]HackingTeam[

RCS 9.5

La suite de hacking para intercepción gubernamental

Manual del administrador del sistema

Propiedad de la información

las solicitudes de copias adicionales de este manual o de la información técnica del producto se deben enviar a:

HT S.r.l.

via della Moscova, 13

20121 Milan (MI)

Italia

Tel.: + 39 02 29 060 603

Fax: + 39 02 63 118 946

Correo electrónico: info@hackingteam.com

Contenido

Lista de diagramas

Glosario

A continuación se detallan las definiciones utilizadas en este manual.

A

Accounting
Sección de la consola en la que se administra el acceso a RCS.

Administrador
Es la persona que permite el acceso al sistema, crea grupos de trabajo y define las operations, los targets y los tipos de datos que se recopilarán.

Administrador del sistema
Persona que instala los servidores y las consolas, actualiza el software y restaura los datos en caso de alguna falla.

Agent
Software de sondeo instalado en los dispositivos a monitorear. Está diseñado para reunir evidence y transmitirla al Collector.

Agent elite
Agent instalado en dispositivos seguros. Le permite recopilar todos los tipos de evidence disponibles.

Agent scout
Reemplaza al agent enviado al dispositivo para verificar el nivel de seguridad antes de instalar agents reales (elite o soldier).

Agent soldier
Agent instalado en dispositivos que no son completamente seguros. Solo le permite recopilar algunos tipos de evidence.

Alerting
Sección de la consola en la que se administran los alerts de nueva evidence.

alerts de evidence
Alertas, usualmente en forma de correos electrónicos, que se envían a los analistas cuando hay nueva evidence que coincide con las reglas establecidas.

Analista
Persona encargada de analizar los datos recopilados durante las operations.

Anonymizer
(opcional) Protege al servidor contra ataques externos y permite permanecer anónimo durante las investigaciones. Transfiere los datos del agent a los Collectors.

Audit
Sección de la consola que reporta las acciones de todos los usuarios y el sistema. Se utiliza para controlar el abuso de RCS.

B

back end
Entorno diseñado para desencriptar y guardar la información que se recopila. Incluye el Master Node y las bases de datos shard.

BRAS
(Broadband Remote Access Server) Dirige el tráfico hacia o desde el DSLAM a la red del ISP y administra la autentificación de los suscriptores del ISP.

BSSID
(Basic Service Set IDentifier) Punto de acceso y su identificador cliente.

C

Carrier
Servicio del Collector: envía los datos recibidos de los Anonymizers a las bases de datos shard o al Master Node.

Collector
Servicio de Collector: recibe los datos que envían los agents a través de la cadena de Anonymizers.

consola
Computadora en la que se instala RCS Console. Accede directamente a RCS Server o al Master Node.

D

Dashboard
Sección de la consola utilizada por el analista. Se usa para tener un resumen rápido del estado de las operations, targets y agents más importantes.

DSLAM
(Digital Subscriber Line Access Multiplexer) Dispositivo de red que usualmente se encuentra en la central telefónica de los operadores de telecomunicaciones. Conecta varias interfaces de líneas de abonados digitales (DSL) a un canal de comunicaciones de alta velocidad digital usando técnicas de multiplexión.

E

Emisor de RCS
Sistema RCS que recibe evidence de los agents y la transfiere a otros sistemas RCS (consultar) a través de las reglas de conexión. Es un sistema RCS completo.

entidad
Grupo de información de Intelligence vinculada con el target y con las personas y lugares involucrados en la investigación.

ESSID
(Extended Service Set IDentifier) También conocido como SSID. Permite identificar la red Wi-Fi.

evidence
Evidence de datos recopilados. El formato depende del tipo de evidence (p. ej.: imagen).

Exploit
Código que se aprovecha de un error o vulnerabilidad y ejecuta un código imprevisto. Se utiliza para infectar a los dispositivos de los targets.

F

factory
Una plantilla para la configuración y compilación de un agent.

front end
Entorno diseñado para comunicarse con los agents para recopilar información y establecer su configuración. Incluye Collectors.

G

Grupo
Entidad de Intelligence que agrupa a varias entidades.

grupo de alerting
Grupo de usuarios que reciben notificaciones por correo cuando se activa una alarma del sistema (por ejemplo, cuando la base de datos excede los límites de espacio disponible). Usualmente este grupo no está vinculado con ninguna operation.

M

Monitor
Sección de la consola en la que se monitorea el estado de los componentes y la licencia.

N

Network Controller
Servicio del Collector: verifica el estado del Network Injector y el Anonymizer y les envía nuevos parámetros de configuración y actualizaciones de software.

Network Injector
Componente de hardware que controla el tráfico de la red del target e inyecta un agent en los recursos web seleccionados. Viene en dos versiones, Appliance o Tactical: la primera es para la implementación en el ISP, la segunda se usa en el campo.

Network Injector Appliance
Versión apilable del Network Injector, para instalarlo en el ISP. Consulte: Tactical Network Injector.

O

operation
Investigación dirigida a uno o más targets, cuyos dispositivos tendrán agents.

P

Person
Entidad de Intelligence que representa a una persona involucrada en la investigación.

Position
Entidad de Intelligence que representa a un lugar involucrado en la investigación.

R

RCS
(Remote Control System). El producto que aquí se documenta.

RCS Console
Software diseñado para interactuar con RCS Server.

RCS Server
Una o más computadoras, según la arquitectura de instalación, donde se instalan los componentes esenciales de RCS: las bases de datos shard, los Network Controller y el Collector.

Receptor de RCS
Sistema RCS que recibe evidence de otros sistemas RCS emisores (consultar) pero nunca directamente de los agents. En comparación con un RCS completo, el receptor de RCS solo cuenta con las funciones de procesamiento de evidence.

reglas de alert
Reglas que crean alerts cuando se almacena nueva evidence o los agents se comunican por primera vez.

reglas de inyección
Opciones de configuración que definen cómo identificar el tráfico HTTP, qué recurso debe inyectarse y qué método se usará para la inyección.

S

secuencia de obtención
Grupo de eventos, acciones y módulos de obtención complejos, que forman parte de la configuración avanzada de agents.

SSH
(Secure SHell) Protocolo de red para la transmisión segura de datos, los servicios del intérprete de comandos remoto o la ejecución de comandos.

System
Sección de la consola en la que se administra el sistema.

T

Tactical Network Injector
Versión portátil del Network Injector, para uso táctico. Consulte: Network Injector Appliance.

TAP
(Test Access Port) Dispositivo de hardware que se instala en una red y que monitorea de forma pasiva el flujo de datos transmitido.

target
La persona física bajo investigación.Se representa por medio de la entidad Target en la sección Intelligence.

Técnico
Persona designada por el administrador para crear y administrar agents.

V

Virtual
Entidad de Intelligence que representa a una ubicación virtual (p. ej.: sitio web) involucrado en la investigación.

VPS
(Virtual Private Server) Servidor remoto en el que se instala el Anonymizer. Usualmente se alquila.

W

WPA

(Wi-Fi Protected Access) Protección de la red Wi-Fi.

WPA 2

(Wi-Fi Protected Access) Protección de la red Wi-Fi.

1

Introducción a esta guía

Presentación

Objetivos de este manual

Este manual sirve como guía para el *Administrador del sistema* para:

- instalar correctamente el sistema RCS y sus componentes
- configurar los componentes desde la consola de administración
- comprender y resolver cualquier problema que pudiera surgir en el sistema

A continuación se muestra la información necesaria para consultar el manual.

Contenido

En esta sección se incluyen los siguientes temas:

Nuevas funciones de la guía

Lista de notas publicadas y actualizaciones a esta ayuda en línea.

Fecha de publicación	***Código***	***Versión de software.***	***Descripción***
24 de noviembre de 2014	Manual del administrador del sistema 1.8 NOV-2014	9.5	Se actualizó el procedimiento de comunicación entre Network Injector y RCS Server, *consulte "**Arquitectura del sistema RCS**" en la página 8* . Se actualizó el procedimiento de la primera sincronización de Network Injector y RCS Server *consulte "**Primera sincronización de Network Injector con RCS Server**" en la página 57* .
20 de septiembre de 2014	Manual del administrador del sistema 1.7 SEP-2014	9.4	Se actualizaron los métodos de comunicación entre el Collector y el Anonymizer, *consulte "**Arquitectura del sistema RCS**" en la página 8* y *"**Qué debería saber acerca de los Anonymizers**" en la página 36* . Se agregó el servicio Master Node RCS Monitor, *consulte "**Arquitectura del sistema RCS**" en la página 8* y *"**Lista de servicios de RCS**" en la página 27* .
23 de junio de 2014	Manual del administrador del sistema 1.6 JUN-2013	9.3	Se agregó una lista de aplicaciones de terceros instalada en el Network Injector, *consulte "**Otras aplicaciones instaladas en Network Injectors**" en la página 55* . Se eliminó el tipo de arquitectura centralizada. Se agregaron varias arquitecturas del sistema RCS, *consulte "**Varias arquitecturas del sistema RCS**" en la página 11* . Se agregaron herramientas para resolver problemas con los componentes de RCS, *consulte "**Procedimiento de verificación del estado de los componentes**" en la página 83* Se agregaron dependencias entre los servicios de RCS, *consulte "**Lista de servicios de RCS**" en la página 27* *consulte "**Lista de servicios de RCS**" en la página 27* *"**Actualización de RCS Server**" en la página 67*

Fecha de publicación	*Código*	*Versión de software.*	*Descripción*
19 de febrero de 2014	Manual del administrador del sistema 1.5 FEB-2014	9.2	Se actualizó el manejo de la instalación y las actualizaciones de los Anonymizers, *consulte "**Instalación y configuración de Anonymizer**" en la página 38* , *"**Actualización del Anonymizer**" en la página 68* . Se agregó el servicio Carrier del Collector, *consulte "**Qué debería saber acerca de RCS**" en la página 10* Se editaron los comandos para revisar el estado de los componentes, *consulte "**Procedimiento de verificación del estado de los componentes**" en la página 83* . Se agregó la descripción de los comandos de terminal para las aplicaciones Tactical Control Center y Appliance Control Center, *consulte "**Comandos de Tactical Control Center y Appliance Control Center**" en la página 56*
30 de septiembre de 2013	Manual del administrador del sistema 1.4 SEP - 2013	9	Se actualizó la documentación de instalación, actualización y administración de Network Injector, *consulte "**Instalación de componentes adicionales**" en la página 35* , *"**Mantenimiento de rutina y actualizaciones del software**" en la página 65* , *"**Administración de los Network Injector**" en la página 112* . Se actualizó la documentación del conector, *consulte "**Administración de conectores**" en la página 110* . Se actualizó la documentación debido a las mejoras a la interfaz de usuario.

Documentación incluida

Los siguientes manuales se incluyen con el software RCS:

Manual	*Destinatarios*	*Código*	*Formato de distribución*
Manual del administrador del sistema(este manual)	Administrador del sistema	Manual del administrador del sistema 1.8 NOV-2014	PDF
Manual del administrador	Administradores	Manual del administrador 1.6 NOV-2014	PDF

Manual	*Destinatarios*	*Código*	*Formato de distribución*
Manual del técnico	Técnicos	Manual del técnico 1.9 NOV-2014	PDF
Manual del analista	Analistas	Manual del analista 1.8 NOV-2014	PDF

Convenciones tipográficas de notas

Las notas previstas en este documento se detallan a continuación (Manual de estilo de Microsoft):

ADVERTENCIA: indica una situación de riesgo que, si no se evita, podría causar lesiones físicas en el usuario o daños en el equipo.

PRECAUCIÓN: indica una situación de riesgo que, si no se evita, puede causar la pérdida de datos.

IMPORTANTE: indica las acciones necesarias para realizar una tarea. Si bien pueden pasarse por alto algunas notas sin que esto afecte a la realización de la tarea, no se deberían omitir las indicaciones importantes.

NOTA: información neutral y positiva que enfatiza o complementa la información del texto principal. Proporciona información que puede aplicarse solo en casos especiales.

Sugerencia: recomendación para la aplicación de técnicas y procedimientos descritos en el texto de acuerdo a ciertas necesidades especiales. Puede sugerirse un método alternativo y no es esencial para la comprensión del texto.

Llamada al servicio: la operation solo puede completarse con la ayuda del servicio técnico.

Convenciones tipográficas de formato

A continuación se muestran las explicaciones de algunas convenciones tipográficas:

Ejemplo	*Estilo*	*Descripción*
Consulte "Datos del usuario"	*cursiva*	indica el título de un capítulo, una sección, una subsección, un párrafo, una tabla o una imagen de este manual u otra publicación a la que se hace referencia.
<ddmmaaaa>	<aaa>	indica un texto que el usuario debe ingresar de acuerdo a cierta sintaxis. En el ejemplo, <ddmmaaaa> es una fecha y un posible valor podría ser “14072011”.
Seleccione uno de los servidores de la lista **[2]**.	**[x]**	indica el objeto citado en el texto que aparece en la imagen adyacente.
Haga clic en **Agregar**. Seleccione el menú **Archivo, Guardar datos**.	**negrita**	indica el texto en la interfaz del operador, que puede ser un elemento gráfico (como una tabla o pestaña) o un botón en la pantalla (como mostrar).
Presione Entrar	primera letra mayúscula	indica el nombre de una tecla en el teclado.
Consulte: Network Injector Appliance.	-	sugiere que compare la definición de una palabra en el glosario o contenido con otra palabra o contenido.

Destinatarios del producto y de esta guía

A continuación se muestra una lista de los profesionales que interactúan con RCS.

Destinatario	*Actividad*	*Habilidades*
Administrador del sistema	Sigue las indicaciones de HackingTeam que se suministran durante la fase contractual. Instala y actualiza los RCS Servers, los Network Injectors y las RCS Cosoles. Programa y se encarga de realizar las copias de seguridad. Restaura las copias de seguridad si se reemplazan los servidores.  **ADVERTENCIA: el administrador del sistema debe tener las habilidades necesarias. HackingTeam no se hace responsable en caso de mal funcionamiento del equipo o de posibles daños ocasionados por la instalación por parte de una persona no profesional.**	Técnico de red experto
Administrador	Crea cuentas y grupos autorizados. Crea operations y targets. Monitorea el estado del sistema y de las licencias.	Administrador de investigación

Destinatario	*Actividad*	*Habilidades*
Técnico	Crea agents y los configura. Establece las reglas de Network Injector	Técnico especialista en intercepciones
Analista	Analiza la evidence y la exporta.	Operativo

Datos de identificación del autor del software

HT S.r.l.
via della Moscova, 13
20121 Milan (MI)
Italia
Tel.: + 39 02 29 060 603
Fax: + 39 02 63 118 946
Correo electrónico: info@hackingteam.com

2

RCS (Remote Control System)

Presentación

Introducción

RCS (Remote Control System) es una solución que soporta investigaciones por medio de la intercepción activa y pasiva de los datos y la información de los dispositivos bajo investigación. De hecho, RCS crea, configura e instala agents de software de forma anónima que recopilan datos e información y envían los resultados a la base de datos central para decodificarlos y guardarlos.

Contenido

En esta sección se incluyen los siguientes temas:

Arquitectura del sistema RCS

Introducción

RCS está instalado en el centro operativo y en las salas de intercepciones de la autoridad propietaria. Puede venir con dispositivos especiales (hardware y software) que se instalan en organizaciones remotas como proveedores de servicios de Internet o servidores remotos.

Esquema de la arquitectura

Los componentes de software se instalan en varios servidores. A continuación se muestra el esquema de la arquitectura:

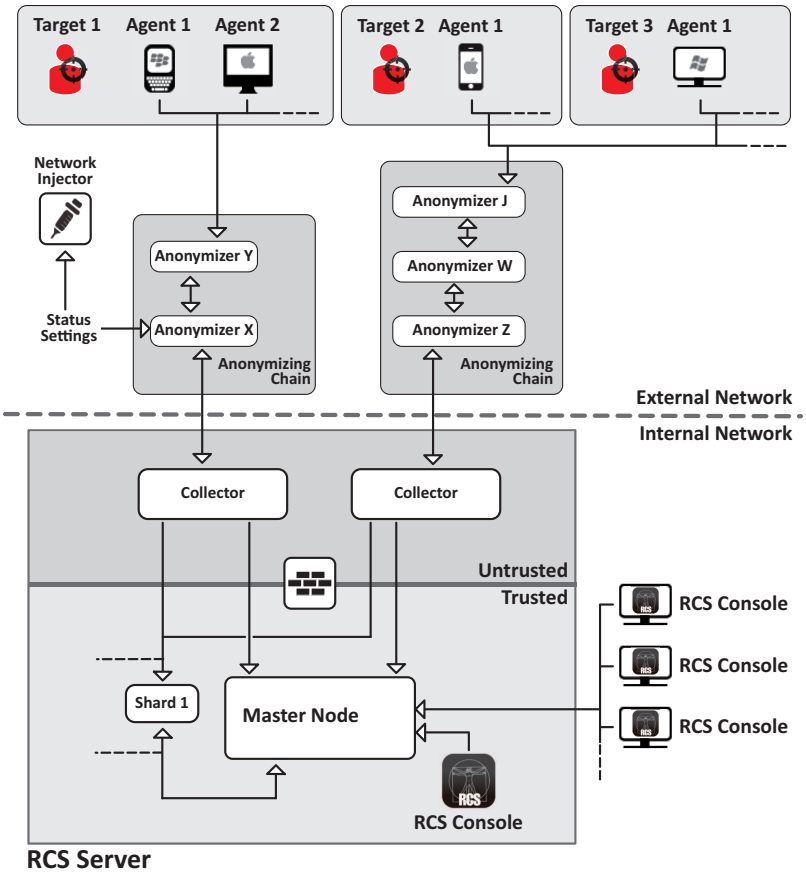


Figura 1: Arquitectura de RCS: esquema lógico

Componentes de la arquitectura

A continuación se muestran los componentes de la arquitectura:

Componente	*Función*	*Instalación*
Agent	Software de error, intercepta y comunica los datos y la información del target a un Anonymizer.	• dispositivos del target • fuentes de datos
Anonymizing chain **Anonymizer**	Grupo de Anonymizers geográficamente distribuidos que garantizan el anonimato del Collector y redireccionan los datos recopilados para proteger los servidores de los ataques remotos. Transfiere datos del agent y el Network Injector a los servidores. Se pueden configurar varios Anonymizers en cadena para aumentar el nivel de protección. Cada cadena conduce a un Collector.	VPS (Servidor privado virtual)
Collector	Uno por cadena de Anonymizers. Hay tres servicios instalados en cada uno: • Collector: recopila datos del agent, los envía al último Anonymizer en la cadena y los Network Injectors los envían al Anonymizer establecido. • Carrier: envía datos a las bases de datos Shards y al Master Node • Network Controller: recibe el estado del Anonymizer y también registra y envía actualizaciones y nuevas configuraciones. Se requiere una licencia única.	uno o más servidores en un entorno de front end
Firewall	Opcional pero muy recomendable, protege al entorno *confiable* donde se procesan y protegen los datos de los entornos *poco confiables* (donde se recopilan los datos).	RCS Server
RCS Console	Consola de configuración, monitoreo y análisis utilizada por los trabajadores de los centros operativos.	• RCS Server • red interna
Master Node	El corazón de RCS Server, administra los flujos de datos, el estado de los componentes e incluye la primera bases de datos shard. Incluye el servicio Worker para decodificar datos antes de guardarlos en la base de datos y el servicio Monitor para monitorear todos los componentes de la arquitectura, incluido el Master Node y envía un correo electrónico en caso de que se active una alarma.	RCS Server

Componente	*Función*	*Instalación*
Network Injector	(opcional) Componente de hardware (Appliance) o de red (Tactical), ejecuta operations de análisis de paquetes y de inyección en las conexiones HTTP del target. Se comunica con el Collector a través de un Anonymizer (y su cadena) para enviar datos y recibir reglas y configuraciones.	• ISP • LAN por cable o inalámbrica (casas, hoteles)
Shard x	Particiones adicionales de la base de datos distribuida de RCS. Shard 0 se incluye en el Master Node. Incluye el servicio Worker que permite decodificar los datos e ingresarlos en la base de datos.	uno o más servidores en un entorno de back end
Target	Personas sujetas a investigación. Cada dispositivo que pertenece al target es una fuente de datos que puede ser monitoreada por un agent.	-

Qué debería saber acerca de RCS

Operations

Los componentes del sistema RCS deben instalarse de forma adecuada tanto en el centro operativo como, a la larga, en un proveedor de servicio de Internet. Usualmente se divide en entornos de *front end*, para la recopilación, intercepción y monitoreo de datos, y en entornos de *back end* para la recopilación de datos y las copias de seguridad.

Flujo y protección de datos

RCS Server separa claramente las actividades en entornos *poco confiables* y entornos *confiables*. El límite está determinado por un firewall residente.

La intercepción de datos se recopila en entornos poco confiables, y luego se redirecciona para proteger la identidad del destinatario (usted). Posteriormente se envía a un recolector de información (Collector) y se envía al entorno confiable a través de un servicio específico (Carrier). Un componente específico de la máquina del Collector (Network Controller) verifica el estado y la configuración de la entidad remota.

En entornos confiables, se administra, establece y monitorea la evidence (Master Node).

Por último, RCS Console es un cliente que se conecta directamente al Master Node. Se puede instalar en cualquier computadora para que la utilicen varios usuarios de RCS.

*Consulte "**Arquitectura del sistema RCS**" en la página 8*

Continuidad del registro de datos

Los agents envían los datos recopilados al Collector. Si la comunicación se interrumpe, no hay conexión o el Collector no funciona, los agents pueden guardar una cantidad de datos determinada hasta que se recupere la conexión. Los datos que exceden el límite admitido se perderán.

Si el Carrier no puede comunicarse con el Master Node (por falta de servicio o porque se está realizando mantenimiento), los datos recibidos se guardan de forma local en el Collector hasta que el Master Node sea restaurado. Una vez restaurado, los datos se envían de forma automática.

Certificados digitales

El Master Node usa certificados digitales HTTPS que garantizan la seguridad de la comunicación entre el Master Node, el Collector y las RCS Consoles.

Algunos agents requieren certificados específicos que se deben crear y guardar en la carpeta \RCS\DB\config\certs.

*Consulte "**Archivos instalados al finalizar la instalación**" en la página 33*

Decodificación de datos

El servicio Worker se instala con cada base de datos shard y decodifica los datos antes de que se guarden en la base de datos. Para las bases de datos distribuidas, cada Shard tiene su propio Worker que recibe datos codificados del Master Node, los decodifica y los guarda en la base de datos. La carga de trabajo se distribuye automáticamente de forma equitativa entre todas las bases de datos shard en el mismo clúster.

Varias arquitecturas del sistema RCS

Introducción

Es posible configurar RCS para que se comunique con otros sistemas RCS para enviar o recibir evidence que recibió de otros agents.

Existen dos escenarios de comunicación posibles:

- de uno a muchos: un sistema RCS recibe toda la evidence de los agents y la distribuye a diversos sistemas RCS que solo muestran y procesan la evidence que les interesa. Por ejemplo, si se reúne evidence de una sola agencia central pero varias cortes locales realizan investigaciones.
- de muchos a uno: varios sistemas RCS reciben evidence de los agents y la envían a un solo sistema RCS que muestra y procesa toda la evidence. Por ejemplo, cuando una sola agencia local reúne y procesa la evidence, pero existe una agencia central que monitorea a las diferentes agencias locales y realiza investigaciones generales.

