]HackingTeam[

RCS 9

The hacking suite for governmental interception

Manuale dell'amministratore di sistema

Proprietà delle informazioni

NOTA: richieste di ulteriori copie di questo manuale o di informazioni tecniche sul prodotto, devono essere indirizzate a:

HT S.r.l.

via della Moscova, 13

20121 Milano (MI)

Italy

Tel.: + 39 02 29 060 603

Fax: + 39 02 63 118 946

e-mail: info@hackingteam.com

Sommario

Elenco degli schemi

Glossario dei termini

Di seguito i termini utilizzati in questo manuale e loro definizione.

A

Accounting
Sezione della console dedicata alla gestione degli accessi a RCS.

Agent elite
Agente installato su dispositivi sicuri. Permette di raccogliere tutti i tipi di evidence disponibili.

Agent scout
Sostituto dell'agent inviato sul dispositivo per verificarne il livello di sicurezza prima di installare gli agent veri e propri (elite o soldier).

Agent soldier
Agente installato su dispositivi non completamente sicuri. Permette di raccogliere solo alcuni tipi di evidence.

Agente
Sonde software installate sui dispositivi sotto monitoraggio. Progettate per raccogliere prove e comunicarle al Collector.

Alerting
Sezione della console dedicata alle segnalazioni di nuove prove.

Amministratore
Colui che abilita l'accesso al sistema agli utenti, crea i gruppi di lavoro e definisce le indagini in essere, gli obiettivi e il tipo di dati da raccogliere.

Amministratore di sistema
Colui che installa i server e le console, si occupa degli aggiornamenti software e del ripristino dei dati in caso di malfunzionamento.

Analista
Persona incaricata dell'analisi dei dati raccolti durante le indagini.

Anonymizer
(opzionale) Protegge il server da attacchi esterni e consente l'anonimato durante le operazioni di indagine. Trasferisce i dati degli agent ai Collector.

Audit
Sezione della console che riporta tutte le azioni degli utenti e del sistema. Utilizzata per controllare abusi di RCS.

avvisi da evidence
Avvisi, normalmente email, inviati agli analisti per avvisarli che una nuova evidence corrisponde alle regole impostate.

B

back end
Ambiente destinato alla decodifica e salvataggio delle informazioni raccolte. In architettura distribuita include il Master Node e i database Shard.

BRAS
(Broadband Remote Access Server) instrada il traffico da/a DSLAM verso la rete dell'ISP e fornisce l'autenticazione per gli iscritti dell'ISP.

BSSID
(Basic Service Set IDentifier) Identificativo dell'Access Point e dei suoi client.

C

Carrier
Servizio del Collector: invia i dati ricevuti dagli Anonymizer agli shard o al Master Node.

Collector
Servizio del Collector: riceve i dati inviati dagli agent, tramite la catena di Anonymizer.

console
Computer su cui è installato RCS Console. Accede direttamente a RCS Server o al Master Node.

D

Dashboard
Sezione della console dedicata all'Analista. Usata per avere una rapida panoramica dello stato delle investigazioni, dei target e degli agent più importanti.

DSLAM
(Digital Subscriber Line Access Multiplexer) apparato di rete, spesso collocato negli scambi telefonici dell'operatore telefonico. Connette più interfacce DSL a un canale di comunicazione digitale ad alta velocità usando le tecniche di multiplexing.

E

entità
Insieme di informazioni di intelligence associate al target e a persone e luoghi coinvolti nell'indagine.

ESSID
(Extended Service Set IDentifier) Conosciuto anche come SSID, identifica la rete WiFi.

evidence
Dati delle prove raccolti. Il formato dipende dal tipo di evidence (es.: immagine).

Exploit
Codice che, sfruttando un bug o una vulnerabilità, porta all'esecuzione di codice non previsto. Utilizzato per infettare i dispositivi dei target.

F

factory
Un modello per la configurazione e la compilazione di agent.

front end
Ambiente destinato a comunicare con gli agent per raccogliere informazioni e impostare la loro configurazione. In architettura distribuita include il Collector e il Network Controller.

G

Gruppo
Entità di intelligence che raggruppa più entità.

gruppo di alerting
Raggruppa gli utenti che devono ricevere notifiche via mail ogni volta che si genera un allarme di sistema (per esempio, il database ha superato il limite di spazio libero disponibile). Normalmente, questo gruppo è associato a nessuna operation.

M

Monitor
Sezione della console dedicata alle segnalazioni degli stati dei componenti e delle licenze.

N

Network Controller
Servizio del Collector: controlla lo stato dei Network Injector e degli Anonymizer, spedendo loro le nuove configurazioni o aggiornamenti software.

Network Injector
Componente hardware che controlla il traffico di rete del target e inietta un agent nelle risorse Web selezionate. Fornito in due versioni, Appliance o Tactical: Appliance è per installazioni presso ISP, mentre Tactical è utilizzato sul campo.

Network Injector Appliance
Versione rack di Network Injector, per l'installazione presso l'ISP. Cfr.: Tactical Network Injector.

O

operation
Investigazione verso uno o più target, i cui dispositivi saranno i destinatari degli agent.

P

Person
Entità di intelligence che rappresenta una persona coinvolta in un'indagine.

Position
Entità di intelligence che rappresenta un luogo coinvolto in un'indagine.

R

RCS
(Remote Control System) il prodotto oggetto di questo manuale.

RCS Console
Software dedicato all'interazione con RCS Server.

RCS Server
Una o più macchine, in base all'architettura di installazione, dove sono installati i componenti alla base di RCS: i database Shard, i Network Controller e Collector.

regole di alert
Regole che creano alert quando una nuova evidence viene salvata o quando l'agent sincronizza per la prima volta.

regole di injection
Impostazioni che definiscono come identificare traffico HTTP, quale risorsa da infettare e quale metodo usare per l'infezione.

S

sequenze di acquisizione
Insieme di eventi, azioni e moduli di acquisizione complessi che costituiscono la configurazione avanzata di un agent.

SSH
(Secure SHell) protocollo di rete per sessioni remote cifrate, servizi remoti o esecuzioni comandi.

System
Sezione della console dedicata alla gestione del sistema.

T

Tactical Network Injector
Versione portatile di Network Injector, per utilizzo tattico. Cfr.: Network Injector Appliance.

TAP
(Test Access Port) dispositivo hardware inserito in reti informatiche che permette il monitoraggio passivo del flusso dati in transito.

target
La persona fisica sotto investigazione. Nella sezione intelligence è rappresentata dall'entità Target.

Tecnico
Colui che su mandato dell'Amministratore crea e gestisce gli agent.

V

Virtual
Entità di intelligence che rappresenta un luogo virtuale (es. un sito web) coinvolto in un'indagine.

VPS
(Virtual Private Server) server remoto su cui installare l'Anonymizer. Normalmente disponibile a noleggio.

W

WPA
(WiFi Protected Access) Protezione per le reti WiFi.

WPA 2
(WiFi Protected Access) Protezione per le reti WiFi.

1

Introduzione a questa Guida

Presentazione

Obiettivi del manuale

Questo manuale guida l'*Amministratore di sistema* a:

- installare correttamente il sistema RCS e i suoi componenti
- configurare i componenti mediante la console di amministrazione
- comprendere e risolvere eventuali problemi sistemistici

Di seguito sono presentate le informazioni necessarie alla consultazione del manuale.

Contenuti

Questa sezione include i seguenti argomenti:

Novità della guida

Elenco note di rilascio e aggiornamenti di questa guida in linea.

Data rilascio	*Codice*	*Versione software*	*Descrizione*
19 Febbraio 2014	Manuale dell'amministratore di sistema 1.5 FEB-2014	9.2	Aggiornata gestione installazione e aggiornamento degli Anonymizer, *vedi "**Installazione e configurazione degli Anonymizer**" a pagina 42 , "**Aggiornamento degli Anonymizer**" a pagina 70* . Aggiunta gestione del servizio Carrier del Collector, *vedi "**Cose da sapere su RCS**" a pagina 11* Modificati comandi per verifica stato dei componenti, *vedi "**Procedure di verifica stato componenti**" a pagina 84* . Aggiunta descrizione comandi da terminale per applicativi Tactical Control center e Appliance Control Center, *vedi "**Comandi Tactical Control Center e Appliance Control Center**" a pagina 57*
30 Settembre 2013	Manuale dell'amministratore di sistema 1.4 SET - 2013	9	Aggiornata documentazione installazione, aggiornamento e gestione dei Network Injector, *vedi "**Installazione componenti opzionali e aggiuntivi**" a pagina 41 , "**Manutenzione ordinaria e aggiornamenti software**" a pagina 67 , "**Gestione dei Network Injector**" a pagina 112* . Aggiornata documentazione sui connectors, *vedi "**Gestione dei connector**" a pagina 110* . Aggiornata documentazione per migliorie apportate all'interfaccia utente.
8 Luglio 2013	Manuale dell'amministratore di sistema -	8.4	Nessun aggiornamento alla documentazione.

Data rilascio	*Codice*	*Versione software*	*Descrizione*
15 Marzo 2013	Manuale dell'amministratore di sistema 1.3 MAR-2013	8.3	Modificate modalità di aggiornamento dei Tactical Network Injector. *Vedi "**Aggiornamento Tactical Network Injector**" a pagina 72* . Modificate modalità di aggiornamento di Network Injector Appliance. *Vedi "**Aggiornamento Network Injector Appliance**" a pagina 70* . Aggiunta descrizione delle regole di connessione a software terze parti. *Vedi "**Gestione dei connector**" a pagina 110* . Il modulo OCR può indicizzare i contenuti delle evidence di tipo file (tutti i formati). *Vedi "**Installazione modulo OCR**" a pagina 36* . Aggiunta descrizione del modulo RCS Translate disponibile su licenza d'uso e installabile con il supporto dell'assistenza tecnica.
15 Ottobre 2012	Manuale dell'amministratore di sistema 1.2 OTT-2012	8.2	Aggiunte utility per il riavvio servizi Windows, *vedi "**Procedure per riavviamento dei servizi** " a pagina 86* . Aggiunto BareTail per Windows, visualizzatore di code di log. *Vedi "**I log di sistema**" a pagina 82* . Aggiunta gestione backup incrementali e obbligo presenza job backup metadata. *Vedi "**Cose da sapere sui backup**" a pagina 105* . Supporto autenticazione invio e-mail per gli alert. *Vedi "**Modifica alla configurazione di Master Node**" a pagina 77* . Modulo OCR facoltativo. *Vedi " **Installazione modulo OCR**" a pagina 36* Aggiunto wizard per creazione gestione rapida dati in archivio. *Vedi "**Descrizione dei wizard da homepage**" a pagina 94* Unica applicazione Tactical Control Center sul Tacitcal Network Injector.
30 Giugno 2012	Manuale dell'amministratore di sistema 1.1 GIU-2012	8.1	File Manager per eliminare i pacchetti di file nella cartella C:\RCS\Collector\public. *Vedi "**Gestione dei frontend**" a pagina 100* .
16 Aprile 2012	Manuale dell'amministratore di sistema 1.0 APR-2012	8.0	Prima pubblicazione

Documentazione fornita

A corredo del software RCS sono forniti i seguenti manuali:

Manuale	*Destinatari*	*Codice*	*Formato di distribuzione*
Manuale dell'amministratore di sistema (questo manuale)	Amministratore di sistema	*Manuale dell'amministratore di sistema 1.5 FEB-2014*	PDF
Manuale dell'amministratore	Amministratori	*Manuale dell'amministratore 1.5 FEB-2014*	PDF
Manuale del tecnico	Tecnici	*Manuale del tecnico 1.6 FEB-2014*	PDF
Manuale dell'analista	Analisti	*Manuale dell'analista 1.5 FEB-2014*	PDF

Convenzioni tipografiche per le segnalazioni

Di seguito le segnalazioni previste in questo documento (Microsoft Manual of Style):

AVVERTENZA: indica una situazione rischiosa che se non evitata, può causare danni fisici all'utente o alle attrezzature.

PRUDENZA: indica una situazione rischiosa che se non evitata, può causare la perdita di dati.

IMPORTANTE: offre indicazioni essenziali al completamento del compito. Mentre le note possono essere trascurate e non inficiano il completamento del compito, le indicazioni importanti non devono essere trascurate.

NOTA: informazioni neutre e positive che enfatizzano o aggiungono informazioni a dei punti nel testo principale. Fornisce informazioni che possono essere applicate solo in casi speciali.

Suggerimento: consiglia l'utente nell'applicare le tecniche e le procedure descritte nel testo ai loro bisogni specifici. Può suggerire un metodo alternativo e non è fondamentale alla comprensione del testo.

Richiede assistenza: l'operazione può essere portata a termine solo su indicazioni dell'assistenza tecnica.

Convenzioni tipografiche per la formattazione

Di seguito la legenda di alcune convenzioni tipografiche:

Esempio	***Stile***	***Descrizione***
*Vedi "**Dati degli utenti**"*	*corsivo*	indica il titolo di un capitolo, una sezione, una sottosezione, un paragrafo, una tabella o una figura di questo manuale, o di un'altra pubblicazione di riferimento.
<ggmmaaaa>	<aaa>	indica un testo che dovrà essere specificato dall'utente secondo una certa sintassi. Nell'esempio <ggmmaaaa> è una data e può diventare "14072011".
Selezionare uno dei server elencati **[2]**.	**[x]**	indica l'oggetto citato nel testo e che compare nell'immagine adiacente.
Fare clic su **Add**. Selezionare il menu **File, Save data.**	**grassetto**	indica una scritta sull'interfaccia operatore, sia di un elemento grafico (es.: tabella, scheda) sia di un pulsante a video.
Premere ENTER	MAIUSCOLO	indica il nome di tasti della tastiera.
Cfr.: Network Injector Appliance	-	suggerisce di confrontare la definizione di un termine in glossario o contenuto con altro termine o contenuto.

Destinatari del prodotto e di questa guida

Di seguito le figure professionali che interagiscono con RCS.

Destinatario	*Attività*	*Competenze*
Amministratore di sistema	Segue le indicazioni dell'assistenza HackingTeam fornite in fase contrattuale. Installa e aggiorna i server RCS, i Network Injector e le RCS Console. Programma e gestisce i backup. Ripristina i backup in caso di sostituzione dei server.  AVVERTENZA: l'amministratore di sistema deve avere tutte le competenze necessarie richieste. HackingTeam non si assume alcuna responsabilità di malfunzionamenti o danni alle attrezzature arrecati da una installazione non professionale.	*Tecnico di reti esperto*
Amministratore	Crea gli account e i gruppi autorizzati. Crea operation e target. Controlla lo stato del sistema e delle licenze.	*Responsabile dell'indagine*
Tecnico	Crea gli agent e li configura. Configura le regole di un Network Injector.	*Tecnico specializzato in intercettazioni*
Analista	Analizza le evidence e le esporta.	*Operativo*

Dati di identificazione dell'autore del software

HT S.r.l.
via della Moscova, 13
20121 Milano (MI)
Italy
Tel.: + 39 02 29 060 603
Fax: + 39 02 63 118 946
e-mail: info@hackingteam.com

2

RCS (Remote Control System)

Presentazione

Introduzione

RCS (Remote Control System) è una soluzione a supporto delle investigazioni che intercetta attivamente e passivamente dati e informazioni dai dispositivi dei bersagli di tali investigazioni. RCS infatti crea, configura e installa nell'assoluto anonimato degli agenti software che raccolgono dati e informazioni e inviano i risultati al database centrale per la decodifica e il salvataggio.

Contenuti

Questa sezione include i seguenti argomenti:

Componenti in architettura All-in-One

Introduzione

RCS è installato presso la centrale operativa e le sale di intercettazione dell'autorità proprietaria. Può essere corredato di apparati speciali (hardware e software) installati presso entità esterne, quali fornitori Internet o server remoti. RCS può essere installato in architettura *All-In-One* o architettura *Distribuita*.

Schema architettura All-In-One

L'architettura All-in-One prevede l'installazione di RCS su un solo server. Di seguito lo schema logico dell'architettura:

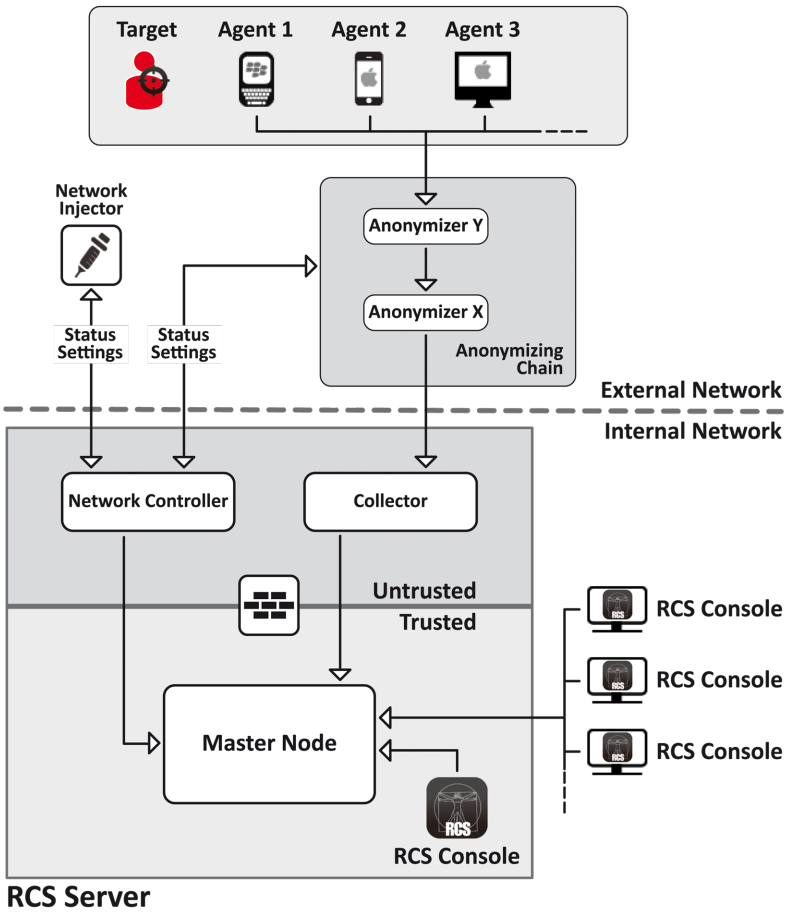


Figura 1: Architettura RCS All-In-One: schema logico

Componenti architettura RCS All-in-One

Di seguito i componenti dell'architettura:

Componente	*Funzione*	*Installazione*
Agente	Cimici software, intercettano e comunicano dati e informazioni del target dell'investigazione a un Anonymizer.	• *dispositivi del target* • *sorgenti dati*
Anonymizing chain **Anonymizer**	Gruppi di Anonymizer geograficamente distribuiti che garantiscono l'anonimato dei Collector e reindirizzano i dati raccolti per proteggere i server da attacchi esterni. Trasferisce i dati degli agent ai server. È possibile configurare più Anonymizer in catena per aumentare il livello della protezione. Ciascuna catena fa capo ad un Collector.	*VPS (Virtual Private Server)*
Collector	Componente del server RCS: il servizio Collector raccoglie i dati degli agent attraverso la catena di Anonymizer, il servizio Carrier invia i dati agli shard e al Master Node.	*server RCS*
Firewall	Opzionale ma fortemente suggerito, protegge l'ambiente *trusted* dove vengono elaborati e memorizzati i dati, dall'ambiente *untrusted*, dove i dati vengono raccolti.	*server RCS*
RCS console	Console di configurazione, monitoraggio e analisi ad uso degli operatori della centrale operativa.	• *server RCS* • *rete interna*
Master Node	Cuore del server RCS, gestisce i flussi dei dati, gli stati dei componenti e include il primo database Shard. Include il servizio Worker per la decodifica dei dati prima del salvataggio sul database.	*server RCS*
Network Controller	(opzionale) Componente del server RCS, invia le configurazioni al Network Injector, alle catene di Anonymizer e acquisisce costantemente il loro stato.	*server RCS*
Network Injector	(opzionale) Componente hardware fisso (Appliance) o portatile (Tactical), esegue operazioni di sniffing e injection sulle connessioni HTTP del target.	• *ISP* • *LAN Wired o Wireless (abitazioni, hotel)*

Componente	*Funzione*	*Installazione*
Target	Bersagli dell'investigazione. Ogni dispositivo in possesso del target rappresenta una sorgente di dati e può essere monitorato da un agent.	-

Componenti architettura distribuita

Introduzione

In casi particolari è possibile installare RCS anche in architettura *distribuita*.

