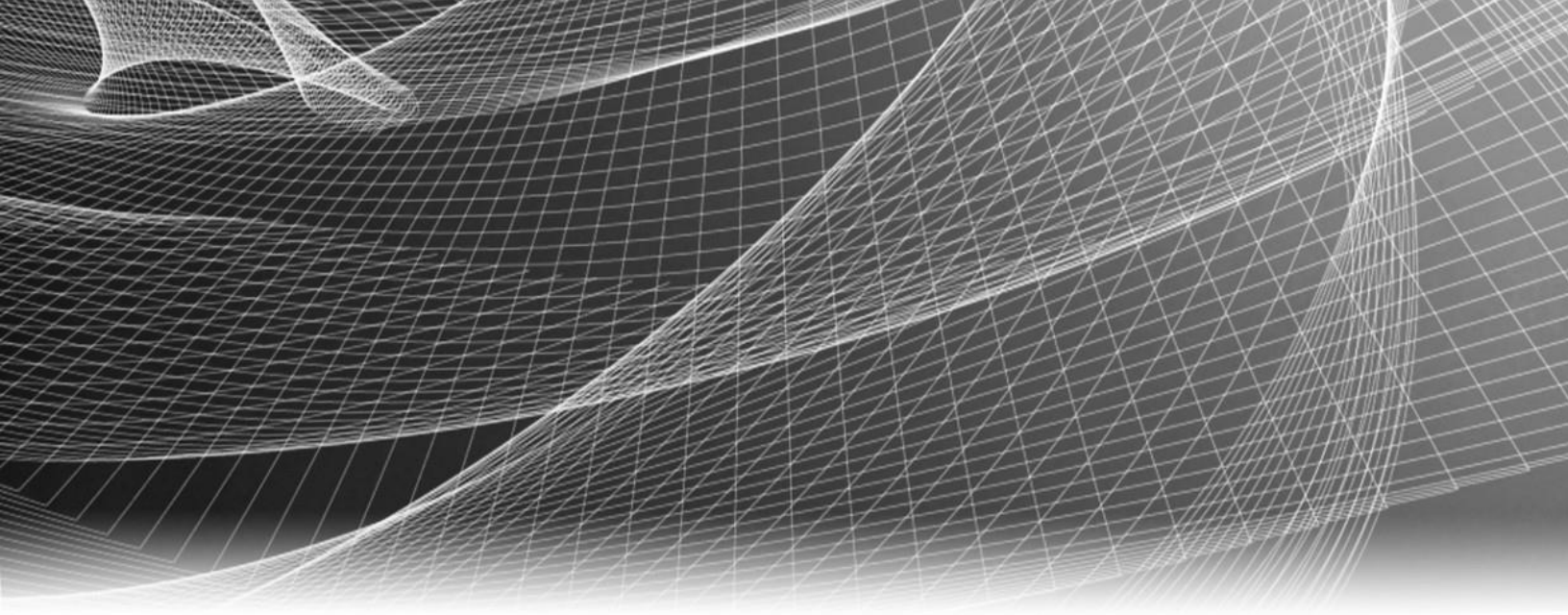


RSA Security Analytics

Actualización e instalación de la recopilación de Windows existente

RSA

EMC²

Marcas comerciales

RSA, el logotipo de RSA y EMC son marcas registradas o marcas comerciales de EMC Corporation en los Estados Unidos y en otros países. Todas las demás marcas comerciales utilizadas en este documento pertenecen a sus respectivos propietarios. Para obtener una lista de las marcas comerciales de EMC, visite mexico.emc.com/legal/emc-corporation-trademarks.htm (visite el sitio web de su país correspondiente).

Acuerdo de licencia

Este software y la documentación asociada son propiedad e información confidencial de EMC, se suministran bajo licencia, y pueden utilizarse y copiarse solamente de acuerdo con los términos de dicha licencia y con el aviso de copyright mencionado a continuación. No se puede suministrar a ninguna persona, ni poner a su disposición de cualquier otra manera, este software ni la documentación, o cualquier copia de estos elementos.
Este documento no constituye ninguna transferencia de titularidad ni propiedad del software, la documentación o cualquier derecho de propiedad intelectual. Cualquier uso o reproducción sin autorización de este software y de la documentación pueden estar sujetos a responsabilidad civil o penal. Este software está sujeto a cambios sin aviso y no debe considerarse un compromiso asumido por EMC.

Licencias de otros fabricantes

Este producto puede incluir software que ha sido desarrollado por otros fabricantes. El texto del acuerdo de licencia que se aplica al software de otros fabricantes en este producto puede encontrarse en el archivo thirdpartylicenses.pdf.

Nota sobre tecnologías de cifrado

Es posible que este producto contenga tecnologías de cifrado. Muchos países prohíben o limitan el uso, la importación o la exportación de las tecnologías de cifrado, y las regulaciones actuales de uso, importación y exportación deben cumplirse cuando se use, importe o exporte este producto.

Distribución

El uso, la copia y la distribución de cualquier software de EMC descrito en esta publicación requieren una licencia de software correspondiente. EMC considera que la información de esta publicación es precisa en el momento de su publicación. La información está sujeta a cambios sin previo aviso.

LA INFORMACIÓN DE ESTA PUBLICACIÓN SE PROPORCIONA "TAL CUAL". EMC CORPORATION NO SE HACE RESPONSABLE NI OFRECE GARANTÍA DE NINGÚN TIPO CON RESPECTO A LA INFORMACIÓN DE ESTA PUBLICACIÓN Y ESPECÍFICAMENTE RENUNCIA A TODA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O CAPACIDAD PARA UN PROPÓSITO DETERMINADO.

Instrucciones de actualización e instalación de la recopilación de Windows existente de SA 10.6

Instrucciones de actualización e instalación de la recopilación de Windows existente de SA 10.6

Descripción general

La recopilación de Windows existente de Security Analytics 10.6 recopila datos de eventos de múltiples dominios de orígenes de eventos de Windows.

Recopilación de orígenes de eventos de Windows existente compatible

Es compatible con la recopilación desde:

- Orígenes de eventos de Windows 2003 y versiones anteriores
- Archivos evt del host ONTAP de NetApp

Este apéndice contiene las siguientes secciones:

- Requisitos de configuración del colector de Windows existente de Security Analytics
- Crear un usuario de dominio no administrativo para cada dominio
- Instalar el colector de Windows existente de Security Analytics 10.6 (instalación inicial)

Última modificación: 16 de febrero de 2016, 17:03 h

Requisitos de configuración

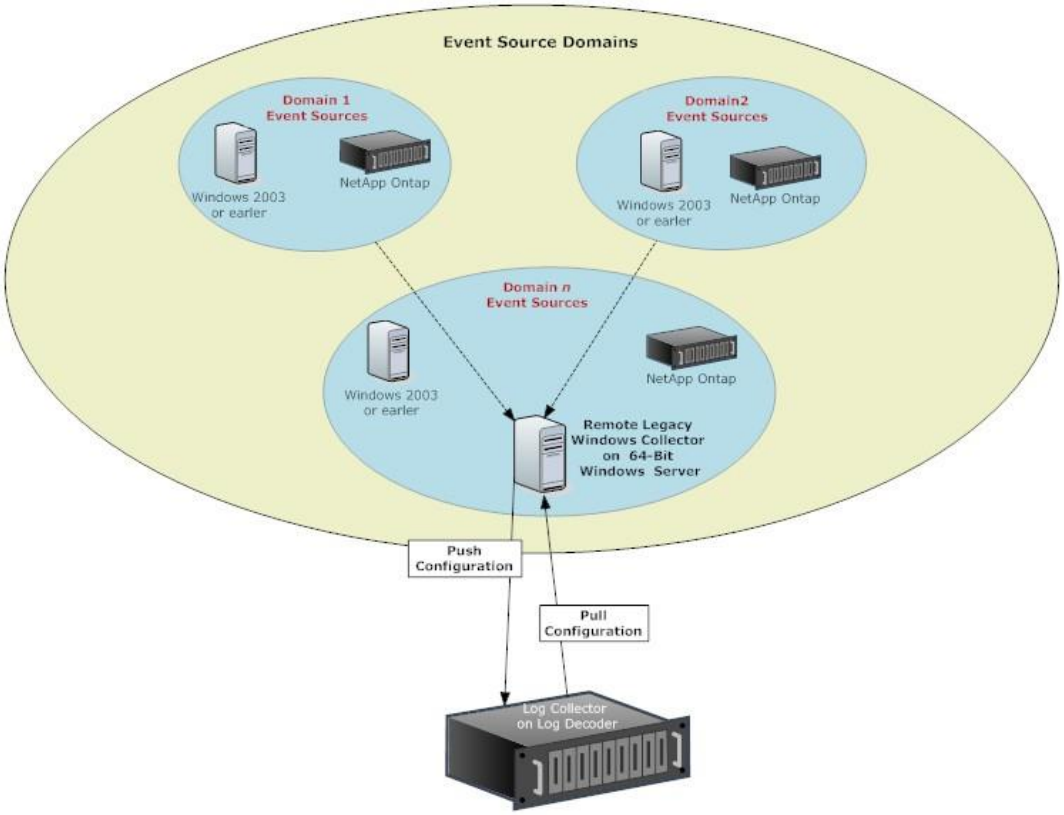
En este tema se proporcionan los requisitos de configuración del colector de Windows existente de Security Analytics.

Requisitos de configuración del colector de Windows existente de Security Analytics

Para configurar el colector de Windows existente de Security Analytics, necesita:

- Cualquier servidor físico o virtual Windows 2008 R2 SP1 de 64 bits que pueda comunicarse con los dominios del origen de eventos de Windows 2003.
- 20 % como mínimo de espacio libre en disco. Por ejemplo, necesita por lo menos 20 GB de espacio libre si la unidad del sistema tiene un tamaño de 100 GB.
- Un usuario de dominio no administrativo para cada dominio (consulte **Crear un usuario de dominio no administrativo**) que tenga acceso a los orígenes de eventos de ese dominio.

Nota: La instalación del colector de Windows existente en un controlador de dominio puede afectar el rendimiento del sistema.



Crear un usuario de dominio no administrativo para cada dominio

En este tema se proporciona una descripción general del procedimiento de configuración secuencial de punto a punto para el protocolo de recopilación de Windows existente, con una lista de verificación que contiene cada paso de configuración.

Contexto

Los pasos de configuración del protocolo de recopilación de Windows existente deben realizarse en la secuencia específica que se indica en la siguiente tabla.

Lista de verificación de la creación de un usuario de dominio no administrativo

Nota: Los pasos de esta lista aparecen en el orden en el cual se deben realizar.

Paso	Descripción	√
1	Cree un usuario de dominio no administrativo (por ejemplo, sauser) en el controlador de dominio de cada dominio.	
2	Configure la seguridad del registro de eventos en el controlador de dominio de cada dominio.	
3	(Condicional) Inhabilite el método de acceso remoto al registro.	

Nota: En la política de seguridad local de un origen de eventos de Windows 2000, debe asignar el derecho de usuario **Administrar registro de seguridad y auditoría** que otorga a un usuario no administrativo acceso al **registro de eventos**.