Esquema de una arquitectura de uno a muchos

A continuación se muestra el esquema de una arquitectura de uno a muchos:

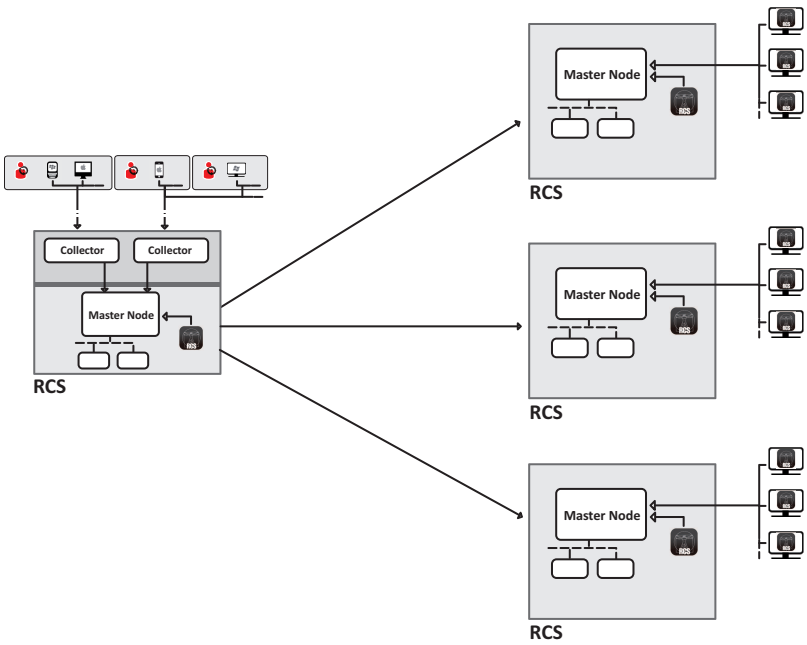


Figura 1: Esquema de arquitectura de RCS de uno a muchos: esquema lógico

Esquema de una arquitectura de muchos a uno

A continuación se muestra el esquema de una arquitectura de muchos a uno:

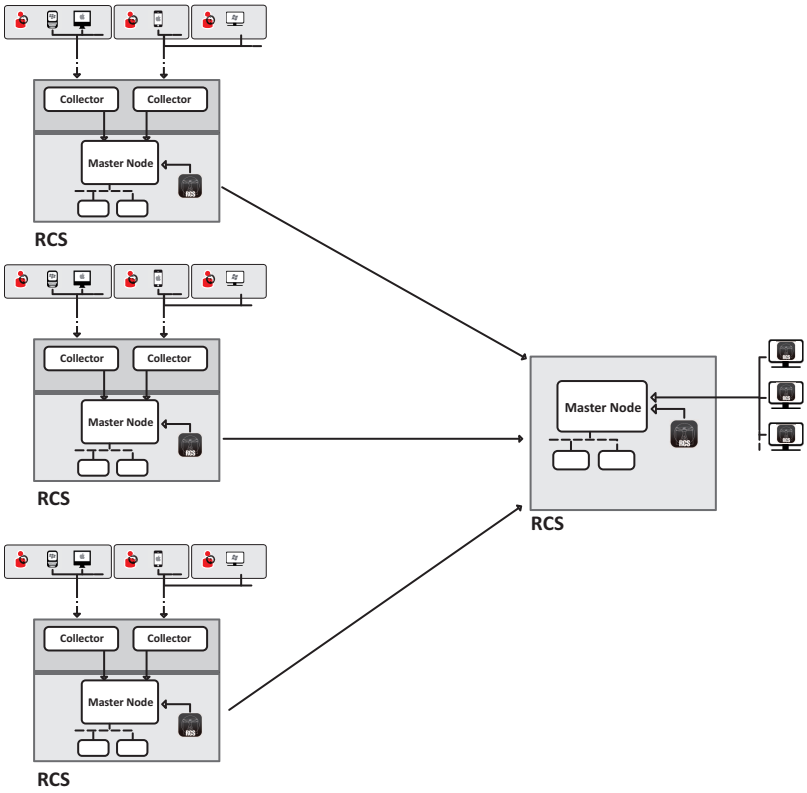


Figura 2: Esquema de arquitectura de RCS de muchos a uno: esquema lógico

Sistemas de emisores de RCS

Un sistema de emisores de RCS (tanto en la arquitectura de uno a muchos como de muchos a uno) es un sistema RCS completo. Incluye la instalación de un Collector y otros componentes adicionales y opcionales que permiten recibir evidence desde agents instalados en los dispositivos de los target. *Consulte "**Arquitectura del sistema RCS**" en la página 8*

La transferencia de datos a uno o más receptores de RCS se establece en RCS Console por medio de las reglas de conexión, *consulte "**Administración de conectores**" en la página 110* .

Sistemas de receptores de RCS

La finalidad principal de un sistema de receptores de RCS (tanto en la arquitectura de muchos a uno como de uno a muchos) es mostrar y procesar la evidence. La evidence que contiene proviene únicamente de uno o más sistemas de receptores de RCS, nunca directamente de los agents.

Las principales operations habilitadas en RCS Console son las que se relacionan con la administración y el procesamiento de evidence. Por otro lado, los agents son completamente administrados y configurados por el sistema de emisores de RCS. Los principales componentes son Master Node, RCS Console y algunos shards adicionales.

NOTA: si se reciben datos de un solo sistema de RCS, la única evidence que se muestra y puede ser procesada es la que proviene de las investigaciones. Si se reciben datos de varios sistemas de RCS, toda la evidence se mostrará y se podrá procesar y comparar en varias investigaciones.

Estructura de datos recibida

Una vez que se reciben los datos, estos se clasifican y se les asigna el mismo nombre que se estableció en la RCS Console del sistema del emisor. Posteriormente es posible cambiar el nombre para poder interpretarlos mejor sin crear problemas de comunicación entre los sistemas.

Si se reciben datos de varios sistemas de RCS, los datos llegan vinculados con el identificador del sistema del emisor de RCS.

Instalación de sistemas de receptores de RCS

NOTA: Los sistemas de receptores de RCS requieren una licencia de usuario específica.

A continuación se puede ver la secuencia de instalación completa:

Paso	*Acción*	*Consulte*
1	Instale el Master Node.	*"Instalación de RCS Server" en la página 21*
2	Revise los registros de instalación.	
3	Asegúrese de que los servicios del Master se hayan iniciado.	
4	Instale RCS Console.	*"Instalación de RCS Console" en la página 28*
5	Instale los shards adicionales que se necesiten.	*"Instalación de componentes adicionales" en la página 59*

3

Introducción a la instalación

Presentación

Introducción

La instalación de RCS se realiza durante la primera instalación o en las actualizaciones sucesivas. Los archivos de instalación se encuentran disponibles en el CD incluido en el paquete o se pueden descargar del portal de soporte técnico de HackingTeam.

Requisitos de instalación

Todo el hardware ya debe estar instalado y en funcionamiento de acuerdo con los requisitos del sistema que HackingTeam comunicó al momento de la confirmación del pedido.

*Consulte "**Requisitos mínimos del sistema**" en la página 17*

NOTA: la instalación de Network Injector es opcional y será documentada en los capítulos subsecuentes.

Contenido

En esta sección se incluyen los siguientes temas:

Contenido del paquete

Contenido del paquete

RCS se entrega en un paquete que incluye:

- un CD de instalación
- una llave USB con la licencia de usuario
- dos llaves USB de hardware (principal y respaldo)

Llamada al servicio: todas las llaves USB se entregan con un código de ID que debe comunicarse al servicio de soporte técnico para todos los repuestos y actualizaciones.

Contenido del paquete de instalación (CD o web)

El paquete de instalación incluido en el CD o que se descargue del portal de soporte técnico de HackingTeam contiene los siguientes archivos, donde 'x' es el raíz del CD:

Carpeta	*Archivos incluidos*	*Descripción*
x:	ChangeLog.pdf	Notas de la versión
x:\doc	RCS_*x.x*_Admin_*y.y*_*Idioma*.PDF RCS_*x.x*_Analist_*y.y*_*Idioma*.PDF RCS_ *x.x* _ SysAdmin_ *y.y*_*Idioma*.PDF RCS_*x.x*_Technician_ *y.y*_*Idioma*.PDF	Instalación de RCS y manuales del usuario. Cada manual está destinado a un rol de usuario específico. • x.x: versión de RCS. • y.y: versión del manual. • Idioma: idioma del manual.
x:\setup	AdoberAIRinstaller.exe	Archivo de instalación de Adobe AIR.
x:\setup	RCS-version.exe	Archivo de instalación de los servidores de RCS.
x:\setup	RCSconsole-version.air	Archivo de instalación de RCS Console.
x:\setup	RCS-ocr-version.exe	Archivo de instalación del módulo OCR (opcional).

Llave USB con la licencia de usuario

El paquete contiene una llave USB con la licencia de usuario para la versión de RCS proporcionada.

El archivo es necesario para la instalación y las actualizaciones del software. Es posible copiarlo de la llave USB a otros dispositivos.

Llave USB de hardware

En el paquete se incluyen dos memorias: una principal, ya asociada a la licencia en la llave USB de licencia, y una de respaldo, lista para ser activada en caso de que la principal falle.

IMPORTANTE: la memoria principal siembre debe estar conectada al Master Node para permitir que se ejecuten todos los servicios de RCS. ¡Todos los servicios se abortarán de forma inmediata si se desconecta la llave!

Requisitos mínimos del sistema

El hardware deberá ser configurado de conformidad con las instrucciones indicadas por el servicio de soporte técnico durante la fase contractual. Las computadoras en las que se instalará RCS deben tener las siguientes características:

Máquina	*Componente*	*Requisito*
Servidor de front end y de back end	Sistema operativo	Microsoft Windows Server 2008 R2 Standard (Inglés)
Computadora para RCS Console	Sistema operativo	Microsoft Windows o Apple Mac OS X.
	Navegador	Firefox 11 IE 9 Chrome
VPS para Anonymizer	Sistema operativo	Linux CentOS 6
Network Injector (Appliance o Tactical)	Sistema operativo	Proporcionado por HackingTeam

Puertos que deberán abrirse en el firewall

Si existe algún firewall instalado entre los componentes de RCS Server, se deben abrir los siguientes puertos TCP para permitir que se comuniquen los servicios:

Desde...	*A...*	*Puerto para abrir*
Anonymizer	Collector	80
Collector	Master Node	443
Collector	remoto	todos
Carrier	Master Node/Shard	442

Desde...	*A...*	*Puerto para abrir*
Master Node	Collector	80
Network Controller	remoto	443
Consola	Master Node	443, 444

Procedimientos del administrador del sistema

Introducción

A continuación se detallan los procedimientos típicos del administrador del sistema con referencias a los capítulos correspondientes.

Procedimientos

Instalar RCS y configurar sus componentes

A continuación se muestra el procedimiento de instalación de componentes de la arquitectura RCS:

Paso	*Acción*
1	Prepare el entorno de instalación. *Consulte "**Introducción a la instalación**" en la página 15 .*
2	Instale las RCS Server. *Consulte "**Instalación de RCS**" en la página 20 .*
3	Instale las RCS Consoles. *Consulte "**Instalación de RCS Console**" en la página 28 .*
4	Instale y configure los Anonymizers. *Consulte "**Instalación y configuración de Anonymizer**" en la página 38*
5	(opcional) Instale un módulo OCR. *Consulte "**Instalación del módulo OCR**" en la página 31*  *Llamada al servicio: para instalar otros módulos RCS, póngase en contacto con los técnicos de HackingTeam.*

Paso	*Acción*
6	(opcional) Instale las bases de datos shard y los Collectors adicionales. *Consulte "**Instalación de componentes adicionales**" en la página 59 .*
7	(opcional) Instale los Network Injectors. *Consulte "**Qué debería saber acerca del Network Injector Appliance**" en la página 40 .* *Consulte "**Qué debería saber acerca de Tactical Network Injector**" en la página 49 .*

Mantener y actualizar el sistema

A continuación se listan referencias a los capítulos sobre cómo mantener el rendimiento y actualizar el sistema:

- *Consulte "**Mantenimiento de rutina y actualizaciones del software**" en la página 65 .*
- *Consulte "**Edición de la configuración del Master Node y del Collector**" en la página 74 .*
- *Consulte "**Resolución de problemas**" en la página 79 .*

Monitoreo del sistema

A continuación se muestran referencias a los capítulos sobre cómo monitorear el sistema:

- *Consulte "**RCS Console para el administrador del sistema**" en la página 89*

4

Instalación de RCS

Presentación

Introducción

La instalación de RCS requiere de la intervención de varios servidores locales y remotos.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de la instalación de RCS

Privilegios de registro

RCS está diseñado para garantizar la máxima seguridad del servidor y de los datos recopilados. Para lograrlo, se definieron cuatro roles que normalmente corresponden a los profesionales que pueden registrarse en el sistema:

- Administrador del sistema: está a cargo exclusivamente de la instalación de hardware y software, y de las copias de seguridad.
- Administrador: está a cargo de todos los acceso al sistema, las investigaciones y las metas de investigación.
- Técnico: está a cargo de la configuración y de la instalación de los agents de intercepción
- Analista: está a cargo del análisis de los datos.

Sugerencia: se pueden asignar varios roles al mismo usuario; por ejemplo, un administrador también puede tener privilegios de técnico.

Usuario administrador y usuario administrador del sistema

Durante la instalación se crea un usuario especial con el nombre "admin", que cuenta con todos los privilegios (administrador del sistema, administrador, técnico y analista) y se usará para establecer todas las configuraciones y funciones de acceso a RCS Console.

Este usuario solo deberá usarse para este propósito. Al finalizar la instalación, recomendamos la creación de uno o más usuarios con los privilegios necesarios de acuerdo con el criterio de su organización.

IMPORTANTE: en este manual, normalmente nos referimos al usuario admin cuando hablamos del administrador del sistema, aun si cuenta con todos los privilegios.

Instalación de RCS Server

Introducción

Normalmente, en una arquitectura distribuida se instalan todos los componentes en uno o más servidores: un servidor para que el entorno de front end recopile datos y administre los dispositivos remotos, y un servidor para que el entorno de back end procese y guarde los datos.

Llamada al servicio: en una arquitectura distribuida se puede aumentar el tamaño. Consúltelo con el servicio técnico de HackingTeam.

NOTA: RCS Console se instalará con un procedimiento diferente, ya sea en el mismo servidor o en otra computadora remota.*Consulte "**Instalación de RCS Console**" en la página 28*

Requisitos de instalación

Antes de instalar un RCS Server se requiere lo siguiente:

- el nombre o la dirección IP de los servidores donde se instalará RCS
- el archivo de licencias, que se encuentra en la llave USB incluida en el paquete que se entrega, o de otra forma si se descarga de Internet.
- la llave de hardware USB, incluida en el paquete.
- para el firewall, abra los puertos para efectuar las operaciones correctas de servicio. *Consulte "**Puertos que deberán abrirse en el firewall**" en la página 17*

Secuencia de instalación

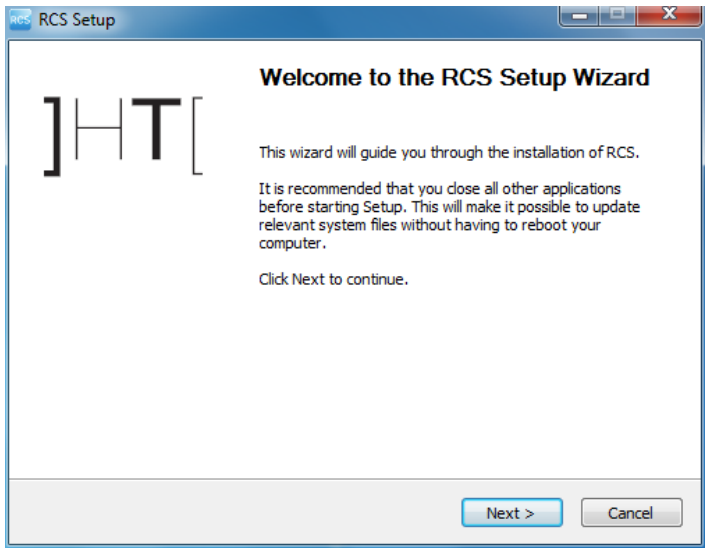
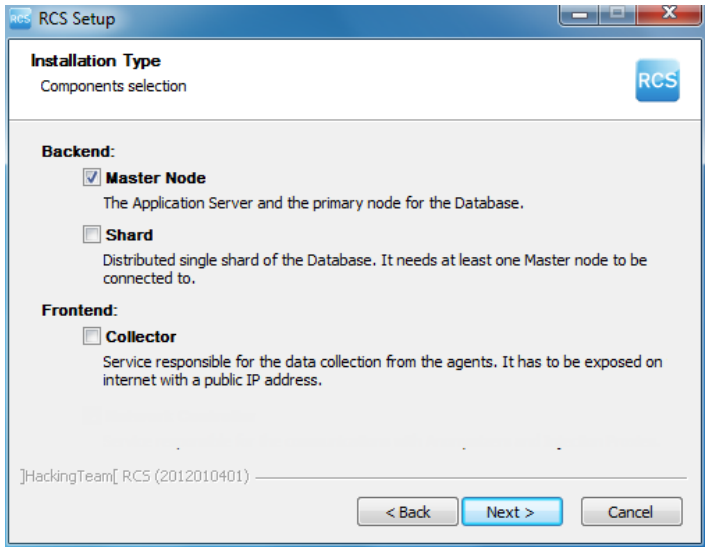
A continuación se puede ver la secuencia de instalación completa:

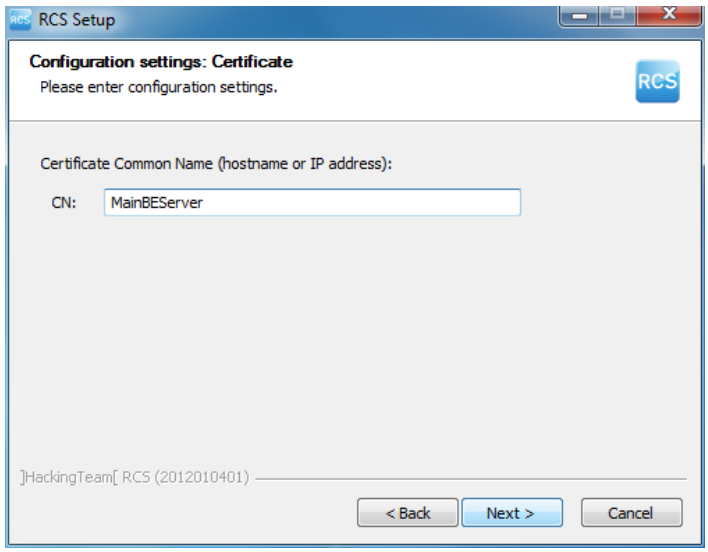
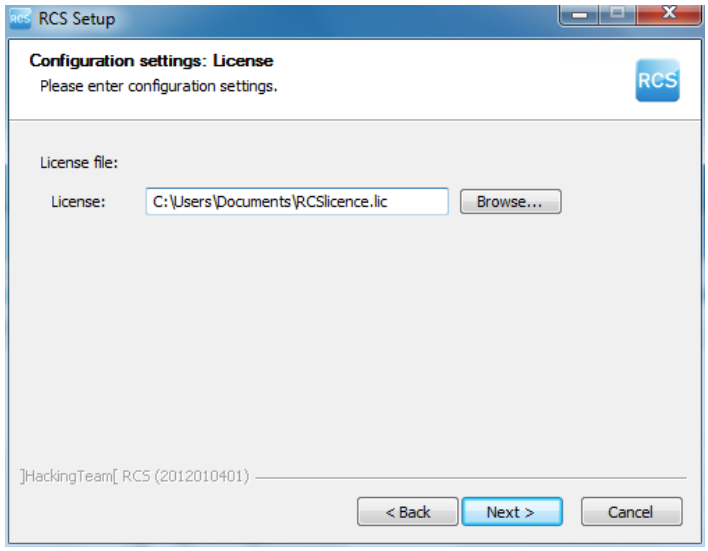
Paso	*Acción*	*Máquina*
1	Prepare lo que se indica en *requisitos de instalación.*	-
2	Instale el Master Node.	*servidor en un entorno de back end*
3	Revise los registros de instalación.	
4	Asegúrese de que los servicios del Master se hayan iniciado.	
5	Instalación del primer Collector.	*servidor en un entorno de front end*
6	Revise los registros de instalación.	
8	Instale RCS Console.	*servidor en un entorno de back end u otra computadora*
9	Configure la carpeta de la copia de seguridad en la unidad remota.	*servidor en un entorno de back end*

Instalación del Master Node

Para instalar el Master Node en el servidor en un entorno de back end:

Pasos	*Resultado*
1. Inserte la llave de hardware.	-

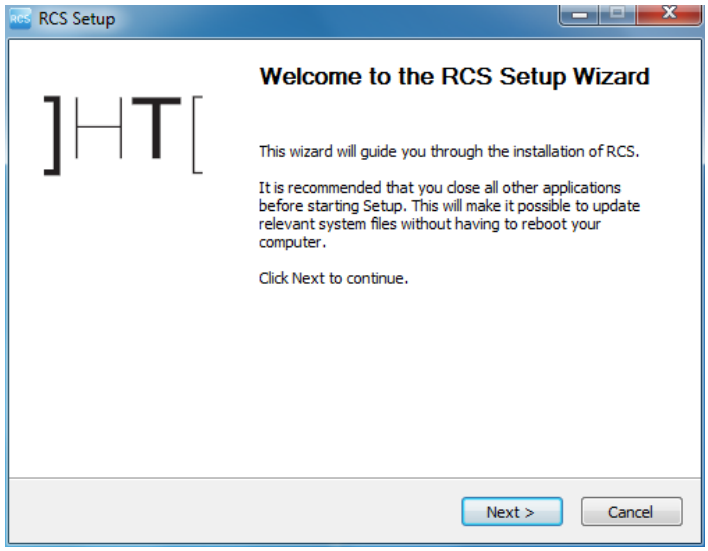
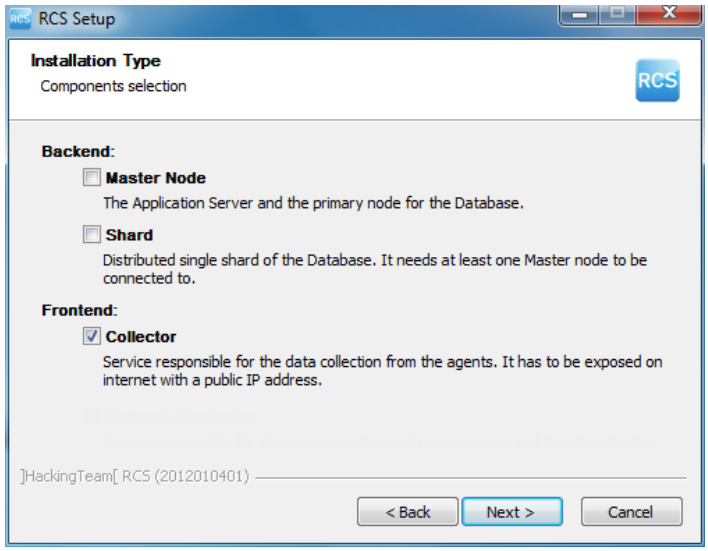
Pasos	*Resultado*
2. Inserte el CD con el paquete de instalación. Ejecute el archivo RCS-version.exe que se encuentra en la carpeta x:\setup, aparecerá la primera ventana del asistente. 3. Haga clic en **Siguiente**.	
4. Seleccione **Master Node.** 5. Haga clic en **Siguiente**.	

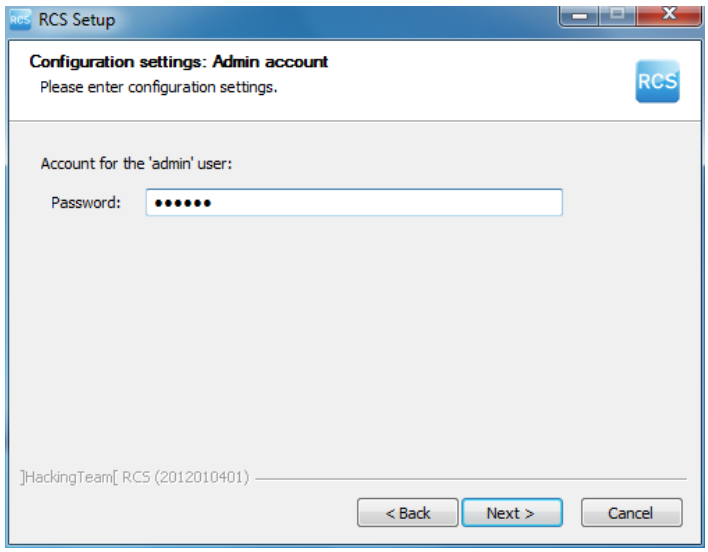
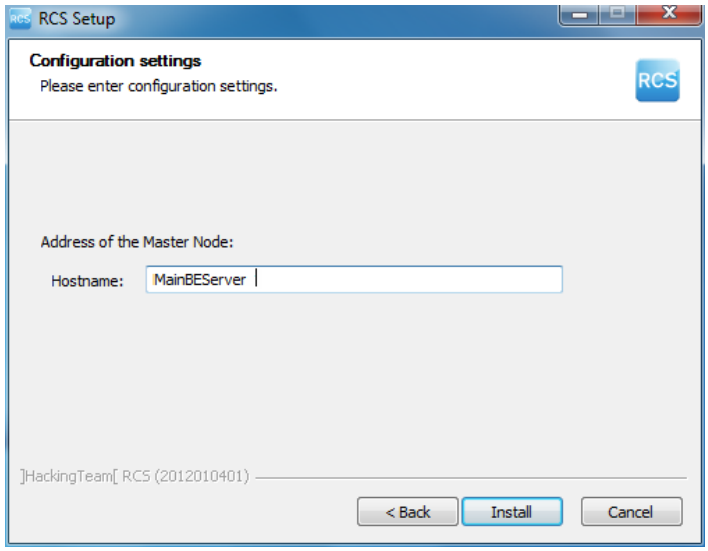
Pasos	*Resultado*
6. Ingrese el nombre o la dirección IP del servidor donde se está instalando el software, y que se indicará en la pantalla de inicio de sesión de RCS Console (p. ej.: RCSMasterNode). **IMPORTANTE: El nombre y la dirección IP deben ser unívocos.** 7. Haga clic en **Siguiente**.	
8. Seleccione el archivo de la licencia. 9. Haga clic en **Siguiente**.	
10. Ingrese la contraseña del administrador del sistema. 11. Haga clic en **Siguiente**: cuando la instalación finalice, los servicios estarán en funcionamiento y listos para recibir datos y comunicarse con RCS Console.	-

NOTA: en caso de que desee cambiar el nombre o la dirección IP del servidor después de la instalación debido a alguna falla, *consulte "**Edición de la configuración del Master Node**" en la página 76* .

