

Guía de seguridad de Operations Manager 2007 R2

Microsoft Corporation

Fecha de publicación: mayo de 2009

Autor

John Downing

Revisores principales

Ian Jirka, Joseph Chan, Lincoln Atkinson, Olof Mases, Ruhiyyih Mahalati, Smita Mahalati y Tim Helton

Revisores secundarios

Eugene Bykov, Clive Eastwood, Doug Bradley, Jakub Oleksy, Ranga Kalyanasundaram y Vitaly Filimonov

Comentarios

Envíe sus sugerencias y comentarios sobre este documento a momdocs@microsoft.com. Incluya el nombre de la guía de seguridad y la fecha de publicación en sus comentarios.

La información que contiene este documento representa el criterio de Microsoft Corporation sobre los temas tratados vigente en la fecha de publicación. Como Microsoft debe reaccionar ante las condiciones cambiantes del mercado, no debe interpretarse como un compromiso por parte de Microsoft, y Microsoft no puede garantizar la exactitud de la información que se presente después de la fecha de publicación.

Este documento sólo tiene fines informativos. MICROSOFT NO OFRECE NINGUNA CLASE DE GARANTÍA, EXPRESA, IMPLÍCITA O ESTATUTARIA, CON RESPECTO A LA INFORMACIÓN QUE CONTIENE ESTE DOCUMENTO.

Es responsabilidad del usuario el cumplimiento de todas las leyes de derechos de autor aplicables. Sin limitar los derechos de autor, ninguna parte de este documento puede ser reproducida, almacenada o introducida en un sistema de recuperación, o transmitida de ninguna forma, ni por ningún medio (ya sea electrónico, mecánico, por fotocopia, grabación o de otra manera), con ningún propósito, sin la previa autorización por escrito de Microsoft Corporation.

Microsoft puede ser titular de patentes, solicitudes de patente, marcas, derechos de autor y otros derechos de propiedad intelectual sobre los contenidos de este documento. El suministro de este documento no le otorga ninguna licencia sobre estas patentes, marcas, derechos de autor ni otros derechos de propiedad intelectual, a menos que ello se prevea en un contrato por escrito de licencia de Microsoft.

A menos que se indique lo contrario, las compañías, las organizaciones, los productos, los nombres de dominio, las direcciones de correo electrónico, los logotipos, las personas, los lugares y los eventos usados en los ejemplos son ficticios. No se pretende ni se debe inferir de ningún modo relación con ninguna compañía, organización, producto, nombre de dominio, dirección de correo electrónico, logotipo, persona, lugar ni evento.

© 2009 Microsoft Corporation. Reservados todos los derechos.

Microsoft, Active Directory, ActiveSync, Internet Explorer, Jscript, SharePoint, SQL Server, Visio, Visual Basic, Visual Studio, Win32, Windows, Windows PowerShell, Windows Server y Windows Vista son marcas comerciales del grupo de compañías de Microsoft.

El resto de marcas comerciales pertenecen a sus respectivos propietarios.

Historial de revisiones

|  |  |
| --- | --- |
| Fecha de publicación | Cambios |
| mayo de 2009 | La versión de Operations Manager 2007 R2 de esta guía contiene las siguientes actualizaciones y adiciones:* Se ha agregado información para la implementación de agentes en sistemas UNIX y Linux.
* Se ha agregado una lista de valores hash para agentes UNIX y Linux.
 |

Contenido

[Seguridad con Operations Manager 2007 R2 7](#_Toc238830667)

[Acerca de la guía de seguridad de Operations Manager 2007 7](#_Toc238830668)

[Nuevas funciones de seguridad en Operations Manager 2007 8](#_Toc238830669)

[Información sobre cuentas para Operations Manager 2007 9](#_Toc238830670)

[Cambio de la contraseña de la cuenta del grupo de aplicaciones del servidor de informes de IIS en Operations Manager 2007 14](#_Toc238830671)

[Cambio de la contraseña de la cuenta de ejecución del servidor de informes en Operations Manager 2007 14](#_Toc238830672)

[Cambio de las cuentas de servicio de configuración y SDK en Operations Manager 2007 15](#_Toc238830673)

[Cambio de la contraseña de la cuenta de servicio de Windows para SQL Server Reporting Service en Operations Manager 2007 16](#_Toc238830674)

[Establecimiento de la cuenta de acción en varios equipos en Operations Manager 2007 17](#_Toc238830675)

[Seguridad basada en funciones en Operations Manager 2007 19](#_Toc238830676)

[Run As Accounts and Run As Profiles in Operations Manager 2007 (Perfiles de ejecución y cuentas de ejecución en Operations Manager 2007) 23](#_Toc238830677)

[Creación de una cuenta de ejecución en Operations Manager 2007 29](#_Toc238830678)

[Creación y configuración de un perfil de ejecución en Operations Manager 2007 31](#_Toc238830679)

[Modificación de un perfil de ejecución existente 34](#_Toc238830680)

[Autenticación y cifrado de datos para equipos de Windows en Operations Manager 2007 35](#_Toc238830681)

[Configuración de la consola de Operations para usar SSL cuando se conecta a un servidor de informes en Operations Manager 2007 43](#_Toc238830682)

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2003 en Operations Manager 2007 44](#_Toc238830683)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2003 en Operations Manager 2007 48](#_Toc238830684)

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2008 en Operations Manager 2007 53](#_Toc238830685)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2008 en Operations Manager 2007 58](#_Toc238830686)

[Eliminación de certificados importados con MOMCertImport en Operations Manager 2007 63](#_Toc238830687)

[Cambio de la cuenta de identificación asociada a un perfil de identificación 64](#_Toc238830688)

[Configuración de un enlace HTTPS para una entidad de certificación de Windows Server 2008 65](#_Toc238830689)

[Autenticación y cifrado de datos para sistemas operativos UNIX y Linux 66](#_Toc238830690)

[Instalación manual de certificados para soporte de varias plataformas 67](#_Toc238830691)

[Uso de firewalls con Operations Manager 2007 69](#_Toc238830692)

[Configuración de la base de datos OperationsManager para escuchar en un puerto TCP/IP específico 74](#_Toc238830693)

[Configuración del almacenamiento de datos de informes para escuchar en un puerto TCP/IP específico 77](#_Toc238830694)

[Uso de certificados con ACS en Operations Manager 2007 80](#_Toc238830695)

[Configuración de certificados en el recopilador de ACS en Operations Manager 2007 81](#_Toc238830696)

[Configuración de certificados en el reenviador de ACS en Operations Manager 2007 83](#_Toc238830697)

[Consideraciones de seguridad para la administración sin agentes en Operations Manager 2007 84](#_Toc238830698)

[Seguridad de la consola web en Operations Manager 2007 85](#_Toc238830699)

[Apéndice A - Lista de operaciones en Operation Manager 2007 86](#_Toc238830700)

[Apéndice B - Lista de valores hash para agentes de UNIX y Linux 90](#_Toc238830701)

Seguridad con Operations Manager 2007 R2

Acerca de la guía de seguridad de Operations Manager 2007

Esta guía le proporciona información relacionada con seguridad correspondiente a Operations Manager 2007. Los temas que se tratan en esta versión de la guía de seguridad se describen en la sección siguiente.

Para futuras versiones de este documento, consulte la [Guía de seguridad de Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=64017) (http://go.microsoft.com/fwlink/?LinkId=64017).

En esta sección

|  |  |
| --- | --- |
| [Información sobre cuentas para Operations Manager 2007](#zbe2bbe81fe1a48e7b2cd3c8a3eab2255) | Describe las cuentas de Operations Manager 2007 para las que proporcionará credenciales. |
| [Seguridad basada en funciones en Operations Manager 2007](#zd49361c238194d14a23a10cf4573c424) | Describe cómo se implementa la seguridad basada en funciones. |
| [Run As Accounts and Run As Profiles in Operations Manager 2007 (Perfiles de ejecución y cuentas de ejecución en Operations Manager 2007)](#zd06fe34a089c42a18ae641e0290451ac) | Describe cómo se usan los perfiles de ejecución y las cuentas de ejecución. |
| [Autenticación y cifrado de datos para equipos de Windows en Operations Manager 2007](#z1d2d66a714704e46bf9434e6e4a42e65) | Describe cómo y cuándo se cifran los datos entre varios componentes de Operations Manager e instrucciones sobre cómo obtener y usar certificados. |
| [Autenticación y cifrado de datos para sistemas operativos UNIX y Linux](#z0a89f3fd0cf346ec82bd8be5e93e783f) | Describe cómo implementar con seguridad agentes en equipos basados en UNIX y en Linux. |
| [Uso de certificados con ACS en Operations Manager 2007](#zb6db0f5df0884020bf876c6a2e38ec13) | Describe cuándo se deben usar los certificados para que la autenticación tenga lugar entre el reenviador de ACS y el recopilador de ACS. |
| [Consideraciones de seguridad para la administración sin agentes en Operations Manager 2007](#zfffedfd386fa4560be76815b4a6efd1d) | Proporciona información sobre las consideraciones de seguridad para la administración sin agentes. |
| [Seguridad de la consola web en Operations Manager 2007](#z702b4b865b914ee98c22360f4bc0bad5) | Muestra cómo usar la capa de sockets seguros (SSL) con la consola web en Operations Manager 2007. |
| [Apéndice A - Lista de operaciones en Operation Manager 2007](#z53f262cfe7f14187995f5180c15e842d) | Muestra las operaciones disponibles, desglosadas por perfil. |
| [Apéndice B - Lista de valores hash para agentes de UNIX y Linux](#z9f418c9465d445f2a0bc7217f8c4c3f0) | Muestra los valores hash para los agentes de UNIX y Linux |

Recursos externos

Para obtener una versión en línea de la ayuda, consulte la [Ayuda de Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=77739) (http://go.microsoft.com/fwlink/?LinkID=77739).

Nuevas funciones de seguridad en Operations Manager 2007

Las siguientes secciones describen funciones relacionadas con la seguridad disponibles en Operations Manager 2007 que no estaban disponibles en Microsoft Operations Manager (MOM) 2005.

Cuentas de ejecución y perfiles de ejecución

En MOM 2005, se usaban las credenciales de una sola cuenta de acción para la ejecución de todas las tareas y respuestas y, por lo tanto, era necesario que esa cuenta de acción tuviera derechos suficientes para todas las aplicaciones supervisadas. Con Operations Manager 2007 se introducen los perfiles de ejecución y las cuentas de ejecución Varias cuentas de ejecución pueden supervisar diversas aplicaciones o componentes y le permiten crear credenciales con los mínimos privilegios posibles para realizar las tareas correspondientes.

La cuenta de ejecución le permite administrar todas las contraseñas y cuentas de todo el grupo de administración desde una ubicación, el servidor de administración raíz.

Funciones de usuario

Puede obtener acceso y manipular Operations Manager 2007 por diversos métodos: a través de la consola de Operations, la consola web, Windows PowerShell o aplicaciones personalizadas. En todos los casos, la seguridad basada en funciones asegura que las credenciales del usuario suministradas sean miembros de una función de usuario en Operations Manager 2007.

Información sobre cuentas para Operations Manager 2007

Durante la instalación y el funcionamiento de Operations Manager 2007, se le solicitará que proporcione credenciales para varias cuentas. Al comienzo de esta sección se proporciona información sobre cuentas de acción. Se incluye información sobre otras cuentas como la cuenta de servicio de configuración y SDK, cuenta de instalación de agente, cuenta de escritura de almacenamiento de datos y cuenta de lectura de datos.

¿Qué es una cuenta de acción?

Las diversas funciones de servidor de Operations Manager 2007, servidor de administración raíz, servidor de administración, servidor de puerta de enlace y agente, contienen un proceso denominado MonitoringHost.exe. MonitoringHost.exe es lo que usa cada función de servidor para realizar las actividades de supervisión, como por ejemplo, ejecutar un monitor o ejecutar una tarea. Por ejemplo, cuando un agente se suscribe al registro de eventos para leer eventos, es el proceso MonitoringHost.exe el que ejecuta esas actividades. A la cuenta de ejecución de un proceso MonitoringHost.exe se le denomina cuenta de acción. A la cuenta de acción para el proceso MonitoringHost.exe que se ejecuta en un agente se le denomina cuenta de acción de agente. A la cuenta de acción que usa el proceso MonitoringHost.exe en un servidor de administración se le denomina cuenta de acción del servidor de administración. A la cuenta de acción que usa el proceso MonitoringHost.exe en un servidor de puerta de enlace se le denomina cuenta de acción del servidor de puerta de enlace.

Cuenta de acción del agente

A menos que se haya asociado una acción con un perfil de ejecución, las credenciales usadas para realizar la acción serán aquellas definidas para la cuenta de acción. Para obtener más información sobre el perfil de ejecución, consulte [Run As Accounts and Run As Profiles in Operations Manager 2007 (Perfiles de ejecución y cuentas de ejecución en Operations Manager 2007)](#zd06fe34a089c42a18ae641e0290451ac) en esta guía. Algunos ejemplos de acciones incluyen lo siguiente:

 Supervisión y recopilación de datos del registro de eventos de Windows

 Supervisión y recopilación de datos del contador de rendimiento de Windows

 Supervisión y recopilación de datos del Instrumental de administración de Windows (WMI)

 Ejecutar acciones como scripts o lotes

MonitoringHost.exe es el proceso que ejecuta estas acciones mediante el uso de credenciales especificadas en la cuenta de acción. Se crea una nueva instancia de MonitoringHost.exe para cada cuenta.

Uso de cuentas con pocos privilegios

Al instalar Operations Manager 2007, puede elegir una o dos opciones mientras asigna la cuenta de acción:

 Sistema local

 Cuenta de dominio o local

Una opción común es especificar una cuenta de dominio que le permita seleccionar un usuario con la cantidad mínima de privilegios necesarios para el entorno.

En los equipos que ejecutan Windows Server 2003, Windows Server 2003 R2 y el sistema operativo Windows Vista, la cuenta de acción predeterminada debe tener los privilegios mínimos siguientes:

 Miembro del grupo Usuarios local

 Miembro del grupo Usuarios del monitor de rendimiento local

 Permiso Permitir el inicio de sesión local (SetInteractiveLogonRight)

Importante

Los privilegios mínimos descritos anteriormente son los privilegios más bajos que admite Operations Manager 2007 para la cuenta de acción. Otras cuentas de ejecución pueden tener privilegios más bajos. Los privilegios reales que necesitarán las cuentas de ejecución dependerán de los módulos de administración que se ejecuten en el equipo y de la forma en que estén configurados. Para obtener más información acerca de los privilegios específicos necesarios, consulte la guía del módulo de administración correspondiente.

Tenga en cuenta los puntos siguientes para elegir las credenciales de la cuenta de acción:

 Una cuenta con privilegios bajos sólo puede usarse en equipos que ejecuten Windows Server 2003, Windows Server 2003 R2 y Windows Vista. En equipos que ejecutan Windows 2000 y Windows XP, la cuenta de acción debe pertenecer al grupo de seguridad local Administradores o al sistema local.

 Una cuenta con privilegios bajos es lo único que necesitan los agentes que se usan para supervisar controladores de dominio.

 Usar una cuenta de dominio requiere tener una contraseña coherente con las directivas de caducidad de la contraseña.

 Debe detener e iniciar el servicio de administración de System Center si la cuenta de acción se ha configurado para usar una cuenta de privilegios bajos y la cuenta de privilegios bajos se agregó a los grupos requeridos mientras se estaba ejecutando el servicio de administración de System Center.

Cuenta de acción de notificación

La cuenta de acción de notificación es una cuenta de ejecución creada por el usuario para configurar notificaciones. Es la cuenta de acción que se usa para crear y enviar notificaciones. Asegúrese de que las credenciales que usa para esta cuenta tengan suficientes derechos para el servidor SMTP, el servidor de mensajería instantánea o el servidor SIP que vaya a usar para las notificaciones.

Si cambia la contraseña para las credenciales especificadas para la cuenta de acción de notificación, tendrá que realizar los mismos cambios de contraseña para la cuenta de ejecución.

Administración de las credenciales de cuenta de acción

Para la cuenta que elija, Operations Manager determinará cuál es la fecha de caducidad de la contraseña y generará una alerta14 días antes de que la cuenta caduque. Cuando cambie la contraseña en Active Directory, puede cambiar la contraseña para la cuenta de acción en Operations Manager en la ficha Cuenta de la página Propiedades de la cuenta de ejecución. Para obtener más información sobre la administración de las credenciales de cuenta de acción, consulte [Cambio de las credenciales para la cuenta de acción en Operations Manager](http://go.microsoft.com/fwlink/?LinkId=88304) (http://go.microsoft.com/fwlink/?LinkId=88304).

Puede usar un script de Windows PowerShell, set-ActionAccount.ps1, para establecer la cuenta de acción en varios equipos. Para obtener más información, consulte el [SC Ops Mgr 2007 Resource Kit (Kit de recursos de System Center Operations Manager 2007)](http://go.microsoft.com/fwlink/?LinkId=92596) (http://go.microsoft.com/fwlink/?LinkId=92596). El script le permite establecer la cuenta de acción en todos los equipos definidos en un grupo de equipos. Consulte Establecimiento de la cuenta de acción en varios equipos en Operations Manager 2007 en la guía de seguridad.

Cuenta de servicio de configuración y SDK

La cuenta de servicio de configuración y SDK es un conjunto de credenciales que usan los servicios de acceso de datos de System Center y de configuración de administración de System Center para actualizar y leer información en la base de datos OperationsManager. Operations Manager asegura que las credenciales usadas para la cuenta de acción de configuración y SDK se asignarán a la función sdk\_user en la base de datos OperationsManager. La cuenta de servicio de configuración y SDK se puede configurar como sistema local o como una cuenta de dominio. No se admite una cuenta de usuario local.

Si el servidor de administración raíz y la base de datos OperationsManager están en equipos diferentes, será necesario cambiar la cuenta de servicio de configuración y SDK a una cuenta de dominio. Para una mayor seguridad, le recomendamos que use una cuenta diferente a la cuenta usada para la cuenta de acción del servidor de administración. Para cambiar estas cuentas, consulte el artículo de Knowledge Base [Cómo cambiar las credenciales de los servicios SDK y de configuración de OpsMgr en Microsoft System Center Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=112435) (http://go.microsoft.com/fwlink/?LinkId=112435).

Cuenta de instalación de agente

Al implementar el agente basado en detecciones, el sistema solicita una cuenta con derechos de usuario de administrador. Esta cuenta se usará para instalar el agente en el equipo y, por tanto, debe ser un administrador local en todos los equipos en los que va a implementar agentes. La cuenta de acción del servidor de administración es la cuenta predeterminada para la instalación de agentes. Si la cuenta de acción del servidor de administración no tiene derechos de administrador, seleccione Cuenta de otro usuario y escriba una cuenta con derechos de administrador. Esta cuenta se cifra antes de usarse y, a continuación, se descarta.

Cuenta de escritura de almacenamiento de datos

La cuenta de escritura de almacenamiento de datos escribe datos desde el servidor de administración raíz o el servidor de administración en el almacenamiento de datos de informes y lee los datos desde la base de datos OperationsManager. Las credenciales proporcionadas para esta cuenta se convertirán en miembro de las funciones dependiendo de la aplicación, como se describe en la tabla siguiente.

|  |  |  |
| --- | --- | --- |
| Aplicación | Base de datos/Función | Función/Cuenta |
| Microsoft SQL Server 2005 | OperationsManager | db\_datareader |
| Microsoft SQL Server 2005 | OperationsManager | dwsync\_user |
| Microsoft SQL Server 2005 | OperationsManagerDW | OpsMgrWriter |
| Microsoft SQL Server 2005 | OperationsManagerDW | db\_owner |
| Operations Manager 2007 | Función de usuario | Administradores de seguridad de informes de Operations Manager |
| Operations Manager 2007 | Cuenta de ejecución | Cuenta de acción de almacenamiento de datos |
| Operations Manager 2007 | Cuenta de ejecución | Cuenta de lectura de sincronización de configuración del almacenamiento de datos |

Si cambia la contraseña para las credenciales especificadas para la cuenta de escritura de almacenamiento de datos, tendrá que realizar los mismos cambios de contraseña para las cuentas siguientes:

 La cuenta de ejecución denominada Cuenta de acción de almacenamiento de datos

 La cuenta de ejecución denominada Cuenta de lectura de sincronización de configuración almacenamiento de datos

Cuenta de lectura de datos

Esta cuenta se usa para implementar informes, definir el usuario que SQL Reporting Services usa para ejecutar consultas en el almacenamiento de datos de informes y para que la cuenta del grupo de aplicaciones de SQL Reporting Services IIS se conecte al servidor de administración raíz.Esta cuenta se agrega al perfil de usuario del administrador de informes.

Las credenciales proporcionadas para esta cuenta se convertirán en miembro de las funciones dependiendo de la aplicación, como se describe en la tabla siguiente.

|  |  |  |
| --- | --- | --- |
| Aplicación | Base de datos/Función | Función/Cuenta |
| Microsoft SQL Server 2005 | Instancia de instalación del servidor de informes | Cuenta de ejecución del servidor de informes |
| Microsoft SQL Server 2005 | OperationsManagerDW | OpsMgrReader |
| Operations Manager 2007 | Función de usuario | Administradores de seguridad de informes de Operations Manager |
| Operations Manager 2007 | Función de usuario | Operadores de informes de Operations Manager |
| Operations Manager 2007 | Cuenta de ejecución | Cuenta de implementación de informes de almacenamiento de datos |
| IIS | Grupo de aplicaciones | ReportServer$<INSTANCIA> |
| Servicio de Windows | SQL Server Reporting Services | Cuenta de inicio de sesión |

Si cambia la contraseña para las credenciales especificadas para la cuenta de lectura de datos, tendrá que realizar los mismos cambios de contraseña para las cuentas siguientes:

 Cuenta de ejecución del servidor de informes

 La cuenta de servicio de SQL Server Reporting Services en el equipo que hospeda SQL Server Reporting Services (SRS)

 La cuenta del grupo de aplicaciones de <INSTANCIA> de IIS ReportServer$

 Cuenta de ejecución denominada Cuenta de implementación de informes de almacenamiento de datos

Vea también

[Cambio de la contraseña de la cuenta de ejecución del servidor de informes en Operations Manager 2007](#zee734cd7ec21444986691ec69f70c8d1)

[Cambio de la contraseña de la cuenta de ejecución del servidor de informes en Operations Manager 2007](#zee734cd7ec21444986691ec69f70c8d1)

[Cambio de las cuentas de servicio de configuración y SDK en Operations Manager 2007](#z3dfae6c41f294d2cb73110536eba4c69)

[Cambio de la contraseña de la cuenta de servicio de Windows para SQL Server Reporting Service en Operations Manager 2007](#zcd0a378ca64b42c5a0a0067766e96d63)

[Establecimiento de la cuenta de acción en varios equipos en Operations Manager 2007](#zdb19cadcde5f47dfad4132204338e953)

Cambio de la contraseña de la cuenta del grupo de aplicaciones del servidor de informes de IIS en Operations Manager 2007

Si se cambia la contraseña para la cuenta que especificó como Cuenta de lectura de datos durante la instalación del servidor de informes, use el procedimiento siguiente para cambiar la contraseña de la cuenta del grupo de aplicaciones del servidor de informes de IIS en el equipo que ejecuta SQL Server Reporting Services.

Para cambiar la cuenta del grupo de aplicaciones del servidor de informes de IIS

|  |
| --- |
| 1. En el equipo que ejecuta SQL Server Reporting Services, en el escritorio de Windows, haga clic en Inicio, seleccione Programas, seleccione Herramientas administrativas y, a continuación, haga clic en Administrador de Internet Information Services (IIS).2. En Administrador de Internet Information Services (IIS), expanda <Nombre del equipo> (equipo local), expanda Grupos de aplicaciones, haga clic con el botón secundario en ReportServer<INSTANCIA> y, a continuación, haga clic en Propiedades.3. En el cuadro de diálogo ReportServer<INSTANCIA> Propiedades, haga clic en Identidad.4. En el cuadro de texto Contraseña, escriba la nueva contraseña y, a continuación, haga clic en Aceptar.5. Cierre el Administrador de Internet Information Services (IIS). |

Vea también

[Cambio de la contraseña de la cuenta de ejecución del servidor de informes en Operations Manager 2007](#zee734cd7ec21444986691ec69f70c8d1)

[Cambio de la contraseña de la cuenta de servicio de Windows para SQL Server Reporting Service en Operations Manager 2007](#zcd0a378ca64b42c5a0a0067766e96d63)

Cambio de la contraseña de la cuenta de ejecución del servidor de informes en Operations Manager 2007

Si se cambia la contraseña para la cuenta que especificó como Cuenta de lectura de datos durante la instalación del servidor de informes, use el procedimiento siguiente para cambiar la contraseña de la cuenta de ejecución del servidor de informes.

