig.log

THE FOLLOWING CERTIFICATE(S) SUPPORT SERVER AUTHENTICATION ENHANCED KEY USAGE(REQUIRED FOR CREATING AN HTTPS LISTENER):
No Valid certificate found to allow creation of an https listener, currently this system will support http only
END OF CERTIFICATE LOOKUP

Checking HTTP SPN (required for WinRM access to this system via Kerberos) has not been assigned another Domain object
No conflicting SPN was found matching the spn (HTTP/WIN-9B4F291E1IM.nw.local) the collector requires to get a service ticket to collect

Discovered HTTP Listener on port 5985

Quick configure for HTTP
WinRM service is already running on this machine.
WinRM is already set up for remote management on this computer.

Adding the Allow unencrypted setting for HTTP Listener

CURRENT LISTENER(S) INFORMATION:
Listener: [Source="GPO"] Address = * Transport = HTTP Port = 5985 Hostname Enabled = true URLPrefix = wsman CertificateThumbprint ListeningOn = 10.200.220.159, 127.0.0.1

Configuring security event log access for the NETWORK SERVICE account (WinRM Service uses this account to read event logs)
sl security /ca:0:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20)
SECURITY LOG ACCESS FOR NETWORK SERVICE ACCOUNT CHECK ENDS
COLLECTION USER RIGHTS CHECK BEGINS HERE...

Checking access to the WinRM WMI Plugin (necessary for SID resolution)
User svc.nw@nw.local with SID S-1-5-21-3821415147-2330323532-580048511-1106 is already added to the WinRM WMI Plugin SDOL (Security analytics can resolve SIDs with this account)

Checking access to the CIM Root (necessary for Event log collection)
User svc.nw@nw.local with SID: S-1-5-21-3821415147-2330323532-580048511-1106 is already enabled for WMI access via WinRM (Security Analytics can collect Event logs using this account)

Checking user svc.nw@nw.local membership to the Event Log Readers group
User svc.nw@nw.local is already a member of Event Log Readers group
COLLECTION USER RIGHTS CHECK ENDS HERE...

Changes have been made that require a WinRM Service restart, restarting...
WinRM Service restarted.
```

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.
```