CA Nimsoft Monitor

Guía del usuario de detección

v7.5

Marzo 2014

Avisos legales

Este sistema de ayuda en línea (el "Sistema") se proporciona con el único propósito de informar al usuario final, pudiendo CA proceder a su modificación o retirada en cualquier momento.

Queda prohibida la copia, transferencia, reproducción, divulgación, modificación o duplicación de la totalidad o parte de este Sistema sin el consentimiento previo y por escrito de CA. Este sistema es información confidencial y propiedad de CA. Está protegido por las leyes sobre los derechos de autor de los Estados Unidos y por tratados internacionales. Este sistema no puede ser divulgado por el usuario ni puede ser utilizado para ningún otro propósito distinto, a menos que haya sido autorizado en virtud de un acuerdo suscrito aparte entre el usuario y CA que rija el uso del software de CA al que se refiere el Sistema (el "Software de CA"). Dicho acuerdo no se verá modificado por ninguno de los los términos de este aviso.

No obstante lo anterior, si dispone de licencias del Software de CA, podrá realizar una copia del Sistema para su uso interno y de sus empleados, siempre y cuando en dicha copia figuren todos los avisos e inscripciones relativos a los derechos de autor de CA..

El derecho a realizar una copia del Sistema solo tendrá validez durante el período en el que la licencia correspondiente al Software de CA esté en vigor. En caso de terminarse la licencia por cualquier razón, es responsabilidad del usuario certificar por escrito a CA que todas las copias, totales o parciales, del Sistema han sido destruidas.

EN LA MEDIDA EN QUE LA LEY APLICABLE LO PERMITA, CA PROPORCIONA ESTE SISTEMA "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO INCLUIDAS, ENTRE OTRAS PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN FIN CONCRETO Y NO INCUMPLIMIENTO. CA NO RESPONDERÁ EN NINGÚN CASO, ANTE VD. NI ANTE TERCEROS, EN LOS SUPUESTOS DE DEMANDAS POR PÉRDIDAS O DAÑOS, DIRECTOS O INDIRECTOS, QUE SE DERIVEN DEL USO DE ESTE SISTEMA INCLUYENDO A TÍTULO ENUNCIATIVO PERO SIN LIMITARSE A ELLO, LA PÉRDIDA DE BENEFICIOS Y DE INVERSIONES, LA INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL, LA PÉRDIDA DEL FONDO DE COMERCIO O LA PÉRDIDA DE DATOS, INCLUSO CUANDO CA HUBIERA PODIDO SER ADVERTIDA CON ANTELACIÓN Y EXPRESAMENTE DE LA POSIBILIDAD DE DICHAS PÉRDIDAS O DAÑOS.

CA es el fabricante de este Sistema.

Este Sistema presenta "Derechos Restringidos". El uso, la duplicación o la divulgación por parte del gobierno de los Estados Unidos está sujeta a las restricciones establecidas en las secciones 12.212, 52.227-14 y 52.227-19(c)(1) - (2) de FAR y en la sección 252.227-7014(b)(3) de DFARS, según corresponda, o en posteriores.

La información legal de software de terceros y de dominio público utilizado en la solución de CA Nimsoft Monitor se documenta en *Licencias de terceros y términos de uso de CA Nimsoft Monitor (*http://docs.nimsoft.com/prodhelp/en_US/Library/Legal.html*).*

Contacte con CA

Contacto con CA Support

Para su comodidad, CA Technologies proporciona un sitio en el que se puede acceder a la información que necesita acerca de los productos de CA para la oficina en casa, pequeñas empresas y acerca de los productos de CA Technologies de empresa. Desde la página http://ca.com/es/support, se puede acceder a los siguientes recursos:

- Información para el contacto telefónico y en línea para poder acceder a los servicios de atención al cliente y de asistencia técnica
- Información sobre foros y comunidades de usuarios
- Descargas de documentación y productos
- Políticas y directrices de CA Support
- Otros recursos útiles adecuados para el producto

Cómo proporcionar comentarios sobre la documentación del producto

Envíe comentarios o preguntas acerca de la documentación del producto de CA Technologies Nimsoft a nimsoft.techpubs@ca.com.

Si desea proporcionar comentarios sobre la documentación de productos de CA Technologies, rellene nuestra breve encuesta de clientes que está disponible en el sitio web de CA Support que se encuentra en http://ca.com/docs.

Historial de revisiones del documento

Versión	Fecha	Cambios
7.5	Marzo de 2014	Actualizaciones secundarias para NMS 7.5.
7.1	Diciembre de 2013	Revisado para NMS 7.1: ■ Se ha actualizado para incluir la detección de dispositivos de IPV6.
7.0	Septiembre de 2013	Revisado para NMS 7.0: ■ Se ha agregado la correlación de dispositivos. ■ Nueva cola llamada probe_discovery. ■ Se han realizado cambios en el Asistente para la detección. ■ Se han eliminado las interfaces de usuario de la sonda de detección. ■ Se ha mejorado el contenido.
6.5	Abril de 2013	Primera edición de la guía, se trata la detección de Nimsoft tal y como está implementada en NMS v6.5.

Contenido

Capítulo 1: Arquitectura de detección

La *detección automatizada* se encarga de encontrar y registrar todos los dispositivos direccionables y los equipos dentro de un entorno de TI gestionado. Cuando varios registros de detección se corresponden a un único dispositivo, se denomina *correlación* de dispositivos. La lista de registros de dispositivos se puede aumentar mediante la importación de dispositivos *basada en archivos XML* o mediante la entrada manual de dispositivos.

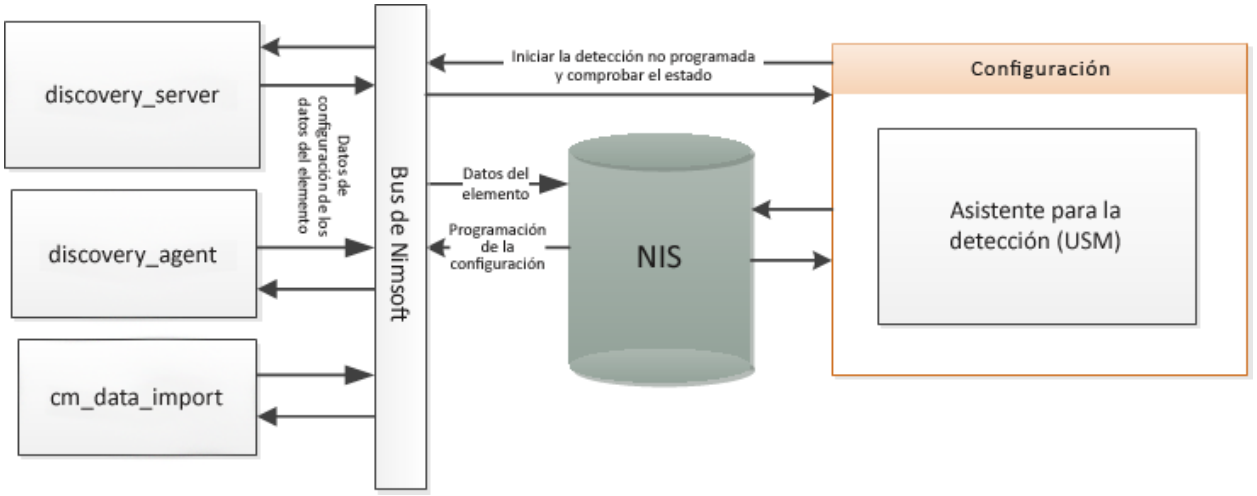
Una parte importante de la monitorización de TI es la creación y mantenimiento de una lista exacta de los dispositivos que se encuentran en el entorno de TI. La *detección automatizada* se encarga de encontrar y enumerar en una lista todos los dispositivos direccionables y los equipos dentro de un entorno de TI gestionado.

Cuando CA Nimsoft Unified Management Portal (UMP) se instala por primera vez, el Asistente para la detección se inicia automáticamente y le solicita que configure y ejecute la detección. El asistente le permite especificar las credenciales de autenticación y definir los intervalos de direcciones IP que se deben explorar. La detección encuentra prácticamente todos los recursos conectados en la red y proporciona información detallada sobre el tipo de dispositivo, la configuración y los datos de los activos/inventario. Mediante ICMP, ARP, DNS, SNMP (v1, v2 y v3), WMI, SSH y NetBIOS, la detección encuentra una amplia gama de dispositivos e información sobre el dispositivo.

