How to enable WMI on Windows Server.

In this articole we describe how to enable WMI on Windows Server.

Step 1. Create an user on Windows Server.

To configure WMI on your device so that NMIS can discover and monitor it, you must create a user who has access to WMI objects on the device.

- 1.- Go to Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups.
- 2.- Right-click Users and select New User.
- 3.- Create a user. Example: nmiswmi



Note: Windows allows certain WMI classes to be pulled only via Administrator account.

- 4.- Select this user (nmiswmi) and right-click to select Properties > Member of tab.
- 5.- Select Distributed COM Users and click Add.

		Propie	edades: nmi	swmi	? X
Control remote)	Perfil de S	Servicios de Esci	ritorio remoto	Marcado
General	М	iembro de	Perfil	Entorno	Sesiones
Miembro de:					
Lusuarios (COM	distribuidos			
Agregar		Quitar	Cualquier camb de usuarios no usuario inicie se	io en la perteneno surtirá efecto hast esión de nuevo.	cia a grupos ta que el
		Aceptar	Cancelar	Aplicar	Ayuda

6.- Click OK to save.

Step 2. Check required DCOM and WMI services for Windows.

The following services must be started and configure for automatic startup:

- Server
- Remote RegistryWindows Management Instrumentation
- 1.- Open the Run menu, press the following logo key + R.

2.- Type the following: services.msc



4.- In the details pane, verify these services are started and set to automatic startup:

- ServerRemote Registry
- Windows Management Instrumentation

9		Servicios			Ŀ	- 🗆 X
Archivo Acción V	/er Ayuda					
I I I I I I I I I I I I I I I I I I I	🗟 🔽 📷 🕨 🔳 🕪					
Servicios (locales)	Servicios (locales)					
	Administración remota de Window (WS-Management)	WMI es	Descripción Proporciona Procesa las s	Estado	Tipo de inicio Manual Manual	Iniciar sesić ∧ Sistema loc Sistema loc ≡
	<u>Detener</u> el servicio <u>Reiniciar</u> el servicio	Imacenamiento s y claves de manteni	Optimiza la Proporciona		Manual Manual	Sistema loc Sistema loc
	Descripción: El servicio Administración remota de Windows (WinRM) implementa el protocolo WS-Management para la administración remota. WS-Management es un protocolo estándar de servicios web usado para la administración remota de software y hardware. El servicio WinRM escucha solicitudes de WS- Management y las procesa en la red. Para tal fin, debe configurarse con una escucha que use la herramienta de línea de comandos winrm.cmd o a través de la directiva de grupo. El servicio WinRM ofrece acceso a los datos WMI y, si está en ejecución,	ndows (WS-Managem automáticas de acces de acceso remoto de Windows ón de dispositivos s seguridad a so a redes s sobre TCP/IP	El servicio A Crea una co Administra Toma decisi Habilita la d Proporciona El inicio de e Servicio cen El protocolo Coordina la El servicio Ai Proporciona Administra I Cora una ma	En ejecu En ejecu En ejecu En ejecu En ejecu En ejecu	Automático Manual Manual Automático (Manual (dese Manual Automático Automático (Manual (dese Automático (Automático (Automático Manual Manual	Servicio de Sistema loc Sistema loc Sistema loc Sistema loc Sistema loc Sistema loc Sistema loc Servicio de Sistema loc Servicio de Sistema loc Servicio loc Sistema loc Servicio loc Sistema loc
	suscripción a eventos. Los mensajes WinRM usan HTTP y	v ^c	Resuelve ide	En ejecu	Automático	Servicio de 🗸
< III >	Extendido Estándar					

Propiedades: Adm	inistración remota de Windows (WS 🗙
General Iniciar sesión	Recuperación Dependencias
Nombre de servicio:	WinRM
Nombre para mostrar:	Administración remota de Windows (WS-Managemen
Descripción:	El servicio Administración remota de Windows (WinRM) implementa el protocolo WS-
Ruta de acceso al eje C:\Windows\System3	cutable: 2\svchost.exe -k NetworkService
Tipo de inicio:	Automático V
Estado del servicio:	En ejecución
Iniciar	Detener Pausar Reanudar
Puede especificar los el servicio desde aquí	parámetros de inicio que se aplican cuando se inicia
Parámetros de inicio:	
	Aceptar Cancelar Aplicar

5.- To change a service property, right-click on the service name, and then click Properties.