Para cambiar la contraseña de la cuenta de ejecución del servidor de informes

|  |
| --- |
| 1. En el equipo que hospeda el servidor de informes, en el escritorio de Windows, haga clic en Inicio, elija Programas, seleccione Microsoft SQL Server 2005, seleccione Herramientas de configuración y, a continuación, haga clic en Configuración de Reporting Services.2. En el cuadro de diálogo Selección de instancia de instalación del servidor de informes, haga clic en Conectar.3. En el panel Administrador de configuración de Reporting Services, en el panel izquierdo, haga clic en Cuenta de ejecución.4. En el panel Cuenta de ejecución, escriba la nueva contraseña de la cuenta de ejecución.5. Haga clic en Aplicar y, a continuación, en Salir para cerrar Administrador de configuración de Reporting Services. |

Vea también

[Cambio de la contraseña de la cuenta del grupo de aplicaciones del servidor de informes de IIS en Operations Manager 2007](#zcd4e215169e74bcfa973e6ee830e7240)

[Cambio de la contraseña de la cuenta de servicio de Windows para SQL Server Reporting Service en Operations Manager 2007](#zcd0a378ca64b42c5a0a0067766e96d63)

Cambio de las cuentas de servicio de configuración y SDK en Operations Manager 2007

Durante la instalación de Operations Manager 2007, se le solicita las credenciales para dos servicios. Los nombres de estos servicios cambiaron con la introducción de Operations Manager 2007 R2. Si desea cambiar la contraseña para las credenciales que proporcionó o usar un conjunto de credenciales diferente, siga el procedimiento de la versión de Operations Manager que esté usando.

Nota

Se deben usar las mismas credenciales para ambos servicios.

Para cambiar los credenciales o la contraseña de los servicios de Operations Manager 2007 SP1

|  |
| --- |
| 1. En el equipo que hospeda el servidor de administración raíz, en el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba services.msc y, a continuación, haga clic en Aceptar.3. En la lista de servicios, haga clic con el botón secundario en Servicio SDK y seleccione Propiedades.4. En el cuadro de diálogo Propiedades de SDK, haga clic en la ficha Iniciar sesión.5. Escriba nuevas credenciales o cambie la contraseña de las credenciales existentes y, a continuación, haga clic en Aceptar.6. En la lista de servicios, haga clic con el botón secundario en Servicio de configuración y seleccione Propiedades.7. En el cuadro de diálogo Propiedades de configuración, haga clic en la ficha Iniciar sesión.8. Escriba nuevas credenciales o cambie la contraseña de las credenciales existentes y, a continuación, haga clic en Aceptar.9. Detenga y reinicie tanto el servicio de configuración como el servicio SDK. |

Para cambiar las credenciales o la contraseña de los servicios de Operations Manager 2007 R2

|  |
| --- |
| 1. En el equipo que hospeda el servidor de administración raíz, en el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba services.msc y, a continuación, haga clic en Aceptar.3. En la lista de servicios, haga clic con el botón secundario en Servicio de acceso de datos de System Center y seleccione Propiedades.4. En el cuadro de diálogo Propiedades de acceso de datos de System Center, haga clic en la ficha Iniciar sesión.5. Escriba nuevas credenciales o cambie la contraseña de las credenciales existentes y, a continuación, haga clic en Aceptar.6. En la lista de servicios, haga clic con el botón secundario en Servicio de configuración de administración de System Center y seleccione Propiedades.7. En el cuadro de diálogo Propiedades de configuración de administración de System Center, haga clic en la ficha Iniciar sesión.8. Escriba nuevas credenciales o cambie la contraseña de las credenciales existentes y, a continuación, haga clic en Aceptar.9. Detenga y reinicie tanto el servicio de acceso de datos de System Center como el servicio de configuración de administración de System Center. |

Cambio de la contraseña de la cuenta de servicio de Windows para SQL Server Reporting Service en Operations Manager 2007

Si se cambia la contraseña para la cuenta que especificó como Cuenta de lectura de datos durante la instalación del servidor de informes, use el procedimiento siguiente para cambiar la cuenta de servicio de Windows para la contraseña de SQL Server Reporting Services en el equipo que ejecuta SQL Server Reporting Services (SRS).

Para cambiar la cuenta de servicio de Windows para SQL Server Reporting Services

|  |
| --- |
| 1. En el escritorio de Windows del equipo que ejecuta SQL Server Reporting Services, haga clic en Inicio, seleccione Configuración y haga clic en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba services.msc y, a continuación, haga clic en Aceptar.3. En Servicios, desplácese por la lista, haga clic con el botón secundario en SQL Server Reporting Services (<INSTANCIA>) y, a continuación, haga clic en Propiedades.4. En el cuadro de diálogo SQL Server Reporting Services (<INSTANCIA>) Propiedades, haga clic en Iniciar sesión.5. En los cuadros de texto Contraseña y Confirmar Contraseña, escriba la nueva contraseña y, a continuación, haga clic en Aceptar.6. Cierre Servicios y, a continuación, cierre Herramientas administrativas. |

Vea también

[Cambio de la contraseña de la cuenta del grupo de aplicaciones del servidor de informes de IIS en Operations Manager 2007](#zcd4e215169e74bcfa973e6ee830e7240)

[Cambio de la contraseña de la cuenta de ejecución del servidor de informes en Operations Manager 2007](#zee734cd7ec21444986691ec69f70c8d1)

Establecimiento de la cuenta de acción en varios equipos en Operations Manager 2007

Este procedimiento muestra cómo se usa un script de Windows PowerShell, set-ActionAccount.ps1, para establecer la cuenta de acción en varios equipos. Tendrá que descargar el script set-ActionAccount.ps1 en el equipo que hospeda la consola de Operations y el shell de comandos de Operations Manager 2007. Para obtener más información sobre el script set-ActionAccount.ps1 consulte el [SC Ops Mgr 2007 Resource Kit (Kit de recursos de System Center Operations Manager 2007)](http://go.microsoft.com/fwlink/?LinkId=92596) (http://go.microsoft.com/fwlink/?LinkId=92596).

Puede especificar los equipos para los que desea cambiar la cuenta de acción mediante la creación de un nuevo grupo de equipos o la selección de un grupo de equipos del inventario detectado. Ambos procedimientos se describen en las secciones siguientes. Para realizar estos procedimientos, se asume que el script set-AcitonAccount.ps1 se ha descargado en la carpeta My Documents de la unidad C de un usuario.

Para establecer la cuenta de acción en varios equipos

|  |
| --- |
| 1. Inicie una sesión en el equipo con una cuenta que sea miembro de la función de Administradores de Operations Manager para el grupo de administración de Operations Manager 2007.2. En la consola de Operations, haga clic en el botón Supervisión.Nota Al ejecutar la consola de Operations en un equipo que no es un servidor de administración, aparece el cuadro de diálogo Conectar a servidor. En el cuadro de texto Nombre de servidor, escriba el nombre del servidor de administración de Operations Manager 2007 al que desea que se conecte la consola de Operations.3. En el panel Supervisión, haga clic con el botón secundario en Supervisión, elija Nueva y, a continuación, haga clic en Vista Estado.4. En el cuadro de diálogo Propiedades, en el cuadro de texto Nombre, escriba un nombre para esta vista (por ejemplo, Mi grupo de equipos).5. En la ficha Criterios, en el cuadro de lista Mostrar datos relacionados con, haga clic en el botón de puntos suspensivos (…).6. En el cuadro de diálogo Seleccionar un tipo de destino, en el cuadro de texto Buscar, escriba Grupo de equipos, haga clic en Ver todos los destinos, seleccione Grupo de equipos en la lista y, a continuación, haga clic en Aceptar.7. En el cuadro de diálogo Propiedades, haga clic en Aceptar.8. En el panel Supervisión, expanda Supervisión y, a continuación, haga clic en la vista que acaba de crear (por ejemplo, haga clic en Mi grupo de equipos).9. En el panel de resultados (por ejemplo, en panel de resultados Mi grupo de equipos), haga clic con el botón secundario en el grupo de equipos que contenga los equipos de destino para los que desea cambiar la cuenta de acción, haga clic en Abrir y, a continuación, haga clic en Shell de comandos.10. En la ventana Windows PowerShell, escriba la ruta al script seguida del nombre del script y, a continuación, escriba la cuenta de acción a la que desea cambiar. Por ejemplo, escriba c:\Documents and Settings\<user>\My Documents\set-ActionAccount "ActionAccount", (donde “ActionAccount” son las credenciales (dominio\nombre de usuario) para la cuenta de acción que desea establecer en varios servidores) y, a continuación, presione Entrar. |

Para establecer la cuenta de acción en varios equipos mediante el inventario detectado

|  |
| --- |
| 1. Inicie una sesión en el equipo con una cuenta que sea miembro de la función de Administradores de Operations Manager para el grupo de administración de Operations Manager 2007.2. En la consola de Operations, haga clic en el botón Supervisión. Nota Al ejecutar la consola de Operations en un equipo que no es un servidor de administración, aparece el cuadro de diálogo Conectar a servidor. En el cuadro de texto Nombre de servidor, escriba el nombre del servidor de administración de Operations Manager 2007 al que desea que se conecte la consola de Operations.3. En el panel Supervisión, expanda la opción Supervisión y haga clic en Inventario detectado.4. En el panel Acciones, expanda la opción Acciones de estado y haga clic en Cambiar tipo de destino.5. En el cuadro de diálogo Seleccionar un tipo de destino, seleccione Ver todos los destinos.6. En el cuadro de texto Buscar, escriba Grupo de equipos.7. En la columna Destino, haga clic en Grupo de equipos y, a continuación, haga clic en Aceptar.8. En el panel de resultados Inventario detectado (Grupo de equipos), haga clic con el botón secundario en el grupo de equipos que contenga los equipos de destino para los que desea cambiar la cuenta de acción, haga clic en Abrir y, a continuación, haga clic en Shell de comandos.9. En la ventana Windows PowerShell, escriba la ruta al script seguida del nombre del script y, a continuación, escriba la cuenta de acción a la que desea cambiar. Por ejemplo, escriba c:\Documents and Settings\<user>\My Documents\set-ActionAccount "ActionAccount", (donde "ActionAccount" son las credenciales (dominio\nombre de usuario) para la cuenta de acción que desea establecer en varios equipos) y, a continuación, presione Entrar. |

Seguridad basada en funciones en Operations Manager 2007

Puede obtener acceso y manipular Operations Manager 2007 mediante el uso de la consola de Operations, la consola Web, Windows PowerShell o aplicaciones personalizadas. En todos los casos, la seguridad basada en funciones asegura que las credenciales del usuario suministradas sean miembros de una función de usuario en Operations Manager.

Operations Manager 2007 puede supervisar muchos tipos diferentes de aplicaciones en la empresa y estas aplicaciones pueden estar administradas por varios equipos. Como administrador de Operations Manager, puede limitar el acceso a cada equipo para que sólo puedan tener acceso a sus propios datos de supervisión. La seguridad basada en funciones le permite obtener acceso a los datos de supervisión, herramientas y acciones de cada equipo.

Terminología y conceptos

En la tabla siguiente se describe la terminología relativa a la seguridad basada en funciones.

|  |  |
| --- | --- |
| Término | Significado |
| Operación/Privilegio | Una acción asegurable, como resolución de alertas, ejecución de tareas, invalidación de monitores, creación de funciones de usuario, visualización de alertas, visualización de eventos, etc. Para obtener una lista de las operaciones disponibles, consulte el Apéndice A. |
| Perfil | Recopilación de operaciones que se concede a una persona; por ejemplo, un administrador o un operador.Operations Manager 2007 contiene los perfiles siguientes: Administrador Operador avanzado Autor Operador Operador de sólo lectura Operador de informes Administrador de seguridad de informes |
| Ámbito | Define las limitaciones de la ejecución de operaciones de perfil, por ejemplo, tareas y grupos. |
| Funciones de usuario | La combinación de un perfil y un ámbito. |
| Asignación de funciones | Una asociación de usuarios y grupos de Windows a funciones de Operations Manager. |

Ámbito

Todos los objetos de módulo de administración, por ejemplo, atributos, monitores, detecciones de objetos, reglas, tareas y vistas tienen delimitado su ámbito en función de los destinos (también denominados tipos o clases). Un destino, tal y como se define en un módulo de administración representa un cierto tipo de objeto. Todos los objetos de este tipo comparten algunas características comunes. Siempre que existan objetos de este tipo, habrá un modo de detección común, un conjunto común de propiedades que se puede detectar y un modo común de supervisarlos. De forma predeterminada, antes de importar un módulo de administración, se crean 163 destinos en Operations Manager 2007.

Los grupos son recopilaciones lógicas de objetos, como equipos basados en Windows, discos duros o instancias de Microsoft SQL Server.

Las tareas pueden ser una tarea de agente o una tarea de consola. Las tareas de agente se pueden ejecutar remotamente en un agente o en un servidor de administración, mientras que las tareas de consola sólo se pueden ejecutar en el equipo local. Además, las tareas de consola no tiene delimitado su ámbito en función de las funciones de usuario, sino que están disponibles a todos los usuarios. En Operations Manager 2007, puede hacer que un archivo de lote o una secuencia de comandos se ejecuten como tarea remota o localmente, pero si la tarea la genera una alerta o un evento, sólo se puede ejecutar localmente.

Las vistas son grupos de objetos administrados que tienen ciertas particularidades en común y que se definen en las propiedades de la vista. Al seleccionar una vista, se envía una consulta a la base de datos de Operations Manager y los resultados de ésta se muestran en el panel de resultados.

Función de usuario

En Operations Manager 2007, una función de usuario se crea definiendo una unión de perfil y ámbito. Puede crear una función de usuario a partir de uno de los cinco perfiles predeterminados, o de uno de los siete perfiles predeterminados si se ha instalado Reporting, y definir a continuación un ámbito adecuado. La tabla siguiente define los tipos de perfil y un ámbito adecuado para cada uno de ellos.

|  |  |  |
| --- | --- | --- |
| Tipo de perfil | Descripción de perfil | Ámbito de función |
| Administrador | Tiene todos los privilegios en Operations Manager; no es compatible con la administración de ámbitos del perfil Administrador. | Acceso total a todos los datos, servicios, herramientas administrativas y herramientas de creación de Operations Manager. |
| Operador avanzado | Tiene acceso de modificación limitado a la configuración de Operations Manager; capacidad para invalidar reglas; monitores para los destinos o grupos de destinos dentro del ámbito configurado. El operador avanzado también hereda los privilegios de operador. | Puede delimitarse el ámbito en relación a cualquier grupo, vista y tarea presentes actualmente y a aquellos importados en el futuro. |
| Autor | Tiene capacidad para crear, editar y eliminar tareas, reglas, monitores y vistas dentro del ámbito configurado. El autor también hereda los privilegios del operador avanzado. | Puede delimitarse el ámbito en relación a cualquier destino, grupo, vista y tarea presentes actualmente y a aquellos importados en el futuro. La función Autor es única en el sentido de que es el único tipo de perfil cuyo ámbito puede delimitarse en relación a los destinos. |
| Operador | Tiene la capacidad de editar o eliminar alertas, ejecutar tareas y obtener acceso a vistas en función del ámbito configurado. El operador también hereda los privilegios del operador de sólo lectura. | Puede delimitarse el ámbito en relación a cualquier grupo, vista y tarea presentes actualmente y a aquellos importados en el futuro. |
| Operador de sólo lectura | Tiene la capacidad de ver alertas y obtener acceso a vistas en función del ámbito configurado. | Puede delimitarse el ámbito en relación a cualquier grupo y vista presentes actualmente y a aquellos importados en el futuro. |
| Operador de informes | Tiene la capacidad de ver informes en función del ámbito configurado. | Ámbito global. |
| Administrador de seguridad de informes | Permite la integración de seguridad de SQL Reporting Services con funciones de Operations Manager. | Sin ámbito. |

Importante

Agregar una cuenta de equipo a un miembro de función de usuario permite a todos los servicios de ese equipo disponer de acceso SDK. Se recomienda no agregar cuentas de equipo a ninguna función de usuario.

Excepto en el caso de la función Administrador, puede agregar grupos de seguridad de Active Directory o cuentas individuales a cualquiera de estas funciones predeterminadas. Puede agregar grupos de seguridad de Active Directory solamente a la función Administrador.

Agregar usuarios o un grupo a una función significa que esas cuentas individuales podrán ejercer los privilegios de función proporcionados a través del ámbito de los objetos (incluidos los objetos heredados).

Nota

Las funciones predeterminadas tienen un ámbito global, lo que les proporciona acceso a todos los grupos, vistas, destinos y tareas, excepto Administrador de seguridad de informes.

Operations Manager también le permite crear funciones personalizadas basadas en los perfiles Operador, Operador de sólo lectura, Autor y Operador avanzado. Al crear la función, podrá precisar mejor el ámbito de los grupos, tareas y vistas a los que la función puede tener acceso. Por ejemplo, puede crear una función denominada "Operador de Exchange" y precisar el ámbito a sólo vistas, tareas y grupos relacionados con Exchange. Las cuentas de usuario asignadas a esta función sólo podrán ejecutar acciones de nivel de operador en objetos relacionados con Exchange.

Importante

Asegúrese de crear un grupo de seguridad de dominios para la función Administradores de Operations Manager. Este grupo se debe crear cuando se ejecute por primera vez la instalación para un grupo de administración.

Para obtener más información sobre cómo administrar funciones de seguridad, cuentas y perfiles en Operations Manager 2007, consulte el tema [Administración de funciones de seguridad, cuentas y perfiles en Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=88131) (http://go.microsoft.com/fwlink/?LinkId=88131).

Run As Accounts and Run As Profiles in Operations Manager 2007 (Perfiles de ejecución y cuentas de ejecución en Operations Manager 2007)

Los monitores, reglas, tareas y detecciones definidos en un módulo de administración requieren credenciales para ejecutarse en un equipo de destino. De forma predeterminada, los monitores, reglas, tareas y detecciones se ejecutan mediante la cuenta de acción predeterminada para el agente o el servidor. Por ejemplo, si la acción se ejecuta en un agente, las credenciales usadas para la acción procederán de la cuenta de acción del agente. Para obtener más información sobre la cuenta de acción, consulte [Información sobre cuentas para Operations Manager 2007](#zbe2bbe81fe1a48e7b2cd3c8a3eab2255) en esta guía.

Las cuentas y los perfiles de ejecución permiten ejecutar diferentes reglas, tareas, monitores o detecciones en distintas cuentas de distintos equipos. Los módulos de administración ya no comparten la misma identidad y, por lo tanto, le permiten usar una cuenta de privilegios bajos como su cuenta de acción. Las cuentas de ejecución admiten los siguientes tipos de cuentas:

 Windows - credenciales de Windows, por ejemplo, dominio\nombre de usuario, o nombre de usuario@Nombrededominiocompleto, y la contraseña asociada

 Cadena de comunidad - cadena de comunidad de SNMP versión 2

 Autenticación básica - autenticación web básica estándar

 Autenticación simple - cualquier combinación genérica de nombre de usuario y contraseña, por ejemplo, formulario web, autenticación de SQL, o cualquier otra combinación que acepte el nombre de usuario y la contraseña

 Autenticación de texto - autenticación web de texto estándar

 Autenticación binaria - autenticación definida por el usuario

 Cuenta de acción - credencial de Windows que sólo se puede asignar al perfil de cuenta de acción

Una cuenta de ejecución le permite especificar los privilegios necesarios para usarla con reglas, tareas, monitores y detecciones destinados a equipos específicos según se considere necesario.

Los datos se cifran entre el servidor de administración raíz y el equipo de destino cuando las credenciales se transfieren y las credenciales se almacenan de forma segura en el equipo de destino.

Una tarea, función, monitor o detección determinada se puede asociar con un perfil de ejecución. La asociación se realiza cuando se crea el módulo de administración. El administrador de Operations Manager tiene la opción de asociar otras cuentas de ejecución para el perfil de ejecución determinado en un equipo de destino.

Por ejemplo, Alice está trabajando en un módulo de administración de SQL y está creando una tarea de obtención de estadísticas de bases de datos. Alice sabe que la cuenta de acción no tendrá derechos suficientes para ejecutar esta tarea; sin embargo, Bob, el administrador de SQL, sí los tiene. Alice tiene que configurar la tarea para que se ejecute con las credenciales de Bob.

Al crear el módulo de administración, Sam crea un perfil de ejecución denominado Operadores de base de datos y lo asocia al módulo de tarea. Cuando se importa en Operations Manager 2007 el módulo de administración de SQL que contiene la tarea de obtención de estadísticas de bases de datos, el perfil de ejecución asociado a la tarea se incluirá en la importación y Operadores de base de datos aparecerá en la lista de perfiles de ejecución disponibles.

El administrador de Operations Manager 2007 creará una cuenta de ejecución configurada con las credenciales de Alice. A continuación, se asocia la cuenta de ejecución con el perfil de ejecución que usará la tarea. También se especifica explícitamente en el perfil de ejecución el equipo de destino donde se usará la cuenta de ejecución.

Nota

La cuenta predeterminada para el perfil de ejecución es la cuenta de acción. Piense convenientemente qué cuenta de acción se debe seleccionar y elija una cuenta con permisos adecuados. En la mayoría de los casos, un administrador de dominio no sería una buena opción.

Los administradores de Operations Manager 2007 pueden asociar diferentes cuentas de ejecución para distintos equipos de destino con cada perfil de ejecución. Esta asociación resulta útil en los casos en los que se usa el perfil de ejecución en distintos equipos y cada uno de ellos requiere una credencial diferente. Alice tiene derechos de usuario para ejecutar la tarea en el equipo 1 que ejecuta SQL Server, mientras que Bob tiene derechos de usuario en el equipo 2 que ejecuta SQL Server. En esta situación, se crean cuentas de ejecución independientes para Alice y para Bob y ambas se asocian a un único perfil de ejecución. Esta asignación se debe realizar en dos equipos independientes.