La lista de dispositivos, a la que se hace referencia como *Inventario*, se puede aumentar mediante la importación de dispositivos basada en archivos XML o mediante la entrada manual de dispositivos. Cuando varios registros de la detección se corresponden a un único dispositivo, la correlación de dispositivos lo reconocerá.

Para mantener el inventario, se puede volver a ejecutar la detección en cualquier momento, modificando las credenciales y los intervalos según sea necesario. También se puede programar la detección para que se ejecute en intervalos regulares.

Este diagrama ilustra el flujo de datos entre los componentes clave de la detección automatizada:



Esta sección contiene los siguientes temas:

Componentes de detección

Todos los componentes de detección se incluyen en una instalación básica de CA Nimsoft Monitor Server.

Asistente para la detección

El Asistente para la detección es donde se configuran las exploraciones de detección. Para iniciar el asistente, abra el portlet Gestor de servicios unificados (USM) en Unified Management Portal (UMP) y seleccione **Acciones**. También se puede ejecutar el asistente desde cualquier nodo del agente de detección en el árbol de detección de USM.

El asistente le permite configurar utilizando cualquiera de los métodos de detección siguientes:

- La *detección automatizada* rellena el inventario de dispositivos explorando la red según los perfiles de autenticación y los ámbitos de exploración que se configuran.
- La *importación basada en archivos* importa una lista de uno o más hosts o dispositivos de red desde un archivo XML.

Estos temas se tratan completamente en la sección sobre el Asistente para la detección (en la página 17).

Sonda del servidor de detección

En la mayoría de las instalaciones, la sonda discovery_server se ejecuta en el concentrador principal. La sonda realiza estas tareas principales:

- Configura agentes de la detección y recopila el estado de los mismos.
- Recopila información acerca de la infraestructura de Nimsoft: los concentradores, los robots, las sondas, los paquetes, los sistemas o dispositivos monitorizados, los subsistemas o elementos monitorizados y la métrica monitorizada.
- Recopila datos de los dispositivos de las sondas que publican información de la detección.
- Aplica reglas de correlación para asociar los registros de dispositivos nuevos, donde sea apropiado, con cualquier registro de dispositivo master ya existente. Un ejemplo es representar los dispositivos con varias páginas principales (dispositivos con varias interfaces de red) con precisión.

La información que se recopila por la sonda discovery_server se guarda en la base de datos de NIS y otros componentes la utilizan en la solución de Nimsoft Monitor.

Nota: Incluso sin ninguna sonda discovery_agent implementada, la sonda discovery_server todavía se necesita para generar los datos necesarios para otros componentes de Nimsoft Monitor.

Sonda del agente de detección

La sonda discovery_agent explora la red de TI, haciendo ping y consultando los dispositivos según las máscaras de subred/intervalos, los perfiles de credenciales y los perfiles seleccionados. Estos parámetros de exploración se configuran dentro del Asistente para la detección.

Importación de datos de CA CM

Esta sonda procesa un archivo XML que describe hosts y dispositivos y agrega esta información al inventario de dispositivos. Esta sonda está ubicada normalmente con el servidor de detección. Cuando se ejecuta la importación basada en archivos desde el Asistente para la detección, la Importación de datos de CA CM realiza el trabajo.

Componentes adicionales que desempeñan un rol en la detección:

Cola probeDiscovery

Esta cola situada en el concentrador principal recopila datos de detección que se procesan por el servidor de detección. En los concentradores secundarios, se configurarán colas probe_discovery para recopilar datos y enrutarlos al concentrador principal. Consulte la sección Configuración de la cola discovery_probe (en la página 15).

Almacén de información de Nimsoft (NIS)

El NIS es la base de datos que tiene todos los datos persistentes en Nimsoft Monitor, incluyendo los datos de detección.

Otras sondas de monitorización de Nimsoft

Todas las sondas de monitorización proporcionan información acerca de los sistemas que se monitorizan al servidor de detección. Varias de estas sondas publican directamente en la cola probeDiscovery. Estas sondas de monitorización ayudan a suplementar la detección automática.

Consideraciones sobre la detección

- La característica *Topología y análisis de la causa raíz* de Nimsoft Monitor utiliza los datos proporcionados por la detección para deducir la estructura de la red y modelarla. El modelo es visible en el portlet Visor de relaciones en Unified Management Portal (UMP). Se puede encontrar más información acerca de los temas de topología y análisis de la causa raíz disponible en la Guía del usuario sobre la topología y el análisis de la causa raíz.
- Los dispositivos que se importan a Nimsoft mediante la importación basada en archivos no se reflejan en la topología o en el análisis de la causa raíz. La topología depende de la información de SNMP recopilada por el agente de detección sobre los dispositivos.

Requisitos previos y plataformas compatibles

- La detección de la versión 7.x requiere NMS 7.x.
- El servidor de detección de la versión 7.x solamente funciona con los agentes de detección de la versión 7.x. El servidor de detección crea una alarma para cualquier agente de detección anterior a la versión 7.0 que encuentre.
- El servidor de detección de la versión 7.x no recopila ningún resultado de la detección de los agentes de detección anteriores a la versión 7.0.

Para plataformas del sistema de NMS compatibles, consulte la Matriz de soporte de compatibilidad de Nimsoft Monitor para obtener más detalles.

Capítulo 2: Configuración de la detección

A continuación se muestra cómo funciona el proceso de detección:

1. Se instala NMS, que incluye los componentes obligatorios para la detección.
2. Si la instalación de NMS incluye concentradores secundarios, se deben configurar colas *probeDiscovery* para que los mensajes de probe_discovery lleguen al concentrador principal. Consulte Configuración de las colas de detección (en la página 15).
3. Se instala UMP, que incluye el Asistente para la detección.
4. Después de instalar UMP, el Asistente para la detección se inicia en USM y le ayuda a través del proceso de configuración de la detección. El usuario podrá realizar las siguientes acciones:
   a. Creación de los perfiles de autenticación (en la página 17)
   b. Definición de los intervalos (en la página 22) (conjuntos o intervalos de direcciones IP y máscaras de IP que definen y vinculan el ámbito de detección)
   c. Programación de la detección (en la página 24).
5. Para aumentar la detección automatizada, se puede preparar un archivo XML con información sobre los dispositivos e importar esta información al inventario de dispositivos (opcional). Consulte Ejecución de la importación basada en archivos (en la página 25).
6. Cuando se complete la detección, se pueden ver los equipos y dispositivos que se han detectado en la red. Consulte Vista de sistemas detectados (en la página 26).

Implementación de NMS

Los componentes (sondas) necesarios para la detección se implementan en el concentrador principal con una instalación básica de CA Nimsoft Monitor:

- Servidor de detección
- Agente de detección
- Importación de datos de CA CM

Tenga presente lo siguiente si desea modificar la implementación predeterminada de sondas de detección:

- Para la detección mínima, solamente se requiere la sonda discovery_server. No se lleva a cabo ninguna exploración de red.
- Para agregar la exploración de red, implemente la sonda discovery_agent en el concentrador principal de NMS o en otro sitio.
- Para la detección óptima en entornos mayores, se pueden implementar más de un agente de detección. Es muy útil para ciertos usuarios, especialmente los proveedores de servicios y los que disponen de redes muy grandes, la implementación de varios agentes de detección en varias ubicaciones.

  Se puede dividir la detección en una red grande entre los límites administrativos por estos motivos:

  - Para proporcionar a usuarios diferentes con el acceso a partes diferentes de la red.
  - En situaciones donde no haya ninguna conectividad directa a los dispositivos situados en un sitio remoto a causa de restricciones del cortafuegos o a la traducción de la dirección de red (NAT). Para una detección eficaz, implemente agentes de detección de tal manera que cada uno de ellos detecte una parte exclusiva de la red.
- Tenga en cuenta que el protocolo de WMI solo es compatible para las sondas discovery_agent que se ejecutan en sistemas Windows.