6.- From the Startup type list box, select Automatic.

7.- If the Service status is not started, click Start.

8.- Click OK.

9.- Close the Services window.

Step 3. Enabling DCOM for Windows Server.

1.- Open the Run menu, press the Windows logo key + R.

2.-Type the following: dcomcnfg

	Ejecutar	x
	Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea abrir con Windows.	
A <u>b</u> rir:	dcomcnfg	~
	Esta tarea se creará con privilegios administrativos.	
	Aceptar Cancelar E <u>x</u> aminar	

- 4.- The Component Services window is displayed.
- 5.- Under Component Services, expand Computers, and then click My Computer.
- 6.- On the Action menu, click Properties.
- 7.- Select the Default Properties tab.
- 8.- Configure the following Default Properties:

Select the Enable Distributed COM on this computer check box.

Using the Default Authentication Level list box, select Connect.

Using the Default Impersonation Level list box, select Identify.

	Propied	ades: Mi PC	? X
Protocolos pre	determinados	Seguridad COM	MSDTC
General	Opciones	Propiedades pred	eterminadas
Habilitar CON	1 distribuido en este	equipo	
Habilitar los \$	Servicios Internet C	OM en este equipo	
- Propiedades p	redeterminadas de	comunicación de COM d	istribuido ——
El nivel de aut	enticación especifi	ca la seguridad en los pa	quetes.
Nivel de aut	enticación predeter	minado:	
Canadar			
El nivel de sup determinar qui	lantación especific én las está llamand	a si las aplicaciones pued o y si la aplicación puede	den realizar
El nivel de sup determinar qui operaciones c Nivel de sup	lantación especific én las está llamand on la identidad del lantación predetem	a si las aplicaciones pued o y si la aplicación puede cliente. ninado:	den realizar
El nivel de sup determinar qui operaciones c Nivel de sup Identificar	elantación especific én las está llamand on la identidad del elantación predetem	a si las aplicaciones pued o y si la aplicación puede cliente. ninado:	den realizar
El nivel de sup determinar qui operaciones c Nivel de sup Identificar Es posible pro referencia si si predeterminad	elantación especific én las está llamand on la identidad del lantación predetem porcionar un sistem e usa la autenticaci o no es anónimo.	a si las aplicaciones pued o y si la aplicación puede cliente. ninado: v a de seguridad para el se ón y el nivel de suplantac ional para seguimiento de	den realizar guimiento de ción
El nivel de sup determinar qui operaciones c Nivel de sup Identificar Es posible pro referencia si s predeterminad	elantación especific én las está llamand on la identidad del lantación predetem porcionar un sistem e usa la autenticaci o no es anónimo. onar seguridad adic	a si las aplicaciones pued o y si la aplicación puede cliente. ninado: v a de seguridad para el se ón y el nivel de suplantad ional para seguimiento de cómo <u>configurar estas p</u>	den realizar eguimiento de ción e referencia

Note: The system displays a message about changing the DCOM Machine wide settings. Click Yes to continue.

۹	Servicios de componentes	L
 Archivo Acción Ver Ventana 	Propiedades: Mi PC ? X]
 Raíz de consola N A Servicios de componentes A ☐ Equipos ▷ ▲ Mi PC ▷ ▲ Visor de eventos (local) ▷ ④ Servicios (locales) 	Protocolos predeterminados Seguridad COM MSDTC General Opciones Propiedades predeterminadas ✓ Habilitar COM distribuido en este equipo ☐ Habilitar los Servicios Internet COM en este equipo Propiedades predeterminadas de comunicación de COM distribuido ☐ nivel de autenticación específica la seguridad en los paquetes.	Acciones Mi PC Acciones ad
Co Va a modi afectará a funcionen	nfiguración de DCOM a nivel de equipo X ficar la configuración de DCOM a nivel de equipo. Esto todas las aplicaciones del equipo y es posible que algunas no correctamente. ¿Desea actualizar la configuración de DCOM?	
	Sí No predeterminado no es anónimo. Proporcionar seguridad adicional para seguimiento de referencia Obtener más información acerca de cómo configurar estas propiedades. Aceptar Cancelar	

Step 4. Configuring DCOM communication for Windows Server.