Perfiles de ejecución en Operations Manager 2007

Además de los perfiles de ejecución creados, Operations Manager 2007 incluye los perfiles de ejecución descritos en la tabla siguiente. Estos perfiles los usa el propio Operations Manager 2007

|  |  |  |
| --- | --- | --- |
| Nombre | Descripción | Cuenta de ejecución |
| Cuenta de Active Directory basada en asignación de agentes | Cuenta usada por Active Directory basada en el módulo de asignación de agentes para publicar la configuración de asignación en Active Directory. | Cuenta de Windows del sistema local |
| Cuenta de administración de agente automática | Esta cuenta se usará para diagnosticar automáticamente errores de agentes. | Ninguna |
| Cuenta de acción de supervisión de clientes | Si se especifica, Operations Manager 2007 la usa para ejecutar todos los módulos de supervisión de clientes. Si no se especifica, Operations Manager 2007 usa la cuenta de acción predeterminada. | Ninguna |
| Cuenta de grupo de administración conectado | El módulo de administración de Operations Manager usa esta cuenta para supervisar el estado de la conexión a los grupos de administración conectados.  | Ninguna |
| Cuenta de almacenamiento de datos | Si se especifica, esta cuenta se usa para ejecutar todas las reglas de recopilación y sincronización de almacenamiento de datos en lugar de la cuenta de acción predeterminada. Si la cuenta de autenticación de SQL Server de almacenamiento de datos no invalida esta cuenta, las reglas de recopilación y sincronización usan esta cuenta para conectar a las bases de datos de almacenamiento de datos mediante la autenticación de Windows integrada. | Ninguna |
| Cuenta de implementación de informes de almacenamiento de datos | Los procedimientos de autoimplementación de informes de almacenamiento de datos usan esta cuenta para ejecutar distintas operaciones relacionadas con la implementación de informes. | Cuenta de implementación de informes de almacenamiento de datos |
| Cuenta de autenticación de SQL Server de almacenamiento de datos | Si se especifica, las reglas de recopilación y sincronización usan este nombre y contraseña de inicio de sesión para conectar a las bases de datos de almacenamiento de datos mediante la autenticación de SQL Server. | Cuenta de autenticación de SQL Server de almacenamiento de datos |
| Cuenta de acción predeterminada | Cuenta de acción predeterminada del servicio de mantenimiento | Las credenciales de la cuenta proporcionadas durante la instalación. |
| Cuenta de acción de actualizaciones del módulo de administración | El notificador de actualizaciones del módulo de administración usa esta cuenta. | Ninguna |
| Cuenta de notificación | Cuenta de Windows usada por las reglas de notificación. Use la dirección de correo electrónico de esta cuenta como dirección de remitente de correo electrónico y mensaje instantáneo. | Ninguna |
| Cuenta de base de datos operativa | Esta cuenta se usa para leer y escribir información en la base de datos OperationsManager. | Ninguna |
| Cuenta de supervisión con privilegios | Este perfil se usa para supervisar lo que sólo se puede realizar en un sistema con un alto nivel de privilegios, por ejemplo supervisar que se requieran permisos de sistema local o de administrador local. Este perfil usa Sistema local como valor predeterminado a menos que se invalide de forma específica para un sistema de destino. | Ninguna |
| Cuenta de autenticación de SQL Server de SDK de informes | Si se especifica, el servicio SDK usa este nombre y contraseña de inicio de sesión para conectar a las bases de datos de almacenamiento de datos mediante la autenticación de SQL Server. | Cuenta de autenticación de SQL Server de SDK de informes |
| Reservado | Este perfil está reservado y no debe usarse. | Ninguna |
| Cuenta de suscripción de alerta de validación | Cuenta usada por el módulo de suscripción de alerta de validación que valida que la suscripciones de notificación están en el ámbito. Este perfil necesita derechos de administrador. | Cuenta de Windows del sistema local |
| Cuenta de acción de Windows Cluster | Este perfil se usa para todas las detecciones y supervisiones de los componentes de Windows Cluster. Este perfil usa las cuentas de acción usadas de forma predeterminada, a menos que el usuario lo rellene específicamente. | Ninguna |
| Cuenta de acción de WS-Management | Este perfil se usa para el acceso a WS-Management. | Ninguna |

Perfiles de ejecución y cuentas de ejecución en Operations Manager 2007 R2

En Operations Manager 2007 R2, se han agregado las siguientes características adicionales para cuentas de ejecución y perfiles de ejecución: distribución y establecimiento de destinos. Las secciones siguientes explican la distribución y el establecimiento de destinos y los efectos que estas características tienen en la seguridad.

Información sobre la distribución y el establecimiento de destinos

Tanto la distribución como el establecimiento de destino de la cuenta de ejecución se deben configurar correctamente para que el perfil de ejecución funcione correctamente.

Cuando configure un perfil de ejecución, debe seleccionar las cuentas de ejecución que desea asociar con el perfil de ejecución. Después de crear esa asociación podrá especificar la clase, el grupo o el objeto sobre el que se deberá usar la cuenta de ejecución para ejecutar tareas, reglas, monitores y detecciones.

La distribución es un atributo de una cuenta de ejecución y en ese atributo puede especificar qué equipos recibirán las credenciales de cuenta de ejecución. Puede elegir la distribución de credenciales de cuenta de ejecución a todos los equipos administrados por agentes o sólo a los equipos seleccionados.

Ejemplo de establecimiento de destino de la cuenta de ejecución: el equipo físico ABC hospeda dos instancias de Microsoft SQL Server, la instancia X y la instancia Y. Cada instancia usa un conjunto de credenciales diferente para la cuenta sa . Puede crear la cuenta de ejecución con las credenciales de sa para la instancia X y una cuenta de ejecución diferente con las credenciales sa para la instancia Y. Cuando configure el perfil de ejecución de SQL Server, deberá asociar las credenciales de la cuenta de ejecución, por ejemplo X e Y, con el perfil y deberá especificar que las credenciales de la instancia X de la cuenta de ejecución deben usarse para la instancia X de SQL Server y que las credenciales Y de la cuenta de ejecución deben usarse para la instancia Y de SQL Server. A continuación, también deberá configurar cada conjunto de credenciales de cuenta de ejecución para que se distribuya al equipo físico ABC.

Ejemplo de distribución de la cuenta de ejecución: SQL Server1 y SQL Server2 son dos equipos físicos diferentes. SQL Server1 usa el conjunto de credenciales NombreUsuario1 y Contraseña1 para la cuenta sa de SQL. SQL Server2 usa el conjunto de credenciales NombreUsuario2 y Contraseña2 para la cuenta sa de SQL. El módulo de administración de SQL tiene un único perfil de ejecución que se usa para todos los servidores SQL Server. A continuación puede definir una cuenta de ejecución para el conjunto de credenciales NombreUsuario1 y otra cuenta de ejecución para el conjunto de credenciales NombreUsuario2. Estas dos cuentas de ejecución se pueden asociar con el perfil de ejecución de SQL Server y se pueden configurar para que se distribuyan a los equipos adecuados. Es decir, NombreUsuario1 se distribuye a SQL Server1 y NombreUsuario2 se distribuye a SQL Server2. La información de las cuentas que se transmite entre el servidor de administración y el equipo designado está cifrada.

Seguridad de la cuenta de ejecución

En Operations Manager 2007 SP1, las credenciales de cuenta de ejecución se distribuyen a todos los equipos administrados por agente (la opción menos segura). En Operations Manager 2007 R2, las credenciales de cuenta de ejecución se distribuyen sólo a los equipos especificados (la opción más segura). Si Operations Manager distribuyera automáticamente la cuenta de ejecución de acuerdo con la detección, se plantearía un riesgo para la seguridad, como se muestra en el siguiente ejemplo. Por ese motivo no se incluyó la opción de distribución automática en Operations Manager.

Por ejemplo, Operations Manager 2007 identifica un equipo como host de SQL Server 2005 basándose en la presencia de una clave del Registro. Se puede crear esa misma clave del Registro en un equipo que no ejecuta realmente una instancia de SQL Server 2005. Si Operations Manager distribuyera automáticamente las credenciales a todos los equipos administrados por agentes identificados como equipos de SQL Server 2005, las credenciales se enviarían al SQL Server impostor y estarían disponibles para cualquier persona con derechos de administrador en ese servidor.

Cuando cree una cuenta de ejecución mediante Operations Manager 2007 R2, se le pedirá que elija si la cuenta de ejecución debe tratarse de un modo Menos seguro o Más seguro. "Más seguro" significa que cuando asocia la cuenta de ejecución con un perfil de ejecución, tiene que proporcionar los nombres de equipo específicos a los que desea que se distribuyan las credenciales de ejecución. Al identificar positivamente los equipos de destino, puede evitar el escenario de suplantación de identidad descrito anteriormente. Si elige la opción menos segura, no tendrá que proporcionar equipos específicos y las credenciales se distribuirán a todos los equipos administrados por agentes.

Nota

En todas las versiones de Operations Manager 2007, las credenciales que seleccione como cuenta de ejecución deben disponer de derechos de inicio de sesión local, ya que, en caso contrario, se producirá un error en el módulo.

Vea también

[Información sobre cuentas para Operations Manager 2007](#zbe2bbe81fe1a48e7b2cd3c8a3eab2255)

[Seguridad basada en funciones en Operations Manager 2007](#zd49361c238194d14a23a10cf4573c424)

Creación de una cuenta de ejecución en Operations Manager 2007

En este procedimiento se describe la creación de una cuenta de ejecución con un conjunto de credenciales de Windows como ejemplo. A continuación, se muestra la edición de las propiedades de la cuenta de ejecución para modificar el nivel de seguridad y la distribución de las credenciales. Se sigue el mismo procedimiento para todos los otros tipos de cuentas. Para obtener más información acerca de otros tipos de cuenta, consulte Tipos de credenciales en Operations Manager 2007.

Las credenciales que se proporcionan en una cuenta de ejecución se utilizan para ejecutar tareas, reglas, monitores y detecciones definidas en el módulo de administración en el que se encuentran. La guía del módulo de administración tiene la configuración necesaria para configurar la cuenta de ejecución y el perfil de ejecución.

Para crear una cuenta de ejecución

|  |
| --- |
| 1. Inicie una sesión en la consola de Operations con una cuenta que sea miembro de la función Administradores de Operations Manager para el grupo de administración de Operations Manager 2007.2. En la consola de Operations, haga clic en Administración.3. En el panel Administración, expanda Administración y Configuración de ejecución, haga clic con el botón secundario en Cuentas y, a continuación, haga clic en Crear cuenta de ejecución4. En la página Introducción del Asistente para crear cuentas de ejecución, haga clic en Siguiente.5. En la página Propiedades generales, realice la acción siguiente:a. Seleccione Windows en la lista Tipo de cuenta de ejecución.b. Escriba un nombre para mostrar en el cuadro de diálogo Nombre para mostrar. c. Si lo desea, escriba una descripción en el cuadro de texto Descripción.d. Haga clic en Siguiente.6. En la página Credenciales, escriba un nombre de usuario y una contraseña y, a continuación, seleccione el dominio de la cuenta que desee convertir en miembro de esta cuenta de ejecución.7. Haga clic en Siguiente.8. En la página Seguridad de distribución, seleccione Menos seguro o Más seguro según corresponda.9. Haga clic en Crear.10. En la página Progreso de creación de la cuenta de ejecución haga clic en Cerrar. |

Cuando crea una cuenta de ejecución se le indica que debe asociar la cuenta de ejecución con el perfil de ejecución, pero no aparece una opción para configurar la distribución de credenciales de la cuenta de ejecución. Ambas actividades se pueden llevar a cabo en el Asistente para configuración de perfil de ejecución. También se puede configurar la distribución de credenciales de la cuenta de ejecución editando las propiedades de la cuenta de ejecución como se muestra a continuación.

Para modificar las propiedades de la cuenta de ejecución

|  |
| --- |
| 1. En la consola de Operations, haga clic en Administración.2. En el panel Administración, expanda el nodo Administración y Configuración de ejecución, y seleccione el contenedor Cuentas.3. En el panel de resultados, haga doble clic en la cuenta de ejecución que desea editar para abrir las propiedades.4. En la página Propiedades de la cuenta de ejecución, puede editar los valores en las fichas Propiedades generales, Credenciales o Distribución. En este caso, seleccione la ficha Distribución.5. En la ficha Distribución, en el área Equipos seleccionados:, haga clic en Agregar para abrir la herramienta Búsqueda de equipos. 6. En la página Búsqueda de equipos, haga clic en la lista Opción: y seleccione una de las siguientes opciones:a. Buscar por nombre de equipo (predeterminado), luego escriba el nombre del equipo en el cuadro de texto Filtrar por: (opcional). b. Mostrar equipos sugeridos, si ya ha asociado el objeto de la cuenta de ejecución con un perfil de ejecución, se muestra aquí una lista de los equipos detectados que alojan el servicio supervisado.c. Mostrar servidores de administración, en algunos casos, por ejemplo, en la supervisión de varias plataformas, un servidor de administración realiza toda la supervisión y, por lo tanto, las credenciales se deben distribuir al servidor de administración que realiza la supervisión.7. Si lo desea, escriba un valor en el cuadro de texto Filtrar por: (opcional) para limitar los resultados y haga clic en Buscar. En el cuadro de texto Elementos disponibles se muestra una lista de equipos que se ajustan a los criterios de búsqueda.8. Seleccione los equipos a los que desea distribuir las credenciales y haga clic en Agregar. Los equipos aparecen en el cuadro de texto Elementos seleccionados.9. Haga clic en Aceptar. Entonces, regresa a la ficha Distribución y se muestran los equipos. Haga clic en Aceptar. |

Vea también

[Creación y configuración de un perfil de ejecución en Operations Manager 2007](#z2225e1098c6b4be08b7ff9ef553067dc)

Creación y configuración de un perfil de ejecución en Operations Manager 2007

El proceso de creación y configuración de un perfil de ejecución personalizado consta de cuatro pasos:

1. Identificar la clase, el grupo o los objetos a los que se aplicará la cuenta de ejecución.

2. Crear y configurar cuentas de ejecución.

3. Asociar las cuentas de ejecución con el perfil de ejecución.

4. Configurar la distribución de las credenciales de objeto de cuenta de ejecución con equipos específicos.

Este procedimiento se puede usar para crear y configurar un nuevo perfil de ejecución o bien puede usar la sección de configuración para modificar o configurar perfiles de ejecución que ya existían en el grupo de administración. Este procedimiento asume que previamente no ha creado una cuenta de ejecución.

Para crear un perfil de ejecución

|  |
| --- |
| 1. Inicie una sesión en la consola de Operations con una cuenta que sea miembro de la función Administradores de Operations Manager para el grupo de administración de Operations Manager 2007.2. En la consola de Operations, haga clic en Administración.3. En el panel Administración, expanda Administración y Configuración de ejecución y seleccione el contenedor Perfiles. Haga clic con el botón secundario en el panel Resultados y, a continuación, haga clic en Crear perfil de ejecución. Si es la primera vez que ejecuta el asistente para crear perfiles de ejecución, asegúrese de leer el texto de la página Introducción.4. Haga clic en Siguiente. 5. En la página Propiedades generales, realice la acción siguiente:a. Escriba un nombre para mostrar para el perfil de ejecución en el cuadro Nombre para mostrar. b. Opcionalmente, escriba una descripción para el perfil de ejecución. c. Haga clic en Nuevo para la lista Seleccionar módulo de administración de destino para crear un módulo de administración de invalidaciones si aún no ha creado uno. Si ya ha creado un módulo de administración de invalidaciones, selecciónelo en la lista desplegable y vaya al paso 9. 6. En el Asistente para crear módulos de administración en la página Propiedades generales, escriba un nombre en el cuadro Nombre. Opcionalmente, escriba una descripción para el módulo de administración. A continuación, haga clic en Siguiente. Sugerencia De forma predeterminada, cuando crea un objeto de módulo de administración, deshabilita una regla o monitor, o bien crea una invalidación, Operations Manager guarda el parámetro en el módulo de administración predeterminado. En lugar de ello, se recomienda crear un módulo de administración independiente para cada módulo de administración sellado que desee personalizar, en lugar de guardar la configuración personalizada en el módulo de administración predeterminado. Para obtener más información, consulte Customizing Management Packs (Personalizar módulos de administración) [http://go.microsoft.com/fwlink/?LinkId=140601 (puede estar en inglés)](http://go.microsoft.com/fwlink/?LinkId=140601) 7. En la página Artículo de conocimientos, haga clic en Editar si desea proporcionar un resumen, configuración, información adicional e información de orígenes de conocimientos externos acerca de este módulo de administración. 8. Haga clic en Crear. Volverá a la página Propiedades generales del asistente para crear perfiles de ejecución. 9. Haga clic en Siguiente. 10. En la página Cuentas de ejecución, haga clic en Agregar para abrir la página Agregar una cuenta de ejecución. 11. Haga clic en Nuevo que inicia el Asistente para crear cuentas de ejecución y abre la página Propiedades generales. 12. En el cuadro Tipo de cuenta de ejecución, seleccione el tipo de cuenta que necesita crear. Se especifica en la guía del módulo de administración. 13. Escriba un nombre en el cuadro de texto Nombre para mostrar:, opcionalmente escriba una descripción y, a continuación, haga clic en Siguiente. 14. En la página Credenciales escriba el nombre de usuario y la contraseña de la credencial real que desee que el perfil de ejecución use en los cuadros de texto Nombre de usuario, Contraseña y Confirmar contraseña respectivos. 15. Asegúrese de que se haya seleccionado el dominio correcto para las credenciales en la lista Dominio. Haga clic en Siguiente. 16. En la página Seguridad de distribución, seleccione la opción Menos seguro o Más seguro tal y como le indique la guía del módulo de administración. Tenga en cuenta que si elige la opción Menos seguro, las credenciales son accesibles para los administradores de los equipos de todos los destinatarios. Para obtener más información acerca de la seguridad de la distribución de credenciales, consulte Perfiles de ejecución y cuentas de ejecución en Operations Manager 2007. 17. Haga clic en Crear 18. En la página Progreso de creación de la cuenta de ejecución, cuando se haya completado la creación, lea la nota de advertencia y, a continuación, haga clic en Cerrar. Volverá a la página Agregar una cuenta de ejecución. 19. En el área Esta cuenta de ejecución se usará para administrar los siguientes objetos seleccione las opciones Todos los objetos con destino o Una clase, grupo u objeto seleccionado, de acuerdo con los valores de configuración de la guía del módulo de administración. 20. Si el cuadro Una clase, grupo u objeto seleccionado se ha rellenado previamente con un valor, haga clic en Aceptar; de lo contrario, haga clic en Seleccionar y seleccione Clase, Grupo u Objeto de acuerdo con las instrucciones de la guía de administración. Se abrirá la página respectiva Búsqueda de clases, Búsqueda de grupos o Búsqueda de objetos. 21. En cualquiera de las herramientas de búsqueda, escriba el criterio de búsqueda o de filtro y haga clic en Buscar. Los resultados se muestran en el cuadro Elementos disponibles. 22. Seleccione el elemento que desee que use el objeto de cuenta de ejecución para administrar y haga clic en Aceptar. 23. Haga clic en Aceptar. Volverá a la página Cuentas de ejecución del Asistente para crear perfiles de ejecución. 24. Si desea agregar cuentas de ejecución adicionales, vuelva a hacer clic en Agregar y repita los pasos 10 a 23; de lo contrario, haga clic en Crear. Nota Este procedimiento asume que ha seleccionado la opción Más seguro y presenta los pasos restantes en orden. Si ha seleccionado la opción Menos seguro vaya al paso 29. 25. En la página Finalización del asistente para crear perfiles de ejecución verá las cuentas de ejecución que se configuraron con el valor Más seguro mostrado como un vínculo. Ahora se debe seleccionar cada cuenta de ejecución de una en una y configurar la distribución de credenciales. 26. Haga doble clic en una cuenta; se abrirá la página Propiedades de la cuenta de ejecución en la ficha Distribución. Verá la selección del nivel de seguridad y los Equipos seleccionados mostrados. Ambos se pueden editar desde aquí. 27. Haga clic en Agregar para el cuadro Equipos seleccionados y realice lo siguiente: a. Seleccione Buscar por nombre de equipo (predeterminado) o Mostrar equipos sugeridos o Mostrar servidores de administración. b. Opcionalmente, escriba un valor en el cuadro de texto Filtrar por: (Opcional). c. Haga clic en Buscar. El conjunto de resultados se devuelve en el cuadro de texto Elementos disponibles. d. Seleccione los equipos que desee del conjunto de resultados y haga clic en Agregar. Los equipos seleccionados se agregarán al cuadro Objetos seleccionados. e. Haga clic en Aceptar. 28. Haga clic en Aceptar. Volverá a la página Finalización del Asistente para crear perfiles de ejecución. Aparecerá una marca de verificación verde al lado de las cuentas para las que haya completado correctamente la configuración de distribución. 29. Haga clic en Cerrar.  |

Vea también

[Creación de una cuenta de ejecución en Operations Manager 2007](#z036d02fdd2654e769099cf8552c86c6d)

[Modificación de un perfil de ejecución existente](#z2fa6561a0f6c468289f7973f1cd8a748)

Modificación de un perfil de ejecución existente

Es posible que los perfiles de ejecución existentes se hayan creado usando el procedimiento Creación y configuración de un perfil de ejecución o tal vez se hayan creado si se importó un módulo de administración que contenía uno. Utilice este procedimiento para modificar las propiedades de un perfil de ejecución existente.

Modificación de un perfil de ejecución existente

|  |
| --- |
| 1. Abra la consola de Operations con una cuenta que sea miembro del grupo de administradores de Operations Manager 2007. 2. Seleccione la vista Administración. 3. En el panel de navegación de la vista Administración, seleccione el contenedor Perfiles. 4. En el panel de resultados, haga doble clic en los perfiles a los que desee editar las propiedades. Esto abre el Asistente para perfiles de ejecución que contiene la configuración anterior. 5. En la página Propiedades generales, puede modificar el valor en los campos Nombre para mostrar y Descripción. 6. Haga clic en Siguiente. 7. En la página Cuentas de ejecución, puede agregar cuentas de ejecución adicionales, editar la configuración de las cuentas existentes y eliminar las cuentas de ejecución que no se deberían asociar con el perfil de ejecución. 8. Una vez realizados los cambios, haga clic en Guardar. 9. En la página Finalización, en el cuadro de texto Cuentas de ejecución más seguras: debe seleccionar cada cuenta y configurar la distribución de las credenciales para cada cuenta de ejecución. Para obtener más información acerca de la configuración de la distribución de credenciales de la cuenta de ejecución, consulte: [Creación y configuración de un perfil de ejecución en Operations Manager 2007](#z2225e1098c6b4be08b7ff9ef553067dc) 10. Una vez configurada la distribución, haga clic en Cerrar.  |

Autenticación y cifrado de datos para equipos de Windows en Operations Manager 2007

Operations Manager 2007 consta de componentes como el servidor de administración raíz, el servidor de administración, el servidor de puerta de enlace, el servidor de informes, la base de datos OperationsManager, el almacenamiento de datos de informes, el agente, la consola web y la consola de Operations. Esta sección explica cómo se realiza la autenticación e identifica los canales de conexión donde se cifran los datos.

Autenticación basada en certificado

Cuando un agente de Operations Manager y un servidor de administración están separados por un bosque que no es de confianza o un límite de grupo de trabajo, es necesario implementar la autenticación basada en certificado. Las secciones siguientes proporcionan información sobre estas situaciones y procedimientos específicos para obtener e instalar certificados de autoridades de certificación basadas en Windows.

Configuración de la comunicación entre agentes y servidores de administración dentro del mismo límite de confianza

Un agente y el servidor de administración usan la autenticación de Windows para autenticarse mutuamente entre sí antes de que el servidor de administración acepte datos del agente. El protocolo Kerberos versión 5 es el método predeterminado para proporcionar autenticación. Para que funcione la autenticación mutua basada en Kerberos, los agentes y el servidor de administración se deben instalar en un dominio de Active Directory. Si un agente y un servidor de administración están en dominios separados, debe existir plena confianza entre los dominios. En este escenario, después de que se haya realizado la autenticación mutua, se cifra el canal de datos entre el agente y el servidor de administración. No se requiere la intervención del usuario para que se realicen la autenticación y el cifrado.

Configuración de la comunicación entre agentes y servidores de administración a través de límites de confianza

Un agente (o agentes) pueden implementarse en un dominio (dominio B) separado del servidor de administración (dominio A) y es posible que no exista confianza bidireccional entre los dominios. Al no haber confianza entre los dos dominios, los agentes de un dominio no se pueden autenticar en el servidor de administración del otro dominio mediante el protocolo Kerberos. La autenticación mutua entre los componentes de Operations Manager 2007 dentro de cada dominio se sigue produciendo.

Una solución a esta situación es instalar un servidor de administración en el mismo dominio en el que residen los agentes e instalar certificados en el servidor de puerta de enlace y el servidor de administración para conseguir autenticación mutua y cifrado de datos. El uso del servidor de puerta de enlace significa que sólo se necesita un certificado en el dominio B y sólo un puerto a través del firewall, como se muestra en la ilustración siguiente.



Para obtener más información, consulte los temas siguientes de esta guía de seguridad:

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2003 en Operations Manager 2007](#z5686fe43d94145eda9380548abf07708)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2003 en Operations Manager 2007](#zb983d345d4b049ff94c88ab56016aceb)

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2008 en Operations Manager 2007](#z3067b41c6eab4cd0a3e5538b57af9b09)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2008 en Operations Manager 2007](#z9d62a00496b3479095d6f05f17eeb77a)

Configuración de la comunicación a través de un dominio – Límite de grupo de trabajo

En su entorno, es posible que tenga uno o dos agentes implementados en un grupo de trabajo dentro de su firewall. El agente del grupo de trabajo no puede autenticarse en el servidor de administración del dominio que usa el protocolo Kerberos. Una solución para esta situación es instalar certificados tanto en el equipo que hospeda el agente como en el servidor de administración al que se conecta el agente, como se muestra en la ilustración siguiente.

Nota

En este escenario, se debe instalar manualmente el agente.



Realice los pasos siguientes en el equipo que hospeda el agente y en el servidor de administración que usa la misma entidad de certificación (CA) para cada uno de ellos:

 Solicite certificados de la CA.