Sugerencia: El agente de detección requiere un acceso de SNMP a los dispositivos de red de solo lectura. Para simplificar la configuración de la detección, considere la posibilidad de configurar el número máximo de dispositivos de red posibles para utilizar una cadena de comunidad "universal" de solo lectura (se recomienda SNMP v3, mejor que v1 o v2c). Por ejemplo, se pueden definir unas credenciales de solo lectura (obtener únicamente) para que sean **nms_get_only**. Configure todos los dispositivos posibles para permitir un acceso de SNMP de solo lectura a través de estas credenciales. Con esto se reduce el número de credenciales de autenticación de SNMP que deben intentarse en los nodos de red y que simplifican ampliamente la configuración de la detección.

Configuración de las colas de detección

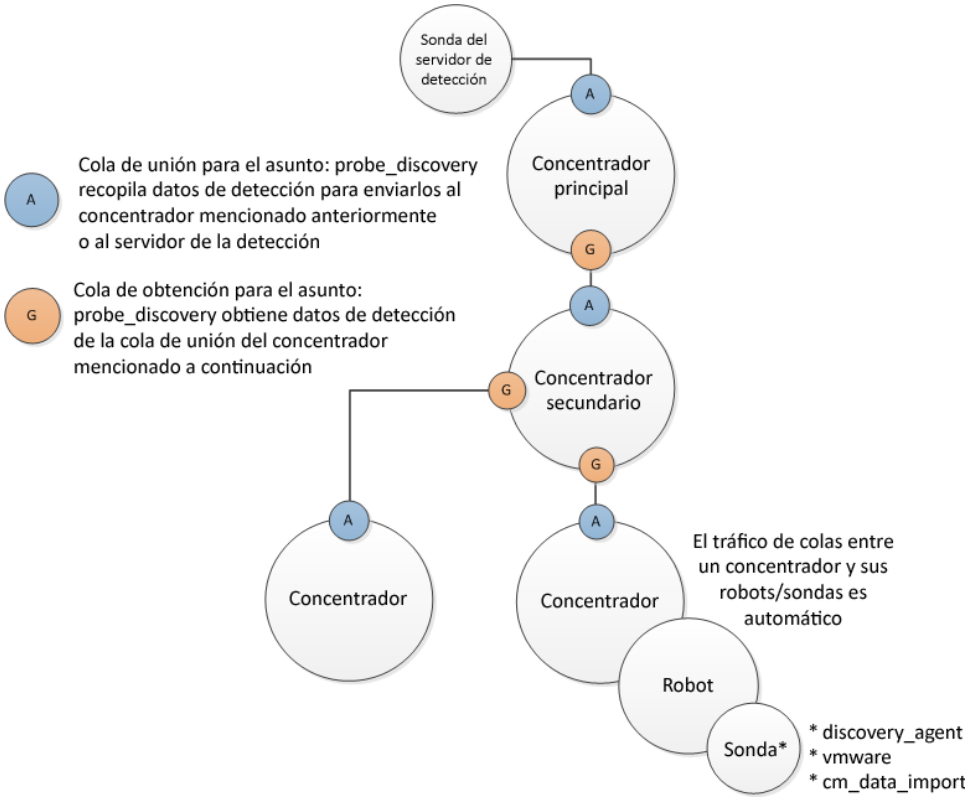
Si todas las sondas del proceso de detección se implementan en un único concentrador, la comunicación de los datos de detección se configura automáticamente. Sin embargo, si se implementan las sondas de detección en concentradores *distintos* del concentrador que hospeda la sonda discovery_server, se debe garantizar que los datos de detección puedan fluir desde esos concentradores hasta el concentrador principal.

Esto se logra configurando colas que gestionan el asunto de *probe_discovery*. Se configurarán las colas de *unión* (que recopilan mensajes) en el concentrador principal y en concentradores que hospedan las sondas siguientes:

- discovery_agent
- vmware 5.10 o posterior
- cm_data_import (esta sonda se implementa normalmente con discovery_serve en el concentrador principal)

Se configurará la cola de *obtención* correspondiente (que recupera mensajes de la cola de unión) en el concentrador principal y en cualquier concentrador que deba transferir los mensajes a otro concentrador.

La ilustración siguiente muestra donde se requieren las colas.



Para configurar colas de detección, siga estos pasos.

1. En el Gestor de la infraestructura, identifique el concentrador en el cual se desea crear una cola. Expanda el nodo del concentrador y haga doble clic en la sonda del concentrador.
2. Haga clic en la ficha **Colas**.
3. Para configurar una cola de *unión*, haga clic en **Nuevo** y, a continuación, especifique lo siguiente:
   - **Activo:** permitido
   - **Nombre:** probeDiscovery
   - **Tipo:** seleccione *unión*
   - **Asunto:** seleccione *probe_discovery*
4. Para configurar una cola de *obtención*, haga clic en **Nuevo** y, a continuación, especifique lo siguiente:
   - **Activo:** permitido
   - **Nombre:** probeDiscovery
   - **Tipo:** seleccione *obtención*
   - **Dirección:** seleccione la dirección del concentrador que tiene la cola de unión
   - **Tamaño del bloque:** especifique el número de mensajes que se deben enviar juntos (opcional; si se espera que la cola asuma una cantidad significativa de mensajes, enviarlos en bloque puede mejorar el rendimiento)

Cuando se han configurado todas las colas obligatorias, ejecute una exploración de detección automatizada (en el Asistente para la detección en USM) para confirmar que las colas son operativas. Revise la lista de los dispositivos detectados. Además de los dispositivos locales, también debe contener los dispositivos que solo son direccionables desde los concentradores secundarios de la infraestructura.

Nota: La configuración de otras colas para los datos de alarmas, calidad del servicio y línea de referencia es un procedimiento similar a la configuración de las colas de unión y obtención. El asunto de la cola cambia según sea necesario por el tipo de datos que se tienen que llevar.

Sugerencia: En las implementaciones pequeñas y medianas de NMS, un asunto de un carácter comodín (*), que lleva cualquier mensaje, puede simplificar la configuración de la cola. No se recomienda el uso de un asunto de carácter comodín en instalaciones grandes de NMS.

Inicio del Asistente para la detección

La primera vez que se abre Unified Management Portal (UMP), aparece en el portlet Gestor de servicios unificados y el Asistente para la detección se inicia automáticamente.

Después de abrir UMP por primera vez, se podrá iniciar el Asistente para la detección manualmente si desea ejecutar la detección o cambiar los valores de configuración de la detección. Se puede iniciar el Asistente para la detección desde el nodo de inventario o desde el menú **Acciones**.

Nota: El Asistente para la detección no se ejecutará después de una actualización de CA Nimsoft Monitor si hay intervalos existentes que definen las direcciones IP *excluidas*. Se debe elegir aceptar que la petición del sistema suprima los intervalos excluidos o eliminarlos manualmente desde la base de datos antes de ejecutar la detección.

Siga estos pasos:

1. Pase el puntero del ratón o haga clic sobre el nombre del agente o intervalo de detección del árbol.

   El icono de lupa () indica agentes de detección y el icono de red () indica intervalos.

2. Haga clic en el icono del engranaje () que se encuentra a la derecha del agente de detección o del nombre del intervalo en el árbol o elija **Asistente para la detección** en el menú **Acciones**.

   Nota: La opción de menú **Asistente para la detección** se activa solamente cuando se hace clic en un agente de detección o en un intervalo en el árbol.

Creación de los perfiles de autenticación

Las fichas WMI, Linux/Unix y SNMP le permiten crear, editar, ver y suprimir perfiles de autenticación para la detección. Un perfil de autenticación contiene información necesaria sobre las credenciales de la detección a fin de acceder y recopilar información sobre los sistemas informáticos y los dispositivos en la red.

Se pueden crear uno o más perfiles de autenticación bajo cada una de las fichas WMI, Linux/Unix y SNMP.

Nota: No se requiere crear perfiles de autenticación para la detección. Sin embargo, solo se utiliza la detección de dirección IP si no existe ningún perfil de autenticación y la información acerca de los sistemas detectados pueda ser limitada.

Seleccione la ficha WMI, Linux/Unix o SNMP y haga clic en el nombre de un perfil de autenticación en el panel izquierdo para poder consultar sus propiedades en el panel de la derecha.