1.- From the DCOM Configuration (dcomcnfg) window, expand Component Services, expand Computers, and select My Computer.

	Ejecutar	x
	Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea abrir con Windows.	
A <u>b</u> rir:	dcomcnfg v]
	🛞 Esta tarea se creará con privilegios administrativos.	
	Aceptar Cancelar E <u>x</u> aminar]

- 2.- On the Action menu, click Properties.
- 3.- Select the Default Protocols tab.
- 4.- Configure the following options:

 - If Connection-oriented TCP/IP is listed in the DCOM Protocols window, go to Step 5.
 If Connection-oriented TCP/IP is not listed in the DCOM Protocol window, select Add.
 From the Protocol Sequence list box, select Connection-oriented TCP/IP.



Step 5. Configuring Windows Server user accounts for DCOM.

You must select an existing account with administrative access or create a normal user account that is a member of an administrative group to access the host.

1.- From the DCOM Configuration (dcomcnfg) window, expand Component Services, expand Computers, and select My Computer.

2.- On the Action menu, click Properties.

3.- Select the COM Security tab.

4.- In Access Permissions, click Edit Default.



5.- Select the user (nmiswmi) or group requiring DCOM access.

Note: If the user or group requiring DCOM access is not listed in the permissions list, you must add the user to the configuration.

6.- Configure the following user permissions:

- Local Access Select the Allow check box.
- Remote Access Select the Allow check box.

Anthen Anthen Martin Martine Ande	
😁 Archivo Acción ver Ventana Ayuda	
← → 2 I Propiedades: Mi PC ? ×	
Aaiz de consola Permisos de acceso Image: Consola Image: Consola <td< td=""><td>Accior Mi P(A</td></td<>	Accior Mi P(A

8.- In Launch and Activation Permissions, click Edit Default.



9.- Select the user or group requiring DCOM access.

Note: If the user or group requiring DCOM access is not in the permissions list, you must add the user to the configuration.

10.- Configure the following user permissions:

- Local Launch Select the Allow check box.
- Remote Launch Select the Allow check box.
- Local Activation Select the Allow check box.
- Remote Activation Select the Allow check box.



12.- Click OK to close the Component Services window.

Step 6. Configuring Windows Server Firewall.

1.- Open the Run menu, press the Windows logo key + R.

2.- Type the following: wf.msc.

	Ejecutar
	Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea abrir con Windows.
A <u>b</u> rir:	wf.msc v
	🛞 Esta tarea se creará con privilegios administrativos.
	Aceptar Cancelar E <u>x</u> aminar

- 4.- Select Inbound Rules.
- 5.- On the Action menu, click New Rule.
- 6.- Select Custom and click Next. The Program window is displayed.



7.- Select All programs, and click Next. The Protocol and Ports window is displayed.

Archivo Acción \	/er Ayuda											
🗢 🄿 🙍 🖬 🗟	? 🖬											
🔗 Firewall de Windov	ws con segur	Reglas de entra	da								Acc	iones
🗱 Reglas de entra	ida	Nombre			Grup	•		Perfil	Habilitado	Acción ^	Re	glas d
📸 Reglas de salid	@			Asistente	e para nue	va regla o	de entrada				x	Nuev
Supervisión	Program	na										Filtra
	Especifique	la ruta completa y el i	nombre del a	archivo ejecuta	able del progra	ma con el qu	e coincide esta	a regla.				Filtra
	Pasos:											Filtrai
	Tipo de l	regla	¿Se	aplica esta re	gla a todos los	; programas o	a uno específ	ico?				Actua
	Program	a										Expor
	 Protocol 	o y puertos	۲	Todos los p La regla se ap	o rogramas olica a todas la	as conexione:	s en el equipo d	que coincio	den con otras			Ayud
	 Ambito Acción 			propiedades	de reglas.							
	 Perfil 		0	Esta ruta d	e acceso de	el programa	:					
	Nombre			Ejemplo:	c:\path\pro	ogram.exe				minar		
					%ProgramF	iles%\browse	r\browser.exe					
			Se	e rvicios Decifique los s	ervicios a los (ue se aplica	esta regla.		Perso	nalizar		
<							< Atrás	9	Siguiente >	Cancelar		