Instalación de Collector

Para instalar varios Collectors en un entorno de front end:

Pasos	*Resultado*
1. Inserte el CD con el paquete de instalación. Ejecute el archivo RCS-version.exe que se encuentra en la carpeta x:\setup, aparecerá la primera ventana del asistente. 2. Haga clic en **Siguiente**.	
3. Seleccione **Collector.** NOTA: todos los servicios del Collector se instalarán automáticamente. 4. Haga clic en **Siguiente**.	

Pasos	*Resultado*
5. Ingrese la contraseña del administrador del sistema indicada en la instalación del Master Node. 6. Haga clic en **Continuar**: se inicia la instalación.	
7. Ingrese el nombre o la dirección IP del Master Node (p. ej.: **RCSMasterNode**). 8. Haga clic en **Instalar**: cuando la instalación finalice, se iniciarán los servicios e intentarán comunicarse con el Master Node. El servidor del entorno de back end está protegido y cualquier inicio de sesión remoto será redireccionado	

Verificar que los servicios se inicien

Asegúrese de que todos los servicios de RCS estén funcionando. Si los servicios no se están ejecutando, inícielos manualmente.

IMPORTANTE: el Collector solo acepta conexiones si el firewall de Windows se está ejecutando.

*Consulte "**Lista de servicios de RCS**" en la página siguiente*

Verificación de los registros de instalación

Si ocurre un error durante la instalación, verifique los registros y si es necesario envíelos al servicio técnico.

*Consulte "**Registros del sistema**" en la página 81*

Verificación de las direcciones IP

Para verificar todas las direcciones, inicie RCS Console, sección **System**, **Frontend**: las direcciones de los Collectors aparecerán en pantalla. *Consulte "**Instalación y configuración de Anonymizer**" en la página 38*

Uninstall

RCS se puede desinstalar desde el Dashboard de Windows

PRECAUCIÓN: Todos los datos guardados se perderán al desinstalar el Master Node. Para un funcionamiento correcto, procure realizar una copia de seguridad. Consulte "Administración de copias de seguridad" en la página 107 .

NOTA: los datos no se perderán al desinstalar otros servidores.

Lista de servicios de RCS

Los servicios de RCS aparecerán al finalizar varias fases de instalación. Uno de los procedimientos necesarios para completar la instalación es verificar que se iniciaron correctamente.

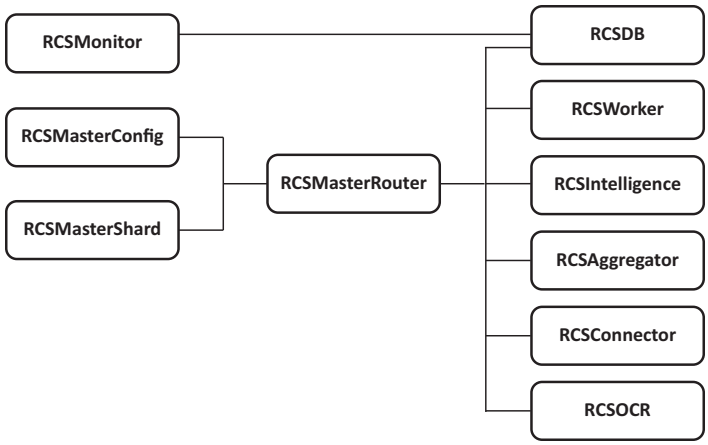
Servicios front end

Los servicios de los servidores front end son:

- RCSCollector
- RCSCarrier
- RCSController

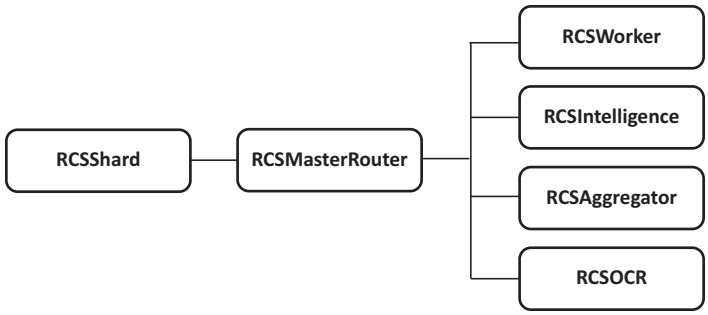
Servicios backend (Master Node)

Los servicios del Master Node y sus dependencias se muestran en el gráfico que se encuentra a continuación. Por ejemplo, el servicio **RCSDB** depende del servicio **RCSMasterRouter** y del servicio **RCSMonitor**.



Servicios backend (Shard)

Los servicios de la base de datos shard y sus dependencias se muestran en el gráfico que se encuentra a continuación.



Para obtener más información

Para reiniciar servicios detenidos, *consulte "**Procedimiento de reinicio de los servicios**" en la página 85* .

Instalación de RCS Console

Introducción

RCS Console es un cliente diseñado para interactuar con el Master Node. Usualmente se instala en las computadoras de la sala de control (para los inspectores y analistas) y todo el personal involucrado en la instalación de RCS la utiliza.

Requisitos

Antes de instalar RCS Console debe:

- tener los servidores RCS instalados
- preparar el nombre o la dirección IP del Master Node
- preparar la contraseña del administrador del sistema del Master Node

Secuencia de instalación

A continuación se muestra la secuencia de instalación de RCS Console:

Paso	*Acción*
1	Instale Adobe AIR.
2	Instale RCS Console.

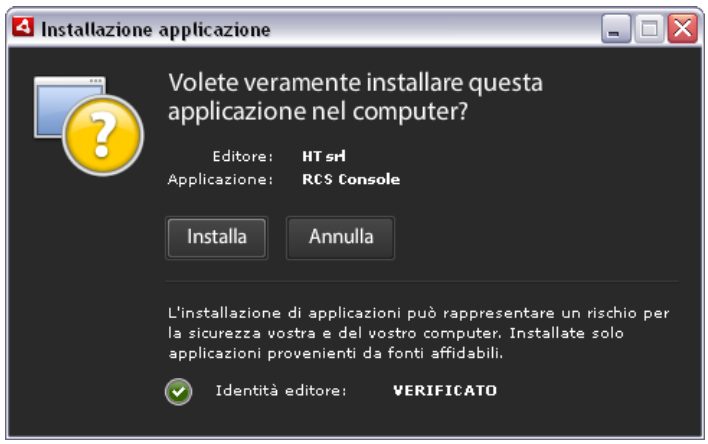
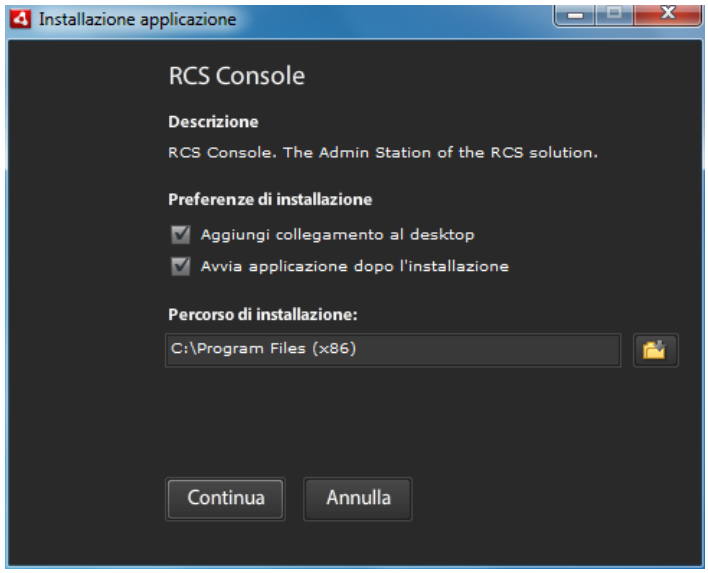
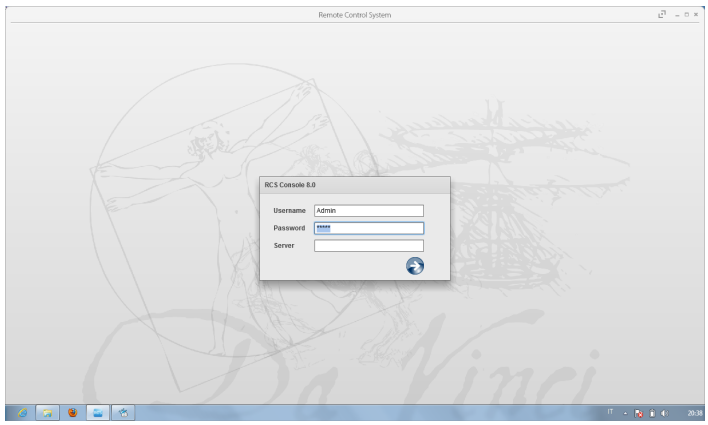
Instalación de Adobe AIR

Para instalar Adobe AIR:

Pasos	*Resultado*
1. Instale Adobe AIR: al final de la instalación no se mostrará ningún ícono en el escritorio.	

Instalación de RCS Console

Para instalar RCS Console:

Pasos	*Resultado*
1. Ejecute el archivo RCSconsole-version.air. 2. Haga clic en **Instalar**.	
3. Establezca las preferencias. 4. Haga clic en **Continuar**: RCS Console se instalará en la computadora.	
5. La ventana de inicio de sesión de RCS Console se mostrará al finalizar la instalación. 6. Ingrese sus credenciales y el nombre o la dirección IP del servidor. 7. Haga clic en  .  NOTA: el administrador del sistema inicia sesión con el nombre "admin" y la contraseña seleccionada durante la instalación.	

Desinstalación de RCS Console

Puede decidir desinstalar RCS Console en cualquier momento para, por ejemplo, utilizar la computadora para otra cosa. Los datos de la base de datos y las preferencias del usuario no se verán afectados de ningún modo.

Creación del usuario administrador

Durante la instalación de RCS se debe crear un usuario administrador de RCS Console. El administrador se encarga de crear todos los usuarios y de administrar las operations y los targets. *Consulte "**Destinatarios del producto y de esta guía**" en la página 5 .*

Para crear un usuario administrador:

Paso	*Acción*
1	Desde **RCS Console,** en la sección **Accounting**, haga clic en **Nuevo usuario** .
2	Ingrese los datos indicados, seleccione el **rol del administrador** y haga clic en **Guardar**: el nuevo usuario aparecerá en el área de trabajo principal con el ícono  . De ahora en adelante el usuario con las credenciales indicadas podrán acceder a RCS Console y ejecutar las funciones previstas.

Instalación del módulo OCR

Introducción

El módulo OCR es un módulo opcional que indexa todo el contenido (p. ej.: además de los documentos tradicionales, también indexa imágenes, archivos de audio, videos) para una búsqueda de texto completo.

NOTA: solo es compatible con los caracteres ASCII y la lectura de izquierda a derecha.

Requisitos de instalación

Es posible instalar el módulo OCR en todas las bases de datos shard del sistema para equilibrar automáticamente la carga de trabajo.

Funcionamiento del módulo OCR

A continuación se describe el funcionamiento del módulo OCR:

Fase	*Descripción*
1	Las imágenes de la evidence de tipo screenshot y todos los tipos de documentos, en espera de conversión se guardan en una cola diferente de la evidence en espera de análisis.
2	El módulo OCR lee la imagen o el documento de la cola y lo convierte en texto. Esta operación puede demorar entre uno y 5 o 10 segundos, según la cantidad de palabras que se deben obtener.
3	El texto de cada imagen o documento se guarda en una base de datos y se etiqueta como texto completo.
4	Los tiempos de conversión y las etiquetas para esa imagen particular se guardan en el archivo de registro del módulo.
5	El analista podrá acceder al texto en la página con la lista de evidence para una búsqueda en el campo **Info** o en la página detallada de esa evidence particular.

Ocupación de espacio en la base de datos para el texto de las etiquetas

Cada pieza de evidence screenshot ocupa más espacio en la base de datos porque siempre está acompañada del texto de las etiquetas. El aumento de espacio no es predecible, puesto que depende de la cantidad de capturas de pantalla obtenidas del agent y de la cantidad de palabras en cada screenshot.

Carga de trabajo del módulo OCR

El módulo OCR ocupa un gran porcentaje de CPU para convertir las capturas de pantalla, pero se ejecuta con una prioridad menor a la de otros procesos.

Por lo tanto, la carga del CPU solo se verá afectada cuando el sistema muestra el texto de la imagen convertida durante el análisis de la evidence.

Es mejor instalarlo inmediatamente en las bases de datos shard y no en el Master Node, que ya está lleno de procesos.

Indicios de una carga excesiva

Verifique cuánto tiempo demora en aparecer el texto en los detalles de esa evidence particular y revise los tiempos registrados al obtener las imágenes. Si se estima que es excesivo y existe otro servidor que está libre (p. ej.: que hospeda a otra base de datos shard o Master Node) instale otro módulo OCR.

De esta forma se dividirá la carga de trabajo entre todos los módulos instalados.

Instalación del módulo OCR

Para instalar un módulo OCR en un entorno de back end:

Pasos	*Resultado*
1. Inserte el CD con el paquete de instalación. Ejecute el archivo RCS-ocr-version.exe que se encuentra en la carpeta x:\setup, aparecerá la primera ventana del asistente. 2. Haga clic en **Siguiente**.	
3. Siga los pasos que se indican a continuación hasta que la instalación haya finalizado: el módulo comenzará a convertir las imágenes la primera vez que se reciba una evidence de tipo screenshot.	-

Verificar el correcto funcionamiento del módulo OCR

Para comprobar si la conversión de la imagen a texto es demasiado lenta o no, vea cuánto se tarda en aparecer el botón  en la página de detalles de la evidence.

Uninstall

El módulo OCR se puede desinstalar desde el Dashboard de Windows.

NOTA: la desinstalación del módulo OCR no pone en riesgo al texto que ya se convirtió y etiquetó.

Archivos instalados al finalizar la instalación

Al finalizar la instalación aparecerán varias carpetas, organizadas de acuerdo al componente opcional instalado:

Carpeta	*Archivos incluidos*
Copia de seguridad	La carpeta contiene los archivos con los datos guardados en las bases de datos. *Consulte "**Administración de copias de seguridad**" en la página 107*  **IMPORTANTE: No se debe tocar el contenido de esta carpeta. Para guardar los datos de la copia de seguridad en discos remotos, utilice la función** Administrador de discos **de Windows e instale el disco como carpeta NTFS. Para ello seleccione esta carpeta como destino.** **Ruta**: C:\RCS\DB\backup
bin	La carpeta contiene las herramientas (p. ej.: rcs-db-config) que se utilizan para configurar los componentes de RCS. *Consulte "**Herramientas de configuración**" en la página 75* **Ruta**: C:\RCS\DB\bin C:\RCS\Collector\bin
certs	La carpeta contiene los certificados utilizados por diversos servicios para acceder al Master Node. Se actualizan cuando se edita la configuración de RCS. *Consulte "**Edición de la configuración del Master Node**" en la página 76* **Ruta**: `\RCS\DB\config\certs`
config	La carpeta contiene archivos de configuración del sistema de números. **Ruta**: C:\RCS\DB\config C:\RCS\Collector\config

log	Archivo de registro de los componentes de RCS.
	*Consulte "**Registros del sistema**" en la página 81*
	Ruta:
	`C:\RCS\DB\log`
	`C:\RCS\Collector\log`

5

Instalación de componentes adicionales

Presentación

Introducción

La instalación de RCS puede incluir la instalación de otros componentes adicionales:

- Anonymizer
- Network Injector
- Base de datos shard
- Collector

Contenido

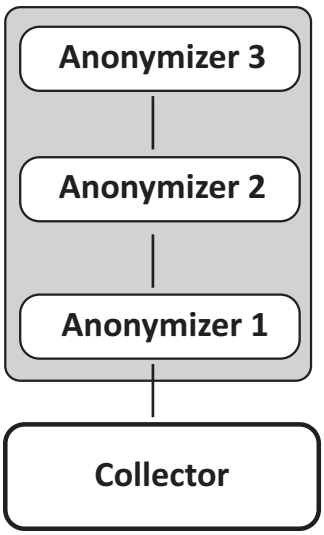
En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de los Anonymizers

Introducción

Un Anonymizer se usa para redireccionar datos de un grupo de agents y Network Injectors. El Anonymizer se instala en un servidor conectado a Internet, que no se puede volver a conectar al resto de la infraestructura como, por ejemplo, un VPS (Servidor privado virtual), alquilado para ese propósito.

Se pueden configurar varios Anonymizers en cadena para aumentar el nivel de protección. Cada cadena conduce a un Collector.



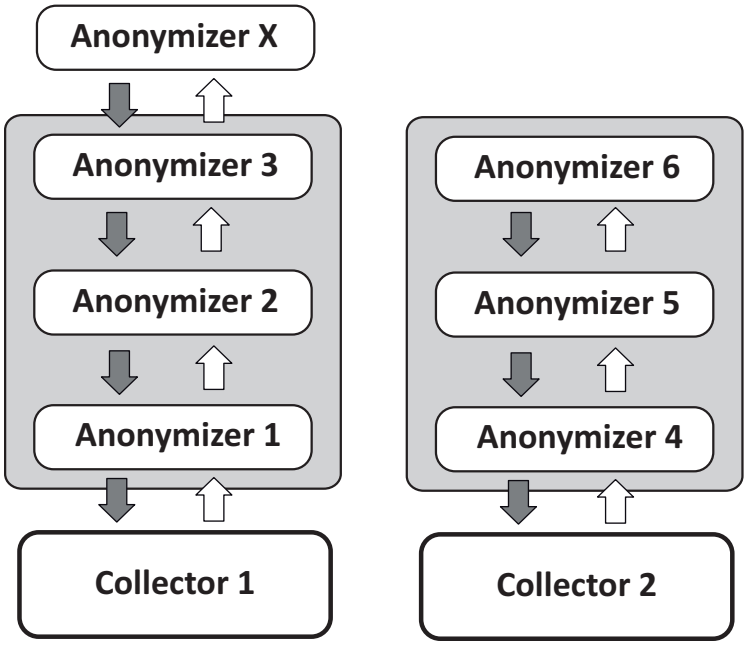
Estado del Anonymizer

Un Anonymizer puede tener distintos estados:

Estado	*Símbolo en RCS Console, System, Frontend*
En cadena operativa	
Fuera de cadena	
Desactivado	

Estado	*Símbolo en RCS Console, System, Frontend*
Anonymizer no reconocido porque aún no entra en contacto con el Collector	
Anonymizer con fallas	

Comunicaciones entre el Anonymizer y el Collector

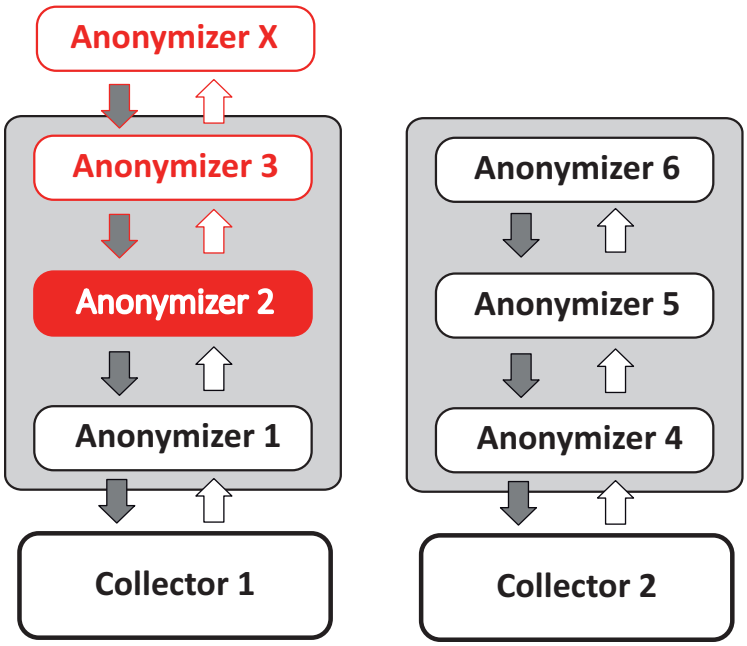


Una vez que se haya instalado y configurado el Anonymizer, este envía el estado y los registros al Collector y recibe las configuraciones y actualizaciones del Collector a través de la cadena de Anonymizers. Por ejemplo, el **Anonymizer 2** envía su estado al **Anonymizer 1**, y este lo envía al **Collector 1**.

NOTA: si un Anonymizer no pertenece a ninguna cadena (p. ej.: el **Anonymizer X** en el gráfico), utilizará la primera cadena de Anonymizers en la configuración para comunicarse con el Collector.

NOTA: para excluir a un Anonymizer de todas las comunicaciones, simplemente desactívelo.

Anonymizer defectuoso



Un Anonymizer averiado (p. ej.: el **Anonymizer 2** en el gráfico) que interrumpe las comunicaciones entre el Collector y los Anonymizers en esta cadena se considera defectuoso. Para continuar trabajando con los demás Anonymizers de la cadena, retire el Anonymizer defectuoso de la cadena y actualice la configuración.

Instalación y configuración de Anonymizer

Requisito de instalación

Un VPS se debe alquilar con los requisitos mínimos de sistema, definidos en la fase contractual para instalar Anonymizers.

*Consulte "**Requisitos mínimos del sistema**" en la página 17*

Instalación

PRECAUCIÓN: use el protocolo SSH para todas las operations de instalación, configuración y transferencia de datos en la unidad remota.

Para instalar el Anonymizer en un servidor privado:

Paso	*Acción*
1	Desde **RCS Console,** en la sección **System**, haga clic en **Frontend**, **Nuevo Anonymizer**.
2	Ingrese los datos indicados y haga clic en **Guardar.** **Resultado**: el Anonymizer aparecerá en la lista de Anonymizers con el ícono  . En la sección **Monitor**, aparecerá un objeto de monitoreo para el Anonymizer agregado.
3	Seleccione el Anonymizer y arrástrelo al Collector o a otro Anonymizer para crear una cadena.
4	Haga clic en **Descargar instalador**. **Resultado**: se genera el archivo del instalador `anon_install.zip` y se guarda en el escritorio de la consola.
5	Conecte el servidor y copie el archivo `anon_install.zip` en un carpeta del servidor.
6	Conecte el servidor, descomprima el archivo e inicie el instalador ingresando: `# sh install` **Resultado**: el Anonymizer se instala en la carpeta del servidor /opt/bbproxy.
7	Desde **RCS Console,** en la sección **System**, **Frontend**, seleccione el Anonymizer y haga clic en **Aplicar configuración**: el Collector enviará la nueva configuración al Anonymizer a través de la cadena de Anonymizers.

Datos del Anonymizer

A continuación se describen los datos del Anonymizer seleccionado:

Datos	*Descripción*
Nombre	Nombre del Anonymizer.
Descripción	Descripción del usuario
Versión	Versión de software. Para ver las versiones de software para todos los componentes, consulte la sección **Monitor**.
Dirección	Dirección IP del VPS donde se instaló el Anonymizer.
Activado	Si está activado, el Anonymizer se conecta para recibir actualizaciones y nuevas configuraciones. Desactive la función para evitar conexiones con Anonymizers en entornos poco confiables o con Anonymizers averiados.
Log	Últimos mensajes registrados. Para ver el contenido del archivo de registro *consulte "**Registros del sistema**" en la página 81*

Verificación de arranque

El Anonymizer envía sus registros a syslog, que los administra y guarda en un archivo. Los archivos usualmente se guardan en los siguientes archivos (según la versión del sistema operativo y la configuración del servicio syslog):

```
/var/log/messages
/var/log/syslog
```

Verificación de dirección IP

Para verificar todas las direcciones del Anonymizer, inicie **RCS Console**, sección **System, Frontend**: las direcciones de los Collectors aparecerán en pantalla. *Consulte "**Actualización del Anonymizer**" en la página 68*

Editar las opciones de configuración

Para editar las opciones de configuración del Anonymizer:

Paso	*Acción*
1	En la sección **System**, **Frontend**, haga clic en el ícono del Anonymizer.
2	Edite los datos indicados y haga clic en **Guardar.** **Resultado**: se actualizará la pantalla.
3	Consulte el estado del Anonymizer en la sección **Monitor**.
4	Haga clic en **Aplicar configuración**. **Resultado**: RCS se conecta con el Anonymizer y transfiere la nueva configuración a través de la cadena de Anonymizers.

Uninstall

Para desinstalar el Anonymizer, elimine la carpeta del servidor /opt/bbproxy y el Anonymizer de RCS Console. *Consulte "**Actualización del Anonymizer**".*

Qué debería saber acerca del Network Injector Appliance

Introducción

Network Injector Appliance es un servidor de red para instalaciones en un segmento interno al conmutador en un proveedor de servicios de Internet.

Es posible inyectar un agent de RCS en páginas web visitadas o archivos descargados, a través de conexiones de targets de monitoreo.

Network Injector Appliance utiliza Network Injector - Network Appliance como sistema operativo y Appliance Control Center como software de control.

NOTA: Network Injector Appliance se proporciona instalado y listo para usar, completo con todas las aplicaciones previstas.

Funciones principales

Network Injector Appliance analiza el tráfico del target y, en caso de que alguna de las reglas establecidas coincida, inyecta agents.