Schema architettura distribuita

L'architettura distribuita prevede l'installazione dei componenti software su più server. Di seguito lo schema dell'architettura:

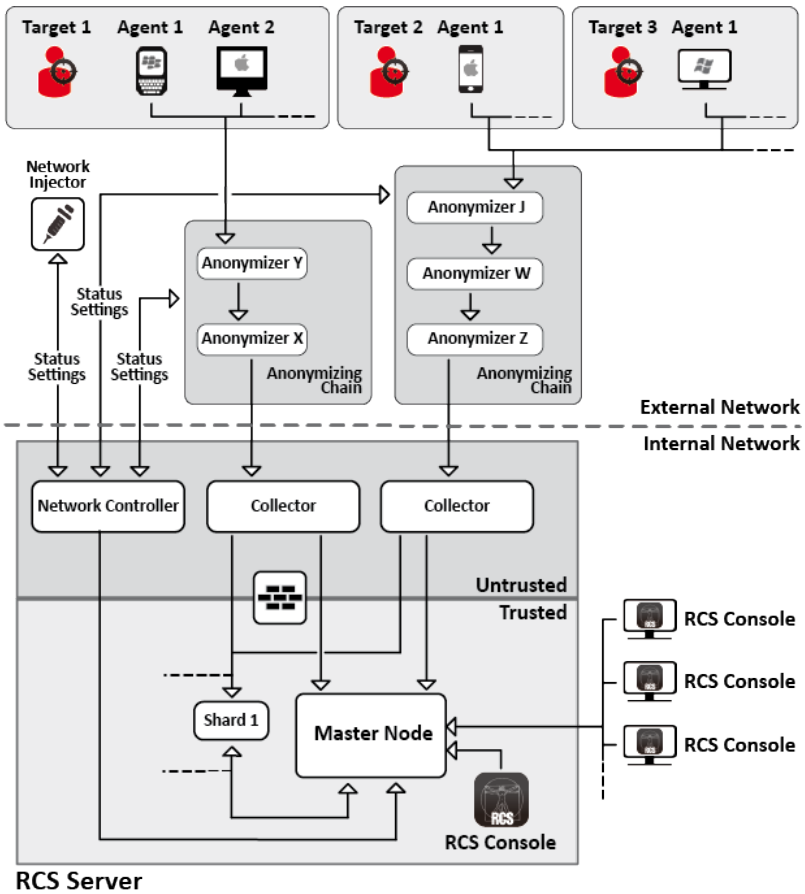


Figura 1: Architettura RCS distribuita: schema logico

Componenti architettura distribuita

Di seguito le differenze dei componenti in architettura distribuita rispetto ai componenti in architettura All-in-One:

Componente	*Funzione*	*Installazione*
Collector	Uno per ogni Anonymizing Chain: il servizio Collector raccoglie i dati degli agent comunicati dall'ultimo Anonymizer della catena, il servizio Carrier invia i dati agli shard e al Master Node. Sottoposto a singola licenza.	*uno o più server in ambiente front end*
Network Controller	Uno per architettura, è compreso nell'installazione del primo Collector.	*un server in ambiente front end*
Shard x	Partizioni aggiuntive del database distribuito RCS. Lo Shard 0 è compreso nel Master Node. Include il servizio Worker per la decodifica dei dati e loro inserimento nel database.	*uno o più server in ambiente back end*

Cose da sapere su RCS

Funzionamento

I componenti del sistema RCS devono essere opportunamente installati e predisposti sia presso la centrale operativa sia, eventualmente, presso i fornitori di servizi Internet. Tipicamente divisi in ambienti di *front end* per tutte le attività di raccolta dati, intercettazione e monitoraggio e l'ambiente di*back end* per tutte le attività di raccolta dati e backup.

Flusso e protezione dei dati

Il server RCS separa nettamente le attività in ambiente *untrusted* da quelle in ambiente *trusted*. Il limite invalicabile è dato da un firewall residente.

In ambiente untrusted vengono raccolti i dati delle intercettazioni, eventualmente reindirizzati per proteggere l'identità del destinatario (Voi) e passati a un collettore di informazioni (Collector) e inviati all'ambiente trusted tramite un serivizio specifico (Carrier). La verifica dello stato e la configurazione delle entità esterne viene demandata a un componente specifico (Network Controller).

In ambiente trusted invece, avviene la vera gestione, configurazione e monitoraggio delle intercettazioni (Master Node).

RCS Console infine, è un client che si collega direttamente al Master Node. Può essere installato liberamente su qualsiasi computer per essere utilizzato dai diversi utenti di RCS.

*Vedi "**Componenti architettura distribuita**" alla pagina precedente .*

Continuità della registrazione dei dati

Gli agent inviano i dati raccolti al Collector. Se la comunicazione viene interrotta, la connettività è assente o il Collector non è in funzione, gli agent riescono a memorizzare una quantità di dati definita in attesa del ripristino della connettività. I dati che superano il limite consentito, sono persi.

Se il Carrier non riesce a comunicare con il Master Node (causa disservizio o manutenzione in corso), i dati ricevuti vengono conservati localmente sul Collector, in attesa che il Master Node sia ripristinato. Una volta ripristinato, i dati sono inviati automaticamente.

Reindirizzamento accesso a Collector

La reale funzione del Collector può essere nascosta, in caso di accesso diretto al servizio di raccolta dei dati, mediante un reindirizzamento su pagine non sospette (es.: Google, sito di e-commerce, e così via). Il reindirizzamento avviene tramite una pagina .HTML configurabile.

*Vedi "**File installati al termine dell'installazione**" a pagina 39*

Certificati digitali

Il Master Node utilizza dei certificati digitali HTTPS che garantiscono la sicurezza della comunicazione tra Master Node, Collector, Network Controller e le RCS Console.

Alcuni agent richiedono certificati specifici che devono essere creati e salvati nella cartella \RCS\DB\config\certs.

*Vedi "**File installati al termine dell'installazione**" a pagina 39*

Decodifica dei dati

Il servizio Worker viene installato insieme a ogni Shard e si occupa della decodifica dei dati prima che questi vengano salvati nel database. In caso di database distribuito, ogni Shard ha un proprio worker che accoglie i dati cifrati dal Master Node, li decodifica e li salva sul database. Il carico di lavoro è automaticamente distribuito equamente tra tutti gli Shard facenti parte del cluster.

Differenze tra la versione RCS 8.0 e RCS 7.6

Di seguito le differenze rispetto alla versione RCS 7.6.

Glossario dei termini

RCS v. 7.6	*RCS 8.0 e successive*
Attività	Operation
Agente	Module
Anonymizer chain	Anonymizing chain

RCS v. 7.6	*RCS 8.0 e successive*
Backdoor	Agente
Backdoor Class	Factory
Collection Node (ASP)	Collector
Injection Proxy Appliance (IPA)	Network Injector Appliance
Log Repository (RCSDB)	Master Node e Shard aggiuntivi
Mobile Collection Node (RSSM)	Collector
RCSAnon	Anonymizer

3

Introduzione all'installazione

Presentazione

Introduzione

L'installazione di RCS è una procedura effettuata alla prima installazione o ai successivi aggiornamenti. I file per l'installazione sono disponibili nel CD inserito nella confezione, o scaricabili dal portale di supporto HackingTeam.

Prerequisiti all'installazione

Tutto l'hardware deve essere già installato e funzionante secondo i requisiti di sistema comunicati da HackingTeam al momento della finalizzazione dell'ordine.

*Vedi "**Requisiti minimi di sistema**" a pagina 16*

NOTA: l'installazione di eventuali Network Injector o Anonymizer è opzionale e sarà documentata nei successivi capitoli.

Contenuti

Questa sezione include i seguenti argomenti:

Contenuto della confezione

Contenuto della confezione

RCS viene consegnato in una confezione che include:

- un CD di installazione
- una chiave USB con licenza d'uso
- due chiavi USB di protezione (principale e backup)

Richiede assistenza: tutte le chiavi USB sono fornite di codice identificativo che deve essere comunicato all'assistenza tecnica per tutte le operazioni di sostituzione e aggiornamento software.

Contenuto pacchetto di installazione (CD o sito web)

Il pacchetto di installazione contenuto nel CD o scaricato dal portale di supporto HackingTeam, contiene i seguenti file, dove 'x' è la root del CD:

Cartella	*File contenuti*	*Descrizione*
x:	ChangeLog.pdf	*Note di rilascio*
x:\doc	RCS_*x.x*_Admin_*y.y*_*Lingua*.PDF RCS_*x.x*_Analist_*y.y*_*Lingua*.PDF RCS_ *x.x* _ SysAdmin_*y.y*_*Lingua*.PDF RCS_*x.x*_Technician_*y.y*_*Lingua*.PDF	*Guide all'installazione e all'uso di RCS. Ogni guida è destinata a un ruolo specifico dell'utente.* • *x.x: versione di RCS .* • *y.y: versione della guida.* • *Lingua: lingua di distribuzione.*
x:\setup	AdoberAIRinstaller.exe	*File installazione Adobe AIR*
x:\setup	RCS-version.exe	*File installazione del/dei server di RCS*
x:\setup	RCSconsole-version.air	*File installazione di RCS Console*
x:\setup	RCS-ocr-version.exe	*File installazione modulo OCR (facoltativo)*

Chiave USB con licenza d'uso

Nella confezione è presente una chiave USB contenente il file di licenza abbinato alla versione di RCS consegnata.

Il file viene richiesto all'installazione e agli aggiornamenti del software. È possibile copiarlo dalla chiave USB su qualsiasi altro supporto.

Chiavi USB di protezione

Nella confezione sono contenute due chiavi di protezione: una principale, già associata alla licenza contenuta nella chiave USB di licenza, e una di backup, pronta per essere attivata nel caso la chiave principale smettesse di funzionare.

IMPORTANTE: la chiave di protezione deve essere sempre collegata al server (in architettura distribuita al Master Node) per permette il funzionamento di tutti i servizi RCS. La disconnessione della chiave comporta un'immediata interruzione di tutti i servizi!

Requisiti minimi di sistema

L'hardware deve essere configurato come indicato dall'assistenza tecnica in fase contrattuale. I computer su cui è installato RCS richiedono le seguenti caratteristiche:

Macchina	*Componente*	*Requisito*
Server front end e back end	Sistema operativo	*Microsoft Windows Server 2008 R2 Standard (English)*
Computer per RCS Console	Sistema operativo	*Microsoft Windows o Apple Mac OS X.*
	Browser	*Firefox 11* *IE 9* *Chrome*
VPS per Anonymizer	Sistema operativo	*Linux CentOS 6*
Network Injector (Appliance o Tactical)	Sistema operativo	*Fornito da HackingTeam*

Porte da aprire nel firewall

In caso di installazione di un firewall tra i componenti dei server RCS, occorre aprire le seguenti porte TCP per permettere la comunicazione tra i servizi:

Dal...	*Al...*	*Porta da aprire*
Anonymizer	Collector	80
Collector	Master Node	443

Dal...	*Al...*	*Porta da aprire*
Collector	esterno	tutte
Carrier	Master Node/Shard	442
Master Node	Collector	80
Network Controller	esterno	443
Console	Master Node	443, 444

Procedure dell'Amministratore di Sistema

Introduzione

Di seguito le procedure tipiche dell'Amministratore di Sistema con un rimando ai capitoli interessati.

Procedure

Installare RCS e configurarne i componenti

Di seguito la procedura per installare i server, le console, gli Shard e Collector aggiuntivi e dei componenti opzionali Anonymizer e Network Injector:

Passo	*Azione*
1	Predisporre l'ambiente di installazione. *Vedi "**Introduzione all'installazione**" a pagina 14 .*
2	Installare il server RCS (in architettura All-In-One o distribuita). *Vedi "**Installazione di RCS**" a pagina 19 .*
3	Installare le RCS Console. *Vedi "**Installazione RCS Console** " a pagina 33 .*
4	(facoltativo) Installare un modulo OCR. *Vedi "**Installazione modulo OCR**" a pagina 36*  *Richiede assistenza: per l'installazione di altri moduli RCS contattare l'assistenza tecnica Hacking Team.*
5	(opzionale) Installare database Shard e Collector aggiuntivi. *Vedi "**Installazione componenti aggiuntivi in architettura distribuita**" a pagina 60 .*

Passo	*Azione*
6	(opzionale) Installare e configurare gli Anonymizer. *Vedi "**Installazione e configurazione degli Anonymizer**" a pagina 42*
7	(opzionale) Installare i Network Injector. *Vedi "**Cose da sapere su Network Injector Appliance**" a pagina 44 .* *Vedi "**Cose da sapere su Tactical Network Injector**" a pagina 51 .*

Mantenere e aggiornare il sistema

Di seguito i rimandi ai capitoli per mantenere le performance e aggiornare il sistema:

- *Vedi "**Manutenzione ordinaria e aggiornamenti software**" a pagina 67 .*
- *Vedi "**Modifica alla configurazione di Master Node e Collector**" a pagina 75 .*
- *Vedi "**Risoluzione dei problemi**" a pagina 80 .*

Monitorare il sistema

Di seguito i rimandi ai capitoli per il monitoraggio del sistema:

- *Vedi "**RCS Console per l'Amministratore di Sistema**" a pagina 90*

4

Installazione di RCS

Presentazione

Introduzione

L'installazione di RCS prevede di intervenire su diversi server locali e remoti.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sull'installazione di RCS

Privilegi di accesso

RCS è stato progettato per garantire la massima sicurezza dei server e dei dati raccolti. Per raggiungere questo obiettivo sono stati definiti quattro ruoli distinti che corrispondono tipicamente alle figure professionali che possono accedere al sistema:

- Amministratore di sistema: responsabile esclusivo dell'installazione hardware e software e dei backup
- Amministratore: responsabile di tutti gli accessi al sistema, delle indagini e degli obiettivi dell'indagine
- Tecnico: responsabile della configurazione e dell'installazione degli agenti di intercettazione
- Analista: responsabile dell'analisi dei dati

Suggerimento: ad un utente è possibile assegnare più ruoli, per esempio un Amministratore può anche avere i privilegi del Tecnico.

Utente admin e utente Amministratore di sistema

In fase di installazione viene creato un utente speciale con nome "admin", in possesso di tutti i privilegi (amministratore di sistema, amministratore, tecnico e analista), che dovrà essere utilizzato per tutte le funzioni di modifica configurazione e accesso a RCS Console.

Questo utente deve essere utilizzato solo per questo scopo. Subito dopo aver completato l'installazione è suggeribile creare, in base alla propria struttura organizzativa, uno o più utenti con i privilegi previsti.

IMPORTANTE: per convenzione, in questo manuale ci riferiamo all'utente admin chiamandolo comunque Amministratore di Sistema, anche se in possesso di tutti i privilegi.

Installazione server RCS in architettura All-in-One

Introduzione

L'installazione del server RCS in architettura All-in-One installa tutti i componenti del server sullo stesso computer.

RCS Console verrà installata con una procedura a parte.

*Vedi "**Installazione RCS Console** " a pagina 33*

Prerequisiti all'installazione

Prima di avviare l'installazione del/dei server RCS sono necessari:

- il nome o indirizzo IP del/dei server su cui si sta installando RCS
- il file licenza, presente sulla chiave USB fornita nella confezione consegnata, o su altro supporto se scaricata da Internet.
- la chiave USB di protezione, fornita nella confezione.
- in caso di firewall aprire le porte per il corretto funzionamento dei servizi. *Vedi "**Porte da aprire nel firewall**" a pagina 16* .

Sequenza di installazione

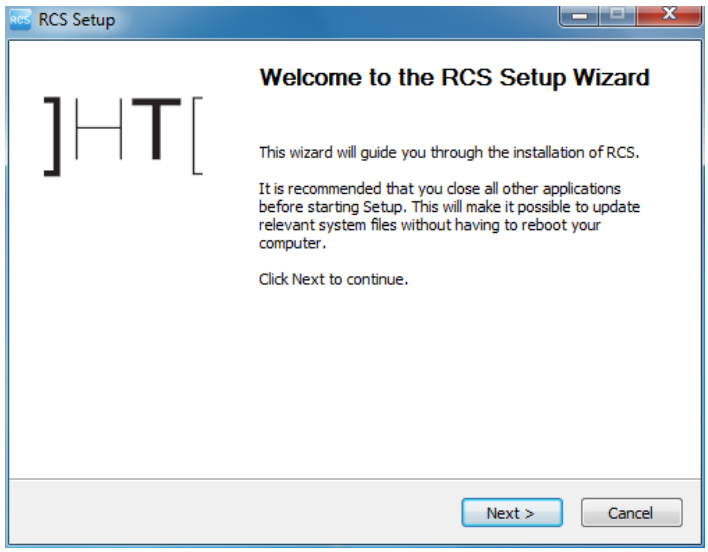
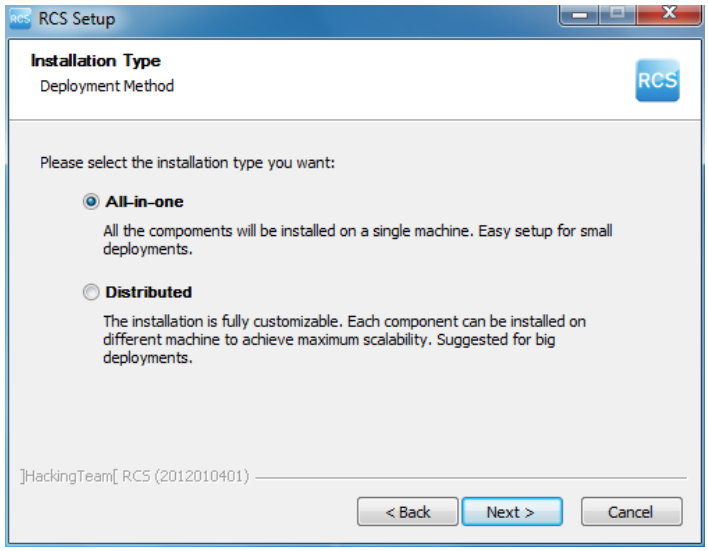
Di seguito la sequenza completa d'installazione in architettura All-in-One:

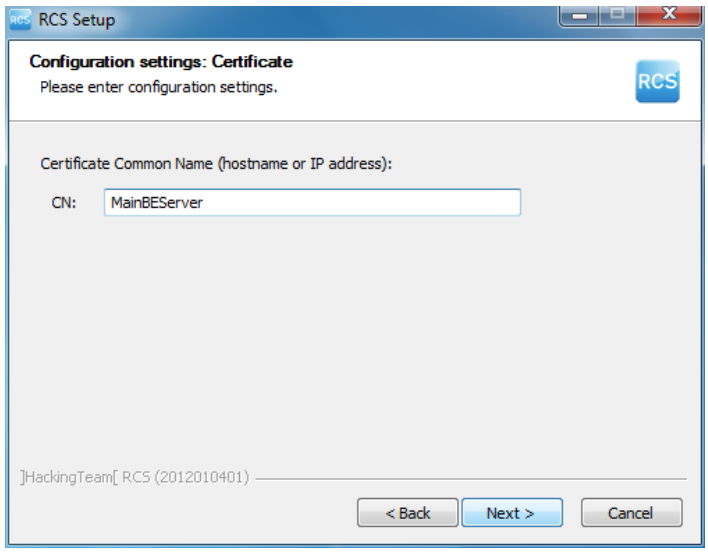
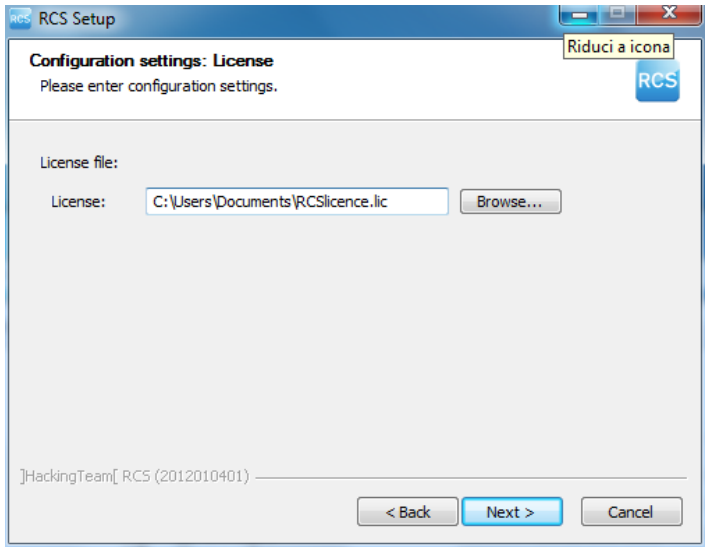
Passo	*Azione*	*Macchina*
1	Preparare quanto indicato in *Prerequisiti all'installazione*.	-
2	Installare RCS.	*server*
3	Verificare l'avviamento dei servizi.	*server*
4	Verificare il log di installazione.	*server*
5	Installare RCS Console.	*server o altro computer*
6	Configurare la cartella di backup su un'unità esterna.	*server*

Installazione

Per installare il server in architettura All-in-One:

Passi	*Risultato*
1. Inserire la chiave di protezione principale.	-

Passi	*Risultato*
2. Inserire il CD con il pacchetto di installazione. Eseguire il file RCS-version.exe nella cartella x:\setup compare la prima finestra del wizard. 3. Fare clic su **Next.**	
4. Selezionare **All-in-One.** 5. Fare clic su **Next.**	

Passi	*Risultato*
6. Inserire il nome o indirizzo IP del server su cui si sta installando il software e che verrà indicato alla login della RCS Console (es.: **RCSserver**). IMPORTANTE: il nome e indirizzo IP devono essere univoci. 7. Fare clic su **Next.**	
8. Selezionare il file della licenza. 9. Fare clic su **Next.**	
10. Inserire la password dell'amministratore di sistema. 11. Fare clic su **Next**: l'installazione viene avviata.	-

NOTA: se per qualche anomalia, è necessario cambiare il nome o indirizzo IP del server, successivamente all'installazione *vedi "Modifica alla configurazione di Master Node" a pagina 77 .*

Verifica dell'avviamento dei servizi

Controllare che tutti i servizi RCS siano presenti e avviati. Se i servizi non si sono avviati è necessario avviarli manualmente.