8.- From the Protocol type list box, select TCP and click Next.

Archivo Acción V	er Ayuda							
🗢 🄿 🞽 🖬 🗟	2 📑							
💣 Firewall de Window	/s con segur	Reglas de entrad	a					Acciones
Reglas de entra Reglas de salida	da	Nombre		Grupo 🔺	Perfil	Habilitado	Acción \land	Reglas o
keglas de segu	@		Asistente par	a nueva regla de entrada				× Nuev
Image: Supervisión	Protoco	lo y puertos						Filtraı
	Especifique	los puertos y protocolo	os a los que se aplica esta regla.					Filtra
	Danani							Filtra
	Tipo de r	regla	¿A qué puertos y protoco	olos se aplica esta regla?				Ver
	 Programa 	a						Actua
	Protocolo	o y puertos	Tino de protocolo:	ТСР				Expor
	Ambito		Número de protocolo:	6	·			Ayud
	Acción							
	Perfil		Puerto local:	Todos los puertos	~			
	Nombre							
			Durate secondari	Ejemplo: 80, 443, 5000-5010				
			Puerto remoto:	I odos los puertos	<u></u>			
				Eiemplo: 80, 443, 5000-5010				
			Configuración ICMP:	Personalia	_			
			conliguiación icimi .	Personaliz				
								1
< III				< Atrás		Siguiente >	Cancelar]

9.- Under Which remote IP addresses does this rule apply to field, select the radio button These IP addresses.

10.- Click Add.

11.- In the IP address or subnet text box, type the IP address of NMIS server.



13.- Click Next.

14.- Select Allow the connection, and click Next.

15.- Select one or more network profiles to which the rule applies and click Next.



16.- Type a name and description for the firewall rule.

Image: Supervision Reglas de entrada Nombre Supervision Nombre Especifique el nombre y la desoripción de esta regla. Pasoa: Tipo de regla Programa Protocolo y puetos Ambto WMI Firewall Rule Nombre Image: Protocolo y puetos Anoto WMI Firewall Rule Descripción (opcional): Nombre
Firewall de Windows con segur Reglas de entrada Nombre Grupo Reglas de salid Reglas de salid Supervisión Nombre Especifique el nombre y la descripción de esta regla. Pasoe: Tipo de regla Protocolo y puertos Ambto WMI Firewall Pule Descripción (opcional): Nombre
Reglas de entrada Nombre Reglas de said Reglas de said Reglas de said Supervisión Nombre Especifique el nombre y la descripción de esta regla. Pasos: Tipo de regla Protocolo y puertos Ambto Nombre: Ambto WIMI Firewall Rule Perfil Descripción (opcional):
Reglas de seigu Reglas de seigu Supervisión Nombre Especifique el nombre y la descripción de esta regla. Pasos: • Tipo de regla • Programa • Protocolo y puertos • Ambito • Ambito • Perfil • Nombre Descripción (opcional):
Nombre F Especifique el nombre y la descripción de esta regla. F Pasos: • Tipo de regla • Tipo de regla • Programa • Protocolo y puertos • Mombre: • Ambito Nombre: • Anbito WMI Firewall Rule • Perfil Descripción (opcional): • Nombre
Especifique el nombre y la descripción de esta regla. F Pasos: V • Tipo de regla V • Programa Nombre: • Arbito VMII Firewall Rule • Acción Descripción (opcional): • Nombre International (opcional):
Pasos: V • Tipo de regla V • Programa V • Protocolo y puertos Nombre: • Ambito Nombre: • Acción VMII Firewall Rule • Perfil Descripción (opcional): • Nombre Image: Control (opcional)
Pasos: v • Tipo de regla // • Programa // • Protocolo y puertos // • Ambito Nombre: • Acción WMI Firewall Rule • Perfil Descripción (opcional): • Nombre
 Tipo de regla Programa Protocolo y puertos Ambito Acción Perfil Descripción (opcional): Nombre
 Programa Protocolo y puertos Ambito Ambito Acción Perfil Descripción (opcional): Nombre
Protocolo y puertos Ambito Acción Perfil Descripción (opcional): Nombre
• Anioto WMI Firewall Rule • Acción Descripción (opcional): • Nombre Image: Control of the second se
Perfil Descripción (opcional): Nombre
Nombre
< III Cancelar Cancelar

