


IT-PRO-006 Rev. 00	<b>CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS</b>	
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 coleta de logs para o ISH Vision.

## 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.

## 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

IT-PRO-006 Rev. 00	CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS	
Classificação: Restrito		

## 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.

### 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 criptografado HTTPS e permitir a exportação do arquivo PEM** necessário para conclusão dos procedimentos de configuração de coleta de logs através do *WinRM* do *Active Directory* para o *RSA NetWitness*.

IT-PRO-006 Rev. 00	CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS	
Classificação: Restrito		

## 6. PROCEDIMENTOS

### 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), **NAT IP Address** (quando aplicável), **IP Address**, **Network Mask**, **Default Gateway**, **DNS Server IP(s)** (quando aplicável), **NTP Server IP(s)** (quando aplicável).



#### Questionário de Pré-Instalação Plataforma de Coleta de Logs

Device Name	Platform Type & Model	NAT IP Address	IP Address	Network Mask	Default Gateway	DNS Server IP(s)	NTP Server IP(s)

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

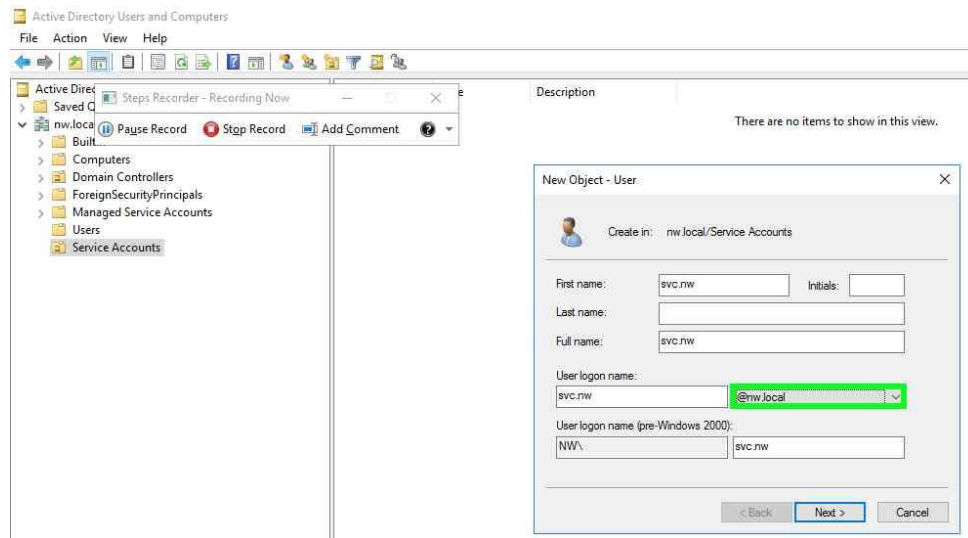
O *RSA NetWitness* utiliza uma porta específica para coleta de *logs* via protocolo criptografado HTTPS. Desta forma, será necessário garantir que o servidor tenha a porta **5986** aberta para entrada de origem do endereço **IP do Log Decoder**.

**Passo 1** - Liberar acesso externo de origem via **IP do Log Decoder** para a **porta TCP 5986** (HTTPS).

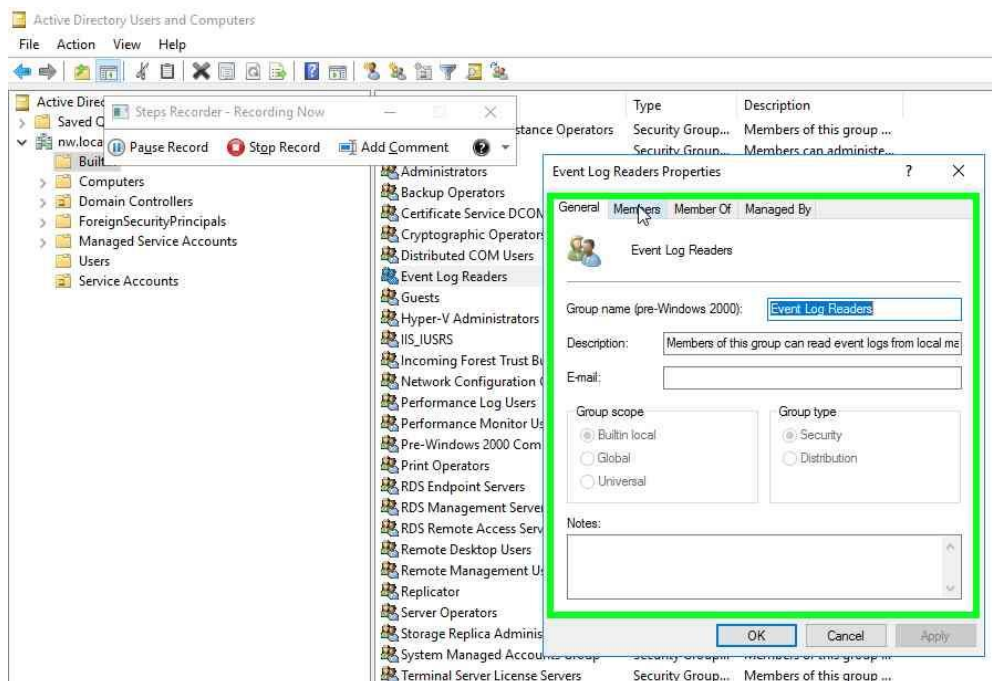
Este passo pode variar de acordo com as tecnologias utilizadas no ambiente. Por exemplo, caso tenha algum antivírus agindo como um *firewall*, essa liberação deverá ser executada no mesmo. Paralelamente deverá ser permitido a comunicação para essa Porta e IP de origem oriundo do *RSA NetWitness* no *Firewall*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

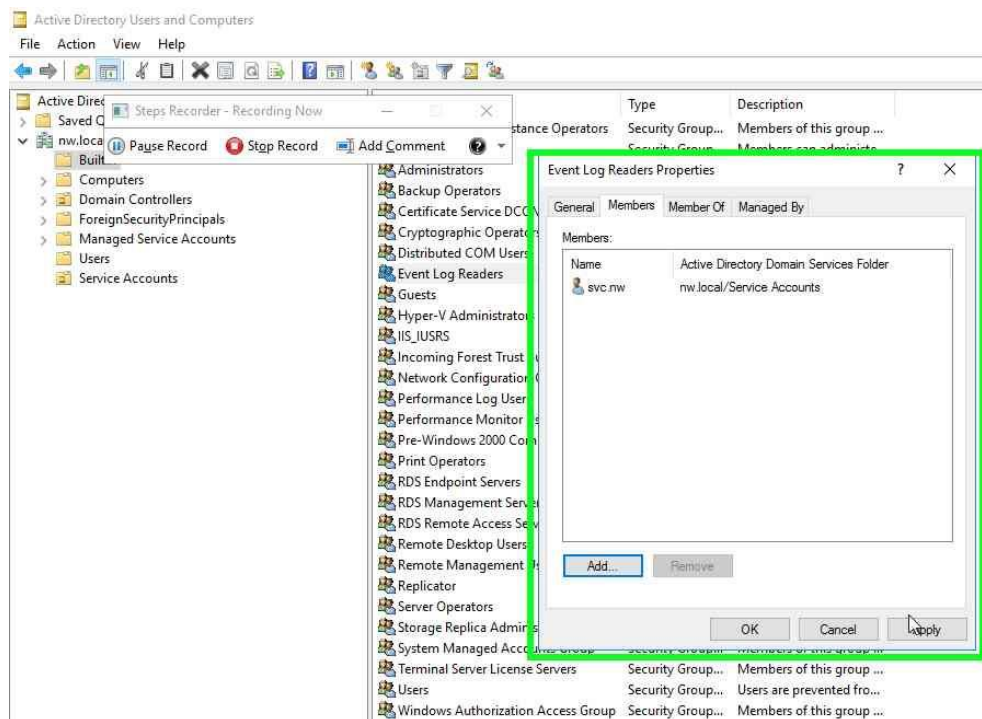
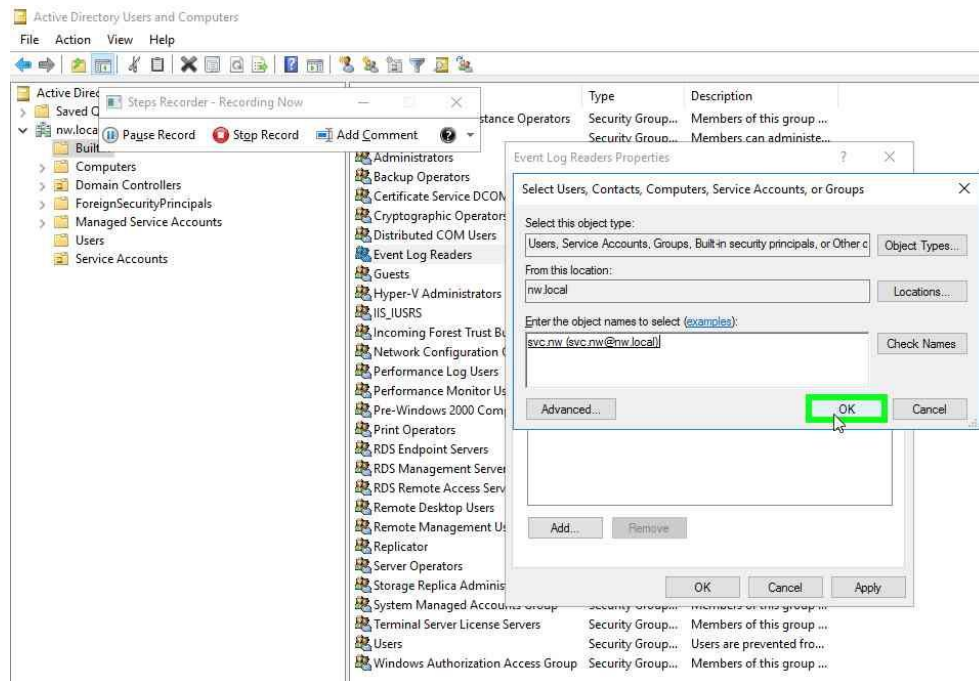
### 6.3 Criação de Usuário para Coleta de Logs