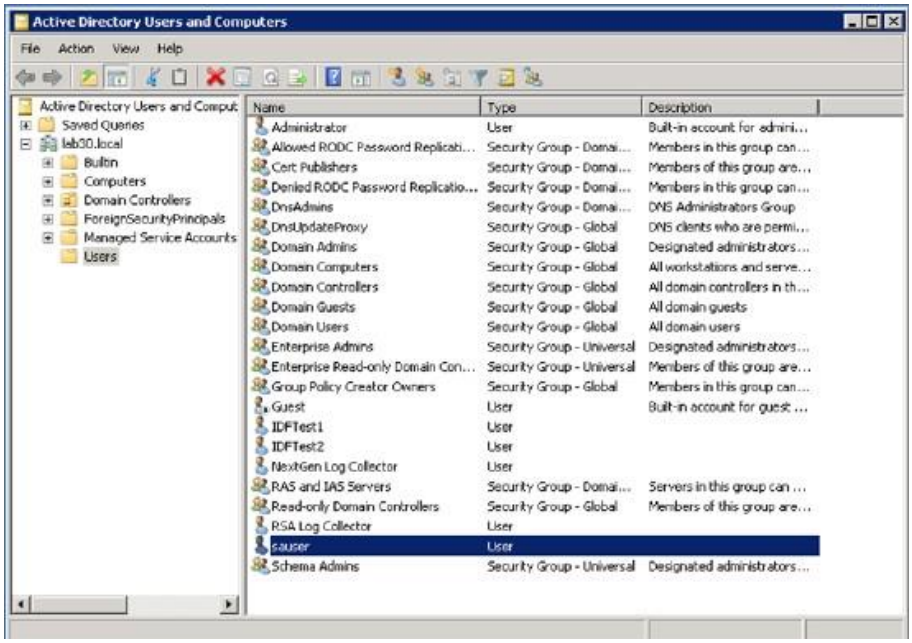
Última modificación: 2 de febrero de 2016, 9:28 h

Paso 1: Crear un usuario de dominio no administrativo

Para crear el usuario del dominio de Security Analytics (por ejemplo, **sauser**) en el controlador de dominio de cada dominio:

1. Inicie sesión en el controlador de dominio.

2. Cree un usuario de dominio no administrativo (por ejemplo, **sauser**).



3. Agregue el nuevo usuario a los grupos de usuarios del escritorio remoto.

Paso 2: Configurar la seguridad del registro de eventos

En este tema se indica cómo configurar la seguridad del registro de eventos en el controlador de dominio de un dominio.

Procedimiento

Para configurar la seguridad del registro de eventos en el controlador de dominio de un dominio:

1. Inicie sesión en el controlador de dominio.
2. Use un editor de texto como Bloc de notas para abrir **Sceregvl.inf** en la carpeta **%Windir%\Inf**.
3. Agregue las siguientes líneas a la sección **[Register Registry Values]**:

```
MACHINE\System\CurrentControlSet\Services\Eventlog\Application\
CustomSD,1,%AppCustomSD%,2 MACHINE\System\CurrentControlSet\Services\Eventlog\
Security\CustomSD,1,%SecCustomSD%,2 MACHINE\System\CurrentControlSet\Services\
Eventlog\System\CustomSD,1,%SysCustomSD%,2 MACHINE\System\CurrentControlSet\
Services\Eventlog\Directory Service\CustomSD,1,%DSCustomSD%,2 MACHINE\System\
CurrentControlSet\Services\Eventlog\DNS Server\CustomSD,1,%DNSCustomSD%,2 MACHINE\
System\CurrentControlSet\Services\Eventlog\File Replication Service\
CustomSD,1,%FRSCustomSD%,2
```

4. Agregue las siguientes líneas a la sección **[Strings]**:

```
AppCustomSD="Eventlog: Security descriptor for Application event log"
SecCustomSD="Eventlog: Security descriptor for Security event log"
SysCustomSD="Eventlog: Security descriptor for System event log"
DSCustomSD="Eventlog: Security descriptor for Directory Service event log"
DNSCustomSD="Eventlog: Security descriptor for DNS Server event log"
FRSCustomSD="Eventlog: Security descriptor for File Replication Service event log"
```

5. Guarde los cambios que hizo en el archivo **Sceregvl.inf** y ejecute el comando **regsvr32 scecli.dll**.
6. Haga clic en **Inicio** > **Herramientas del administrador** > **Administración de directivas de grupo** y complete los siguientes pasos:
   a. Expanda el árbol **Dominios**, haga clic con el botón secundario en el dominio y seleccione la opción **Crear un GPO en este dominio y vincularlo aquí**.
   b. Especifique un nombre para la política de GPO y haga clic en **Aceptar**.
   c. Seleccione la política de GPO que acaba de crear.
   d. Seleccione el dominio en el panel derecho, haga clic con el botón secundario y seleccione **Exigir**.
   e. En **Filtrado de seguridad**, haga clic en **Agregar**.
   f. En **Seleccionar usuario**, **equipo y grupo**, escriba **Equipos del dominio**, haga clic en **Comprobar nombres** y, a continuación, haga clic en **Aceptar**.

7. Haga clic con el botón secundario en la política de GPO que acaba de crear y haga clic en **Editar**.
8. Haga doble clic en las siguientes ramas para expandirlas:
   - **Configuración del equipo**
   - **Configuración de Windows**
   - **Configuración de seguridad**
   - **Políticas locales**
   - **Opciones de seguridad**
9. Busque la nueva configuración de **Eventing** en el panel derecho.

10. En el panel derecho, haga doble clic en Event log: Security descriptor for Application event log y agregue una cadena SDDL.

Nota: En los siguientes pasos, el ***SID*** (por ejemplo, `S-1-5-21-3244245077-2111152846-3233386924-1114`) es el SID de un usuario de dominio no administrativo específico (por ejemplo, **sauser**).

Si necesita recuperar el SID:

1. Ejecute el siguiente comando en PowerShell.
   Asegúrese de cambiar el nombre de usuario según corresponda (por ejemplo, cambie el nombre de usuario a **sauser**).
   ```
   ([System.Security.Principal.NTAccount]'sauser').translate([system.security.principal.securityidentifier]) | Format-List
   ```
2. Copie el campo de valor:
   ```
   BinaryLength       : 28
   AccountDomainSid   : S-1-5-21-3244245077-2111152846-3233386924
   Value              : S-1-5-21-3244245077-2111152846-3233386924-1114
   ```

Si el cuadro Configuración de la política de seguridad:

- No está vacío, agregue la siguiente cadena al valor del cuadro: `(A;; 0x1;;;SID)`.
  Por ejemplo:
  `(A;; 0x1;;;S-1-5-21-3244245077-2111152846-3233386924-1114)`
- Está vacío, inserte la siguiente cadena en el cuadro:
  `O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x7;;;SO)(A;;0x3;;;IU)(A; 0x1;;;SID.`
  Por ejemplo:
  `O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x7;;;SO)(A;;0x3;;;IU)(A; 0x1;;;S-1-5-21-3244245077-2111152846-3233386924-1114)`

11. Repita los pasos 9 y 10 para **Event log: Security descriptor for Security event log e Event log: Security descriptor for System event log**.

Paso 3 (condicional): Inhabilitar el método de acceso remoto al registro

El método de acceso remoto al registro se habilita de manera predeterminada cuando se configura un origen de eventos de Windows existente en Security Analytics. Si desea inhabilitar este método, debe deseleccionar el parámetro **Usar inicialización del registro remoto** (consulte **Configurar el acceso remoto al registro** [https://sadocs.emc.com/0_en-us/088_SA106/135_LLGds/96_LegWinPro/10_LegWinProc/10_CnfgLegWinESRec/00_CnfgRmtRgstryAcc] en la ayuda de Security Analytics para obtener información sobre este parámetro) y completar los procedimientos que se indican en este tema.

Inhabilitar el método de acceso remoto al registro

Para inhabilitar el método de acceso remoto al registro:

1. Deseleccione el parámetro **Usar inicialización del registro remoto**.
2. Agregue el usuario de Security Analytics (por ejemplo, **sauser**) a la administración de WMI y DCOMCNFG en cada origen de eventos de Windows 2003 o anterior.
3. Agregue la política de seguridad local en cada origen de eventos de Windows 2000.

Agregar un usuario de dominio no administrativo a WMI y DCOMCNFG en cada origen de eventos existente

En esta sección se presentan los pasos para agregar un usuario de dominio no administrativo a WMI y DCOMCNFG en un:

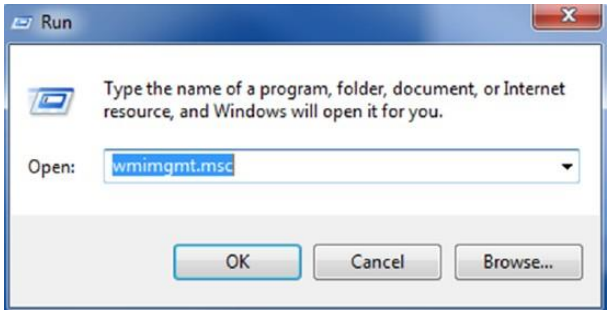
- Origen de eventos de Windows 2003
- Origen de eventos de Windows 2000

Origen de eventos de Windows 2003

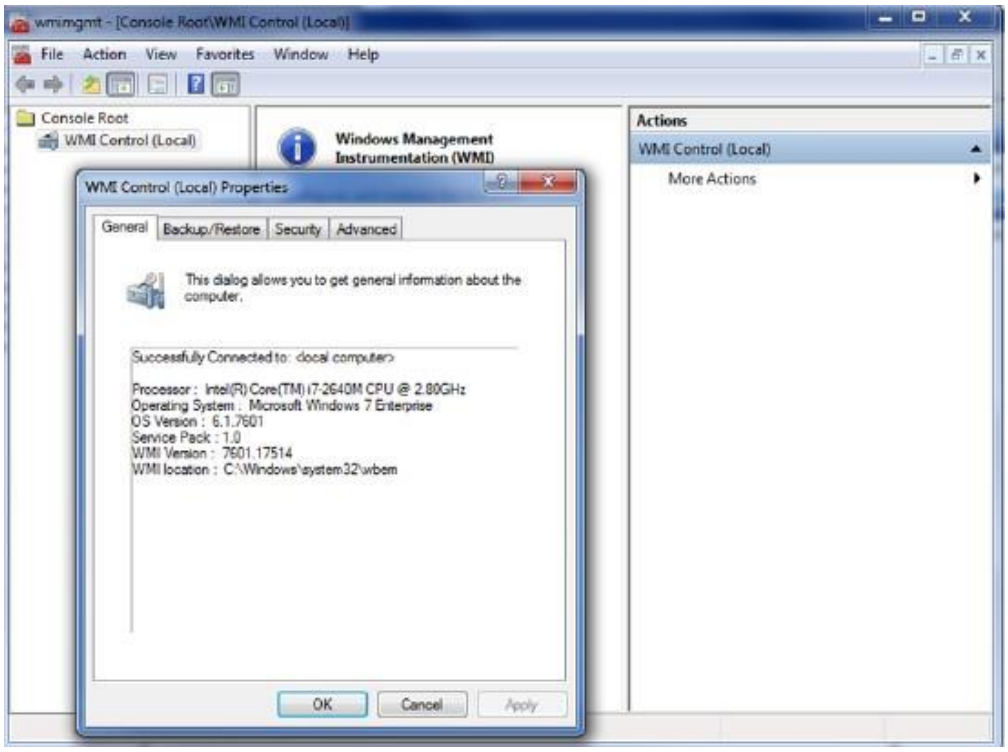
Para agregar el usuario de Security Analytics (por ejemplo, **sauser**) a la administración de WMI y DCOMCNFG en cada origen de eventos de Windows 2003 o anterior:

1. Inicie sesión en el origen de eventos.

2. Ejecute **wmimgmt.msc**.

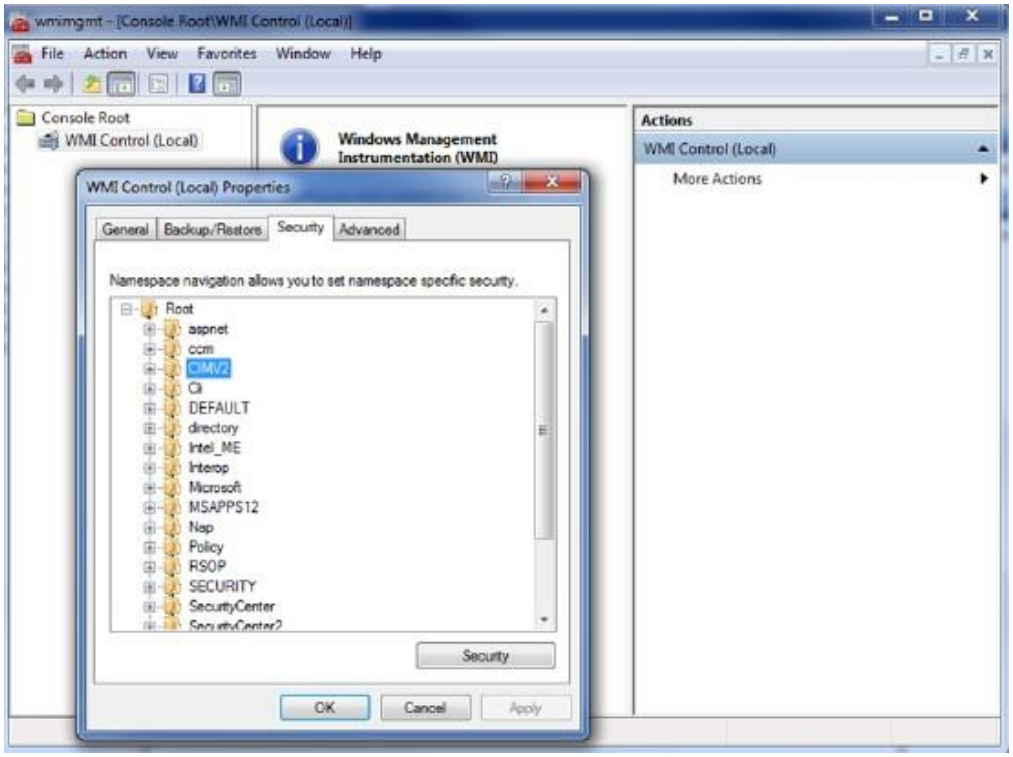


3. Agregue el usuario de Security Analytics bajo la opción de seguridad **wmi\root\CIMV2**.
   a. Haga clic con el botón secundario en **Control WMI** y, a continuación, haga clic en **Propiedades**.



   b. Haga clic en la pestaña **Seguridad** y, a continuación, haga clic en **Root\CIMV2**.

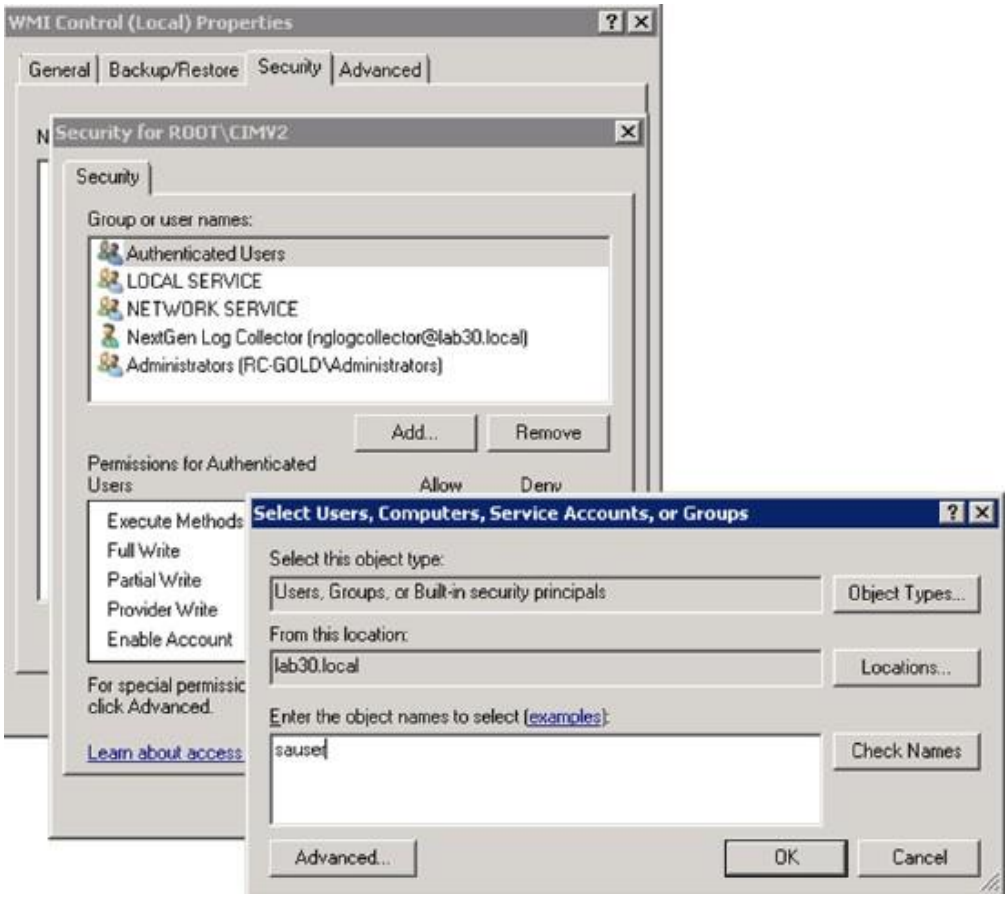
c. Haga clic en Security.

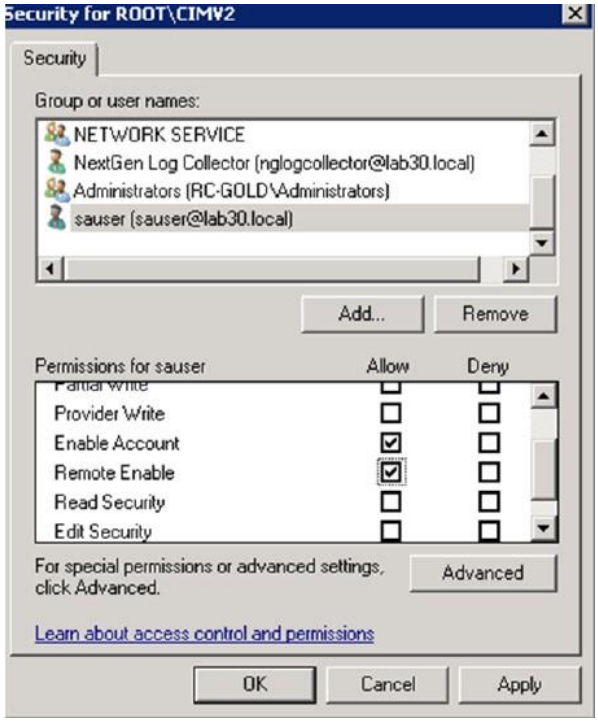


d. En la sección **Nombres de grupos o usuarios**, haga clic en **Agregar…** para crear un usuario.

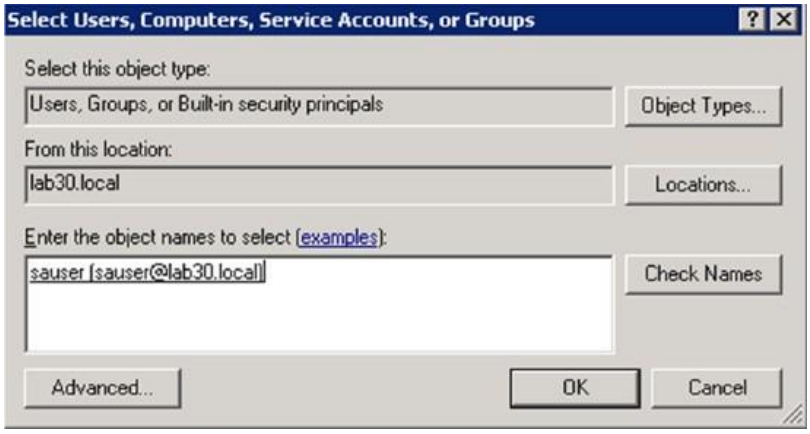
e. Seleccione los permisos **Habilitar cuenta** y **Llamada remota habilitada** para ese usuario.

f. Ingrese el usuario (por ejemplo, **sauser**).



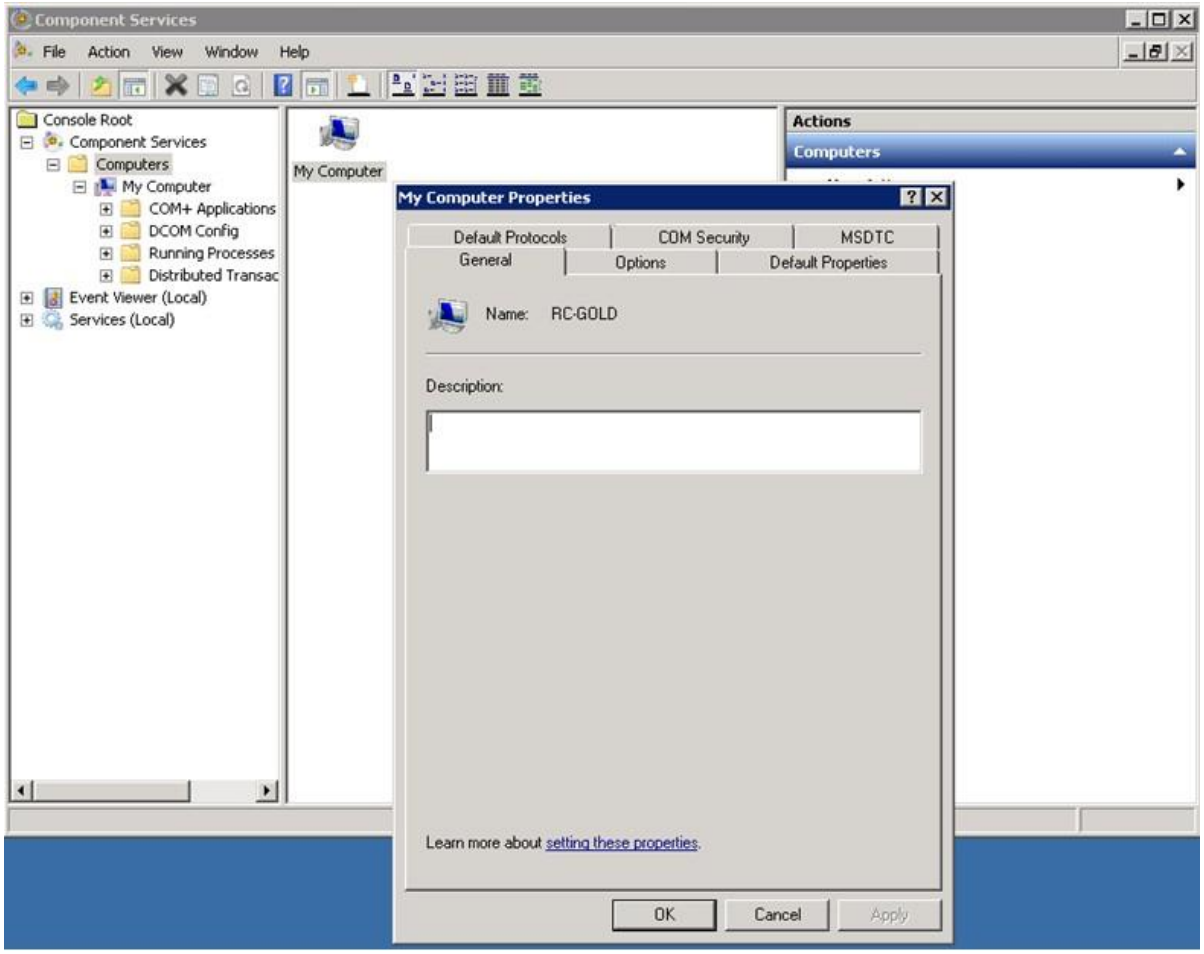


g. Haga clic en **Comprobar nombres** para verificar que el nuevo usuario se haya agregado correctamente.