17.- Click Finish. You can now exit the Windows Firewall with Advanced Security panel.

Step 7. Configuring WMI user access for Windows Server.

The user or group you configured for DCOM access must also have Windows Management Instrumentation (WMI) permission.

- 1.- Open the Run menu, press the Windows logo key + R.
- 2.- Type the following: wmimgmt.msc
- 3.- Click OK.



4.- Right-click on WMI Control (Local), select Properties. The WMI Control (Local) Properties window is displayed.



5.- Click the Security tab. The Namespace navigation is displayed.

6.- From the Namespace menu tree, expand Root, click CIMV2.



7.- Click the Security button the menu tree. The Security for ROOT\CIMV2 window is displayed.

roi wivii (iocai)

Instrumental de administración de Windows (WMI) 1 ? x Propiedades: Control WMI (local) Configur General Seguridad Copia de seguridad y/o restauración Opciones avanzadas La navegación de espacio de nombres le permite establecer la seguridad especifica de espacio de nombres. \sim AccessLogging E-Q CIMV2 🗄 🕛 🚺 🗄 🐌 DEFAULT im inectory 🗄 🕡 🚺 Hardware ≣ 🗄 🕖 Interop InventoryLogging 🗄 🕖 msdtc nap 🖻 🕘 RSOP E D SECURITY 🤰 ServiceModel ÷... Ė٠ StandardCimv2 Seguridad

Aceptar

Cancelar

Aplicar

8.- Select the user or group requiring WMI access.

Note: If the user or group requiring WMI access is not listed in the permissions list, you must add the user to the configuration.

9.- Select the check boxes to add the following permissions:

- Execute Methods Select the Allow check box.
- Provider Write Select the Allow check box.
- Enable Account Select the Allow check box.
- Remote Enable Select the Allow check box.

🚟 Archivo Acción Ver Favo	oritos Ventana	Ayuda
🔶 🏟 🞽 📰 🗐 🚺		
Archivo Acción Ver Favo Archivo Acción Ver Favo Raíz de consola Control WMI (local)	vritos Ventana	Ayuda trumental de administración de Windows (WMI) Propiedades: Control WMI (local) Copia de seguridad y/o restauración General Copia de seguridad y/o restauración Seguridad Copia de seguridad y/o restauración Seguridad para ROOT\CIMV2 Seguridad Nombres de grupos o usuarios: Seguridad Nombres de grupos o usuarios: Seguridad Servicio de red Servicio de red Administradores (WIN-SJLNF25QVLF\Administradores)
		Administradores (WIN-SJLNF25QVLF\Administradores) Agregar Quitar Permisos de nmiswmi Permitir Denegar Ejecutar métodos Escritura completa Escritura parcial Escritura de proveedor Habilitar cuenta Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas. Aceptar Cancelar

Note: If the user or group you are configuring is a system administrator, the allow permission check boxes might be selected as the permissions are inherited.

10.- Click OK.

11.- Close the WMIMGMT - WMI Control (Local) window.

Step 8. Configuring DCOM access for Windows Server.

1.- Open the Run menu, press the Windows logo key + R.

