


IT-PRO-008 Rev. 00	CONFIGURAÇÃO DO MSSQL PARA COLETA DE LOGS	
Classificação: Restrito		

1. OBJETIVO

Este documento tem como objetivo auxiliar nos procedimentos de configuração do envio de eventos do Microsoft SQL Server para o ISH Vision.

2. AVISO LEGAL

Esta Instrução de Trabalho trata-se de um guia passo-a-passo para configurações no ambiente com SQL Server e 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.

4. ANEXOS

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


Item	Tipo	Título
01	Script Powershell	winrmconfig.ps1

5. SUMÁRIO EXECUTIVO

Este documento fornece informações para configurar os serviços *SQL Server* para permitir que o *RSA NetWitness* colete logs de eventos de SQL.

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

IT-PRO-008 Rev. 00	CONFIGURAÇÃO DO MSSQL PARA COLETA DE LOGS	
Classificação: Restrito		

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 *Listener* (HTTP/HTTPS) que aceite solicitações de um *collector*, como ferramenta de configuração;
- 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.

6. Pré-requisitos (Matriz de Compatibilidade)

Antes de realizar qualquer procedimento de configuração verifique se tanto o serviço quanto o sistema operacional possuem versões suportadas e homologadas pela RSA. Esta informação pode ser encontrada no **RSA NetWitness® Platform 11.3 Guides**, através do endereço <https://community.rsa.com/docs/DOC-105599>.

A tabela abaixo apresenta as versões e sistemas homologados para permitir estas configurações de espelhamento de portas.

Tabela 1 - Pré-requisitos para SQL Event Source


Abreviação	Descrição
SQL	SQL Server 2008 ou superior
Acesso	Acesso ao servidor e a console SQL

7. PROCEDIMENTOS

7.1 Servidores de SQL 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 Servidores SQL que terão seus logs coletados.

Acesse a planilha “Logs” dentro deste arquivo eletrônico e preencha corretamente as colunas: **Device Name (Hostname)**, **Platform Type & Model** (Serviço/Produto), **NAT IP**

IT-PRO-008 Rev. 00	CONFIGURAÇÃO DO MSSQL PARA COLETA DE LOGS	
Classificação: Restrito		

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)

7.2 Liberação de porta e endereço IP para Log Decoder

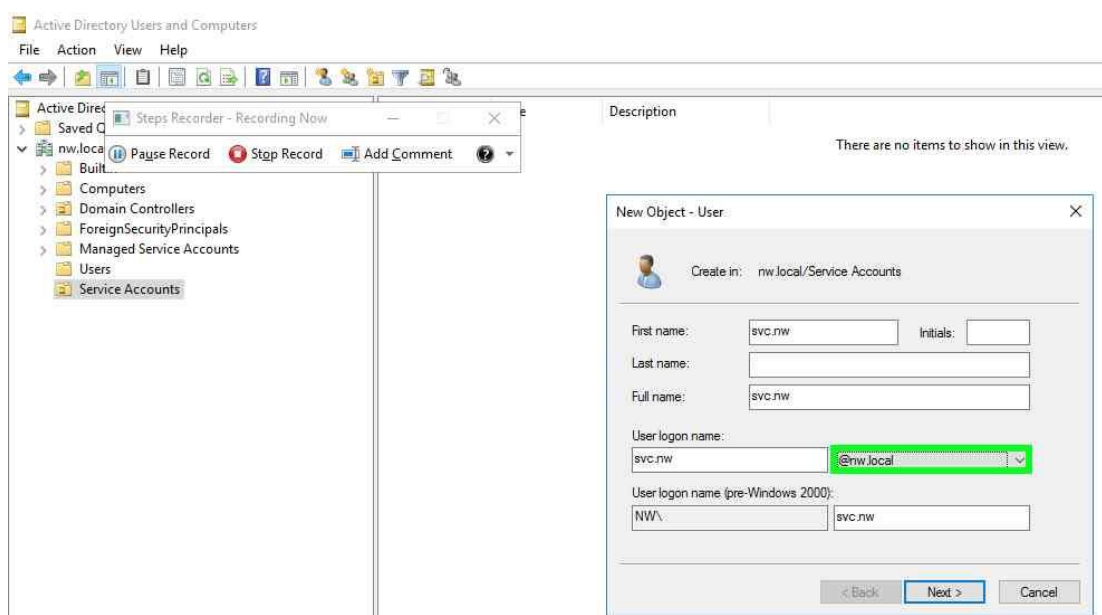
O *RSA NetWitness* utiliza uma porta específica para coleta de *logs* via protocolo HTTP. Desta forma, será necessário garantir que o servidor tenha a porta **5985** aberta para entrada de origem do endereço **IP do Log Decoder**.


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.