Network Injector Appliance se comunica con RCS a través de un Anonymizer (y su cadena, *consulte "**Qué debería saber acerca de los Anonymizers**" en la página 36*). Las comunicaciones se realizan cada 30 segundos para recibir reglas de identificación e infección, y enviar estados y registros.

Es posible configurar el software de control Appliance Control Center para acceso remoto.

Conexiones de red

Network Injector Appliance requiere dos conexiones de red: una para interceptar el tráfico del target y la otra para inyectar agents y comunicarse con RCS Server.

Sugerencia: Network Injector Appliance es independiente. Se la puede dejar funcionando sin tener que comunicarse con RCS Server.

Llamada al servicio: dadas las características de Network Injector Appliance, este manual solo brinda las indicaciones esenciales de conexiones, permitiendo al servicio técnico brindar aquellos aspectos estratégicos que se definen en la fase de configuración y distribución.

Clave de autentificación

Para comunicarse con RCS Server de forma segura se debe instalar una clave de autentificación en el Network Injector. La clave deberá generarse cuando el objeto Network Injector se cree en RCS Console y se instalará a través del Appliance Control Center durante la primera sincronización del Network Injector con RCS, *consulte "**Primera sincronización de Network Injector con RCS Server**" en la página 57* .

Esquema de conexión estándar

Esquema típico para un conmutador de acceso que dirige los datos hacia el Network Injector Appliance:

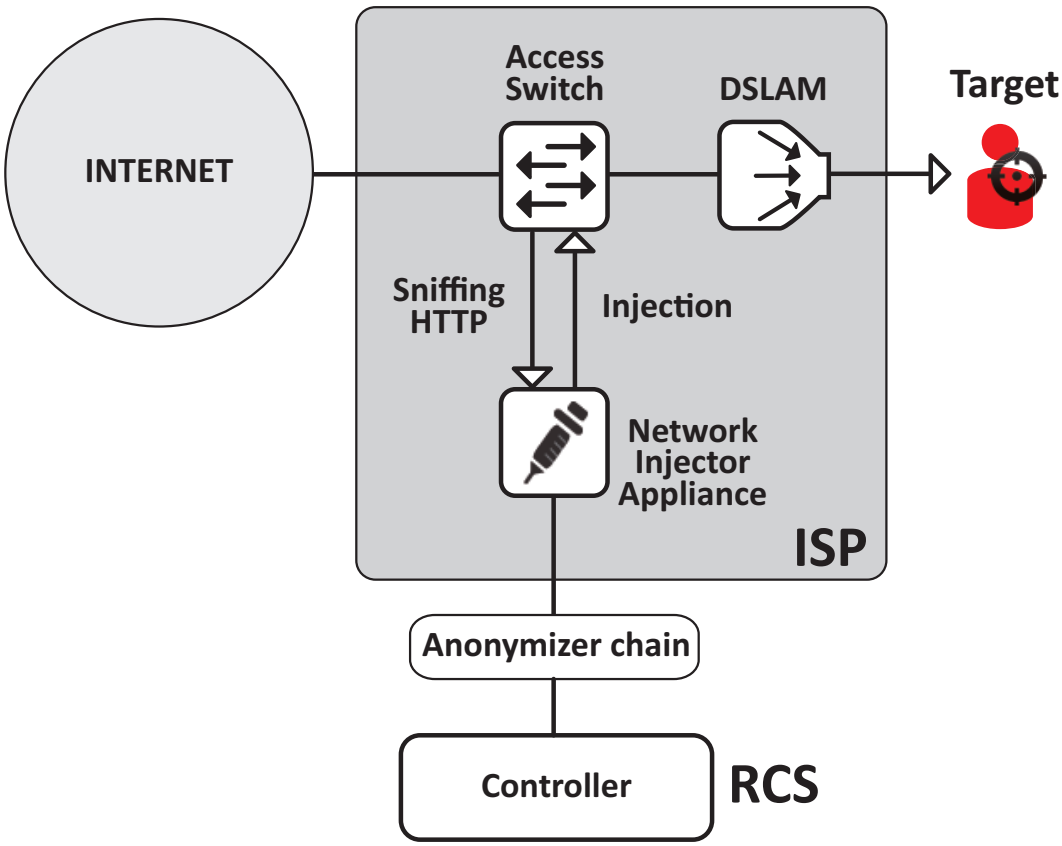


Figura 1: Network Injector Appliance: esquema físico

Esquema de conexiones como segmento interno al conmutador

Esquema típico con dispositivo TAP para acelerar el enrutamiento de los datos del conmutador de acceso:

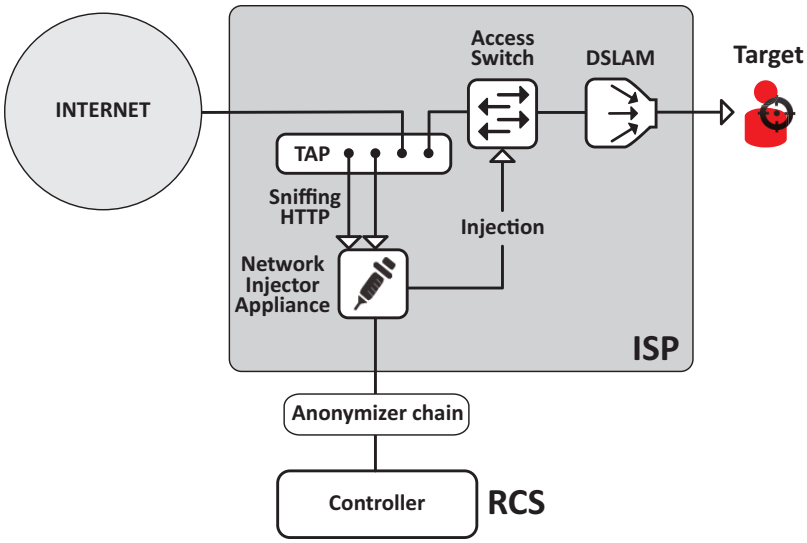


Figura 2: Network Injector Appliance con TAP: esquema físico

Análisis de datos a través de TAP, puerto SPAN

Un dispositivo TAP suele estar instalado en el proveedor de servicios de Internet, y es la solución más adecuada para el monitoreo de tráfico.

El uso de un puerto SPAN tiene las siguientes desventajas:

- el uso del CPU del conmutador puede aumentar significativamente debido al uso del puerto
- el puerto SPAN en el conmutador puede estar en uso

Instalación de Network Injector Appliance

Introducción

Network Injector Appliance se entrega con el sistema operativo Network Appliance y el software de control Appliance Control Center, instalados previamente y configurados. El hardware debe estar instalado con el proveedor de servicios de Internet y sincronizado con RCS Server.

Contenido del paquete

El paquete incluye una serie de conectores GBIC para monitorear la fibra óptica y las conexiones RJ45.

Secuencia de instalación

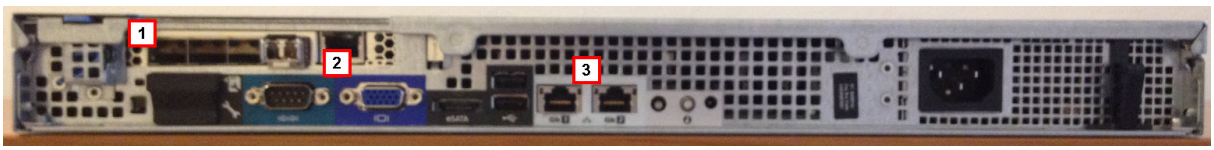
Sugerencia: prepare el Network Injector Appliance en sus oficinas antes de instalarlo en el proveedor de Internet.

A continuación se puede ver la secuencia de instalación completa:

Paso	*Acción*	*Párrafo*
1	Conecte Network Injector Appliance a la red.	*"**Conexiones de red**" en la página opuesta*
2	Instale el sistema operativo de Network Appliance NOTA: al momento de la compra el sistema operativo ya está instalado.	*"**Instalación y configuración del sistema operativo**" en la página opuesta*
3	Sincronización de Network Injector con RCS Server	*"**Primera sincronización de Network Injector con RCS Server**" en la página 57*
4	Verifique el estado del Network Injector	*"**Verifique el estado del Network Injector**" en la página 58*
5	Transfiera el Network Injector Appliance al proveedor de servicios de Internet y cambie las direcciones de red para activar el acceso a Internet.	-

Descripción del panel posterior

A continuación se describe el panel posterior:



A continuación se puede ver una lista de componentes visibles:

Área	*Componente*	*Descripción*
1	**Puertos de análisis de paquetes**	Hasta cuatro conexiones para los conmutadores de tráfico en los targets que serán monitoreados o hasta dos para dispositivos redundantes. NOTA: se admiten conexiones de fibra óptica o cobre.
2	**Placa madre**	Salidas estándar de las PC para conectar el monitor y el teclado para iniciar las herramientas `sysconf` o realizar actualizaciones desde el CD de instalación. *Consulte "**Procedimientos de mantenimiento de rutina**" en la página 66*
3	**Puertos de administración e infección**	**Puerto 1**: conexión de red con Network Controller para la recepción de parámetros de configuración y el envío del estado. La dirección debe establecerse con Network Manager. **Puerto 2**: conexión de la red para la inyección de tráfico.

Conexiones de red

Sugerencia: prepare el Network Injector Appliance. Para eso, conéctelo a su red y configure los parámetros antes de transferirlo al proveedor de Internet.

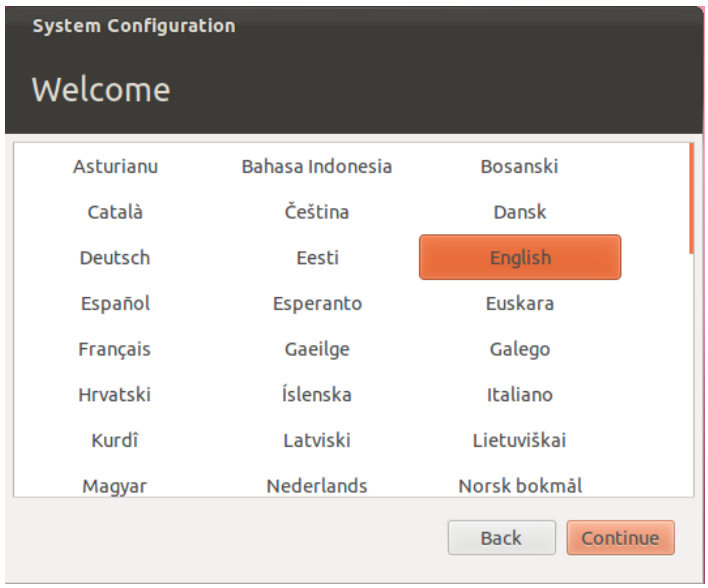
A continuación se describe el procedimiento de conexión a la red:

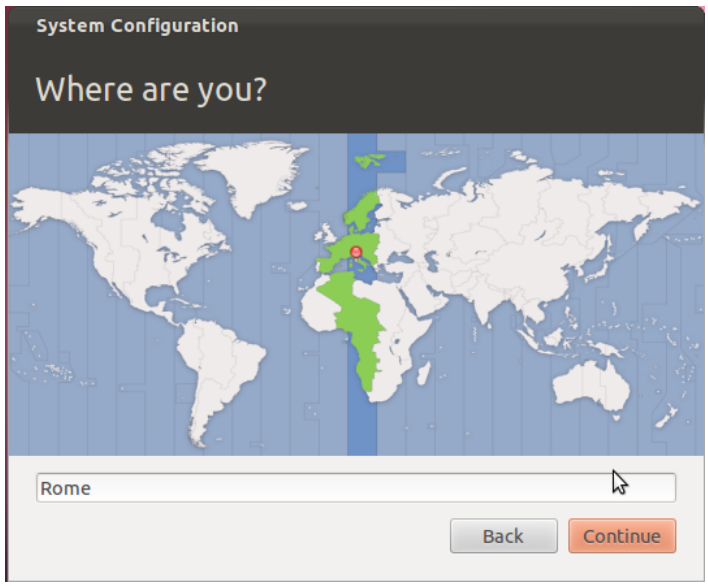
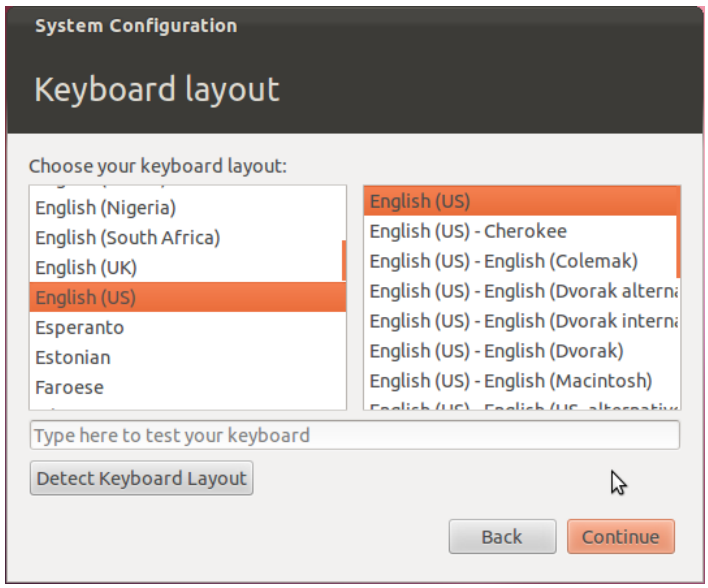
Pasos	*Esquema*
1. Conecte el conmutador de tráfico del target a los puertos de análisis de paquetes **[1].** **IMPORTANTE: para dispositivos redundantes, conecte ambos dispositivos.** 2. Conecte los puertos de administración (puerto 1) e inyección (puerto 2) **[3]** a Internet. 3. Conecte el monitor y el teclado **[2]**.	

Instalación y configuración del sistema operativo

Network Injector Appliance se proporciona instalado y listo para usar, completo y con todas las aplicaciones previstas. También se puede instalar usando un disco de restauración.

A continuación se describe el procedimiento:

Pasos	*Resultado*
1. Conecte la computadora a la red con un cable Ethernet e inserte el CD de instalación.	-
2. Seleccione Network Appliance para la instalación de la versión para servidor: se iniciará la instalación del sistema operativo y la computadora se apagará al finalizar. **IMPORTANTE: la computadora debe permanecer conectada a Internet durante todo el proceso de instalación.**	-
3. Reinicie la computadora portátil.	-
4. Aparece la primera ventana de instalación. 5. Seleccione el idioma.	

Pasos	***Resultado***
6. Seleccione la zona horaria correcta.	
7. Se lee el esquema del teclado. Solo cámbielo si es necesario.	

Pasos	*Resultado*
8. Ingrese los datos del usuario: inicia la instalación del sistema operativo.	
9. Al terminar de instalar el sistema operativo aparece la página de inicio de sesión normal. Se instala el sistema operativo y el software de control Appliance Control Center en la computadora.	-

Verificación de la dirección IP

Para verificar las direcciones IP del Network Injector, abra RCS Console, la sección **Monitor**: la dirección IP se indica en la columna **Address** del Network Injector mostrado.

Cambio de la dirección IP

Si la dirección IP del Network Injector cambia, se mostrará un nuevo elemento en la sección **Monitor** de RCS Console. Se incluirán dos elementos para ese Network Injector: uno con la nueva dirección, en verde (componente en funcionamiento), y el otro con la dirección anterior, en rojo. Elimina el elemento con la dirección anterior.

Uninstall

Para desinstalar un Network Injector Appliance, simplemente elimine el objeto en RCS Console y apague el dispositivo.

*Consulte "**Administración de los Network Injector**" en la página 112*

Qué debería saber acerca de Tactical Network Injector

Introducción

Tactical Network Injector es una computadora portátil para la instalación táctica en una LAN o en redes Wi-Fi. Además, se puede utilizar para desbloquear la contraseña del sistema operativo a fin de permitir que ocurran infecciones físicas (p. ej.: a través de Silent Installer).

Tactical Network Injector utiliza Network Injector - Tactical Devices como sistema operativo y Tactical Control Center como software de control.

NOTA: Tactical Network Injector se proporciona instalado y listo para usar, completo con codificación de disco y todas las aplicaciones previstas.

Funciones principales

El Tactical Network Injector identifica dispositivos en una red por cable o Wi-Fi e inyecta agents. Funciona en base a reglas de identificación (automática o manual) o inyección establecidas en la RCS Console. También se puede conectar a redes Wi-Fi protegidas, simular ser un punto de acceso a una red Wi-Fi y desbloquear la contraseña del sistema operativo.

Tactical Network Injector se comunica con RCS a través de un Anonymizer (y su cadena, *consulte "**Qué debería saber acerca de los Anonymizers**" en la página 36*). Las comunicaciones se realizan cada 30 segundos para recibir reglas de identificación e infección, y enviar estados y registros.

Este software de control de Tactical Control Center se puede configurar por acceso remoto.

Conexiones de red

Tactical Network Injector requiere dos conexiones de red: una para interceptar el tráfico del target y la otra para inyectar agents y comunicarse con RCS Server.

Sugerencia: después de configurarlo, Tactical Network Injector es independiente. Se requiere una conexión de Internet para obtener las reglas actualizadas de RCS y enviar los registros (sincronización).

Clave de autentificación

Para comunicarse con RCS Server de forma segura se debe instalar una clave de autentificación en el Network Injector. La clave deberá generarse cuando el objeto Network Injector se cree en RCS Console y se instalará a través del Tactical Control Center durante la primera sincronización del Network Injector con RCS, *consulte "**Primera sincronización de Network Injector con RCS Server**" en la página 57* .

Esquema de conexión estándar

Esquema típico de Wi-Fi donde Tactical Network Injector está conectado a la misma red Wi-Fi que los dispositivos del target.

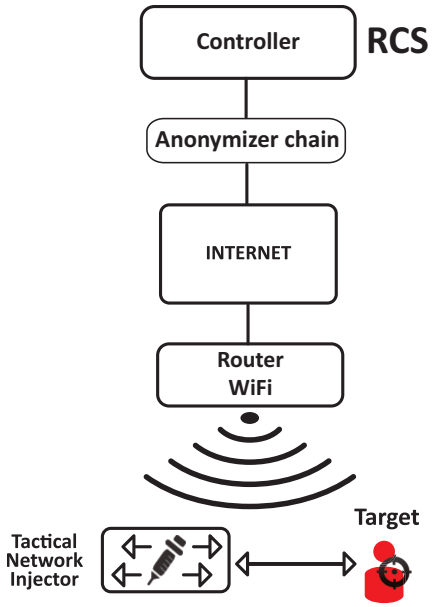


Figura 1: Tactical Network Injector: esquema de conexión estándar

Esquema de conexión en un punto de acceso emulado

Esquema típico en un entorno Wi-Fi donde Tactical Network Injector emula un punto de acceso a una red Wi-Fi abierta para atraer a los dispositivos del target.

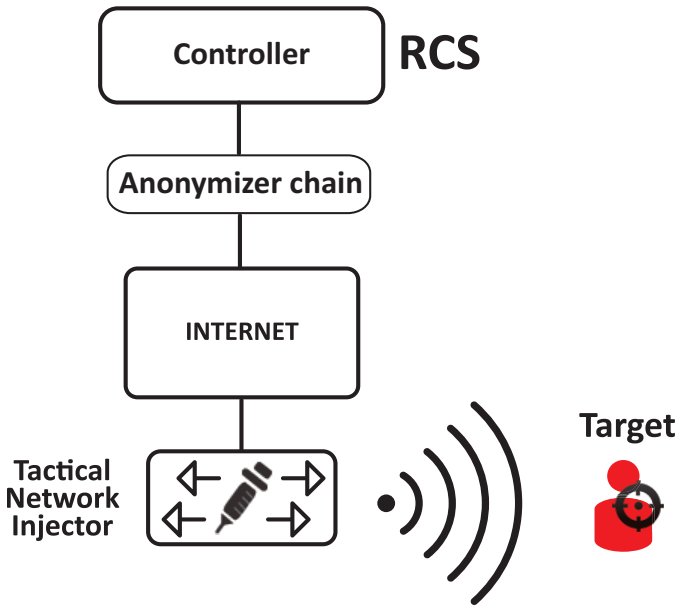


Figura 2: Tactical Network Injector: esquema de emulación de punto de acceso

Instalación de Tactical Network Injector

Introducción

Tactical Network Injector se entrega con el sistema operativo Tactical Device y el software de control Tactical Control Center, instalados previamente y configurados. Debe sincronizarse con RCS Server.

IMPORTANTE: la instalación requiere los archivos de autentificación de Master Node y para la sincronización se necesita la creación del Network Injector en RCS Console. Prepárese para las instalaciones lejos del centro operativo.

Contenido del paquete

El paquete incluye una computadora portátil y un CD de instalación.

Secuencia de instalación

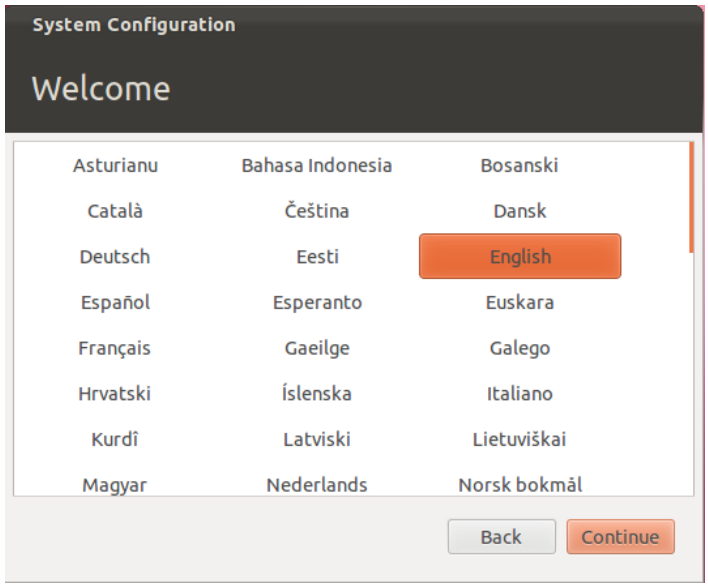
A continuación se puede ver la secuencia de instalación completa:

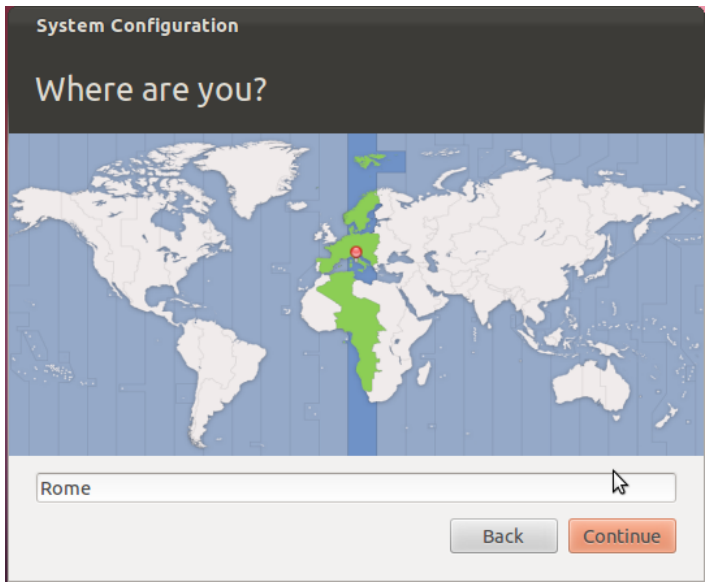
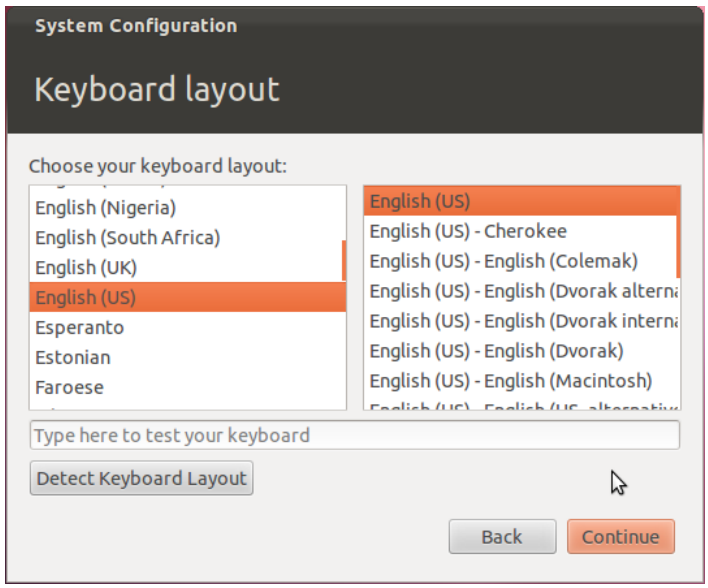
Paso	*Acción*	*Párrafo*
1	Instale el sistema operativo Tactical Device NOTA: al momento de la compra el sistema operativo ya está instalado.	*"Instalación y configuración del sistema operativo" abajo*
2	Sincronización de Network Injector con RCS Server	*"Primera sincronización de Network Injector con RCS Server" en la página 57*
3	Verifique el estado del Network Injector	*"Verifique el estado del Network Injector" en la página 58*

Instalación y configuración del sistema operativo

Tactical Network Injector se proporciona instalado y listo para usar, completo con todas las aplicaciones previstas. También se puede instalar usando un disco de restauración.