Para modificar un perfil de autenticación existente, selecciónelo y edite los campos como sea necesario. A continuación, haga clic en **Guardar**. Para suprimir un perfil de autenticación, haga clic en el icono de la papelera de reciclaje () que se encuentra al lado del nombre del perfil en el panel izquierdo y, a continuación, haga clic en **Guardar**.

Siga estos pasos para crear un perfil de autenticación:

1. Haga clic en **Nuevas credenciales** del panel izquierdo.
2. Introduzca información en todos los campos obligatorios.

   Los campos obligatorios se esbozan en rojo.
3. Haga clic en **Siguiente**.

   La información que se introduce se guarda cuando se hace clic en **Siguient** y se incluye en el Asistente para la detección.

Linux/Unix

Los perfiles de autenticación de Linux/Unix utilizan SSH o Telnet para acceder y detectar los sistemas Linux y Unix.

Descripción

Nombre para el perfil de autenticación.

ID

Este campo de sólo lectura es el ID del sistema de Nimsoft para este perfil de autenticación, que se asigna cuando se guarda el perfil. Identifica el perfil especialmente para la reutilización en otras áreas de USM que hacen referencia a los perfiles de autenticación.

Usuario

Nombre del usuario.

Contraseña

La contraseña del usuario. Seleccione la casilla de verificación **Mostrar las nuevas contraseñas** para verificar el texto introducido.

SSH o Telnet

Seleccione el protocolo de comunicación para utilizar, SSH (shell seguro) o Telnet (ninguna autenticación segura ni cifrado).

Nota: El Agente de detección utiliza la autenticación de *contraseña* para conectarse a un dispositivo de destino sobre SSH. El Agente de detección no se puede comunicar con un dispositivo donde está configurado SSH para otros métodos de autenticación, como la autenticación por medio de teclado interactivo o mediante clave pública. El Agente de detección tampoco es compatible con la autenticación de clave pública ni con la autenticación de pregunta-respuesta.

SNMP

La detección de CA Nimsoft es compatible con las versiones de SNMP 1, 2c y 3. SNMP v3 agrega funciones de seguridad que no ofrecen v1 y v2c. Como resultado, los campos de configuración del perfil de autenticación en el Asistente para la detección, los cuales tratan la seguridad y la privacidad (cifrado), solamente están activos cuando se selecciona **3** en el menú desplegable **Versión.**

Se recomiendan las siguientes prácticas recomendables:

- Cree un conjunto mínimo de perfiles de autenticación de SNMP que proporcionarán, en conjunto, acceso a SNMP para todos los dispositivos y hosts de red que sean compatibles con SNMP.
- Configure tantos dispositivos de red como sea posible para utilizar credenciales de solo lectura "universales". Por ejemplo, se puede definir una credencial de solo lectura (obtener únicamente) para que sea **nms_get_only**. A continuación, se pueden configurar todos los dispositivos posibles para permitir un acceso de SNMP de solo lectura a través de esta credencial universal. Con esto se reduce el número de credenciales de autenticación de SNMP que deben intentarse en los nodos de red y que simplifican ampliamente la configuración de la detección.
- Si hay dispositivos que aceptan las credenciales de SNMP únicas, cree un perfil de autenticación para cada una de ellas. Se puede especificar un puerto único dentro del intervalo que va del 1 al 65535 para el perfil. Si no se especifica ningún puerto, se utilizará el puerto predeterminado 161.

Campo (SNMP v1 o v2)	Parámetros	Descripción
Descripción	Sí	Nombre para el perfil de autenticación

ID		Este campo de sólo lectura es el ID del sistema de Nimsoft para este perfil de autenticación, que se asigna cuando se guarda el perfil. Identifica el perfil especialmente para la reutilización en otras áreas de USM que hacen referencia a los perfiles de autenticación.
Versión	Sí	La versión de SNMP que es compatible con el dispositivo monitorizado. Cuando se selecciona la versión 1 o 2, solamente se encuentra activo el campo Comunidad.
Comunidad	Sí	La cadena de comunidad de SNMP. Seleccione la casilla de verificación **Mostrar las nuevas contraseñas** para ver el texto introducido. Tenga en cuenta que esta cadena se envía a través de la red en un texto claro como parte de las solicitudes SNMP v1 o v2c, las cuales pueden plantear un riesgo de seguridad.

Campo (SNMP v3)	**Parámetros**	**Descripción**
Descripción	Sí	Nombre para el perfil de autenticación
ID		Este campo de sólo lectura es el ID del sistema de Nimsoft para este perfil de autenticación, que se asigna cuando se guarda el perfil. Identifica el perfil especialmente para la reutilización en otras áreas de USM que hacen referencia a los perfiles de autenticación.
Versión	Sí	La versión de SNMP que es compatible con el dispositivo monitorizado. Las versiones 1, 2c y 3 son compatibles. Cuando se selecciona v3, se activan otros campos para la seguridad y la privacidad.
Contraseña	Consulte la nota	La contraseña asociada con el dispositivo SNMP v1/v2c o el usuario SNMP v3. Seleccione la casilla de verificación **Mostrar las nuevas contraseñas** para ver el texto introducido. **Nota:** Este campo se activa y requiere la selección de un tipo de seguridad **AuthNoPriv** o **AuthPriv**. Consulte la descripción para el siguiente campo Seguridad.
Usuario	Sí	Nombre del usuario SNMP v3 que se utiliza para acceder al dispositivo monitorizado. Es necesario para todos los niveles de seguridad de SNMP v3. Consulte la descripción para el siguiente campo Seguridad.

Método	Sí	Método de cifrado SNMP v3: al seleccionar la seguridad de **AuthPriv** (consulte la descripción para el siguiente campo Seguridad): ■ **Ninguno** ■ **MD5** - algoritmo de síntesis del mensaje MD5 (HMAC-MD5-96) ■ **SHA** - algoritmo de hash seguro (HMAC-SHA-96)
Seguridad	Sí	Nivel de seguridad de SNMP v3 del usuario. Dependiendo del nivel de seguridad que se seleccione, se activan o desactivan otros campos de seguridad. ■ **NoAuthNoPriv:** mensajes enviados no autenticados y no cifrados ■ **AuthNoPriv**: mensajes enviados autenticados pero no cifrados ■ **AuthPriv:** mensajes enviados autenticados y cifrados
Contraseña de privilegios	Consulte la nota	La contraseña de privacidad de SNMP v3 que debe utilizarse si se selecciona el nivel de seguridad de **AuthPriv**. Debe tener ocho caracteres como mínimo. No se debe confundir con la contraseña del usuario (autenticación). **Nota:** Este campo se activa y requiere la selección de un tipo de seguridad **AuthPriv**.
Protocolo de privilegios	Consulte la nota	Protocolo de privacidad de SNMP v3 (cifrado) para utilizar. ■ **DES:** Data Encryption Standard ■ **AES:** Advanced Encryption Standard **Nota:** Activado y necesario si se selecciona **AuthPriv**.

WMI

La detección de WMI (interfaz de gestión de Windows) explora los servidores de detección y los host que ejecuta Windows para recopilar la información del sistema. La detección de WMI se ejecuta solamente en los agentes de detección hospedados en sistemas de Windows.

Descripción

Nombre para el perfil de autenticación.

ID

Este campo de sólo lectura es el ID del sistema de Nimsoft para este perfil de autenticación, que se asigna cuando se guarda el perfil. Identifica el perfil especialmente para la reutilización en otras áreas de USM que hacen referencia a los perfiles de autenticación.

Usuario

Nombre del usuario, en la forma **Dominio\nombre del usuario**. **nombre_usuario** y **Dirección_IP\nombre_usuario** también están permitidos.

Contraseña

Contraseña de usuario. Seleccione la casilla de verificación **Mostrar las nuevas contraseñas** para ver el texto introducido.

Definición de intervalos

Utilice la ficha Intervalos del Asistente para la detección para definir direcciones de red, intervalos o máscaras donde están los dispositivos que se tiene que detectar. Como mínimo se deberá introducir un intervalo de red para que se ejecute la detección.

Se puede asignar cualquier combinación de perfiles de autenticación de SNMP, Linux/Unix y WMI a un intervalo. Los registros del proceso de detección registran *cualquier* dispositivo dentro de un intervalo que responda a una solicitud en un protocolo, incluyendo un simple ping de ICMP. Esto significa que se pueden incluir nodos finales (como servidores, impresoras de red, sistemas de almacenamiento de redes o estaciones de trabajo) en un intervalo, aunque no respondan a solicitudes a través de SNMP u otros protocolos de gestión.