**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 **Grupo Event Log Readers**.







IT-PRO-006 Rev. 00	<b>CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS</b>	
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).

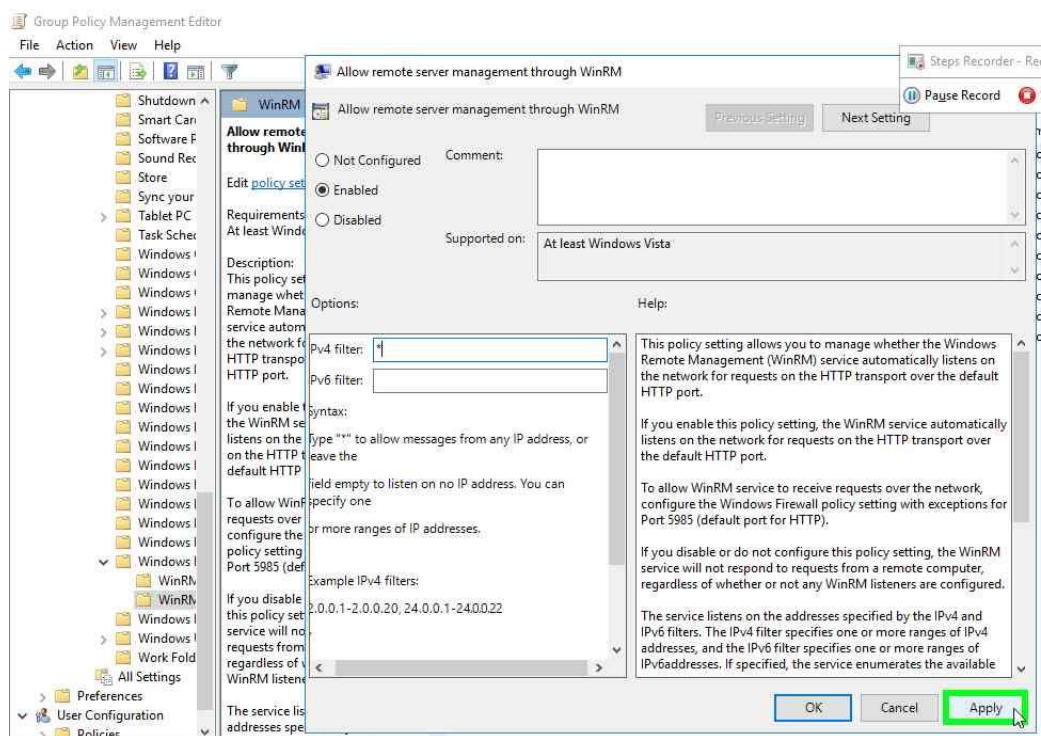
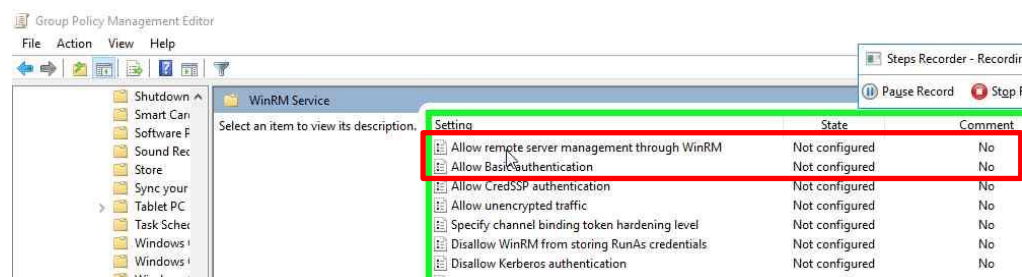
**Passo 1** - Na política *Default Domain Controller Policy* acessar o **WinRM Service**:

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

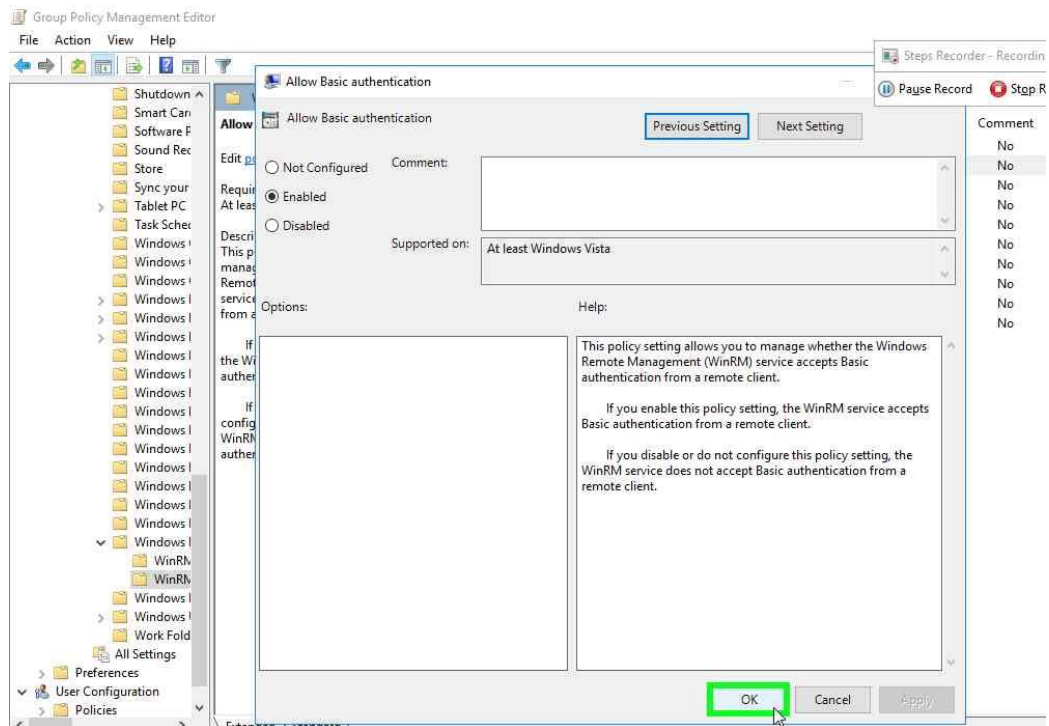
**Passo 2** - Habilitar as seguintes configurações:

***Allow remote server management through WinRM - Enabled***

***Allow Basic Authentication – Enabled***



IT-PRO-006 Rev. 00	<b>CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS</b>	
Classificação: Restrito		