A continuación se describe el procedimiento:

Pasos	*Resultado*
1. Conecte la computadora a la red con un cable Ethernet e inserte el CD de instalación.	-
2. Seleccione Tactical Device para la instalación de la versión para computadora portátil: se inicia la instalación del sistema operativo y la computadora se apaga al finalizar. **IMPORTANTE: la computadora debe permanecer conectada a Internet durante todo el proceso de instalación.**	-
3. Reinicie su computadora portátil; ingrese la *contraseña* para desbloquear el disco codificado. La contraseña para el primer arranque es "firstboot".	-
4. Aparece la primera ventana de instalación. 5. Seleccione el idioma.	

Pasos	***Resultado***
6. Seleccione la zona horaria correcta.	
7. Se lee el esquema del teclado. Solo cámbielo si es necesario.	

Pasos	*Resultado*
8. Ingrese los datos del usuario: inicia la instalación del sistema operativo. **ADVERTENCIA: si pierde su contraseña deberá volver a instalar el Tactical Network Injector.** **IMPORTANTE: la contraseña ingresada se convierte en la nueva contraseña del disco codificado que se pedirá cada vez que se encienda la computadora portátil. La contraseña también se solicita cuando el usuario inicia sesión.**	
9. Al terminar de instalar el sistema operativo aparece la página de inicio de sesión normal. Se instala el sistema operativo y el software de control Tactical Control Center en la computadora.	-

Verificación de la dirección IP

Para verificar las direcciones IP del Network Injector, abra RCS Console, la sección **Monitor**: la dirección IP se indica en la columna **Address** del Network Injector mostrado.

Cambio de la dirección IP

Si la dirección IP del Network Injector cambia, se mostrará un nuevo elemento en la sección **Monitor** de RCS Console. Se incluirán dos elementos para ese Network Injector: uno con la nueva dirección, en verde (componente en funcionamiento), y el otro con la dirección anterior, en rojo. Elimina el elemento con la dirección anterior.

Uninstall

Para desinstalar Tactical Control Center, simplemente elimínelo de la computadora. Para desinstalar un Tactical Network Injector, simplemente elimine el objeto en RCS Console y apague el dispositivo.

*Consulte "**Administración de los Network Injector**" en la página 112*

Otras aplicaciones instaladas en Network Injectors

Introducción

Los Network Injectors vienen instalados con algunas aplicaciones útiles de terceros.

Aplicaciones

A continuación se encuentran las aplicaciones instaladas en Tactical Network Injector y Network Injector Appliance:

NOTA: para ver las instrucciones de las aplicaciones, consulte los documentos entregados por los fabricantes de las aplicaciones.

Nombre de la aplicación	*Descripción*
Disniff	Paquete de herramientas que permite interceptar el tráfico de la red
hping3	Generador de tráfico en la red
Kismet	Herramienta de monitoreo para las redes Wireless 802.11b
Macchanger	Herramienta para cambiar la dirección MAC de la interfaz de red
Nbtscan	Detector de red que permite encontrar la información de los nombres NetBIOS
Netdiscover	Escáner de dirección de red activa/pasiva por medio de consultas ARP
Ngrep	grep de tráfico de red
Nmap	Mapeador de red
P0f	Herramienta Passive OS fingerprinting
SsIsniff	Herramienta de ataque Man-in-the-middle para tráfico de red SSL/TLS
SsIstrip	Herramienta de ataque Man-in-the-middle y hijacking para tráfico de red SSL/TLS
Tcpdump	Analizador de tráfico de red desde el intérprete de comandos
Wireshark	Analizador del tráfico de red
Xprobe	Herramienta de identificador de OS remoto

Comandos de Tactical Control Center y Appliance Control Center

Introducción

Existen algunos comandos de terminal disponibles para administrar las aplicaciones de Tactical Control Center y Appliance Control Center.

NOTA: Para ejecutar estos comandos se requieren privilegios de administrador.

Comandos

A continuación se describen los comandos disponibles para Tactical Control Center y Appliance Control Center:

Comandos de Tactical Control Center	***Comandos de Appliance Control Center***	***Función***
`tactical`	`appliance`	Inicia la aplicación.
`tactical -d` o bien `tactical --desync`	`appliance -d` o bien `appliance --desync`	Desconecta el sistema de RCS Server actualmente sincronizado.
`tactical -l` o bien `tactical --log`	`appliance -l` o bien `appliance --log`	Muestra los registros de los procesos de infección actuales. NOTA: la ventana de la aplicación debe estar abierta.
`tactical -s` o bien `tactical --show-logs`	`appliance -s` o bien `appliance --show-logs`	Muestra todos los archivos de registro guardados en el sistema de archivos.
`tactical - r` o `tactical --report`	`appliance - r` o `appliance --report`	Crea un informe del sistema y lo guarda en la carpeta Home del usuario.
`tactical - v` o bien `Tactical --version`	`appliance - v` o bien `appliance --version`	Muestra la versión de la aplicación.
`tactical -h` o bien `tactical --help`	`appliance -h` o bien `appliance --help`	Muestra los comandos disponible.

Primera sincronización de Network Injector con RCS Server

Introducción

La primera sincronización de Network Injector es necesaria para permitir las comunicaciones entre Network Injector y el RCS Server y para crear y enviar reglas de análisis de paquetes e infecciones. Una vez que se instale y sincronice, Network Injector consultará el servidor cada 30 segundos.

Sincronización de Network Injector con RCS Server

Para completar la instalación de Network Injector, se debe instalar la clave de autentificación y se debe sincronizar Network Injector con el RCS Server.

NOTA: la instalación de la clave de autentificación solo es necesaria durante la primera sincronización.

A continuación se muestra el procedimiento para Network Injector Appliance y Tactical Network Injector:

Paso	*Acción*
1	Desde **RCS Console,** en la sección **System**, **Network Injector**, haga clic en **Nuevo Anonymizer**.
2	Ingrese los datos indicados y haga clic en **Guardar.** *Consulte "**Datos del Network Injector**" en la página 115* **Resultado**: el Network Injector se muestra en la lista y el nuevo objeto a monitorear se agrega a la sección Monitor.
3	Seleccione el Network Injector recién creado y haga clic en **Export Key** **Resultado**: se generará un archivo .zip con la clave de autentificación.
4	Guarde el archivo .zip generado.
5	Desde Appliance Control Center o Tactical Control Center, en la sección **System Management** y luego **Server Management**, ingrese la dirección IP y el puerto de comunicación del Anonymizer. NOTA: el puerto de comunicación predeterminado es 80.
6	Haga clic en **Import key** y seleccione el archivo .zip generado por RCS Console que guardó anteriormente.

Paso	*Acción*
7	Haga clic en **Configurar**. **Resultado**: Network Injector comienza a comunicarse con el Anonymizer.
8	Consulte el estado del Network Injector en la sección **Monitor** de RCS Console. *Consulte "**Verifique el estado del Network Injector**" abajo*

Verifique el estado del Network Injector

Introducción

Network Injector se sincroniza con RCS Server para descargar las versiones actualizadas del software de control, así como las reglas de identificación y de inyección, para enviarlas a los registros.

Es posible monitorear el estado de Network Injector desde RCS Console.

Específicamente:

- en la sección **Monitor**: para identificar cuándo Network Injector se sincroniza y cuándo solicita transferencias de datos.
- en la sección **System**, **Network Injector**: para ver los registros enviados por Network Injector.

Identificar cuándo se sincroniza Network Injector

A continuación se describe el procedimiento:

Paso	*Acción*
1	En la sección **Monitor**, seleccione la fila correspondiente al objeto Network Injector que desea analizar. Verifique la columna **Estado**: si está marcada en verde, el Network Injector está sincronizado. Esta situación ocurre cuando en el software Control Center (Appliance o Tactical): • se hizo clic en **Config.**, el operador colocó nuevas reglas o actualizaciones de forma manual; • se hizo clic en **Start** o hay una infección en curso.  **IMPORTANTE: RCS solo puede enviar las reglas y actualizaciones aplicadas cuando Network Injector está sincronizado.**

Ver los registros de Network Injector

A continuación se describe el procedimiento:

Paso	Acción
1	En la sección **System**, **Network Injectors**, seleccione el Network Injector que desea analizar, haga doble clic o un solo clic en **Editar** **Resultado**: se abrirá una ventana con los datos de Network Injector y los registros guardados. *Consulte "**Datos del Network Injector**" en la página 115* NOTA: solo se recibirán y se mostrarán los registros si Network Injector está sincronizado.

Instalación de componentes adicionales

Introducción

Es posible agregar bases de datos Shard (para grandes volúmenes de datos) y Collectors adicionales (uno por cada cadena de Anonymizer).

Llamada al servicio: el diseño de la arquitectura distribuida debe consultarse con el servicio técnico de HackingTeam.

Requisitos de instalación de los componentes adicionales

Antes de instalar componentes adicionales, complete la instalación del Master Node y el Collector.

*Consulte "**Instalación de RCS Server**" en la página 21*

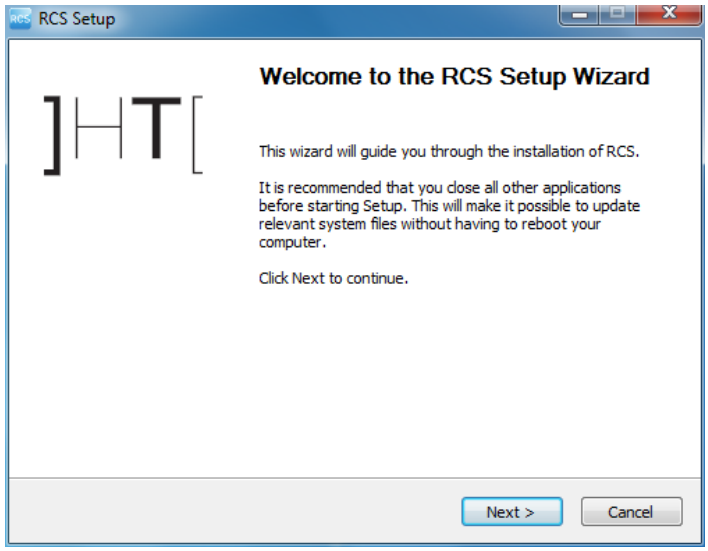
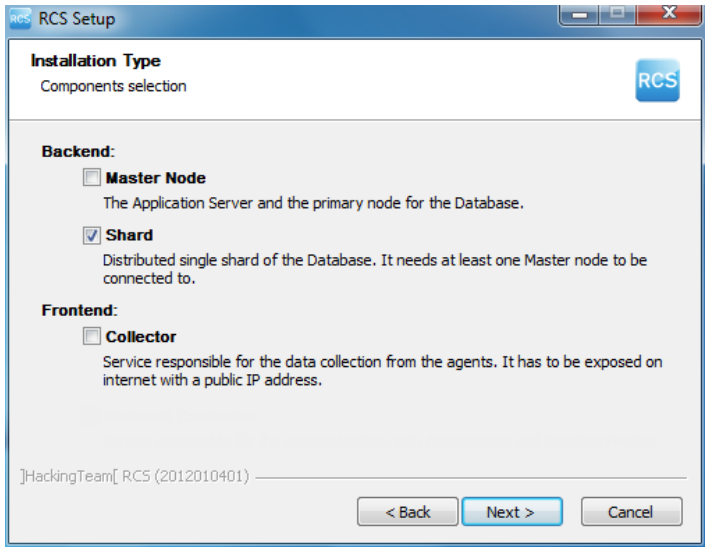
Secuencia de instalación

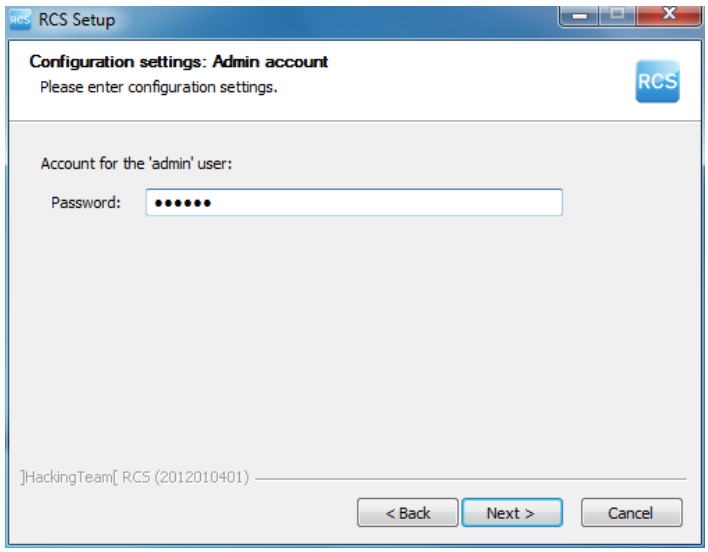
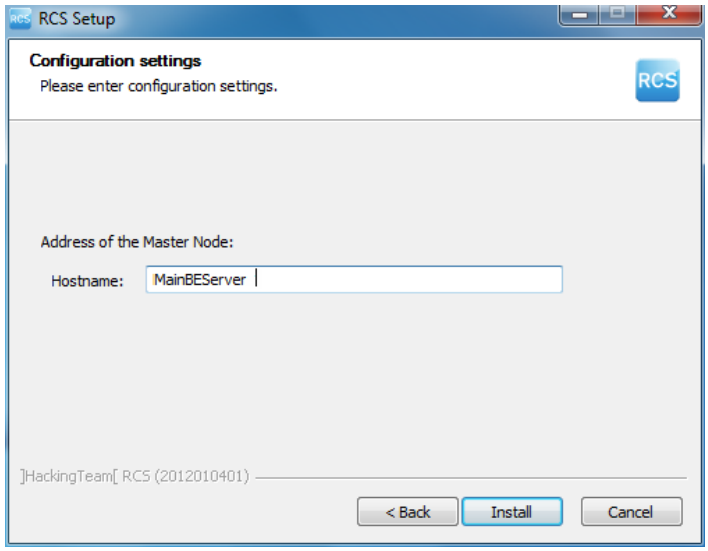
A continuación se describe la secuencia completa de instalación de los componentes adicionales:

Paso	Acción	Máquina
1	Prepare lo que se indica en *requisitos de instalación.*	-
2	Instale las bases de datos shard adicionales.	*servidor en un entorno de back end*
3	Revise los registros de instalación.	
4	Instale los Collectors adicionales.	*servidor en un entorno de front end*
5	Revise los registros de instalación.	
6	Revise los objetos instalados en las secciones **System**, **Backend** y **Frontend**.	*RCS Console*

Instalación de bases de datos shard adicionales

Para instalar una base de datos shard adicional en un entorno de back end:

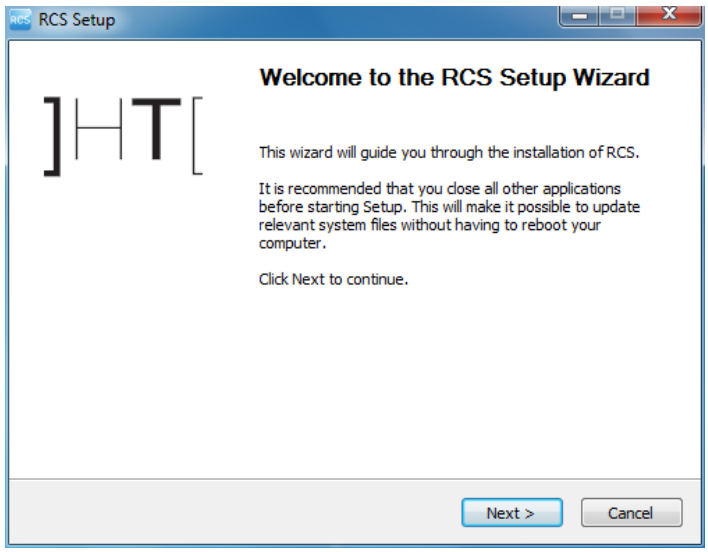
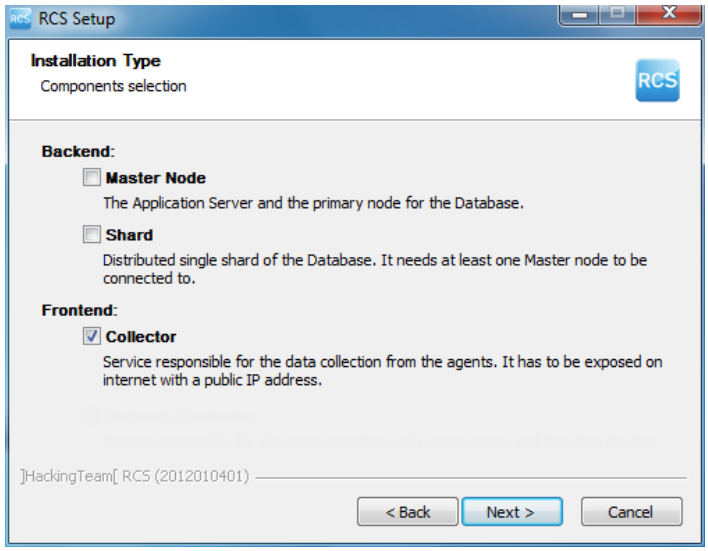
Pasos	*Resultado*
1. Inserte el CD con el paquete de instalación. Ejecute el archivo RCS-version.exe que se encuentra en la carpeta x:\setup, aparecerá la primera ventana del asistente. 2. Haga clic en **Siguiente**.	
3. Seleccione **Shard.** 4. Haga clic en **Siguiente**.	

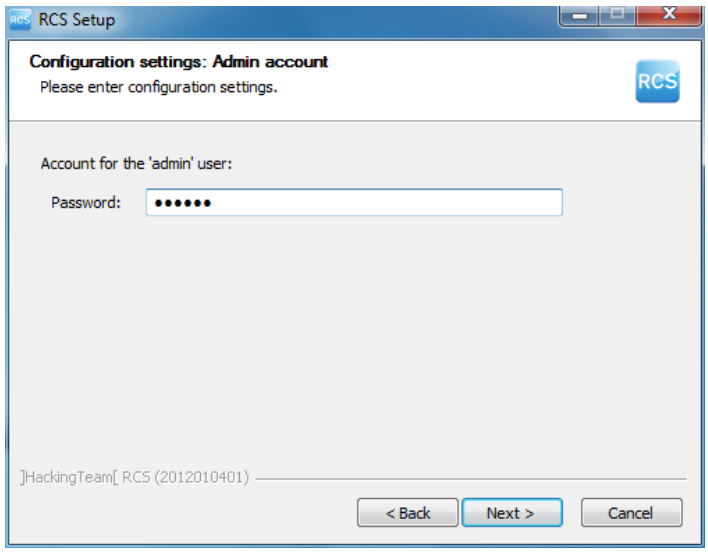
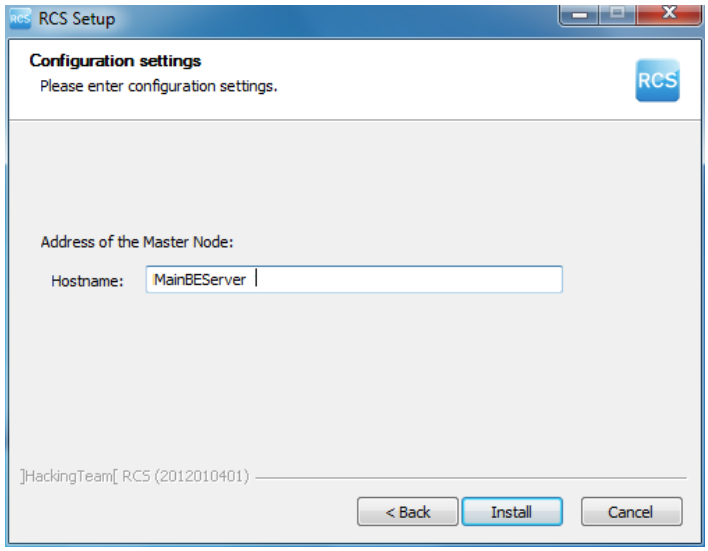
Pasos	*Resultado*
5. Ingrese la contraseña del administrador del sistema. 6. Haga clic en **Siguiente**: cuando la instalación finalice, los servicios estarán en funcionamiento y listos para recibir datos y comunicarse con RCS Console.	
7. Ingrese el nombre o la dirección IP del Master Node (p. ej.: **RCSMasterNode**). 8. Haga clic en **Instalar**: cuando la instalación finalice, se iniciarán los servicios e intentarán comunicarse con el Master Node. El servidor del entorno de back end está protegido y cualquier inicio de sesión remoto será redireccionado	

NOTA: en caso de que desee cambiar el nombre o la dirección IP del servidor después de la instalación debido a alguna falla, *consulte "**Edición de la configuración del Master Node**" en la página 76* .

Instalación de un Collector adicional

Para instalar varios Collectors en un entorno de front end:

Pasos	*Resultado*
1. Inserte el CD con el paquete de instalación. Ejecute el archivo RCS-version.exe que se encuentra en la carpeta x:\setup, aparecerá la primera ventana del asistente. 2. Haga clic en **Siguiente**.	
3. Seleccione **Collector.** NOTA: todos los servicios del Collector se instalarán automáticamente. 4. Haga clic en **Siguiente**.	

Pasos	*Resultado*
5. Ingrese la contraseña del administrador del sistema indicada en la instalación del Master Node. 6. Haga clic en **Continuar**: se inicia la instalación.	
7. Ingrese el nombre o la dirección IP del Master Node (p. ej.: **RCSMasterNode**). 8. Haga clic en **Instalar**: cuando la instalación finalice, se iniciarán los servicios e intentarán comunicarse con el Master Node. El servidor del entorno de back end está protegido y cualquier inicio de sesión remoto será redireccionado	

Verificar que los servicios se inicien

Asegúrese de que todos los servicios de RCS estén funcionando. Si los servicios no se están ejecutando, inícielos manualmente.

IMPORTANTE: el Collector solo acepta conexiones si el firewall de Windows se está ejecutando.

Consulte "Lista de servicios de RCS" en la página 27

Verificación de los registros de instalación

Si ocurre un error durante la instalación, verifique los registros y si es necesario envíelos al servicio técnico.

*Consulte "**Registros del sistema**" en la página 81*

Verificación de las direcciones IP

Para verificar todas las direcciones, inicie RCS Console, sección **System**, **Frontend**: las direcciones de los Collectors aparecerán en pantalla. *Consulte "**Instalación y configuración de Anonymizer**" en la página 38*

Uninstall

RCS se puede desinstalar desde el Dashboard de Windows

PRECAUCIÓN: los datos se perderán al desinstalar una base de datos shard. Para un funcionamiento correcto, procure realizar una copia de seguridad. Consulte "Administración de copias de seguridad" en la página 107 .

NOTA: los datos no se perderán al desinstalar un Collector.

6

Mantenimiento de rutina y actualizaciones del software

Presentación

Introducción

El mantenimiento de rutina incluye actualizaciones de RCS y las operaciones programadas o indicadas por el servicio de soporte técnico para mantener un buen rendimiento del sistema.

ADVERTENCIA: la falta de mantenimiento puede ocasionar un comportamiento impredecible del sistema.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca del mantenimiento de RCS

Recepción de actualizaciones

El servicio de soporte técnico publica en el portal de soporte técnico el paquete de actualización para cada versión de software RCS. El paquete puede asociarse con un nuevo archivo de licencia, el cual puede ser necesario durante el procedimiento de actualización.

Descargue el paquete y complete el procedimiento de actualización.

Comportamiento de la máquina durante la actualización

Durante las actualizaciones, no se garantiza que los servicios normales del sistema funcionen.

Todos los datos recibidos normalmente y administrados por la máquina que se está actualizando se mantienen durante el período necesario y se recuperarán automáticamente tan pronto como el sistema reanude a su funcionamiento normal.

Procedimientos de mantenimiento de rutina

Introducción

A continuación se detallan los procedimientos recomendados para mantener un alto rendimiento del sistema.

ADVERTENCIA: la falta de mantenimiento puede ocasionar un comportamiento impredecible del sistema.

Revisión y eliminación de archivos de registro

Propósito: verificar la cantidad de archivos de registro y eliminar los más antiguos para evitar ocupar demasiado espacio en el disco duro.

Frecuencia sugerida: depende de la cantidad de agents que se están monitoreando. Es posible que una vez al mes sea suficiente para verificar el espacio ocupado de los discos.

Verificación de espacio disponible en el disco de respaldo

Propósito: verificar regularmente el disco de respaldo en base a la cantidad y a la frecuencia de copias de seguridad en la **sección RCS ConsoleSystem.**

Frecuencia recomendada: depende de la frecuencia de las copias de seguridad y del tamaño.

Actualizaciones del sistema operativo Linux

Propósito: mantener siempre actualizado el sistema operativo Linux instalado en el VPS que hospeda a los Anonymizers y a los Network Injectors.

Actualización de RCS Server

Requisitos de actualización

Como medida de precaución, siga los pasos a continuación antes de actualizar RCS Server:

Paso	*Acción*
1	Detenga todos los servicios de RCS. *Consulte "**Lista de servicios de RCS**" en la página 27* .
2	Cree una copia completa del contenido de la carpeta, C:\RCS\ Master Node y cualquier shard adicional.
3	Una vez que lo copie, reinicie los servicios de RCS.