Si no se asigna ningún perfil de autenticación a un intervalo, se realiza una detección básica mediante los protocolos que no requieren autenticación, pero es posible que la detección no haya finalizado y que la información acerca de los sistemas detectados se limite.

Prácticas recomendables para la creación de intervalos

Para cada agente de detección, revise los intervalos asignados para minimizar los tiempos de espera predecibles. Para optimizar el rendimiento y evitar las entradas duplicadas, todos los agentes de detección deberían detectar una parte exclusiva de la red.

Sugerencias para reducir el tiempo de ejecución de la detección:

- El agente de detección prueba todas las credenciales en las direcciones IP y espera un tiempo de espera (o de éxito) con cada intento. El uso de una única credencial dentro un intervalo que tiene una alta probabilidad de éxito inmediato en los nodos del intervalo puede acelerar la detección de manera considerable.
- Cuando se aplica un perfil de autenticación a un intervalo, asegúrese de que la mayoría o todos los dispositivos definidos por ese intervalo aceptarán el perfil de autenticación.
- Si se incluyen los dispositivos que no responden a solicitudes en cualquier protocolo de gestión, colóquelos en un intervalo de la detección sin perfiles de autenticación asignados al ámbito.

- Si se utiliza SNMP para un dispositivo que acepta solamente una cadena de comunidad SNMP única, cree un intervalo de tipo **Único** y especifique la dirección IP del dispositivo. Asigne el perfil de autenticación correspondiente al intervalo.
- A fin de evitar mensajes/alertas de autenticación innecesarios, al utilizar SNMP asigne solamente una credencial de autenticación de SNMP por intervalo de detección.

Creación de un intervalo

Siga estos pasos:

1. Haga clic en **Nuevo intervalo** en el panel izquierdo de la ficha Intervalos.
2. Introduzca un nombre para el intervalo.
3. En la sección Definición del intervalo, especifique las áreas de la red donde desee realizar la detección:
   - **Máscara:** máscara de bits para una subred mediante la notación de enrutamiento entre dominio sin clases (CIDR) con una dirección IPv4 de base y un prefijo de enrutamiento. Por ejemplo: 195.51.100.0/24. El valor /24 hace referencia a una subred de clase C de 256 direcciones. Otros posibles valores como referencia: /30 (4 direcciones) y /16 (65.536 direcciones o una subred de clase B).

     Nota: Cuando se especifica una máscara de subred, se muestra el número de direcciones IP que representa la máscara (el número de host efectivo menos dos). Solo se admiten máscaras que usen 20 o más.
   - **Intervalo:** intervalo de direcciones IPv4.
   - **Único**: una única dirección IPv4 o IPv6. Se pueden utilizar formatos de dirección IPv6 abreviados y direcciones IPv6 que hagan referencia a direcciones IPv4. Tenga en cuenta que las direcciones IPv6 de difusión por proximidad, multidifusión, bucle invertido y las rutas predeterminadas *no* se pueden usar.

   También puede hacer clic en el icono Añadir varias IP () situado por encima de la sección Definición del intervalo. Copie y pegue las direcciones IP en el cuadro de diálogo Importar direcciones IP. Después de hacer clic en **Aceptar**, los errores se resaltan en rojo.
4. Haga clic en **Intervalo de IP nuevo o dirección IP única** para agregar otro intervalo de IP, una dirección o una máscara, si lo desea.

5. En la sección Credenciales, se pueden asignar perfiles de autenticación al intervalo seleccionado. De forma predeterminada, todos los perfiles de autenticación están seleccionados.

   Si se tiene un gran número de perfiles de autenticación en la lista, se puede introducir el nombre de un perfil para filtrar la lista.

   Para ver solamente los perfiles seleccionados, haga clic en la casilla de verificación **Ocultar perfiles sin utilizar**.

6. Cuando haya terminado de definir los intervalos, haga clic en **Siguiente**.

Programar detección

En la ficha Programación, se puede programar la detección para ejecutarla en el futuro, y/o se puede ejecutar la detección inmediatamente. Se puede programar la ejecución de una única detección o de ejecuciones repetitivas.

Una detección programada no interrumpe ninguna detección que ya esté ejecutándose. Si durante la programación de una ejecución de la detección hay otra ejecución de la detección en curso, se ignorará la detección programada.

Si se selecciona **Ejecutar detección ahora** y la detección está en curso, la ejecución de la detección actual finaliza y se ejecutará la nueva versión.

Siga estos pasos para iniciar y/o programar una detección:

1. Deje la casilla de verificación **Ejecutar detección ahora** seleccionada a menos que no se desee ejecutar la detección cuando se completa el Asistente para la detección.
2. Para programar la detección, seleccione la casilla de verificación **Programar detección**.
3. Introduzca información en los campos de nombre y hora.

   El campo de hora está en el formato de 24 horas. La hora es la hora local del usuario.

4. Para programar las ejecuciones de detección repetitivas, seleccione la casilla de verificación **Repetir cada** e introduzca el número de horas para el intervalo de periodicidad.
5. Haga clic en **Finalizar** para completar el Asistente para la detección.

Navegación en el Asistente para la detección

Hay unas cuantas cosas que deben tenerse en cuenta al utilizar el Asistente para la detección:

- Si se hace clic en el botón **Cerrar** o en el icono **X** de la barra de títulos antes de completar el Asistente para la detección, se le solicitará si desea guardar los cambios. Si se ejecuta la detección haciendo clic en **Finalizar** en la pantalla final del Asistente para la detección, los cambios se conservarán.
- Si la información válida se introduce en los campos obligatorios de un perfil de autenticación o de un intervalo de red, la información se guarda automáticamente cuando se hace clic en **Siguiente**. Los campos obligatorios se esbozan en rojo.
- Las contraseñas de los perfiles de autenticación se muestran como asteriscos. Si se desea ver una contraseña tal y como se escribe, haga clic en el icono Mostrar contraseña () que se encuentra al lado del campo **Contraseña**. Después de hacer clic en **Siguiente**, la contraseña se volverá a mostrar como asteriscos.

Ejecución de la importación basada en archivos

Mediante la importación de archivos, los administradores de CA Nimsoft podrán importar información de dispositivos y de host a CA Nimsoft Monitor sin exploraciones de red ni entradas manuales. Como no es necesario explorar el entorno de las TI, la importación de archivos de los dispositivos provoca menos alertas de seguridad y puede ser más rápido que la detección automatizada que utiliza el Asistente para la detección.

Nota: Si el sistema detecta una exploración automatizada de la red y se incluye también en una importación de archivos, la importación de archivos tendrá precedencia. Si la información acerca del sistema es distinta, la información en el archivo XML para la importación de archivos será la información que se almacenará en la base de datos.

Siga estos pasos:

1. Cree un archivo XML que contenga información acerca de los dispositivos y de los equipos de red.

   Para obtener más detalles sobre el contenido del archivo XML, consulte el Esquema del archivo XML (en la página 34).

2. Expanda el nodo **Detección** en la vista de árbol en el Gestor de servicios unificados.
3. Pase el puntero por encima del nodo **Externo** en el árbol y haga clic en el icono de importación () o haga clic en el nodo **Externo** y elija **Importación de la detección** en el menú **Acciones**.

4. Vaya al archivo XML en el explorador de archivos y, a continuación, haga clic en **Aceptar.**

   La información del dispositivo se importa a la base de datos de Nimsoft. El proceso mediante discovery_server se inicia y puede tardar varios minutos o más en finalizar.

5. Para ver los dispositivos importados, haga clic en el nodo **Externo**.

   Los dispositivos se muestran en la tabla de la derecha.