## 6.5 Emissão de Certificado via *Root CA* para HTTPS

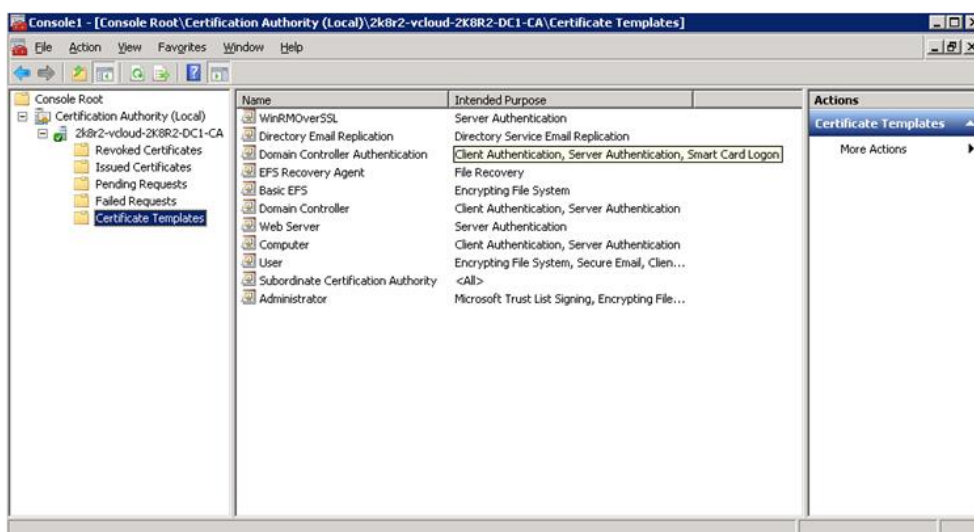
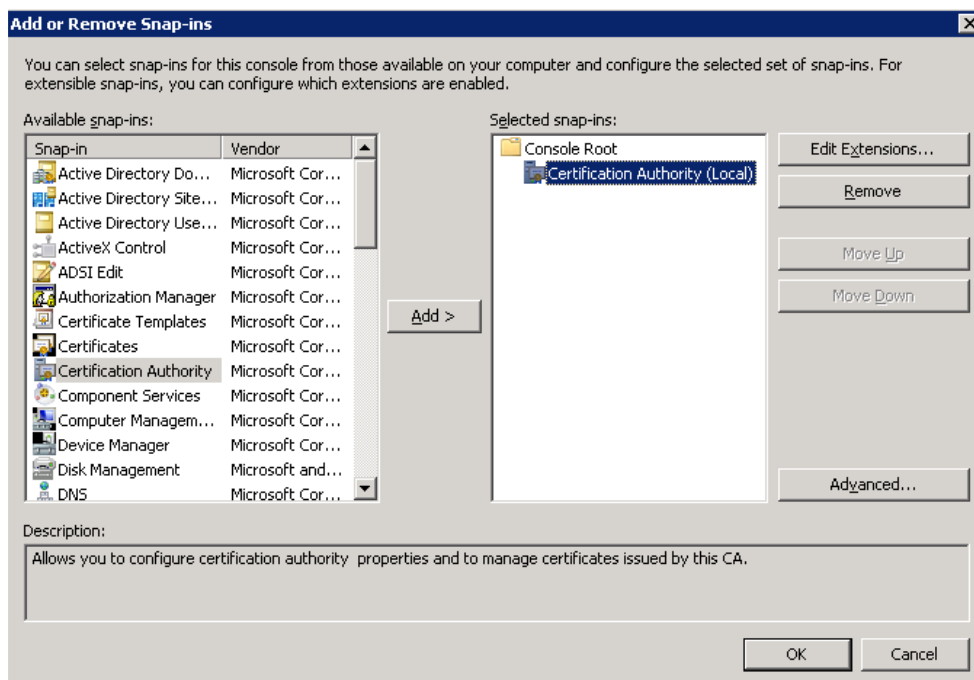
**Nota:** Este procedimento é opcional e deverá ser executado caso não possua nenhum *template* de certificado baseado em *Web Server* com as mesmas configurações indicadas neste guia.

Para que seja possível o funcionamento do *WinRM* via HTTPS é necessário **configurar** um ***Template*** de Certificado (caso não possua algum) para que seja emitido o certificado para os controladores de domínio. **Para mais detalhes deste procedimento, vide anexo 02 (página 17).**

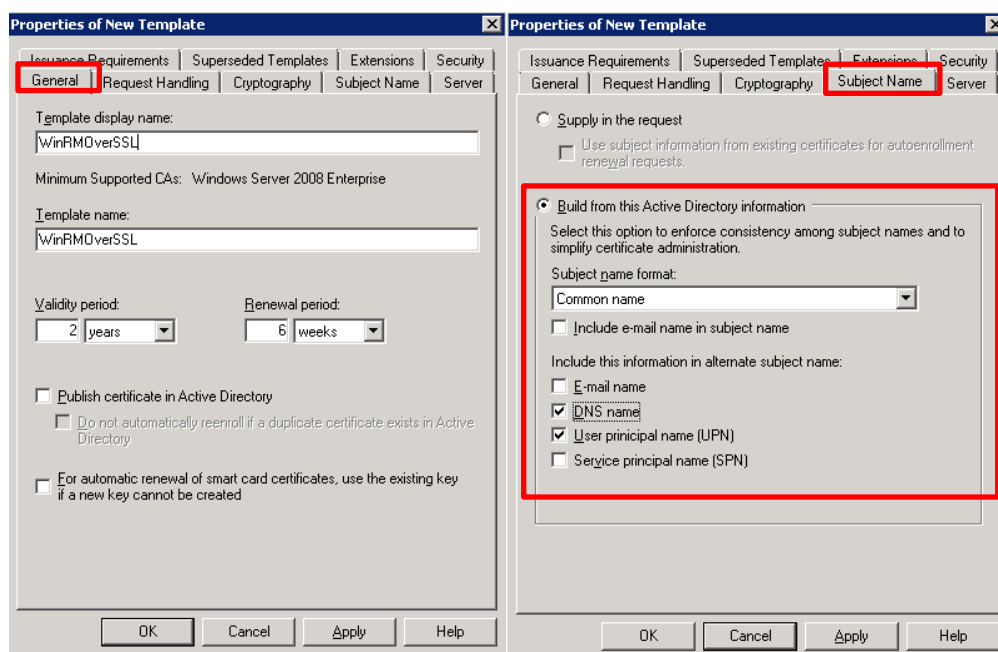
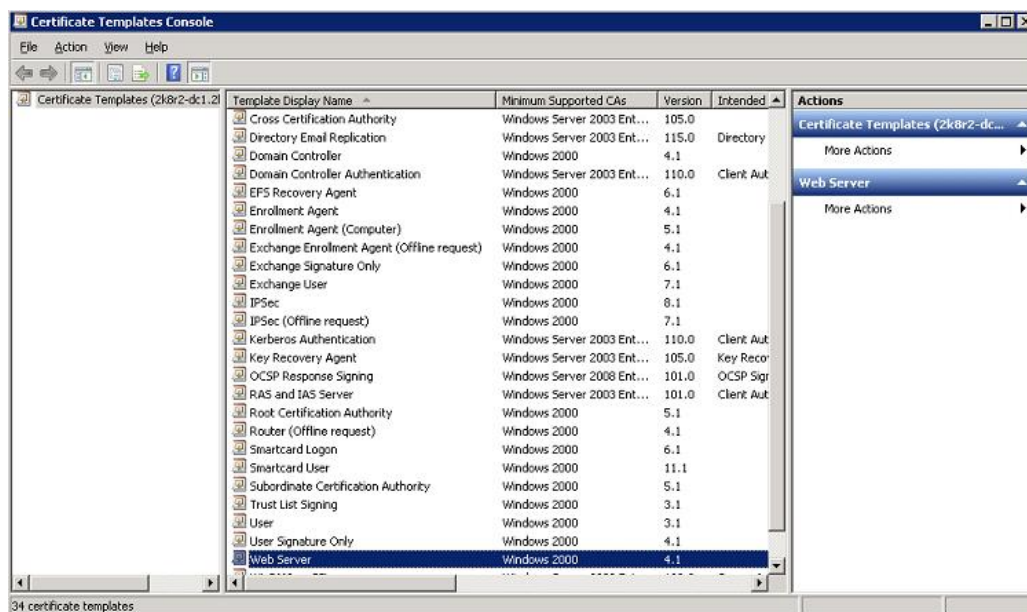
### Passo 1 - Criar o *Template* de Certificado

As imagens abaixo são meramente ilustrativas para este passo.

O Administrador de Domínio pode utilizar o método que preferir e for de seu conhecimento prático, para realizar este passo de criar o *template*.