Formas de actualización

Una vez que se inicia el instalador, identifica los componentes de la máquina y sugiere una actualización automática.

Actualización de los RCS Server

IMPORTANTE: la llave de hardware siempre debe estar insertada en el servidor.

Para actualizar RCS, repita los siguientes pasos para cada servidor:

Paso	*Acción*
1	Ejecute el archivo de instalación `rcs-Versión.exe`: se mostrará la lista de los componentes instalados que se actualizarán automáticamente. Haga clic en **Siguiente**.
2	Seleccione el nuevo archivo de licencia del paquete de instalación. Haga clic en **Siguiente**.

Actualización de RCS Console

Requisitos de actualización

En RCS Console no se guarda ningún dato. El software se puede actualizar sin ninguna precaución especial.

Actualización de RCS Console

En caso de ser necesario, el servidor actualiza automáticamente la consola después de cada acceso.

De forma alternativa, repita el procedimiento de instalación usando los archivos del nuevo paquete de instalación.

*Consulte "**Instalación de RCS Console**" en la página 28*

Actualización del Anonymizer

Requisitos de actualización

En los Anonymizers no se guarda ningún dato. El software se puede actualizar sin ninguna precaución especial.

Actualización del Anonymizer

Desde **RCS Console**, en la sección **System, Frontend**, seleccione el Anonymizer que desea actualizar y haga clic en **Actualizar**.

IMPORTANTE: mantenga actualizado el sistema operativo Linux

Si no es posible actualizarlo, repita el procedimiento de instalación usando los archivos que se encuentran en el nuevo paquete de instalación.

*Consulte "**Instalación y configuración de Anonymizer**" en la página 38*

Actualización del Network Injector Appliance

Introducción

Existen tres maneras de actualizar el Network Injector Appliance:

- completamente, incluido el sistema operativo, *consulte "**Actualización completa del Network Injector Appliance**" abajo* .
- parcialmente, guarda datos, con una infección en curso *consulte "**Actualización parcial con infección en curso**" en la página opuesta* .
- parcialmente, guarda datos, sin infección en curso *consulte "**Actualización parcial con infección en curso**" en la página 70* .

Actualización completa del Network Injector Appliance

PRECAUCIÓN: la actualización elimina todos los datos en la máquina.

Si tiene el archivo .iso actualizado, siga este procedimiento para instalar la actualización del sistema operativo:

Paso	*Acción*
1	Inserte el CD con la nueva versión del sistema operativo y arranque desde el CD: el contenido del disco será eliminado y se reinstalarán los archivos del sistema operativo y del Network Injector. Este procedimiento se tarda 20 minutos.  **IMPORTANTE: seleccione Network Appliance para la instalación de la versión para servidor.**
2	Reinicie el servidor: se debe confirmar el procedimiento.  ***PRECAUCIÓN: se eliminará todo el contenido del disco duro.*** **Resultado**: Network Injector Appliance está instalado.

Actualización parcial con infección en curso

Estas son las fases durante una actualización del software de Appliance Control Center, cuando hay una infección en curso:

 **IMPORTANTE: para actualizar, primero sincronice el Network Injector y el RCS Server.** ***Consulte "Primera sincronización de Network Injector con RCS Server" en la página 57***

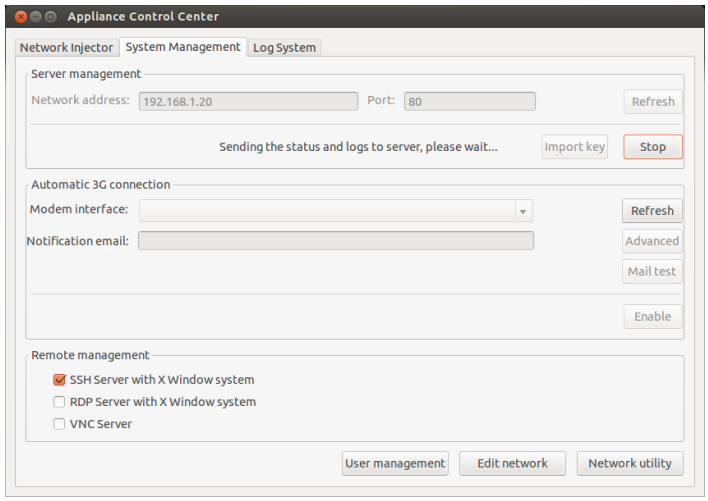
 **IMPORTANTE: asegúrese de que el dispositivo a actualizar esté conectado a Internet para descargar los paquetes adicionales necesarios para la actualización.**

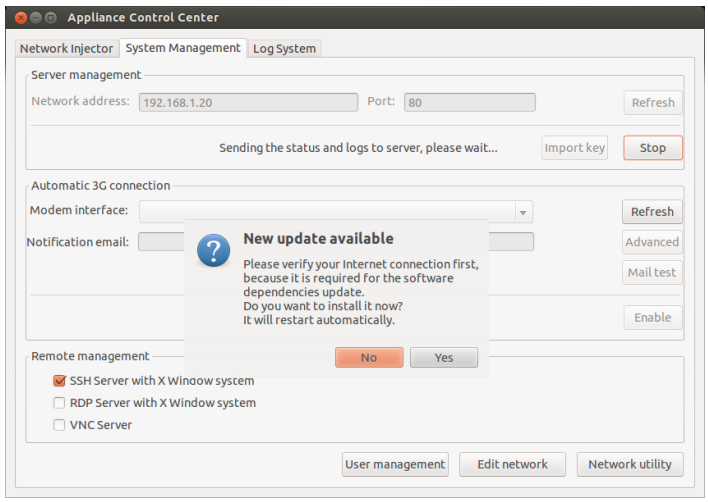
Fase	*Descripción*
1	Desde **RCS Console**, en la sección **System**, **Network Injector**, seleccione el Network Injector que desea actualizar y haga clic en **Update**
2	En la siguiente solicitud de comunicación del Network Injector, el Anonymizer asignado enviará la actualización que se instalará automáticamente.  NOTA: el tiempo de espera para la comunicación del Network Injector será de un minuto como máximo. Puede revisar el progreso de la operation en el área de descarga de RCS Console.  NOTA: la fase de instalación solo comienza si la ventana de la aplicación Appliance Control Center está cerrada. Cuando la actualización finaliza, se reinicia la infección con el software de actualización.

Actualización parcial con infección en curso

Estas son las fases en un software Appliance Control Center durante una actualización, cuando no hay una infección en curso:

IMPORTANTE: asegúrese de que el dispositivo a actualizar esté conectado a Internet para descargar los paquetes adicionales necesarios para la actualización.

Paso	*Acción*
1. Desde RCS Console, en la sección **System**, **Network Injector**, seleccione el Network Injector que desea actualizar y haga clic en **Actualizar**	
2. Consulte "**Appliance Control Center**"	-
3. En la pestaña **System Management**, haga clic en **Configure**: la sincronización está activada.	

Paso	*Acción*
4. Durante la sincronización, Network Injector consulta RCS cada 30 segundos. Aparece un mensaje al final del primer intervalo, solicitando consentimiento para instalar. NOTA: si no se instala la actualización, se instalará automáticamente en el siguiente inicio de la infección o se mostrará una solicitud de autorización en el siguiente reinicio del Appliance Control Center.	
5. Instale la actualización.	
6. Cuando la actualización finalice, el Appliance Control Center se reiniciará.	-

Actualización de Tactical Network Injector

Introducción

Existen dos formas de actualizar Tactical Network Injector:

- completamente, incluido el sistema operativo, *consulte "**Actualización full del Tactical Network Injector**" abajo* .
- parcialmente *consulte "**Actualización parcial**" en la página siguiente* .

Actualización full del Tactical Network Injector

PRECAUCIÓN: la actualización elimina todos los datos en la máquina.

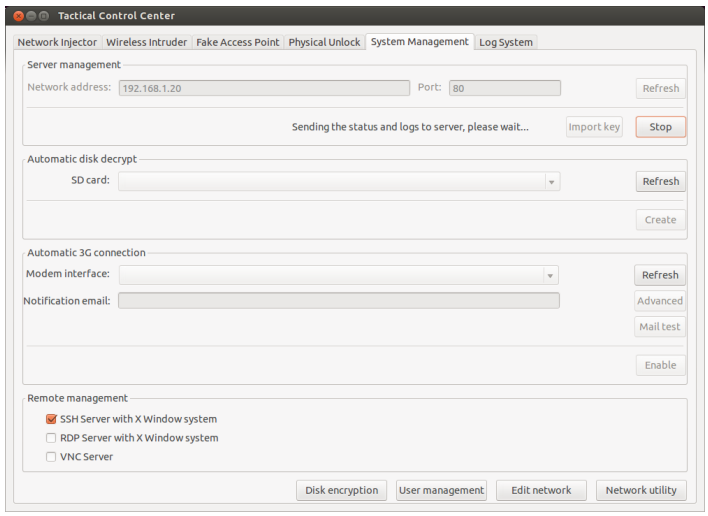
Si tiene el archivo .iso actualizado, siga este procedimiento para instalar la actualización del sistema operativo:

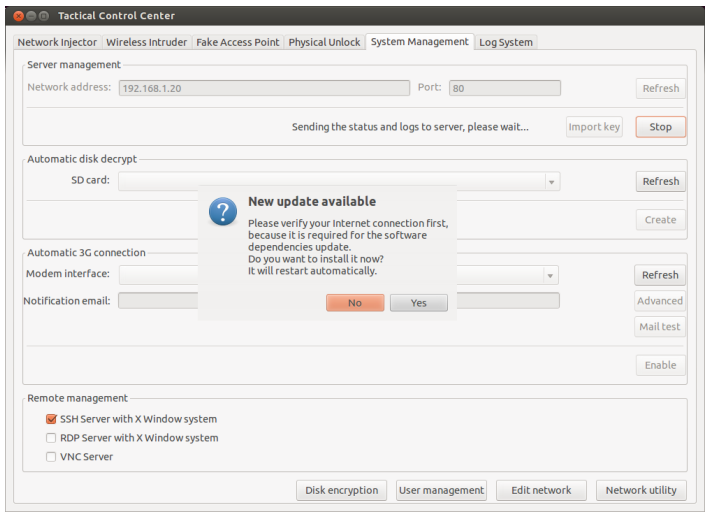
Paso	*Acción*
1	Inserte el CD con la nueva versión del sistema operativo y arranque desde el CD: el contenido del disco será eliminado y se reinstalarán los archivos del sistema operativo y del Network Injector. Este procedimiento se tarda 20 minutos. **IMPORTANTE: seleccione la instalación de Tactical Device para la versión de computadora portátil.**
2	Reinicie el servidor: se debe confirmar el procedimiento. ***PRECAUCIÓN: se eliminará todo el contenido del disco duro.*** **Resultado**: Network Injector Appliance está instalado.

Actualización parcial

Estas son las fases de actualización de Tactical Control Center:

IMPORTANTE: asegúrese de que el dispositivo a actualizar esté conectado a Internet para descargar los paquetes adicionales necesarios para la actualización.

Paso	*Acción*
1. Desde **RCS Console**, en la sección **System**, **Network Injector**, seleccione el Network Injector que desea actualizar y haga clic en **Update**	
2. Abra **Tactical Control Center**	-
3. En la pestaña **Network Injector**, haga clic en **Config.**: la sincronización está activada.	

Paso	*Acción*
4. Durante la sincronización, Network Injector consulta RCS cada 30 segundos. Aparece un mensaje al final del primer intervalo, solicitando consentimiento para instalar. NOTA: si la actualización no está instalada, aparecerá una solicitud de autorización de instalación la próxima vez que se inicie el Tactical Control Center.	
5. Instale la actualización.	
6. Cuando la actualización finalice, el Tactical Control Center se reiniciará.	-

7

Edición de la configuración del Master Node y del Collector

Presentación

Introducción

Es posible hacer cambios en la configuración de los componentes después de la instalación en caso de ser necesario.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de la configuración

Qué puede editar

Es posible editar los siguientes datos de instalación del Master Node y del Collector:

- el nombre/dirección IP del Master Node
- la contraseña del administrador del sistema
- la carpeta de archivos de respaldo
- el servidor de correos de salida para enviar correos electrónicos de alert

Cuándo hacer cambios en la configuración

Puede que se necesite cambiar el nombre/dirección IP o la contraseña cuando se reemplacen los servidores, o debido al ingreso de datos incorrectos durante la instalación.

IMPORTANTE: es muy recomendable especificar una carpeta de archivos de respaldo en otro lugar, por ejemplo, en un dispositivo remoto, para proteger los datos de la copia de seguridad.

Orden a seguir para cambiar la configuración

Debido a que el servidor donde está instalado el Master Node es el sistema "maestro", para cambiar la instalación se debe seguir este orden:

1. Cambiar el nombre/dirección IP o contraseña del Master Node
2. Informar al Collector el nuevo nombre/dirección IP o contraseña

Enviar por correo la configuración del servidor

El sistema RCS se pude configurar para enviar un correo electrónico cuando se reciben las primeras piezas de evidence de un target. Las direcciones de correo electrónico deben tener privilegios de analista y pertenecer al grupo de alerting establecido para la operation.

Para hacer esto, es necesario establecer la configuración del remitente del servidor de correos de salida y, especialmente, el nivel de autentificación necesario.

*Consulte "**Herramientas de configuración**" abajo*

Herramientas de configuración

Herramientas de RCS

La configuración se realiza a través de algunas herramientas en el intérprete de comandos de Windows que se encuentra en la carpeta C:\RCS\DB\bin o C:\RCS\Collector\bin (en base al tipo de instalación).

Entre las herramientas de configuración de componentes se incluyen:

- para el Master Node: **rcs-db-config**
- para el Collector: **rcs-collector-config**

Sintaxis de los comandos de herramientas

La sintaxis de los comandos de herramientas es la siguiente:

```
> rcs-db-config -x AAA
> rcs-collector-config -x AAA
```

Donde:

- -x: opción seleccionada
- AAA: valor ingresado

Otras opciones

Para diagnósticos rápidos, el servicio técnico puede solicitar que se ejecuten otros comandos. Para una sintaxis correcta, ingrese:

```
> rcs-db-config --help
> rcs-collector-config --help
```

Llamada al servicio: use las otras opciones solo si así se lo indica el servicio técnico.

Sugerencia: la sintaxis "-x" es la versión corta de la sintaxis "--xxxxx": "`rcs-db-config -n`" es lo mismo que "`rcs-db-config --CN`"

Edición de la configuración del Master Node

En la carpeta C:\RCS\DB\bin o C:\RCS\Collector\bin (según el tipo de instalación) ingrese los siguientes comandos:

Para editar...	***Ingrese...***

el nombre/dirección IP del Master Node	`> rcs-db-config -n Nombre -g`
	o
	`> rcs-db-config -n DirecciónIP -g`
	Resultado: los certificados se actualizan y aparecen en la carpeta \RCS\DB\config\certs. También se deberá cambiar la configuración del Collector. *Consulte "**Edición de la configuración del Collector**" en la página siguiente*

la contraseña del sistema de usuarios	`> rcs-db-config -R Nombre de usuario` **Resultado**: se pedirá la nueva contraseña para guardarla en la base de datos. Esta operation renueva automáticamente la fecha de vencimiento de la contraseña.

Para editar...	*Ingrese...*
la carpeta de archivos de respaldo	`> rcs-db-config -B Carpeta`  NOTA: "*Carpeta*" puede ser la ruta de la carpeta `RCS\db` o una ruta absoluta.  **IMPORTANTE: cualquier archivo de respaldo en la carpeta establecida previamente se copiará en la nueva carpeta.** **Resultado**: todos los archivos subsecuentes de la copia de seguridad se guardan en la nueva carpeta.  Sugerencia: se puede instalar un dispositivo remoto en una carpeta NTFS mediante el **Administrador de discos** de Windows: de esta manera se puede usar un disco remoto para la copia de seguridad.

la configuración del servidor de correos de salida para correos electrónicos de alert	`> rcs-db-config -M -server NombreDelServidor:NúmeroDePuerto`
	para establecer el nombre y el puerto del servidor de correos de salida a utilizar.
	`> rcs-db-config -from RemitenteDelCorreo`
	para establecer el correo electrónico del remitente del correo de alert (p. ej.: "alert@myplace.com").
	`> rcs-db-config -user NombreDeUsuario`
	Para establecer el nombre de usuario del remitente del correo electrónico.
	`> rcs-db-config -pass Contraseña`
	Para establecer su contraseña.
	`> rcs-db-config -auth TipoDeAutentificación`
	Para establecer el tipo de autentificación a utilizar ("simple", "inicio de sesión" o "cram_md5").

Edición de la configuración del Collector

En la carpeta C:\RCS\DB\bin o C:\RCS\Collector\bin (según el tipo de instalación) ingrese los siguientes comandos:

A...	*Ingrese...*

comunicar el nuevo nombre o dirección IP del Master Node	`> rcs-collector-config -d` *`Nombre`* `-u admin -p` *`Contraseña`* `-t`
	o
	`> rcs-collector-config -d` *`DirecciónIP`* `-u admin -p` *`Contraseña`* `-t`
	  **IMPORTANTE: la "*Contraseña*" debe coincidir con la que se usa para iniciar sesión en el Master Node.**
	Resultado: los certificados se restauran en la carpeta \RCS\DB\config\certs.

Verificación de la configuración

Es posible verificar la configuración previa y actual mediante las herramientas de RCS.
Para verificar la configuración previa y actual, inicie las herramientas respectivas sin ninguna opción:

```
> rcs-db-config
> rcs-collector-config
```

Ejemplo de resultado de verificación de la configuración

A continuación se puede ver un ejemplo de verificación:

```
Configuración actual:
 {"CA_PEM"=>"rcs.pem",
 "DB_CERT"=>"rcs-db.crt",
 "DB_KEY"=>"rcs-db.key",
 "LISTENING_PORT"=>443,
 "HB_INTERVAL"=>30,
 "WORKER_PORT"=>5150,
 "CN"=>"172.20.20.157",
 "BACKUP_DIR"=>"backup",
 "PERF"=>true,
 "SMTP"=>"mail.abc.com:25",
 "SMTP_FROM"=>"alert@abc.com",
 "SHARD"=>"shard0000"}
```

8

Resolución de problemas

Presentación

Introducción

RCS es un sistema donde la mayor atención debe estar en transmitir, decodificar y guardar los datos recopilados. El diseño de RCS se centra en evitar la pérdida de datos y en el manejo rápido de los errores potenciales que pudieran ocurrir.

Contenido

En esta sección se incluyen los siguientes temas:

Fallas potenciales

Fallas potenciales de instalación

A continuación se listan las fallas potenciales que podrían llegar a ocurrir durante la instalación y las acciones recomendadas:

Si...	*Entonces...*
La instalación no avanza	asegúrese de que la llave de hardware esté insertada correctamente.
RCS Console no se puede conectar al servidor	• asegúrese de haber iniciado sesión con el nombre del administrador del sistema, su contraseña y el nombre del servidor donde se instaló el Master Node. o • revise el archivo de registro Master Node para ver si hay errores.

Posibles problemas en el servidor

A continuación se listan las fallas potenciales que podrían llegar a ocurrir durante el uso del producto y las acciones recomendadas:

Si...	*Y...*	*Entonces...*
no se puede conectar al Master Node	la llave de hardware está insertada correctamente, pero el servicio del Master Node no se inicia	• verifique el estado del servicio Master Node. • solicite una llave de protección de reemplazo.
ya no llegan datos del agents	desde la RCS Console, se ejecuta el Collector y se comunica correctamente	revise el estado del Collector.
el Master Node no está disponible	el Collector se está ejecutando	• verifique si hay alguna actualización en curso • verifique el archivo de registro del Collector
las imágenes no se convierten en texto	el módulo OCR está instalado	verifique qué tan lentamente el módulo registra e instala otro módulo OCR.
El Collector no está disponible	-	reinicie el servicio RCS Collector.

Si...	*Y...*	*Entonces...*
los datos están en la cola del Master Node	los datos más recientes no aparecen en RCS	verifique el estado de servicio del trabajador, para Master Node y otras Shards, y los servicios de los que depende.
el Network Controller indica que hay un error	-	inicie sesión en la máquina del Collector deseado y verifique el archivo de registro.

Problemas potenciales con las copias de seguridad

A continuación se listan las fallas potenciales que podrían llegar a ocurrir durante el respaldo y las acciones recomendadas:

Si...	*Entonces...*
el estado de copia de seguridad es **error**	verifique el espacio disponible en el disco y reinicie manualmente la copia de seguridad

Para obtener más información

Para revisar el estado de los componentes, *consulte "**Procedimiento de verificación del estado de los componentes**" en la página 83*

Para reiniciar los servicios, *Consulte "**Procedimiento de reinicio de los servicios**" en la página 85* .

Registros del sistema

Introducción

Cada componente de RCS genera registros diarios que permiten analizar las posibles causas de fallas o errores. El análisis de contenido de los archivos le permite seguir las operations de RCS paso a paso para encontrar las causas de los errores (p. ej.: el servicio se inició pero se detuvo inmediatamente después).

Herramienta de análisis de registros

A continuación se muestran los motivos que pueden llevar al análisis de los registros:

Componente	*Motivo del análisis*
Master Node	Verificar problemas con RCS Console.
Collector	Verificar la recepción de datos desde los agents.

Componente	*Motivo del análisis*
Carrier	Verificar el envío de datos a las a las bases de datos shard y al Master Node.
Módulo OCR	Verificar una respuesta lenta al indexar el contenido exportado.
Módulo Translate	Verificar una respuesta lenta en la traducción del contenido.
Network Controller	Verificar el estado del Network Injector o del Anonymizer.
Network Injector	Verificar las operations completadas.
Anonymizer	Verificar el flujo de datos entrantes de los agents.

Ejemplo de archivo de registro

El nombre del archivo de registro tiene la siguiente sintaxis: `componente aaaa-mm-dd.log` (p. ej.: `rcs-dbdb 2012-02-04.log`)

Archivos de registro de RCS

A continuación se muestran los archivos de registro generados por los componentes durante la instalación completa:

Componente	*Carpeta*
Master Node	C:\RCS\DB\log
Collector	C:\RCS\Collector\log
Carrier	C:\RCS\Collector\log
Módulo OCR	C:\RCS\DB\log
Módulo Translate	C:\RCS\DB\log
Network Controller	C:\RCS\Collector\log
Network Injector	/var/log/syslog
Anonymizer	/var/log

ADVERTENCIA: la falta de archivos de registro indica que no se completó la instalación.

Vista rápida del registro

Con la instalación de RCS se incluye BareTail, una aplicación que le permite ver el contenido de varios archivos de registro de forma inmediata.

Para ejecutar BareTail, ingrese:

```
> rcs-db-log
```

Contenido del archivo de registro

Cada registro está identificado por uno de los siguientes niveles de gravedad:

Nivel de gravedad	*Descripción*
Fatal	RCS no está funcionando y requiere reparación (p. ej.: no hay configuración, no hay certificados).
Error	Hay un error en un componente pero RCS puede garantizar la cobertura de los servicios principales (p. ej.: Master Node no funciona).
Debug	Solo se muestra si se activa por instrucciones del servicio de soporte técnico, aumenta y proporciona más detalles sobre los registros para resolver los problemas encontrados.
Info	Nota de información.

Procedimiento de verificación del estado de los componentes

Introducción

A continuación se muestran los procedimientos típicos para verificar el estado del hardware y el software.

Verificación de la licencia instalada

Verifique todas las licencias instaladas en RCS, incluyendo las actualizaciones.

Comando

En la carpeta C:\RCS\DB\bin, ingrese **rcs-db-license.**

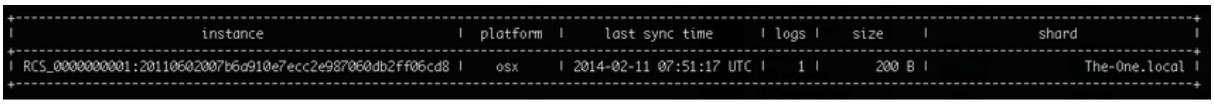
Verificación del estado del Master Node

Asegúrese de que el Master Node comunique regularmente los datos a las bases de datos a través de los servicios Worker.

Comando

En la carpeta C:\RCS\DB\bin, ingrese **rcs-db-queue.**

Resultado: a continuación se muestra un ejemplo.



instance	platform	last sync time	logs	size	shard
RCS_0000000001:20110602007b6a910e7ecc2e987060db2ff06cd8	osx	2014-02-11 07:51:17 UTC	1	200 B	The-One.local

Qué verificar

Si los valores *logs* y *size* empiezan a aumentar significativamente, es posible que sea porque el servicio Worker no está funcionando. Verifique el estado en cada servicio Worker.

Verificación del estado de los servicios Worker

Asegúrese de que el servicio Worker esté funcionando correctamente para decodificar y guardar datos en las bases de datos.