IMPORTANTE: il Collector accetta connessioni solo se il firewall di Windows è attivo.

Vedi "Elenco dei servizi RCS avviati" a pagina 32

Verifica dei log di installazione

Nel caso di malfunzionamenti durante l'installazione, è necessario consultare i log ed eventualmente inviarli all'assistenza tecnica.

Vedi "I log di sistema" a pagina 82

Verificare gli indirizzi IP

Per verificare tutti gli indirizzi, aprire RCS Console, sezione **System**, **Frontend**: nello schema compare l'indirizzo del server (Collector).*Vedi "Installazione e configurazione degli Anonymizer" a pagina 42*

Disinstallazione

È possibile disinstallare RCS direttamente dal Pannello di Controllo di Windows.

PRUDENZA: La disinstallazione del server RCS causa la perdita di tutti i dati nel frattempo memorizzati. Per operare correttamente provvedere a fare il backup dei dati.
Vedi "Gestione dei backup" a pagina 107

Installazione server RCS in architettura distribuita

Introduzione

L'installazione in architettura distribuita installa tipicamente i componenti su due o più server: un server per l'ambiente front end per la raccolta dei dati e la gestione delle entità esterne e un server per l'ambiente back end, per l'elaborazione e il salvataggio dei dati.

Richiede assistenza: l'architettura distribuita permette diverse espansioni. Verificare con l'assistenza tecnica HackingTeam.

NOTA: RCS Console verrà installata con una procedura a parte, sullo stesso server o su altro computer remoto.

Prerequisiti all'installazione

Prima di avviare l'installazione del/dei server RCS sono necessari:

- il nome o indirizzo IP del/dei server su cui si sta installando RCS
- il file licenza, presente sulla chiave USB fornita nella confezione consegnata, o su altro supporto se scaricata da Internet.
- la chiave USB di protezione, fornita nella confezione.
- in caso di firewall aprire le porte per il corretto funzionamento dei servizi. *Vedi "**Porte da aprire nel firewall**" a pagina 16* .

Sequenza di installazione

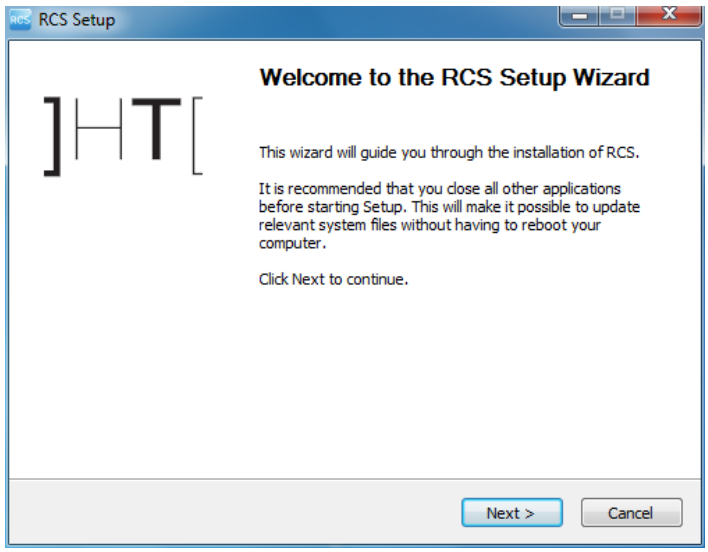
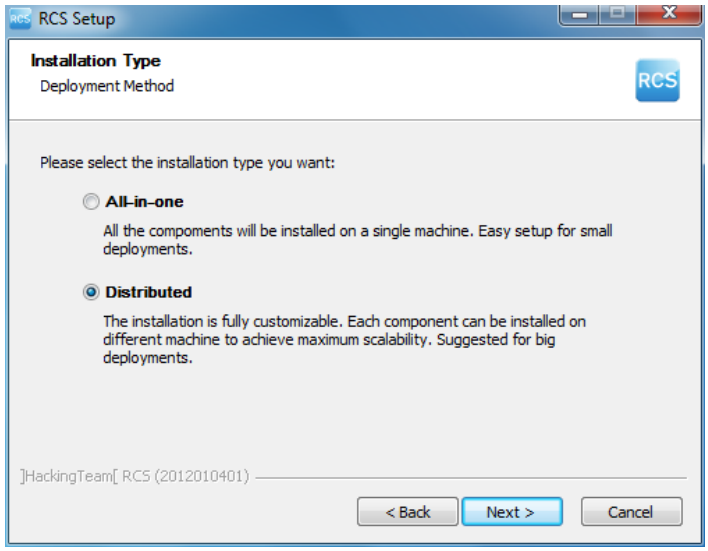
Di seguito la sequenza completa d'installazione in architettura distribuita:

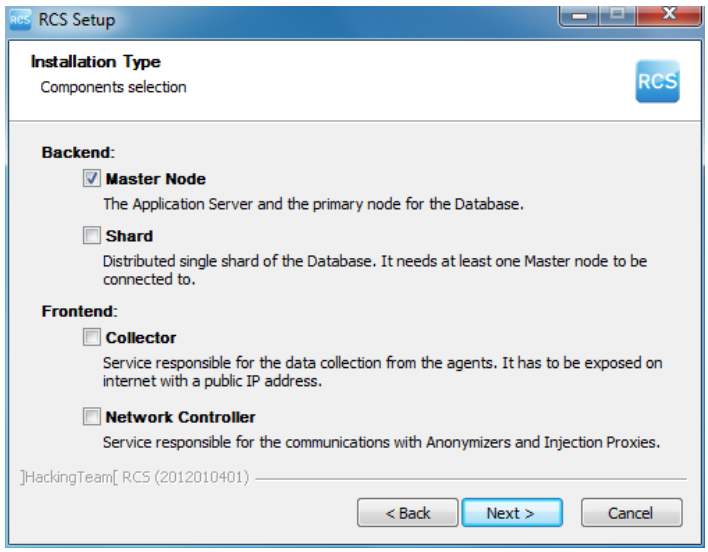
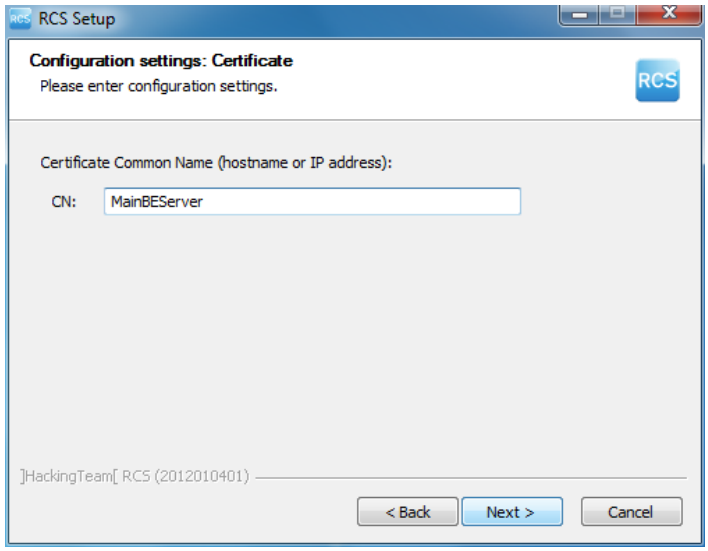
Passo	*Azione*	*Macchina*
1	Preparare quanto indicato in *Prerequisiti all'installazione.*	-
2	Installare il Master Node.	*server in ambiente back end*
3	Verificare i log di installazione.	
4	Verificare l'avviamento dei servizi del Master Node.	
5	Installare Collector e Network Controller.	*server in ambiente front end*
6	Verificare i log di installazione.	
7	Verificare reindirizzamento del Collector.	*stesso server o altro computer*
8	Installare RCS Console.	*server in ambiente back end o altro computer*
9	Configurare la cartella di backup su un'unità esterna.	*server in ambiente back end*

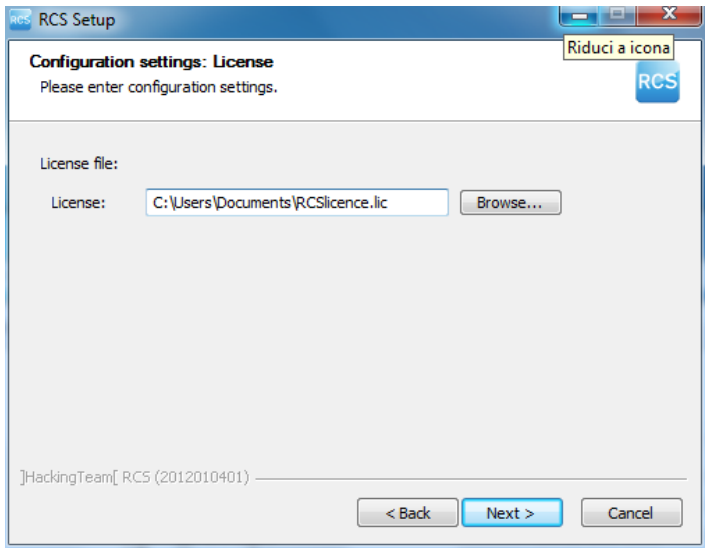
Installazione del Master Node

Per installare il Master Node sul server in ambiente back end:

Passi	*Risultato*
1. Inserire la chiave di protezione principale.	-

Passi	*Risultato*
2. Inserire il CD con il pacchetto di installazione. Eseguire il file RCS-version.exe nella cartella x:\setup: compare la prima finestra del wizard. 3. Fare clic su **Next.**	
4. Selezionare **Distributed.** 5. Fare clic su **Next.**	

Passi	*Risultato*
6. Selezionare **Master Node.** 7. Fare clic su **Next.**	
8. Inserire il nome o indirizzo IP del server su cui state installando il software e che verrà indicato alla login della RCS Console (es.: RCSMasterNode). IMPORTANTE: il nome e indirizzo IP devono essere univoci. 9. Fare clic su **Next.**	

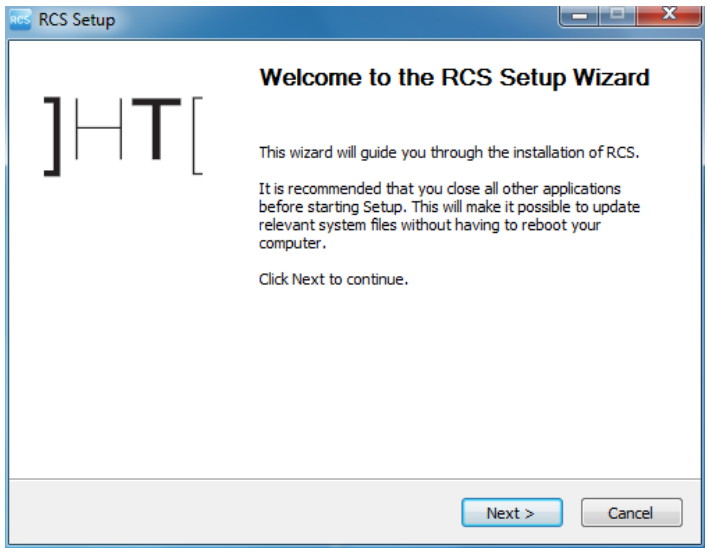
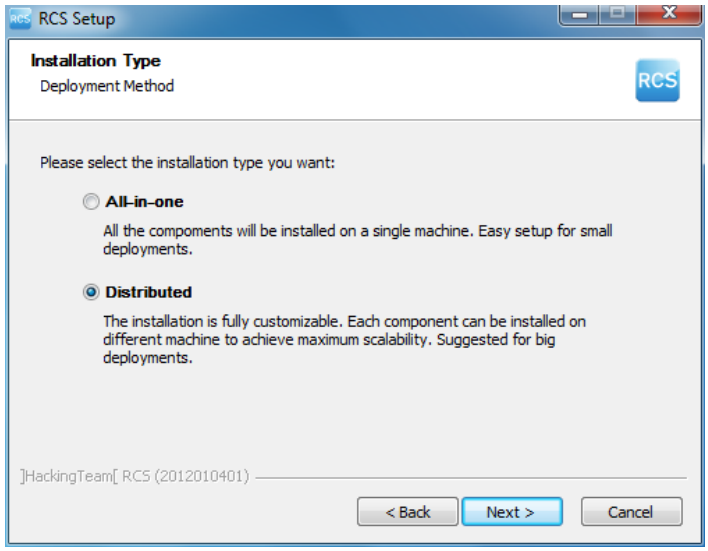
Passi	*Risultato*
10. Selezionare il file della licenza. 11. Fare clic su **Next.**	
12. Inserire la password dell'amministratore di sistema.	
13. Fare clic su **Next**: al termine dell'installazione i servizi si avviano e sono pronti alla ricezione dei dati e alla comunicazione con RCS Console.	-

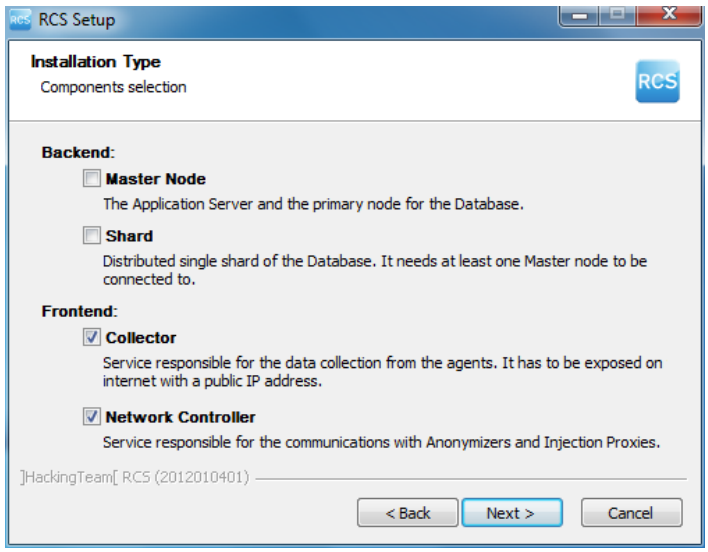
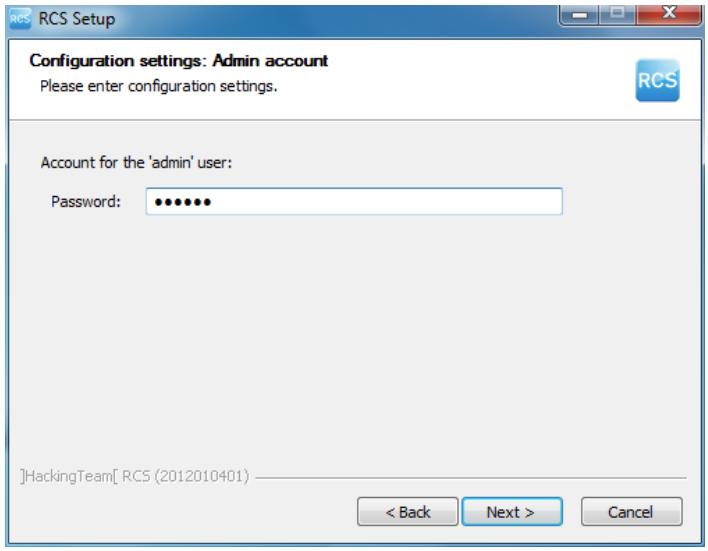
NOTA: se per qualche anomalia, è necessario cambiare il nome o indirizzo IP del server, successivamente all'installazione *vedi "**Modifica alla configurazione di Master Node**" a pagina 77* .

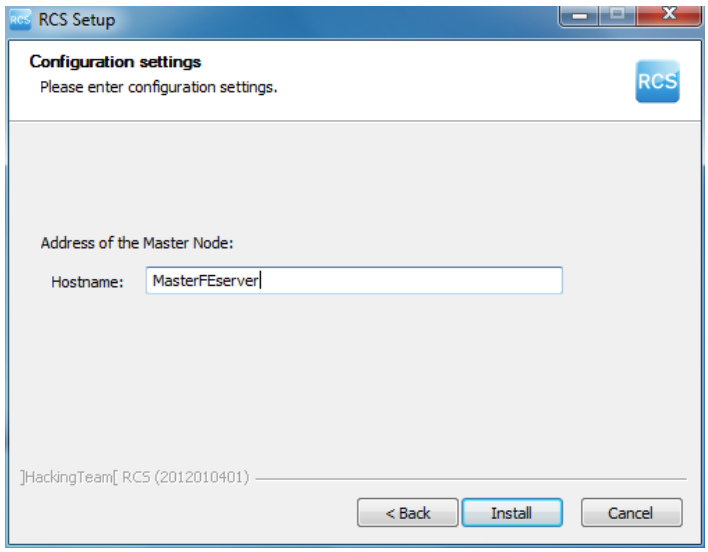
Installazione del Collector e del Network Controller

Per installare il/i Collector e il/i Network Controller in ambiente front end:

Passi	*Risultato*
1. Inserire la chiave di protezione principale.	-

Passi	*Risultato*
2. Inserire il CD con il pacchetto di installazione. Eseguire il file RCS-version.exe nella cartella x:\setup: compare la prima finestra del wizard. 3. Fare clic su **Next.**	
4. Selezionare **Distributed.** 5. Fare clic su **Next.**	

Passi	*Risultato*
6. Selezionare **Collector** e **Network Controller.** NOTA: il servizio Carrier è installato automaticamente con il servizio Controller. 7. Fare clic su **Next.**	
8. Inserire la password dell'amministratore di sistema indicata nell'installazione del Master Node. 9. Fare clic su **Next**: l'installazione viene avviata.	

Passi	*Risultato*
10. Inserire il nome o indirizzo IP del server del Master Node (es.: **RCSMasterNode**) 11. Fare clic su **Install**: al termine dell'installazione i servizi si avviano e cercano di comunicare con Master Node. Il server in ambiente back end è protetto e qualsiasi accesso esterno è reindirizzato.	

Verifica dell'avviamento dei servizi

Controllare che tutti i servizi RCS siano presenti e avviati. Se i servizi non si sono avviati è necessario avviarli manualmente.

IMPORTANTE: il Collector accetta connessioni solo se il firewall di Windows è attivo.

Vedi "Elenco dei servizi RCS avviati" alla pagina successiva

Verifica del reindirizzamento del Collector

Per verificare se le l'installazione del Collector è andata a buon fine:

Se	*Allora*
sul server	• aprire un browser • digitare `localhost` • **Risultato**: il browser deve essere reindirizzato su Google.
sul altro computer	• aprire un browser • digitare `http://Nome o Indirizzo IP server di front end`. • **Risultato**: il browser deve essere reindirizzato su Google.

Suggerimento: è possibile modificare il reindirizzamento o creare una pagina personalizzata. Per farlo modificare la pagina `decoy.html`.

Vedi "File installati al termine dell'installazione" a pagina 39

Verifica dei log di installazione

Nel caso di malfunzionamenti durante l'installazione, è necessario consultare i log ed eventualmente inviarli all'assistenza tecnica.

*Vedi "**I log di sistema**" a pagina 82*

Verificare gli indirizzi IP

Per verificare tutti gli indirizzi, aprire RCS Console, sezione **System**, **Frontend**: nello schema compaiono gli indirizzi dei Collector. *Vedi "**Installazione e configurazione degli Anonymizer**" a pagina 42*

Disinstallazione

È possibile disinstallare RCS direttamente dal Pannello di Controllo di Windows.

PRUDENZA: la disinstallazione del Master Node causa la perdita di tutti i dati nel frattempo memorizzati. Per operare correttamente provvedere a fare il backup dei dati. Vedi "Gestione dei backup" a pagina 107 .

NOTA: la disinstallazione degli altri server non mette a rischio i dati memorizzati.

Elenco dei servizi RCS avviati

I servizi RCS compaiono al termine delle varie fasi di installazione. Controllare il loro corretto avviamento è una delle procedure di verifica del completamento dell'installazione.

Di seguito l'elenco dei servizi:

Architettura	*Servizi*	*Server in ambiente*
All-in-One	RCSMasterConfig RCSMasterRouter RCSMasterShard RCSMasterWorker RCSMasterDb RCSCollector RCSCarrier RCSController RCSDB Mongodb	*back end*

Architettura	*Servizi*	*Server in ambiente*
Distribuita	RCSCollector RCSCarrier RCSController	*front end*
	RCSMasterConfig RCSMasterRouter RCSMasterShard RCSMasterWorker RCSMasterDb RCSDB Mongodb	*back end solo con il Master Node*
	RCSWorker RCSShard	*back end con Shard aggiuntivi*

NOTA: Network Controller non compare tra i servizi perché è una configurazione del servizio RCSCollector.

Per saperne di più

Per riavviare eventuali servizi fermi *vedi "**Procedure per riavviamento dei servizi** " a pagina 86* .