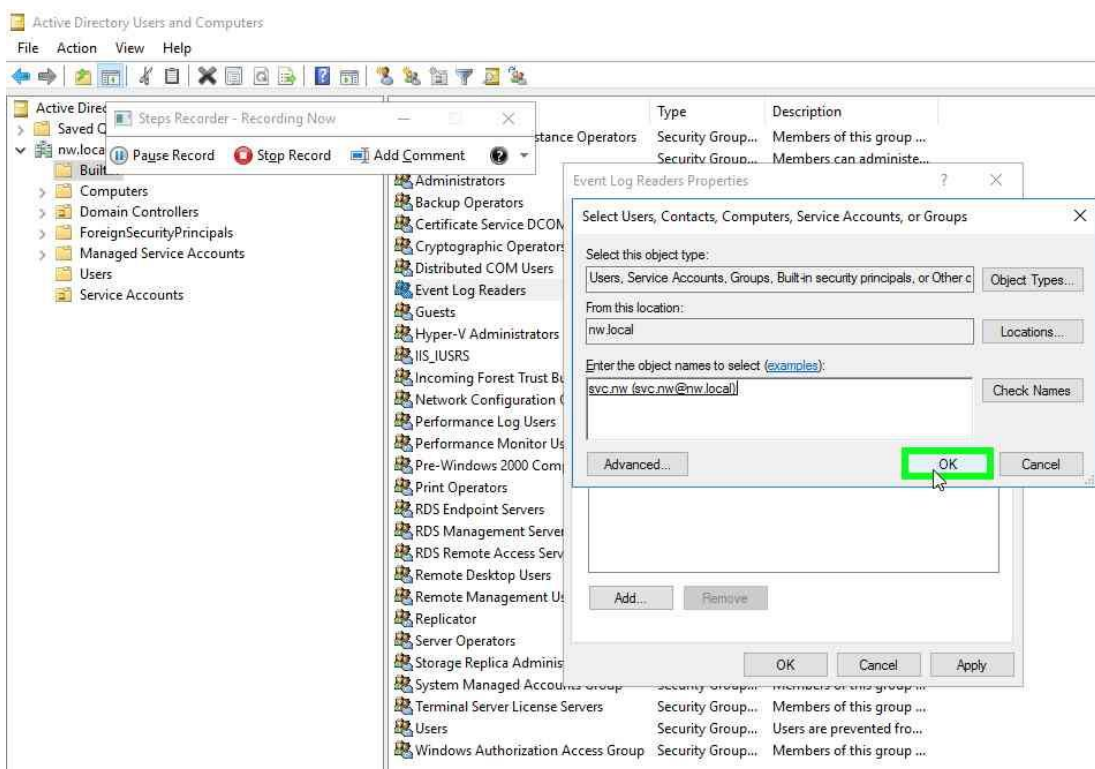
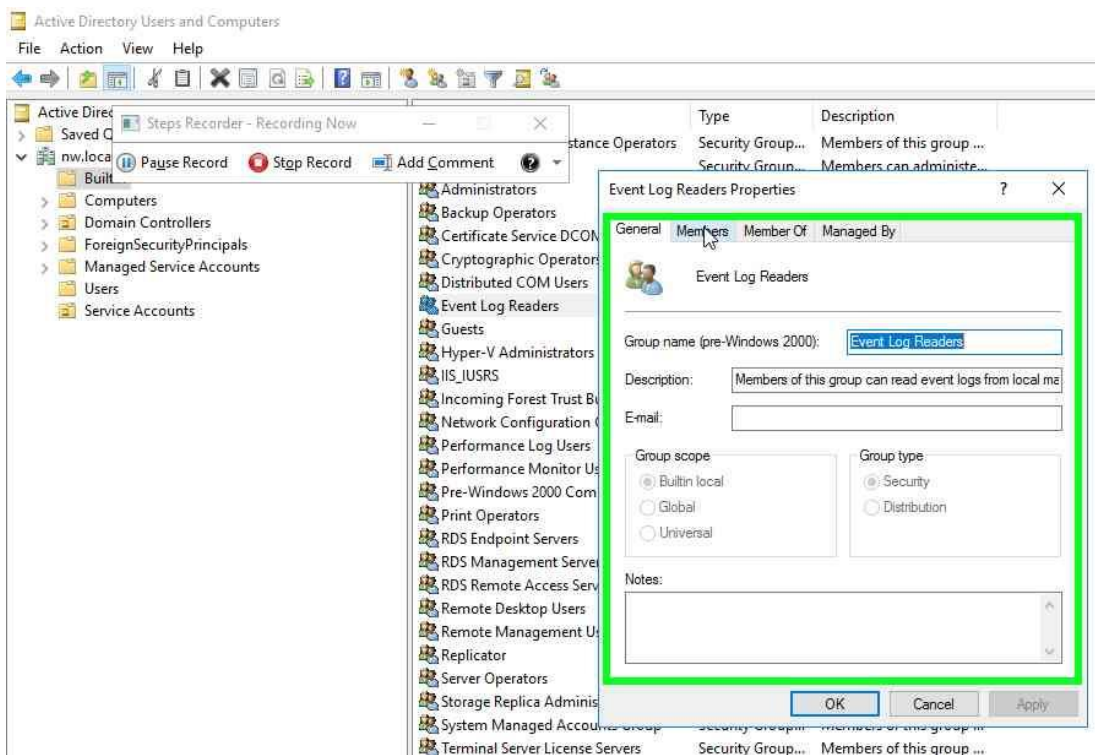
7.3 Criação de Usuário para Coleta de Logs