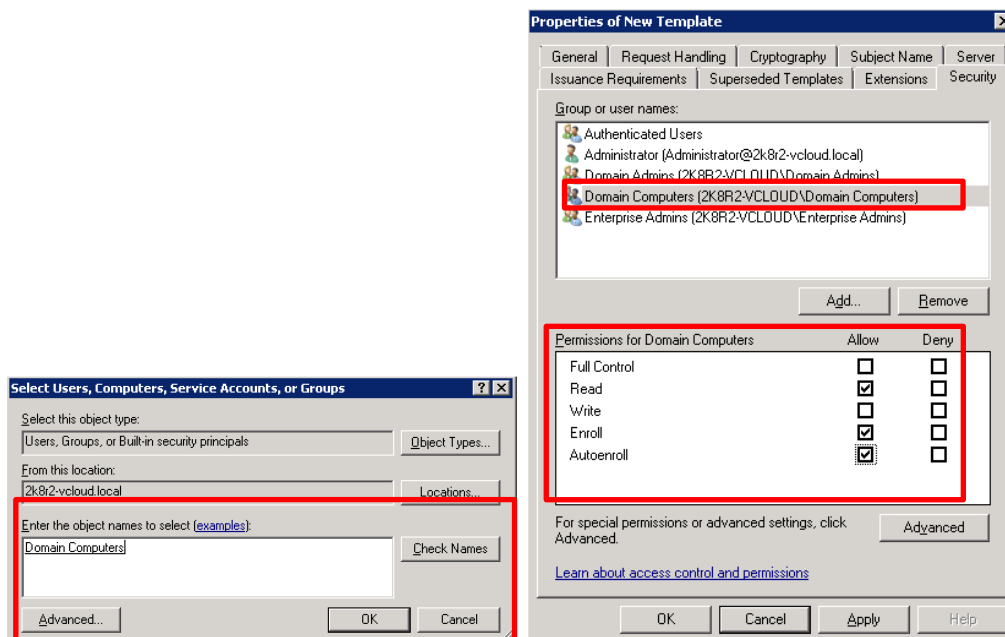






Na aba “**Subject Name**” habilite “**Built from this AD information**” e no menu drop-down “**Subject name format**”, selecione “**Common name**”.

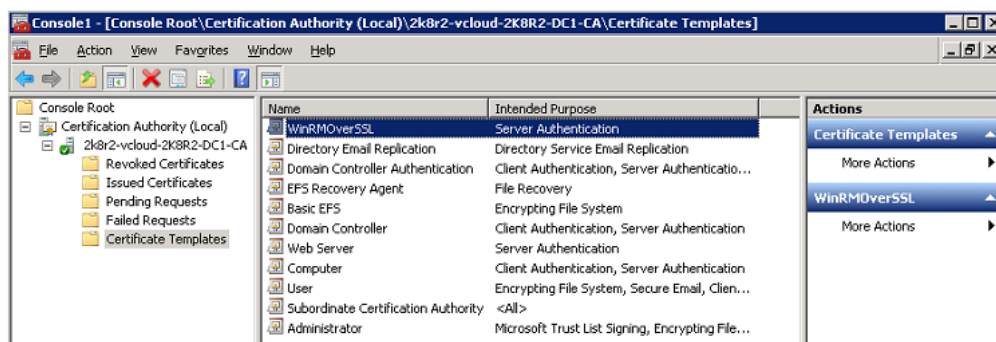
Em “**Alternate subject name**” deixe selecionado “**DNS Name**” e “**User principal name (UPN)**”.



Na aba “**Security**” clique em adicionar e adicione o *object name* “**Domain Computers**” (ou grupo criado especificamente para este serviço)

As permissões para “**Domain Computers**” devem estar “**Allow**” para “**Read**”, “**Enroll**” e “**Autoenroll**”.


Por fim, para habilitar este novo *template*, na console **Certification Authority**, clique com o botão direito do mouse em **Certificate Templates**, em seguida “**New > Certificate Template to issue**”, e selecione apenas o template que foi criado.



## Passo 2 – Configurar Auto Enrollment via GPO

Após criação do *template* é necessário configurar uma GPO para **Auto Enrollment** (emissão automática do certificado via GPO).

**Nota:** Dependendo do escopo da GPO, as configurações de certificado e WinRM podem ser feitas em GPOs separadas ou em uma única GPO.

IT-PRO-006 Rev. 00	<b>CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS</b>	
Classificação: Restrito		

### Passo 3 – Validar as configurações da GPO e a emissão do certificado.

Neste passo, utilize o procedimento padrão de valiação de seu próprio ambiente.

O objetivo do passo 3 é apenas ter certeza de que o certificado foi emitido e que as políticas para *auto enrollment* foi criadas.

***O certificado tem que conter, obrigatoriamente, o FQDN do servidor e o EKU ser do tipo Server Authentication.***

#### 6.5.1 Emissão de Certificado via MMC para HTTPS

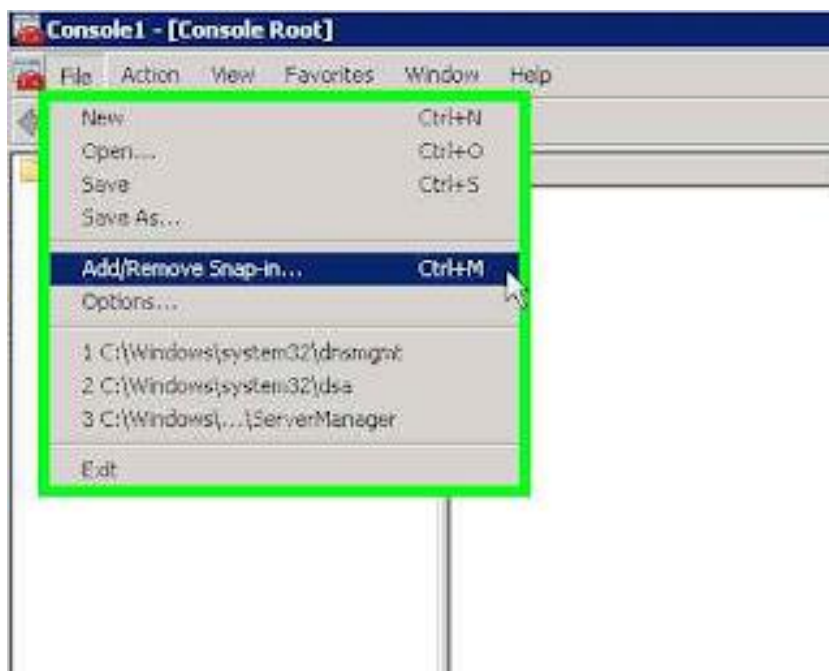
Uma alternativa para emissão de um certificado válido, é realizar o procedimento através do MMC (*Microsoft Management Console*).

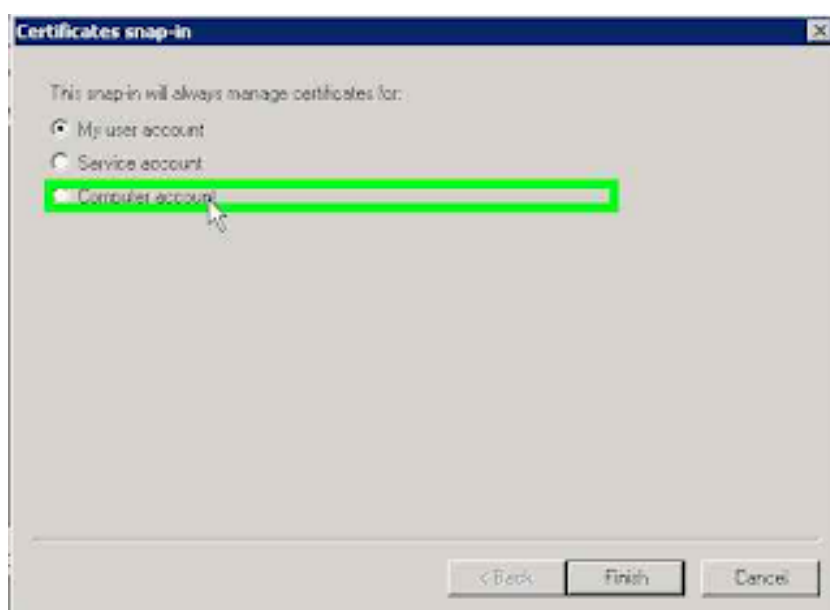
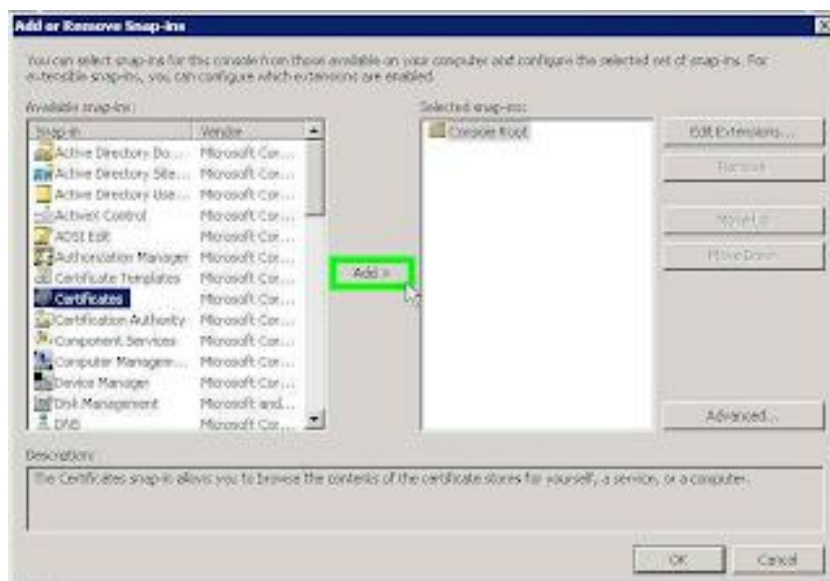
Vale lembrar que é apenas um método alternativo e 100% funcional, para o caso de não ser possível a emissão deste certificado através dos procedimentos anteriores.