 Apruebe las solicitudes de certificado de la CA.

 Instale los certificados aprobados en los almacenes de certificados del equipo.

 Use la herramienta MOMCertImport para configurar Operations Manager 2007.

Estos son los mismos pasos necesarios para la instalación de certificados en un servidor de puerta de enlace, excepto en que en este caso, no se instala o ejecuta la herramienta de aprobación de la puerta de enlace. Para obtener más información, consulte los temas siguientes de esta guía de seguridad:

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2003 en Operations Manager 2007](#z5686fe43d94145eda9380548abf07708)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2003 en Operations Manager 2007](#zb983d345d4b049ff94c88ab56016aceb)

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2008 en Operations Manager 2007](#z3067b41c6eab4cd0a3e5538b57af9b09)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2008 en Operations Manager 2007](#z9d62a00496b3479095d6f05f17eeb77a)

Certificate Generation Wizard

Los pasos necesarios para generar, recuperar e instalar certificados están en esta guía de seguridad. Se ha diseñado un asistente para la generación de certificados para simplificar este proceso. Para obtener más información, consulte la entrada de blog [Obtaining Certificates for Non-Domain Joined Agents Made Easy With Certificate Generation Wizard (Obtención de certificados para agentes no asociados a un dominio facilitada por el asistente para la generación de certificados)](http://go.microsoft.com/fwlink/?LinkId=128392) (http://go.microsoft.com/fwlink/?LinkId=128392).

Nota

El uso del asistente para la generación de certificados se proporciona TAL Y COMO ES y no otorga ningún derecho. El uso de esta utilidad está sujeto a los términos especificados en <http://www.microsoft.com/info/cpyright.htm>

Confirmación de la instalación del certificado

Si ha instalado correctamente el certificado, se escribe el evento siguiente en el registro de eventos de Operations Manager.

|  |  |  |  |
| --- | --- | --- | --- |
| Nivel | Origen | Id. de evento | general |
| información | Conector OpsMgr | 20053 | El conector OpsMgr ha cargado correctamente el certificado de autenticación especificado. |

Durante la instalación de un certificado, se ejecuta la herramienta MOMCertImport. Cuando ha finalizado la herramienta MOMCertImport, el número de serie del certificado que importó se escribe en el registro, en la subclave siguiente.

Precaución

La modificación incorrecta del Registro puede dañar gravemente el sistema. Antes de realizar cambios en el Registro, se recomienda hacer una copia de seguridad de los datos de valor que contenga el equipo.

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Machine Settings

Autenticación y cifrado de datos entre el servidor de administración raíz, el servidor de administración, el servidor de puerta de enlace y los agentes

La comunicación entre estos componentes de Operations Manager comienza con la autenticación mutua. Si los certificados están presentes en ambos extremos del canal de comunicaciones, los certificados se usarán para autenticación mutua; de lo contrario, se usa el protocolo Kerberos versión 5.Si dos componentes están separados a través de un dominio que no es de confianza, se debe realizar la autenticación mutua mediante certificados.

Las comunicaciones normales como eventos, alertas y la implementación de un módulo de administración se producen a través de este canal. La ilustración anterior muestra un ejemplo de una aleta generada en uno de los agentes que se enruta al servidor de administración raíz (RMS). Desde el agente al servidor de puerta de enlace, el paquete de seguridad de Kerberos se utiliza para cifrar los datos, porque el servidor de puerta de enlace y el agente están en el mismo dominio. El servidor de puerta de enlace descifra la alerta, que se vuelve a cifrar mediante certificados para el servidor de administración. Una vez que el servidor de administración recibe la alerta, el servidor de administración descifra el mensaje, lo vuelve a cifrar mediante el protocolo Kerberos y lo envía al RMS, donde se descifra la alerta.

La comunicación entre el RMS y el agente puede incluir información de credenciales; por ejemplo, datos de configuración y tareas. El canal de datos entre el agente y el servidor de administración agrega otra capa de cifrado al cifrado de canal normal. No requiere la intervención del usuario.

Servidor de administración raíz y base de datos OperationsManager

La información de cuenta de ejecución se almacena en un formulario cifrado en la base de datos OperationsManager mediante un par de claves simétricas creado por Operations Manager 2007. Si fuera necesario reemplazar el servidor de administración (RMS), el nuevo RMS no podría leer los datos cifrados de la base de datos. La herramienta SecureStorageBackup, incluida en Operations Manager 2007, se usa para realizar una copia de seguridad y restaurar esta clave de cifrado.

Importante

Ejecute la herramienta SecureStorageBackup para exportar la clave del servidor de administración raíz para realizar la copia de seguridad. Sin una copia de seguridad de la clave del servidor de administración raíz, tendría que volver a especificar todos los valores de cuentas de ejecución en caso de tener que volver a generar el RMS. En entornos de mayor tamaño, esta regeneración puede implicar cientos de cuentas. Para obtener más información sobre la herramienta SecureStorageBackup, consulte el tema [How to Backup and Restore Encryption Keys in Operations Manager 2007 (Cómo realizar una copia de seguridad de las claves de cifrado y restaurar dichas claves en Operations Manager 2007)](http://go.microsoft.com/fwlink/?LinkId=87387) (http://go.microsoft.com/fwlink/?LinkId=87387).

Para obtener información sobre la recuperación de desastres que implican la pérdida del servidor de administración raíz con o sin la copia de seguridad de la clave de cifrado, consulte el artículo de Knowledge Base titulado [La clave de cifrado del servidor de administración de raíz no está disponible después de reemplazar o reinstalar el servidor de administración de raíz en Microsoft System Center Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=112310) (http://go.microsoft.com/fwlink/?LinkId=112310).

Servidor de administración raíz y consola de Operations, servidor de consola web y servidor de informes

Autenticación y cifrado de datos entre el servidor de administración raíz (RMS) y la consola de Operations, el servidor de consola web, o el servidor de informes se consigue mediante el uso de la tecnología de Windows Communication Foundation (WCF) (anteriormente con el código "Indigo"). El intento inicial de autenticación se realiza mediante el uso de credenciales del usuario. Primero se intenta el protocolo Kerberos. Si el protocolo Kerberos no funciona, se realiza otro intento mediante NTLM. Si la autenticación sigue generando error, se le solicita al usuario que proporcione credenciales. Una vez que se ha llevado a cabo la autenticación, se cifra la secuencia de datos como función del protocolo Kerberos o de SSL, si se usa NTLM.

En el caso de un servidor de informes y un RMS, después de que se ha producido la autenticación, se establece una conexión de datos entre el RMS y el servidor de informes de SQL Server. Esto se consigue mediante el uso estricto del protocolo Kerberos; por lo tanto, el RMS y el servidor de informes deben residir en dominios de confianza. Para obtener información sobre WCF, consulte el artículo de MSDN [¿Qué es Windows Communication Foundation?](http://go.microsoft.com/fwlink/?LinkId=87429) (http://go.microsoft.com/fwlink/?LinkId=87429).

Servidor de administración y almacenamiento de datos de informes

Entre un servidor de administración y el almacenamiento de datos de informes existen dos canales de comunicación:

 El proceso de host de supervisión generado por el servicio de mantenimiento en un servidor de administración o un servidor de administración raíz

 El servicio SDK en el servidor de administración raíz

Proceso de host de supervisión y almacenamiento de datos de informes

De forma predeterminada, el proceso de host de supervisión generado por el servicio de mantenimiento, que es responsable de escribir eventos recopilados y contadores de informes en el almacenamiento de datos, consigue la autenticación de Windows integrada al ejecutarse como la cuenta de escritura de datos especificada durante la instalación de Reporting. La credencial de la cuenta está almacenada de forma segura en una cuenta de ejecución denominada Cuenta de acción de almacenamiento de datos. Esta cuenta de ejecución es miembro de un perfil de ejecución denominado Cuenta de almacenamiento de datos (que está asociada con las reglas de recopilación reales).

Si el almacenamiento de datos de informes y el servidor de administración están separados por un límite de confianza (por ejemplo, cada uno reside en dominios diferentes sin confianza), no funcionará la autenticación de Windows integrada. Para solucionar esta situación, el proceso de host de supervisión se puede conectar al almacenamiento de datos de informes mediante la autenticación de SQL Server. Para ello, cree una nueva cuenta de ejecución (del tipo Cuenta simple) con la credencial de cuenta SQL y conviértala en miembro del perfil de ejecución denominado Cuenta de autenticación de SQL Server de almacenamiento de datos, con el servidor de administración como el equipo de destino.

Importante

De forma predeterminada, al perfil de ejecución Cuenta de autenticación de SQL Server de almacenamiento de datos se le asignó una cuenta especial a través del uso de la cuenta de ejecución del mismo nombre. Nunca realice cambios en la cuenta asociada con la cuenta de ejecución, Cuenta de autenticación de SQL Server de almacenamiento de datos. En su lugar, cree su propia cuenta y su propia cuenta de ejecución y convierta a la cuenta de ejecución en miembro del perfil de ejecución Cuenta de autenticación de SQL Server de almacenamiento de datos al configurar la autenticación de SQL Server.

A continuación, se describe la relación de las diversas credenciales de cuenta, cuentas de ejecución y perfiles de ejecución para la autenticación de Windows integrada y la autenticación de SQL Server.

Valor predeterminado: Autenticación de Windows integrada

Perfil de ejecución: Cuenta de almacenamiento de datos

     Cuenta de ejecución: Cuenta de acción de almacenamiento de datos

          Credenciales: Cuenta de escritura de datos (especificada durante la instalación)

Perfil de ejecución: Cuenta de autenticación de SQL Server de almacenamiento de datos

     Cuenta de ejecución: Cuenta de autenticación de SQL Server de almacenamiento de datos

          Credenciales: Cuenta especial creada por Operations Manager (no la cambie)

Opcional: Autenticación de SQL Server

Perfil de ejecución: Cuenta de autenticación de SQL Server de almacenamiento de datos

     Cuenta de ejecución: Una cuenta de ejecución creada.

          Credenciales: Una cuenta creada.

El servicio de acceso de datos de System Center o el servicio SDK y el almacenamiento de datos de informes

El servicio SDK que se encuentra en Operations Manager 2007 SP1 se denomina servicio de acceso de datos de System Center en Operations Manager 2007 R2.

De forma predeterminada, el servicio de acceso de datos de System Center, o el servicio SDK, que es responsable de la lectura de datos del almacenamiento de datos de informes y de que estén disponibles en el área de parámetros de informe, consigue la autenticación de Windows integrada al ejecutarse como la cuenta de configuración y SDK definida durante la instalación de Operations Manager 2007.

Si el almacenamiento de datos de informes y el servidor de administración están separados por un límite de confianza (por ejemplo, cada uno reside en dominios diferentes sin confianza), no funcionará la autenticación integrada de Windows. Para solucionar esta situación, el servicio de acceso de datos de System Center o el servicio SDK se pueden conectar al almacenamiento de datos de informes mediante la autenticación de SQL Server. Para ello, cree una nueva cuenta de ejecución (del tipo Cuenta simple) con la credencial de cuenta SQL y conviértala en miembro del perfil de ejecución denominado Cuenta de autenticación de SQL Server de informes SDK, con el servidor de administración como el equipo de destino.

Importante

De forma predeterminada, al perfil de ejecución Cuenta de autenticación de SQL Server de informes SDK se le asignó una cuenta especial a través del uso de la cuenta de ejecución del mismo nombre. Nunca realice cambios en la cuenta asociada con la cuenta de ejecución Cuenta de autenticación de SQL Server de informes SDK. En su lugar, cree su propia cuenta y su propia cuenta de ejecución y convierta a la cuenta de ejecución en miembro del perfil de ejecución Cuenta de autenticación de SQL Server de informes SDK al configurar la autenticación de SQL Server.

A continuación, se describe la relación de las diversas credenciales de cuenta, cuentas de ejecución y perfiles de ejecución para la autenticación de Windows integrada y la autenticación de SQL Server.

Valor predeterminado: Autenticación de Windows integrada

Cuenta de servicio de configuración y SDK (definida durante la instalación de Operations Manager)

Perfil de ejecución: Cuenta de autenticación de SQL Server de SDK de informes

     Cuenta de ejecución: Cuenta de autenticación de SQL Server de SDK de informes

          Credenciales: Cuenta especial creada por Operations Manager (no la cambie)

Opcional: Autenticación de SQL Server

Perfil de ejecución: Cuenta de autenticación de SQL Server de almacenamiento de datos

     Cuenta de ejecución: Una cuenta de ejecución creada.

          Credenciales: Una cuenta creada.

Consola de Operations y servidor de informes

La consola de Operations se conecta al servidor de informes en el puerto 80 mediante HTTP. La autenticación se realiza mediante la autenticación de Windows. Los datos se pueden cifrar mediante el canal SSL. Para obtener más información sobre el uso de SSL entre la consola de Operations y el servidor de informes, consulte [Configuración de la consola de Operations para usar SSL cuando se conecta a un servidor de informes en Operations Manager 2007](#z6edab54f881c4a28a406f9f6005eb485) posteriormente en la guía de seguridad.

Servidor de informes y almacenamiento de datos de informes

La autenticación entre el servidor de informes y el almacenamiento de datos de informes se consigue mediante la autenticación de Windows. La cuenta que se especificó como la cuenta de lectura de datos durante la instalación de Reporting se convierte en la cuenta de ejecución del servidor de informes. Si es necesario cambiar la contraseña para la cuenta, deberá realizar el mismo cambio de contraseña mediante el administrador de configuración de Reporting Services en SQL Server 2005. Para obtener más información sobre el restablecimiento de esta contraseña, consulte [Cambio de la contraseña de la cuenta de ejecución del servidor de informes en Operations Manager 2007](#zee734cd7ec21444986691ec69f70c8d1). Los datos entre el servidor de informes y el almacenamiento de datos de informes no se cifran.

Vea también

[Cambio de la contraseña de la cuenta de ejecución del servidor de informes en Operations Manager 2007](#zee734cd7ec21444986691ec69f70c8d1)

[Configuración de la consola de Operations para usar SSL cuando se conecta a un servidor de informes en Operations Manager 2007](#z6edab54f881c4a28a406f9f6005eb485)

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2003 en Operations Manager 2007](#z5686fe43d94145eda9380548abf07708)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2003 en Operations Manager 2007](#zb983d345d4b049ff94c88ab56016aceb)

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2008 en Operations Manager 2007](#z3067b41c6eab4cd0a3e5538b57af9b09)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2008 en Operations Manager 2007](#z9d62a00496b3479095d6f05f17eeb77a)

[Eliminación de certificados importados con MOMCertImport en Operations Manager 2007](#zbafc843025be497fb5deece29c69b7e6)

Configuración de la consola de Operations para usar SSL cuando se conecta a un servidor de informes en Operations Manager 2007

Antes de configurar la consola de Operations para usar SSL cuando se conecta a un servidor de informes, debe instalar primero un certificado SSL en IIS y, a continuación, configurar la consola de Operations para usar SSL.

En el servidor de informes, inicie el Administrador de Internet Information Services (IIS) para solicitar e instalar un certificado SSL.Para obtener más información sobre cómo implementar SSL en IIS, consulte el artículo de Knowledge Base [Cómo implementar SSL en IIS](http://go.microsoft.com/fwlink/?LinkId=87862) (http://go.microsoft.com/fwlink/?LinkId=87862).

Use el procedimiento siguiente para configurar la consola de Operations para usar SSL.

Para configurar la consola de Operations para usar SSL

|  |
| --- |
| 1. Inicie una sesión en el equipo con una cuenta que sea miembro de la función de Administradores de Operations Manager para el grupo de administración de Operations Manager 2007.2. En la consola de Operations, haga clic en el botón Administración.Nota Al ejecutar la consola de Operations en un equipo que no es un servidor de administración, aparece el cuadro de diálogo Conectar a servidor. En el cuadro de texto Nombre de servidor, escriba el nombre del servidor de administración de Operations Manager 2007 al que desea que se conecte la consola.3. En el panel Administración, expanda las opciones Administración y Administración del dispositivo y, a continuación, haga clic en Configuración.4. En el panel Configuración, haga clic con el botón secundario en Informes y, a continuación, haga clic en Propiedades.5. En la ficha General , en Configuración del servidor de informes, haga clic en la lista desplegable URL del servidor de informes y seleccione https://.6. Edite la URL y reemplace :80 por :443 y, a continuación, haga clic en Aceptar. |

Vea también

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2003 en Operations Manager 2007](#z5686fe43d94145eda9380548abf07708)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2003 en Operations Manager 2007](#zb983d345d4b049ff94c88ab56016aceb)

[Eliminación de certificados importados con MOMCertImport en Operations Manager 2007](#zbafc843025be497fb5deece29c69b7e6)

Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2003 en Operations Manager 2007

Los procedimientos siguientes proporcionan los pasos necesarios para obtener un certificado de una entidad de certificación (CA) de empresa mediante Servicios de Certificate Server, que es un componente de Windows 2000 Server y Windows Server 2003. Para obtener un certificado de esta forma, debe realizar lo siguiente:

 Descargar el certificado (CA) raíz de confianza.

 Importar el certificado (CA) raíz de confianza.

 Crear una plantilla de certificados.

 Solicite un certificado de una entidad de certificación de empresa.

 Importe el certificado en Operations Manager.

Para descargar el certificado (CA) raíz de confianza

|  |
| --- |
| 1. Inicie sesión en el equipo donde ha instalado un certificado: por ejemplo, el servidor de puerta de enlace o el servidor de administración.2. Inicie Internet Explorer y conéctese al equipo que hospeda los Servicios de Certificate Server: por ejemplo, http://<nombre de servidor>/certsrv.3. En la página de bienvenida, haga clic en Descargar certificado de CA, cadena de certificados o CRL.4. En la página Descargar certificado de CA, cadena de certificados o CRL, haga clic en Método de codificación, haga clic en Base 64 y, a continuación, haga clic en Descargar cadena de certificados de CA.5. En el cuadro de diálogo Descarga de archivos, haga clic en Guardar y guarde el certificado; por ejemplo, Trustedca.p7b.6. Cuando finalice la descarga, cierre Internet Explorer. |

Para importar el certificado (CA) raíz de confianza

|  |
| --- |
| 1. En el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba mmc y, a continuación, haga clic en Aceptar.3. En la ventana Consola1, haga clic en Archivo y, a continuación, haga clic en Agregar o quitar complemento.4. En el cuadro de diálogo Agregar o quitar complemento, haga clic en Agregar.5. En el cuadro de diálogo Agregar un complemento independiente, haga clic en Certificados y, a continuación, en Agregar.6. En el cuadro de diálogo Complemento de certificados, seleccione Cuenta de equipo y, a continuación, haga clic en Siguiente.7. En el cuadro de diálogo Seleccionar equipo, asegúrese de que Equipo local: (el equipo donde se está ejecutando esta consola) está seleccionado y, a continuación, haga clic en Finalizar.8. En el cuadro de diálogo Agregar un complemento independiente, haga clic en Cerrar.9. En el cuadro de diálogo Agregar o quitar complemento, haga clic en Aceptar.10. En la ventana Consola1, expanda Certificados (equipo local), expanda Entidades de certificación raíz de confianza y, a continuación, haga clic en Certificados.11. Haga clic con el botón secundario en Certificados, seleccione Todas las tareas y, a continuación, haga clic en Importar.12. En el asistente para importación de certificados, haga clic en Siguiente.13. En la página Archivo para importar, haga clic en Examinar y seleccione la ubicación donde se descargó el archivo de certificados de la entidad de certificación, por ejemplo, TrustedCA.p7b, seleccione el archivo y, a continuación, haga clic en Abrir.14. En la página Archivo para importar, seleccione Colocar todos los certificados en el siguiente almacén, asegúrese de que aparece Entidades de certificación raíz de confianza en el cuadro Almacén de certificados y, a continuación, haga clic en Siguiente.15. En la página Finalización del Asistente para importación de certificados, haga clic en Finalizar. |

Para crear una plantilla de certificados

|  |
| --- |
| 1. En el equipo que hospeda la entidad de certificación de empresa, en el escritorio de Windows, haga clic en Inicio, seleccione Programas, seleccione Herramientas administrativas y, a continuación, haga clic en Entidad de certificación.2. En el panel de navegación, expanda el nombre de la entidad de certificación, haga clic con el botón secundario en Plantillas de certificado y, a continuación, haga clic en Administrar.3. En la consola Plantillas de certificado, en el panel de resultados, haga clic con el botón secundario en IPSec (solicitud sin conexión) y, a continuación, haga clic en Plantilla duplicada.4. En el cuadro de diálogo Propiedades de plantilla nueva, en la ficha General, en el cuadro de texto Nombre para mostrar de plantilla, escriba un nombre nuevo para esta plantilla (por ejemplo, OperationsManagerCert).5. En la ficha Tratamiento de la solicitud, seleccione Permitir que la clave privada se pueda exportar y, a continuación, haga clic en CSP.6. En el cuadro de diálogo Selección del proveedor de servicios de cifrado (CSP), seleccione el proveedor de servicios de cifrado que mejor se adapte a sus necesidades de negocio y, a continuación, haga clic en Aceptar.Nota Windows 2000 Server funcionará con Proveedor de cifrado mejorado de Microsoft 1.0. Windows Server 2003 y Windows XP funcionarán con Proveedor de cifrado Microsoft RSA SChannel.7. Haga clic en la ficha Extensiones y, en Extensiones incluidas en esta plantilla, haga clic en Directivas de aplicación y, a continuación, en Editar.8. En el cuadro de diálogo Editar extensión de directivas de aplicación, haga clic en Seguridad IP IKE intermedia y, a continuación, haga clic en Quitar. 9. Haga clic en Agregar en la lista Directivas de aplicación, mantenga presionada la tecla CTRL para seleccionar varios elementos, haga clic en Autenticación de cliente y Autenticación de servidor y, a continuación, haga clic en Aceptar.10. En el cuadro de diálogo Editar extensión de directivas de aplicación, haga clic en Aceptar.11. Haga clic en la ficha Seguridad, asegúrese de que el grupo Usuarios autenticados tiene permisos de lectura e inscripción y, a continuación, haga clic en Aceptar. |

Para agregar la plantilla a la carpeta de plantillas de certificado

|  |
| --- |
| 12. 0. 1. En el complemento Entidad de certificación, haga clic con el botón secundario en la carpeta Plantillas de certificado, seleccione Nueva y, a continuación, haga clic en Plantilla de certificado que se va a emitir.2. En el cuadro Habilitar plantillas de certificados, seleccione la plantilla de certificado que ha creado y, a continuación, haga clic en Aceptar. |

Para solicitar un certificado de entidad de certificación de empresa

|  |
| --- |
| 1. Inicie sesión en el equipo donde desea instalar un certificado (por ejemplo, servidor de puerta de enlace o servidor de administración).2. Inicie Internet Explorer y conéctese al equipo que hospeda Servicios de Certificate Server (por ejemplo, http://<nombre de servidor>/certsrv).3. En la página de bienvenida de Servicios de Certificate Server de Microsoft, haga clic en Solicitar un certificado.4. En la página Solicitar un certificado, haga clic en O enviar una solicitud avanzada de certificado.5. En la página Solicitud avanzada de certificado, haga clic en Crear y enviar una solicitud a esta CA.6. En la página Solicitud avanzada de certificado, haga lo siguiente:a. En Plantilla de certificados, seleccione el nombre de la plantilla que ha creado (por ejemplo, OperationsManagerCert).b. En Identificando información para plantillas sin conexión, en el campo Nombre, escriba un nombre único, por ejemplo, el nombre de dominio completo (FQDN) del equipo para el que está solicitando el certificado. En el resto de los campos, escriba la información correspondiente.Nota Se genera el identificador de evento 20052 de error si el FQDN especificado en el campo Nombre no coincide con el nombre del equipo.c. En Opciones de clave, haga clic en Crear un conjunto de claves nuevo; en el campo CSP, seleccione el proveedor de servicios de cifrado que mejor se adapte a sus necesidades de negocio; en Tamaño de clave, seleccione el tamaño de clave que mejor se adapte a sus necesidades de negocio; seleccione Nombre automático de contenedor de claves; asegúrese de que esté marcado Marcar claves como exportables; elimine Exportar claves al archivo; elimine Habilitar la protección de clave privada de alta seguridad y, a continuación, haga clic en Almacenar el certificado en el almacén de certificados del equipo local.Nota Windows 2000 Server funcionará con Proveedor de cifrado mejorado de Microsoft 1.0. Windows Server 2003 y Windows XP funcionarán con Proveedor de cifrado Microsoft RSA SChannel.d. En Opciones adicionales, en Formato de la solicitud, seleccione CMC; en la lista Algoritmo hash, seleccione SHA-1. Desactive Guardar solicitud en un archivo y, a continuación, en el campo Nombre descriptivo, escriba el nombre de dominio completo (FQDN) del equipo para el que está solicitando el certificado.e. Haga clic en Enviar.f. Si se muestra el mensaje Posible infracción de scripting, haga clic en Sí.g. En la página Certificado emitido, haga clic en Instalar este certificado.h. Si se muestra el cuadro de diálogo Posible infracción de scripting, haga clic en Sí.i. En la página Certificado instalado, cuando vea el mensaje Se ha instalado satisfactoriamente su certificado nuevo, cierre el explorador. |

Para importar certificados con MOMCertImport

|  |
| --- |
| 1. Inicie sesión en el equipo con una cuenta que sea miembro del grupo de administradores.2. En el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.3. En el cuadro de diálogo Ejecutar, escriba cmd y, a continuación, haga clic en Aceptar.4. En el símbolo del sistema, escriba <letra\_unidad>: (donde <letra\_unidad> es la unidad donde está situado el disco de instalación de Operations Manager 2007) y, a continuación, presione Entrar.5. Escriba cd\SupportTools\i386 y después presione ENTRAR.Nota En equipos de 64 bits, escriba cd\SupportTools\amd646. Escriba lo siguiente:MOMCertImport /SubjectName <Nombre de sujeto del certificado>7. Presione Entrar. |

Vea también

[Configuración de la consola de Operations para usar SSL cuando se conecta a un servidor de informes en Operations Manager 2007](#z6edab54f881c4a28a406f9f6005eb485)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2003 en Operations Manager 2007](#zb983d345d4b049ff94c88ab56016aceb)

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2008 en Operations Manager 2007](#z3067b41c6eab4cd0a3e5538b57af9b09)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2008 en Operations Manager 2007](#z9d62a00496b3479095d6f05f17eeb77a)

[Eliminación de certificados importados con MOMCertImport en Operations Manager 2007](#zbafc843025be497fb5deece29c69b7e6)

Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2003 en Operations Manager 2007

Los procedimientos siguientes proporcionan los pasos necesarios para obtener un certificado de una entidad de certificación (CA) de empresa mediante Servicios de Certificate Server, que es un componente de Windows 2000 Server y Windows Server 2003. Para obtener un certificado de esta forma, deberá:

Realizar los procedimientos siguientes:

 Descargar el certificado (CA) raíz de confianza.