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

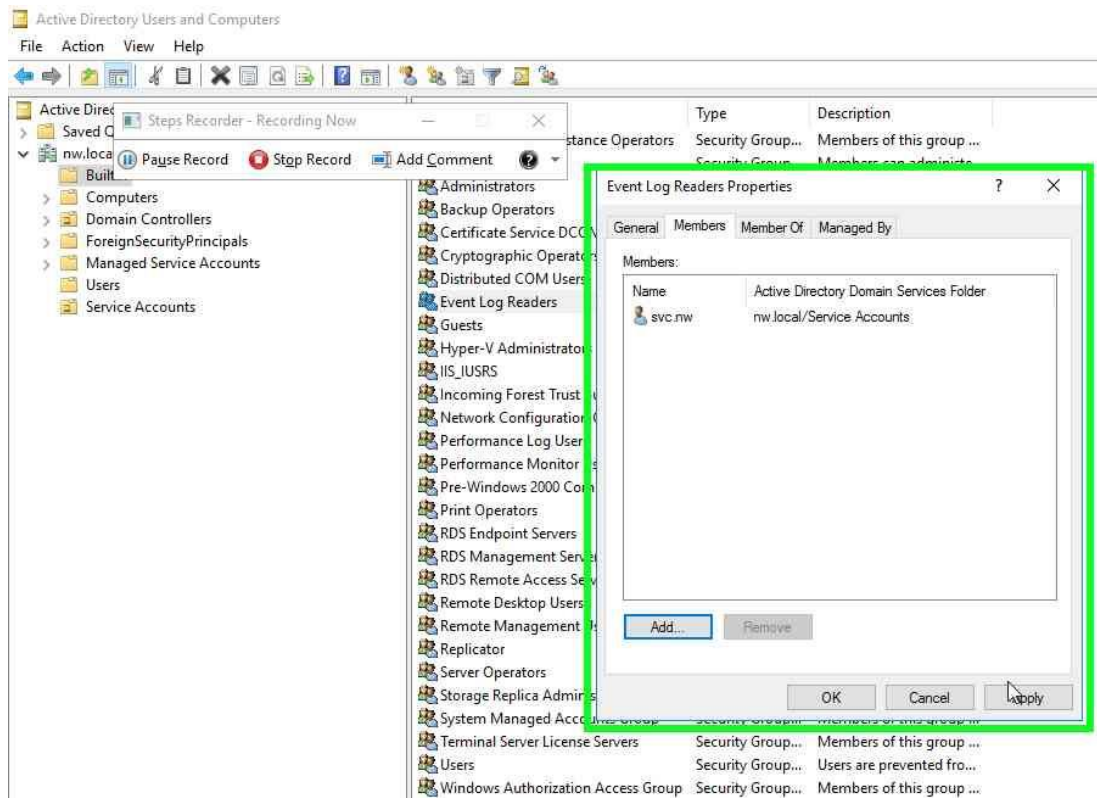


IT-PRO-008 Rev. 00	CONFIGURAÇÃO DO MSSQL PARA COLETA DE LOGS	
Classificação: Restrito		

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

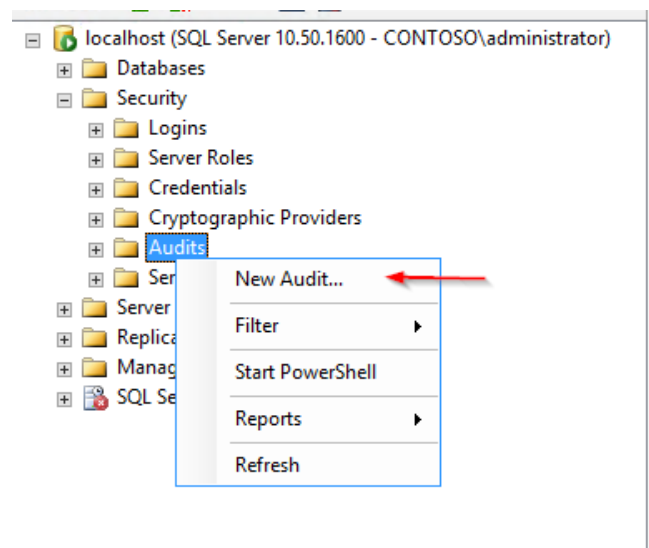


IT-PRO-008 Rev. 00	CONFIGURAÇÃO DO MSSQL PARA COLETA DE LOGS	
Classificação: Restrito		