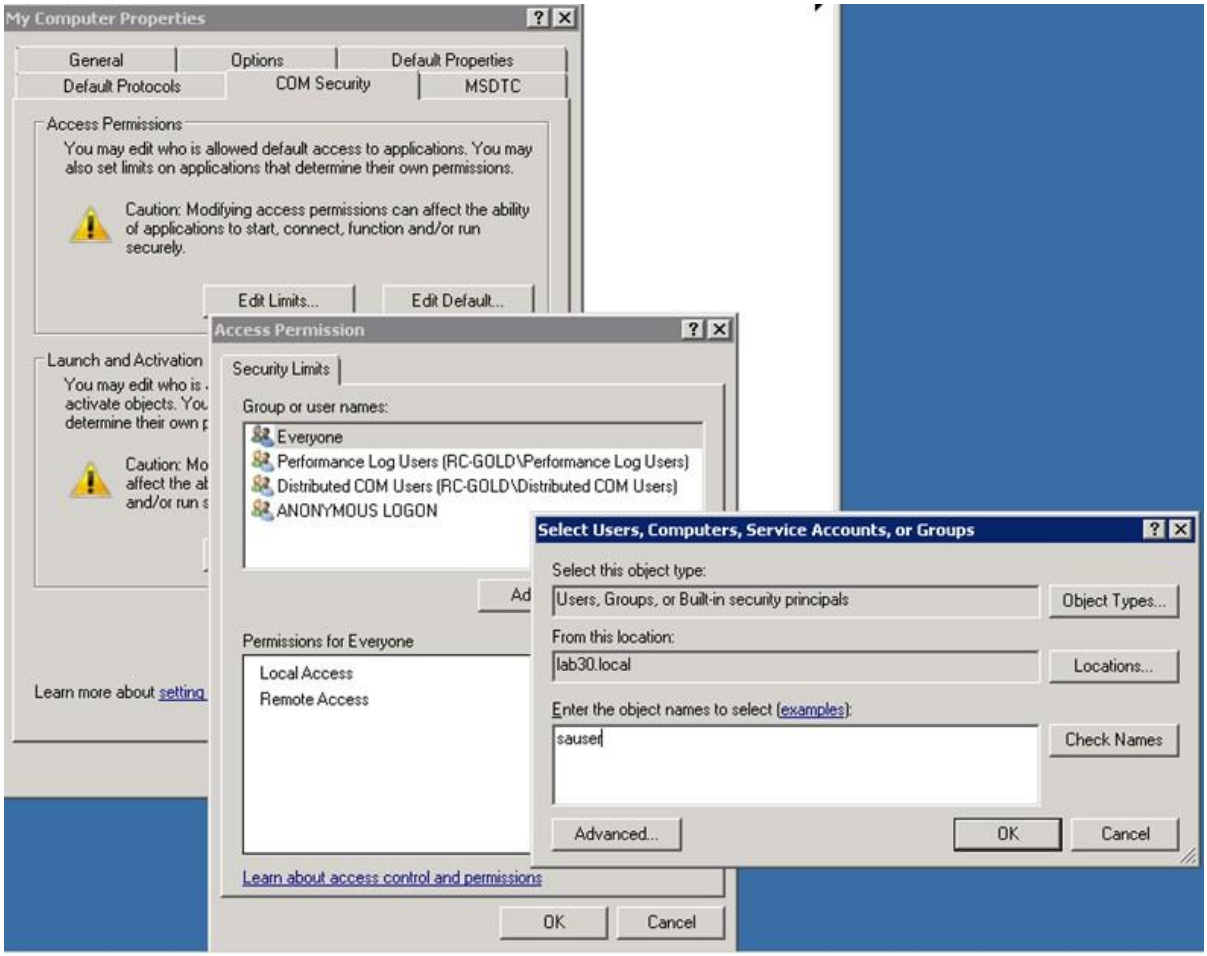


h. Haga clic en **Aplicar**, **Aceptar** y **Aceptar**.

4. Agregue un usuario bajo **DCOMCNFG**:
   a. Ejecute **dcomcnfg**.
   b. Haga clic en **Raíz de consola** > **Servicios de componentes** > **Equipos** > **Mi PC**.
   c. Haga clic con el botón secundario en **Mi PC** y haga clic en **Propiedades**.



5. En **Permisos de acceso:**
   a. Haga clic en **Editar límites**.
   b. Agregue el usuario de Security Analytics (por ejemplo, **sauser**).
   c. Habilite los permisos **Acceso local** y **Acceso remoto**.
   d. Haga clic en **Aceptar**.
6. En **Permisos de inicio y activación**:
   a. Haga clic en **Editar límites**.
   b. Agregue el usuario de Security Analytics (por ejemplo, **sauser**).
   c. Active los permisos **Ejecución local**, **Ejecución remota**, **Activación local** y **Activación remota**.
   d. Haga clic en **Aceptar** dos veces para cerrar el cuadro de propiedades.

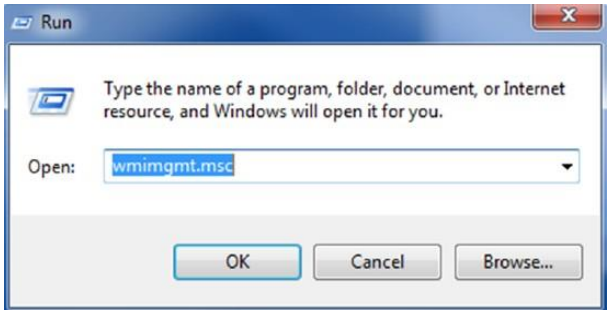


Origen de eventos de Windows 2000

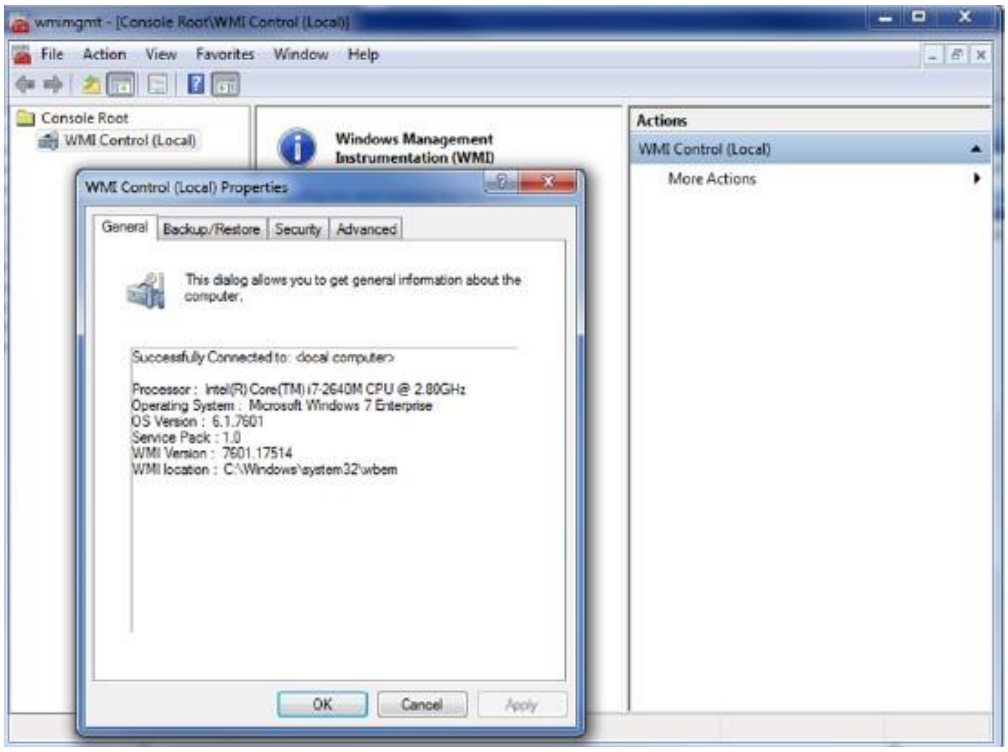
Para agregar el usuario de Security Analytics (por ejemplo, **sauser**) a la administración de WMI y DCOMCNFG en cada origen de eventos de Windows 2000:

1. Inicie sesión en el origen de eventos.

2. Ejecute **wmimgmt.msc**.

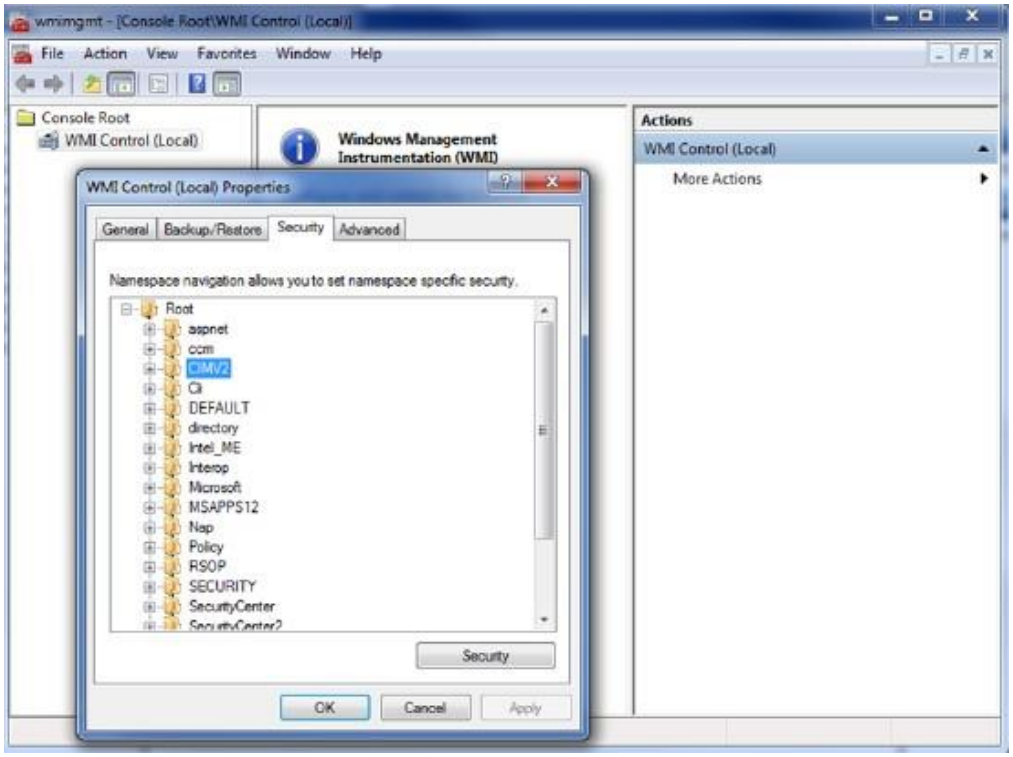


3. Agregue el usuario de Security Analytics bajo la opción de seguridad **wmi\root\CIMV2**.
   a. Haga clic con el botón secundario en **Control WMI** y, a continuación, haga clic en **Propiedades**.



   b. Haga clic en la pestaña **Seguridad** y, a continuación, haga clic en **Root\CIMV2**.