2.- Type the following command to open the registry editor: regedit

	Ejecutar		
	Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea abrir con Windows.		
A <u>b</u> rir:	regedit	•	
	Esta tarea se creará con privilegios administrativos.		
	Aceptar Cancelar E <u>x</u> aminar		

Note: You must be a system administrator to edit registry settings.

4.- Locate the following registry location: HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

5.- Right-click the entry {76A64158-CB41-11D1-8B02-00600806D9B6}, then click Permissions.

🔊 Ec	litor del Registro
Archivo Edición Ver Favoritos Ayuda	
Archivo Edición Ver Favoritos Ayuda > - {75587F04-6EFF-443e-BED5-6371172996 > - {756c119d-9124-4693-80d8-2c1e49afab > - {756c119d-9124-4693-80d8-2c1e49afab > - {75718C9A-F029-11D1-A1AC-00C04FB6 > - {75847177-f077-4171-bd2c-a6bb2164fb > - {75599EBA-0679-3D43-BDC4-02E4D6371 > - {7559378A-7E89-11d2-B116-00805FC73 > - {75fG17E9-423B-483F-8A2E-AA2CADAc > - {7658F2A2-0A83-11d2-A484-00C04F8EF > - {7669CAD6-BDEC-11D1-A6A0-00C04F8 > - {7668F2AE-D650-11d1-9811-00C04FC31	Permisos de {76A64158-CB41-11D1-8B02-00 Seguridad Nombres de grupos o usuarios: TODOS LOS PAQUETES DE APLICACIONES SYSTEM Administradores (WIN-SJLNF25QVLF\Administradores) Usuarios (WIN-SJLNF25QVLF\Usuarios) TrustedInstaller
>	Agregar Cuttar Permisos de TODOS LOS Permitir PAQUETES DE APLICACIONES Permitir Control total

6.- Click the Advanced button. The Advanced Security Settings are displayed.

Archivo Edición Ver Favoritos Ayuda	
{75587F04-6EFF-443e-BED5-6371172996 ~	
{756c119d-9124-4693-80d8-2c1e49afab	Permisos de {76A64158-CB41-11D1-8B02-00
{75718C9A-F029-11D1-A1AC-00C04FB6	
▷ -]]] {75847177-f077-4171-bd2c-a6bb2164fb	Segundad
{7584c670-2274-4efb-b00b-d6aaba6d38	Nombres de grupos o usuarios:
{75999EBA-0679-3D43-BDC4-02E4D637	TODOS LOS PAQUETES DE APLICACIONES
{75C9378A-7E89-11d2-B116-00805FC73	& SYSTEM
{75dff2b7-6936-4c06-a8bb-676a7b00b2	& Administradores (WIN-SJLNF25QVLF\Administradores)
{75FC37F9-423B-483F-8A2E-AA2CADA4	& Usuarios (WIN-SJLNF25QVLF\Usuarios)
7658F2A2-0A83-11d2-A484-00C04F8EF	A TrustedInstaller
7669CAD6-BDEC-11D1-A6A0-00C04FB	
766BF2AE-D650-11d1-9811-00C04FC31	Agregar Quitar
76765b11-3f95-4af2-ac9d-ea55d8994f1	Permisos de TODOS LOS
767EE1f6-2006-43EA-8278-90B37AC8FI	PAQUETES DE APLICACIONES Permitir Denegar
769B8B68-64F7-3B61-B744-160A9FCC3	Control total
⊿ 3 {76A64158-CB41-11D1-8B02-00600806D	Leer 🔽
InProcServer32	Permisos especiales
]] ProgID	
Programmable	
TypeLib	
Version	Para especificar permisos especiales o Opciones avanzadas
VersionIndependentProgID	en Opciones avanzadas.
76be8257-c4c0-4d37-90c0-a23372254d	
	Aceptar Cancelar Aplicar
Equipo\HKEY_CLASSES_KOUT\CLSID\{/0A04158-CB41-11D1	

7.- In the Owner field, click Change.