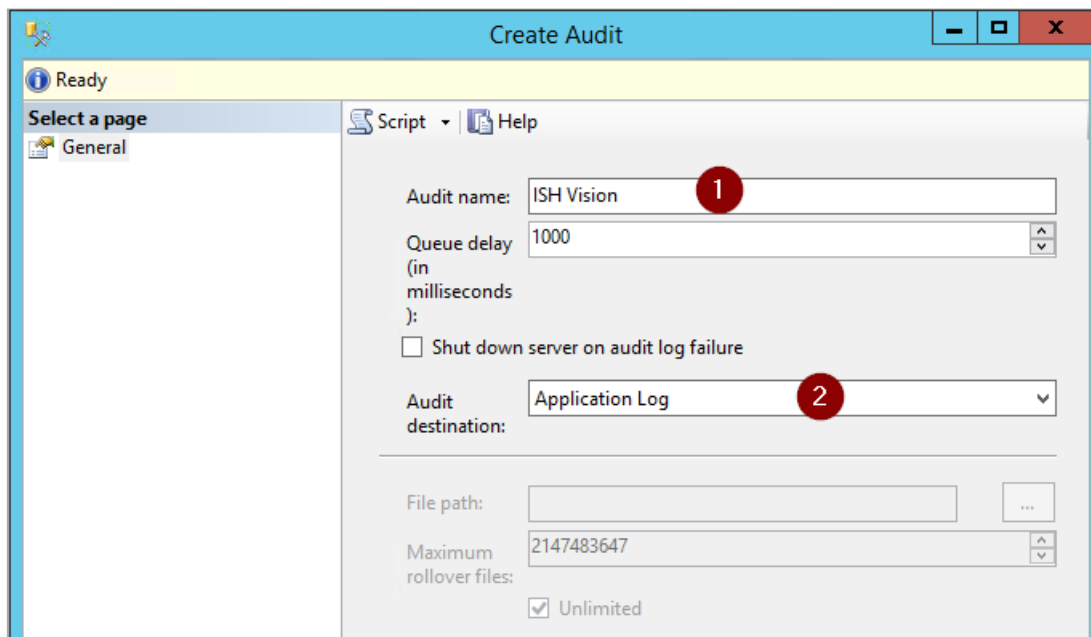
7.4 Criação de Audits

Passo 1: Clique em Server > Audit > New Audit...

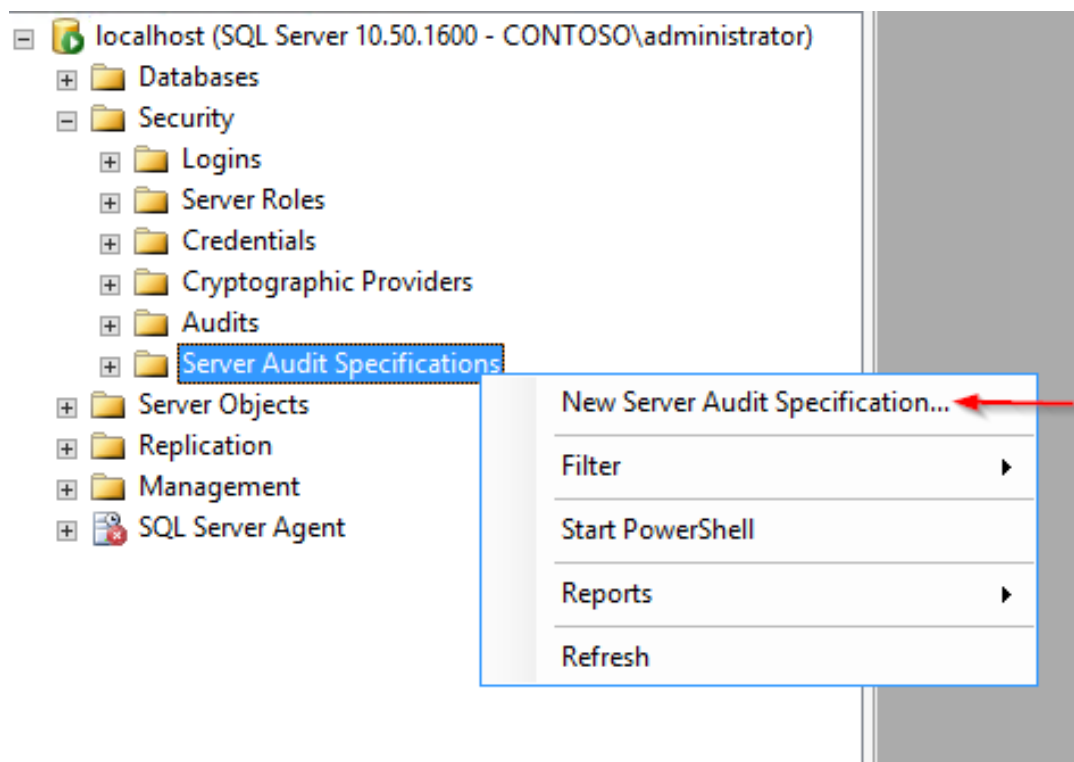


Passo 2: Em *Audit Name* insira o nome do Audit e em *Audit destination* selecione *Application Log*.