Installazione RCS Console

Introduzione

RCS Console è il client preposto a interagire con il Master Node. Viene tipicamente installato sui computer delle sale operative (per ispettori e analisti) e ad uso di tutto il personale coinvolto nell'installazione di RCS.

NOTA: nel caso di architettura All-in-One è possibile installare un RCS Console anche sullo stesso server RCS.

Prerequisiti

Prima di avviare l'installazione di RCS Console è necessario:

Se si sta installando..	*Allora occorre...*
RCS All-in-One	• aver installato il server RCS • preparare il nome o indirizzo IP del server • preparare la password dell'Amministratore di sistema

Se si sta installando..	*Allora occorre...*
RCS Distribuito	• aver installato il/i server RCS • preparare il nome o indirizzo IP del Master Node • preparare la password dell'Amministratore di sistema del Master Node

Sequenza di installazione

La sequenza completa dell'installazione di RCS Console è la seguente:

Passo	*Azione*
1	Installare Adobe AIR.
2	Installare RCS Console.

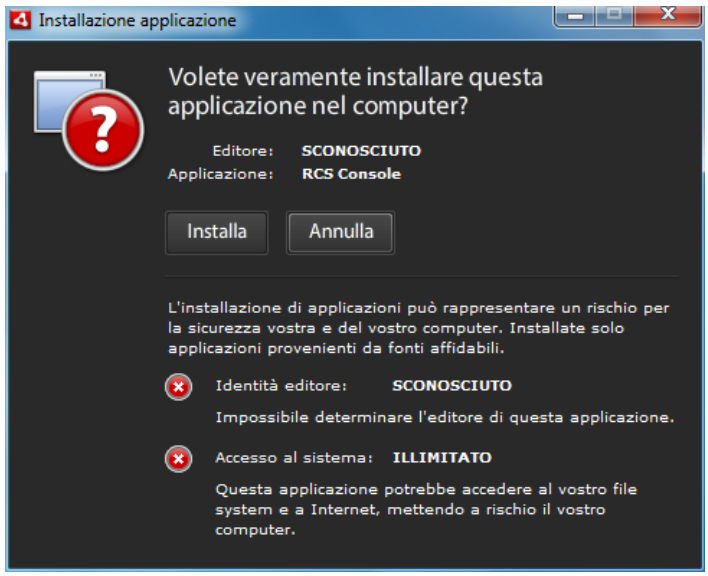
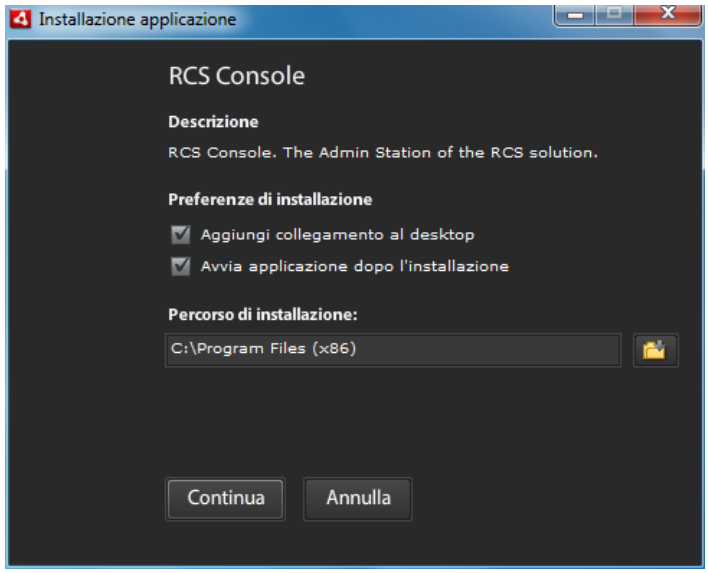
Installazione di Adobe AIR

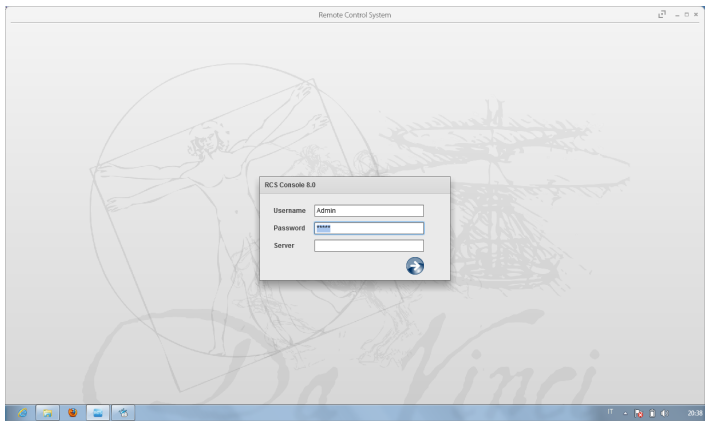
Per installare Adobe AIR:

Passi	*Risultato*
1. Installare Adobe AIR: nessuna icona compare sul desktop al termine dell'installazione.	

Installazione RCS Console

Per installare RCS Console:

Passi	*Risultato*
1. Eseguire il file RCSconsole-version.air 2. Fare clic su **Installa**.	
3. Impostare eventuali preferenze. 4. Fare clic su **Continua**: RCS Console viene installata sul computer.	

Passi	*Risultato*
5. Al termine dell'installazione compare la schermata di login di RCS Console. 6. Inserire le credenziali e il nome/indirizzo IP del server. 7. Fare clic su  .  NOTA: l'Amministratore di sistema eseguirà la login con il nome "admin" e la password scelta in fase di installazione.	

Disinstallazione di RCS Console

È possibile in qualsiasi momento decidere di disinstallare RCS Console, per esempio per destinare il computer ad un altro uso, oppure per rimuovere RCS Console dal server All-in-One e installarla su un computer separato. I dati dei database e le preferenze dell'utente non vengono in alcun modo intaccati.

Creazione dell'utente Amministratore

In fase di installazione di RCS, è necessario creare un utente Amministratore di RCS Console. L'Amministratore avrà il compito di creare tutti gli altri utenti e gestire operation e target. *Vedi "**Destinatari del prodotto e di questa guida**" a pagina 5 .*

Per creare l'utente Amministratore:

Passo	*Azione*
1	Da **RCS Console,** nella sezione **Accounting**, fare clic su **New user** .
2	Compilare i dati richiesti, selezionando il ruolo **Administrator** e fare clic su **Save**: nell'area di lavoro principale il nuovo utente compare con l'icona  . da questo momento l'utente con le credenziali indicate può fare la login in RCS Console e accedere alle funzioni previste.

Installazione modulo OCR

Introduzione

Il modulo OCR è un modulo opzionale che indicizza tutti i contenuti (es.: oltre a tutti i formati dei documenti tradizionali anche immagini, audio, video) per la ricerca full-text.

NOTA: supporta solo caratteri ASCII e la lettura da sinistra verso destra.

Prerequisiti all'installazione

In caso di architettura all-in-one installare il modulo sul Master Node.

In caso di architettura distribuita installare un primo modulo OCR sullo Shard per non appesantire il carico di lavoro del Master Node.

Funzionamento del modulo OCR

Di seguito la descrizione del funzionamento del modulo OCR:

Fase	*Descrizione*
1	Le immagini di evidence di tipo screenshot, in attesa di conversione, sono memorizzate in una coda separata da quella delle evidence in attesa di essere analizzate.
2	Il modulo OCR legge dalla coda l'immagine e la converte in testo. L'operazione può durare da uno a 5-10 secondi in base alla quantità di parole da acquisire.
3	Il testo di ogni immagine viene salvato nel database e indicizzato come full-text.
4	Nel file di log del modulo vengono registrati i tempi di conversione e indicizzazione della singola immagine.
5	Il testo viene reso disponibile per l'Analista sia nella pagina con l'elenco delle evidence per una ricerca nel campo **Info**, sia nella pagina di dettaglio della singola evidence.

Occupazione di spazio nel database dei testi indicizzati

Ogni evidence di tipo screenshot occuperà più spazio nel database perché viene sempre accompagnata dai suoi testi indicizzati. L'aumento di spazio non può essere prevedibile perché dipende sia dalla quantità di screenshot acquisite dall'agent, sia dalla quantità di parole contenute dentro ogni screenshot.

Carico di lavoro di un modulo OCR

Il modulo OCR occupa parecchia CPU durante la conversione di una screenshot, ma viene eseguito con una priorità inferiore rispetto agli altri processi.

L'effetto del carico della CPU si avrà quindi solo con il ritardo con cui il sistema mostra la presenza del testo convertito dell'immagine durante l'analisi delle evidence.

In caso di architettura distribuita si può da subito preferire l'installazione sugli Shard e non sul Master Node, già carico di processi.

Sintomi di carico eccessivo

In fase di acquisizione delle immagini occorre controllare il tempo con cui il testo viene reso disponibile nel dettaglio della singola evidence e controllare i tempi registrati nel log. Se sono giudicati eccessivi e se si ha un altro server libero (es.: quello di un altro database shard o del Master Node) è necessario ripetere l'installazione di un altro modulo OCR.

In questo modo il carico di lavoro sarà suddiviso tra tutti i moduli installati.

Installazione del modulo OCR

Per installare un modulo OCR in ambiente back end:

Passi	*Risultato*
1. Inserire il CD con il pacchetto di installazione. Eseguire il file RCS-ocr-version.exe nella cartella x:\setup: compare la prima finestra del wizard. 2. Fare clic su **Next.**	
3. Procedere con i passaggi successivi fino al completamento dell'installazione: il modulo inizierà a convertire le immagini alla prima ricezione di evidence tipo screenshot.	-

Verificare il corretto funzionamento del modulo OCR

Per verificare se la conversione in testo di un'immagine è troppo lenta, controllare nella pagina di dettaglio della singola evidence il tempo necessario alla comparsa del pulsante .

Disinstallazione

È possibile disinstallare il modulo OCR direttamente dal Pannello di Controllo di Windows.

NOTA: la disinstallazione di un modulo OCR non mette a rischio i testi già convertiti e indicizzati.

File installati al termine dell'installazione

Al termine dell'installazione compariranno diverse cartelle la cui organizzazione varia in base al tipo di architettura e in base al componente opzionale installato:

Cartella	*File contenuti*
backup	La cartella contiene i file con i dati registrati nei database. *Vedi "**Gestione dei backup**" a pagina 107* IMPORTANTE: Il contenuto di questa cartella non deve essere assolutamente toccato. Per salvare i dati di backup su dischi esterni utilizzare la funzione di **Gestione Dischi** di Windows e montare il disco come cartella NTFS, selezionando questa cartella come destinazione. **Percorso**: C:\RCS\DB\backup
bin	La cartella contiene le utility (es.: rcs-db-config) per configurare i componenti di RCS. *Vedi "**Utility per la configurazione**" a pagina 76* **Percorso**: C:\RCS\DB\bin C:\RCS\Collector\bin
certs	La cartella contiene i certificati utilizzati dai vari servizi per accedere al Master Node. Vengono aggiornati quando si riconfigura RCS. *Vedi "**Modifica alla configurazione di Master Node**" a pagina 77* **Percorso**: \RCS\DB\config\certs

Cartella	*File contenuti*
config	La cartella contiene: • pagina `decoy.htm` per il reindirizzamento o per la personalizzazione del landing al server di accessi esterni indesiderati. Può essere personalizzata. *Vedi "**Procedure di manutenzione ordinaria**" a pagina 68* • File di licenza copiato dalla chiave USB. • Export.zip: file contenente i fogli di stile da personalizzare per l'esportazione delle evidence. **Percorso**: C:\RCS\DB\config C:\RCS\Collector\config
log	File di log dei componenti di RCS. *Vedi "**I log di sistema**" a pagina 82* **Percorso**: C:\RCS\DB\log C:\RCS\Collector\log

5

Installazione componenti opzionali e aggiuntivi

Presentazione

Introduzione

L'installazione di RCS può prevedere l'installazione di ulteriori componenti opzionali e aggiuntivi:

- Network Injector
- Anonymizer
- database Shard
- Collector

Contenuti

Questa sezione include i seguenti argomenti:

Installazione e configurazione degli Anonymizer

Introduzione

L'installazione degli Anonymizer in catena è opzionale e serve a reindirizzare i dati di un gruppo di agent. L'Anonymizer è installato su un server esposto su Internet non ricollegabile al resto dell'infrastruttura, come ad esempio un VPS (Virtual Private Server), noleggiato allo scopo. Una volta installato e configurato, l'Anonymizer comunica il proprio stato al Network Controller ogni 30 secondi.

Prerequisito all'installazione

Per l'installazione degli anonymizer è necessario provvedere al noleggio di un VPS con i requisiti minimi di sistema già definiti in fase contrattuale.

*Vedi "**Requisiti minimi di sistema**" a pagina 16*

Installazione

PRUDENZA: utilizzare il protocollo SSH per tutte le operazioni di installazione, configurazione e trasferimento dati verso le entità remote.

Per installare l'Anonymizer su un server privato:

Passo	*Azione*
1	Da **RCS Console,** nella sezione **System**, fare clic su **Frontend**, **Nuovo Anonymizer**.
2	Compilare i dati richiesti, e fare clic su **Salva.** **Risultato**: l'Anonymizer compare nell'elenco degli Anonymizer con l'icona  . Nella sezione **Monitor** compare un oggetto di monitoraggio per l'Anonymizer inserito.
3	Selezionare l'Anonymizer e trascinarlo in corrispondenza del Collector o in corrispondenza di un altro Anonymizer con cui creare la catena. **Risultato**: l'Anonymizer compare nell'elenco degli Anonymizer con l'icona  .
4	Fare clic su **Download installer**. **Risultato**: il file installer `anon_install.zip` viene generato e salvato sul desktop della console.
5	Collegarsi al server e copiare il file `anon_ install.zip` in una cartella di appoggio del server.

Passo	*Azione*
6	Collegarsi al server, espandere il file e mandare in esecuzione l'installer digitando il comando: `# sh install` **Risultato**: l'Anonymizer viene installato nella cartella/opt/bbproxy del server e si mette in ascolto sulla porta 443.
7	Da **RCS Console,** nella sezione **System**, **Frontend**, selezionare l'Anonymizer e fare clic su **Apply configuration**.

Dati di un Anonymizer

Di seguito la descrizione dei dati dell'Anonymizer selezionato:

Dato	*Descrizione*
Name **Description**	Descrizione libera.
Version	Versione software. Per vedere le versioni software di tutti i componenti vedi la sezione **Monitor**.
Address	Indirizzo IP del VPS dove è stato installato l'Anonymizer.
Port	443. Per vedere le porte da aprire in caso di firewall *vedi "**Porte da aprire nel firewall**" a pagina 16* .
Monitor via NC	Se abilitato, il Network Controller acquisisce lo stato dell'Anonymizer ogni 30 secondi. Se non abilitato, l'Anonymizer funziona regolarmente ma Network Controller non ne verifica lo stato. Da usare per evitare connessioni verso Anonymizer posti in ambienti untrusted.
Log	Ultimi messaggi registrati nei log. Per vedere il contenuto dei file di log *vedi "**I log di sistema**" a pagina 82*

Verifica dell'avviamento

L'Anonymizer invia i propri log al syslog che li gestisce e li salva su file. I file sono salvati normalmente nei seguenti file (in base alla versione del sistema operativo e alla configurazione del servizio syslog):

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

Verifica degli indirizzi IP

Per verificare tutti gli indirizzi degli Anonymizer, avviare **RCS Console**, sezione **System**, **Frontend**: nello schema compaiono gli indirizzi. *Vedi "**Aggiornamento degli Anonymizer**" a pagina 70*

Modifica alla configurazione

Per modificare la configurazione di un Anonymizer:

Passo	*Azione*
1	Nella sezione **System**, **Frontend**, fare clic sull'icona dell'Anonymizer.
2	Modificare i dati richiesti, e fare clic su **Save.** **Risultato**: lo schema viene aggiornato.
3	Verificare lo stato dell'Anonymizer nella sezione **Monitor**.
4	Fare clic su **Apply configuration**. **Risultato**: RCS si collega all'Anonymizer e trasferisce la nuova configurazione.

Disinstallazione

Per disinstallare l'Anonymizer cancellare la cartella /opt/bbproxy nel server privato e rimuovere l'Anonymizer da RCS Console. *Vedi "**Aggiornamento degli Anonymizer**".*

Cose da sapere su Network Injector Appliance

Introduzione

Network Injector Appliance è un server di rete per installazioni in un segmento intra-switch presso un fornitore di servizi Internet.

Tramite il monitoraggio delle connessioni del target, permette di iniettare un agent RCS nelle pagine web visitate o nelle applicazioni o file scaricati dal target.

Network Injector Appliance utilizza come sistema operativo Network Injector - Network Appliance e come software di gestione Appliance Control Center.

NOTA: Network Injector Appliance è fornito già installato e pronto all'uso completo di tutti gli applicativi previsti.

Funzionamento

Network Injector Appliance analizza il traffico del target e, in caso di corrispondenza con le regole configurate, vi inietta gli agent.

RCS interroga Network Injector Appliance ogni 30 secondi per ricevere lo stato e i log e invia le regole di injection.

Funzioni di Appliance Control Center

Il software di gestione Appliance Control Center permette di:

- Abilitare la sincronizzazione con RCS per ricevere le regole di identificazione e di injection aggiornate e inviare log.
- Aggiornare Appliance Control Center con l'ultima versione fornita da RCS Console.
- Identificare automaticamente i dispositivi connessi tramite le regole e infettarli.

Connessioni alla rete

Network Injector Appliance richiede due connessioni alla rete: una per intercettare il traffico del target, l'altra per fare injection degli agent e per comunicare con il server RCS.

Suggerimento: dopo che è stato configurato, Network Injector Appliance è indipendente. È possibile quindi lasciarlo operare senza ulteriore comunicazione col server RCS.

Richiede assistenza: data la peculiarità di Network Injector Appliance, il presente manuale si limita a dare solo le strette indicazioni di connessione, lasciando all'assistenza tecnica tutti quegli aspetti strategici che vengono definiti in fase di start-up e consegna.

Schema di collegamento standard

Schema tipico nel caso di un Access Switch che riesca a instradare i dati verso Network Injector Appliance:

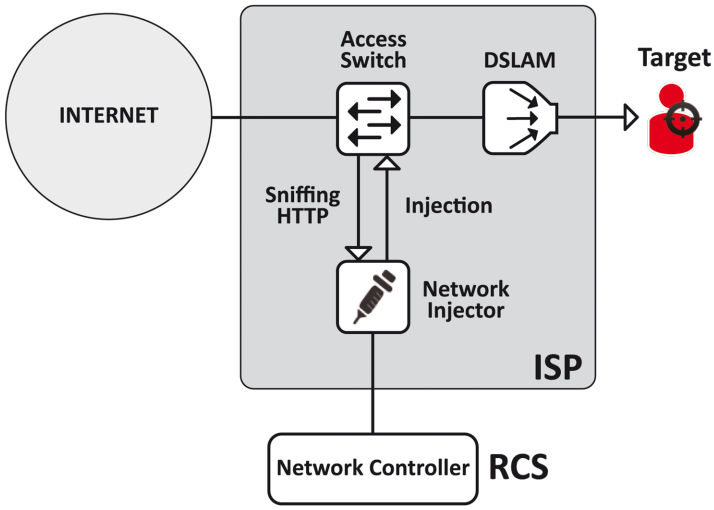


Figura 1: Network Injector Appliance: schema fisico

Schema di collegamento come segmento intra-switch

Schema tipico con dispositivo TAP per potenziare l'instradamento dei dati dell'Access Switch:

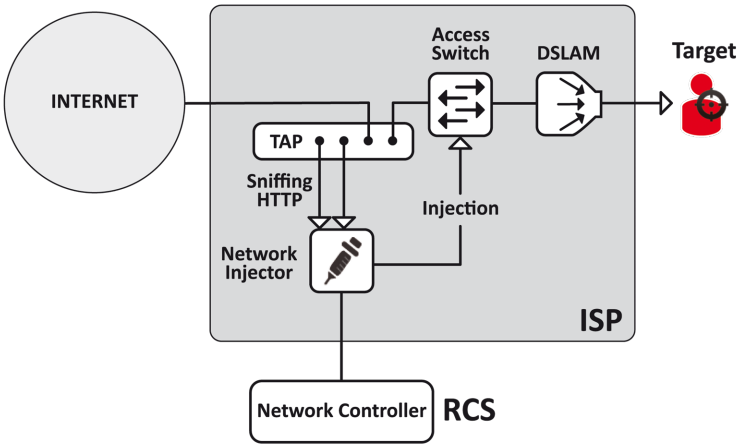


Figura 2: Network Injector Appliance con TAP: schema fisico

Sniffing dei dati tramite TAP, porta SPAN

Un dispositivo TAP è spesso già presente presso il fornitore di servizi Internet, ed è la soluzione più adatta per il monitoraggio del traffico.

L'uso invece della porta SPAN ha i seguenti svantaggi:

- l'utilizzo della CPU dello switch può incrementare sensibilmente a causa dell'uso della porta
- la porta SPAN sullo switch potrebbe essere già utilizzata.