##### Passo 1 – Abra o serviço de MMC (via executar ou cmd):

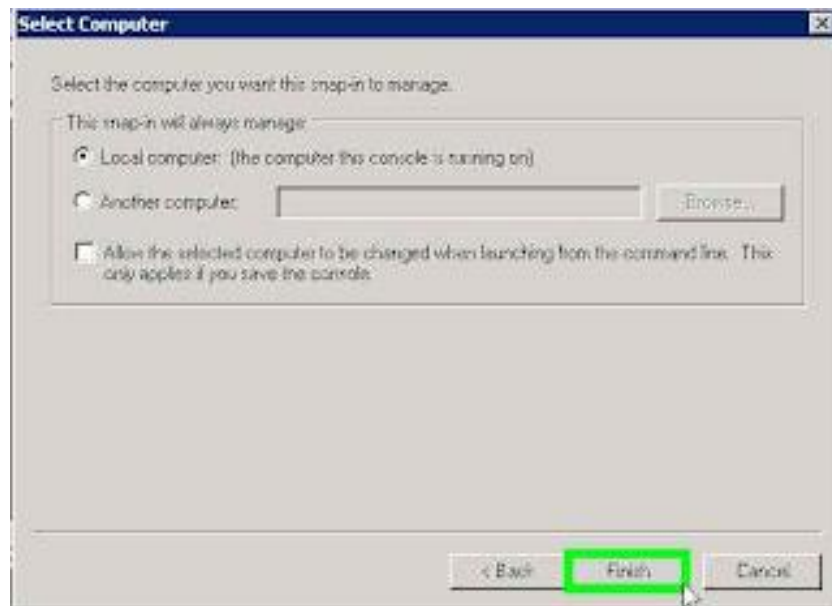
*MMC>>Com o serviço aberto, pressione CTRL+M ou acesse menu file > Add/Remove Snap-in*

Em seguida, siga os passos a seguir conforme indicado nos prints de tela:

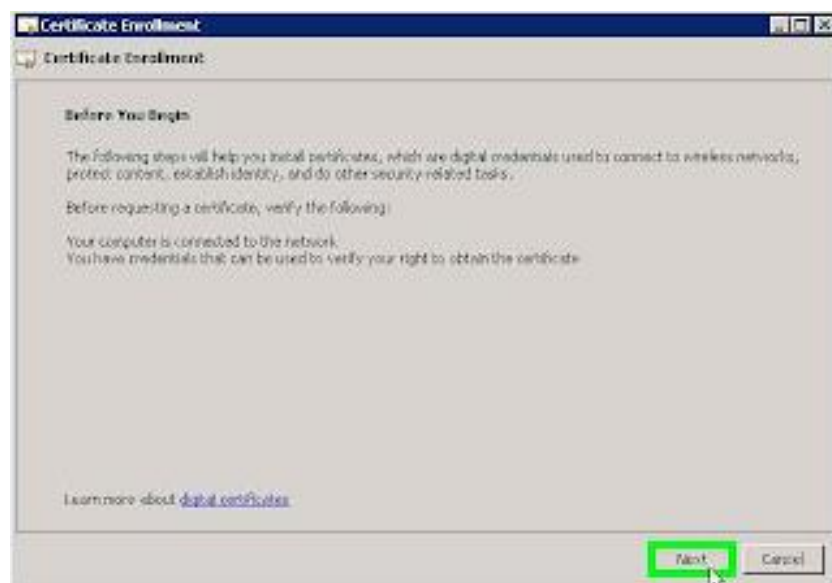


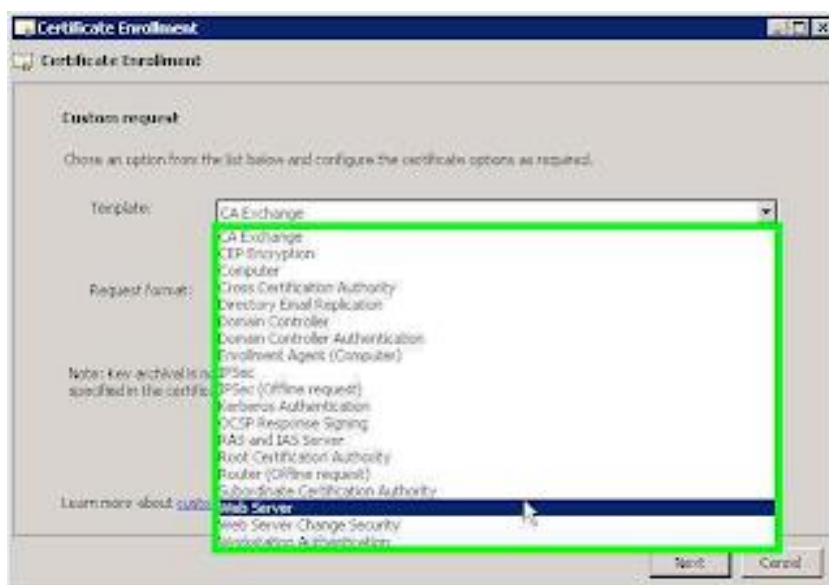
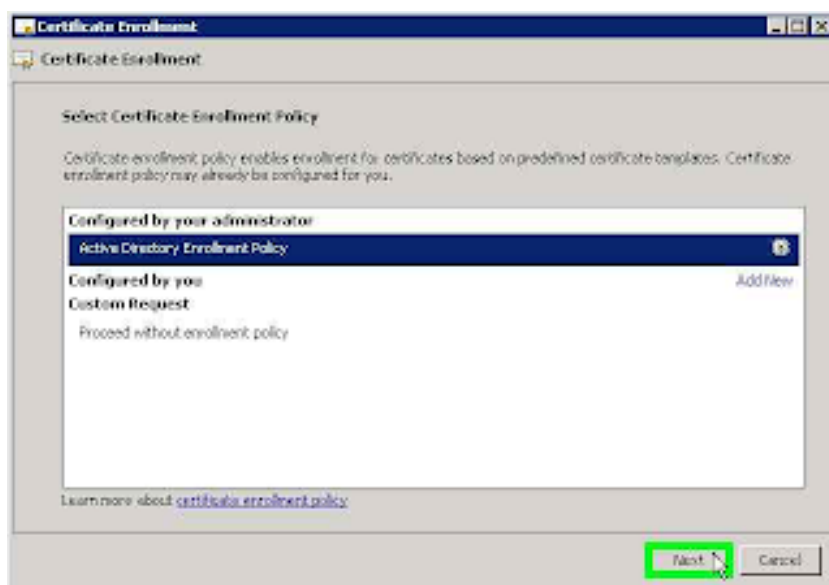


IT-PRO-006 Rev. 00	<b>CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS</b>	
Classificação: Restrito		



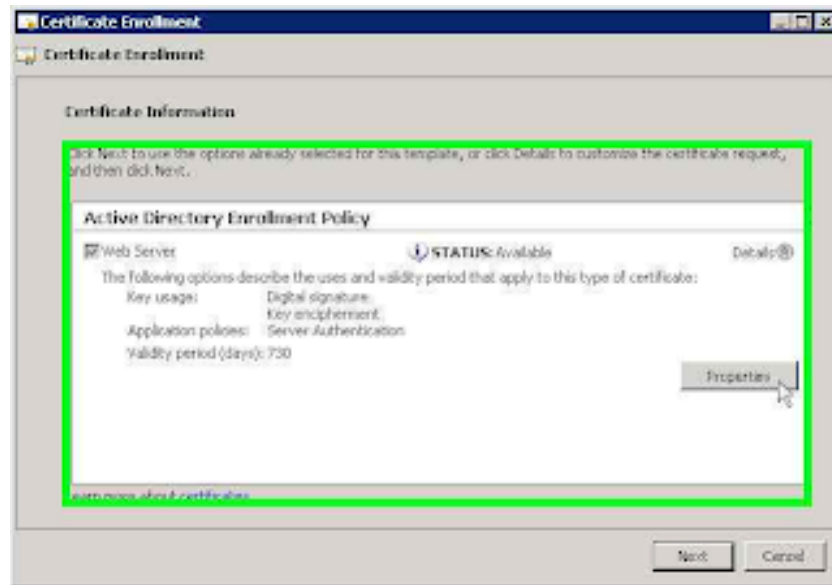
Agora será necessário realizar “*Request Certificate*”. Pode iniciar uma “*Request New Certificate*”:



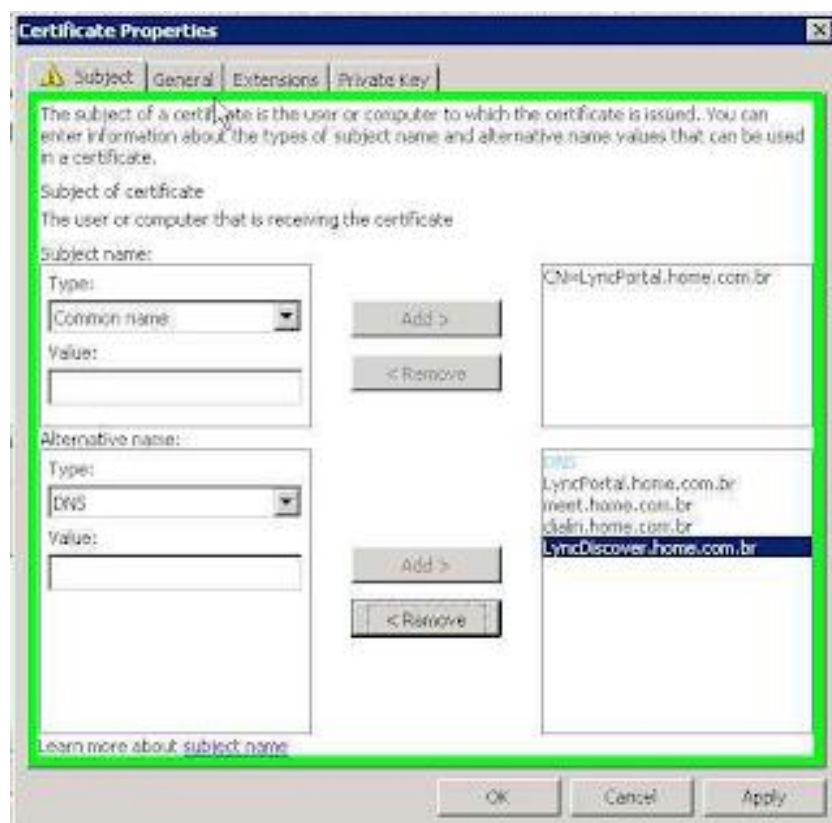





IT-PRO-006 Rev. 00	<b>CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS</b>	
Classificação: Restrito		



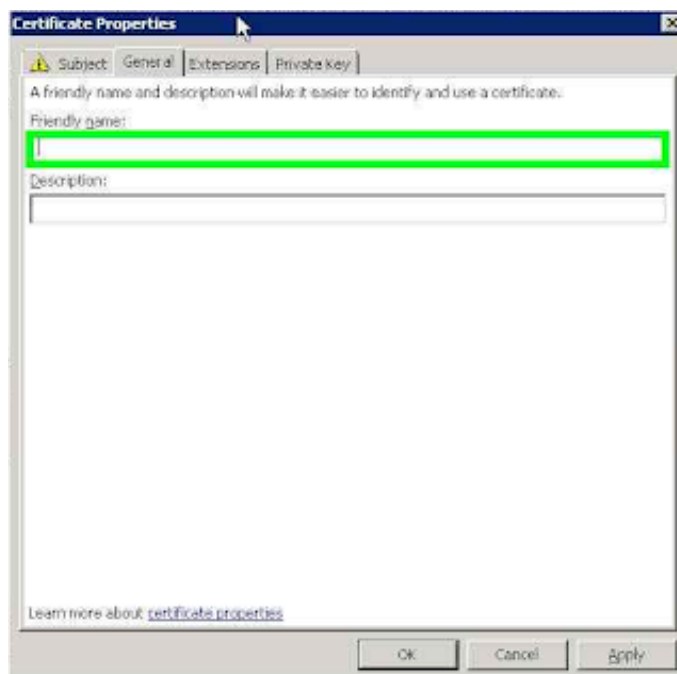
As vezes pode ser que ao invés de surgir “*Properties*”, aparece um link solicitando para preencher as configurações necessárias para o certificado.



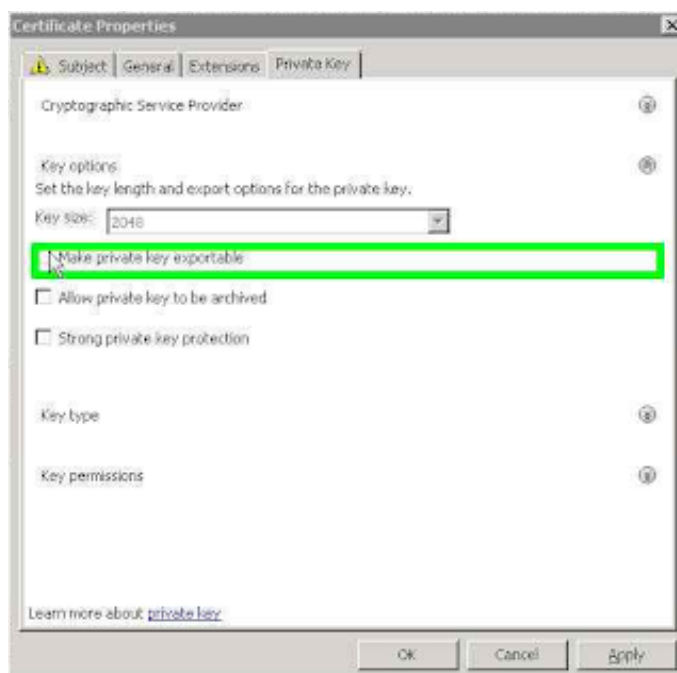
Na aba “*Subject*” da janela Certificate Properties, configure o “*Common Name*” em “*Subject Name*” para o nome completo do Domain Controller, por exemplo, **HOSTNAMEDC.DOMINIO-SITE.COM.BR**.


<b>IT-PRO-006</b> Rev. 00	<b>CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS</b>	
<b>Classificação:</b> Restrito		

Em “*Alternative name*”, configure o tipo para “*DNS*”, seguindo o mesmo padrão de CN inserido anteriormente, por exemplo, **HOSTNAMEDC.DOMINIO-SITE.COM.BR**.



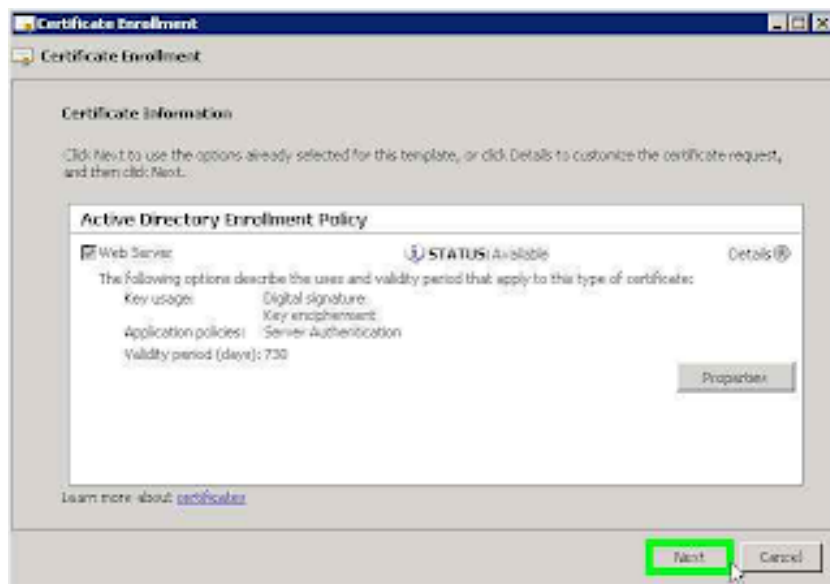
Na aba “*General*”, preencha o campo “*Friendly name*” com o mesmo valor inserido anteriormente em **CN/DNS: HOSTNAMEDC.DOMINIO-SITE.COM.BR**.



IT-PRO-006 Rev. 00	<b>CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS</b>	
Classificação: Restrito		

Na aba “*Private Key*”, abra as opções para “*Key options*” e marque a caixa “*Make private key exportable*”.

Por fim, confirme e aplique as configurações.