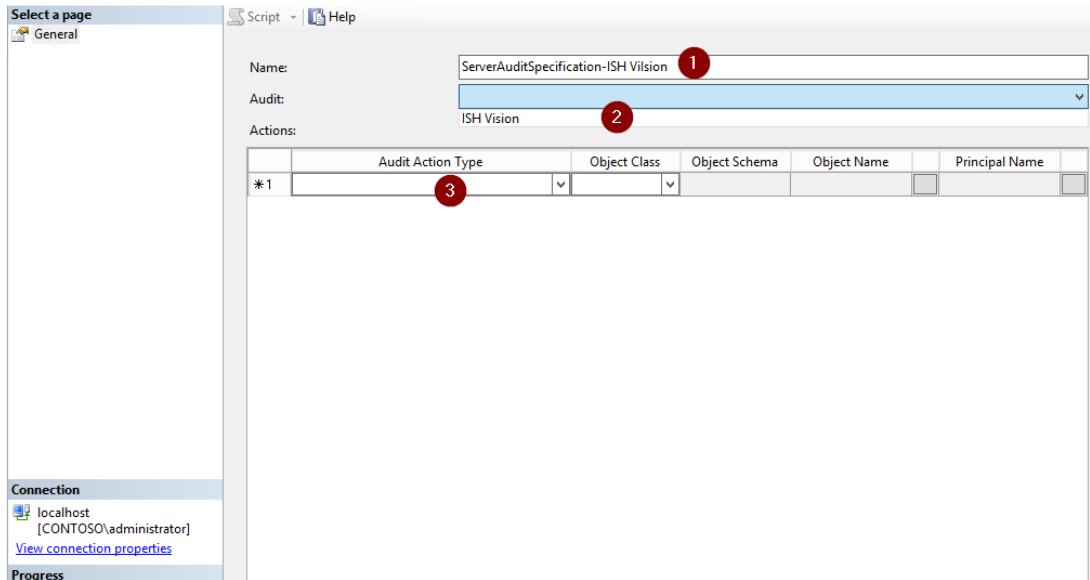
IT-PRO-008 Rev. 00	CONFIGURAÇÃO DO MSSQL PARA COLETA DE LOGS	
Classificação: Restrito		



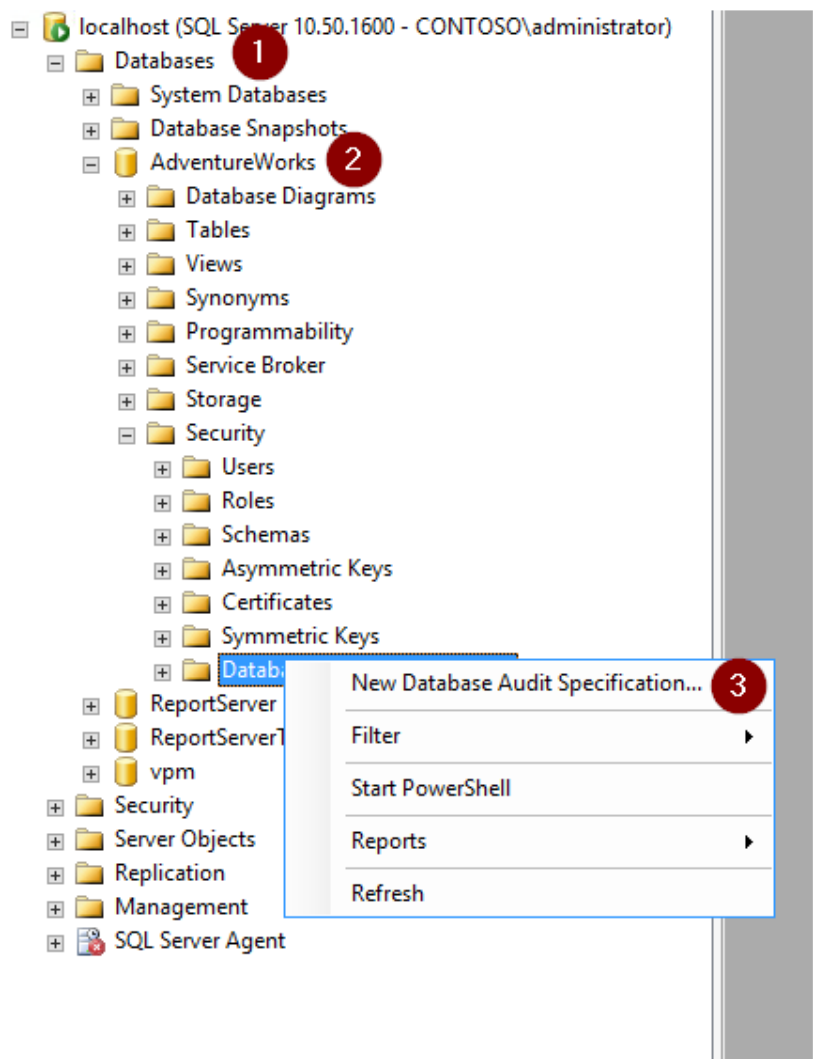
Passo 3: Em *Server Audit Specifications*, clicar em *New Server Audit Specification...*