Método de importación alternativo:

La sonda cm_data_import monitoriza un directorio para los archivos XML válidos y, si encuentra uno, importa automáticamente la información a la base de datos. Aquí aparece cómo funciona el proceso:

1. Copie el archivo XML que se ha preparado en el directorio <directorio de instalación de Nimsoft>\Probes\Service\cm_data_import**import** en el sistema que hospeda la sonda cm_data_import.
2. La sonda cm_data_import explora este directorio en intervalos regulares (el valor predeterminado es 60 segundos).
3. Si la sonda encuentra un archivo de importación válido, importe la información sobre el dispositivo al archivo de la base de datos de Nimsoft.
4. La sonda mueve el archivo a una subcarpeta de marca de tiempo en el directorio <directorio de instalación de Nimsoft>\Probes\Service\cm_data_import**processed**, también en el host de la sonda y registra los resultados del proceso.

Vista de sistemas detectados

El nodo **Detección** en la vista de árbol del Gestor de servicios unificados permite visualizar los equipos y los dispositivos que se han detectado en la red.

La sección Detección del árbol contiene agentes de detección con intervalos de red bajo cada agente de detección. El árbol también tiene un nodo Automático y otro Externo.

Los iconos que aparecen junto a los nodos de árbol identifican el tipo de nodo y proporcionan información adicional:

 - Nodo de detección o agente de detección de nivel superior.

 - Intervalo de red.

 - Automático. Algunas sondas detectan sistemas automáticamente y los sistemas aparecen en este nodo.

 - Externo. Los sistemas clasificados bajo este nodo se han importado mediante la detección de archivos.

 - Se programa una detección. Pase el puntero sobre el icono para ver la siguiente hora de programación en la información sobre herramientas.

 - Detección en curso. La proporción de azul indica el progreso de detección.

 - Ninguna detección programada.

Haga clic en un nodo del árbol para ver los sistemas asociados y sus propiedades en la tabla de la derecha. Para ver las propiedades para todos los sistemas detectados, haga clic en el nodo **Detección**.

Un gráfico circular sobre la tabla muestra información acerca de los sistemas detectados para el nodo seleccionado. Elija un criterio distinto (**Tipo de dispositivo**, **Sistema operativo,** etc.) del menú desplegable para cambiar los datos que aparecen en el gráfico circular.

Haga clic en un segmento del gráfico circular o en un elemento de la leyenda del gráfico para filtrar los sistemas. Solamente aparecen en la tabla los sistemas que se representan en el segmento y estos se reflejan en los vínculos de respuesta de la derecha. Haga clic de nuevo en el intervalo o en el elemento de la leyenda para borrar el filtro.

Los vínculos de respuesta de la derecha de los sistemas de la lista del gráfico circular se agrupan en función de las últimas respuestas a la solicitud del agente de detección. Haga clic en uno de estos vínculos, como **Reciente (último día)**, para filtrar los sistemas. Estos sistemas son los únicos que aparecen en el gráfico circular y en la tabla. Haga clic de nuevo en el vínculo para borrar el filtro.

Nota: Los sistemas que no responden se borran definitivamente de la base de datos. De forma predeterminada, 30 días después de la última respuesta de un sistema, el sistema se suprimirá de la base de datos.

El campo Filtro rápido que se encuentra debajo de los vínculos de respuesta permite filtrar por el texto en las columnas de la tabla **Nombre**, **Dirección IP, Dominio**, **Nombre del SO** y **Origen**.

Haga clic en un encabezado de columna para ordenar la tabla por la columna.

Un icono clave () en la tabla indica que un agente de detección ha podido realizar la autenticación con el sistema mediante uno de los perfiles de autenticación definidos. Pase el puntero sobre el icono clave para ver el tipo y el nombre del perfil de autenticación utilizado.

Se pueden exportar datos para un agente de detección o un intervalo de red. Los datos incluyen más columnas que las que aparecen en la tabla Inventario. Los datos se exportan a un archivo .csv que se guarda en la ubicación que elija. Para exportar datos, haga clic en un agente de detección o en un intervalo de red en el árbol. A continuación, seleccione **Exportar grupo** en el menú **Acciones**.

Nota: Cuando se elige **Exportar grupo**, se exportan todos los sistemas para el agente de detección seleccionado o para el intervalo de red seleccionado sin tener en cuenta si se ha filtrado la visualización en la vista Inventario.

Apéndice A: Configuración avanzada

Nota: Se configuran los valores de configuración de la exploración de detección automatizada como, por ejemplo, los intervalos de red y los perfiles de credenciales de autenticación, dentro del Asistente para la detección que ejecuta dentro del portlet de USM en UMP. Para obtener más información, consulte la sección sobre el Asistente para la detección (en la página 17).

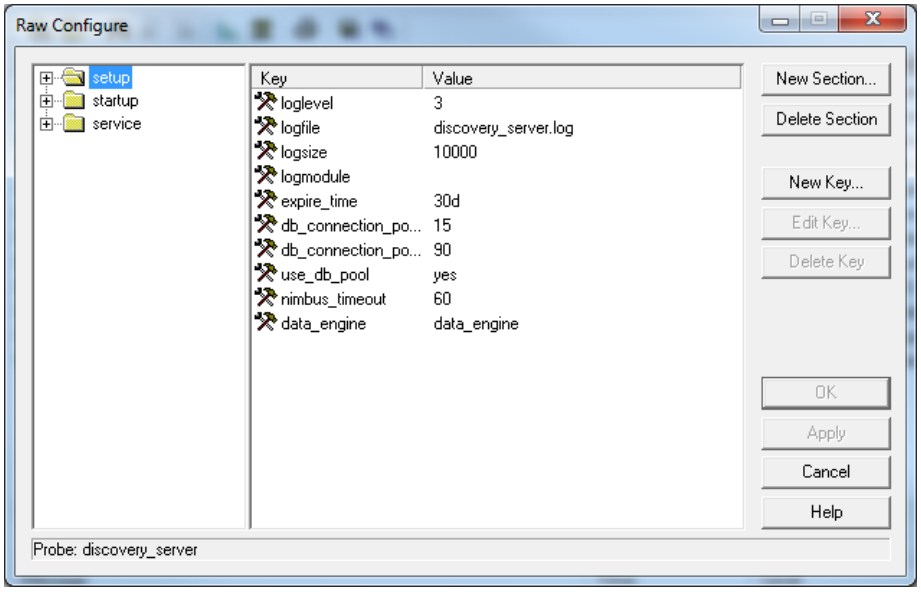
Esta sección contiene los siguientes temas:

Ejecución de discovery_server en un robot distinto del concentrador principal

De forma predeterminada, el servidor de detección se ejecuta en el concentrador principal, que es el mismo robot donde se está ejecutando data_engine. El servidor de detección se puede ejecutar en un robot diferente siempre que el servidor de detección se pueda comunicar con la sonda data_engine y el servidor de base de datos desde su nueva ubicación. Para ejecutar el servidor de detección en un robot distinto del concentrador principal, siga estos pasos:

1. Desactive o suprima el servidor de detección en el concentrador principal, solo puede estar implementada una instancia del servidor de detección.
2. En el Gestor de la infraestructura, haga clic en la sonda discovery_server que se encuentra en el concentrador secundario. En la Consola de administración, haga clic en el icono situado al lado de discovery_server en el concentrador secundario.
3. Seleccione Configuración sin formato.

4. En la ventana de contenido vaya a la clave de configuración > data_engine y haga clic en el botón Editar clave. En la Consola de administración, haga clic en el campo del valor para editarlo.



5. Especifique la dirección completa de la sonda data_engine (*/dominio/concentrador_principal/robot_principal*/data_engine). Se puede realizar una búsqueda de la dirección de data_engine en el Gestor de la infraestructura bajo la categoría SLM del concentrador principal.
6. Active o reinicie discovery_server en su nueva ubicación.

Establecimiento del tamaño máximo de la memoria dinámica de Java

El tamaño máximo predeterminado de la memoria dinámica de Java para las sondas discovery_server y discovery_agent se establece mediante la opción Configuración sin formato.