Comando

En la carpeta C:\RCS\DB\bin, ingrese **rcs-db-queue.**

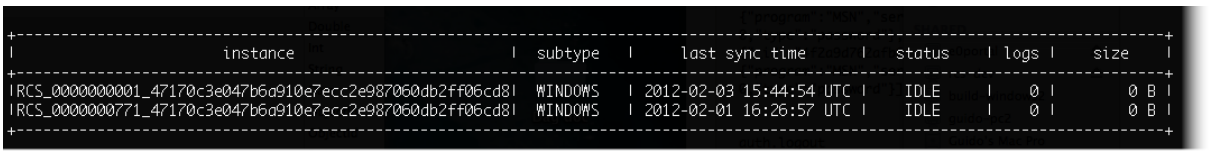
Verificación del estado del agent a través del Collector

Asegúrese de que los agents comunican regularmente su estado a RCS, y de que envían sus datos al Collector. Una falla persistente del Collector puede ocasionar la pérdida de datos en el agent.

Comando

En la carpeta C:\RCS\Collector\bin, ingrese **rcs-collector-queue**.

Resultado: se muestra el informe de estado del Collector



instance	subtype	last sync time	status	logs	size
RCS_0000000001_47170c3e047b6a910e7ecc2e987060db2ff06cd8	WINDOWS	2012-02-03 15:44:54 UTC	IDLE	0	0 B
RCS_0000000771_47170c3e047b6a910e7ecc2e987060db2ff06cd8	WINDOWS	2012-02-01 16:26:57 UTC	IDLE	0	0 B

Qué verificar

Last sync time debe ser lo más reciente posible, compatible con los métodos establecidos de sincronización para cada agent: un *Last sync time* reciente indica que el los agents se comunican correctamente con el Collector. Si *Last sync time* no es reciente, espere a que ocurran otras sincronizaciones para verificar si está actualizado. Como alternativa, puede verificar los registros del Collector para comprobar si hubo intentos de sincronización: en este caso se debe informar al servicio técnico.

El valor **logs** debe ser mínimo debido a que se trata de los datos guardados por el Collector en espera para ser enviados al Master Node a través del Carrier. Si el valor es alto, el Master Node no está funcionando, no está conectado o el Carrier no funciona correctamente. Verificación del estado del Master Node y los registros del Carrier.

Si el problema está en la conexión con el Master Node, la cantidad de registros se reducirá en el momento en que la conexión se restaure.

Verificación del inicio del Network Injector

Los registros de Network Injector normalmente se guardan en la carpeta /var/log/syslog.

Verificar los componentes del sistema

Verificar el estado del componente del sistema y ver la topología de los componentes front end y back end.

Comando

En la carpeta C:\RCS\DB\bin, ingrese **rcs-db-status**. Utilice el siguiente comando para ver la sintaxis correcta y la descripción de todas las opciones:

```
> rcs-db-status --help
```

Es posible crear archivos de servicios

Crea un archivo .zip file con toda la información que necesita el equipo de servicio técnico.

Comando

En la carpeta C:\RCS\DB\bin o C:\RCS\Collector\bin ingrese **rcs-db-diagnostic** o **rcs-collector-diagnostic**, respectivamente. Utilice el siguiente comando para ver la sintaxis correcta y la descripción de todas las opciones:

```
> rcs-db-diagnostic --help
> rcs-collector-diagnostic --help
```

Por ejemplo, la opción `--hide-addresses` le permite eliminar todas las referencias a las direcciones IP o nombres de dominio en los archivos.

Para obtener más información

Para ver los registros *consulte "Registros del sistema" en la página 81*

Procedimiento de reinicio de los servicios

Introducción

En caso de fallas, los servicios se pueden restaurar con esta herramienta en lugar de usar la función Administración de servicios de Windows.

IMPORTANTE: para reiniciar los servicios e identificar las causas de la falla, es necesario tener en cuenta las interdependencias de los servicios. ***Consulte "Lista de servicios de RCS" en la página 27 .***

A continuación se muestran las formas típicas de iniciar, detener y reiniciar los servicios.

Servicio	*Comandos*
RCSDB	• `> rcs-db-service start` • `> rcs-db-service stop` • `> rcs-db-service restart`
MongoDB	• `> rcs-db-mongo-service start` • `> rcs-db-mongo-service stop` • `> rcs-db-mongo-service restart`
Collector	• `> rcs-collector-service start` • `> rcs-collector-service stop` • `> rcs-collector-service restart`
Carrier	• `> rcs-carrier-service start` • `> rcs-carrier-service stop` • `> rcs-carrier-service restart`
Network Controller	• `> rcs-controller-service start` • `> rcs-controller-service stop` • `> rcs-controller-service restart`
Worker	• `> rcs-worker-service start` • `> rcs-worker-service stop` • `> rcs-worker-service restart`
Network Injector	 ***PRECAUCIÓN: use el protocolo SSH para todas las operations de instalación, configuración y transferencia de datos en la unidad remota.*** Para reiniciar el servicio con la misma configuración o con una nueva, abra el Appliance Control Center, si es necesario, reinicie y restablezca el servicio haciendo clic en **Reiniciar**.

Anonymizer	 ***PRECAUCIÓN: use el protocolo SSH para todas las operations de instalación, configuración y transferencia de datos en la unidad remota.***
	
	Para reiniciar el servicio, ingrese el siguiente comando:
	`# /etc/init.d/bbproxy restart`
	Para detener el servicio, ingrese el siguiente comando:
	`# /etc/init.d/bbproxy stop`
	
	  **IMPORTANTE: la sintaxis de los comandos hace referencia a la versión CentOS 6 del sistema operativo Linux.**

Procedimientos de reparación de los componentes de hardware

Introducción

A continuación se muestran los procedimientos típicos de los componentes de hardware que se usarán en caso de fallas de hardware.

Reemplazo de la llave de hardware

Si la llave de hardware principal deja de funcionar, debe reemplazarse inmediatamente con la llave de respaldo, incluida en el paquete que se entregó. Póngase en contacto con el servicio técnico para obtener un archivo de licencias compatible con la llave de respaldo.

A continuación se muestran las instrucciones para reemplazar y activar una nueva llave:

Fase	*Quién*	*Qué hace*
1	el cliente	*informa a HackingTeam sobre el error.*
2	HackingTeam	*envía un nuevo archivo de licencia asociado con la llave de hardware de respaldo.*
3	el cliente	*reemplaza la llave principal con la llave de respaldo e inicia el procedimiento para asignar el nuevo archivo de licencia.*
4	el cliente	*envía la llave defectuosa a HackingTeam.*
5	HackingTeam	*reemplaza la llave defectuosa con una nueva llave de respaldo y se la envía al cliente.*

Reemplazo del Master Node

A continuación se describe el procedimiento recomendado:

Paso	*Acción*
1	Restaurar un servidor, repitiendo todas las operations de instalación. *Consulte "**Instalación de RCS Server**" en la página 21*
2	Seleccione la copia de seguridad más reciente (full o metadatos). Si la copia de seguridad más reciente es de metadatos, posteriormente se puede restaurar la copia de seguridad full. De hecho, la copia de seguridad no es destructiva y complementa la información de la que dispone. *Consulte "**Qué debería saber acerca de las copias de seguridad**" en la página 104*

Reemplazo de una base de datos shard

A continuación se describe el procedimiento recomendado:

Paso	*Acción*
1	Repita el procedimiento de instalación completo. *Consulte "**Instalación de RCS Server**" en la página 21*
2	Restaure la última copia de seguridad full. *Consulte "**Administración de copias de seguridad**" en la página 107*

Reemplazo del Collector

Repita el procedimiento de instalación completo.
*Consulte "**Instalación de RCS Server**" en la página 21*

Reemplazo de un Anonymizer

Repita el procedimiento de instalación completo.
*Consulte "**Instalación y configuración de Anonymizer**" en la página 38*

Reemplazo de un Network Injector Appliance

Repita el procedimiento de instalación completo.
*Consulte "**Instalación de Network Injector Appliance**" en la página 43*

Reemplazo de un Tactical Injector Appliance

Repita el procedimiento de instalación completo.
*Consulte "**Instalación de Tactical Network Injector**" en la página 51*

9

RCS Console para el administrador del sistema

Presentación

El rol del administrador del sistema

El rol del *Administrador del sistema* es:

- completar la instalación con la configuración de los Anonymizers, los Network Injectors y las copias de seguridad
- verificar el espacio en la bases de datos shard
- controlar el funcionamiento de los Collectors, Anonymizers, Network Injectors y otros componentes del sistema, y solucionar los problemas que se presenten
- actualizar los componentes del sistema
- administrar las copias de seguridad

Funciones activadas

Para realizar sus actividades asignadas, el administrador del sistema tiene acceso a las siguientes funciones:

- **System**
- **Monitor**

Contenido

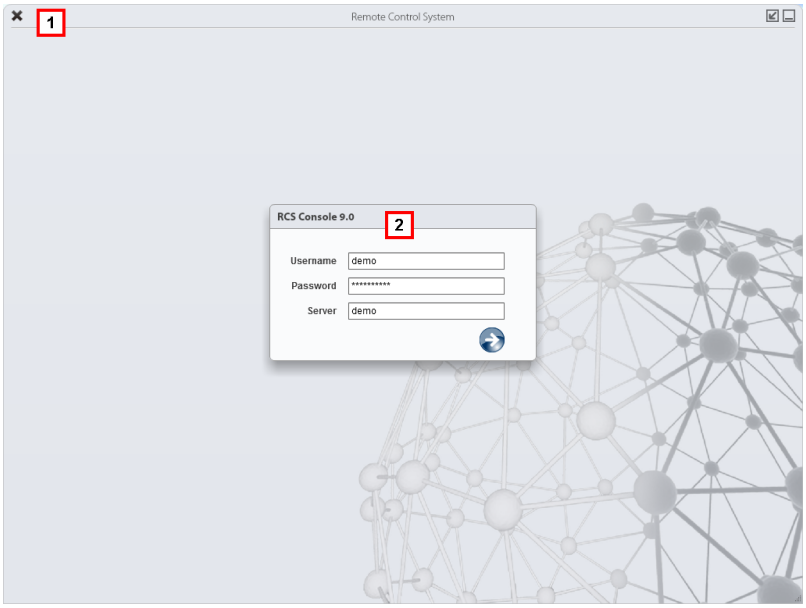
En esta sección se incluyen los siguientes temas:

Pantalla inicial de RCS Console

Cuando se abre RCS Console, se le pide que ingrese sus datos de inicio de sesión que estableció el administrador.

Cómo se ve la página de inicio de sesión

Así es como se ve la página de inicio de sesión:



Área	*Descripción*
1	Barra de título con botones de comando: Cierra RCS Console. Botón para ampliar la ventana. Botón para minimizar la ventana.
2	Ventana de diálogo para ingresar al sistema.

Acceso a RCS Console

Para acceder a las funciones de RCS Console:

Paso	*Acción*
1	En **Nombre de usuario** y **Contraseña,** ingrese sus datos de inicio de sesión asignados por el administrador.
2	En **Servidor,** ingrese el nombre del equipo o la dirección del servidor al que desea conectarse.
3	Haga clic en : aparecerá la página principal con los menús activados según los privilegios de su cuenta. *Consulte "**Descripción de la página principal**" abajo* .

Descripción de la página principal

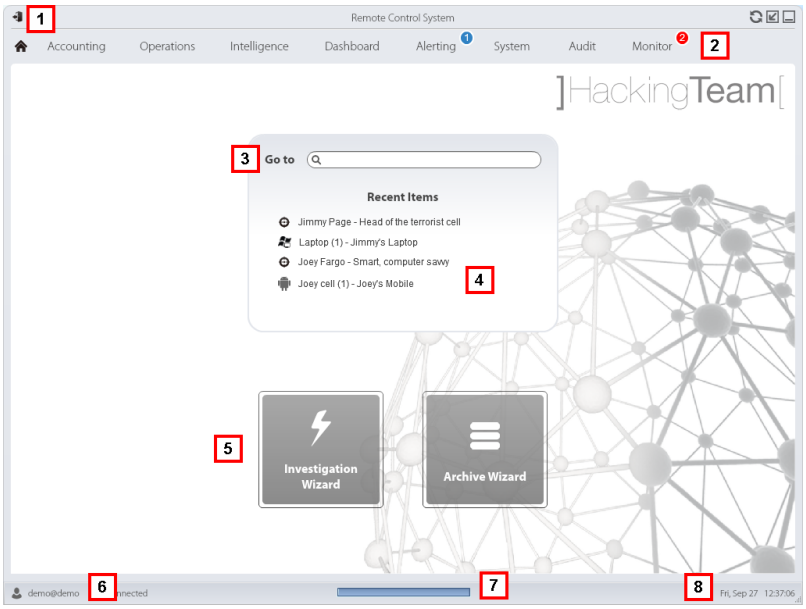
Para ver la página principal:	• haga clic en

Introducción

Al abrir RCS Console se mostrará la página principal. Todos los usuarios verán la misma página. Los menús se verán activos según los privilegios asignados a la cuenta.

Cómo se ve

Así es como se ve la página principal, con elementos guardados que se abrieron recientemente. Detalle de los elementos y las acciones comunes:



Área	*Descripción*
1	Barra de título con botones de comando.
2	Menú de RCS con las funciones activas para el usuario.
3	Cuadro de búsqueda para buscar operations, targets, agents y entidades, por nombre o descripción.
4	Enlaces a los cinco elementos abiertos (operation en la sección **Operations**, operation en la sección **Intelligence**, target, agent y entidad).
5	Botones del asistente.
6	Usuario conectado con opciones para cambiar el idioma y la contraseña.
7	Área de descarga con una barra de progreso durante la exportación o compilación.
8	Fecha y hora actuales con opciones para cambiar la zona horaria.

Asistentes en la página principal

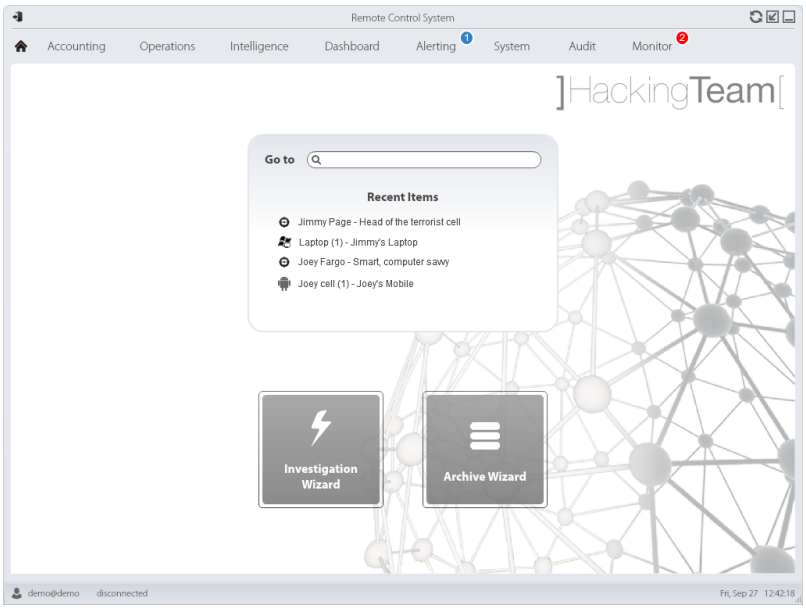
Para ver la página principal:	• haga clic en 

Introducción

Para los usuarios con ciertos privilegios, en RCS Console se muestran los botones que permiten abrir los asistentes.

Cómo se ve

Así es como se ve la página principal con los asistentes activados:



Botón	*Función*
	Abre el asistente para crear rápidamente un agent.  NOTA: el botón solo se activa para los usuarios con privilegios Administrador y Técnico.
	Abre el asistente para guardar rápidamente los datos de operation y target.  NOTA: el botón solo se activa para los usuarios con privilegios Administrador y Administrador del sistema.

Guardar rápido

Este asistente le permite administrar rápidamente los datos de la operation o target para guardarlos o eliminarlos de la base de datos.

Los datos se guardan en un respaldo y pueden restaurarse en cualquier momento.

A continuación se explican las diversas opciones:

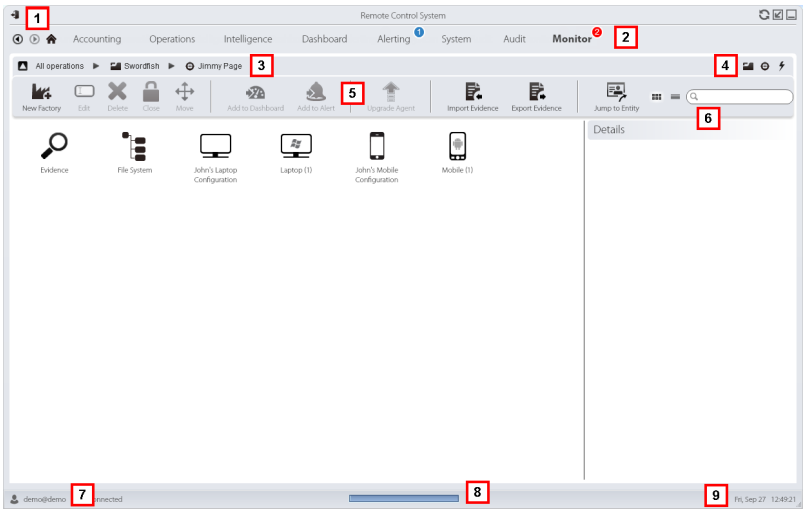
Opción	*Descripción*
Respaldar todos los datos	Guarda todos los datos de la operation o del target seleccionado en un archivo de respaldo de tipo completo. La copia de seguridad aparecerá en una lista de copias de seguridad y se podrá restaurar en cualquier momento.
Eliminar todos los datos del sistema	Elimina toda la evidence de la operation o el target seleccionado de la base de datos. La operation y el target permanecerán abiertos y en funcionamiento, solo se reducirá el tamaño de la base de datos. ***PRECAUCIÓN: si esta opción se combina con la copia de seguridad instantánea, use un nombre para la copia de seguridad que indique claramente que la evidence correspondiente fue eliminada del sistema.***
Cerrar el objeto	Cierra la operation o el target seleccionado. ***PRECAUCIÓN: la operation y el target se cerrarán y no se podrán volver a abrir. Los agents ya no enviarán más datos, pero todavía podrá consultar la evidence que ya se recibió.***
Eliminar el objeto del sistema	Elimina los datos de la operation o el target seleccionado. Se eliminan todos los datos de la operation, los targets, los agents y toda la evidence de la base de datos. ***PRECAUCIÓN: la eliminación de una operation o target es irreversible, por lo que se perderán todos los datos vinculados con dicha operation o target.***

Elementos y acciones comunes de la interfaz

Cada página del programa usa elementos comunes y permite realizar acciones similares.
Para facilitar la comprensión del manual, en este capítulo se describirán los elementos y acciones compartidos por ciertas funciones.

Cómo se ve RCS Console

Así es como se ve usualmente la página de RCS Console. En este ejemplo se muestra la página de un target:



Área	*Descripción*
1	Barra de título con botones de comando: Salir de RCS. Botón para volver a cargar la página. Botón para ampliar la ventana. Botón para minimizar la ventana.
2	• Botón Anterior del historial de navegación • Botón Siguiente del historial de navegación • Botón para regresar a la página principal • Menú de RCS con las funciones activas para el usuario.

Área	*Descripción*

3 Barra de navegación de la operation. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Regresar al nivel superior.
	Muestra la página de la operation (sección **Operations**).
	Muestra la página del target.
	Muestra la página de la factory.
	Muestra la página del agent.
	Muestra la página de la operation (sección **Intelligence**).
	Muestra la página de la entidad.

4 Botones que permiten mostrar todos los elementos, independientemente del grupo al que pertenecen. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Muestra todas las operations.
	Muestra todos los targets.
	Muestra todos los agents.
	Muestra todas las entidades.

5 Barra de herramientas de la ventana.

6 Botones y cuadro de búsqueda:

Objeto	*Descripción*
	Cuadro de búsqueda. Escriba parte del nombre para que aparezca una lista con los elementos que contienen esas letras.
	Muestra los elementos en una tabla.
	Muestra los elementos como íconos.

7 Usuario conectado con opciones para cambiar el idioma y la contraseña.

Área	*Descripción*
8	Área de descarga con una barra de progreso durante la exportación o compilación. Los archivos se descargan en el escritorio, en la carpeta Descarga de RCS. • Barra superior: porcentaje de generación en el servidor • Barra inferior: porcentaje de descarga desde el servidor a RCS Console.
9	Fecha y hora actuales con opciones para cambiar la zona horaria.

Acciones siempre disponibles en la interfaz

Cambiar el idioma de la interfaz o la contraseña

Para cambiar el idioma de la interfaz o la contraseña:

Paso	*Acción*
1	Haga clic en **[7]** para que aparezca una ventana de diálogo con los datos del usuario.
2	Cambie el idioma o la contraseña y haga clic en **Guardar** para confirmar y salir.

Cambiar la fecha y la hora de RCS Console a su zona horaria

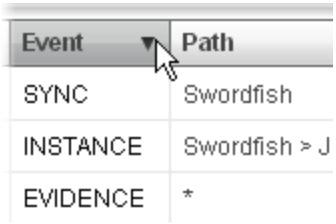
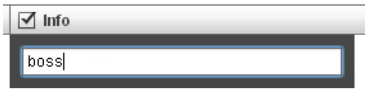
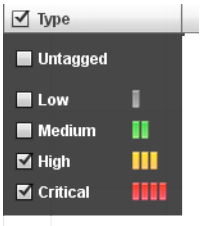
Para convertir todas las fechas y horas a su zona horaria:

Paso	*Acción*
1	Haga clic en **[9]** para que aparezca una ventana de diálogo con la fecha y la hora actuales: **Hora UTC**: hora media de Greenwich (GMT) **Hora local**: fecha y hora donde se encuentra instalado el RCS Server **Hora de la consola**: fecha y hora de la consola que se está utilizando y que se puede cambiar.
2	Cambie la zona horaria y haga clic en **Guardar** para confirmar y salir: todas las fechas y horas se cambiarán según lo que haya indicado.

Acciones relacionadas con las tablas

RCS Console muestra varios datos en forma de tablas. Las tablas le permiten:

- ordenar los datos por columna en orden ascendente o descendente
- filtrar datos por columna

Acción	*Descripción*
Ordenar por columna	Haga clic en el encabezado de la columna para ordenarla de forma ascendente o descendente. 
Filtrar un texto	Escriba una parte del texto que desea buscar: se mostrarán solo los elementos que contengan esas letras.  Al escribir el mismo texto que en el ejemplo se mostrarán elementos con una descripción como: • "my**boss**" • "**boss**anova"
Filtrar en base a una opción	Seleccione una opción: se mostrarán los elementos que coincidan con la opción seleccionada. 
Filtrar en base a varias opciones	Seleccione una o más opciones: se mostrarán los elementos que coincidan con las opciones seleccionadas. 
Cambiar el tamaño de la columna	Seleccione el borde de la columna y arrástrelo.

Administración de los front end

Para administrar los front end:	• Sección System, Frontend

Alcance de la función

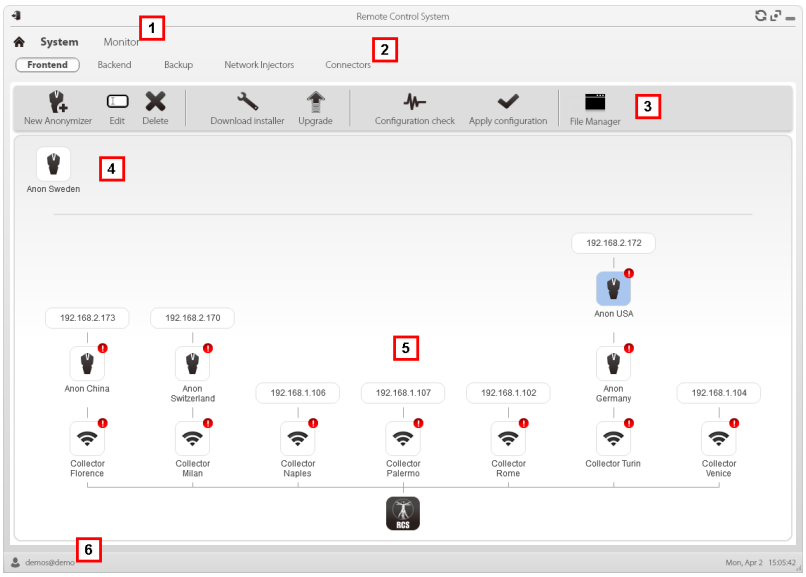
Cuando RCS está funcionando, esta función le permite monitorear los Anonymizers y Collectors, cambiar la configuración del Anonymizer y de las cadenas, y actualizar los VPS.

Durante la instalación, esta función le permite crear un nuevo "objeto" de Anonymizer que actúa como una conexión lógica entre la RCS Console y el componente de software a instalar en un VPS.

NOTA: la función solo se activa si el usuario tiene autorización **Administración de front end**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Menú **System**.