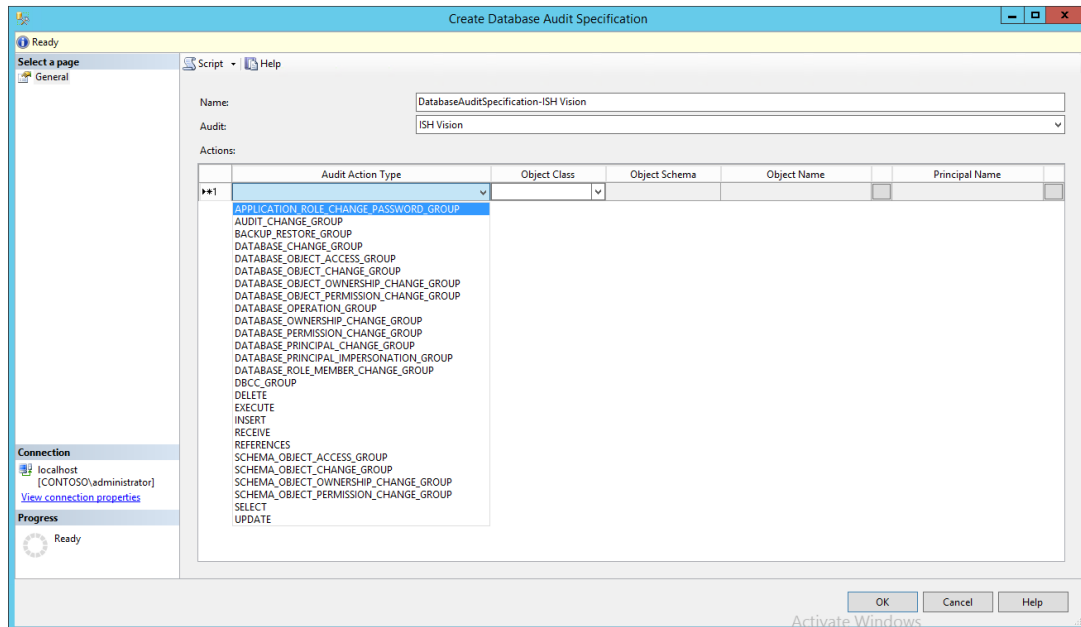
Passo 4: Defina um nome, em *Audit* Selecione a Auditoria criada anteriormente e posteriormente selecione quais ações você deseja auditar.



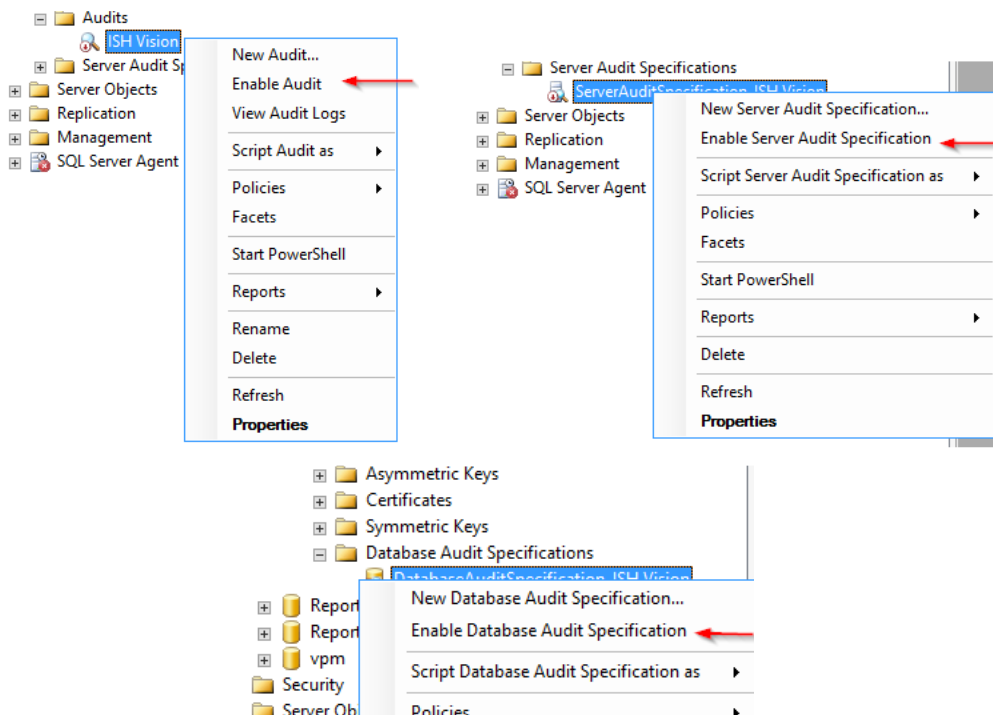
Passo 5: Habilite a Auditoria nas *Databases* que deseja monitorar. Selecione “*MinhaDatabase*” > *Security* > *New Database Audit Specification*.



Passo 6: Dê um nome a auditoria de database, selecione o **Audit** Criado no primeiro passo e posteriormente selecione as ações que deseja auditar.



Passo 7: Lembre-se de habilitar as Auditorias criadas, conforme imagens abaixo.



Passo 8: Para validar o funcionamento, verifique se no log de application do Event Viewer o eventid 33205 está sendo criado.