Installazione di Network Injector Appliance

Introduzione

Network Injector Appliance viene fornito con il sistema operativo Network Appliance e il software di gestione Appliance Control Center già installati e configurati. Occorre provvedere alla sua installazione hardware presso il fornitore di servizi Internet e alla sincronizzazione con il server RCS.

Contenuto della confezione

Nella confezione sono presenti una serie di connettori GBIC per il monitoraggio di connessioni a fibra ottica e RJ45.

Sequenza di installazione

Suggerimento: preparare Network Injector Appliance presso i propri uffici prima di installarlo presso il fornitore Internet.

Di seguito la sequenza completa d'installazione:

Passo	*Azione*	*Paragrafo*
1	Collegare Network Injector Appliance alla propria rete.	*"**Connessioni alla rete**" alla pagina successiva*
2	Installare il sistema operativo Network Appliance NOTA: all'acquisto il sistema operativo è già installato.	*"**Installazione e configurazione del sistema operativo**" alla pagina successiva*
3	Sincronizzare il Network Injector al server RCS	*"**Prima sincronizzazione dei Network Injector con il server RCS**" a pagina 58*
4	Verificare lo stato del Network Injector	*"**Verifica dello stato dei Network Injector** " a pagina 59*
5	Trasferire Network Injector Appliance presso il fornitore di servizi Internet e modificare gli indirizzi di rete per abilitare l'accesso a Internet.	-

Descrizione del pannello posteriore

Di seguito il pannello posteriore:

Di seguito l'elenco dei componenti visibili sul pannello:

Area	*Componente*	*Descrizione*
1	**Porte di sniffing**	*Fino a quattro connessioni alle derivazioni del traffico dei target da controllare o fino a due nel caso di apparati in ridondanza.* *NOTA: ammessa la connessione in fibra ottica o in rame.*

Area	*Componente*	*Descrizione*
2	**Scheda madre**	*Uscite standard PC per collegare monitor e tastiera per lanciare l'utility* `sysconf` *o gli eventuali aggiornamenti totali da CD di installazione.* *Vedi "**Procedure di manutenzione ordinaria**" a pagina 68*
3	**Porte di gestione e injection**	***Porta 1**: connessione di rete verso Network Controller per la ricezione dei parametri di configurazione e l'invio dello stato. L'indirizzo deve essere configurato con Network Manager.* ***Porta 2**: connessione di rete per l'injection di traffico.*

Connessioni alla rete

Suggerimento: preparare Network Injector Appliance collegandolo prima alla propria rete e impostando i parametri e provvedendo poi al trasferimento presso il fornitore Internet.

Di seguito la procedura per il collegamento alla rete:

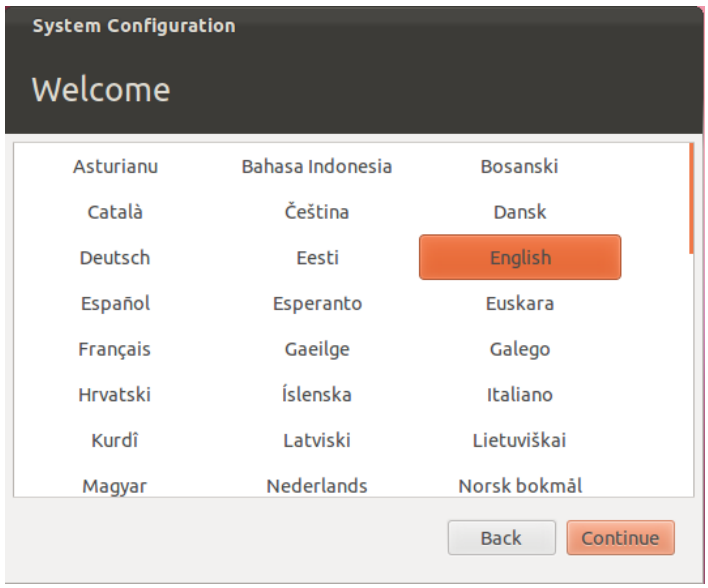
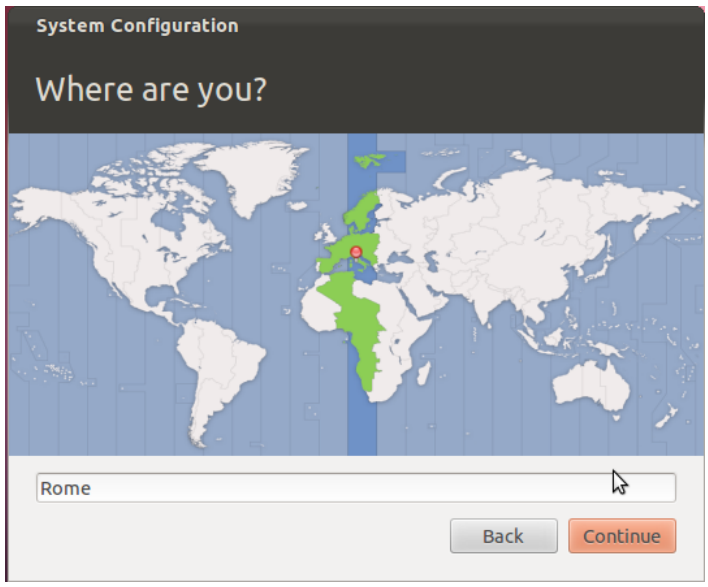
Passi	*Schema*
1. Collegare la derivazione del traffico del target alle porte di sniffing **[1].** IMPORTANTE: in presenza di apparati in ridondanza, collegare ambedue gli apparati.	
2. Collegare le porte di gestione (porta 1) e injection (porta 2) **[3]** alla rete Internet.	
3. Collegare monitor e tastiera **[2].**	

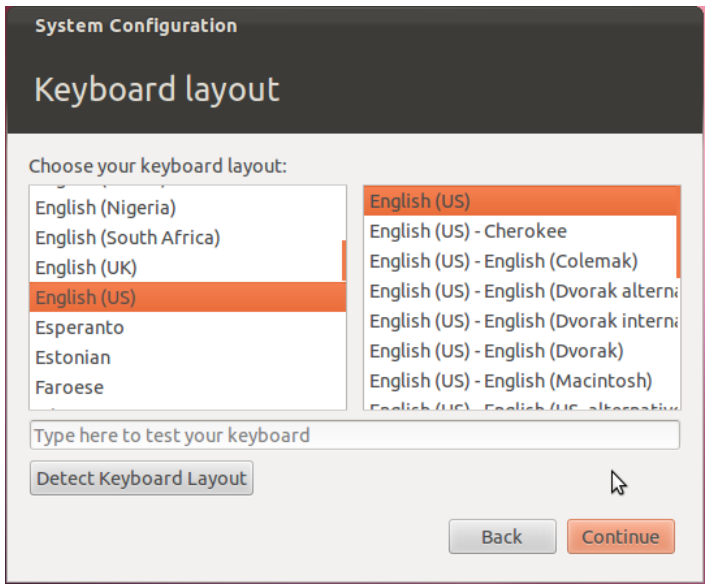
Installazione e configurazione del sistema operativo

Network Injector Appliance è fornito già installato e pronto all'uso completo di tutti gli applicativi previsti. È comunque possibile eseguire l'installazione tramite un disco di ripristino.

Di seguito la procedura:

Passi	*Risultato*
1. Collegare in rete il computer tramite un cavo Ethernet ed inserire il CD di installazione..	-

Passi	*Risultato*
2. Scegliere di installare la versione Network Appliance per server: viene avviata l'installazione del sistema operativo e al termine il computer si spegne. IMPORTANTE: la connessione alla rete Internet deve durare per tutta l'installazione.	-
3. Riavviare il portatile.	-
4. Compare la prima finestra del setup. 5. Selezionare la lingua.	
6. Selezionare il fuso orario appropriato.	

Passi	*Risultato*
7. Viene rilevato il layout della tastiera. Cambiarlo solo se necessario.	
8. Inserire i dati utente: si avvia il setup del sistema operativo.	
9. Al termine dell'installazione del sistema operativo compare la pagina di login standard. Il sistema operativo e il software di gestione Appliance Control Center sono installati sul computer.	-

Modifica dell'indirizzo IP

Se l'indirizzo IP dell'apparato del Network Injector cambia, reinstallare il Network Injector e sincronizzare. *Vedi "**Sequenza di installazione**" a pagina 47 , "**Prima sincronizzazione dei Network Injector con il server RCS**" a pagina 58*

Per verificare gli indirizzi, aprire RCS Console, sezione **System**, **Network Injector** e visualizzare i dati di ogni Network Injector. *Vedi "**Dati dei Network Injector**" a pagina 115 .*

Disinstallazione

Per disinstallare un Network Injector Appliance è sufficiente eliminare l'oggetto in RCS Console e spegnere l'apparato.

*Vedi "**Gestione dei Network Injector**" a pagina 112*

Cose da sapere su Tactical Network Injector

Introduzione

Tactical Network Injector è un computer portatile per installazioni tattiche in LAN o reti WiFi.

Tactical Network Injector utilizza come sistema operativo Network Injector - Tactical Device e come software di gestione Tactical Control Center.

NOTA: Tactical Network Injector è fornito già installato e pronto all'uso, completo di cifratura del disco e di tutti gli applicativi previsti.

Funzioni del Tactical Control Center

Tactical Control Center permette di:

- Abilitare la sincronizzazione con RCS per ricevere le regole di identificazione e di injection aggiornate e inviare log.
- Aggiornare Tactical Control Center con l'ultima versione fornita da RCS Console.
- Identificare automaticamente i dispositivi connessi tramite le regole e infettarli.
- Identificare manualmente i dispositivi connessi tramite le regole e infettarli.
- Fare il cracking delle password di reti WiFi protette.
- Simulare una rete WiFi per attirare i dispositivi target.

Connessioni alla rete

Tactical Network Injector richiede due connessioni alla rete: una per intercettare il traffico del target, l'altra per fare injection degli agent e per comunicare con il server RCS.

Suggerimento: dopo che è stato configurato, Tactical Network Injector è indipendente. È necessaria la connessione verso Internet per ottenere da RCS le regole aggiornate e inviare i log (sincronizzazione).

Schema di collegamento standard

Schema tipico in ambiente WiFi dove il Tactical Network Injector è connesso alla stessa rete WiFi dei dispositivi del target.

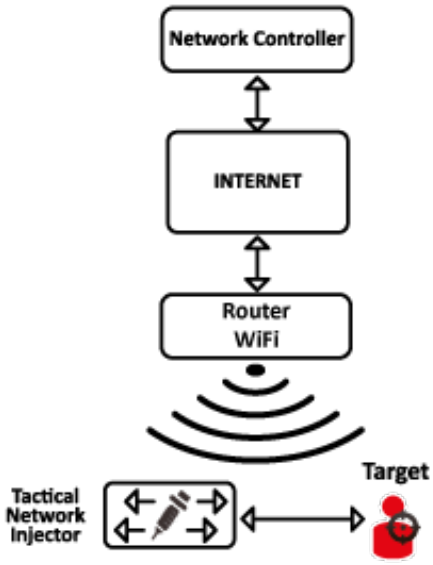


Figura 1: Tactical Network Injector: schema di collegamento standard

Schema di collegamento in emulazione Access Point

Schema tipico in ambiente WiFi dove il Tactical Network Injector emula l'access point di reti WiFi aperte per attrarre i dispositivi target:

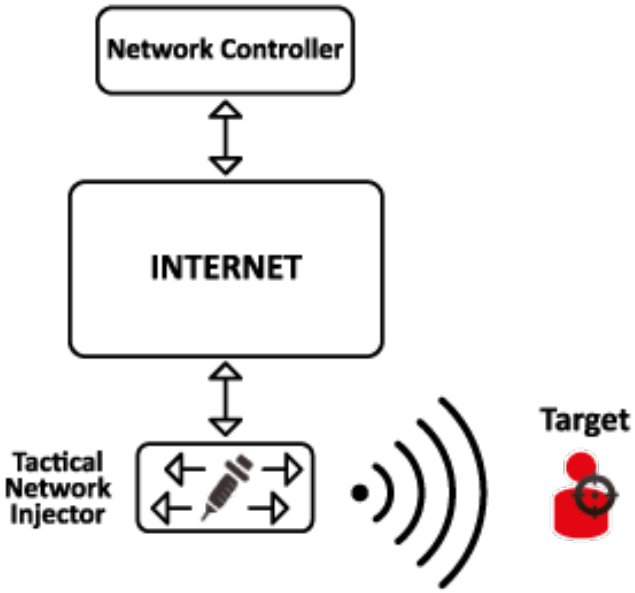


Figura 2: Tactical Network Injector: schema in emulazione di access point

Installazione di Tactical Network Injector

Introduzione

Tactical Network Injector viene fornito con il sistema operativo Tactical Device e il software di gestione Tactical Control Center già installati e configurati. Occorre sincronizzarlo al server RCS.

IMPORTANTE: l'installazione richiede dei file di autenticazione presenti in Master Node, e la sincronizzazione richiede la creazione del Network Injector su RCS Console. Organizzarsi opportunamente se l'installazione avviene lontano dal centro operativo.

Contenuto della confezione

Nella confezione sono presenti un portatile e un CD di installazione.

Sequenza di installazione

Di seguito la sequenza completa d'installazione:

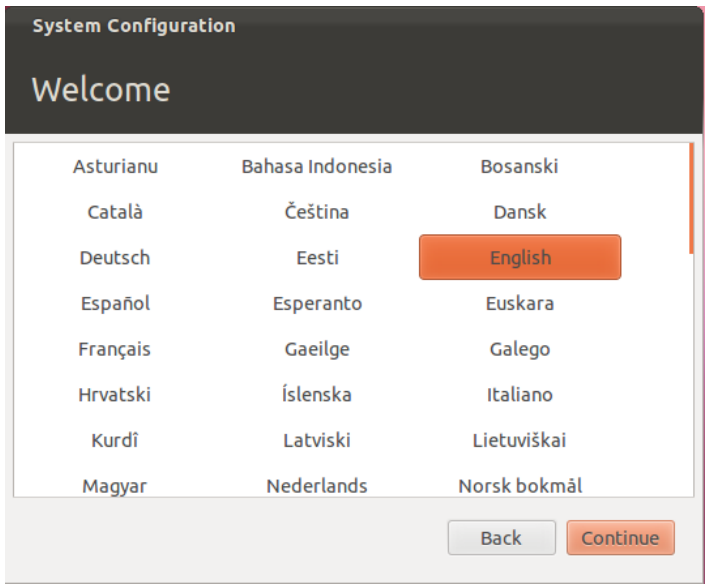
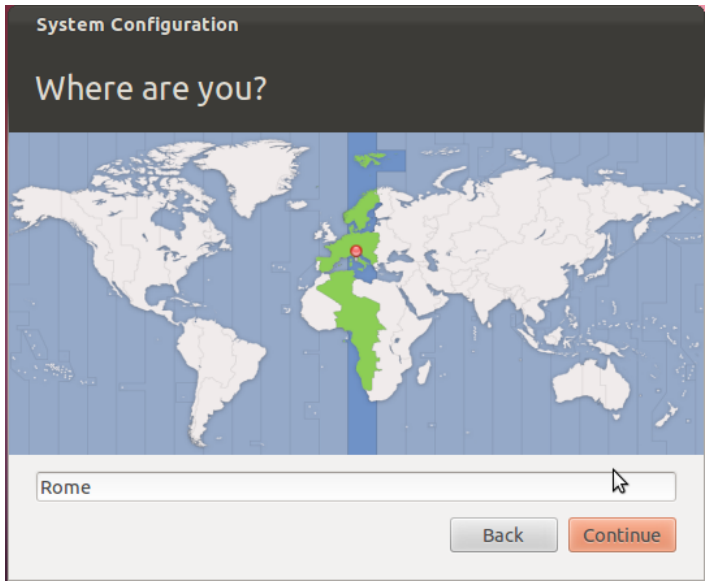
Passo	*Azione*	*Paragrafo*
1	Installare il sistema operativo Tactical Device NOTA: all'acquisto il sistema operativo è già installato.	*"Installazione e configurazione del sistema operativo" nel seguito*
2	Sincronizzare il Network Injector al server RCS	*"Prima sincronizzazione dei Network Injector con il server RCS" a pagina 58*
3	Verificare lo stato del Network Injector	*"Verifica dello stato dei Network Injector " a pagina 59*

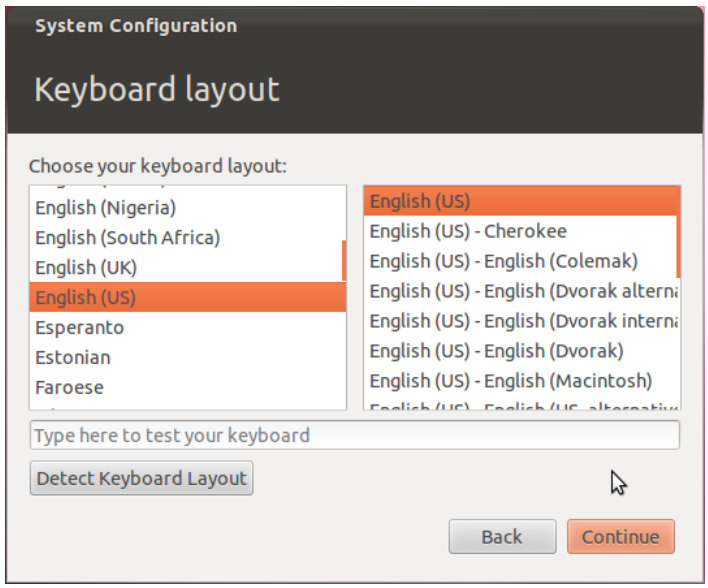
Installazione e configurazione del sistema operativo

Tactical Network Injector è fornito già installato e pronto all'uso completo di tutti gli applicativi previsti. È comunque possibile eseguire l'installazione tramite un disco di ripristino.

Di seguito la procedura:

Passi	*Risultato*
1. Collegare in rete il portatile tramite un cavo Ethernet ed inserire il CD di installazione	-
2. Scegliere di installare la versione Tactical Device per pc portatili: viene avviata l'installazione del sistema operativo e al termine il computer si spegne. IMPORTANTE: la connessione alla rete Internet deve durare per tutta l'installazione.	-
3. Riavviare il portatile: inserire la *passphrase* per sbloccare il disco cifrato. Al primo avvio la passphrase è "firstboot".	-

Passi	*Risultato*
4. Compare la prima finestra del setup. 5. Selezionare la lingua.	
6. Selezionare il fuso orario appropriato.	

Passi	*Risultato*
7. Viene rilevato il layout della tastiera. Cambiarlo solo se necessario.	
8. Inserire i dati utente: si avvia il setup del sistema operativo. ATTENZIONE: se si perde la password occorre reinstallare Tactical Network Injector. IMPORTANTE: la password inserita diventa la passphrase di cifratura del disco richiesta a ogni avvio del portatile. La password sarà richiesta anche alla login dell'utente.	
9. Al termine dell'installazione del sistema operativo compare la pagina di login standard. Il sistema operativo e il software di gestione Tactical Control Center sono installati sul portatile.	-

Modifica dell'indirizzo IP

Nel caso in cui l'indirizzo IP dell'apparato del Network Injector cambi, reinstallare il Network Injector ed eseguire la prima sincronizzazione. *Vedi "**Sequenza di installazione**" a pagina 53 , "**Prima sincronizzazione dei Network Injector con il server RCS**" alla pagina successiva*

Per verificare gli indirizzi, aprire RCS Console, sezione **System**, **Network Injector** e visualizzare i dati di ogni Network Injector. *Vedi "**Dati dei Network Injector**" a pagina 115*

Disinstallazione

Per disinstallare Tactical Control Center è sufficiente rimuoverlo dal computer. Per disconnettere un Tactical Network Injector è sufficiente eliminare l'oggetto in RCS Console e spegnere l'apparato.

*Vedi "**Gestione dei Network Injector**" a pagina 112*

Comandi Tactical Control Center e Appliance Control Center

Introduzione

Sono disponibili alcuni comandi da terminale per gestire gli applicativi Tactical Control Center e Appliance Control Center.

NOTA: per eseguire i comandi è necessario possedere i privilegi di Amministratore.

Comandi

Di seguito i comandi disponibili per Tactical Control Center e per Appliance Control Center:

Comando Tactical Control Center	*Comando Appliance Control Center*	*Funzione*
`tactical`	`appliance`	Avvia l'applicativo.
`tactical -d` oppure `tactical --desync`	`appliance -d` oppure `appliance --desync`	Dissocia il sistema dal server RCS con cui è attualmente sincronizzato.
`tactical -l` oppure `tactical --log`	`appliance -l` oppure `appliance --log`	Visualizza i log del processo di infezione in corso. NOTA: la finestra dell'applicativo deve essere aperta.
`tactical -s` oppure `tactical --show-logs`	`appliance -s` oppure `appliance --show-logs`	Visualizza tutti i file di log salvati nel file system.