## 6.6 Configuração do *Listener* HTTPS

Após configurar a GPO e validar se o certificado foi emitido, você deve configurar o WinRM para escutar via HTTPS.

**Passo 1** – Utilize o comando abaixo para verifique o estado atual do *listener*

```
winrm e winrm/config/listener
```

**Passo alternativo** – Se verificar que o HTTPS não está habilitado, execute o comando abaixo

```
winrm quickconfig -transport:https
```

repita o passo 1 e confirme se o HTTPS 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 HTTPS, obtenha o securechannel (mesmo que *chanellAccess*) do *event log* utilizando o comando abaixo:

```
wevtutil gl security
```

IT-PRO-006 Rev. 00	CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS	
Classificação: Restrito		

```
C:\Users\Administrator>wevutil gl security
'wevutil' 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.

### 6.7 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:

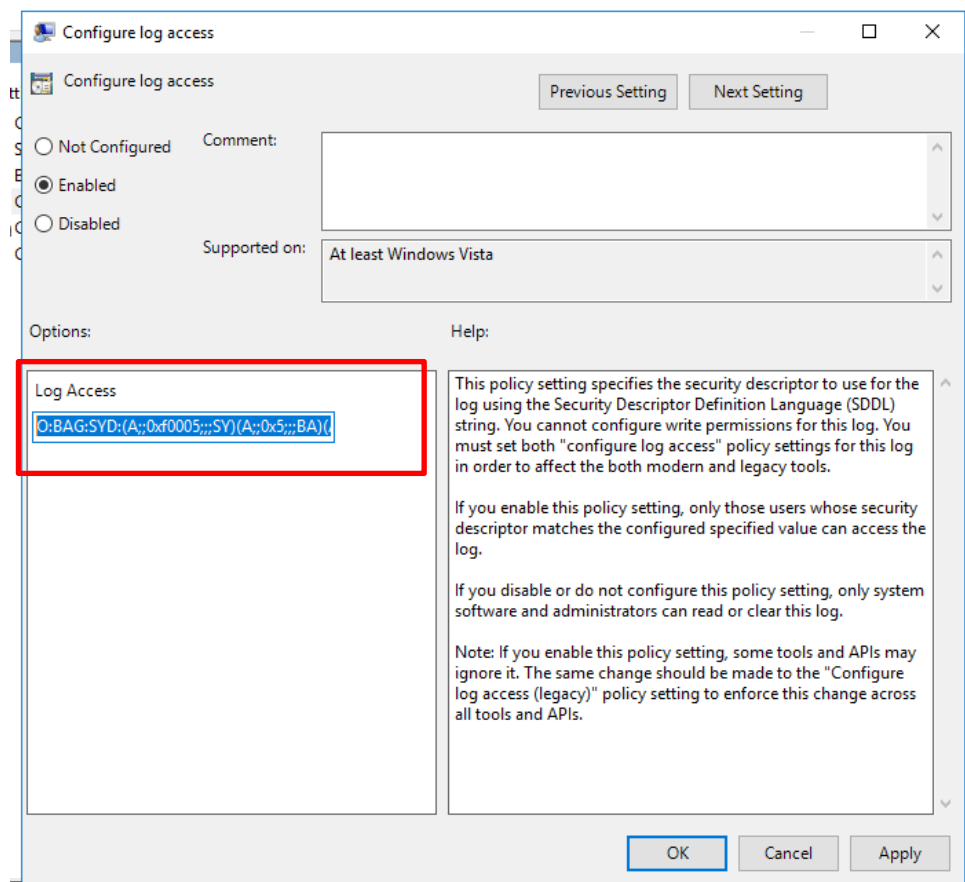
*Computer Configuration >> Policies >> Administrative Templates >> Windows Components >> Event Log Service >> Security*

**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
 <b>Configure log access</b>	<b>Enabled</b>	No
 Control Event Log behavior when the log file reaches its ma...	Not configured	No

IT-PRO-006 Rev. 00	<b>CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS</b>	
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.

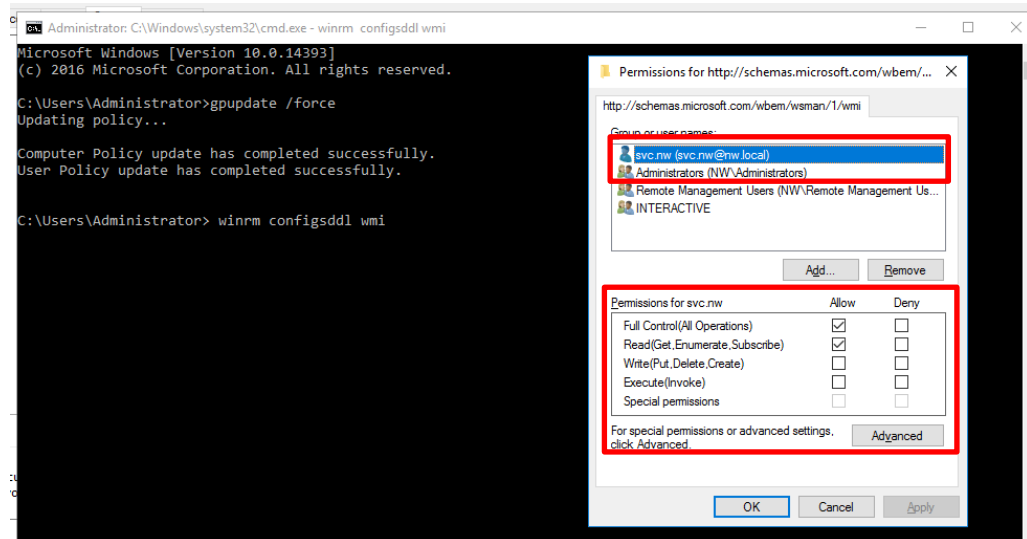
*rsop.msc*

IT-PRO-006 Rev. 00	<b>CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS</b>	
Classificação: Restrito		

**Passo 3** - Após validar que a configuração do log foi aplicada, execute o comando abaixo:

*winrm configsddl wmi*

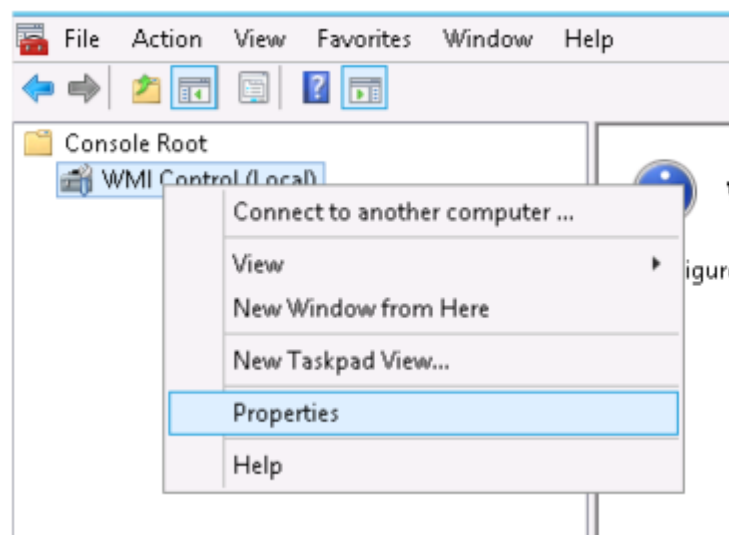
Na janela que é aberta dê permissão **Full Control** e **Read** para a conta de serviço que foi criada na seção 6.3 deste guia.



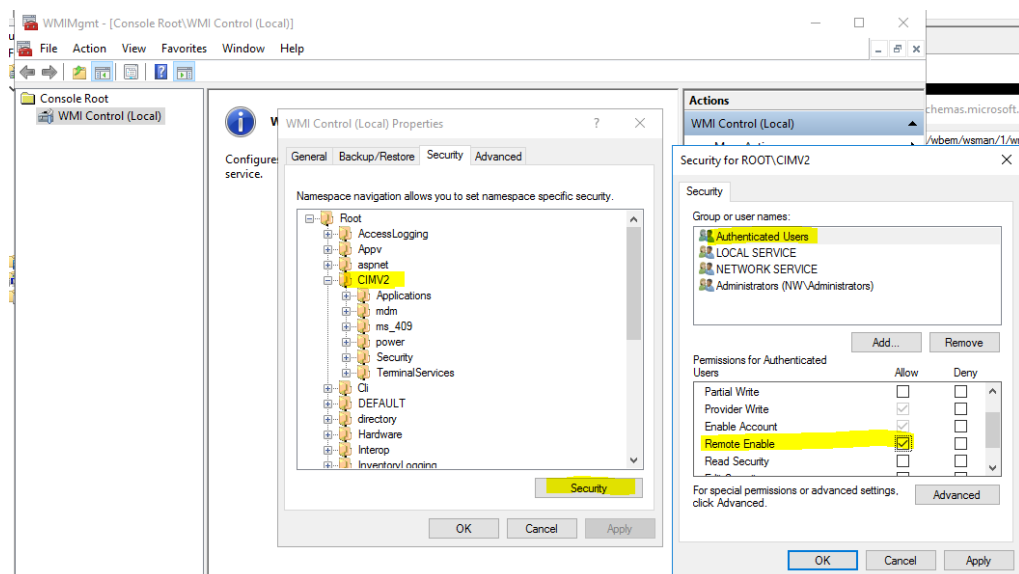
## 6.8 Permissões para o WMI

**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**).

## 6.9 Linkar Certificado ao 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 ShowAllCerts
```