 Importar el certificado (CA) raíz de confianza.

 Solicitar un certificado de una entidad de certificación independiente.

 Aprobar la solicitud de certificado pendiente. Si los Servicios de Certificate Server se han configurado para aprobar automáticamente certificados, continúe con el procedimiento siguiente para recuperar el certificado. De lo contrario, es necesario que el administrador de la entidad de certificación emita el certificado mediante el procedimiento de recuperación de certificados.

 Recuperar el certificado.

 Mediante la utilidad MOMCertImport, importe el certificado en Operations Manager.

Para descargar el certificado (CA) raíz de confianza

|  |
| --- |
| 1. Inicie sesión en el equipo donde ha instalado un certificado: por ejemplo, el servidor de puerta de enlace o el servidor de administración.2. Inicie Internet Explorer y conéctese al equipo que hospeda los Servicios de Certificate Server: por ejemplo, http://<nombre de servidor>/certsrv.3. En la página de bienvenida, haga clic en Descargar certificado de CA, cadena de certificados o CRL.4. En la página Descargar certificado de CA, cadena de certificados o CRL, haga clic en Método de codificación, haga clic en Base 64 y, a continuación, haga clic en Descargar cadena de certificados de CA.5. En el cuadro de diálogo Descarga de archivos, haga clic en Guardar y guarde el certificado; por ejemplo, Trustedca.p7b.6. Cuando finalice la descarga, cierre Internet Explorer. |

Para importar el certificado (CA) raíz de confianza

|  |
| --- |
| 1. En el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba mmc y, a continuación, haga clic en Aceptar.3. En la ventana Consola1, haga clic en Archivo y, a continuación, haga clic en Agregar o quitar complemento.4. En el cuadro de diálogo Agregar o quitar complemento, haga clic en Agregar.5. En el cuadro de diálogo Agregar un complemento independiente, haga clic en Certificados y, a continuación, en Agregar.6. En el cuadro de diálogo Complemento de certificados, seleccione Cuenta de equipo y, a continuación, haga clic en Siguiente.7. En el cuadro de diálogo Seleccionar equipo, asegúrese de que Equipo local: (el equipo donde se está ejecutando esta consola) está seleccionado y, a continuación, haga clic en Finalizar.8. En el cuadro de diálogo Agregar un complemento independiente, haga clic en Cerrar.9. En el cuadro de diálogo Agregar o quitar complemento, haga clic en Aceptar.10. En la ventana Consola1, expanda Certificados (equipo local), expanda Entidades de certificación raíz de confianza y, a continuación, haga clic en Certificados.11. Haga clic con el botón secundario en Certificados, seleccione Todas las tareas y, a continuación, haga clic en Importar.12. En el asistente para importación de certificados, haga clic en Siguiente.13. En la página Archivo para importar, haga clic en Examinar y seleccione la ubicación donde se descargó el archivo de certificados de la entidad de certificación, por ejemplo, TrustedCA.p7b, seleccione el archivo y, a continuación, haga clic en Abrir.14. En la página Archivo para importar, seleccione Colocar todos los certificados en el siguiente almacén, asegúrese de que aparece Entidades de certificación raíz de confianza en el cuadro Almacén de certificados y, a continuación, haga clic en Siguiente.15. En la página Finalización del Asistente para importación de certificados, haga clic en Finalizar. |

Para solicitar un certificado de una entidad de certificación independiente

|  |
| --- |
| 1. Inicie sesión en el equipo donde desee instalar un certificado (por ejemplo, el servidor de puerta de enlace o el servidor de administración).2. Inicie Internet Explorer y conéctese al equipo que hospeda los Servicios de servidor de certificados (por ejemplo, http://<nombre\_servidor>/certsrv).3. En la página de bienvenida de Servicios de Certificate Server de Microsoft, haga clic en Solicitar un certificado.4. En la página Solicitar un certificado, haga clic en O enviar una solicitud avanzada de certificado.5. En la página Solicitud avanzada de certificado, haga clic en Crear y enviar una solicitud a esta CA.6. En la página Solicitud avanzada de certificado, haga lo siguiente:a. En Identificando información, en el campo Nombre, escriba un nombre único, como el nombre de dominio completo (FQDN), del equipo para el que está solicitando el certificado. Escriba la información correspondiente en el resto de campos.Nota Se genera el identificador de evento 20052 de error si el FQDN especificado en el campo Nombre no coincide con el nombre del equipo.b. En Tipo de certificado necesario:haga clic en la lista y, a continuación, seleccione Otros. En el campo OID, escriba 1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2.c. En Opciones de clave, selecciones las siguientes opciones:Haga clic en Crear un conjunto de claves nuevoEn el campo CSP, seleccione Proveedor de cifrado mejorado de Microsoft 1.0En Uso de la clave, seleccione ambosEn Tamaño de clave, seleccione 1024Seleccione Nombre automático de contenedor de clavesSeleccione Marcar claves como exportablesElimine Exportar claves al archivo (no es necesario en Windows Server 2008 AD CS)Elimine Habilitar la protección de clave privada de alta seguridadHaga clic en Almacenar el certificado en el almacén de certificados del equipo local.d. En Opciones adicionales:En Formato de la solicitud, seleccione CMCEn la lista Algoritmo hash, seleccione SHA-1Elimine Guardar solicitud en un archivoEn el campo Nombre descriptivo, escriba el nombre de dominio completo (FQDN) del equipo para el que está solicitando el certificado.e. Haga clic en Enviar.f. Si se muestra el cuadro de diálogo Posible infracción de seguridad, haga clic en Sí.g. Cuando aparezca la página Certificado pendiente, cierre el explorador. |

Para aprobar la solicitud de certificado pendiente

|  |
| --- |
| 1. Inicie sesión en el equipo que hospeda los Servicios de Certificate Server como administrador de la entidad de certificación.2. En el escritorio de Windows, haga clic en Inicio, seleccione Programas, seleccione Herramientas administrativas y, a continuación, haga clic en Entidad de certificación.3. En Entidad de certificación, expanda el nodo del nombre de la entidad de certificación y, a continuación, haga clic en Solicitudes pendientes.4. En el panel de resultados, haga clic con el botón secundario en la solicitud pendiente del procedimiento anterior, seleccione Todas las tareas y, a continuación, haga clic en Emitir.5. Haga clic en Certificados emitidos y confirme que el certificado que acaba de emitir aparece en la lista.6. Cierre Entidad de certificación. |

Para recuperar el certificado

|  |
| --- |
| 1. Inicie sesión en el equipo donde desee instalar un certificado (por ejemplo, el servidor de puerta de enlace o el servidor de administración).2. Inicie Internet Explorer y conéctese al equipo que hospeda Servicios de Certificate Server (por ejemplo, http://<nombre de servidor>/certsrv).3. En la página de bienvenida a Servicios de Certificate Server de Microsoft, haga clic en Ver el estado de una solicitud de certificado pendiente.4. En la página Ver el estado de una solicitud de certificado pendiente, haga clic en el certificado que ha solicitado.5. En la página Certificado emitido, haga clic en Instalar este certificado.6. En el cuadro de diálogo Posible infracción de scripting, haga clic en Sí.7. En la página Certificado instalado, después de ver el mensaje Se ha instalado satisfactoriamente su certificado nuevo, cierre el explorador. |

Para importar certificados con MOMCertImport

|  |
| --- |
| 1. Inicie sesión en el equipo con una cuenta que sea miembro del grupo de administradores.2. En el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.3. En el cuadro de diálogo Ejecutar, escriba cmd y, a continuación, haga clic en Aceptar.4. En el símbolo del sistema, escriba <letra\_unidad>: (donde <letra\_unidad> es la unidad donde está situado el disco de instalación de Operations Manager 2007) y, a continuación, presione Entrar.5. Escriba cd\SupportTools\i386 y después presione Entrar.Nota En equipos de 64 bits, escriba cd\SupportTools\amd646. Escriba lo siguiente:MOMCertImport7. En el cuadro de diálogo Seleccionar certificado, seleccione el certificado que recuperó en la sección anterior y, a continuación, haga clic en Aceptar.Nota Para ayudarle a seleccionar el certificado correcto si aparece más de un certificado, seleccione el certificado para el que se indican los usos previstos como Autenticación de servidor, Autenticación de cliente y el certificado cuyo nombre descriptivo coincide con el nombre descriptivo definido anteriormente en el paso 6d del procedimiento Para solicitar un certificado de una entidad de certificación independiente.8. En el cuadro de diálogo de comando, aparecerá el mensaje El certificado se ha instalado correctamente. Consulte el rastreador de eventos del registro de Operations Manager para comprobar la conectividad del canal. |

Vea también

[Configuración de la consola de Operations para usar SSL cuando se conecta a un servidor de informes en Operations Manager 2007](#z6edab54f881c4a28a406f9f6005eb485)

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2003 en Operations Manager 2007](#z5686fe43d94145eda9380548abf07708)

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2008 en Operations Manager 2007](#z3067b41c6eab4cd0a3e5538b57af9b09)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2008 en Operations Manager 2007](#z9d62a00496b3479095d6f05f17eeb77a)

[Eliminación de certificados importados con MOMCertImport en Operations Manager 2007](#zbafc843025be497fb5deece29c69b7e6)

Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2008 en Operations Manager 2007

Use los procedimientos de este tema para obtener un certificado del equipo Windows Server 2008 que hospeda los Servicios de Certificate Server de Active Directory (AD CS) de raíz de empresa. Se usa la utilidad de línea de comandos CertReq para solicitar y aceptar un certificado, y una interfaz web para enviar y recuperar el certificado.

Se da por supuesto que se tiene AD CS instalado, que se ha creado un enlace HTTPS y que se ha instalado el certificado asociado. Se puede obtener información sobre la creación de un enlace HTTPS en el tema [Configuración de un enlace HTTPS para una entidad de certificación de Windows Server 2008](#z8b74f9c422fd495cac9e61f2e2a0d719).

Importante

El contenido de este tema se basa en la configuración predeterminada para AD CS de Windows Server 2008; por ejemplo, la configuración de la longitud de la clave en 2048, seleccionando el proveedor de almacenamiento de claves de software de Microsoft como CSP y usando Algoritmo hash seguro 1 (SHA1). Evalúe estas selecciones en relación con los requisitos de la directiva de seguridad de la empresa.

El proceso de alto nivel para obtener un certificado de la entidad de certificación (CA) de empresa se indica a continuación:

1. Descargar el certificado (CA) raíz de confianza.

2. Importar el certificado (CA) raíz de confianza.

3. Crear una plantilla de certificados.

4. Agregar la plantilla a la carpeta de plantillas de certificado.

5. Crear un archivo de información de instalación para usar con la utilidad de línea de comandos CertReq.

6. Crear un archivo de solicitud.

7. Enviar una solicitud a la entidad de certificación.

8. Importar el certificado en el almacén de certificados.

9. Importar el certificado en Operations Manager con MOMCertImport.

Para descargar el certificado (CA) raíz de confianza

|  |
| --- |
| 1. Inicie sesión en el equipo donde ha instalado un certificado: por ejemplo, el servidor de puerta de enlace o el servidor de administración.2. Inicie Internet Explorer y conéctese al equipo que hospeda los Servicios de Certificate Server: por ejemplo, http://<nombre de servidor>/certsrv.3. En la página de bienvenida, haga clic en Descargar certificado de CA, cadena de certificados o CRL.4. En la página Descargar certificado de CA, cadena de certificados o CRL, haga clic en Método de codificación, haga clic en Base 64 y, a continuación, haga clic en Descargar cadena de certificados de CA.5. En el cuadro de diálogo Descarga de archivos, haga clic en Guardar y guarde el certificado; por ejemplo, Trustedca.p7b.6. Cuando finalice la descarga, cierre Internet Explorer. |

Para importar el certificado (CA) raíz de confianza

|  |
| --- |
| 1. En el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba mmc y, a continuación, haga clic en Aceptar.3. En la ventana Consola1, haga clic en Archivo y, a continuación, haga clic en Agregar o quitar complemento.4. En el cuadro de diálogo Agregar o quitar complemento, haga clic en Agregar.5. En el cuadro de diálogo Agregar un complemento independiente, haga clic en Certificados y, a continuación, en Agregar.6. En el cuadro de diálogo Complemento de certificados, seleccione Cuenta de equipo y, a continuación, haga clic en Siguiente.7. En el cuadro de diálogo Seleccionar equipo, asegúrese de que Equipo local: (el equipo donde se está ejecutando esta consola) está seleccionado y, a continuación, haga clic en Finalizar.8. En el cuadro de diálogo Agregar un complemento independiente, haga clic en Cerrar.9. En el cuadro de diálogo Agregar o quitar complemento, haga clic en Aceptar.10. En la ventana Consola1, expanda Certificados (equipo local), expanda Entidades de certificación raíz de confianza y, a continuación, haga clic en Certificados.11. Haga clic con el botón secundario en Certificados, seleccione Todas las tareas y, a continuación, haga clic en Importar.12. En el asistente para importación de certificados, haga clic en Siguiente.13. En la página Archivo para importar, haga clic en Examinar y seleccione la ubicación donde se descargó el archivo de certificados de la entidad de certificación, por ejemplo, TrustedCA.p7b, seleccione el archivo y, a continuación, haga clic en Abrir.14. En la página Archivo para importar, seleccione Colocar todos los certificados en el siguiente almacén, asegúrese de que aparece Entidades de certificación raíz de confianza en el cuadro Almacén de certificados y, a continuación, haga clic en Siguiente.15. En la página Finalización del Asistente para importación de certificados, haga clic en Finalizar. |

Para crear una plantilla de certificados

|  |
| --- |
| 1. En el equipo que hospeda la entidad de certificación de empresa, en el escritorio de Windows, haga clic en Inicio, seleccione Programas, seleccione Herramientas administrativas y, a continuación, haga clic en Entidad de certificación.2. En el panel de navegación, expanda el nombre de la entidad de certificación, haga clic con el botón secundario en Plantillas de certificado y, a continuación, haga clic en Administrar.3. En la consola Plantillas de certificado, en el panel de resultados, haga clic con el botón secundario en IPSec (solicitud sin conexión) y, a continuación, haga clic en Plantilla duplicada.4. En el cuadro de diálogo Plantilla duplicada, seleccione Windows Server 2003 Enterprise Edition y, a continuación, haga clic en Aceptar.Nota La opción para Windows Server 2008 Enterprise Edition no es compatible en este momento.5. En el cuadro de diálogo Propiedades de plantilla nueva, en la ficha General, en el cuadro de texto Nombre para mostrar plantilla, escriba un nombre nuevo para esta plantilla; por ejemplo, OperationsManagerCert.6. En la ficha Tratamiento de la solicitud, seleccione Permitir que la clave privada se pueda exportar.7. Haga clic en la ficha Extensiones y, en Extensiones incluidas en esta plantilla, haga clic en Directivas de aplicación y, a continuación, en Editar.8. En el cuadro de diálogo Editar extensión de directivas de aplicación, haga clic en Seguridad IP IKE intermedia y, a continuación, haga clic en Quitar. 9. Haga clic en Agregar en la lista Directivas de aplicación, mantenga presionada la tecla CTRL para seleccionar varios elementos, haga clic en Autenticación de cliente y Autenticación de servidor y, a continuación, haga clic en Aceptar.10. En el cuadro de diálogo Editar extensión de directivas de aplicación, haga clic en Aceptar.11. Haga clic en la ficha Seguridad, asegúrese de que el grupo Usuarios autenticados tiene permisos de lectura e inscripción y, a continuación, haga clic en Aceptar.12. Cierre la consola de plantillas de certificado. |

Para agregar la plantilla a la carpeta de plantillas de certificado

|  |
| --- |
| 1. En el equipo que hospeda la entidad de certificación de empresa, en el complemento Entidad de certificación, haga clic con el botón secundario en la carpeta Plantillas de certificado, seleccione Nueva y, a continuación, haga clic en Plantilla de certificado que se va a emitir.2. En el cuadro Habilitar plantillas de certificados, seleccione la plantilla de certificado que ha creado; por ejemplo, haga clic en OperationsManagerCert y, a continuación, haga clic en Aceptar. |

Para crear un archivo de información de instalación (.inf)

|  |
| --- |
| 1. En el equipo que hospeda el componente de Operations Manager para el que está solicitando el certificado, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba Bloc de notas y, a continuación, haga clic en Aceptar.3. Cree un archivo de texto que contenga los siguientes elementos:[NewRequest]Subject="CN=<FQDN del equipo para el que se crea el certificado, por ejemplo, el servidor de puerta de enlace o el servidor de administración.>"Exportable=TRUEKeyLength=2048KeySpec=1KeyUsage=0xf0MachineKeySet=TRUE[EnhancedKeyUsageExtension]OID=1.3.6.1.5.5.7.3.1OID=1.3.6.1.5.5.7.3.24. Guarde el archivo con la extensión .inf, por ejemplo, RequestConfig.inf.5. Cierre el Bloc de notas. |

Para crear un archivo de solicitud para usar con una entidad de certificación de empresa

|  |
| --- |
| 1. En el equipo que hospeda el componente de Operations Manager para el que está solicitando el certificado, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba cmd y, a continuación, haga clic en Aceptar.3. En la ventana de comandos, escriba CertReq –New –f RequestConfig.inf CertRequest.reqy, a continuación, presione Entrar.4. Con el Bloc de notas, abra el archivo obtenido (por ejemplo, CertRequest.req), y copie el contenido de este archivo en el portapapeles. |

Para enviar una solicitud a una entidad de certificación de empresa

|  |
| --- |
| 1. En el equipo que hospeda el componente de Operations Manager para el que solicita un certificado, inicie Internet Explorer y, a continuación, conéctese al equipo que hospeda los servicios de Certificate Server; por ejemplo, https://<nombre de servidor>/certsrv.Nota Si no se ha configurado un enlace HTTPS en el sitio web de Servicios de Certificate Server, el navegador no podrá conectarse. Consulte el tema [Configuración de un enlace HTTPS para una entidad de certificación de Windows Server 2008](#z8b74f9c422fd495cac9e61f2e2a0d719) en esta guía.2. En la pantalla de bienvenida Servicios de Certificate Server para Active Directory de Microsoft, haga clic en Solicitar un certificado.3. En la página Solicitar un certificado, haga clic en solicitud avanzada de certificado.4. En la página Solicitud avanzada de certificado, haga clic en Enviar una solicitud de certificado con un archivo codificado en base64 CMC o PKCS #10 o una solicitud de renovación con un archivo codificado en base64 PKCS #7.5. En la página Enviar una solicitud de certificado o una solicitud de renovación, en el cuadro de texto Guardar solicitud, pegue el contenido del archivo CertRequest.req que copió en el paso 4 del procedimiento anterior.6. En el cuadro Plantilla de certificado, seleccione la plantilla de certificado que ha creado; por ejemplo, haga clic en OperationsManagerCert y, a continuación, haga clic en Enviar.7. En la página Certificado emitido, seleccione Codificado en Base64 y, a continuación, haga clic en Descargar certificado.8. En el cuadro de diálogo Descarga de archivo – Advertencia de seguridad, haga clic en Guardar y guarde el certificado; por ejemplo, como NewCertificate.cer.9. Cierre Internet Explorer. |

Para importar el certificado en el almacén de certificados

|  |
| --- |
| 1. En el equipo que hospeda el componente de Operations Manager para el que está configurando el certificado, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba cmd y, a continuación, haga clic en Aceptar.3. En la ventana de comandos, escriba CertReq –Accept NewCertifiate.cery, a continuación, presione Entrar. |

Para importar el certificado en Operations Manager con MOMCertImport

|  |
| --- |
| 1. Inicie sesión en el equipo en el que instaló el certificado con una cuenta que sea miembro del grupo de administradores.2. En el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.3. En el cuadro de diálogo Ejecutar, escriba cmd y, a continuación, haga clic en Aceptar.4. En el símbolo del sistema, escriba <letra\_unidad>: (donde <letra\_unidad> es la unidad donde está situado el disco de instalación de Operations Manager 2007) y, a continuación, presione Entrar.5. Escriba cd\SupportTools\i386 y después presione Entrar.Nota En equipos de 64 bits, escriba cd\SupportTools\amd646. Escriba lo siguiente:MOMCertImport /SubjectName <Nombre de sujeto del certificado>7. Presione Entrar. |

Vea también

[Configuración de la consola de Operations para usar SSL cuando se conecta a un servidor de informes en Operations Manager 2007](#z6edab54f881c4a28a406f9f6005eb485)

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2003 en Operations Manager 2007](#z5686fe43d94145eda9380548abf07708)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2003 en Operations Manager 2007](#zb983d345d4b049ff94c88ab56016aceb)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2008 en Operations Manager 2007](#z9d62a00496b3479095d6f05f17eeb77a)

[Eliminación de certificados importados con MOMCertImport en Operations Manager 2007](#zbafc843025be497fb5deece29c69b7e6)

Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2008 en Operations Manager 2007

Use los procedimientos de este tema para obtener un certificado de un equipo basado en Windows Server 2008 independiente que hospeda los Servicios de Certificate Server de Active Directory (AD CS). Se usa la utilidad de línea de comandos CertReq para solicitar y aceptar un certificado, y una interfaz web para enviar y recuperar el certificado.

Se da por supuesto que se tiene AD CS instalado, que se está usando un enlace HTTPS y que se ha instalado el certificado asociado. Se puede obtener información sobre la creación de un enlace HTTPS en el tema [Configuración de un enlace HTTPS para una entidad de certificación de Windows Server 2008](#z8b74f9c422fd495cac9e61f2e2a0d719).