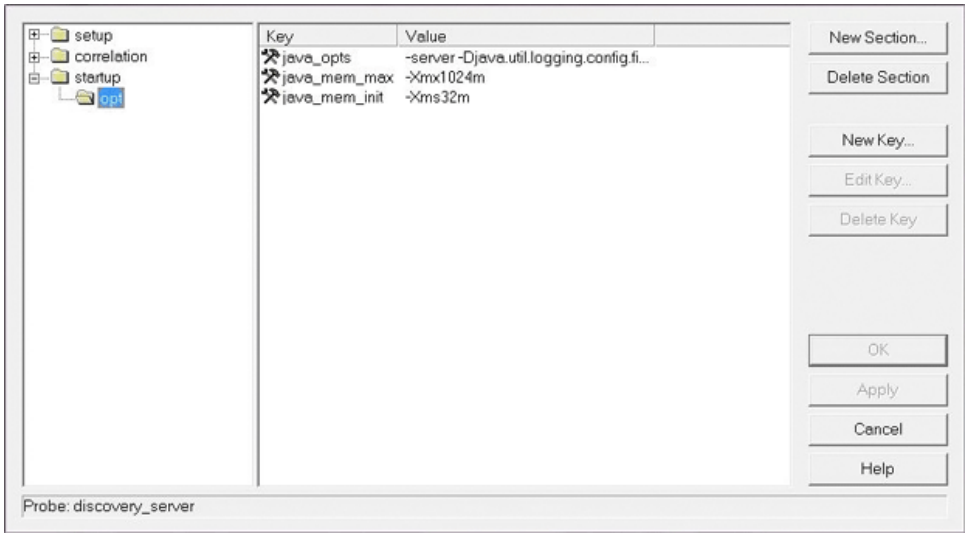
Servidor de detección

El tamaño máximo predeterminado de la memoria dinámica de Java se establece en 1 GB y está pensado para ser compatible con hasta 5000 robots. Para sistemas con más de 5000 robots, el tamaño máximo de la memoria dinámica de Java se debe aumentar en 1 GB por cada 5000 robots adicionales.

Ejemplo: 2 GB de 5001 a 10000 robots; 3 GB de 10001 a 15000 robots.

Para establecer el tamaño máximo de la memoria dinámica de Java:

1. En el Gestor de la infraestructura, mantenga la tecla Mayús y haga clic con el botón secundario del ratón en la sonda discovery_agent, y seleccione **Configuración sin formato**. En la Consola de administración, haga clic en el icono situado al lado de discovery_agent y seleccione **Configuración sin formato**.
2. Vaya a **Inicio** y, a continuación, abra **opt**.
3. En la ventana de contenido seleccione **java_mem_max**. En el Gestor de infraestructura, haga clic en el botón **Editar clave**. En la Consola de administración, haga clic en el campo del valor para editarlo.



4. Introduzca el valor nuevo utilizando incrementos de 1024 MB.
   - 1 GB = -Xmx1024m
   - 2 GB = -Xmx2048m

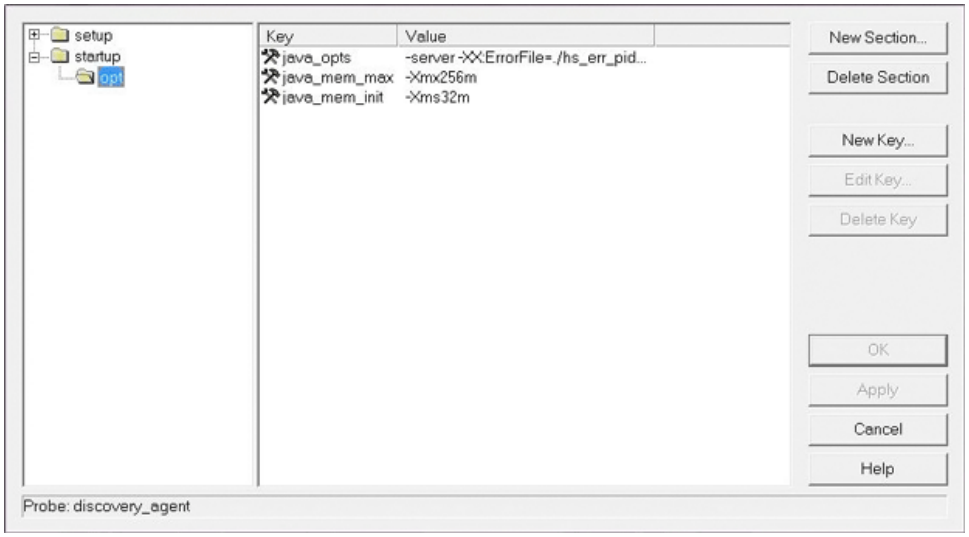
Agente de detección

El tamaño máximo predeterminado de la memoria dinámica de Java se establece en 256 MB. Para intervalos de detección muy grandes (equivalentes a una subred de clase B o con más de 30000 dispositivos direccionables), se recomienda aumentar la adjudicación máxima de la memoria dinámica hasta 512 MB o 1024 MB.

Para establecer el tamaño máximo de la memoria dinámica de Java:

1. En el Gestor de la infraestructura, mantenga la tecla Mayús y haga clic con el botón secundario del ratón en la sonda discovery_agent, y seleccione **Configuración sin formato**. En la Consola de administración, haga clic en el icono situado al lado de discovery_agent y seleccione **Configuración sin formato**.
2. Vaya a **Inicio** y, a continuación, abra **opt**.

3. En la ventana de contenido seleccione **java_mem_max**. En el Gestor de infraestructura, haga clic en el botón **Editar clave**. En la Consola de administración, haga clic en el campo del valor para editarlo.



4. Especifique el nuevo valor.
   - 512 MB = -Xmx512m
   - 1 GB = -Xmx1024m

Referencia sobre la importación basada en archivos

La función de detección llamada *importación basada en archivos* proporciona una forma conveniente de importar datos de descripción de dispositivos a la base de datos de detección. La importación basada en archivos proporciona una alternativa a la detección automatizada para rellenar el inventario de la detección, sin incurrir en la sobrecarga de explorar el entorno de TI.

La sonda cm_data_import procesa los datos de dispositivos incluidos en un archivo XML. Inicie el proceso con uno de estos métodos.

Método 1

1. Abra un explorador de archivos desde el nodo externo del Asistente para la detección en USM.
2. Vaya al archivo XML preparado en el sistema de archivos local para procesarlo y haga clic en **Aceptar**.
3. Se procesa el archivo. Cuando el proceso está completo:
   - Los dispositivos se publican en el bus de Nimsoft. discovery_server recibe esta información y agrega los dispositivos a la base de datos del dispositivo.
   - Los dispositivos se muestran en USM.

Método 2

1. Copie un archivo XML en el directorio *<Nimsoft>\Probes\Service\cm_data_import\import* en el sistema que hospeda la sonda cm_data_import.
2. La sonda cm_data_import reconoce los archivos nuevos y los procesa. Esta sonda explora el directorio en un intervalo configurable (el valor predeterminado es de 60 segundos). Cuando el proceso está completo:
   - cm_data_import mueve el archivo a una subcarpeta con una marca de tiempo en *<Nimsoft>\Probes\Service\cm_data_import\processed*.
   - El resultado del proceso se registra.
   - La sonda publica los dispositivos en el bus de Nimsoft. discovery_server recibe esta información y agrega los dispositivos a la base de datos del dispositivo.
   - Los dispositivos se muestran en USM.

Los dispositivos son visibles en la interfaz de USM bajo Grupos o enumerados bajo la rama **Externa** del árbol de detección.

Nota: Los dispositivos importados mediante la importación basada en archivos no se reflejan en la topología de Nimsoft.

Esquema de archivo XML

Esta sección describe cómo crear un archivo XML para utilizarlo con la detección basada en archivos.

El archivo XML debe incluir estas propiedades obligatorias para cada host o dispositivo:

- PrimaryIPv4Address - Enumera la dirección de IPv4. Aunque la etiqueta PrimaryIPv6Address existe, las direcciones de IPv6 no son compatibles actualmente con la detección.
- Origen: es importante configurar correctamente el origen. Consulte los detalles en la propiedad Origen de la tabla siguiente.

Aquí aparece un ejemplo de XML que ilustra cómo importar un dispositivo con la dirección IP 1.2.3.4 y el origen "MyOrigin" a la base de datos.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<DevicesToImport xmlns="http://nimsoft.com/2012/11/cm-data-import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <Device>
                <PrimaryIPV4Address>1.2.3.4</PrimaryIPV4Address>
                <Origin>myOrigin</Origin>
        </Device>
</DevicesToImport>
```

Se pueden incluir más propiedades opcionales, como aparece en el ejemplo siguiente. Se puede encontrar también este archivo de ejemplo, denominado example1MaximalDevice.xml, en el directorio <directorio de instalación de Nimsoft>\Probes\Service\cm_data_import**schema**, que se encuentra en el sistema que hospeda la sonda cm_data_import, normalmente se trata del concentrador principal.