Application Number of events: 8.887 (!) New events available				
Level	Date and Time	Source	Event ID	Task C...
Information	06/02/2019 14:32:20	MSSQLSERVER	33205	Logon
Information	06/02/2019 14:32:20	MSSQLSERVER	33205	Logon
Information	06/02/2019 14:32:20	MSSQLSERVER	33205	Logon
Information	06/02/2019 14:32:20	MSSQLSERVER	33205	Logon
Information	06/02/2019 14:32:20	MSSQLSERVER	33205	Logon
Information	06/02/2019 14:32:20	MSSQLSERVER	33205	None
Information	06/02/2019 14:32:20	MSSQLSERVER	33205	None
Information	06/02/2019 14:32:20	MSSQL SERVER	33205	None

Passo 9: Aplique a mesma política utilizada para enviar o *log* do *Active Directory* nos servidores *SQL* que encaminharão *logs* para o *ISH Vision*.

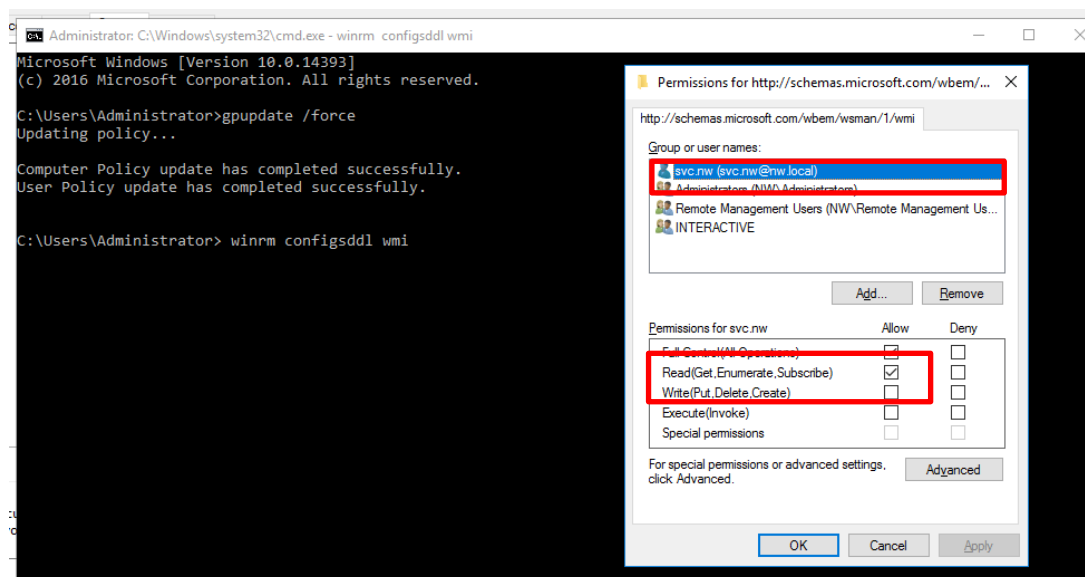
7.5 Permissões de acesso aos logs

Nota: Deverá ser realizado em todos os *Domain Controllers*.

Passo 1: Execute o comando abaixo e adicione o usuário criado para ler os *logs* com permissão de **Full control** e **Read**:

`winrm configsddl wmi`

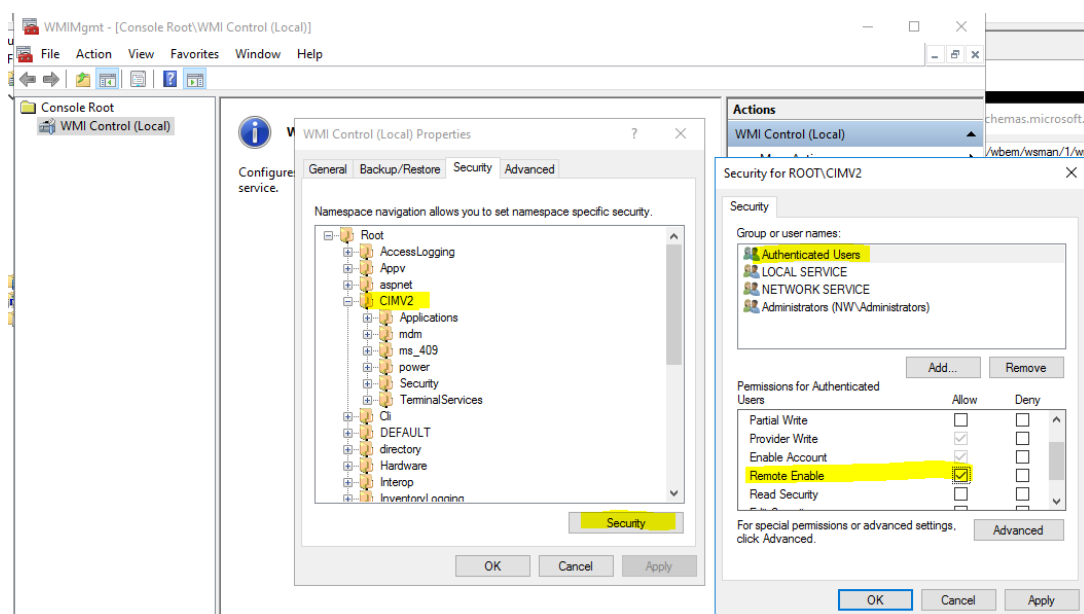
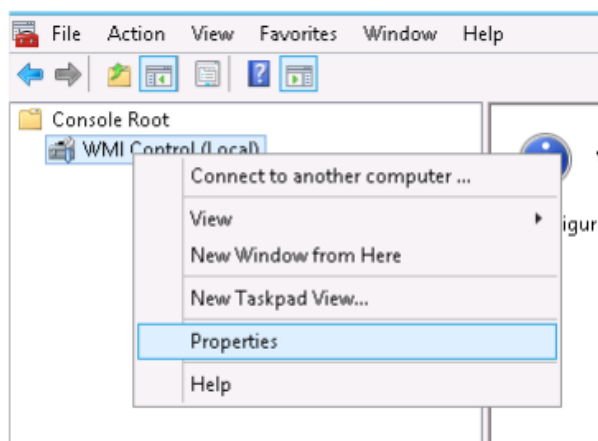
Na janela que é aberta dê **permissão Full Control** e **Read** para a conta de serviço que foi criada na seção 6.3 deste guia.