Área	*Descripción*
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Crea un nuevo Anonymizer.
	Permite editar los datos de Anonymizer. Después de editar, haga clic en **Recargar registro**. Muestra los últimos registros.  Sugerencia: haga doble clic Anonymizer para verificar/editar los datos.
	Elimina un Anonymizer. Esto no elimina el Anonymizer instalado en el VPS.
	Genera el instalador para la primera instalación del Anonymizer y lo guarda en el escritorio. Copie el archivo a través de SSH en un VPS remoto y ejecútelo.
	Actualiza la versión de software del Anonymizer desde un equipo remoto.
	Comportamiento simulado del agent. Se conecta a cada Anonymizer de la cadena hasta la puerta de enlace del Collector, y regresa los resultados de conexión.
	Configuración de actualización en todos los Anonymizers. Este comando se usa después de agregar, eliminar o cambiar la cadena de Anonymizers en uso.
	Muestra los paquetes creados automáticamente en el Collector por los vectores **Exploit, WAP Push y QR Code**, disponibles para el dispositivo del target. Los archivos que ya no están en uso se pueden eliminar.  ***PRECAUCIÓN: la eliminación anticipada de archivos puede comprometer la infección por parte de los vectores.***  NOTA: no aparecerá ningún archivo copiado manualmente en la carpeta.

4	Anonymizers configurados que aún no están incluidos en ninguna cadena.

Área	*Descripción*
5	Cadenas de Anonymizers en el sistema con la dirección IP del último elemento.  : Anonymizer (para ver el significado de los distintos símbolos, *consulte "**Qué debería saber acerca de los Anonymizers**" en la página 36*  : el Collector está funcionando.  : el Collector no funciona.
6	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 95* .

Para instalar, editar o cancelar un Anonymizer *consulte "**Instalación y configuración de Anonymizer**" en la página 38* .

Agregar un Anonymizer a la configuración

Para agregar un Anonymizer *consulte "**Instalación y configuración de Anonymizer**" en la página 38* .

Cambiar la configuración del Anonymizer

Para cambiar la configuración de un Anonymizer *consulte "**Instalación y configuración de Anonymizer**" en la página 38* .

Datos del administrador de archivos

A continuación se muestra la descripción de cada elemento:

Campo	*Descripción*
Hora	Fecha y hora de la instalación del vector en el dispositivo.
Nombre	Nombre del archivo creado por el instalador.
Factory	Factory que generó el instalador.
Usuario	Usuario que creó el instalador.

Administración de backend

Para administrar los back end:	• **Sección System, Backend**

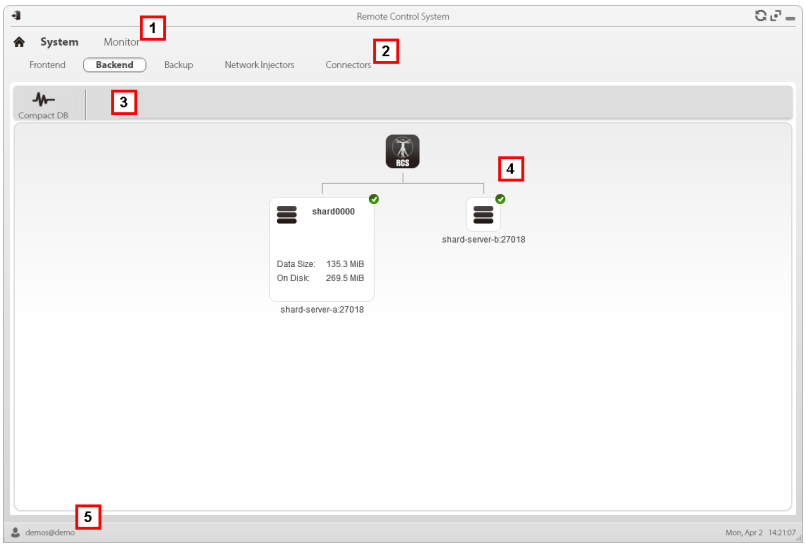
Alcance de la función

Cuando RCS está funcionando, esta función le permite consultar el estado de la base de datos y el espacio disponible en el disco.

NOTA: la función solo se activa si el usuario tiene autorización **Administración de back end**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Menú **System**.

Área	*Descripción*
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Comprime la base de datos.

4	Estructura de las bases de datos shard con su estado y el espacio ocupado y libre en el disco.
	 NOTA: la base de datos 0 es la que está incluida en el Master Node.
5	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 95* .

Para obtener más información sobre las copias de seguridad*consulte "**Qué debería saber acerca de las copias de seguridad**" abajo* .

Datos importantes sobre las bases de datos shard

A continuación se describen los datos de la base de datos shard seleccionada:

Campo	*Descripción*
Espacio ocupado.	Espacio ocupado.
Espacio total disponible	Espacio total en el dispositivo shard.
NombreDelServidor:puerto	Puerto del servidor shard

Qué debería saber acerca de las copias de seguridad

Responsabilidades de la administración

El administrador del sistema debe proteger los datos registrados y establecer la frecuencia de los distintos tipos de copias de seguridad.

Métodos de respaldo

RCS guarda todo el contenido de las bases de datos en la carpeta especificada al hacer cambios en la configuración de RCS. *Consulte "Edición de la configuración del Master Node" en la página 76*

Una copia de seguridad puede guardar uno o más tipos de datos. Los tipos de copia de seguridad son:

- metadatos
- full
- operation
- target

Copia de seguridad de metadatos

El tipo de copia de seguridad metadatos es rápido y guarda toda la configuración del sistema, permitiendo la recuperación rápida de las operations normales del sistema en caso de problemas. Este tipo de copia de seguridad no incluye la evidence recopilada. Se recomienda realizar una copia de seguridad diaria.

ADVERTENCIA: la ausencia de una copia de seguridad metadatos reciente puede ocasionar la pérdida de los agents instalados en varios dispositivos.

NOTA: la tarea que regula la copia de seguridad semanal de tipo metadatos se establece de forma predeterminada y se activa cada vez que se reinicia el sistema. La tarea predeterminada no se puede eliminar.

Copia de seguridad full

La copia de seguridad **full** contiene toda la evidence, por lo que se puede tardar mucho tiempo. Como puede restablecerse luego de una copia de seguridad metadatos, se recomienda realizarla una vez por mes.

Copia de seguridad de la operation

La copia de seguridad de la **operation** guarda todas las operations abiertas y cerradas. Como puede restablecerse luego de una copia de seguridad metadatos, se recomienda realizarla una vez por mes.

Copia de seguridad del target

La copia de seguridad del **target** guarda todos los datos abiertos y cerrados del target. Como puede restablecerse luego de una copia de seguridad metadatos, se recomienda realizarla una vez por mes.

Copia de seguridad incremental

Las copias de seguridad **full**, de **operations** y de **targets** también pueden ser incrementales. De esta manera el sistema guarda los datos generados a partir de la fecha y la hora de la última copia de seguridad. La primera copia de seguridad incremental siempre es completa (full, de operation o de target). Solo las subsecuentes podrán ser incrementales.

NOTA: si la opción incremental se elimina y se vuelve a aplicar a una tarea, la siguiente copia de seguridad de la tarea será completa.

Sugerencia: coloque el nombre de la tarea de manera que se la reconozca como copia de seguridad incremental (p. ej.: "Increm_últimaSemana").

Sugerimos que ejecute una copia de seguridad completa (full, de operation o de target) una vez por mes, y una copia de seguridad incremental una vez por semana.

Restauración de copias de seguridad por motivos drásticos

PRECAUCIÓN: solo se debe considerar una restauración de copia de seguridad para situaciones drásticas, como un reemplazo de la base de datos.

Se debe restaurar una copia de seguridad cada vez que se reemplace un servidor.

Restauración de copia de seguridad

IMPORTANTE: la restauración de la copia de seguridad nunca es destructiva. Por este motivo, la restauración no debe utilizarse para recuperar elementos cambiados accidentalmente.

A continuación se muestran algunos ejemplos:

Si es después de la última copia de seguridad	*Entonces la restauración*
un elemento fue eliminado	recupera el elemento eliminado.
un elemento fue editado	deja el elemento cambiado.
se agregó un nuevo elemento	deja el elemento cambiado.

IMPORTANTE: la copia de seguridad no restaura información u operations que se hayan cerrado por error (eliminadas).

IMPORTANTE: para restaurar una copia de seguridad incremental, restaure todas las copias empezando por la más antigua.

Copia de seguridad completa por motivos serios

Introducción

En casos extremos (p. ej.: migración del servidor a un hardware diferente, restauración de datos corrupta), ejecute una copia de seguridad completa.

Ejecutar copia de seguridad

Cómo ejecutar una copia de seguridad:

Paso	*Acción*
1	Detenga todos los servicios de RCS.
2	Cree una copia completa de la carpeta C:\RCS\.

Restauración de copia de seguridad

Cómo restaurar una copia de seguridad:

Paso	*Acción*
1	Instale un sistema RCS como si fuera nuevo.
2	Detenga todos los servicios de RCS.
3	Sustituya la nueva carpeta C:\RCS\ con la que copió anteriormente.
4	Reinicie los servicios.

Administración de copias de seguridad

Para administrar las copias de seguridad:	• **Sección System, Backup**

Alcance de la función

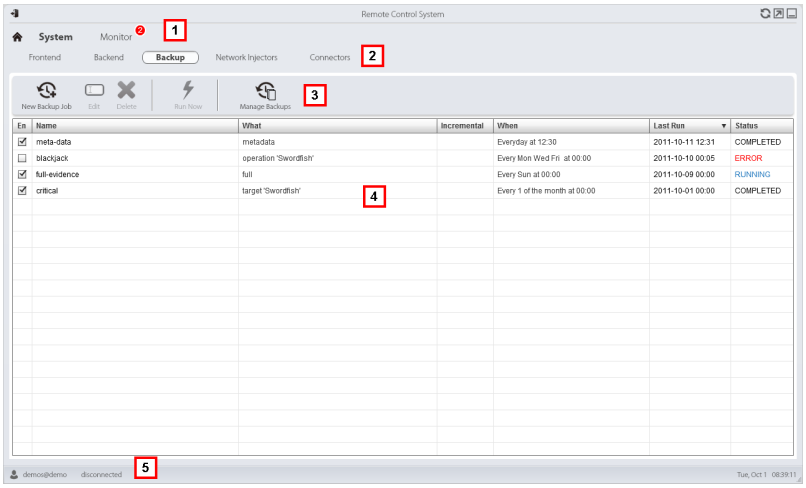
Cuando RCS está funcionando, esta función le permite consultar el último estado de la copia de seguridad, crear nuevos procesos de copia de seguridad o ejecutar inmediatamente un proceso de respaldo.

Durante el mantenimiento de RCS, esta función le permite reparar datos dañados, restaurándolos con una copia de seguridad.

NOTA: la función solo se activa con los permisos **Copia de seguridad y restauración del sistema**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Menú **System**.

Área	*Descripción*
3	Barra de herramientas del proceso de respaldo. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Agrega un proceso de respaldo.
	Edita un proceso de respaldo, por ejemplo, para desactivarlo o cambiar su frecuencia.  **IMPORTANTE: no use esta función para cambiar el tipo de datos procesados. Es mejor desactivar el proceso y crear uno nuevo con un nombre coherente.**
	Elimina un proceso de respaldo. No elimina los archivos de la copia de seguridad generados por el proceso.
	Ejecuta las copias de seguridad aun si están desactivadas.
	Consulte la lista de copias de seguridad completas. Los botones se describen a continuación:  restaura los datos desde el archivo de respaldo seleccionado.  ***PRECAUCIÓN: la restauración de datos es una operación delicada. Asegúrese de haber entendido completamente los mecanismos de restauración de RCS.Consulte "Qué debería saber acerca de las copias de seguridad" en la página 104***  elimina la copia de seguridad seleccionada.

4	Lista de procesos de respaldo programados (activados y desactivados) con el estado de la última copia de seguridad.
5	Barra de estado de RCS.

Datos importantes del proceso de respaldo

A continuación se describen los datos del proceso de respaldo seleccionado:

Campo	*Descripción*
Activado	Activa/desactiva el proceso de respaldo. Úselo para desactivar temporalmente el proceso, por ejemplo, al reemplazar el dispositivo de respaldo.  Sugerencia: para activar/desactivar rápidamente un proceso, marque el cuadro de verificación en la columna **En** de la lista.
Qué	Datos a incluir en la copia de seguridad. **Metadatos**: toda la configuración del sistema: base de datos, Collector, Network Injector, Anonymizer, agent. Esto es lo mínimo necesario para restaurar el sistema en caso de un desastre. Toda la información requerida para recopilar información del agent está contenida en este tipo de copia de seguridad. **Full**: copia de seguridad completa de la configuración del sistema y los datos de intercepción (operation y target). Su ejecución puede tardar un tiempo. **Operation**: copia de seguridad de la operation indicada, con los datos incluidos. **Target**: copia de seguridad del target indicado, con los datos incluidos.
Cuándo	Frecuencia de la copia de seguridad. **UTC**: zona horaria.
Nombre	Nombre a asignar a la copia de seguridad.

Administración de conectores

Para administrar los conectores:	• **Sección System, Connectors**

Alcance de la función

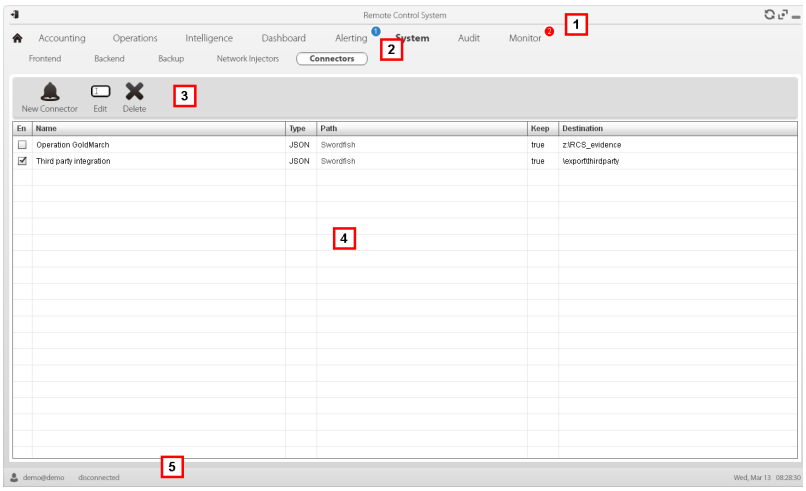
Esta función le permite crear reglas de conexión con otros RCS Servers instalados con licencias específicas o software de terceros. La evidence recibida por RCS será clasificada en base a estas reglas.

 **IMPORTANTE: esta función requiere una licencia de usuario.**

 NOTA: la función solo se activa si el usuario tiene autorización **Administración de conectores**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Menú **System**.
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:
4	Lista de reglas de conexión.
5	Barra de estado de RCS.

Ícono	*Descripción*
	Agregar una regla de conexión.
	Editar la regla de conexión seleccionada.
	Eliminar la regla de conexión seleccionada.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 95* .

Datos importantes sobre las reglas de conexión

A continuación se describen los datos de la regla seleccionada:

Campo	*Descripción*
Ruta de acceso	El nombre de la operation o del target de quien se envía la evidence. Si no se especifica, todas las operations y la evidence se enviarán al software de un tercero.
Tipo	Tipo de almacenamiento de la evidence: • **Local**: la evidence se envía a una carpeta local • **Remote**: la evidence se envía al sistema RCS.
Formato	Formato de evidence. • **JSON, XML** para el tipo **Local** • **RCS** para el tipo **Remoto**
Guardar evidence	Si se selecciona, se mantendrá una copia de la evidence en la base de datos de RCS.  ***PRECAUCIÓN: si no se selecciona, esta evidence ya no se podrá ver en RCS, y no se podrán recibir alerts.***
Target	Ruta de la carpeta local donde se envía la evidence (p. ej.: "C:\evidenciaRCS") o dirección IP del servidor de RCS.  NOTA: la evidence solo puede enviarse a un RCS Server con una licencia de usuario específica. El ID que se vinculará a la evidence enviada se puede asignar en el archivo de configuración del sistema.

Administración de los Network Injector

Para administrar los Network Injectors:	• Sección **System**, **Network Injectors**

Propósito

Durante la instalación, esta función le permite:

- crear un nuevo "objeto" Network Injector que crea la conexión lógica entre RCS Console y ese dispositivo de hardware particular.
- exportar la clave de autentificación que se instalará en Network Injector para activar las comunicaciones con RCS Console.

 NOTA: la función está activada solo si el usuario tiene autorización **Administración de Network Injector**.

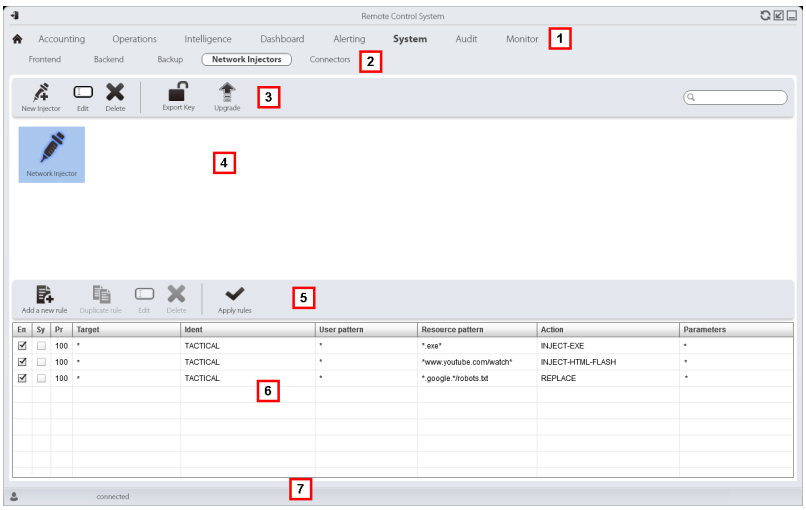
Qué puede hacer

Con esta función usted puede:

- crear un nuevo Network Injector
- exportar la clave de autentificación de Network Injector
- actualizar el software de Appliance Control Center o Tactical Control Center
- ver los registros y consultar el estado de Network Injector

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Menú **System**.

Área	*Descripción*
3	Barra de herramientas del Network Injector. A continuación se muestra la descripción de cada elemento:

Acción	*Función*
	Agrega un nuevo Network Injector
	Permite editar los datos del Network Injector y ver los registros.
	Elimina el Network Injector seleccionado.
	Genera un archivo .zip con la clave de autentificación de Network Injector.
	Actualiza el software de Appliance Control Center o Tactical Control Center. Si el Network Injector es un tipo de Appliance, se actualizará automáticamente durante la próxima sincronización siempre que haya un proceso de infección activo. Si, en lugar de esto, es del tipo Tactical, el operador debe seleccionar dónde se actualizará la aplicación. *Consulte "**Actualización del Network Injector Appliance**" en la página 68 , "**Actualización de Tactical Network Injector**" en la página 71*

4	Lista de Network Injectors.
5	Barra de herramientas de inyección.
6	Lista de reglas del Network Injector seleccionado
7	Barra de estado de RCS. .

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 95* .

Para obtener más información sobre la instalación de Network Injector Appliance *consulte "**Instalación de Network Injector Appliance**" en la página 43*

Para obtener más información acerca de la instalación de Tactical Network Injector, *consulte "**Instalación de Tactical Network Injector**" en la página 51* .

Para obtener más información sobre los datos de Network Injector *consulte "**Datos del Network Injector**" en la página opuesta*

Actualización del software de control de Network Injector

Para actualizar Network Injector:

Paso	*Acción*
1	• Seleccione el Network Injector • Haga clic en **Actualizar**: se mostrarán los datos de la actualización. • Haga clic en **Aceptar**: RCS recibe la solicitud para enviar la actualización al Network Injector.

IMPORTANTE: Network Injector solo recibe las reglas de actualización de software cuando se sincroniza con RCS Server. ***Consulte "Verifique el estado del Network Injector" en la página 58***

Datos del Network Injector

A continuación se describen los datos del Network Injector:

Datos	*Descripción*
Nombre	Nombre del Network Injector
Descripción	Descripción libre.
Versión	Versión de software. Para ver las versiones de software de todos los componentes *consulte "Monitoreo del sistema (Monitor)" abajo* .
Log	Últimos mensajes registrados. NOTA: Tactical Network Injector registra las actualizaciones según la frecuencia con que el operador activa la sincronización. Para ver el contenido del archivo de registro *consulte "Registros del sistema" en la página 81* : actualiza la lista. : elimina los registros vistos.

Monitoreo del sistema (Monitor)

Para monitorear el sistema:	• Sección **Monitor**

Propósito

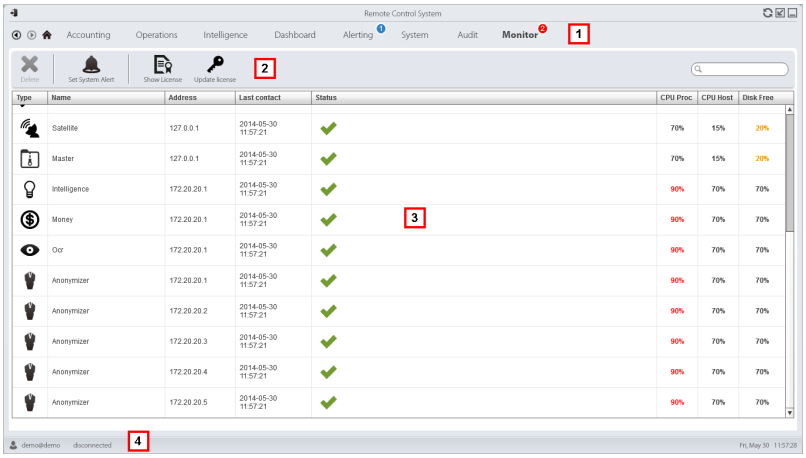
Esta función le permite:

- monitorear el estado del sistema en términos de hardware y software
- eliminar elementos bajo monitoreo que se desinstalaron
- monitorear las licencias usadas en comparación con las que se compraron

Llamada al servicio: póngase en contacto con su gerente de cuenta de HackingTeam si necesita más licencias.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS. Monitor 1 : indica la cantidad actual de alarmas del sistema que se activaron.
2	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Elimina el componente a monitorear.

Área	*Descripción*
3	Lista de componentes de RCS y su estado:  Alarma (genera y envía un correo electrónico al grupo de alerting)  Advertencia  Componente en funcionamiento
4	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 95* .

Para ver una descripción de los datos en esta ventana *consulte "**Datos de monitoreo del sistema (Monitor)**" abajo* .

Eliminar un componente bajo monitoreo

Para eliminar un componente desinstalado:

Paso	*Acción*
1	Seleccione el componente.
2	Haga clic en **Eliminar**: RCS ya no leerá el estado de ese componente. Solo las instalaciones subsecuentes de nuevos componentes actualizarán automáticamente la lista.  NOTA: la eliminación por error de un componente que aún está instalado no es destructiva. El estado del componente se reparará la siguiente vez que la página se vuelva a cargar.

Datos de monitoreo del sistema (Monitor)

Datos del monitoreo de los componentes del sistema

A continuación se muestran los datos de monitoreo del sistema:

Datos	*Descripción*
Tipo	Tipo y nombre de los componentes monitoreados.
Nombre	A continuación se muestran algunos ejemplos:  Anonymizer  Carrier  Collector  Database  Network Controller
Dirección	Dirección IP del componente.
Último contacto	Fecha y hora de la última sincronización.
Estado	Estado del componente en la última sincronización:  Alarma: el componente no está funcionando, póngase en contacto con el grupo de alerting para repararlo de inmediato.  Advertencia: el componente indica una situación de riesgo, póngase en contacto con el administrador del sistema para que realice las revisiones necesarias.  Componente en funcionamiento.
Proceso de CPU	% de uso de CPU por parte del proceso particular.
Host de CPU	% de uso de CPU por parte del servidor.
Espacio libre en el disco	% de espacio libre en el disco.

Datos de monitoreo de la licencia

A continuación se describen los datos de monitoreo de la licencia: para las licencias restringidas, el formato es "x/y", donde "x" es la cantidad de licencias que el sistema utiliza actualmente e "y" es la cantidad máxima de licencias.

PRECAUCIÓN: si todas las licencias están en uso, cualquier agent nuevo quedará en una cola de espera hasta que se libere una licencia o se compren más licencias.

Datos	*Descripción*
Tipo de licencia	Tipo de licencia actualmente en uso para los agents. **reusable**: una licencia de agent puede volver a utilizarse después de que se desinstala. **oneshot**: la licencia de un agent solo es válida para una instalación.  NOTA: la licencia solo puede actualizarse si el usuario tiene autorización **Modificación de licencias**.
Usuarios	Cantidad de usuarios actualmente en uso por parte del sistema y cantidad máxima admitida.
Agent	Cantidad de agents actualmente utilizados por el sistema y cantidad máxima admitida.
De escritorio **Móvil**	Cantidad de agents de escritorio y móviles actualmente utilizados por el sistema y cantidades máximas admitidas, respectivamente.
Servidores distribuidos	Cantidad de bases de datos actualmente utilizadas por el sistema y cantidad máxima admitida.
Collectors	Cantidad de Collectors actualmente utilizados por el sistema y cantidad máxima admitida.
Anonymizers	Cantidad de Anonymizers actualmente utilizados por el sistema y cantidad máxima admitida.

]HackingTeam[

HT S.r.l.
via della Moscova, 13
20121 Milan (MI)
Italia
tel.: + 39 02 29 060 603
fax:+ 39 02 63 118 946
www.hackingteam.com
e-mail:info@hackingteam.com

RCS 9.5 Manual del administrador del sistema
Manual del administrador del sistema 1.8 NOV-2014

info@hackingteam.com