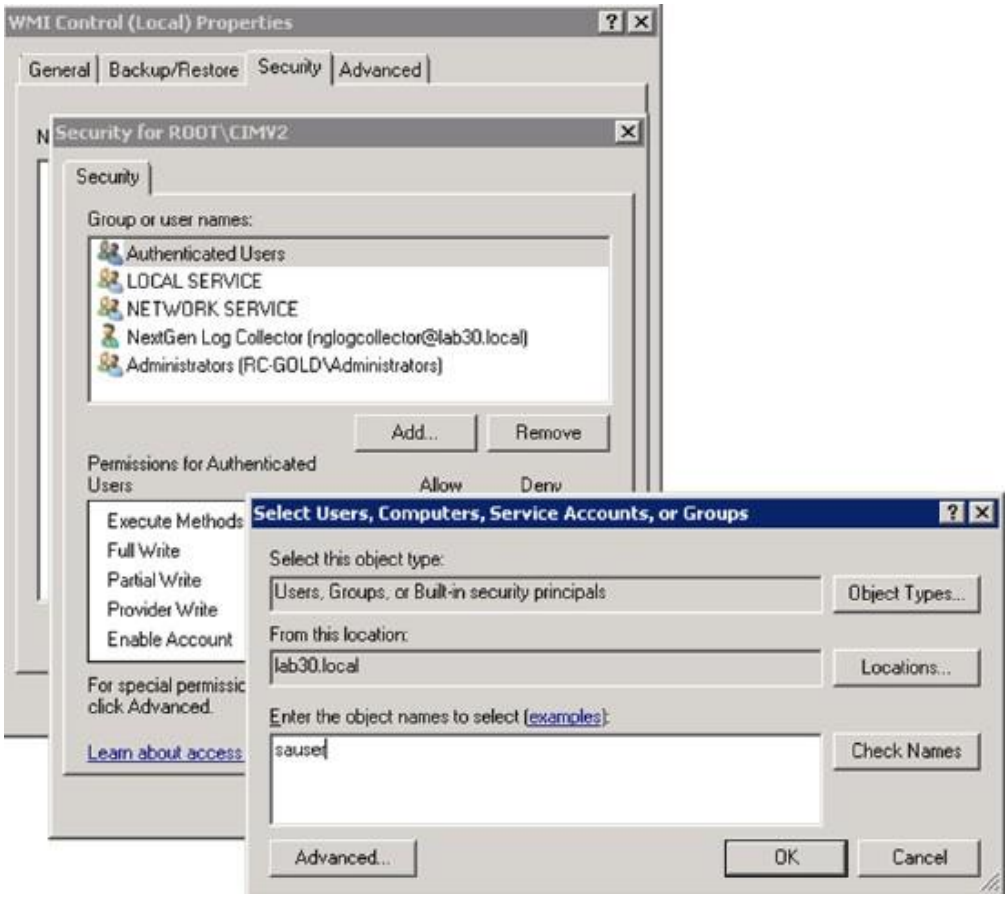
c. Haga clic en Security.

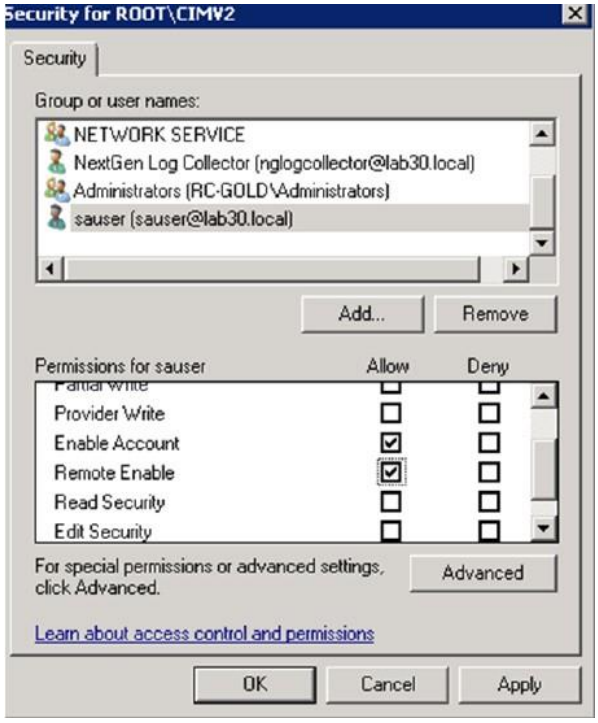


d. En la sección **Nombres de grupos o usuarios**, haga clic en **Agregar…** para crear un usuario.

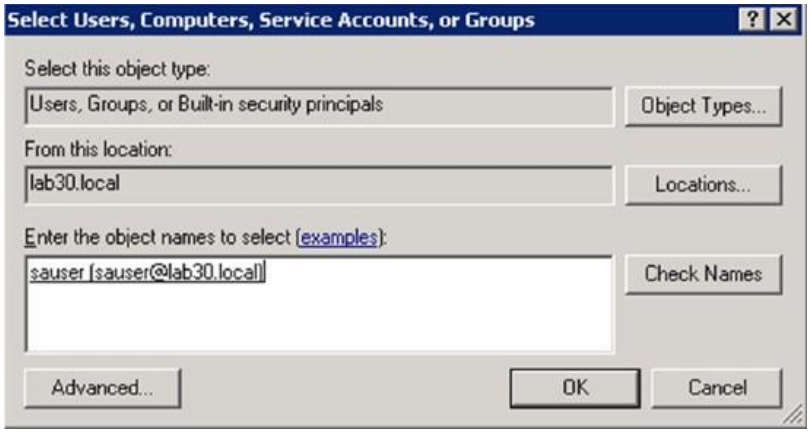
e. Seleccione los permisos **Habilitar cuenta** y **Llamada remota habilitada** para ese usuario.

f. Ingrese el usuario (por ejemplo, **sauser**).





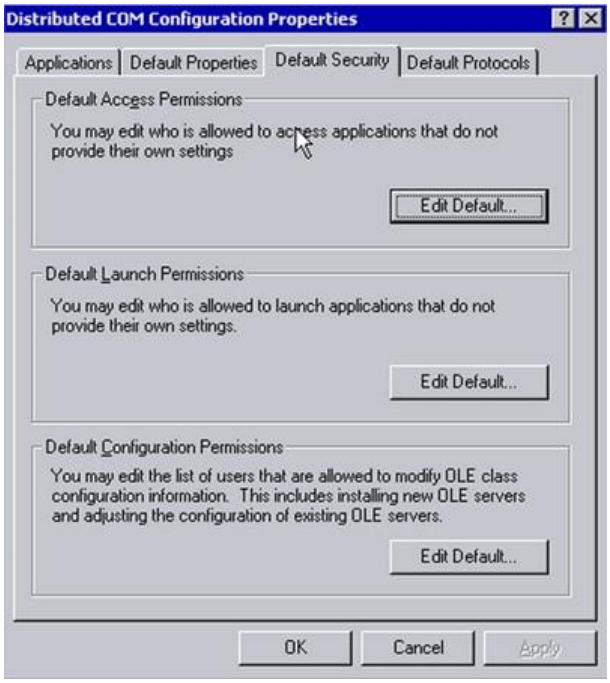
g. Haga clic en **Comprobar nombres** para verificar que el nuevo usuario se haya agregado correctamente.



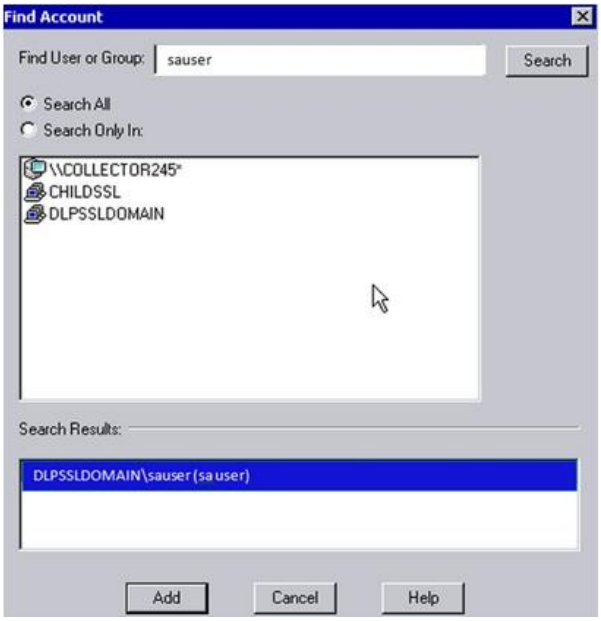
h. Haga clic en **Aplicar**, **Aceptar** y **Aceptar**.

4. Ejecute **dcomcnfg** para agregar un usuario bajo **DCOMCNFG**.

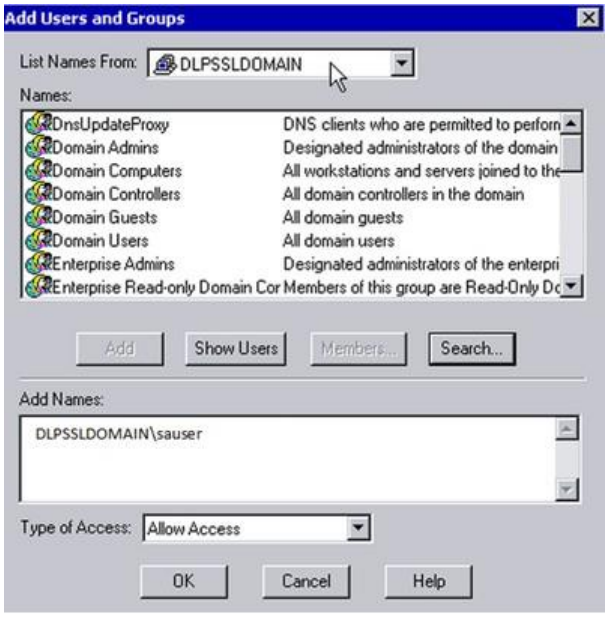
5. Seleccione la pestaña **Seguridad predeterminada**.