Importante

El contenido de este tema se basa en la configuración predeterminada para AD CS de Windows Server 2008; por ejemplo, la configuración de la longitud de la clave en 2048, seleccionando el proveedor de almacenamiento de claves de software de Microsoft como CSP y usando Algoritmo hash seguro 1 (SHA1). Evalúe estas selecciones en relación con los requisitos de la directiva de seguridad de la empresa.

El proceso de alto nivel para obtener un certificado de la entidad de certificación (CA) independiente se indica a continuación:

1. Descargar el certificado (CA) raíz de confianza.

2. Importar el certificado (CA) raíz de confianza.

3. Crear un archivo de información de instalación para usar con la utilidad de línea de comandos CertReq.

4. Crear un archivo de solicitud.

5. Enviar una solicitud a la entidad de certificación con el archivo de solicitud.

6. Aprobar la solicitud de certificado pendiente.

7. Recuperar el certificado de la entidad de certificación.

8. Importar el certificado en el almacén de certificados.

9. Importar el certificado en Operations Manager con MOMCertImport.

Para descargar el certificado (CA) raíz de confianza

|  |
| --- |
| 1. Inicie sesión en el equipo donde ha instalado un certificado: por ejemplo, el servidor de puerta de enlace o el servidor de administración.2. Inicie Internet Explorer y conéctese al equipo que hospeda los Servicios de Certificate Server: por ejemplo, http://<nombre de servidor>/certsrv.3. En la página de bienvenida, haga clic en Descargar certificado de CA, cadena de certificados o CRL.4. En la página Descargar certificado de CA, cadena de certificados o CRL, haga clic en Método de codificación, haga clic en Base 64 y, a continuación, haga clic en Descargar cadena de certificados de CA.5. En el cuadro de diálogo Descarga de archivos, haga clic en Guardar y guarde el certificado; por ejemplo, Trustedca.p7b.6. Cuando finalice la descarga, cierre Internet Explorer. |

Para importar el certificado (CA) raíz de confianza

|  |
| --- |
| 1. En el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba mmc y, a continuación, haga clic en Aceptar.3. En la ventana Consola1, haga clic en Archivo y, a continuación, haga clic en Agregar o quitar complemento.4. En el cuadro de diálogo Agregar o quitar complemento, haga clic en Agregar.5. En el cuadro de diálogo Agregar un complemento independiente, haga clic en Certificados y, a continuación, en Agregar.6. En el cuadro de diálogo Complemento de certificados, seleccione Cuenta de equipo y, a continuación, haga clic en Siguiente.7. En el cuadro de diálogo Seleccionar equipo, asegúrese de que Equipo local: (el equipo donde se está ejecutando esta consola) está seleccionado y, a continuación, haga clic en Finalizar.8. En el cuadro de diálogo Agregar un complemento independiente, haga clic en Cerrar.9. En el cuadro de diálogo Agregar o quitar complemento, haga clic en Aceptar.10. En la ventana Consola1, expanda Certificados (equipo local), expanda Entidades de certificación raíz de confianza y, a continuación, haga clic en Certificados.11. Haga clic con el botón secundario en Certificados, seleccione Todas las tareas y, a continuación, haga clic en Importar.12. En el asistente para importación de certificados, haga clic en Siguiente.13. En la página Archivo para importar, haga clic en Examinar y seleccione la ubicación donde se descargó el archivo de certificados de la entidad de certificación, por ejemplo, TrustedCA.p7b, seleccione el archivo y, a continuación, haga clic en Abrir.14. En la página Archivo para importar, seleccione Colocar todos los certificados en el siguiente almacén, asegúrese de que aparece Entidades de certificación raíz de confianza en el cuadro Almacén de certificados y, a continuación, haga clic en Siguiente.15. En la página Finalización del Asistente para importación de certificados, haga clic en Finalizar. |

Para crear un archivo de información de instalación (.inf)

|  |
| --- |
| 1. En el equipo que hospeda el componente de Operations Manager para el que está solicitando el certificado, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba Bloc de notas y, a continuación, haga clic en Aceptar.3. Cree un archivo de texto que contenga los siguientes elementos:[NewRequest]Subject="CN=<FQDN del equipo para el que se crea el certificado, por ejemplo, el servidor de puerta de enlace o el servidor de administración.>"Exportable=TRUEKeyLength=2048KeySpec=1KeyUsage=0xf0MachineKeySet=TRUE[EnhancedKeyUsageExtension]OID=1.3.6.1.5.5.7.3.1OID=1.3.6.1.5.5.7.3.24. Guarde el archivo con la extensión .inf, por ejemplo, RequestConfig.inf.5. Cierre el Bloc de notas. |

Para crear un archivo de solicitud para usar con una entidad de certificación independiente

|  |
| --- |
| 1. En el equipo que hospeda el componente de Operations Manager para el que está solicitando el certificado, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba cmd y, a continuación, haga clic en Aceptar.3. En la ventana de comandos, escriba CertReq –New –f RequestConfig.inf CertRequest.reqy, a continuación, presione Entrar.4. Abra el archivo obtenido (por ejemplo, CertRequest.req) con el Bloc de notas. Copie el contenido de este archivo en el portapapeles. |

Para enviar una solicitud a una entidad de certificación independiente

|  |
| --- |
| 1. En el equipo que hospeda el componente de Operations Manager para el que solicita un certificado, inicie Internet Explorer y, a continuación, conéctese al equipo que hospeda los servicios de Certificate Server (por ejemplo, https://<nombre de servidor>/certsrv).Nota Si no se ha configurado un enlace HTTPS en el sitio web de Servicios de Certificate Server, el navegador no podrá conectarse. Consulte el tema [Configuración de un enlace HTTPS para una entidad de certificación de Windows Server 2008](#z8b74f9c422fd495cac9e61f2e2a0d719) en esta guía.2. En la pantalla de bienvenida Servicios de Certificate Server para Active Directory de Microsoft, haga clic en Solicitar un certificado.3. En la página Solicitar un certificado, haga clic en solicitud avanzada de certificado.4. En la página Solicitud avanzada de certificado, haga clic en Enviar una solicitud de certificado con un archivo codificado en base64 CMC o PKCS #10 o una solicitud de renovación con un archivo codificado en base64 PKCS #7.5. En la página Enviar una solicitud de certificado o una solicitud de renovación, en el cuadro de texto Guardar solicitud, pegue el contenido del archivo CertRequest.req que copió en el paso 4 del procedimiento anterior y, a continuación, haga clic en Enviar.6. Cierre Internet Explorer. |

Para aprobar la solicitud de certificado pendiente

|  |
| --- |
| 1. Inicie sesión como administrador de la entidad de certificación en el equipo que hospeda los Servicios de Certificate Server de Active Directory.2. En el escritorio de Windows, haga clic en Inicio, seleccione Programas, seleccione Herramientas administrativas y, a continuación, haga clic en Entidad de certificación.3. En Entidad de certificación, expanda el nodo del nombre de la entidad de certificación y, a continuación, haga clic en Solicitudes pendientes.4. En el panel de resultados, haga clic con el botón secundario en la solicitud pendiente del procedimiento anterior, seleccione Todas las tareas y, a continuación, haga clic en Emitir.5. Haga clic en Certificados emitidos y confirme que el certificado que acaba de emitir aparece en la lista.6. Cierre Entidad de certificación. |

Para recuperar el certificado

|  |
| --- |
| 1. Inicie sesión en el equipo donde desee instalar un certificado; por ejemplo, el servidor de puerta de enlace o el servidor de administración.2. Inicie Internet Explorer y conéctese al equipo que hospeda los Servicios de Certificate Server (por ejemplo, http://<nombre del servidor>/certsrv).3. En la página de bienvenida Servicios de Certificate Server para Active Directory de Microsoft, haga clic en Ver el estado de una solicitud de certificado pendiente.4. En la página Ver el estado de una solicitud de certificado pendiente, haga clic en el certificado que ha solicitado.5. En la página Certificado emitido, seleccione Codificado en Base64 y, a continuación, haga clic en Descargar certificado.6. En el cuadro de diálogo Descarga de archivo – Advertencia de seguridad, haga clic en Guardar y guarde el certificado; por ejemplo, como NewCertificate.cer.7. En la página Certificado instalado, después de ver el mensaje Se ha instalado satisfactoriamente su certificado nuevo, cierre el explorador.8. Cierre Internet Explorer. |

Para importar el certificado en el almacén de certificados

|  |
| --- |
| 1. En el equipo que hospeda el componente de Operations Manager para el que está configurando el certificado, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba cmd y, a continuación, haga clic en Aceptar.3. En la ventana de comandos, escriba CertReq –Accept NewCertifiate.cery, a continuación, presione Entrar. |

Para importar el certificado en Operations Manager con MOMCertImport

|  |
| --- |
| 1. Inicie sesión en el equipo en el que instaló el certificado con una cuenta que sea miembro del grupo de administradores.2. En el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.3. En el cuadro de diálogo Ejecutar, escriba cmd y, a continuación, haga clic en Aceptar.4. En el símbolo del sistema, escriba <letra\_unidad>: (donde <letra\_unidad> es la unidad donde está situado el disco de instalación de Operations Manager 2007) y, a continuación, presione Entrar.5. Escriba cd\SupportTools\i386 y después presione Entrar.Nota En equipos de 64 bits, escriba cd\SupportTools\amd646. Escriba lo siguiente:MOMCertImport /SubjectName <Nombre de sujeto del certificado>7. Presione Entrar. |

Vea también

[Configuración de la consola de Operations para usar SSL cuando se conecta a un servidor de informes en Operations Manager 2007](#z6edab54f881c4a28a406f9f6005eb485)

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2003 en Operations Manager 2007](#z5686fe43d94145eda9380548abf07708)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2003 en Operations Manager 2007](#zb983d345d4b049ff94c88ab56016aceb)

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2008 en Operations Manager 2007](#z3067b41c6eab4cd0a3e5538b57af9b09)

[Eliminación de certificados importados con MOMCertImport en Operations Manager 2007](#zbafc843025be497fb5deece29c69b7e6)

Eliminación de certificados importados con MOMCertImport en Operations Manager 2007

Use el procedimiento siguiente para quitar certificados que se hayan importado con la herramienta MOMCertImport.

Para quitar certificados importados con la herramienta MOMCertImport

|  |
| --- |
| 1. Inicie sesión en el equipo con una cuenta que sea miembro del grupo de administradores.2. En el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.3. En el cuadro de diálogo Ejecutar, escriba cmd y, a continuación, haga clic en Aceptar.4. En el símbolo del sistema, escriba <letra\_unidad>: (donde <letra\_unidad> es la unidad donde está situado el disco de instalación de Operations Manager 2007) y, a continuación, presione Entrar.5. Escriba cd\SupportTools\i386 y después presione Entrar.Nota En equipos de 64 bits, escriba cd\SupportTools\amd646. Escriba lo siguiente:MOMCertImport /Removey, a continuación, presione Entrar. |

Vea también

[Configuración de la consola de Operations para usar SSL cuando se conecta a un servidor de informes en Operations Manager 2007](#z6edab54f881c4a28a406f9f6005eb485)

[Obtención de un certificado mediante una entidad de certificación de empresa de Windows Server 2003 en Operations Manager 2007](#z5686fe43d94145eda9380548abf07708)

[Obtención de un certificado mediante una entidad de certificación independiente de Windows Server 2003 en Operations Manager 2007](#zb983d345d4b049ff94c88ab56016aceb)

Cambio de la cuenta de identificación asociada a un perfil de identificación

De forma predeterminada, los perfiles de ejecución siguientes tienen una cuenta de ejecución asociada a ellos.

 Cuenta de almacenamiento de datos

 Cuenta de lectura de sincronización de configuración del almacenamiento de datos

 Cuenta de implementación de informes de almacenamiento de datos

 Cuenta de autenticación de SQL Server de almacenamiento de datos

 Cuenta de autenticación de SQL Server de SDK de informes

Por ejemplo, el perfil de identificación denominado Cuenta de autenticación de SQL Server de almacenamiento de datos está asociado con la cuenta de identificación denominada Cuenta de autenticación de SQL Server de almacenamiento de datos. Como ejemplo, puede usar el siguiente procedimiento para cambiar la cuenta de ejecución asociada al perfil de ejecución denominado Cuenta de autenticación de SQL Server de almacenamiento de datos. Se supone que la nueva cuenta de identificación que desea asociar a este perfil de identificación ya se ha creado. Para obtener más información sobre los perfiles y las cuentas de ejecución, consulte el tema [Administración de funciones de seguridad, cuentas y perfiles en Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=88131) (http://go.microsoft.com/fwlink/?LinkId=88131).

Para cambiar la cuenta de identificación asociada a un perfil de identificación

|  |
| --- |
| 1. Inicie una sesión en el equipo con una cuenta que sea miembro de la función de Administradores de Operations Manager para el grupo de administración de Operations Manager 2007.2. En la consola de Operations, haga clic en el botón Administración.Nota Al ejecutar la consola de Operations en un equipo que no es un servidor de administración, aparece el cuadro de diálogo Conectar a servidor. En el cuadro de texto Nombre de servidor, escriba el nombre del servidor de administración de Operations Manager 2007 al que desea que se conecte la consola.3. En el panel Administración, expanda Administración y Seguridad y, a continuación, haga clic en Perfiles de ejecución.4. En el panel Perfiles de identificación, haga clic con el botón secundario en Cuenta de autenticación de SQL Server de almacenamiento de datos y, a continuación, haga clic en Propiedades.5. En el cuadro de diálogo Perfil de identificación - Cuenta de autenticación de SQL Server de almacenamiento de datos, haga clic en la ficha Cuentas de identificación.6. En Cuentas de identificación, haga clic en el equipo de destino y, a continuación, en Editar.7. En el cuadro de diálogo Editar cuenta de ejecución alternativa, haga clic en la lista Cuenta de ejecución, seleccione la nueva cuenta de ejecución que desea asociar a este perfil de ejecución y, a continuación, haga clic en Aceptar.8. En el cuadro de diálogo Perfil de identificación - Cuenta de autenticación de SQL Server de almacenamiento de datos, haga clic en Aceptar. |

Configuración de un enlace HTTPS para una entidad de certificación de Windows Server 2008

Si está configurando por primera vez una nueva CA para el uso con Operations Manager 2007, use el procedimiento siguiente para configurar un enlace HTTPS para la entidad de certificación (CA).

Para configurar un enlace HTTPS

|  |
| --- |
| 1. En el equipo que hospeda la CA, en el escritorio de Windows, haga clic en Inicio, seleccione Programas, seleccione Herramientas administrativas y, a continuación, haga clic en Administrador de Internet Information Services (IIS).2. En el cuadro de diálogo Administrador de Internet Information Services (IIS), en el panel Conexiones, expanda su nombre de equipo, expanda Sitios y, a continuación, haga clic en Sitio web predeterminado.3. En el panel Acciones, haga clic en Enlaces.4. En el cuadro de diálogo Enlaces de sitios , haga clic en Agregar. 5. En el cuadro de diálogo Agregar enlace de sitio, en el menú Tipo, seleccione https.6. En la lista Certificado SSL, seleccione la entrada que coincida con el nombre de su equipo y, a continuación, haga clic en Aceptar.7. En el cuadro de diálogo Enlaces de sitios , haga clic en Cerrar.8. En el panel Conexiones, en Sitio web predeterminado, haga clic en CertSrv.9. En el panel /CertSrv Home, haga clic con el botón secundario en Configuración de SSL y, a continuación, haga clic en Abrir característica.10. En el panel Configuración de SSL, haga clic en Requerir SSL y, a continuación, haga clic en Requerir SSL de 128 bits.11. En el panel Acciones, haga clic en Aplicar y cierre el Administrador de Internet Information Services (IIS). |

Autenticación y cifrado de datos para sistemas operativos UNIX y Linux

Con Operations Manager 2007 R2, puede implementar agentes en equipos basados en UNIX o Linux. En un entorno como este, no es posible la autenticación de Kerberos. Por este motivo, se usan certificados entre el servidor de administración y los equipos basados en UNIX o Linux. En este escenario, el servidor de administración autofirma los certificados. (Aunque es posible usar certificados de terceros, estos no son necesarios.)

Existen dos métodos que puede usar para implementar agentes. Puede usar el Asistente para detectar o instalar manualmente un agente. De estos dos métodos, la instalación manual de un agente es la opción más segura. Cuando usa el Asistente para detectar para forzar la instalación de agentes en equipos basados en UNIX o Linux, confía en que el equipo en el que está realizando la implementación es realmente el equipo que cree que es. Cuando se usa el Asistente para detectar para implementar agentes, conlleva un mayor riesgo que cuando se realiza la implementación en equipos de una red pública o en una DMZ. En esta sección de la guía de seguridad, se explica la implementación manual de un agente en un equipo basado en UNIX o Linux.

Cuando se usa el Asistente para detectar para implementar un agente, el Asistente para detectar realiza las funciones siguientes:

|  |  |
| --- | --- |
| Implementación | El Asistente para detectar copia el paquete del agente en el equipo basado en UNIX o Linux e inicia el proceso de instalación. |
| Firma de certificados | Operations Manager recupera el certificado del agente, firma el certificado, vuelve a implementar el certificado en el agente y reinicia el agente. |
| Detección | El Asistente para detectar detecta el equipo y comprueba que el certificado es válido. Si el Asistente para detectar verifica que el equipo se puede detectar y que el certificado es válido, el Asistente para detectar agrega el equipo recién detectado a la base de datos OperationsManager. |

Cuando implementa manualmente un agente, realiza los dos primeros pasos que normalmente gestiona el Asistente para detectar, implementación y firma de certificado. A continuación, usa el Asistente para detectar para agregar el equipo a la base de datos OperationsManager.

Si ya existen certificados en el sistema, se vuelven a usar durante la instalación de agentes. No se crean certificados nuevos. Los certificados no se eliminan automáticamente cuando se desinstala un agente. Debe eliminar manualmente los certificados de la carpeta /etc/opt/microsoft/scx/ssl. Para regenerar los certificados en la instalación, debe quitar esta carpeta antes de la instalación de agentes.

Los valores hash para los archivos binarios de agentes están disponibles en el [Apéndice B - Lista de valores hash para agentes de UNIX y Linux](#z9f418c9465d445f2a0bc7217f8c4c3f0) en esta guía.

Para obtener instrucciones sobre cómo implementar manualmente un agente, consulte el tema “Instalación manual de agentes multiplataforma” en la [Guía de operaciones de Operations Manager 2007 R2](http://go.microsoft.com/fwlink/?LinkId=146211) (http://go.microsoft.com/fwlink/?LinkID=146211), y use el procedimiento siguiente para instalar los certificados.

Consideraciones de Firewall de UNIX y Linux

Si tiene un firewall en su equipo basado en UNIX o Linux, debe abrir el puerto 1270 (entrante). El nombre del puerto no se puede configurar. Si implementa agentes en un entorno de baja seguridad y usa el Asistente para detectar para implementar y firmar los certificados, debe abrir el puerto SSH. El número de puerto SSH se puede configurar. De forma predeterminada, SSH usa el puerto entrante TCP 22.

Instalación manual de certificados para soporte de varias plataformas

Antes de iniciar este procedimiento, se debe haber instalado manualmente un agente. Para realizar el procedimiento, necesitará una raíz o una cuenta elevada.

Para instalar certificados para soporte de varias plataformas

|  |
| --- |
| 1. En el equipo que hospeda el sistema operativo UNIX o Linux, localice el archivo /etc/opt/microsoft/scx/ssl/scx-host-<hostname>.pem y cópielo o transfiéralo de forma segura a cualquier ubicación del equipo que hospede Operations Manager 2007 R2.2. En el equipo que hospeda Operations Manager 2007 R2, en el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.3. En el cuadro de diálogo Ejecutar, escriba cmdy, a continuación, presione Entrar.4. Cambie directorios a la ubicación en la que copió scx.pem.5. Escriba el comando scxcertconfig -sign scx-host-<hostname>.pem scx\_new.pemy, a continuación, presione Entrar. Este comando autofirmará su certificado (scx-host-<hostname>.pem) y guardará el nuevo certificado (scx-host-<hostname>\_new.pem).Nota Asegúrese de que la ubicación en la que esté instalado Operations Manager esté en su comando de ruta o use la ruta completa del archivo scxcertconfig.exe.6. Copie o transfiera de forma segura el archivo scx\_new.pem en la carpeta /etc/opt/microsoft/scx/ssl del equipo que hospeda el sistema operativo UNIX o Linux. De este modo, se reemplaza el archivo scx-host-<hostname>.pem original. 7. Reinicie el agente. Para ello, escriba sxadmin –restart. |

Para detectar un equipo UNIX o Linux mediante Operations Manager 2007 R2

|  |
| --- |
| 1. En el equipo que hospeda Operations Manager 2007 R2, inicie la consola de Operations Manager y haga clic en Administración.2. En el panel Administración, haga clic en Asistente para detectar.3. En el Asistente para administrar equipos y dispositivos, en la página Tipo de detección, haga clic en Equpos Unix/Linux y, a continuación, en Siguiente.4. En la página Método de detección, haga clic en Agregar.5. En el cuadro de diálogo Definir criterios de detección, en el área Ámbito de detección, seleccione Nombre DNS y escriba el nombre de dominio completo del equipo UNIX o Linux que desee agregar.6. En el área Credenciales, escriba el nombre de usuario y la contraseña de una cuenta válida y, a continuación, haga clic en Aceptar.7. En la página Método de detección, asegúrese de que no se haya seleccionado Habilitar detección basada en SSH. Si es necesario, seleccione el servidor de administración que usó para firmar el certificado y, a continuación, haga clic en Detectar.8. En la página Seleccionar los equipos que se administrarán, seleccione el equipo y, a continuación, haga clic en Siguiente.9. En la página Resumen, haga clic en Listo. |

Uso de firewalls con Operations Manager 2007

Guía de configuración de seguridad

La Guía de configuración de seguridad de Microsoft Operations Manager 2007 proporciona información esencial sobre cómo proteger más o aumentar la seguridad del entorno Operations Manager 2007 mediante el asistente para configuración de seguridad (SCW). SCW es una herramienta de reducción de la superficie expuesta a ataques para productos que ejecutan los sistemas operativos de Windows Server 2003 Service Pack 1 (SP1), sistemas operativos de Windows Server 2003 Service Pack 2 (SP2) y sistemas operativos de Windows Server 2003 R2.

Además de útiles recomendaciones prácticas de configuración, esta guía incluye información sobre cómo actualizar un agente que se ha bloqueado, cómo personalizar números de puerto que han cambiado las configuraciones predeterminadas y algunos ejemplos para aumentar la seguridad de un servidor y un agente. Aunque casi todos los administradores de servidores se pueden beneficiarse de esta guía, tiene por objeto producir las mayores ventajas para administradores responsables de la seguridad de Operations Manager 2007. Para obtener más información, consulte [Funciones del SCW y guía de configuración de seguridad de System Center Operations Manager 2007 para Windows Server 2003](http://go.microsoft.com/fwlink/?LinkId=120136) (http://go.microsoft.com/fwlink/?LinkId=120136).

Conexión a Almacenamiento de datos de informes a través de un firewall

En esta sección se describe cómo configurar el entorno para que se pueda ubicar un almacén de datos de informes tras un firewall.

Nota

No está permitido separar la consola de Operations, el servidor de administración raíz, el servidor de administración o el servidor de informes por un firewall o a través de un límite de confianza.

En un entorno en el que el almacenamiento de datos de informes está separado del servidor de administración raíz y el servidor de informes mediante un firewall, no se puede usar la autenticación integrada de Windows. Es necesario realizar los pasos para configurar la autenticación de SQL Server. En las siguientes secciones se explica cómo habilitar la autenticación de SQL Server entre el servidor de administración raíz (o el servidor de administración), el servidor de informes y el almacenamiento de datos de informes, como se muestra en la ilustración siguiente.



Servidor de administración y almacenamiento de datos de informes

Los siguientes pasos son necesarios para habilitar la autenticación de SQL Server:

1. En el equipo que hospeda el almacenamiento de datos de infomes, cree un inicio de sesión SQL en la función adecuada para lectura y escritura. Las credenciales proporcionadas para esta cuenta deben pertenecer a las siguientes funciones en la base de datos OperationsManagerDW en el equipo que ejecuta SQL Server:

a. OpsMgrWriter

b. db\_owner (solamente para el grupo de administración propietario en la base de datos)

2. En el equipo que hospeda el servidor de administración raíz, cree una Cuenta de ejecución (de tipo simple) con las credenciales indicadas en el paso anterior.