Comando Tactical Control Center	*Comando Appliance Control Center*	*Funzione*
`tactical - r` oppure `tactical --report`	`appliance - r` oppure `appliance --report`	Crea un report del sistema e lo salva nella cartella Home dell'utente.
`tactical - v` oppure `Tactical --version`	`appliance - v` oppure `appliance --version`	Visualizza la versione dell'applicativo.
`tactical -h` oppure `tactical --help`	`appliance -h` oppure `appliance --help`	Visualizza i comandi disponibili.

Prima sincronizzazione dei Network Injector con il server RCS

Introduzione

La prima sincronizzazione di un Network Injector è necessaria per permettere al tecnico di creare e inviare le regole di sniffing e injection e per inserire l'apparato nel polling di Network Controller. Una volta installato e sincronizzato, Network Injector comunica il proprio stato al Network Controller ogni 30 secondi.

Sincronizzare un Network Injector con il server RCS

Per completare l'installazione di un Network Injector è necessario sincronizzare il Network Injector e il server RCS.

Di seguito la procedura sia per Network Injector Appliance che Tactical Network Injector:

Passo	*Azione*
1	Connettere alla rete il Network Injector e da **Network Manager**, **Connection information** identificare il suo indirizzo IP NOTA: l'indirizzo IP deve essere raggiungibile dal server RCS. Verificare facendo un ping da RCS Collector. Se esiste un firewall tra il server RCS e il Network Injector, aprire la porta 443.
2	Aprire **Appliance Control Center** o **Tactical Control Center** e fare clic su **Config**
3	Da **RCS Console,** nella sezione **System**, **Network Injector** fare clic su , **Nuovo Injector**.
4	Compilare i dati richiesti inserendo nel campo **Address** l'indirizzo IP del Network Injector, e fare clic su **Save** *Vedi "Dati dei Network Injector" a pagina 115* **Risultato**: il Network Injector compare nell'elenco e nella sezione Monitor viene aggiunto il nuovo oggetto da monitorare.

Passo	*Azione*
5	Verificare lo stato del Network Injector nella sezione **Monitor**. *Vedi "**Verifica dello stato dei Network Injector** " nel seguito*

Verifica dello stato dei Network Injector

Introduzione

I Network Injector si sincronizzano con il server RCS per scaricare versioni del software di gestione aggiornate, le regole di identificazione e di injection e contestualmente spedire i loro log.

Dalla RCS Console è possibile monitorare lo stato del Network Injector.

In particolare:

- nella sezione **Monitor**: per individuare i momenti in cui il Network Injector è sincronizzato e quindi disponibile allo scambio di dati.
- nella sezione **System**, **Network Injector**: per visualizzare i log che il Network Injector invia.

Individuare quando il Network Injector è sincronizzato

Di seguito la procedura:

Passo	*Azione*
1	Nella sezione **Monitor**, selezionare la riga corrispondente all'oggetto Network Injector che si vuole analizzare.. Controllare la colonna **Status**: se è presente un segno di spunta verde il Network Injector è sincronizzato. Questa situazione si verifica quando dal software Control Center (Appliance o Tactical): • è stato premuto il pulsante **Config**, l'operatore manualmente si è messo in attesa di regole nuove o aggiornamenti; • è stato premuto il tasto **Start** o comunque è in corso un'infezione. **IMPORTANTE: solo quando il Network Injector è sincronizzato può ricevere da RCS le regole applicate e gli aggiornamenti.**

Visualizzare i log dei Network Injector

Di seguito la procedura :

Passo	*Azione*
1	Nella sezione **System**, **Network Injector**, selezionare il Network Injector che si vuole analizzare, fare doppio clic o fare clic su **Edit** **Risultato**: si apre la finestra con i dati del Network Injector e i log registrati. *Vedi "**Dati dei Network Injector**" a pagina 115* NOTA: i log vengono ricevuti e visualizzati solo se il Network Injector è sincronizzato.

Installazione componenti aggiuntivi in architettura distribuita

Introduzione

L'installazione in architettura distribuita permette di aggiungere database Shard (per grossi volumi di dati) e ulteriori Collector (uno per ogni catena di Anonymizer).

Richiede assistenza: la progettazione dell'architettura distribuita deve essere verificata con l'assistenza tecnica HackingTeam.

Prerequisiti all'installazione di componenti aggiuntivi

Prima di installare i componenti aggiuntivi completare l'installazione del Master Node e del Collector.

*Vedi "**Installazione server RCS in architettura distribuita**" a pagina 24 .*

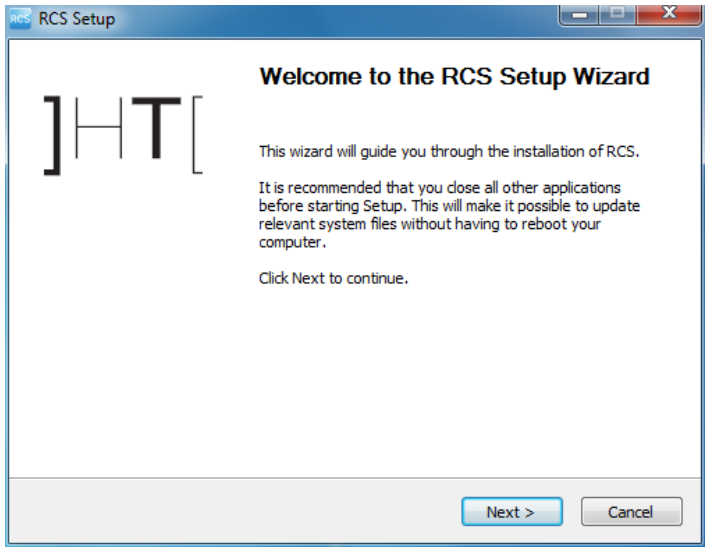
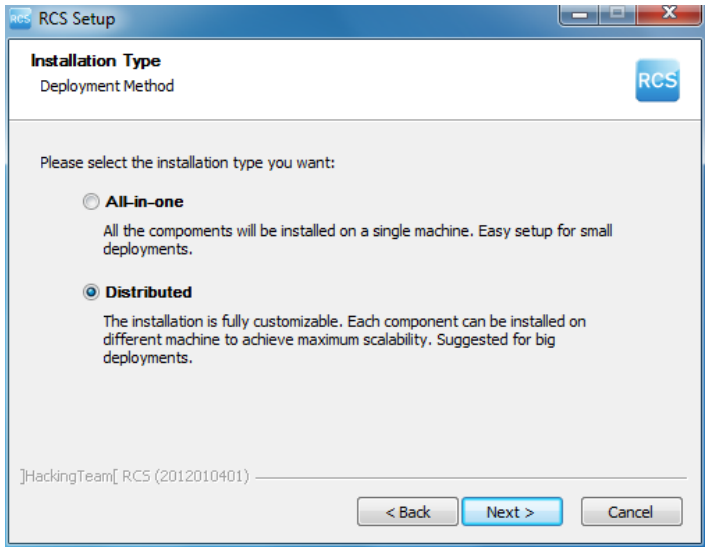
Sequenza di installazione

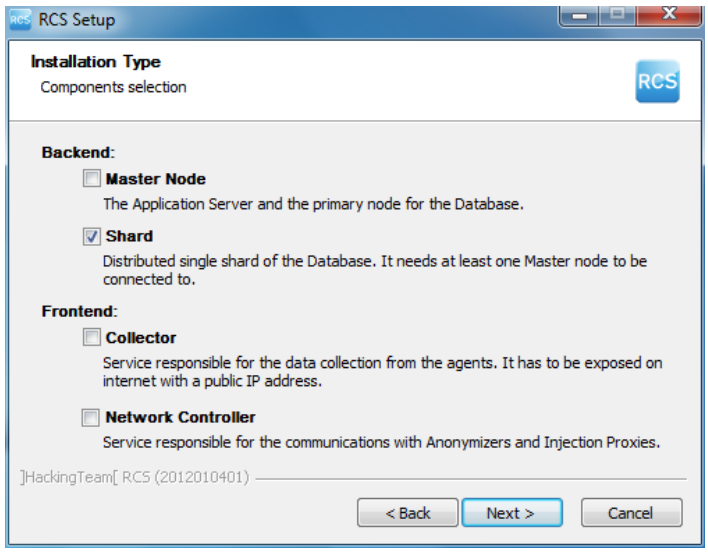
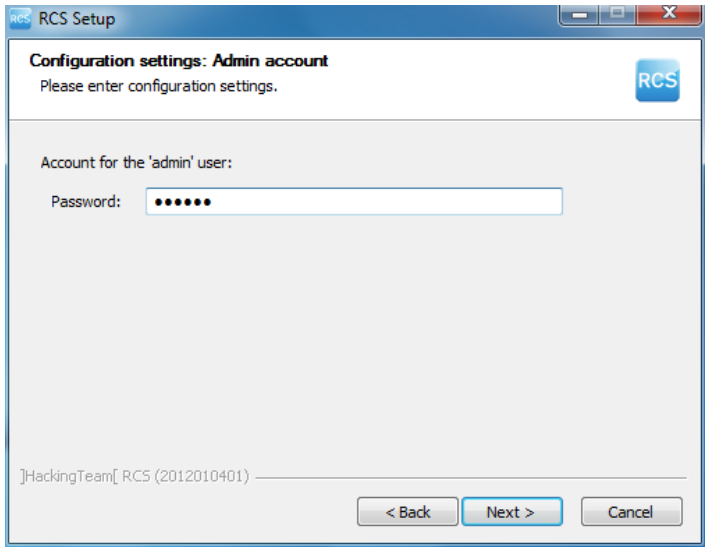
Di seguito la sequenza completa d'installazione dei componenti aggiuntivi:

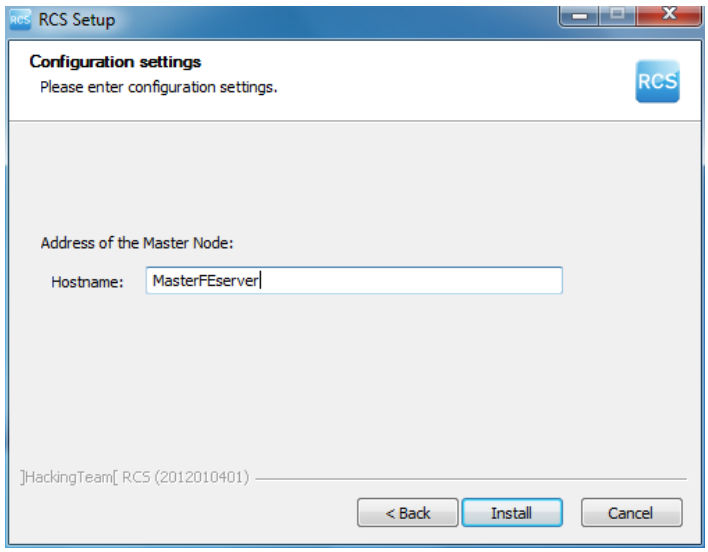
Passo	*Azione*	*Macchina*
1	Preparare quanto indicato in *Prerequisiti all'installazione.*	-
2	Installare i database Shard aggiuntivi.	*server in ambiente back end*
3	Verificare i log di installazione.	
4	Installare i Collector aggiuntivi.	*server in ambiente front end*
5	Verificare i log di installazione.	
6	Verificare reindirizzamenti di ogni Collector.	*stesso server o altro computer*
7	Verificare nella sezione **System**, **Backed** e **Frontend** la presenza degli oggetti installati.	*RCS Console*

Installazione del database Shard aggiuntivo

Per installare un ulteriore database Shard in ambiente back end:

Passi	*Risultato*
1. Inserire il CD con il pacchetto di installazione. Eseguire il file RCS-version.exe nella cartella x:\setup: compare la prima finestra del wizard. 2. Fare clic su **Next.**	
3. Selezionare **Distributed.** 4. Fare clic su **Next.**	

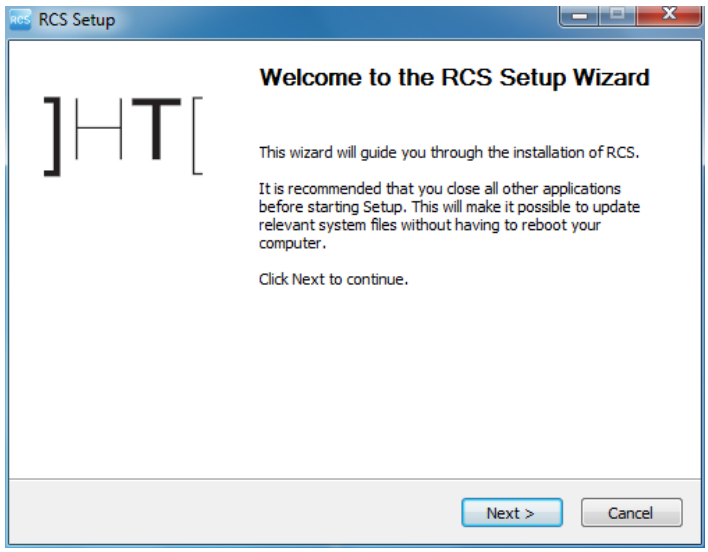
Passi	*Risultato*
5. Selezionare **Shard.** 6. Fare clic su **Next.**	
7. Inserire la password dell'amministratore di sistema. 8. Fare clic su **Next**: al termine dell'installazione i servizi si avviano e sono pronti alla ricezione dei dati e alla comunicazione con RCS Console.	

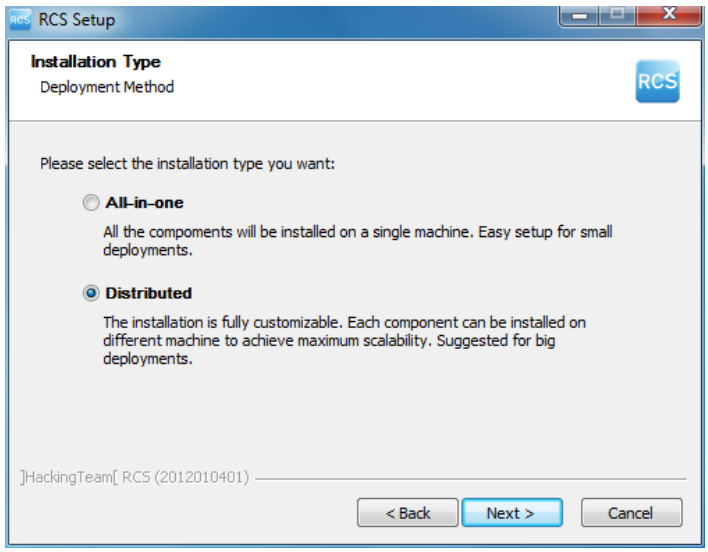
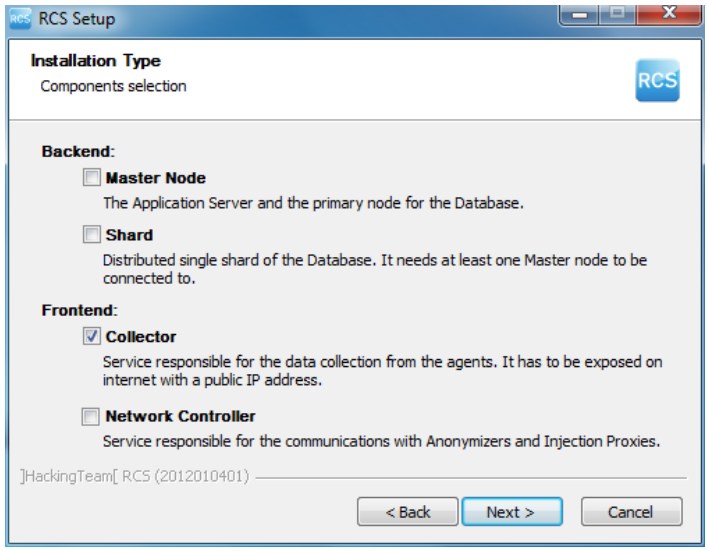
Passi	*Risultato*
9. Inserire il nome o indirizzo IP del server del Master Noder(es.: **RCSMasterNode**) 10. Fare clic su **Install**: al termine dell'installazione i servizi si avviano e cercano di comunicare con Master Node. Il server in ambiente back end è protetto e qualsiasi accesso esterno è reindirizzato.	

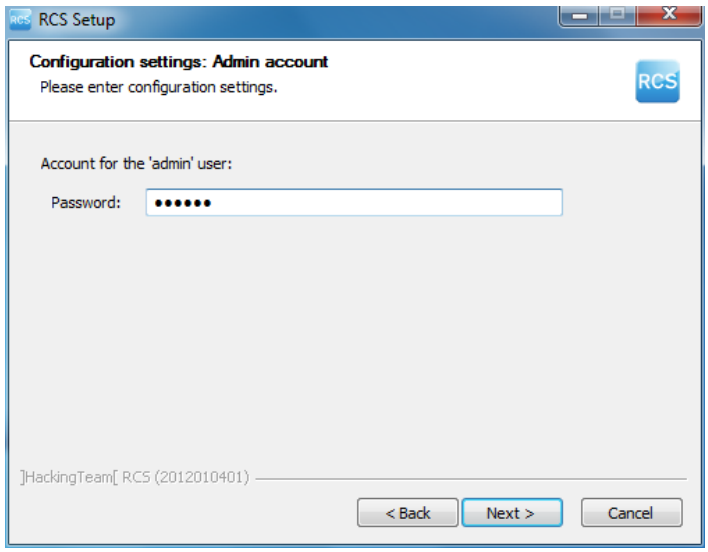
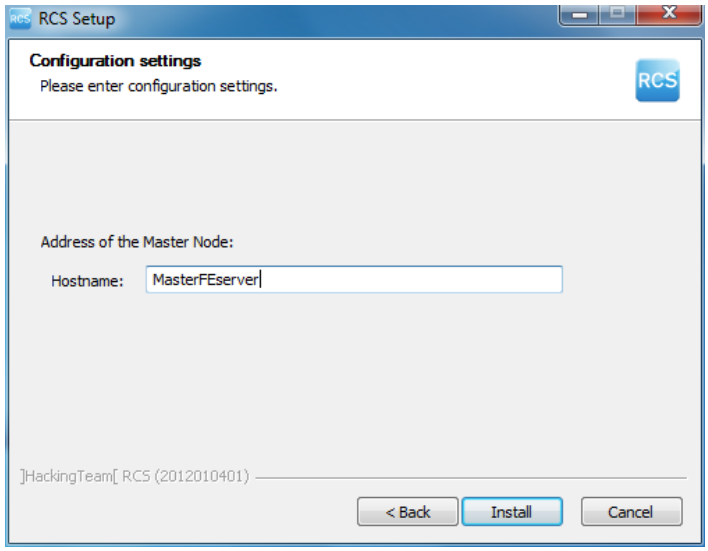
NOTA: se per qualche anomalia, è necessario cambiare il nome o indirizzo IP del server, successivamente all'installazione *vedi "Modifica alla configurazione di Master Node" a pagina 77* .

Installazione di Collector aggiuntivi

Per installare più Collector in ambiente front end:

Passi	*Risultato*
1. Inserire il CD con il pacchetto di installazione. Eseguire il file RCS-version.exe nella cartella x:\setup: compare la prima finestra del wizard. 2. Fare clic su **Next.**	

Passi	*Risultato*
3. Selezionare **Distributed.** 4. Fare clic su **Next.**	
5. Selezionare **Collector.** NOTA: il servizio Carrier è installato automaticamente con il servizio Controller. 6. Fare clic su **Next.**	

Passi	*Risultato*
7. Inserire la password dell'amministratore di sistema indicata nell'installazione del Master Node. 8. Fare clic su **Next**: l'installazione viene avviata.	
9. Inserire il nome o indirizzo IP del server del Master Noder(es.: **RCSMasterNode**) 10. Fare clic su **Install**: al termine dell'installazione i servizi si avviano e cercano di comunicare con Master Node. Il server in ambiente back end è protetto e qualsiasi accesso esterno è reindirizzato.	

Verifica dell'avviamento dei servizi

Controllare che tutti i servizi RCS siano presenti e avviati. Se i servizi non si sono avviati è necessario avviarli manualmente.

IMPORTANTE: il Collector accetta connessioni solo se il firewall di Windows è attivo.

Vedi "Elenco dei servizi RCS avviati" a pagina 32

Verifica del reindirizzamento del Collector

Per verificare se le l'installazione del Collector è andata a buon fine:

Se	*Allora*
sul server	• aprire un browser • digitare `localhost` • **Risultato**: il browser deve essere reindirizzato su Google.
sul altro computer	• aprire un browser • digitare `http://Nome o Indirizzo IP server di front end`. • **Risultato**: il browser deve essere reindirizzato su Google.

Suggerimento: è possibile modificare il reindirizzamento o creare una pagina personalizzata. Per farlo modificare la pagina `decoy.html`.

Vedi "File installati al termine dell'installazione" a pagina 39

Verifica dei log di installazione

Nel caso di malfunzionamenti durante l'installazione, è necessario consultare i log ed eventualmente inviarli all'assistenza tecnica.

Vedi "I log di sistema" a pagina 82

Verificare gli indirizzi IP

Per verificare tutti gli indirizzi, aprire RCS Console, sezione **System**, **Frontend**: nello schema compaiono gli indirizzi dei Collector. *Vedi "Installazione e configurazione degli Anonymizer" a pagina 42*

Disinstallazione

È possibile disinstallare RCS direttamente dal Pannello di Controllo di Windows.