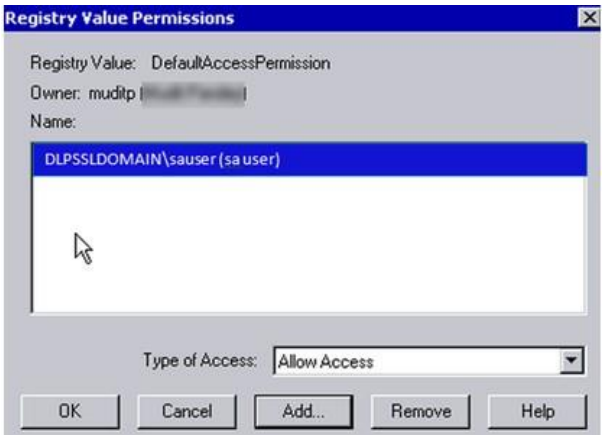
6. Haga clic en **Editar permisos**.
7. Busque **sauser**.



8. Haga clic en **Agregar**, seleccione **Permitir acceso** en la lista desplegable del campo **Tipo de acceso** y haga clic en **Aceptar**.



Se muestra la página **Permisos de valores del registro**.



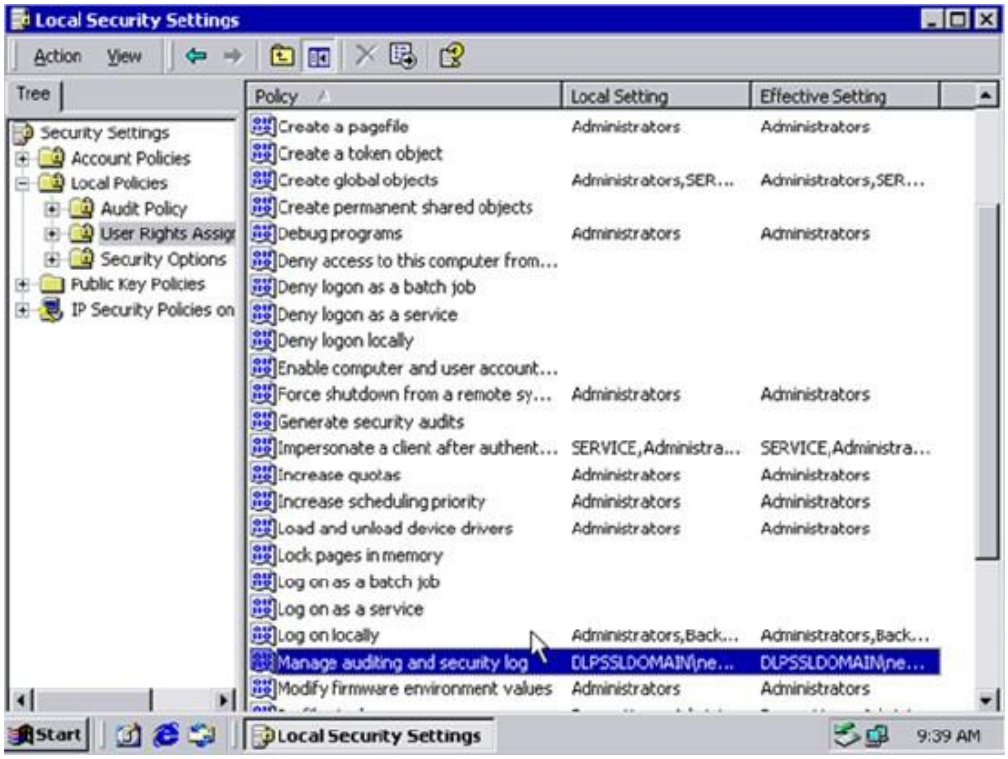
9. Haga clic en **Aceptar**.

Agregar la política de seguridad local en el origen de eventos de Windows 2000

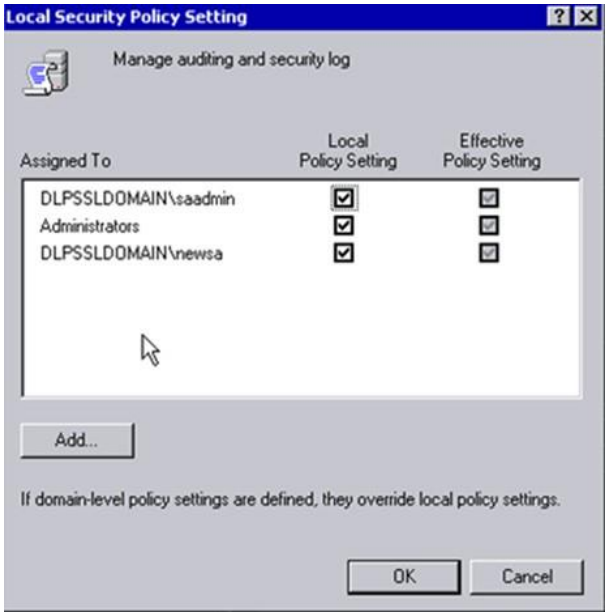
Para agregar la política de seguridad local en cada origen de eventos de Windows 2000, siga estos pasos:

1. En la línea de comandos, ejecute el comando **secpol.msc**.
   Se muestra la ventana Configuración de seguridad local.

2. En la carpeta **Directivas locales**, seleccione la carpeta **Asignación de derechos de usuario**.

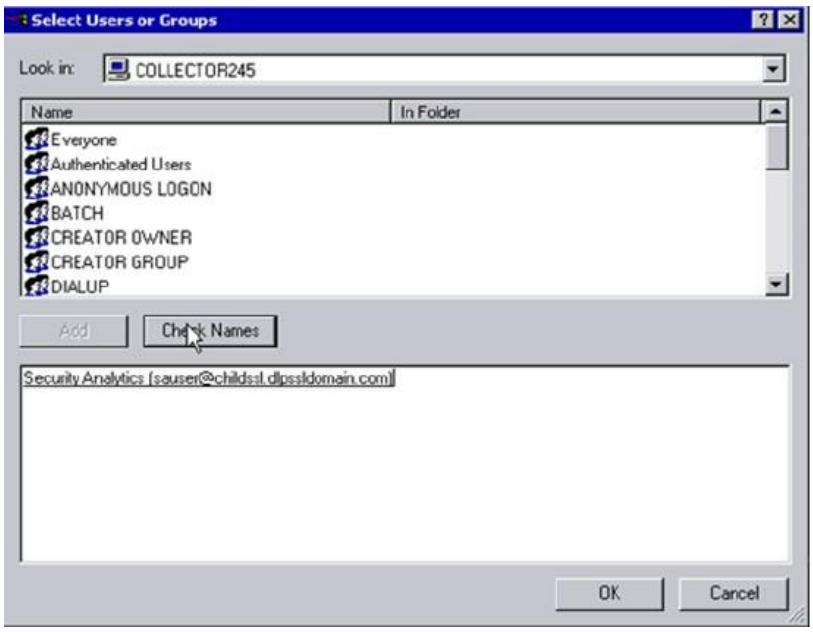


3. Seleccione **Administrar registro de seguridad y auditoría**, haga clic con el botón secundario y seleccione **Seguridad**. Se muestra el cuadro de diálogo Configuración de directiva de seguridad local.
4. Haga clic en **Agregar**.



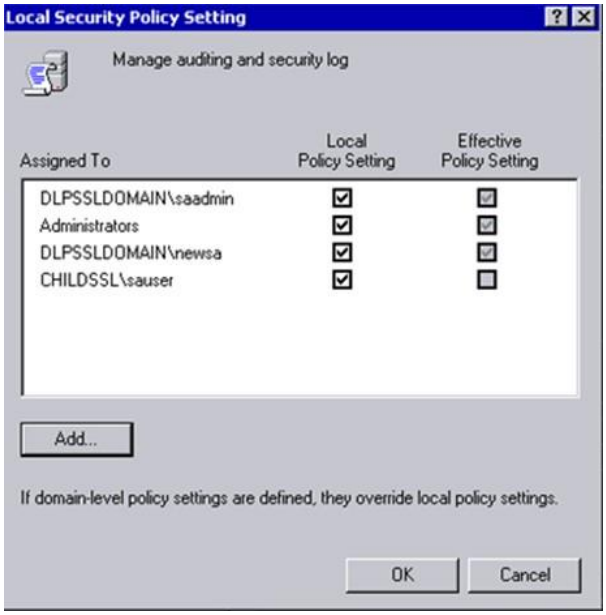
Se muestra el cuadro de diálogo Seleccionar usuarios o grupos.

5. Ingrese el nombre de usuario no administrativo [por ejemplo, **Security Analytics** (**sauser@childssl.dlpssldomain.com**) y haga clic en **Comprobar nombres**.



Se muestra el cuadro de diálogo Configuración de directiva de seguridad local.

6. Haga clic en **Aceptar** dos veces para actualizar la configuración de la política de seguridad local.



Habilitar SSL para la recopilación de Windows existente si no está habilitado

Para habilitar SSL para la recopilación de Windows existente de Security Analytics, antes de agregar el Remote Collector de la LWC a Security Analytics, realice lo siguiente:

1. Transfiera los dos archivos siguientes mediante SFTP de un host de Security Analytics al escritorio de la LWC.
   `/var/lib/puppet/ssl/certs/sa.pem`
   `/var/lib/puppet/ssl/certs/ca.pem`
2. En la LWC:
   a. Detenga el servicio Log Collector si está en ejecución.
   b. Copie `sa.pem` al directorio `/ProgramData/netwitness/ng/logcollector/trustpeers/`.
   c. Copie `ca.pem` al directorio `/ProgramData/netwitness/ng/logcollector/truststore/`.

   Nota: RSA recomienda usar la huella digital para los nombres de los archivos con el fin de asegurarse de que sean únicos (por ejemplo, los directorios `/etc/netwitness/ng/logcollector/truststore` y `/etc/ netwitness/ng/logcollector/trustpeer`).

   d. Reinicie el servicio Log Collector.
3. En Security Analytics, si no configuró el Remote Collector de Windows existente (vale decir, agregar el Remote Collector de la LWC y configurar en él la recopilación de Windows existente), siga estos pasos:

   Nota: Si configuró el Remote Collector de la LWC en Security Analytics, el servicio se muestra de color verde junto con el número de versión de la LWC.

   a. Agregue el Remote Collector de la LWC.
   b. Configure el servicio LWC en el Remote Collector.

Actualizar el colector de Windows existente de Security Analytics de 10.4.1.x-10.5.1.x a 10.6

En este tema se indica cómo actualizar el colector de Windows existente de Security Analytics 10.4.1.x-10.5.1.x a 10.6.