3. Asocie la Cuenta de ejecución con el Perfil de ejecución denominado cuenta de autenticación de SQL Server de almacenamiento de datos, para ello establezca como destino del Perfil de ejecución a cada uno de los servidores de administración. Para obtener más información, consulte [Cambio de la cuenta de identificación asociada a un perfil de identificación](#z146d6c71df244a14a620d3a8b7e97643) en esta guía.

Si hay un firewall entre el servidor de administración y el almacenamiento de datos de informes, será necesario abrir el puerto 1433.

Servidor de informes y almacenamiento de datos de informes

Si hay un firewall o límite de confianza en el servidor de informes y el almacenamiento de datos de informes, será necesario establecer comunicaciones de punto a punto.

La cuenta que se especificó como cuenta de lectura de datos durante la instalación de Reporting se convierte en la cuenta de ejecución del servidor de informes y es esa cuenta la que se utilizará para conectar con el almacenamiento de datos de informes.

Es necesario determinar qué número de puerto usa el equipo que ejecuta SQL Server en almacenamiento de datos de informes y escribir este número en la tabla dbo.MT\_DataWarehouse de la base de datos OperationsManager. Consulte [Configuración del almacenamiento de datos de informes para escuchar en un puerto TCP/IP específico](#ze76d2ccf9c4e4099a5c2986ff642b39e) en esta guía.

Servidor de informes y servidor de administración raíz separados por un firewall

Es posible que aparezca un mensaje "No se puede verificar si el usuario actual está en la función sysadmin" al instalar Reporting si el servidor de informes y el servidor de administración de raíz están separados por un firewall. Este mensaje de error puede aparecer incluso si se han abierto puertos de firewall adecuados. Este mensaje de error aparece después de escribir el nombre del equipo del servidor de administración de raíz y hacer clic en Siguiente. Este error puede aparecer también porque la instalación de Reporting no pudo conectarse a la base de datos OperationsManager en el servidor de administración raíz. En este entorno será necesario determinar qué número de puerto va a usar el equipo que ejecuta SQL Server y configurar la base de datos OperationsManager para que use ese número de puerto. Consulte [Configuración de la base de datos OperationsManager para escuchar en un puerto TCP/IP específico](#z95dfcc61c9374470ace5328d574732fc) en esta guía.

Asignación de puertos

En la tabla siguiente se muestra la interacción de componentes de Operations Manager 2007 a través de un firewall, incluida información acerca de los puertos usados para la comunicación entre componentes, la dirección para la que se debe abrir el puerto entrante y si se puede cambiar el número de puerto.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Componente A de Operations Manager 2007 SP1 | Número de puerto y dirección | Componente B de Operations Manager 2007 SP1 | Configurable | Nota |
| servidor de administración raíz  | 1433 ---> | Base de datos OperationsManager | Sí (instalación) |   |
| servidor de administración  | 1433 ---> | Base de datos OperationsManager | Sí (instalación) |   |
| servidor de administración | 5723, 5724 ---> | servidor de administración raíz  | No | El puerto 5724 debe estar abierto para instalar este componente y se puede cerrar después de haber instalado este componente. |
| servidor de puerta de enlace | 5723 ---> | servidor de administración raíz  | No |   |
| servidor de administración raíz | 1433 ---> | Almacenamiento de datos de informes | No |   |
| Servidor de informes | 5723, 5724 ---> | servidor de administración raíz  | No | El puerto 5724 debe estar abierto para instalar este componente y se puede cerrar después de haber instalado este componente. |
| Consola de Operations  | 5724 ---> | servidor de administración raíz | No |   |
| Origen del marco del conector  | 51905 ---> | servidor de administración raíz | No |   |
| Servidor de consola web  | 5724 ---> | servidor de administración raíz | No |   |
| Explorador de consola Web | 51908 ---> | Servidor de consola web | Sí (Administración de IIS) | El puerto 51908 es el puerto predeterminado usado al seleccionar la autenticación de Windows. Si selecciona Autenticación de formularios, deberá instalar un certificado SSL y configurar un puerto disponible para la funcionalidad https del sitio Web de la consola Web de Operations Manager 2007. |
| servidor de administración raíz conectado (local) | 5724 ---> | servidor de administración raíz conectado (conectado) | No |   |
| Agente instalado con MOMAgent.msi | 5723 ---> | servidor de administración raíz  | Sí (instalación) |   |
| Agente instalado con MOMAgent.msi | 5723 ---> | servidor de administración  | Sí (instalación) |   |
| Agente instalado con MOMAgent.msi | 5723 ---> | servidor de puerta de enlace  | Sí (instalación) |   |
| servidor de puerta de enlace | 5723 ---> | servidor de administración  | Sí (instalación) |   |
| Agente (reenviador de servicios de recopilación de auditoría) | 51909 ---> | recopilador de servicios de recopilación de auditoría del servidor de administración | Sí (Registro) |   |
| Datos de supervisión de excepciones sin agentes del cliente  | 51906 ---> | recurso compartido de archivos de supervisión de excepciones sin agente del servidor de administración | Sí (Asistente de supervisión de cliente) |   |
| Datos del Programa de mejora de la experiencia del usuario del cliente  | 51907 ---> | punto (final del Programa de mejora de la experiencia del usuario) del servidor de administración | Sí (Asistente de supervisión de cliente) |   |
| Consola de Operations (informes) | 80 ---> | SQL Reporting Services | No | La consola de Operations utiliza el puerto 80 para conectar con el sitio web de SQL Reporting Services. |
| Servidor de informes  | 1433 ---> | Almacenamiento de datos de informes  | Sí |   |
| servidor de administración (Recopilador de servicios de recopilación de auditoría) | 1433 ---> | Base de datos de servicios de recopilación de auditoría  | Sí |   |

Configuración de la base de datos OperationsManager para escuchar en un puerto TCP/IP específico

Realice los pasos siguientes para configurar un puerto estático para la base de datos OperationsManager:

 Use el administrador de configuración de SQL Server para deshabilitar el direccionamiento del puerto dinámico, especifique un puerto estático, deshabilite y detenga el servicio SQL Server Browser y, a continuación, reinicie el servicio <Instancia> de SQL Server.

 Edite la tabla dbo.MT\_ManagementGroup con el número de puerto estático.

 Edite el registro para configurar el número de puerto estático en el servidor de administración raíz.

Precaución

La modificación incorrecta del Registro puede dañar gravemente el sistema. Antes de realizar cambios en el Registro, debe hacer copia de seguridad de los datos importantes.

Para configurar el número de puerto de la base de datos OperationsManager

|  |
| --- |
| 1. Inicie sesión en el equipo que hospeda la base de datos OperationsManager.2. En el escritorio de Windows, haga clic en Inicio, elija Programas, seleccione Microsoft SQL Server 2005, elija Herramientas de configuración y, a continuación, haga clic en Administrador de configuración de SQL Server.3. En el cuadro de diálogo Administrador de configuración de SQL Server, expanda Configuración de red de SQL Server 2005 y, a continuación, haga clic en Protocolos de <INSTANCIA>.4. En el panel de resultados, haga clic con el botón secundario en TCP/IP y, a continuación, haga clic en Propiedades.5. En el cuadro de diálogo Propiedades TCP/IP, haga clic en la ficha Direcciones IP. 6. Algunas direcciones IP aparecen en el formato IP1, IP2, hasta IPAll. Una de estas direcciones es para la dirección IP del adaptador de bucle invertido, 127.0.0.1. Las direcciones IP adicionales aparecen para cada dirección IP del equipo. Expanda IP1, IP2, hasta IPAll.7. Para las áreas IPn, si el cuadro de diálogo Puertos dinámicos TCP contiene un 0, que indica que el motor de base de datos está escuchando los puertos dinámicos, elimine el 0.8. En el área IPAll, si el cuadro de diálogo Puertos dinámicos TCP contiene un número de puerto (que indica el número de puerto dinámico que se asignó) elimine el número de puerto. 9. En el área IPAll, en el cuadro de diálogo Puerto TCP, escriba el número de puerto estático que desea usar y, a continuación, haga clic en Aceptar.10. En el cuadro de diálogo Administrador de configuración de SQL Server, haga clic en Servicios de SQL Server 2005.11. En el panel de resultados Administrador de configuración de SQL Server, haga clic con el botón secundario en SQL Server Browser y seleccione Propiedades.12. En el cuadro de diálogo Propiedades de SQL Server Browser, haga clic en la ficha Servicio.13. En la ficha Servicio, haga clic en Modo de inicio. En la lista Modo de inicio, haga clic en Deshabilitado y, a continuación, en Aceptar.14. En el panel de resultados del administrador de configuración de SQL Server, haga clic con el botón secundario en SQL Server Browser y, a continuación, haga clic en Detener.15. En el panel de resultados, haga clic con el botón secundario en SQL Server (<nombre de instancia>) y, a continuación, haga clic en Reiniciar.16. Cierre el Administrador de configuración de SQL Server. |

Para escribir el número de puerto de SQL Server en la tabla dbo.MT\_ManagementGroup

|  |
| --- |
| 1. En el equipo que hospeda la base de datos OperationsManager, en el escritorio de Windows, haga clic en Inicio, Programas, Microsoft SQL Server 2005 y, a continuación, en SQL Server Management Studio.2. En el cuadro de diálogo Conectar a servidor, en la lista Tipo de servidor, seleccione Motor de base de datos.3. En la lista Nombre de servidor, escriba el nombre del servidor, la instancia y el número de puerto para su base de datos OperationsManager (por ejemplo, equipo\<instancia>).4. En la lista Autenticación, seleccione Autenticación de Windows y, a continuación, haga clic en Conectar.5. En el panel de exploración de objetos, expanda Bases de datos y OperationsManager, expanda Tablas, haga clic con el botón secundario en dbo.MT\_ManagementGroup y, a continuación, haga clic en Abrir tabla.6. En el panel de resultados, desplácese a la derecha hasta la columna titulada SQLServerName\_<guid>. 7. En la primera fila, escriba equipo\<instancia> seguido de una coma, un espacio y, a continuación, el número de puerto de SQL Server (por ejemplo, equipo\INSTANCIA1, <puerto>).8. Haga clic en Archivo y, a continuación, en Salir. |

Para editar el registro en el servidor de administración raíz

|  |
| --- |
| 1. Inicie sesión en el equipo que hospeda el servidor de administración raíz.2. En el escritorio de Windows, haga clic en Inicio, seleccione Ejecutar, escriba regedit y, a continuación, haga clic en Aceptar.3. En la página Editor del Registro, expanda HKEY\_LOCAL\_MACHINE, SOFTWARE, Microsoft, Microsoft Operations Manager y 3.0 y, a continuación, haga clic en Instalación.4. En el panel de resultados, haga clic con el botón secundario en DatabaseServerName y, a continuación, haga clic en Modificar.5. En el cuadro de diálogo Editar cadena, en el cuadro de texto Información del valor, anexe la entrada del nombre del servidor de la base de datos con una coma y un espacio y, a continuación, escriba el número del puerto. Por ejemplo, <nombre\_de\_equipo>\<instancia>, <número de puerto>.6. Haga clic en Aceptar. |

Configuración del almacenamiento de datos de informes para escuchar en un puerto TCP/IP específico

Realice los procedimientos siguientes para configurar un puerto estático para el almacenamiento de datos de informes:

 Use el administrador de configuración de SQL Server para deshabilitar el direccionamiento del puerto dinámico, especifique un puerto estático, deshabilite y detenga el servicio SQL Server Browser y, a continuación, reinicie el servicio <Instancia> de SQL Server.

 Edite la tabla dbo.MT\_ManagementGroup con el número de puerto estático.

 Edite la tabla dbo.MemberDatabase con el número de puerto estático.

 Edite el registro para configurar el número de puerto estático en el servidor de administración raíz.

Precaución

La modificación incorrecta del Registro puede dañar gravemente el sistema. Antes de realizar cambios en el Registro, debe hacer copia de seguridad de los datos importantes.

 Edite la configuración de SQL Server Reporting Services.

Para configurar el número de puerto de la base de datos OperationsManager

|  |
| --- |
| 1. Inicie sesión en el equipo que hospeda el almacenamiento de datos de informes.2. En el escritorio de Windows, haga clic en Inicio, elija Programas, seleccione Microsoft SQL Server 2005, elija Herramientas de configuración y, a continuación, haga clic en Administrador de configuración de SQL Server.3. En el cuadro de diálogo Administrador de configuración de SQL Server, expanda Configuración de red de SQL Server 2005 y, a continuación, haga clic en Protocolos de <INSTANCIA>.4. En el panel de resultados, haga clic con el botón secundario en TCP/IP y, a continuación, haga clic en Propiedades.5. En el cuadro de diálogo Propiedades TCP/IP, haga clic en la ficha Direcciones IP. 6. Algunas direcciones IP aparecen en el formato IP1, IP2, hasta IPAll. Una de estas direcciones es para la dirección IP del adaptador de bucle invertido, 127.0.0.1. Las direcciones IP adicionales aparecen para cada dirección IP del equipo. Expanda IP1, IP2, hasta IPAll.7. Para las áreas IPn, si el cuadro de diálogo Puertos dinámicos TCP contiene un 0, que indica que el motor de base de datos está escuchando los puertos dinámicos, elimine el 0.8. En el área IPAll, si el cuadro Puertos dinámicos TCP contiene un número de puerto (que indica el número de puerto dinámico que se asignó), elimine el número de puerto. 9. En el área IPAll, en el cuadro de diálogo Puerto TCP, escriba el número de puerto estático que desea usar y, a continuación, haga clic en Aceptar.10. En el cuadro de diálogo Administrador de configuración de SQL Server, haga clic en Servicios de SQL Server 2005.11. En el panel de resultados Administrador de configuración de SQL Server, haga clic con el botón secundario en SQL Server Browser y seleccione Propiedades.12. En el cuadro de diálogo Propiedades de SQL Server Browser, haga clic en la ficha Servicio.13. En la ficha Servicio, haga clic en Modo de inicio. En la lista Modo de inicio, haga clic en Deshabilitado y, a continuación, en Aceptar.14. En el panel de resultados del administrador de configuración de SQL Server, haga clic con el botón secundario en SQL Server Browser y, a continuación, haga clic en Detener.15. En el panel de resultados, haga clic con el botón secundario en SQL Server (<nombre de instancia>) y, a continuación, haga clic en Reiniciar.16. Cierre el Administrador de configuración de SQL Server. |

Para escribir el número de puerto de SQL Server en la tabla dbo.MT\_ManagementGroup

|  |
| --- |
| 1. En el equipo que hospeda la base de datos OperationsManager, en el escritorio de Windows, haga clic en Inicio, Programas, Microsoft SQL Server 2005 y, a continuación, en SQL Server Management Studio.2. En el cuadro de diálogo Conectar a servidor, en la lista Tipo de servidor, seleccione Motor de base de datos.3. En la lista Nombre de servidor, escriba el servidor y la instancia de la base de datos OperationsManager (por ejemplo, equipo\INSTANCIA1).4. En la lista Autenticación, seleccione Autenticación de Windows y, a continuación, haga clic en Conectar.5. En el panel de exploración de objetos, expanda Bases de datos y OperationsManager, expanda Tablas, haga clic con el botón secundario en dbo.MT\_DataWarehouse y, a continuación, haga clic en Abrir tabla.6. En el panel de resultados, desplácese a la derecha hasta la columna titulada MainDatabaseServerName\_<guid>. 7. En la primera fila, escriba equipo\<instancia> seguido de una coma, un espacio y, a continuación, el número de puerto de SQL Server (por ejemplo, equipo\<instancia>, <puerto>).8. Haga clic en Archivo y, a continuación, en Salir. |

Para escribir el número de puerto de SQL Server en la tabla dbo.MemberDatabase

|  |
| --- |
| 1. En el equipo que hospeda el almacenamiento de datos de informes, en el escritorio de Windows, haga clic en Inicio, Programas, Microsoft SQL Server 2005 y, a continuación, en SQL Server Management Studio.2. En el cuadro de diálogo Conectar a servidor, en la lista Tipo de servidor, seleccione Motor de base de datos.3. En la lista Nombre de servidor, escriba el servidor y la instancia de la base de datos OperationsManager (por ejemplo, equipo\<instancia>).4. En la lista Autenticación, seleccione Autenticación de Windows y, a continuación, haga clic en Conectar.5. En el panel de exploración de objetos, expanda Bases de datos y OperationsManagerDW, expanda Tablas, haga clic con el botón secundario en dbo.MemberDatabase y, a continuación, haga clic en Abrir tabla.6. En el panel de resultados, desplácese a la derecha hasta la columna titulada Nombre de servidor. 7. En la primera fila, escriba equipo\<instancia> seguido de una coma, un espacio y, a continuación, el número de puerto de SQL Server (por ejemplo, equipo\<instancia>, <puerto>).8. Haga clic en Archivo y, a continuación, en Salir. |

Para editar el registro en el servidor de informes

|  |
| --- |
| 1. Inicie sesión en el equipo que hospeda el servidor de administración raíz.2. En el escritorio de Windows, haga clic en Inicio, seleccione Ejecutar, escriba regedit y, a continuación, haga clic en Aceptar.3. En la página Editor del Registro, expanda HKEY\_LOCAL\_MACHINE, SOFTWARE, Microsoft, MicrosoftOperations Manager y 3.0 y, a continuación, haga clic en Informes.4. En el panel de resultados, haga clic con el botón secundario en DWDBInstance y, a continuación, haga clic en Modificar.5. En el cuadro de diálogo Editar cadena, en el cuadro de texto Información del valor, anexe la entrada del nombre del servidor de la base de datos con una coma y un espacio y, a continuación, escriba el número del puerto. Por ejemplo, <nombre\_de\_equipo>\<instancia>, <número de puerto>.6. Haga clic en Aceptar. |

Para editar SQL Server Reporting Services

|  |
| --- |
| 1. Inicie sesión en el equipo que hospeda el servidor de administración raíz.2. Inicie Internet Explorer y conéctese a http://<nombre de equipo>/informes$<nombre de instancia>.3. Haga clic en la ficha Contenido.4. En el lado derecho de la barra de herramientas, haga clic en Mostrar detalles.5. Haga clic en Principal de almacenamiento de datos.6. En el cuadro de texto Cadena de conexión, busque la línea origen=<equipo>\<instancia>;inicial.7. Anexe el nombre de instancia con una coma y un espacio y, a continuación, escribe al número de puerto estático. Por ejemplo, origen=<equipo>\<instancia>, <puerto>;inicial.8. Haga clic en Aplicar y, a continuación, cierre el explorador. |

Uso de certificados con ACS en Operations Manager 2007

Cuando el reenviador del Servicio de recopilación de auditorías (ACS) se encuentra en un dominio separado del dominio en el que se encuentra el recopilador de ACS, y no existe confianza bidireccional entre los dos dominios, se deben usar certificados para que pueda tener lugar la autenticación entre el reenviador de ACS y el recopilador de ACS.

Se da por supuesto que los siguientes eventos ya han tenido lugar en el equipo que hospeda el reenviador de ACS antes de configurar certificados para ACS:

 Se ha instalado un agente en el equipo que servirá de reenviador de ACS. Para obtener más información, consulte el tema [Implantación del agente Operations Manager 2007 con el Asistente para la instalación del agente](http://go.microsoft.com/fwlink/?LinkId=91128) (http://go.microsoft.com/fwlink/?LinkId=91128).

 Se ha instalado un certificado (y un certificado de la entidad de certificación [CA]) en el equipo que hospeda el agente. Para obtener más información, consulte el tema [Certificados en Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=91129) (http://go.microsoft.com/fwlink/?LinkId=91129).

En el equipo que hospeda el recopilador de ACS, se supone que se ha realizado lo siguiente antes de configurar certificados para ACS.

 Se ha instalado un certificado (y un certificado de CA) en el servidor de administración que hospeda el recopilador de ACS. Para obtener más información, consulte el tema [Certificados en Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=91129) (http://go.microsoft.com/fwlink/?LinkId=91129).

 Se ha aprobado el agente pendiente y la comunicación entre el agente y el servidor de administración funciona correctamente (el agente aparece como Correcto en la consola de Operations Manager y los módulos de administración se han implementado en el agente). Para obtener más información, consulte el tema [Aprobación de un agente Operations Manager 2007 instalado para un grupo de administración con MOMAgent.msi](http://go.microsoft.com/fwlink/?LinkId=91130) (http://go.microsoft.com/fwlink/?LinkId=91130).

 Se han instalado el recopilador y la base de datos de ACS. Para obtener más información, consulte el tema [Instalación de un recopilador y una base de datos de ACS](http://go.microsoft.com/fwlink/?LinkId=91142) (http://go.microsoft.com/fwlink/?LinkId=91142).

A continuación, se muestra información general de alto nivel de los pasos que son necesarios realizar para usar certificados con ACS.

Nota

Los certificados usados en diversos componentes de Operations Manager 2007 (por ejemplo, recopilador de ACS, reenviador de ACS, agente, servidor de puerta de enlace, servidor de administración o servidor de administración raíz) deben ser emitidos por la misma CA.

En el equipo que hospeda el recopilador de ACS:

 Ejecute ADTServer -c.

 Asigne el certificado del reenviador de ACS en Active Directory.

 En la consola de Operations Manager, habilite ACS.

En el equipo que hospeda el reenviador de ACS:

 Exporte el certificado a un disco, una unidad flash USB o un recurso compartido de red.

 Ejecute ADTAgent -c.

Vea también

[Configuración de certificados en el recopilador de ACS en Operations Manager 2007](#z37a183962d9048dcadebd05efb1f5bc9)

[Configuración de certificados en el reenviador de ACS en Operations Manager 2007](#zbf6d6411846048b3b367a58ac543bcfa)

Configuración de certificados en el recopilador de ACS en Operations Manager 2007

Una vez se hayan instalado los certificados entre el agente y el servidor de administración y se haya implementado ACS, realice los procedimientos siguientes en los equipos que hospeden el recopilador de ACS como parte de los pasos necesarios para que ACS pueda usar certificados.

Nota

Una vez que haya completado estos procedimientos, tendrá que habilitar los reenviadores de ACS. Para obtener más información, consulte el tema [How To Enable ACS Forwarders In Operations Manager 2007 (Habilitación de reenviadores de ACS en Operations Manager 2007)](http://go.microsoft.com/fwlink/?LinkId=91143) (http://go.microsoft.com/fwlink/?LinkId=91143).

Para asignar un certificado al recopilador de ACS

|  |
| --- |
| 1. En el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba cmd y, a continuación, haga clic en Aceptar.3. En el símbolo del sistema, escriba <letra\_unidad>: (donde <letra\_unidad> es la unidad en la que está instalado el sistema operativo) y, a continuación, presione Entrar.4. Escriba cd %systemroot% y, a continuación, presione Entrar.5. Escriba cd system32\security\adtserver y, a continuación, presione Entrar.6. Escriba net stop adtserver y, a continuación, presione Entrar.7. Escriba adtserver -c y, a continuación, presione Entrar.8. En la lista numerada de certificados, busque el certificado usado para Operations Manager, escriba el número de la lista (debe ser 1) y, a continuación, presione Entrar.9. Escriba net start adtserver y, a continuación, presione Entrar. |

Para configurar la asignación de nombre al certificado

|  |
| --- |
| 1. Inicie sesión en el equipo que hospede Active Directory.2. En el escritorio de Windows, haga clic en Inicio, seleccione Programas, seleccione Herramientas administrativas y, a continuación, haga clic en Usuarios y equipos de Active Directory.3. Expanda el nombre de dominio, haga clic con el botón secundario en Equipos, seleccione Nuevo y, a continuación, haga clic en Equipo.4. En el cuadro de diálogo Nuevo objeto - Equipo, escriba el nombre NetBIOS del equipo que hospeda el reenviador de ACS y, a continuación, haga clic en Siguiente. Repita este paso para todos los equipos que hospeden un reenviador de ACS.5. En el cuadro de diálogo Administrado, asegúrese de que no esté seleccionado Éste es un equipo administrado, y, a continuación, haga clic en Siguiente.6. En el cuadro de diálogo Nuevo objeto - Equipo, haga clic en Finalizar.7. En Usuarios y equipos de Active Directory, en el panel derecho, haga clic con el botón secundario en el equipo (o equipos) agregados y, a continuación, haga clic en Asignaciones de nombres.8. En el cuadro de diálogo Asignación de identidad de seguridad, haga clic en Certificados X.509 y, a continuación, en Agregar.9. En el cuadro de diálogo Agregar certificado, haga clic en el menú Buscar en, seleccione la ubicación en la que se encuentra el certificado exportado y, a continuación, haga clic en Abrir.10. En el cuadro de diálogo Agregar certificado, asegúrese de seleccionar Usar Asunto para identidad de seguridad alternativa y, a continuación, haga clic en Aceptar.11. En el cuadro de diálogo Asignación de identidad de seguridad, haga clic en Aceptar.12. Repitas los pasos 4–11 para cada equipo que haya agregado. |

Vea también

[Uso de certificados con ACS en Operations Manager 2007](#zb6db0f5df0884020bf876c6a2e38ec13)

[Configuración de certificados en el reenviador de ACS en Operations Manager 2007](#zbf6d6411846048b3b367a58ac543bcfa)

Configuración de certificados en el reenviador de ACS en Operations Manager 2007

Una vez se hayan instalado los certificados entre el agente y el servidor de administración y se haya implementado ACS, realice los procedimientos siguientes en los equipos que hospeden el reenviador de ACS como parte de los pasos necesarios para que ACS pueda usar certificados.