7.6 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**).

7.7 Linkar Listener HTTP ao Usuário

Nota: Este procedimento deve ser realizado em todos os SQL Servers que enviarão eventos.

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 -User user@domain
```

IT-PRO-008 Rev. 00	CONFIGURAÇÃO DO MSSQL PARA COLETA DE LOGS	
Classificação: Restrito		

Informe o usuário criado na seção 7.3 deste guia.

```
PS C:\Users\Administrator\Desktop> .\winrmconfig.ps1 -Action enable -ListenerType http -User rsa@contoso.local]
winrmconfig script version 1.17
More verbose logging can be found in C:\Users\ADMINI-1\AppData\Local\Temp\2\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

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="GP0"] Address = * Transport = HTTP Port = 5985 Hostname Enabled = true URLPr
efix = wsman CertificateThumbprint ListeningOn = 10.101.13.251, 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 rsa@contoso.local] with SID S-1-5-21-4190919838-2717515234-3068202919-1105 is already
added to the WinRM WMI Plugin SDDL (Security analytics can resolve SIDs with this account)

Checking access to the CIM Root (necessary for Event log collection)
User rsa@contoso.local] with SID: S-1-5-21-4190919838-2717515234-3068202919-1105 is already enabled
for WMI access via WinRM (Security Analytics can collect Event logs using this account)

Checking user rsa@contoso.local] membership to the Event Log Readers group
User rsa@contoso.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.
PS C:\Users\Administrator\Desktop>
```


7.8 Report Mode

Nota: Este procedimento deve ser realizado em todos os *SQL Server* que enviarão eventos.

Passo 1: No mesmo local do passo 1 da seção 7.7, execute o comando abaixo:

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

Verifique se houve algum erro, salve a saída deste comando (*print* de tela) em boa resolução.

IT-PRO-008 Rev. 00	CONFIGURAÇÃO DO MSSQL PARA COLETA DE LOGS	
Classificação: Restrito		

```

PS C:\Users\administrator.CONTOSO\Desktop> .\winrmconfig.ps1 -Action Report -User rsa@contoso.local
winrmconfig script version 1.17
More verbose logging can be found in C:\Users\ADMINI~1\CON\AppData\Local\Temp\2\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

CURRENT LISTENER(S) INFORMATION:
Listener: [Source="GP0"] Address = * Transport = HTTP Port = 5985 Hostname Enabled = true URLPr
efix = wsman CertificateThumbprint ListeningOn = 127.0.0.1, 198.18.0.244

Since an HTTP Listener exists then checking the Allow unencrypted setting for the HTTP Listener, which if not set would
cause collection to fail.
SECURITY LOG ACCESS FOR NETWORK SERVICE ACCOUNT CHECK BEGINS(WINRM SERVICE USES THIS ACCOUNT TO READ EVENT LOGS)
Network Service SID is already added to the Security Channel ACL (Security Analytics can collect Security Event logs usi
ng the rsa@contoso.local account)
SECURITY LOG ACCESS FOR NETWORK SERVICE ACCOUNT CHECK ENDS

COLLECTION USER RIGHTS CONFIGURATION BEGINS...

Checking access to the WinRM WMI Plugin (necessary for SID resolution)
User rsa@contoso.local with SID S-1-5-21-1939321115-3864531406-4019967091-1108 is already
added to the WinRM WMI Plugin SDDL (Security analytics can resolve SIDs with this account)

Checking access to the CIM Root (necessary for Event log collection)
User rsa@contoso.local with SID: S-1-5-21-1939321115-3864531406-4019967091-1108 is already enabled
for WMI access via WinRM (Security Analytics can collect Event logs using this account)

Checking user rsa@contoso.local membership to the Event Log Readers group
User rsa@contoso.local is already a member of Event Log Readers group

COLLECTION USER RIGHTS CHECK ENDS HERE...

```

8. REFERÊNCIAS

RSA Link. SCOTT, Marcus. **Microsoft SQL Server Event Source Configuration Guide**. 2019. Disponível em: <<https://community.rsa.com/docs/DOC-40241>> Acesso nov 2019.