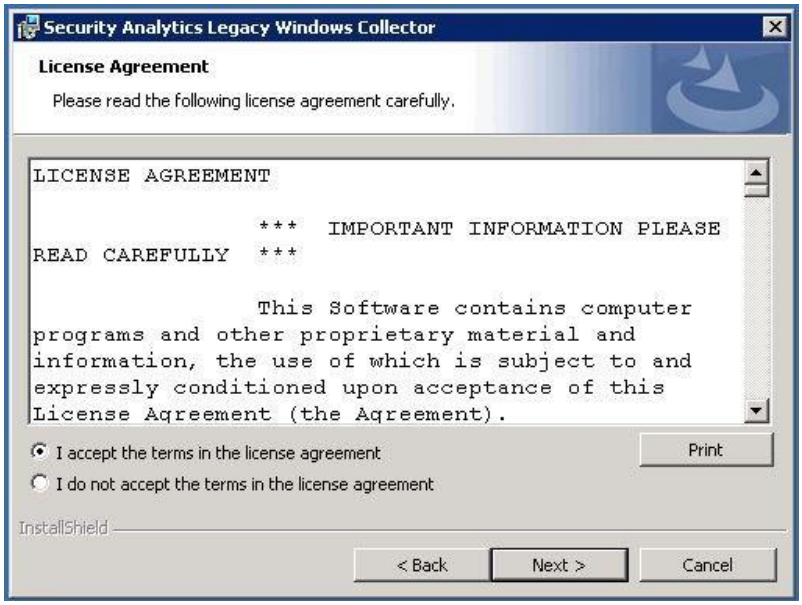
Procedimiento

Para actualizar el colector de Windows existente de Security Analytics 10.4.1.x-10.5.1.x a 10.6 en un servidor Windows 2008 R2 SP1 de 64 bits, realice lo siguiente:

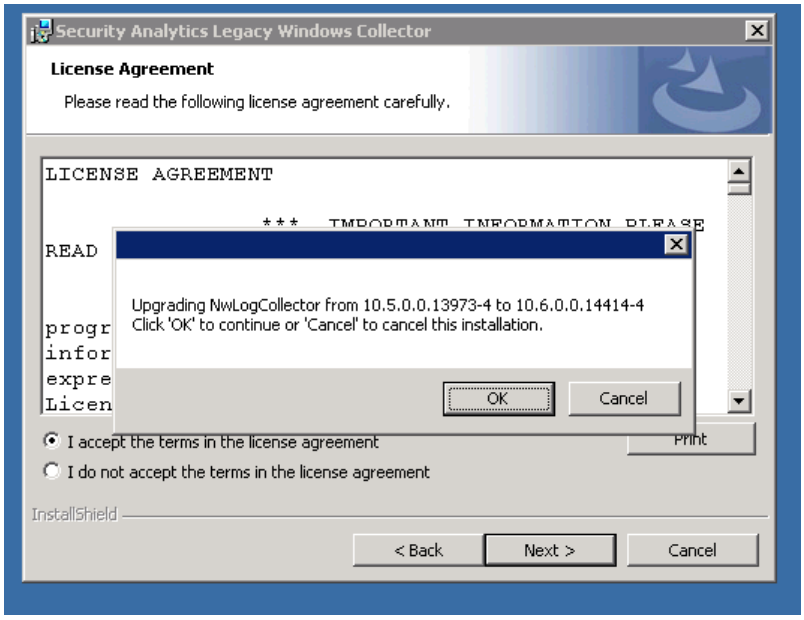
1. Busque en **SCOL** (https://auth.rsasecurity.com/) el archivo **SA-10.6.0.0-LegacyWindowsCollector.zip**, descárguelo y descomprímalo.
2. Inicie sesión en una máquina Windows 2008 con un usuario de dominio no administrativo (o un administrador local). Consulte **Crear un usuario de dominio no administrativo para cada dominio** si necesita instrucciones para crear un usuario de dominio no administrativo.
3. Copie el archivo **Security AnalyticsLegacyWindowsCollector-version-number.exe** al servidor de Windows 2008.
4. Haga clic con el botón secundario en **Security AnalyticsLegacyWindowsCollector-version-number.exe** y seleccione **Ejecutar como administrador**.
   Se muestra la página **Preparando la instalación…** del Asistente para instalación de actualizaciones.

Una vez que el programa de instalación de la actualización extrae los archivos de instalación del colector de Windows existente de Security Analytics, se muestra la página **Bienvenido…**

5. Haga clic en **Siguiente**.
   Se muestra la página Acuerdo de licencia.

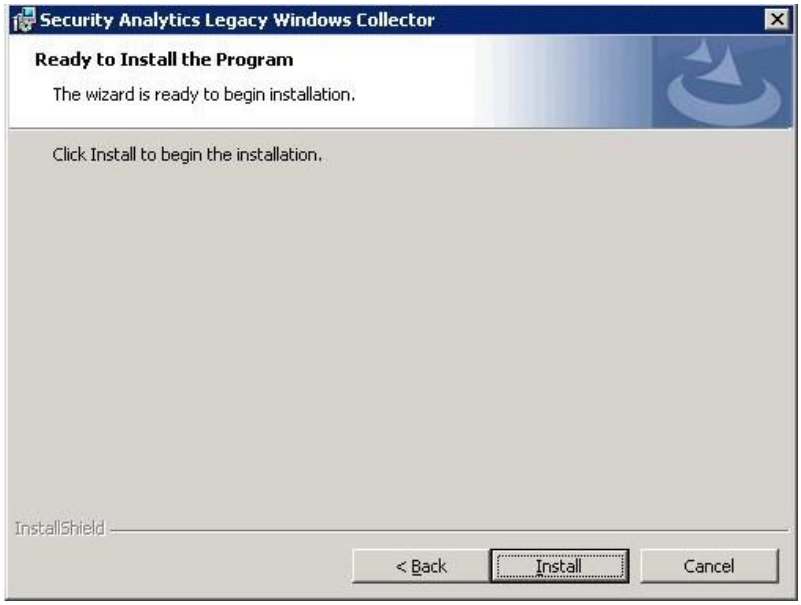


6. Lea detenidamente el acuerdo de licencia, seleccione el botón de opción **Acepto los términos del acuerdo de licencia** y haga clic en **Siguiente**.
   Antes de comenzar con la actualización, el asistente pregunta si desea continuar con la instalación de la actualización o cancelarla.

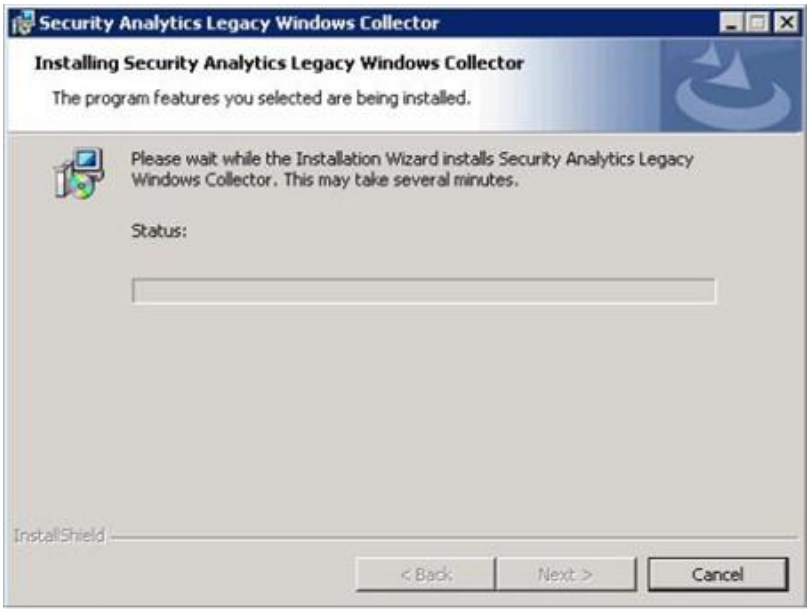


7. Haga clic en **Aceptar** para continuar instalando la actualización.
8. Ingrese un nombre de usuario y una contraseña y haga clic en **Siguiente**.
   Se muestra la página Preparado para instalar el programa.

> **Nota:** Si las credenciales no son válidas, se muestra el mensaje **Credenciales no válidas**.

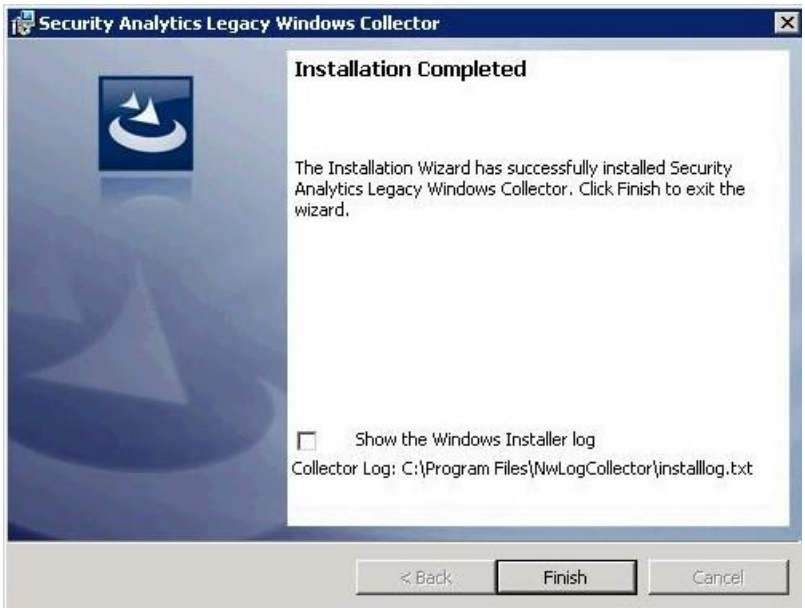


9. Haga clic en **Instalar**.
   Se muestra la página Instalando el colector de Windows existente de Security Analytics.



   Cuando se completa la instalación de la actualización, se habilita el botón **Siguiente**.

10. Haga clic en **Siguiente**.
    Se muestra la página Instalación completada.



11. (Opcional) Si desea revisar un registro de la instalación de la actualización, seleccione la casilla de verificación **Mostrar el registro del instalador de Windows**.

12. Haga clic en **Finalizar**.

> **Nota:** Consulte los siguientes archivos de registro si necesita solucionar problemas:
> - **%systemDrive%\Netwitness\ng\logcollector\MessageBroker.log**
> - **%systemDrive%\Program Files\NwLogCollector\installlog.txt**
>
> Ejecute `C:\Program Files\NwLogCollector\ziplogfiles.vbs` para generar el archivo *`hostname`*`_WLCversion_timestamp.zip` que contiene todos los archivos de registro más la información necesaria para la solución de problemas.

Esto pone fin a la actualización del colector de Windows existente a Security Analytics 10.6.