Para exportar el certificado

|  |
| --- |
| 1. En el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba mmc y, a continuación, haga clic en Aceptar.3. En el menú Archivo, haga clic en Agregar o quitar complemento. 4. En el cuadro de diálogo Agregar o quitar complemento, haga clic en Agregar.5. En el cuadro de diálogo Agregar un complemento independiente, haga clic en Certificados y, a continuación, en Agregar.6. En el cuadro de diálogo Complemento de certificados, seleccione Cuenta de equipo y, a continuación, haga clic en Siguiente.7. En el cuadro de diálogo Seleccionar equipo, seleccione Equipo local (el equipo en el que se está ejecutando esta consola) y, a continuación, haga clic en Finalizar.8. En el cuadro de diálogo Agregar un complemento independiente, haga clic en Cerrar.9. En el cuadro de diálogo Agregar o quitar complemento, haga clic en Aceptar.10. En el panel Raíz de consola\Certificados (Equipo local), expanda Certificados (Equipo local), expanda Personal y, a continuación, haga clic en Certificados.11. En el panel de resultados, haga clic con el botón secundario en el certificado que usa para Operations Manager, seleccione Todas las tareas y, a continuación, haga clic en Exportar.12. En la página Bienvenido del Asistente para exportación de certificados, haga clic en Siguiente.13. En la página Exportar la clave privada, seleccione No exportar la clave privada y, a continuación, haga clic en Siguiente.14. En la página Formato de archivo de exportación, seleccione DER binario codificado X.509 (.CER) y, a continuación, haga clic en Siguiente.15. En la página Archivo para exportar, haga clic en Examinar.16. En la página Guardar como, seleccione una carpeta y un nombre de archivo para el certificado, asegúrese de que Guardar como tipo esté establecido en DER binario codificado X.509 (\*.cer) y, a continuación, haga clic en Guardar.Nota Tendrá que copiar este certificado en el equipo que hospeda el recopilador de ACS, por lo que deberá elegir una ubicación desde la que pueda leer el recopilador de ACS, o deberá considerar guardar el certificado en un disco, una unidad flash USB o un recurso compartido de red. Además, es recomendable que incluya el nombre del equipo en el nombre del archivo si exporta certificados desde más de un equipo.17. En la página Archivo para exportar, asegúrese de que la ruta y el nombre del archivo sean correctos, haga clic en Siguiente y, a continuación, haga clic en Finalizar. |

Para ejecutar el comando adtagent

|  |
| --- |
| 1. En el escritorio de Windows, haga clic en Inicio y, a continuación, en Ejecutar.2. En el cuadro de diálogo Ejecutar, escriba cmd y, a continuación, haga clic en Aceptar.3. En el símbolo del sistema, escriba <letra\_unidad>: (donde <letra\_unidad> es la unidad en la que está instalado el sistema operativo) y, a continuación, presione Entrar.4. Escriba cd %systemroot% y, a continuación, presione Entrar.5. Escriba cd system32 y, a continuación, presione Entrar.6. Escriba adtagent -c y, a continuación, presione Entrar.7. Podrá ver una lista numerada de certificados. Busque el certificado usado para Operations Manager, escriba el número de la lista (debe ser 1) y, a continuación, presione Entrar.8. Escriba exit para cerrar la ventana de comandos. |

Vea también

[Configuración de certificados en el recopilador de ACS en Operations Manager 2007](#z37a183962d9048dcadebd05efb1f5bc9)

[Uso de certificados con ACS en Operations Manager 2007](#zb6db0f5df0884020bf876c6a2e38ec13)

Consideraciones de seguridad para la administración sin agentes en Operations Manager 2007

La administración sin agentes le permite supervisar equipos sin instalar un agente en ellos. Por ejemplo, puede usar la administración sin agentes en equipos que están en entornos especiales donde no pueden instalarse agentes.

El servidor de administración se comunica con el equipo administrado sin agentes a través del puerto RPC (TCP 135) y el intervalo de puertos DCOM y, por lo tanto, no se puede usar administración sin agentes de un equipo fuera de un firewall.

Para usar la administración sin agente, la cuenta de acción del servidor de administración debe ser administrador local en el equipo remoto y estar en el mismo dominio, o bien debe existir una relación de confianza entre los dominios. Por ejemplo, un agente proxy con una cuenta de privilegios bajos no podrá tener acceso al espacio de nombres WMI y, por lo tanto, no se podrán ejecutar las reglas, los scripts ni los monitores.

Seguridad de la consola web en Operations Manager 2007

El servidor de consola web proporciona una alternativa basada en explorador al panel Supervisión de la consola de Operations de Operations Manager 2007. El servidor de consola web se suele usar cuando se desea tener acceso a los datos de supervisión de los grupos de administración de Operations Manager 2007 de las siguientes maneras:

 Desde Internet

 Sin instalar la consola de Operations

 Desde una ubicación con conectividad de ancho de banda bajo

 Cuando las notificaciones están configuradas para contener hipervínculos a las alertas correspondientes en la consola web

La instalación de la consola web implica la instalación de un nuevo sitio web y un nuevo grupo de aplicaciones en Internet Information Services (IIS). El nuevo sitio web se denomina consola web de Operations Manager 2007 y el nuevo grupo de aplicaciones se denomina OPWebConsoleApp. El puerto predeterminado para tener acceso a la consola web desde un explorador mediante autenticación basada en Windows es 51908.

Durante la instalación de la consola web, se le solicita que seleccione Autenticación de Windows o Autenticación por formularios. Con la autenticación de Windows, Microsoft recomienda encarecidamente el uso de SSL. Con la Autenticación por formularios, se requiere SSL.

La autenticación de Windows se puede usar si todos los usuarios tienen acceso a Operations Manager desde la intranet.

Nota

El servidor de consola web se debe instalar en el servidor de administración raíz si selecciona Autenticación de Windows.

Si los usuarios acceden a la consola web desde Internet, seleccione Autenticación por formularios.

Nota

Lo más recomendable para obtener acceso a la consola web desde Internet es usar autenticación basada en formularios con SSL con la consola web.

Tanto en la autenticación basada en formularios como en la autenticación basada en Windows, las credenciales que proporcione deben pertenecer a una función de usuario en Operations Manager 2007.

Exponer la consola web en Internet

Lo más recomendable para implementar el acceso a Internet en la consola web es colocar el servidor de consola web en una red perimetral con acceso a Internet. Configure la consola web para usar la autenticación basada en formularios e instale un certificado SSL/TLS en IIS. Tendrá que abrir el puerto 5724 entre el servidor de la consola web y Operations Manager 2007. El canal entre el servidor de consola web y el servidor de administración raíz está cifrado.

Para obtener más información, consulte el artículo de Knowledge Base [Cómo implementar SSL en IIS](http://go.microsoft.com/fwlink/?LinkId=87862) (http://go.microsoft.com/fwlink/?LinkId=87862).

Apéndice A - Lista de operaciones en Operation Manager 2007

Este apéndice proporciona una lista de las operaciones disponibles para cada perfil en Operations Manager 2007.

Operador de informes

El perfil Operador de informes incluye un conjunto de privilegios diseñado para usuarios que necesitan tener acceso a informes. Una función basada en el perfil Operador de informes garantiza a los miembros la capacidad para ver informes conforme al ámbito configurado.

Recuperar la instancia del almacenamiento de datos para el grupo de administración

Escribir en informes favoritos

Eliminar informes favoritos

Leer informes favoritos

Actualizar informes favoritos

Leer informes

Ejecutar informes

Operador de sólo lectura

El perfil Operador de sólo lectura incluye un conjunto de privilegios diseñado para usuarios que necesitan tener acceso de sólo lectura a alertas y vistas. Una función basada en el perfil Operadores de sólo lectura garantiza a los miembros la capacidad para ver alertas y obtener acceso a vistas conforme al ámbito configurado.

Leer alertas

Recuperar la instancia del almacenamiento de datos para el grupo de administración

Leer el estado de una resolución

Leer la instancia de un conector

Leer tareas de consola

Enumerar objetos de diagnóstico

Enumerar los resultados del diagnóstico

Enumerar objetos de detección tal y como se definen en un módulo de administración

Leer reglas de detección

Leer eventos

Escribir en tareas de consola favoritas

Eliminar tareas de consola favoritas

Enumerar tareas de consola favoritas

Actualizar tareas de consola favoritas

Escribir vistas favoritas

Eliminar vistas favoritas

Enumerar vistas favoritas

Actualizar vistas favoritas

Enumerar objetos de supervisión

Enumerar clases de supervisión

Enumerar clases de relación de supervisión

Enumerar módulos de administración

Enumerar tipos de monitor

Enumerar tipos de módulo

Enumerar monitores

Enumerar invalidaciones

Enumerar datos de rendimiento

Enumerar objetos de detección tal y como se definen en un módulo de administración

Enumerar el estado de recuperaciones pasadas

Enumerar la relación entre los objetos supervisados

Enumerar reglas

Enumerar búsquedas guardadas

Actualizar búsquedas guardadas

Escribir en búsquedas guardadas

Eliminar búsquedas guardadas

Enumerar estado

Permite tener acceso a grupos de administración conectados

Enumerar vistas

Enumerar tipos de vistas

Operador

El perfil Operador incluye un conjunto de privilegios diseñado para usuarios que necesitan tener acceso a alertas, vistas y tareas. Una función basada en el perfil Operadores confiere a sus miembros la capacidad de interactuar con las alertas, ejecutar tareas y obtener acceso a vistas en función del ámbito que tengan configurado. El perfil Operador contiene todos los privilegios que se encuentran en el perfil Operador de sólo lectura además de los que se presentan a continuación.

Actualizar alertas

Ejecutar diagnóstico

Crear tareas favoritas

Eliminar tareas favoritas

Enumerar tareas favoritas

Actualizar tareas favoritas

Ejecutar rutinas de recuperación

Actualizar la configuración del modo de mantenimiento

Enumerar acciones de notificación

Eliminar acciones de notificación

Actualizar acciones de notificación

Enumerar extremos de notificación

Enumerar destinatarios de notificación

Eliminar destinatarios de notificación

Actualizar de destinatarios de notificación

Enumerar suscripciones de notificación

Eliminar suscripciones de notificación

Actualizar suscripciones de notificación

Enumerar tareas

Enumerar estado de tarea

Ejecutar tareas

Operador avanzado

El perfil Operador avanzado incluye un conjunto de privilegios diseñado para usuarios que necesitan, además de los privilegios propios de Operador, acceso a una capacidad limitada para modificar las configuraciones de supervisión. Una función basada en el perfil Operadores avanzados confiere a sus miembros la capacidad de invalidar la configuración de reglas y monitores para destinos o grupos de destinos específicos dentro del ámbito configurado. El perfil Operador avanzado contiene todos los privilegios que se encuentran en el perfil Operador y Operador de sólo lectura además de los que se presentan a continuación.

Actualizar módulos de administración

Enumerar plantillas

Autor

El perfil Autor incluye un conjunto de privilegios diseñado para crear la configuración de supervisión. Una función basada en el perfil Autores confiere a sus miembros la capacidad de crear, editar y eliminar la configuración de supervisión (tareas, reglas, monitores y vistas) dentro del ámbito configurado. Si resulta conveniente, se puede configurar que los autores tengan también privilegios de operador avanzado con ámbito delimitado por grupos. El perfil Autor contiene todos los privilegios que se encuentran en el perfil Operador avanzado, Operador y Operador de sólo lectura además de los que se presentan a continuación.

Crear módulos de administración

Eliminar módulos de administración

Enumerar perfiles de ejecución

Administrador

El perfil Administrador incluye plenos privilegios en Operations Manager. No se admiten ámbitos para el perfil Administrador. El perfil Administrador contiene todos los privilegios que se encuentran en el perfil Autor, Operador avanzado, Operador y Operador de sólo lectura además de los que se presentan a continuación.

Crear un estado de resolución

Eliminar un estado de resolución

Actualizar un estado de resolución

Implementar un agente

Reparar o actualizar un agente instalado

Desinstalar un agente

Enumerar configuración de agente

Actualizar configuración de agente

Enumerar agentes

Iniciar o detener la administración de equipos o dispositivos a través de un servicio de mantenimiento proxy

Enumerar equipos o dispositivos administrados a través de un servicio de mantenimiento proxy

Insertar una nueva instancia de un equipo o dispositivo

Eliminar una instancia de un equipo o dispositivo

Ejecutar tarea de detección

Crear eventos

Enumerar configuración global

Actualizar configuración global

Exportar módulos de administración

Enumerar servidores de administración

Eliminar extremo de notificación

Actualizar extremo de notificación

Crear datos de rendimiento

Crear cuentas de ejecución

Eliminar cuentas de ejecución

Enumerar cuentas de ejecución

Actualizar cuentas de ejecución

Crear asignaciones entre cuentas de ejecución y perfiles de ejecución

Eliminar asignaciones entre cuentas de ejecución y perfiles de ejecución

Enumerar asignaciones entre cuentas de ejecución y perfiles de ejecución

Actualizar asignaciones entre cuentas de ejecución y perfiles de ejecución

Crear grupos de administración conectados

Eliminar grupos de administración conectados

Enumerar funciones de usuario

Eliminar funciones de usuario

Actualizar funciones de usuario

Escribir informes favoritos

Eliminar informes favoritos

Leer informes favoritos

Actualizar informes favoritos

Leer informes

Ejecutar informes

Administrador de seguridad de informes

El perfil Administrador de seguridad de informes incluye un conjunto de privilegios diseñado para habilitar la integración de la seguridad de SQL Server Reporting Services con Operations Manager.

Exportar módulos de administración

Enumerar clases definidas en los módulos de administración

Enumerar módulos de administración

Ejecutar informes

Enumerar reglas

Apéndice B - Lista de valores hash para agentes de UNIX y Linux

Este apéndice indica los valores hash para valores binarios de agentes para equipos basados en UNIX y Linux.

Valores hash de MD5

|  |  |  |
| --- | --- | --- |
| Agente | Archivo | Hash de MD5 |
| AIX 5.3 POWER | scx-1.0.4-248.aix.5.ppc.lpp.gz | a8ef3ebbed8cef7e98030b77ce01079f |
| AIX 6.1 POWER | scx-1.0.4-248.aix.6.ppc.lpp.gz | 9d9a43a34576cc29cd150b947017d3fe |
| HPUX 11iv2 IA64 | scx-1.0.4-248.hpux.11iv2.ia64.depot.Z | 6d4faad6e35830d8df01cf2afcc33243 |
| HPUX 11iv2 PARISC | scx-1.0.4-248.hpux.11iv2.parisc.depot.Z | 12a611c53a9f02b8c49be1a6d4966e58 |
| HPUX 11iv3 IA64 | scx-1.0.4-248.hpux.11iv3.ia64.depot.Z | 855518128e2a96b976b2dbdca6dec164 |
| HPUX 11iv3 PARISC | scx-1.0.4-248.hpux.11iv3.parisc.depot.Z | 5a08f1eadb99dc30d1ec25b2a8add395 |
| RHEL 4 x64 | scx-1.0.4-248.rhel.4.x64.rpm | 4e6a0800d2a579c35837373ee988a3f2 |
| RHEL 4 x86 | scx-1.0.4-248.rhel.4.x86.rpm | 5d059616e158d0cb0d36e43c81e4b218 |
| RHEL 5 x64 | scx-1.0.4-248.rhel.5.x64.rpm | 1f47c05508f94ecd4329facbf6ff4d97 |
| RHEl 5 x86 | scx-1.0.4-248.rhel.5.x86.rpm | ac291fff0ae029c46b4bb9b0fc65226e |
| SLES 9 x86 | scx-1.0.4-248.sles.9.x86.rpm | 2a81ce3f40eabe605f1c8ddcad141c28 |
| SLES 10 x64 | scx-1.0.4-248.sles.10.x64.rpm | 9911d90e16445b32ecc4d6aed9775ff1 |
| SLES 10 x86 | scx-1.0.4-248.sles.10.x86.rpm | 04f77082ddb4c12da045b298dc1eab61 |
| Solaris 8 SPARC | scx-1.0.4-248.solaris.8.sparc.pkg.Z | b3f5ab647d34d54b43f0810bb002f4c6 |
| Solaris 9 SPARC | scx-1.0.4-248.solaris.9.sparc.pkg.Z | eb67396ee081155615b5a2d5e851a176 |
| Solaris 10 SPARC | scx-1.0.4-248.solaris.10.sparc.pkg.Z | 99ed166b51517b4356f66276b2b223dc |
| Solaris 10 x86 | scx-1.0.4-248.solaris.10.x86.pkg.Z | dcf30dc553939aed648d0353342005cd |

Valores hash de SHA1

|  |  |  |
| --- | --- | --- |
| Agente | Archivo | SHA1 |
| AIX 5.3 POWER | scx-1.0.4-248.aix.5.ppc.lpp.gz | da18adfccd7eae140ddca6177b9470e0b5776dfc |
| AIX 6.1 POWER | scx-1.0.4-248.aix.6.ppc.lpp.gz | cf702d3e13254eb6c8eb476c748eba346b5e775b |
| HPUX 11iv2 IA64 | scx-1.0.4-248.hpux.11iv2.ia64.depot.Z | ceaf9b0d732ac94184d7ccedfdb2e3b4c1b761d7 |
| HPUX 11iv2 PARISC | scx-1.0.4-248.hpux.11iv2.parisc.depot.Z | cfa64d3d29f4ce7404229c6418983946cb46d415 |
| HPUX 11iv3 IA64 | scx-1.0.4-248.hpux.11iv3.ia64.depot.Z | 2e33c132f73e8355f663c864e9c5f39ac4a7c1c0 |
| HPUX 11iv3 PARISC | scx-1.0.4-248.hpux.11iv3.parisc.depot.Z | e1836db997d1992fdf9a0d2c9b41938f5bf880ec |
| RHEL 4 x64 | scx-1.0.4-248.rhel.4.x64.rpm | 7061fbaa60f7b7b260445a26a0783f2b663c18df |
| RHEL 4 x86 | scx-1.0.4-248.rhel.4.x86.rpm | a36c7c3abed1db65bf1c21d5d1eb0b30ef57afe3 |
| RHEL 5 x64 | scx-1.0.4-248.rhel.5.x64.rpm | c112b0093c020615ee93e61b32e8f705a0f324b3 |
| RHEl 5 x86 | scx-1.0.4-248.rhel.5.x86.rpm | 9bf4a5e8acaf24497cd24bf16017a1b173cb1d50 |
| SLES 9 x86 | scx-1.0.4-248.sles.9.x86.rpm | 63796e9167ce6a04fe82eb5202c3c98dfa0dd37c |
| SLES 10 x64 | scx-1.0.4-248.sles.10.x64.rpm | 391004f7535a7185d6817ed327c024b2d0e3777a |
| SLES 10 x86 | scx-1.0.4-248.sles.10.x86.rpm | b6b9923b47753d013b69f1abd638f1a9c0788234 |
| Solaris 8 SPARC | scx-1.0.4-248.solaris.8.sparc.pkg.Z | 08c2059863c4aaa5ee79790a83bb8f9da4b3240a |
| Solaris 9 SPARC | scx-1.0.4-248.solaris.9.sparc.pkg.Z | 21f14b470de0e8d311c66d55e438c55688c5aadf |
| Solaris 10 SPARC | scx-1.0.4-248.solaris.10.sparc.pkg.Z | de0ddcf80dce18e0599ec20d29b57145126cee55 |
| Solaris 10 x86 | scx-1.0.4-248.solaris.10.x86.pkg.Z | 499526bb43cb3ce9db6d7cf122b6bd5f15858bb4 |

Valores hash de SHA256

|  |  |  |
| --- | --- | --- |
| Agente | Archivo | SHA256 |
| AIX 5.3 POWER | scx-1.0.4-248.aix.5.ppc.lpp.gz | 40f93e6c5dabc07ae983814bd24bae2f9f53448dcd51d5cb4ac43e47e51a2506 |
| AIX 6.1 POWER | scx-1.0.4-248.aix.6.ppc.lpp.gz | 670e02e9af19bb3aea0593947676843faf6c360694bed41cd3a0bc0fd20fbbcc |
| HPUX 11iv2 IA64 | scx-1.0.4-248.hpux.11iv2.ia64.depot.Z | a60e92bcfb53b7d49bfb2dcc909690cb955800922fd54e496a27796e684ec3fc |
| HPUX 11iv2 PARISC | scx-1.0.4-248.hpux.11iv2.parisc.depot.Z | 553390b3ef4cc21375bc307855bb16c9865b196c4403605fe1df079f9f503d74 |
| HPUX 11iv3 IA64 | scx-1.0.4-248.hpux.11iv3.ia64.depot.Z | f102b4c36447b1a2c6a6b374228fba03ec0547e3750826a94578d28a219f516a |
| HPUX 11iv3 PARISC | scx-1.0.4-248.hpux.11iv3.parisc.depot.Z | 8d43eab9b481d51f4b9efb74ec5eb03e08eb5d8556032e745588e9b3a2eb327d |
| RHEL 4 x64 | scx-1.0.4-248.rhel.4.x64.rpm | 382b7d7afd1075cc188626b59b8f48b1c7666bdfc29c6bed1ab3e8191c9394fe |
| RHEL 4 x86 | scx-1.0.4-248.rhel.4.x86.rpm | 281d51128b98526f2223fcea93ebd72cf1b46ee81f4f5a65a08c17d39c2fb7dc |
| RHEL 5 x64 | scx-1.0.4-248.rhel.5.x64.rpm | 6448da9d2fbdc75e662255edbf22e4523c38f614baf9a0bcea9795a17be578d4 |
| RHEl 5 x86 | scx-1.0.4-248.rhel.5.x86.rpm | 70408343a052ea77960315dd76ff70b9b42aad2c8c41c50997e2d5e2d30f0b1d |
| SLES 9 x86 | scx-1.0.4-248.sles.9.x86.rpm | e628120ae89004d828bd8334330b2c44ea6cb165985b39149d28084e8849f86a |
| SLES 10 x64 | scx-1.0.4-248.sles.10.x64.rpm | 20be0a828a355f907f9a8a7dedbd8900e83f9be14b304c10054d9619b0c9998d |
| SLES 10 x86 | scx-1.0.4-248.sles.10.x86.rpm | 854262692e324bcbf78501a6b5d5199a10b4e608bcbed6524a82bee205d1f256 |
| Solaris 8 SPARC | scx-1.0.4-248.solaris.8.sparc.pkg.Z | ad3754a5064d7733b7b096c111efbf5630927852c07b16ea0799bf7aefb1740a |
| Solaris 9 SPARC | scx-1.0.4-248.solaris.9.sparc.pkg.Z | 81bec81c17ea8a86833accbda8c6045147b08f38b600b7cea0dcc730a59b2d90 |
| Solaris 10 SPARC | scx-1.0.4-248.solaris.10.sparc.pkg.Z | a37a23b3ec25f8c1294c248d13cb73bbe5a7ea8fe2631bfbb42c847f724a90da |
| Solaris 10 x86 | scx-1.0.4-248.solaris.10.x86.pkg.Z | 54abb0189e2b70c13644c901dc495b045bdc1e2a087a634b222ca42b4826d6c9 |