```
  <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
  <DevicesToImport xmlns="http://nimsoft.com/2012/11/cm-data-import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <Device>
              <Origin>myOrigin</Origin>
              <Label>myComputer</Label>
              <Description>aquí se introduce la descripción de myComputer</Description>
              <PrimaryDnsName>myComputer.myCompany.com</PrimaryDnsName>
              <PrimaryIPV4Address>1.2.3.4</PrimaryIPV4Address>
              <PrimaryIPV6Address>fe80::223:ebff:fe06:9d40%10</PrimaryIPV6Address>
              <PrimaryMacAddress>F0-4D-A2-25-5B-7A</PrimaryMacAddress>
              <PrimaryOSType>WindowsServer-2008</PrimaryOSType>
              <PrimaryOSVersion>6.1.7601</PrimaryOSVersion>
              <ProcessorType>x86-64</ProcessorType>
              <Vendor>Dell Inc.</Vendor>
              <Model>PowerEdge T620</Model>
              <PhysSerialNumber>123-456-789-ABCD</PhysSerialNumber>
              <PrimaryDeviceRole>VirtualMachine</PrimaryDeviceRole>
              <PrimarySoftwareRole>DatabaseServer</PrimarySoftwareRole>
              <DBServerType>MSSQLServer</DBServerType>
              <WmiAuthId>3</WmiAuthId>
              <ShellAuthId>5</ShellAuthId>
              <SnmpAuthId>7</SnmpAuthId>
              <AppServerType>Unknown</AppServerType>
              <VirtualizationEnvironment>VMware</VirtualizationEnvironment>
              <MonitorFrom>monitoringRobotHostName</MonitorFrom>
       </Device>
</DevicesToImport>
```

En la siguiente tabla se describen todas las propiedades XML. Para las propiedades que hacen referencia a la apertura de enumeraciones, vaya a <ruta de instalación de Nimsoft>\Probes\Service\cm_data_import**schema** y abra o **usm-openenums.xml** o **cm-data-import-openenums.xml** para ver los valores definidos para cada instancia de la enumeración. Se recomienda utilizar valores definidos por las enumeraciones abiertas, aunque no sea estrictamente obligatorio.

Para implementar un robot en un sistema importado mediante USM y ADE, son necesarias algunas propiedades adicionales además de la dirección IP y del origen. Estas acciones se explican en la tabla que aparece a continuación.

Propiedad	¿Obligatorio?	Descripción
Origen	Sí	Los datos de la calidad del servicio de las sondas se etiquetan con un nombre de origen para identificar el origen de los datos. El nombre de origen establece como predeterminado el nombre del concentrador de Nimsoft pero se puede anular en el concentrador o en el robot (controlador) para separar los datos en un entorno de multicliente. Para garantizar que los datos de la calidad del servicio de las sondas se correlacionen con este dispositivo, el nombre del origen que se especifica aquí debería coincidir con el nombre de origen que desee utilizar en la infraestructura de concentradores y robots de Nimsoft.
Etiqueta	No	Una descripción o título breve.
Descripción	No	Descripción de texto del dispositivo.
PrimaryDnsName	No	El nombre de sistema del dominio de la entidad que se puede utilizar para la correlación.
PrimaryIPV4Address	Es obligatorio especificar una dirección de IPv4.	Una dirección IPv4 para la entidad que se puede utilizar para la correlación y la identidad.
PrimaryIPV6Address	No	Una dirección IPv6 para la entidad que se puede utilizar para la correlación y la identidad. La dirección se expresa mediante la notación de IPv6 formal y total (8 grupos de hasta 4 dígitos de carácter hexa, utilizando solamente la mayúscula donde sea aplicable; los dos puntos se utilizan para separar los distintos elementos).
OtherIPAddresses	No	Una entidad puede tener varias direcciones IP. Este elemento captura los valores de esas direcciones, mientras que los elementos PrimaryIPAddress están diseñados para ser utilizados para la correlación e identidad. Los diversos valores están separados por comas. Los valores de IPv4 o de IPv6 se pueden especificar pero las direcciones se deben formatear siguiendo los patrones de regex definidos por usm-core:IPV4AddressFormat o usm-core:IPV6AddressFormat.

Propiedad	¿Obligatorio?	Descripción
PrimaryMacAddress	No	Una dirección MAC para la entidad que se puede utilizar para la correlación y la identidad. La dirección se expresa como 6 grupos de 2 dígitos de carácter hexa (solamente en mayúscula), separado por guiones.
OtherMacAddress	No	Una entidad puede tener varias direcciones MAC. Este elemento captura los valores de esas direcciones, mientras que el elemento PrimaryMacAddress está diseñado para ser utilizado para la correlación. Los diversos valores están separados por comas y se formatean siguiendo el patrón de regex definido por usm-core:MacAddressFormat.
PrimaryOSType	Requerido por el Motor de implementación automatizada (ADE) para la implementación de robots	Tipo de SO definido por la enumeración abierta OSTypeEnum. Para Linux, ADE requiere el nombre de la distribución de Linux (por ejemplo, **Linux-RedHat**).
PrimaryOSVersion	No	Detalles de la versión del sistema operativo.
ProcessorType	Requerido por el Motor de implementación automatizada (ADE) para la implementación de robots	Entorno/tipo de procesador (como "x86") tal y como ha definido la enumeración abierta ProcessorEnvironmentEnum.
Provider	No	El distribuidor de hardware/nombre del fabricante, tal y como ha definido la enumeración abierta VendorEnum.
Model	No	El nombre/número de modelo de hardware.
PhysSerialNumber	No	Una cadena identificadora que asigna el fabricante de hardware e imprimida en una etiqueta que se engancha al componente. Los datos para este elemento se deberían introducir directamente desde la etiqueta del fabricante en el componente (que puede ser una etiqueta de RFID) o leerse en el campo entPhysicalSerialNum de la base de información gestionada (MIB) de la entidad SNMP. Tenga en cuenta que una entidad virtual NO tendría un PhysSerialNumber.

Propiedad	¿Obligatorio?	Descripción
PrimaryDeviceRole	No	El rol del dispositivo tal y como define la enumeración abierta DeviceRoleEnum.
PrimarySoftwareRole	No	El rol del software tal y como define la enumeración abierta SoftwareRoleEnum.
DBServerType	No	El tipo de servidor de la base de datos cuya instancia se define por la enumeración abierta DBServerTypeEnum.
AppServerType	No	El tipo de servidor de aplicaciones, tal y como define la enumeración abierta AppServerTypeEnum.
VirtualizationEnvironment	No	Valor que indica el entorno de virtualización específico (gestor del hipervisor) de un sistema virtual o hipervisor. Los valores se definen en la enumeración abierta VirtualizationTypeEnum.
WmiAuthId	ADE requiere WmiAuthId o ShellAuthID para la implementación de robots	Un ID de perfil de autenticación definido de Nimsoft que debe utilizarse para el acceso de WMI. Este es el campo de ID en el perfil de autenticación de WMI.
ShellAuthId	ADE requiere WmiAuthId o ShellAuthID para la implementación de robots	Un ID de perfil de autenticación definido de Nimsoft que debe utilizarse para el acceso de SSH o Telnet. Este es el campo de ID en el perfil de autenticación de la shell.
SnmpAuthId	No	Un ID de perfil de autenticación definido de Nimsoft que debe utilizarse para el acceso de SNMP. Este es el campo de ID en el perfil de autenticación de SNMP.
MonitorFrom	No	Si el dispositivo se monitoriza remotamente, este valor especifica el sistema desde el cual se monitorizará el dispositivo. El valor se puede especificar como una dirección IP, un nombre de host simple, un nombre de dominio completo o una dirección de Nimsoft (/NimsoftDomain/HubName/RobotName). Un robot de Nimsoft se deberá instalar en el sistema que aquí se especifica. Si el robot no se instala, este dispositivo no se importará. El nombre de origen que utiliza el robot debería coincidir con el origen especificado para que este dispositivo garantice que los datos de la calidad del servicio desde las sondas se correlacionan con este dispositivo.