Instalar el colector de Windows existente de 10.6 (instalación inicial)

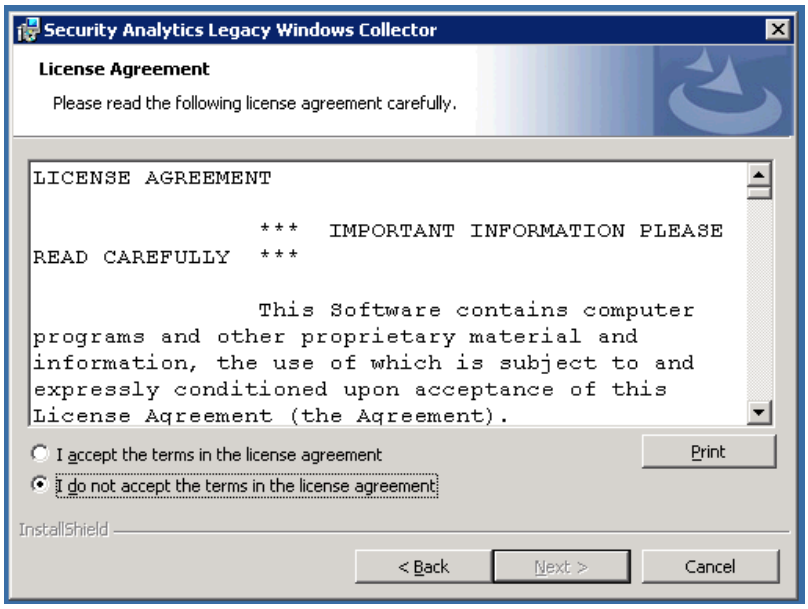
En este tema se indica cómo instalar el colector de Windows existente de 10.6 en un servidor Windows 2008 R2 SP1 de 64 bits

Procedimiento

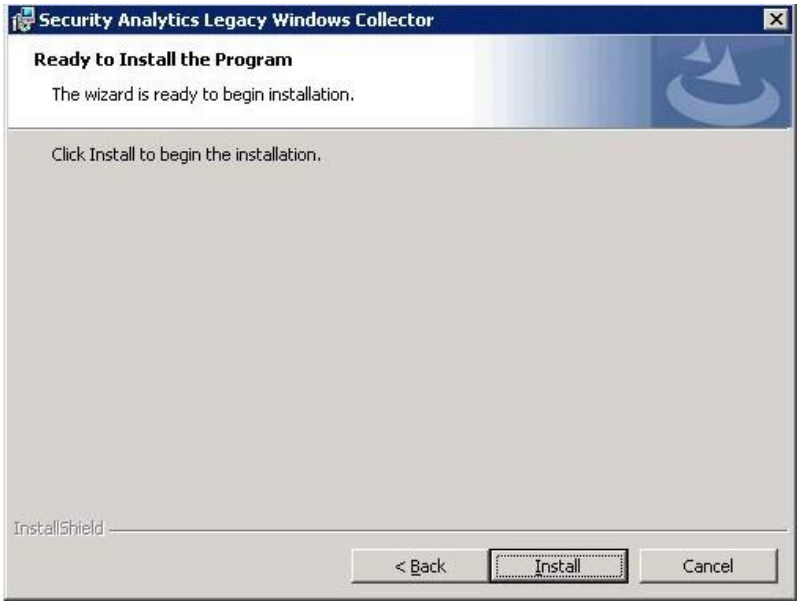
Para instalar el colector de Windows existente de Security Analytics en un servidor Windows 2008 R2 SP1 de 64 bits:

1. Busque **10.6 Legacy Windows Collector** en SCOL, haga clic para descargar **SA-10.6.0.0-LegacyWindowsCollector.zip** y descomprima el archivo.
2. Inicie sesión en una máquina Windows 2008 con un usuario de dominio no administrativo (o un administrador local).
3. Consulte **Crear un usuario de dominio no administrativo para cada dominio** si necesita instrucciones para crear un usuario de dominio no administrativo.
4. Copie el archivo **SALegacyWindowsCollector-version-number.exe** al servidor de Windows 2008.
5. Haga clic con el botón secundario en **SALegacyWindowsCollector-version-number.exe** y seleccione **Ejecutar como administrador**.
   Se muestra la página **Bienvenido…** del asistente para la instalación.

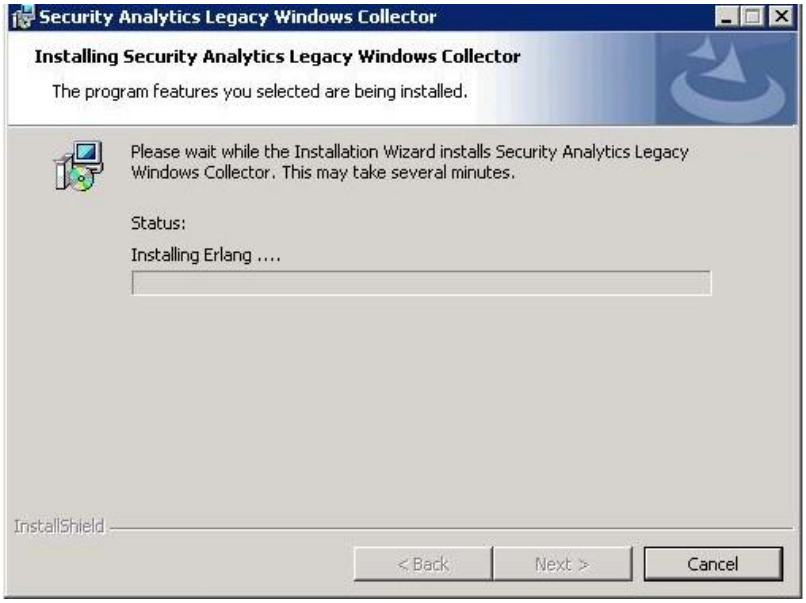
6. Haga clic en **Siguiente**.
   Se muestra la página Acuerdo de licencia.

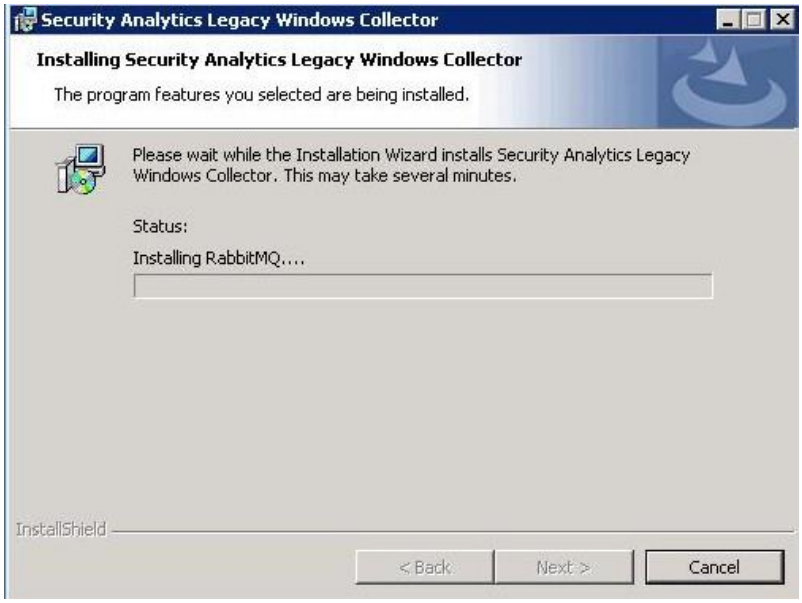


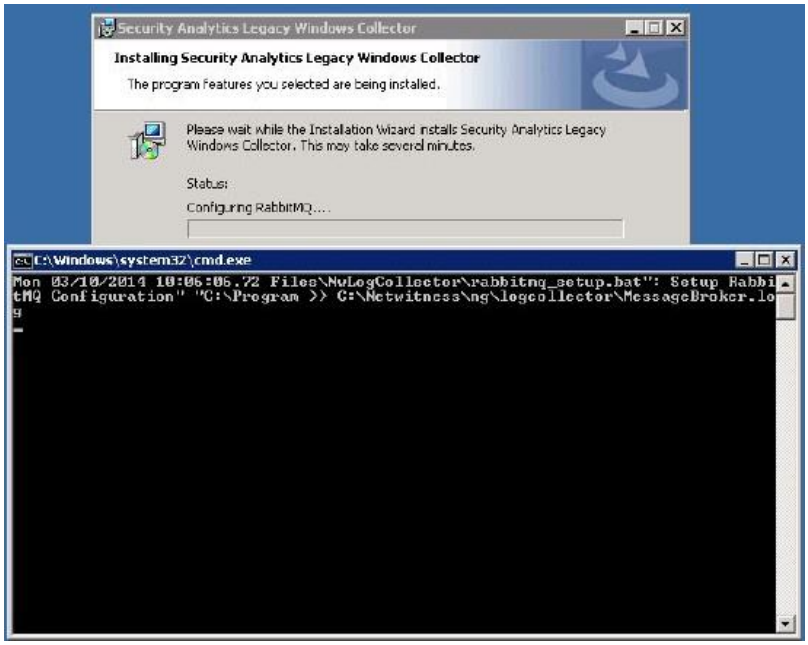
7. Lea detenidamente el acuerdo de licencia, seleccione el botón de opción **Acepto los términos del acuerdo de licencia** y haga clic en **Siguiente**.
   Se muestra la página Preparado para instalar el programa.



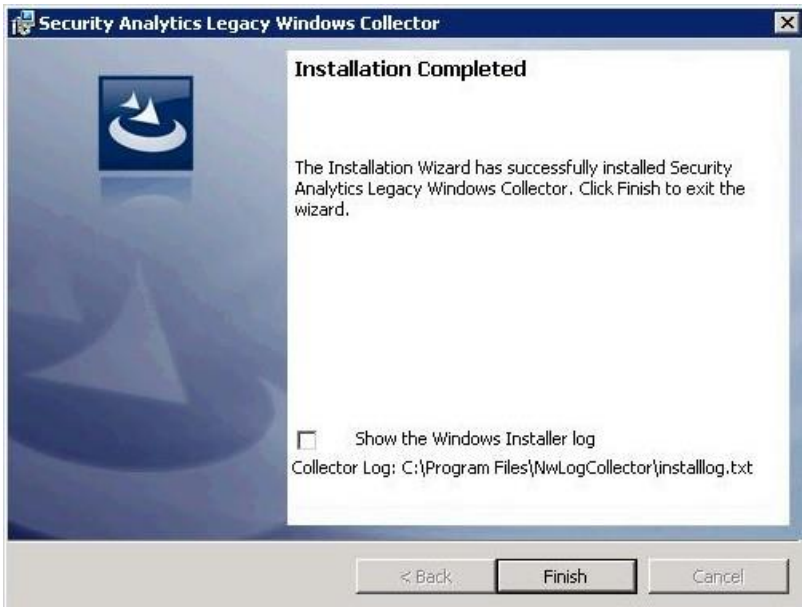
8. Haga clic en **Instalar**.
   Se muestra la página Instalando el colector de Windows existente de Security Analytics.







Se muestra la página Instalación completada.



9. (Opcional) Si desea revisar un registro de la instalación, seleccione la casilla de verificación **Mostrar el registro del instalador de Windows**.
10. Haga clic en **Finalizar**.

> **Nota:** Consulte los siguientes archivos de registro si necesita solucionar problemas:
>
> - **%systemDrive%\Netwitness\ng\logcollector\MessageBroker.log**
> - **%systemDrive%\Program Files\NwLogCollector\installlog.txt**
>
> Ejecute **C:\Program Files\NwLogCollector\ziplogfiles.vbs** para generar el archivo **hostname_WLCversion_timestamp.zip** que contiene todos los archivos de registro más la información necesaria para la solución de problemas.

Esto pone fin a la instalación del colector de Windows existente de 10.6. Consulte la **Guía de configuración para la recopilación de Windows existente y NetApp** (https://sadocs.emc.com/0_en-us/088_SA106/135_LLGds/96_LegWinPro) en la ayuda de Security Analytics 10.6 para encontrar instrucciones sobre cómo configurar la recopilación de Windows existente en Security Analytics.

Historial de revisiones

Revisión	Fecha	Descripción	Autor
1.0	16 de febrero de 2016	Versión inicial	Info Design & Devel (dfo)