B	Config	uración de seguridad ava	nzada para {76A6	54158-CB41-11D1-8B02	-00600806D9B6}		X
Pro	pietario:	TrustedInstaller Cambia	r				
Р	ermisos	Auditoría Acceso efe	ctivo				
Para entr Entr	a obtener rada y hag radas de p	información adicional, haga dol Ja clic en Editar (si está disponibl Jermiso:	ole clic en una entrada e).	a de permiso. Para modificar u	una entrada de permiso, s	eleccione l	la
	Тіро	Entidad de seguridad	Acceso	Heredada de	Se aplica a		
88	Perm	TrustedInstaller	Control total	Ninguno	Esta clave y sus su	bclaves	
8	Perm	SYSTEM	Leer	Ninguno	Esta clave y sus su	bclaves	
8	Perm	Administradores (WIN-SJLNF	Leer	Ninguno	Esta clave y sus su	bclaves	
8	Perm	Usuarios (WIN-SJLNF25QVLF\	Leer	Ninguno	Esta clave y sus su	bclaves	
	Perm	TODOS LOS PAQUETES DE AP.	. Leer	Ninguno	Esta clave y sus su	bclaves	
A	Agregar Habilitar	Quitar Ver					

8.- In the Enter the object name field, set the owner as Administrators.

Archivo	Edición	Ver Favoritos Ayuda		
	Þ 🆺 {	75587F04-6EFF-443e-BED5		
		Configuración	de seguridad avanzada para {76A64158-CB41-11D1-8B02-00600806D9B	36} – D X
	$\Delta \cdot \Delta \cdot \Delta \cdot \Delta \cdot \Delta \cdot \Delta$	Propietario: Tru Permisos Au	stedInstaller <u>Cambiar</u> Seleccionar Usuario o Grupo	
	Þ	Para obtener informaci	Seleccionar este tipo de objeto:	niso, seleccione la
	Þ	entrada y haga clic en	Usuario, Grupo, o Entidad de seguridad integrada Tipos de objeto	
	Þ	Entradas de permiso:	Desde esta ubicación:	
	D = D =	Tipo Entidad	WIN-SJLNF25QVLF Ubicaciones	
	Þ	Rerm Trustedl	Escriba el nombre de objeto para seleccionar (ejemplos):	sus subclaves
	⊿ •	& Perm Adminis	WIN-SJLNF25QVLF\Administradores Comprobar nombres	sus subclaves
		Rerm Usuarios		sus subclaves
		Perm TODOS	Opciones avanzadas Aceptar Cancelar	subclaves
<		Agregar Quit	ar Ver	
Equipo\H	KEY_C	Habilitar herencia		
		🗌 Reemplazar todas las	entradas de permisos de objetos secundarios por entradas de permisos heredables de este	objeto
			Aceptar Car	ncelar Aplicar

10.- In the Permissions entries field, select your user and click Edit.

11.- Configure the following parameters for your user:

In the Type field, select Allow.

In the Applies to field, select This key and subkeys.

In the Basic permissions field, select Full Control. By default, selecting Full Control adds Read as a permission type.

8	Entrada de p	ermiso para {76A64158-CB41-11D1-8B02-00600806D9B6}	
Entidad de seguri	dad: nmiswmi (WIN-SJLNF25QVLF\r	miswmi) Seleccionar una entidad de seguridad	
Tipo:	Permitir	~	
Se aplica a:	Esta clave y sus subclaves	~	
Permisos básicos:			Mostrar permisos avanzados
√ Ca	ontrol total		
✓ Le	er ermisos especiales		
Aplicar estos p	ermisos solo a objetos y/o contened	ores dentro de este contenedor	Borrar todo
		Act	ivar MAceptar Cancelar

12.- Click OK to return to the Advanced Security Settings window.

13.- In the Owner field, click Change.

14.- In the Enter the object name field, set the owner as your nmiswmi user.