PRUDENZA: la disinstallazione di un database Shard causa la perdita di tutti i dati nel frattempo memorizzati. Per operare correttamente provvedere a fare il backup dei dati. Vedi "Gestione dei backup" a pagina 107 .

NOTA: la disinstallazione di un Collector non mette a rischio i dati memorizzati.

6

Manutenzione ordinaria e aggiornamenti software

Presentazione

Introduzione

La manutenzione ordinaria comprende le operazioni di aggiornamento di RCS e gli interventi programmati o indicati dall'assistenza tecnica per mantenere consistenti le performance del sistema.

ATTENZIONE: la mancata manutenzione può provocare comportamenti non prevedibili del sistema.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sulla manutenzione di RCS

Ricezione degli aggiornamenti

A ogni rilascio software di RCS, l'assistenza tecnica mette a disposizione sul portale di supporto il pacchetto di aggiornamento. Il pacchetto può essere associato ad un nuovo file di licenza, eventualmente richiesto durante la procedura di aggiornamento.

Scaricare il pacchetto e procedere con le procedure di aggiornamento.

Comportamento delle macchine in aggiornamento

Durante l'aggiornamento il normale servizio dei sistemi potrebbe non essere garantito.

Tutti i dati normalmente ricevuti e gestiti dalla macchina in aggiornamento sono mantenuti per il periodo necessario e recuperati automaticamente non appena il sistema diventa nuovamente disponibile.

Procedure di manutenzione ordinaria

Introduzione

Di seguito le procedure suggerite per mantenere elevate le performance del sistema.

ATTENZIONE: la mancata manutenzione può provocare comportamenti non prevedibili del sistema.

Controllo e eliminazione dei file di log

Scopo: controllare la quantità di file di log ed eliminare quelli più vecchi, per evitare l'eccessivo riempimento delle unità disco.

Frequenza suggerita: dipende dalla quantità di agent che si stanno tenendo sotto controllo. Una volta al mese potrebbe essere sufficiente per verificare l'occupazione dei dischi.

Controllo dello spazio disponibile sul disco di backup

Scopo: controllare regolarmente il disco di backup, in base alla quantità e frequenza dei backup previsti in **RCS Console** sezione **System** .

Frequenza suggerita: dipende dalla frequenza e dimensione dei backup.

Aggiornamenti sistemi operativi Linux

Scopo: mantenere sempre aggiornati i sistemi operativi Linux installati sui VPS che ospitano gli Anonymizer e sui Network Injector.

Aggiornamento del server RCS

Prerequisiti all'aggiornamento

PRUDENZA: effettuare un backup completo prima di procedere con l'aggiornamento.
Vedi "Gestione dei backup" a pagina 107

Modalità di aggiornamento

Una volta avviato l'installer, questo identifica i componenti presenti sulla macchina e invita all'aggiornamento automatico. La procedura è quindi identica sia in architettura All-in-One, sia in architettura distribuita.

Aggiornamento del/dei server RCS

IMPORTANTE: la chiave di protezione deve essere sempre inserita nel server.

Per aggiornare RCS ripetere i passaggi seguenti per ogni server:

Passo	*Azione*
1	Avviare il file di installazione `rcs-`*`Versione`*`.exe`: compare l'elenco dei componenti già installati e che saranno automaticamente aggiornati. Fare clic su **Next.**
3	Selezionare il nuovo file di licenza recuperato dal pacchetto di installazione. Fare clic su **Next.**

Aggiornamento di RCS Console

Prerequisiti all'aggiornamento

Nessun dato è salvato nella RCS Console. È quindi possibile aggiornare il software senza alcuna particolare precauzione.

Aggiornamento di RCS Console

La console viene automaticamente aggiornata dal server, se necessario, a seguito di ogni login.

In alternativa è possibile ripetere la procedura di installazione utilizzando i file contenuti nel nuovo pacchetto di installazione.

Vedi "Installazione RCS Console " a pagina 33

Aggiornamento degli Anonymizer

Prerequisiti all'aggiornamento

Nessun dato è salvato negli Anonymizer. È quindi possibile aggiornare il software senza alcuna particolare precauzione.

Aggiornamento degli Anonymizer

Da **RCS Console**, nella sezione **System**, **Frontend** selezionare l' Anonymizer che si vuole aggiornare e fare clic su **Aggiorna**.

IMPORTANTE: mantenere aggiornato il sistema operativo Linux

Se l'aggiornamento non va a buon fine, ripetere la procedura di installazione utilizzando i file contenuti nel nuovo pacchetto di installazione.

*Vedi "**Installazione e configurazione degli Anonymizer**" a pagina 42*

Aggiornamento Network Injector Appliance

Introduzione

Network Injector Appliance può essere aggiornato in tre modi:

- completamente, sistema operativo incluso, *vedi "**Aggiornamento totale di Network Injector Appliance**" nel seguito* .
- parzialmente, salvando i dati, con un'infezione in corso *vedi "**Aggiornamento parziale con infezione in corso** " nella pagina di fronte* .
- parzialmente, salvando i dati, senza infezioni in corso *vedi "**Aggiornamento parziale senza infezione in corso**" nella pagina di fronte*

Aggiornamento totale di Network Injector Appliance

PRUDENZA: l'aggiornamento completo elimina tutti i dati contenuti nella macchina.

Se si è in possesso della versione aggiornata del file .iso, eseguire la seguente procedura per installare l'aggiornamento del sistema operativo:

Passo	*Azione*
1	Inserire il CD di installazione con la nuova versione del sistema operativoe fare il boot da CD: il contenuto del disco viene cancellato e viene reinstallato sia il sistema operativo sia i file relativi al Network Injector. Sono richiesti circa 20 minuti. **IMPORTANTE: scegliere di installare la versione Network Appliance per server.**
2	Riavviare il server: viene chiesta la conferma a procedere. ***PRUDENZA: tutto l'hard disk viene cancellato.*** **Risultato**: Network Injector Appliance viene installato.

Aggiornamento parziale con infezione in corso

Queste sono le fasi per un aggiornamento del software Appliance Control Center quando è in corso un'infezione:

IMPORTANTE: per aggiornare sincronizzare il Network Injector e il server RCS una prima volta. ***Vedi "Prima sincronizzazione dei Network Injector con il server RCS" a pagina 58***

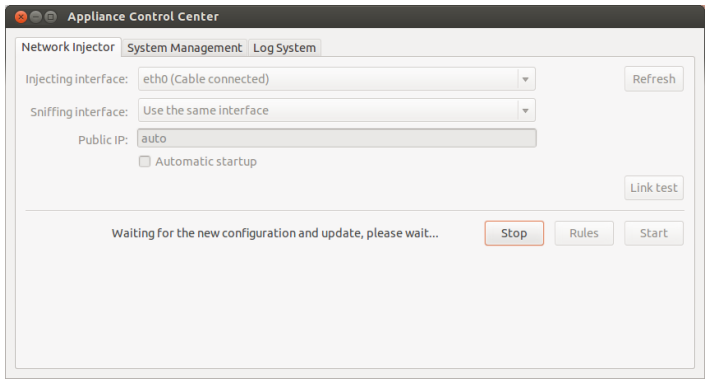
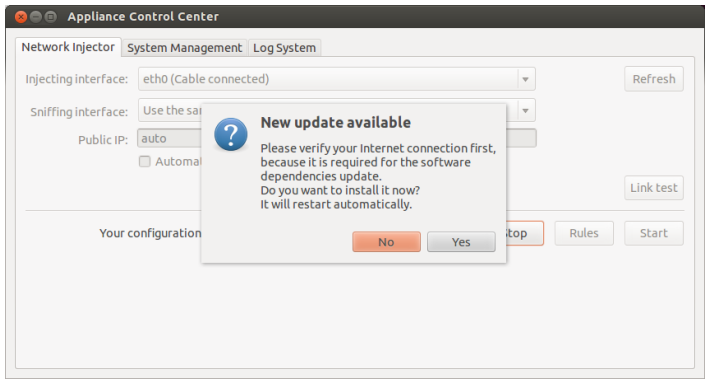
IMPORTANTE: assicurarsi che il dispositivo da aggiornare sia connesso ad Internet per scaricare eventuali pacchetti aggiuntivi necessari all'aggiornamento.

Fase	*Descrizione*
1	Da **RCS Console**, nella sezione **System**, **Network Injector** selezionare il Network Injector che si vuole aggiornare e fare clic su **Aggiorna**.
2	Poiché è in corso un'infezione, il Network Injector riceve subito l'aggiornamento e lo installa automaticamente. NOTA: la fase di installazione inizia solo se la finestra dell'applicativo è chiusa. Ad aggiornamento concluso, verrà fatta ripartire l'infezione con il software aggiornato.

Aggiornamento parziale senza infezione in corso

Queste sono le fasi per un aggiornamento dell'Appliance Control Center quando non è in corso un'infezione:

IMPORTANTE: assicurarsi che il dispositivo da aggiornare sia connesso ad Internet per scaricare eventuali pacchetti aggiuntivi necessari all'aggiornamento.

Passo	*Azione*
1. Da RCS Console, nella sezione **System**, **Network Injector** selezionare il Network Injector che si vuole aggiornare e fare clic su **Aggiorna**	
2. Aprire **Appliance Control Center**	-
3. Nella scheda **Network Injector** fare clic sul pulsante **Config**: la sincronizzazione viene abilitata.	
4. Durante la sincronizzazione, RCS interroga il Network Injector ogni 30 secondi. Allo scadere del primo intervallo compare un messaggio per chiedere il consenso a installare. NOTA: se non si installa l'aggiornamento, questo sarà installato automaticamente alla successivo avvio di un'infezione, oppure, oppure comparirà una richiesta di autorizzazioen a installare al successivo riavvio di Appliance Control Center.	
5. Installare l'aggiornamento.	
6. Ad aggiornamento concluso, Appliance Control Center viene riavviato.	-

Aggiornamento Tactical Network Injector

Introduzione

Tactical Network Injector può essere aggiornato in due modi:

- completamente, sistema operativo incluso, *vedi "**Aggiornamento completo Tactical Network Injector** " nel seguito* .
- parzialmente *vedi "**Aggiornamento parziale** " nel seguito* .

Aggiornamento completo Tactical Network Injector

PRUDENZA: l'aggiornamento completo elimina tutti i dati contenuti nella macchina.

Se si è in possesso della versione aggiornata del file .iso, eseguire la seguente procedura per installare l'aggiornamento del sistema operativo:

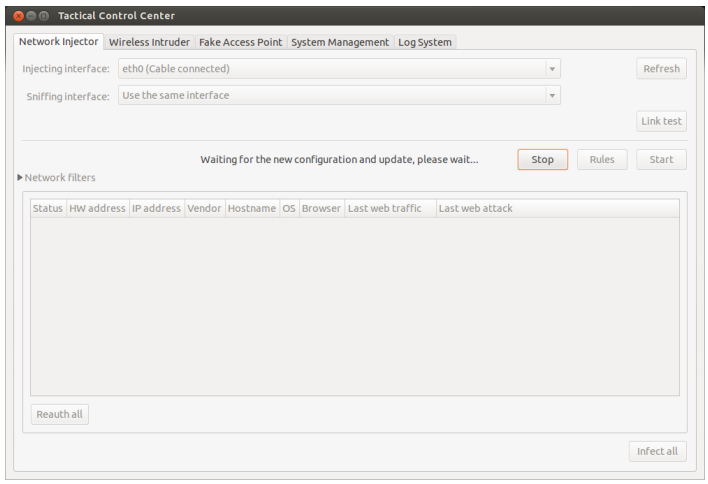
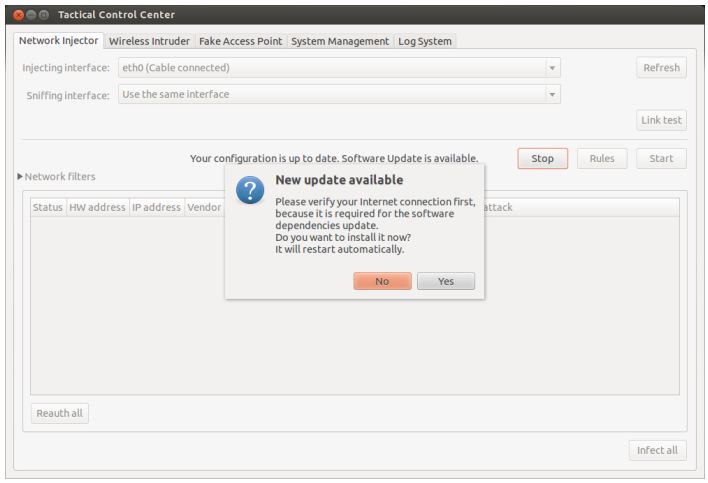
Passo	*Azione*
1	Inserire il CD di installazione con la nuova versione del sistema operativo e e fare il boot da CD: il contenuto del disco viene cancellato e viene reinstallato sia il sistema operativo sia i file relativi al Network Injector. Sono richiesti circa 20 minuti. **IMPORTANTE: scegliere di installare la versione Tactical Device per pc portatili.**
2	Riavviare il server: viene chiesta la conferma a procedere. ***PRUDENZA: tutto l'hard disk viene cancellato.*** **Risultato**: Network Injector Appliance viene installato.

Aggiornamento parziale

Queste sono le fasi per un aggiornamento del Tactical Control Center:

IMPORTANTE: assicurarsi che il dispositivo da aggiornare sia connesso ad Internet per scaricare eventuali pacchetti aggiuntivi necessari all'aggiornamento.

Passo	*Azione*
1. Da **RCS Console**, nella sezione **System**, **Network Injector** selezionare il Network Injector che si vuole aggiornare e fare clic su **Aggiorna.**	
2. Aprire **Tactical Control Center**	-

Passo	*Azione*
3. Nella scheda **Network Injector** fare clic su **Config**: la sincronizzazione viene abilitata.	
4. Durante la sincronizzazione, RCS interroga il Network Injector ogni 30 secondi. Allo scadere del primo intervallo compare un messaggio per chiedere il consenso a installare. NOTA: se non si installa l'aggiornamento comparirà una richiesta di autorizzazione a installare al successivo riavvio di Tactical Control Center.	
5. Installare l'aggiornamento.	
6. Ad aggiornamento concluso, Tactical Control Center viene riavviato.	-

7

Modifica alla configurazione di Master Node e Collector

Presentazione

Introduzione

Successivamente all'installazione, in caso di necessità, è possibile cambiare la configurazione dei componenti.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sulla configurazione

Cosa è possibile modificare

È possibile modificare i seguenti dati inseriti in installazione del Master Node e del Collector:

- il nome/indirizzo IP del Master Node
- password dell'Amministratore di sistema
- la cartella dei backup
- il server di posta in uscita per l'invio delle e-mail di alert

Quando cambiare la configurazione

La necessità di cambiare nome/indirizzo IP o password può sopravvenire per sostituzioni dei server o semplicemente per una digitazione errata dei dati in fase di installazione.

IMPORTANTE: specificare invece una diversa cartella di backup, per esempio su un dispositivo esterno, è una prassi caldamente consigliata per proteggere i dati di backup.

Ordine di modifica della configurazione

Poiché il server dove è installato il Master Node è appunto "master" del sistema, nel modificare l'installazione occorre rispettare questo ordine:

1. Modificare nome/indirizzo IP o password in Master Node
2. Notificare al Collector il nuovo nome/indirizzo IP o password del Master Node

Impostazione server di posta

Il sistema RCS può essere configurato per inviare delle e-mail nel caso di ricezione delle prime prove provenienti da un target. I destinatari delle e-mail devono avere i privilegi di Analista e far parte del gruppo di alerting previsto per quella operation.

Per farlo è necessario riconfigurare il server di posta in uscita impostando i dati del mittente e soprattutto il livello di autenticazione desiderato.

*Vedi "**Utility per la configurazione**" nel seguito*

Utility per la configurazione

Le utility di RCS

La configurazione avviene tramite l'esecuzione di alcune utility eseguite dal prompt dei comandi di Windows nella cartellaC:\RCS\DB\bin o C:\RCS\Collector\bin (in base al tipo di installazione).

Le utility per la configurazione dei componenti sono:

- per Master Node: **rcs-db-config**
- per Collector: **rcs-collector-config**

NOTA: la procedura per la configurazione di RCS in architettura All-in-One, è identica a quella di RCS in architettura distribuita.

Sintassi dei comandi delle utility

La sintassi del comando delle utility è la seguente:

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

Dove:

- -x: opzione selezionata
- AAA: valore inserito

Altre opzioni

Ai fini di una diagnostica tempestiva, l'assistenza tecnica può chiedere di lanciare ulteriori comandi. Per conoscere la sintassi corretta digitare:

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

Richiede assistenza: utilizzare le altre opzioni solo su indicazione dell'assistenza tecnica.

Suggerimento: la sintassi "-x" è la versione abbreviata della sintassi "--xxxxx": "`rcs-db-config -n`" è uguale a "`rcs-db-config --CN`"

Modifica alla configurazione di Master Node

Dalla cartella C:\RCS\DB\bin o C:\RCS\Collector\bin (in base al tipo di installazione) digitare i seguenti comandi:

Per modificare...	***Digitare...***

il nome/indirizzo IP del Master Node	`> rcs-db-config -n Nome -g`
	oppure
	`> rcs-db-config -n IndirizzoIP -g`
	
	Risultato: i certificati vengono aggiornati e compaiono nella cartella \RCS\DB\config\certs. Occorre modificare anche la configurazione di Collector. *Vedi "**Modifica alla configurazione di Collector**" alla pagina successiva*

Per modificare...	*Digitare...*
la password dell'Amministratore di sistema (admin)	`> rcs-db-config -R Password` **Risultato**: i certificati vengono aggiornati e compaiono nella cartella \RCS\DB\config\certs. Occorre modificare anche la configurazione di Collector. *Vedi "**Modifica alla configurazione di Collector**" nel seguito*
la cartella dei backup	`> rcs-db-config -B Cartella` NOTA: "*Cartella*" può essere un percorso relativo alla cartella `RCS\db` o un percorso assoluto. IMPORTANTE: eventuali backup presenti nella cartella configurata in precedenza vanno copiati in quella nuova. **Risultato**: tutti i backup successivi vengono eseguiti nella nuova cartella. Suggerimento: è possibile montare un disco esterno su una cartella NTFS tramite la **Gestione Dischi** di Windows: in questo modo si può usare un disco esterno per i backup.

le impostazioni del server di posta in uscita per le e-mail di alert	`> rcs-db-config -M -server NomeHost:NumeroPorta`
	per impostare il nome del server per la posta in uscita e la porta da usare.
	`> rcs-db-config -from EmailMittente`
	per impostare l'e-mail del mittente per le e-mail di alert (es.: "alert@myplace.com").
	`> rcs-db-config -user NomeUtente`
	Per impostare il nome utente del mittente delle e-mail.
	`> rcs-db-config -pass Password`
	Per impostare la sua password.
	`> rcs-db-config -auth TipoAutenticazione`
	Per impostare il tipo di autenticazione da usare ("plain", "login" oppure "cram_md5").

Modifica alla configurazione di Collector

Dalla cartella C:\RCS\DB\bin o C:\RCS\Collector\bin (in base al tipo di installazione) digitare i seguenti istruzioni:

Al...	*Digitare...*

comunicare il nuovo nome/indirizzo IP del Master Node	`> rcs-collector-config -d Nome -u admin -p Password -t`
	oppure
	`> rcs-collector-config -d IndirizzoIP -u admin -p Password -t`
	  IMPORTANTE: "*Password*" deve corrispondere a quella attiva sul Master Node.
	
	Risultato: i certificati vengono recuperati dalla cartella \RCS\DB\config\certs.

Verifica della configurazione

È possibile tramite le utility RCS, verificare le impostazioni precedenti e attuali della configurazione.