IT-PRO-006 Rev. 00	CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS	
Classificação: Restrito		

```
winrmconfig script version 1.11
More verbose logging can be found in C:\Users\ADMINI~2\AppData\Local\Temp\2\winrmconfig.log
The following certificates were found:

    Cert Begins
Subject: CN=UWSvc-2K8R2-DC1
Issuer: CN=UWSvc-2K8R2-DC1
NotBefore: 06/13/2013 15:12:20
NotAfter: 06/11/2023 15:12:20
Thumbprint: 615B8BD73770C2AC229A407F010ADS2D146ED98A
Extensions:
Enhanced Key Usage: Server Authentication
Extensions ends
    Cert Ends

    Cert Begins
Subject: CN=2k8r2-vccloud-2K8R2-DC1-CA, DC=2k8r2-vccloud, DC=local
Issuer: CN=2k8r2-vccloud-2K8R2-DC1-CA, DC=2k8r2-vccloud, DC=local
NotBefore: 06/13/2013 15:07:36
NotAfter: 06/13/2018 15:17:35
Thumbprint: 1C6E2FBA47C625824BF316421F0C1D7219420485
Extensions:
Extensions ends
    Cert Ends

    Cert Begins
Subject: CN=2k8r2-dci.2k8r2-vccloud.local
Issuer: CN=2k8r2-vccloud-2K8R2-DC1-CA, DC=2k8r2-vccloud, DC=local
NotBefore: 04/07/2015 00:46:21
NotAfter: 04/06/2016 00:46:21
Thumbprint: 0B9F7C13540FA7FEFPE2E38D2E13C2460EC8BF52
Extensions:
Enhanced Key Usage: Client Authentication
Enhanced Key Usage: Server Authentication
Extensions ends
    Cert Ends

C:\temp>
```

Este comando irá exibir todos os certificados criados, identifique o certificado criado anteriormente e copie o ThumbPrint.

**Passo 2** – No mesmo local do passo 1 desta seção, execute o comando abaixo:

*.\winrmconfig.ps1 -Action enable -ListenerType https -Port 5986 -User user@domain -ThumbPrint XXXXXXXXXXXXXXXX*

*Informe o usuário criado na seção 6.3 deste guia.*

*Informe o ThumbPrint copiado anteriormente no passo 1 desta seção.*

```
winrmconfig script version 1.0
More verbose logging can be found in C:\Users\ADMINI~2\AppData\Local\Temp\2\winrmconfig.log
THE FOLLOWING CERTIFICATES SUPPORT SERVER AUTHENTICATION ENHANCED KEY USAGE(REQUIRED FOR CREATING AN HTTPS LISTENER):
Cert Thumbprint: 615B8BD73770C2AC229A407F010ADS2D146ED98A Expires: 06/11/2023 15:12:20 Subject: CN=UWSvc-2K8R2-DC1
Cert Thumbprint: 0B9F7C13540FA7FEFPE2E38D2E13C2460EC8BF52 Expires: 04/06/2016 00:46:21 Subject: CN=2k8r2-dci.2k8r2-vccloud.local
END OF CERTIFICATE LOOKUP

Discovered HTTPS Listener on port 5999

HTTPS Listener requested
HTTPS Listener already configured on port 5999 which is different than selected: 5986 so deleting...
Attempting to delete the existing HTTPS Listener on port 5999
Creating HTTPS Listener with: thumbprint 0B9F7C13540FA7FEFPE2E38D2E13C2460EC8BF52 Port 5986 PQM 2k8r2-dci.2k8r2-vccloud.local
HTTPS listener created successfully on port 5986
Removing the allow unencrypted setting while creating HTTPS Listener (for added Security)
Shipping firewall rule for port 5986 inbound access as the firewall service is not running


CURRENT LISTENERS> INFORMATION:
Listener: Address = Transport = HTTPS Port = 5986 Hostname = 2k8r2-dci.2k8r2-vccloud.local Enabled = true URLPrefix = /
CertificateThumbprint = 0B9F7C13540FA7FEFPE2E38D2E13C2460EC8BF52 ListeningOn = 127.0.0.1, 192.168.26.120, ::1, fe80::100:7
fffe::11, fe80::100:7fffe::11, fe80::100:7fffe::11, fe80::100:7fffe::11

Configuring security event log access for the NETWORK SERVICE account (WinRM Service uses this account to read event logs)
Network Service S10 is already added to the Security Channel ACL (Security Analytics can collect Security Event logs using the newoluser@2k8r2-vccloud account)
SECURITY LOG ACCESS FOR NETWORK SERVICE ACCOUNT CHECK ENDS
COLLECTION USER RIGHTS CHECK BEGINS HERE...

Checking access to the WinRM UMI Plugin (necessary for SID resolution)
User: newoluser@2k8r2-vccloud with SID: S-1-5-21-4205194981-1966230051-3092141446-72291 is not part of the WinRM UMI Plugin (SID resolution
could not be possible using this account) so adding to SDDL...
Created new UMI Plugin with newoluser@2k8r2-vccloud's SID
Checking access to the CIM Root (necessary for Event log collection)
User: newoluser@2k8r2-vccloud with SID: S-1-5-21-4205194981-1966230051-3092141446-72291 is already enabled
for UMI access via WinRM (Security Analytics can collect Event logs using this account)

Checking user newoluser@2k8r2-vccloud membership to the Event Log Readers group
User newoluser@2k8r2-vccloud 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.
```

IT-PRO-006 Rev. 00	<b>CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS</b>	
Classificação: Restrito		

É interessante realizar um double-check dos listeners atuais para HTTPS 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*

**Passo alternativo** – Caso tenha identificado que o certificado configurado para o listener do HTTPS não possua o mesmo ThumbPrint setado anteriormente, você pode excluir o listener e tentar o procedimento novamente:

*winrm delete winrm/config/Listener?Address=\*&Transport=HTTPS*

## 6.10 Exportar o arquivo PEM

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

**Passo 1** – No mesmo local do passo 1 da seção 6.9, execute o comando abaixo, para gerar o arquivo PEM:

*.\winrmconfig.ps1 -Action exportcert*

O comando acima irá exportar um arquivo com extensão PEM no mesmo local em que se encontra o script “winrmconfig.ps1”.

## 6.11 Report Mode

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

**Passo 1** – No mesmo local do passo 1 da seção 6.9, execute o comando abaixo:

*.\winrmconfig.ps1 -Action Report -User user@domain*

Salve a saída deste comando (print de tela) em boa resolução.

## 6.12 Envio de arquivos para ISH

Durante a execução de todos os procedimentos anteriores, foram gerados alguns arquivos e/ou relatórios de comandos, conforme solicitado/executado em cada passo.

Ao final destes procedimentos, envie para a ISH Tecnologia:

*Todo(s) arquivo(s) gerado(s) com extensão .PEM*

*Relatório da seção 6.11 (print de tela)*

*Cada arquivo deverá estar devidamente identificado para cada Domain Controller onde foi executado.*

Dica: Organize os arquivos em pastas ou ZIP, para cada DC.

IT-PRO-006 Rev. 00	<b>CONFIGURAÇÃO DO WINRM PARA PERMITIR COLETA DE LOGS VIA HTTPS</b>	
Classificação: Restrito		

## 7. REFERÊNCIAS

**RSA Link. Configure Windows Collection.** 2019. Disponível em:  
<<https://community.rsa.com/docs/DOC-43410>> Acesso out 2019.

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

**SCOTT, Marcus. RSA Link. Microsoft WinRM Configuration and Troubleshooting.** 2016. Disponível em: <<https://community.rsa.com/docs/DOC-43306>> Acesso out 2019.

**SCOTT, Marcus. RSA Link. Microsoft WinRM Configuration Guide.** 2016. Disponível em: <<https://community.rsa.com/servlet/JiveServlet/downloadBody/58163-102-7-256542/WinRM+Configuration+Guide.pdf>> Acesso out 2019.