Con	figuración de seguridad avan	zada para {76A64	4158-CB41-11D1-8B02	2-00600806D9B6} 📃 🗖 🗙
Propietario: nmiswmi (WIN-SJLNF25QVLF\nmiswmi) Cambiar				
Permiso	s Auditoría Acceso efec	tivo		
Para obtener información adicional, haga doble clic en una entrada de permiso. Para modificar una entrada de permiso, seleccione la entrada y haga clic en Editar (si está disponible). Entradas de permiso:				
Tipo	Entidad de seguridad	Acceso	Heredada de	Se aplica a
🍇 Perm	TrustedInstaller	Control total	Ninguno	Esta clave y sus subclaves
🍇 Perm	SYSTEM	Leer	Ninguno	Esta clave y sus subclaves
🍇 Perm	Administradores (WIN-SJLNF	Leer	Ninguno	Esta clave y sus subclaves
🍇 Perm	Usuarios (WIN-SJLNF25QVLF\	Leer	Ninguno	Esta clave y sus subclaves
📳 Perm	TODOS LOS PAQUETES DE AP	Leer	Ninguno	Esta clave y sus subclaves
🤱 Perm	nmiswmi (WIN-SJLNF25QVLF	Control total	Ninguno	Esta clave y sus subclaves
Agregar Quitar Editar Habilitar herencia				
Reemplazar todas las entradas de permisos de objetos secundarios por entradas de permisos heredables de este objeto				
				Aceptar Cancelar Aplicar

15.- Click OK until you return to the Registry Editor.

16.- Repeat this process for the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

💣 Ed	itor del Registro
Archivo Edición Ver Favoritos Ayuda	N Permisos de {76A64158-CB41-11D1-8B02-00
 ▷ □ ▷ (7542E960-79C7-11D1-88F9- ▷ □ ▷ (7548A939-2776-46CF-8F62- ▷ □ ▷ (756c119d-9124-4693-80d8-2 ▷ □ ▷ (75718C9A-F029-11D1-A1AC ▷ □ ▷ (75847177-f077-4171-bd2c-a ▷ □ ▷ (7584c670-2274-4efb-b00b-c ▷ □ ▷ (7599EBA-0679-3D43-BDC4 ▷ □ ▷ (75978A-7E89-11d2-B116- ▷ (759ff2b7-6926.4c66-29bb-6 	Nombres de grupos o usuarios: Inmiswmi (WIN-SJLNF25QVLF\nmiswmi) Administradores (WIN-SJLNF25QVLF\Administradores) Usuarios (WIN-SJLNF25QVLF\Usuarios) TrustedInstaller <
> 1 (7367267-9336-4606-3806-6 > 1 (75FC37F9-4238-483F-8A2E- > 1 (7658F2A2-0A83-11d2-A484- > 1 (7669CAD6-BDEC-11D1-A6A > 1 (7668F2AE-D650-11d1-9811- > 1 (76765b11-3f95-4af2-ac9d-e > 1 (767EE1f6-2006-43EA-8278-9 > 1 (769B8B68-64F7-3B61-B744-	Permisos de nmiswmi Permitir Denegar Control total Image: Control total Image: Control total Leer Image: Control total Image: Control total Permisos especiales Image: Control total Image: Control total
ImprocServer32 ProgID Programmable ImprocServer32 Programmable Equipo\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow643	Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas. Opciones avanzadas Aceptar Cancelar Aplicar

17.- Close the Registry Editor.

Step 9. Testing the WMI connection from NMIS.

1.- Create a credential file like this:

2.- Use this command to test WMI connection.

```
# /usr/local/nmis9/bin/wmic -A /tmp/credential2.txt //X.X.X.X "select Caption,Manufacturer,Model,Name from
Win32_ComputerSystem"
```

Where: X.X.X.X is the IP Address of Windows Server

Command output:

```
# /usr/local/nmis9/bin/wmic -A /tmp/credential.txt //192.168.0.105 "select Caption,Manufacturer,Model,Name from
Win32_ComputerSystem"
CLASS: Win32_ComputerSystem
Caption|Manufacturer|Model|Name
WIN-SJLNF25QVLF|VMware, Inc.|VMware Virtual Platform|WIN-SJLNF25QVLF
```