Per verificare i valori precedenti e attuali della configurazione, lanciare le rispettive utility senza alcuna opzione:

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

Esempio output verifica configurazione

Di seguito un esempio di verifica:

```
Current configuration:
{"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

Risoluzione dei problemi

Presentazione

Introduzione

RCS è un sistema dove l'attenzione principale deve essere orientata verso la trasmissione, decodifica e salvataggio costante dei dati raccolti. La progettazione di RCS è orientata a prevenire qualsiasi perdita di dati e a gestire nel più breve tempo possibile il malfunzionamento che si può essere verificato.

Contenuti

Questa sezione include i seguenti argomenti:

Malfunzionamenti possibili

Possibili problemi durante l'installazione

Di seguito un elenco di possibili problemi che possono sorgere durante l'installazione e il rimando alle azioni suggerite:

Se...	*Allora...*
l'installazione non avanza	controllare la presenza della chiave di protezione e inserirla correttamente.
RCS console non riesce a connettersi al server	• Verificare che la login sia stata fatta con il nome dell'Amministratore di sistema, la sua password, e il nome del server dove è stato installato il Master Node. oppure • connettersi al server da browser con "https://*NomeServer*" o "https://*NomeServerBackend*" • Il browser ispeziona il certificato HTTPS e restituisce alcuni indizi per capire cosa è stato errato.

Possibili problemi con i server

Di seguito un elenco di possibili problemi che possono sorgere durante l'uso del prodotto e il rimando alle azioni suggerite:

Se	*E..*	*Allora*
non è possibile connettersi al Master Node	la chiave di protezione è correttamente inserita, ma il servizio Master Node non è avviato	• *controllare lo stato del servizio Master Node.* • *richiedere sostituzione chiave di protezione.*
non arrivano più dati dagli agent	da RCS Console il Collector è funzionante e comunica correttamente	*controllare lo stato del Collector.*
il Master Node non è disponibile	il Collector è funzionante	• *controllare se c'è un aggiornamento in corso* • *controllare il file di log del Collector*
le immagini non vengono convertite in testo	il modulo OCR è installato	*controllare l'effettivo rallentamento nel log del modulo e installare (se in architettura distribuita) un altro modulo OCR.*
il Collector non è disponibile	-	*riavviare il servizio RCScollector.*

Se	*E..*	*Allora*
i dati sono accodati nel Master Node	su RCS Console non compaiono più dati recenti	*controllare lo stato del servizio Worker per il Master Node e per gli altri Shard.*
Network Controller riporta un errore		*Collegarsi alla macchina dove è installato Network Injector o Anonymizer e controllare il file di log.*

Possibili problemi con i backup

Di seguito un elenco di possibili problemi che possono sorgere durante l'esecuzione dei backup e il rimando alle azioni suggerite:

Se	*E..*	*Allora*
lo stato di un backup è **error**	-	controllare lo spazio disponibile su disco e rilanciare manualmente il backup.

Per saperne di più

Per come verificare lo stato dei componenti *vedi "**Procedure di verifica stato componenti**" a pagina 84*

Per riavviare i servizi *Vedi "**Procedure per riavviamento dei servizi** " a pagina 86*

I log di sistema

Introduzione

Ogni componente di RCS genera dei log giornalieri molto utili per analizzare possibili cause di malfunzionamenti o anomalie. L'analisi del contenuto dei file permette di seguire passo passo le operazioni di RCS e comprendere eventuali cause di malfunzionamenti (es.: servizio avviato ma subito fermato, servizio avviato ma con il reindirizzamento dalla pagina deploy.htm non corretto).

Utilità dell'analisi dei log

Di seguito le motivazioni che possono portare all'analisi dei log:

Componente	*Motivazione analisi*
Master Node	Verificare problemi con RCS Console.
Collector	Verificare la ricezione dei dati dagli agent.
Carrier	Verificare l'invio dei dati agli shard e al Master Node.

Componente	*Motivazione analisi*
Modulo OCR	Verificare eventuali rallentamenti nell'indicizzazione dei contenuti estratti.
Modulo Translate	Verificare eventuali rallentamenti nella traduzione dei contenuti.
Network Controller	Se si hanno dubbi sullo stato di Network Injector o Anonymizer.
Network Injector	Verificare le operazioni effettuate.
Anonymizer	Verificare il flusso dati in arrivo dagli agent.

Esempio file di log

Il nome del file di log si presenta con la seguenti sintassi: `*Componente* aaaa-mm-gg.log` (es.: `rcs-dbdb 2012-02-04.log`)

File di log di RCS

Di seguito i file di log generati dai componenti in una installazione completa:

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

AVVERTENZA: l'assenza del file di log denota una installazione incompleta.

Visualizzazione rapida dei log

Nell'installazione di RCS è compresa l'installazione di BareTail, un'applicazione che permette di visualizzare istantaneamente il contenuto di più file di log.

Per attivare BareTail digitare:

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

Contenuto di un file di log

Ogni traccia è identificata da un livello di gravità tra i seguenti:

Livello gravità	*Descrizione*
Fatal	RCS non sta funzionando ed è necessario intervenire (es.: mancanza configurazione, mancanza certificati).
Error	C'è un errore in un componente, ma RCS riesce a garantire la copertura dei servizi principali (es.: Master Node non funzionante).
Debug	(compare solo se abilitato su indicazione dell'assistenza tecnica, aumenta e rendere più dettagliati gli indizi nel log che permettono di risolvere i problemi riscontrati).
Info	Nota informativa.

Procedure di verifica stato componenti

Introduzione

Di seguito le tipiche procedure per verificare lo stato di hardware e software.

Verifica delle licenze installate

Verificare tutte le licenze installate in RCS, aggiornamenti inclusi.

Comando

Nella cartella C:\RCS\DB\bin digitare **rcs-db-license**

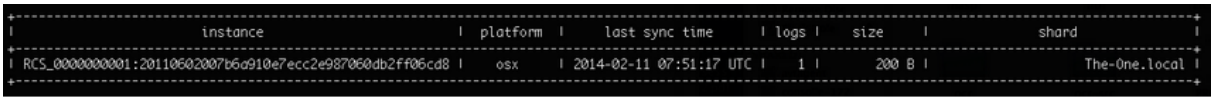
Verifica dello stato del Master Node

Verificare che il Master Node stia comunicando regolarmente i dati ai database tramite i servizi Worker.

Comando

Nella cartella C:\RCS\DB\bin digitare **rcs-db-queue.**

Risultato: di seguito un esempio.



Cosa controllare

Se i valori di *logs* e *size* iniziano a incrementare considerevolmente, ciò può essere causato dal servizio Worker che non sta funzionando. Controllare lo stato di ogni servizio Worker.

Verifica dello stato dei servizi Worker

Verificare che il servizio Worker stia correttamente lavorando per la decodifica e per il salvataggio dei dati nei database.

Comando

Nella cartella C:\RCS\DB\bin digitare **rcs-db-queue.**

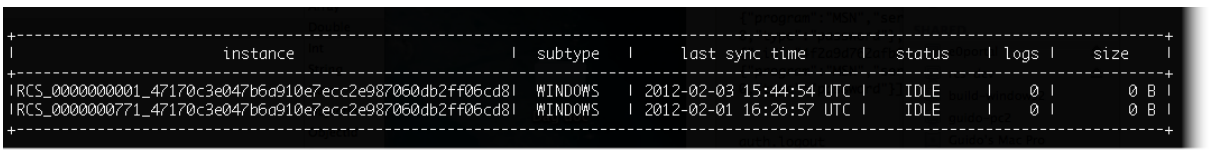
Verifica dello stato degli agent tramite il Collector

Verificare che gli agent stiano comunicando regolarmente il loro stato a RCS tramite il Network Controller e che stiano inviando i loro dati al Collector. Un malfunzionamento persistente del Collector infatti può causare la perdita dei dati degli agent.

Comando

Nella cartella C:\RCS\Collector\bin digitare **rcs-collector-queue**

Risultato: compare il report di status 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 |
+-----------------------------------------------------------------------------------------------------------------------+
```

Cosa controllare

Il valore di *Last sync time* deve essere più recente possibile, compatibilmente con le modalità di sincronizzazione configurate per ciascun agent: un *Last sync time* recente indica che gli agent comunicano correttamente col Collector. Se *Last sync time* non è recente, attendere eventuali altre sincronizzazioni per vedere se viene aggiornato. In alternativa, controllare i log del Collector per vedere se ci sono dei tentativi di sincronizzazione: in questo caso segnalarlo all'assistenza.

Il valore di *logs* deve essere minimo, perché rappresenta i dati memorizzati dal Collector e in attesa di essere inviati al Master Node tramite il Carrier. Se il valore è elevato, significa che il Master Node non è funzionante o non è collegato o il Carrier è malfunzionante. Controllare lo stato del Master Node e i log del Carrier.

Se il problema è la connessione con il Master Node, il numero di log decrementerà non appena la connessione sarà ristabilita.

Verifica dell'avviamento del Network Injector

I log di Network Injector vengono salvati normalmente nella cartella /var/log/syslog.

Per saperne di più

Per la visualizzazione dei log *vedi "I log di sistema" a pagina 82*

Procedure per riavviamento dei servizi

Introduzione

In caso di anomalie, è possibile riavviare i servizi tramite utility invece di utilizzare la funzione Gestione Servizi di Windows.

Di seguito le tipiche procedure per avviare, fermare e riavviare i servizi.

Servizio	*Comandi*
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`

Servizio	*Comandi*
Network Injector	 ***PRUDENZA: utilizzare il protocollo SSH per tutte le operazioni di installazione, configurazione e trasferimento dati verso le entità remote.*** Per riavviare il servizio con la stessa configurazione o una nuova, aprire Appliance Control Center, riconfigurare se necessario e riavviare il servizio attraverso il pulsante **Restart**.

Anonymizer	 ***PRUDENZA: utilizzare il protocollo SSH per tutte le operazioni di installazione, configurazione e trasferimento dati verso le entità remote.***
	
	 Per riavviare il servizio digitare il seguente comando:
	 `# /etc/init.d/bbproxy restart`
	 Per fermare il servizio digitare il seguente comando:
	 `# /etc/init.d/bbproxy stop`
	
	  **IMPORTANTE: la sintassi dei comandi fa riferimento alla versione del sistema operativo Linux CentOS 6**

Procedure di intervento sui componenti hardware

Introduzione

Di seguito le tipiche procedure di intervento da utilizzare in caso di malfunzionamenti di componenti hardware.

Sostituzione chiave di protezione

Se la chiave di protezione principale smette di funzionare, è necessario sostituirla rapidamente con la chiave di protezione di backup, contenuta nella confezione consegnata. Contattare l'assistenza per ottenere un file di licenza compatibile con la chiave di backup.

Di seguito la descrizione della sostituzione e attivazione della nuova chiave:

Fase	*Chi*	*Fa cosa*
1	Il cliente	*Segnala a HackingTeam il guasto.*
2	HackingTeam	*invia un nuovo file di licenza associato alla chiave di protezione di backup.*
3	Il cliente	*sostituisce la chiave principale con quella di backup e avvia la procedura per l'assegnazione del nuovo file di licenza.*
4	Il cliente	*invia la chiave guasta ad HackingTeam.*

Fase	Chi	Fa cosa
5	HackingTeam	*sostituisce la chiave guasta con una nuova chiave di backup e la invia al cliente.*

Sostituzione del Master Node

Di seguito la procedura suggerita:

Passo	Azione
1	Ripristinare una macchina server rieseguendo tutte le operazioni di installazione. *Vedi "**Installazione server RCS in architettura All-in-One**" a pagina 20* oppure *"**Installazione server RCS in architettura distribuita**" a pagina 24*
2	Selezionare il backup più recente (full o metadata). Se il backup più recente è di tipo metadata è possibile ripristinare successivamente il full. Il backup infatti non è distruttivo e integra le informazioni in suo possesso con quelle già presenti. *Vedi "**Cose da sapere sui backup**" a pagina 105*

Sostituzione di uno Shard

Di seguito la procedura suggerita:

Passo	Azione
1	Rieseguire tutta la procedura di installazione. *Vedi "**Installazione server RCS in architettura distribuita**" a pagina 24*
2	Ripristinare l'ultimo backup full. *Vedi "**Gestione dei backup**" a pagina 107*

Sostituzione del Collector/Network Controller

Rieseguire tutta la procedura di installazione.

*Vedi "**Installazione server RCS in architettura distribuita**" a pagina 24*

Sostituzione di un Anonymizer

Rieseguire tutta la procedura di installazione.

*Vedi "**Installazione e configurazione degli Anonymizer**" a pagina 42*

Sostituzione di un Network Injector Appliance

Rieseguire tutta la procedura di installazione.

*Vedi "**Installazione di Network Injector Appliance**" a pagina 46*

Sostituzione di un Tactical Network Injector

Rieseguire tutta la procedura di installazione.

*Vedi "**Installazione di Tactical Network Injector**" a pagina 53*

9

RCS Console per l'Amministratore di Sistema

Presentazione

Ruolo dell'Amministratore di Sistema

Il ruolo dell'*Amministratore di Sistema* è:

- completare l'installazione con la configurazione degli Anonymizer, dei Network Injector, dei Backup
- controllare l'occupazione dei database Shard
- controllare il funzionamento dei Collector, Anonymizer, Network Injector e degli altri componenti del sistema
- aggiornare i componenti di sistema
- gestire i backup
- risolvere eventuali problemi

Funzioni abilitate

Per completare le attività che gli competono, L'Amministratore di Sistema ha accesso alle seguenti funzioni:

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

Contenuti

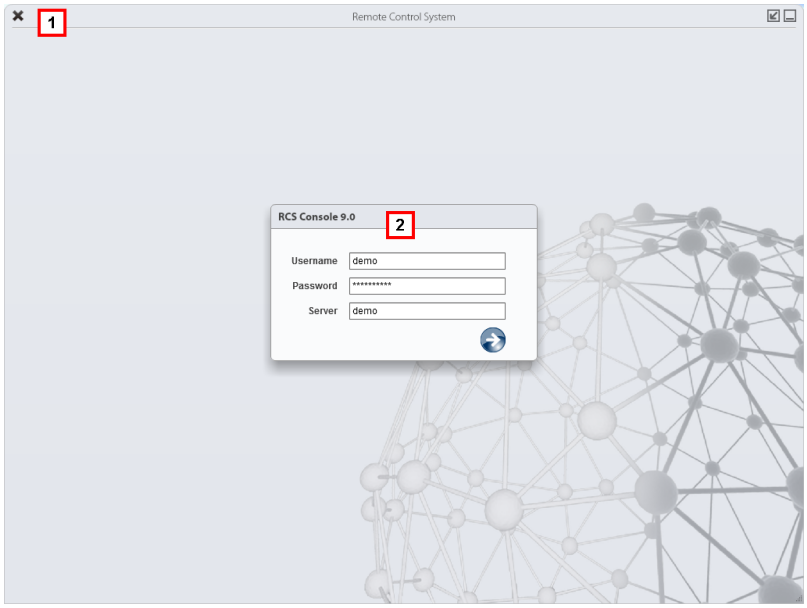
Questa sezione include i seguenti argomenti:

Avvio di RCS Console

All'avvio, RCS Console chiede di inserire le proprie credenziali precedentemente impostate dall'Amministratore.

Come si presenta la pagina di login

Ecco come viene visualizzata la pagina di login:



Area	*Descrizione*
1	Barra del titolo con pulsanti di comando: Chiusura di RCS Console. Pulsante di ingrandimento della finestra. Pulsante di riduzione a icona della finestra.
2	Finestra di dialogo per inserimento delle proprie credenziali.

Accedere a RCS Console

Per accedere alle funzioni di RCS Console:

Passo	*Azione*
1	In **Username** e **Password** inserire le credenziali come assegnate dall'Amministratore.

Passo	*Azione*
2	In **Server** inserire il nome della macchina o l'indirizzo del server cui ci si vuole collegare.
3	Fare clic su  : si presenta l'homepage con i menu abilitati in base ai privilegi del proprio account. *Vedi "**Descrizione della homepage**" nel seguito .*

Descrizione della homepage

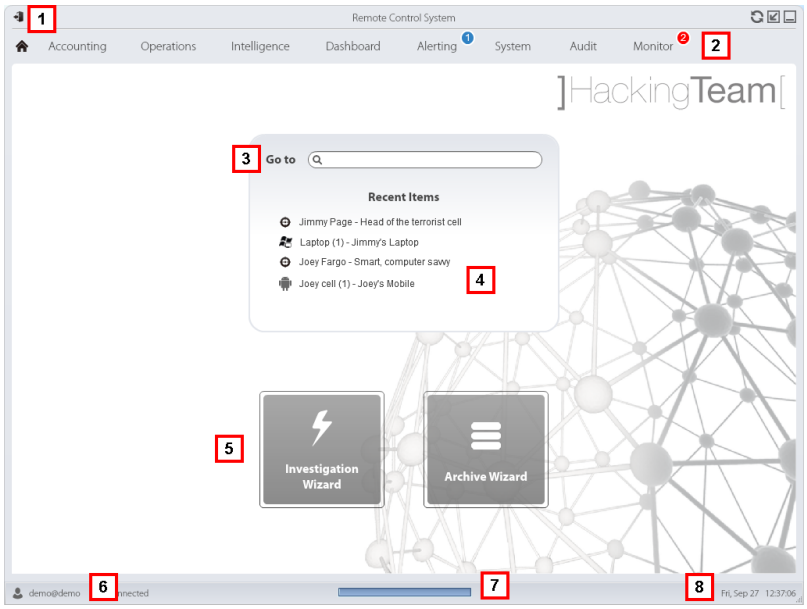
Per visualizzare l'homepage:	• fare clic su 

Introduzione

RCS Console presenta all'avvio questa homepage, unica per tutti gli utenti. I menu abilitati dipendono dai ruoli assegnati al proprio account.

Come si presenta

Ecco come viene visualizzata l'homepage con già presente una cronologia degli argomenti recenti. Per il dettaglio degli elementi e le azioni comuni:



Area	*Descrizione*
1	Barra del titolo con pulsanti di comando.

Area	*Descrizione*
2	Menu di RCS con le funzioni abilitate per l'utente
3	Casella di ricerca per cercare tra i nomi di operation, target, agent e entità, per nome o descrizione.
4	Collegamenti agli ultimi cinque elementi aperti (operation della sezione Operations, operation della sezione Intelligence, target,agent e entità).
5	Pulsanti per avvio dei Wizard.
6	Utente connesso con possibilità di cambiare la lingua e la password.
7	Area download con possibilità durante un'esportazione o una compilazione di vedere lo stato di avanzamento.
8	Data e ora attuale con possibilità di cambio fuso orario.

Descrizione dei wizard da homepage

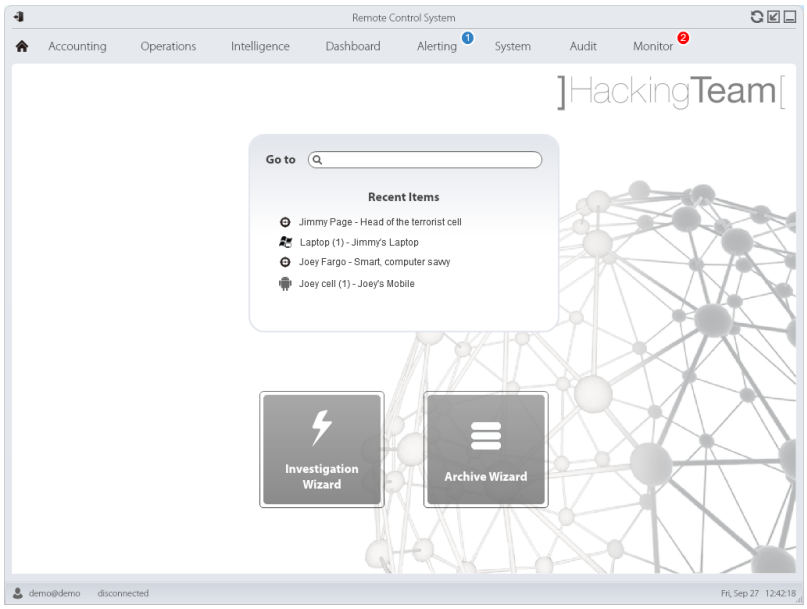
Per visualizzare l'homepage:	• fare clic su 

Introduzione

Per utenti con certi privilegi RCS Console presenta dei pulsanti che attivano dei wizard.

Come si presenta

Ecco come viene visualizzata l'homepage con i wizard abilitati:



Pulsante	*Funzione*
	Apre il wizard per la creazione rapida di un agent. NOTA: pulsante abilitato solo per utenti con privilegi di Amministratore e di Tecnico.
	Apre il wizard per l'archiviazione rapida dei dati di operation e target. NOTA: pulsante abilitato solo per utenti con privilegi di Amministratore e di Amministratore di sistema.

Archive Wizard

Questo wizard permette di gestire rapidamente i dati di operation o target aperti allo scopo di archiviarli e eliminarli dal database per alleggerirlo.

I dati sono archiviati in backup e possono essere ripristinati in qualsiasi momento.

Di seguito la spiegazione delle diverse opzioni:

Opzione	*Descrizione*
Archive all data into a backup	Salva tutti i dati dell'operation o del target scelto in un file di backup di tipo full. Il backup compare nell'elenco dei backup programmati e può essere ripristinato in qualsiasi momento.

Opzione	*Descrizione*
Remove all data from the live system	Elimina dal database tutte le evidence dell'operation o del target selezionato. L'operation o il target restano aperti e funzionanti. Solo il database viene ridotto di dimensione.  PRUDENZA: se combinate questa opzione con il backup istantaneo date un nome particolare al backup in modo che sia evidente che le evidence corrispondenti sono stati eliminate dal sistema.
Mark the item as closed	Chiude l'operation o il target selezionato.  PRUDENZA: l'operation o il target vengono chiusi senza possibilità di essere riaperti. Gli agent non inviano più i dati, ma è possibile consultare le evidence già ricevute.
Delete the item from the system	Elimina tutti i dati dell'operation o del target selezionato. Vengono eliminati dai database i dati dell'operation, dei target, degli agent e tutte le evidence.  PRUDENZA: eliminare un'operation/target è un'azione irreversibile e causa la perdita dei dati associati a quella operation/target.

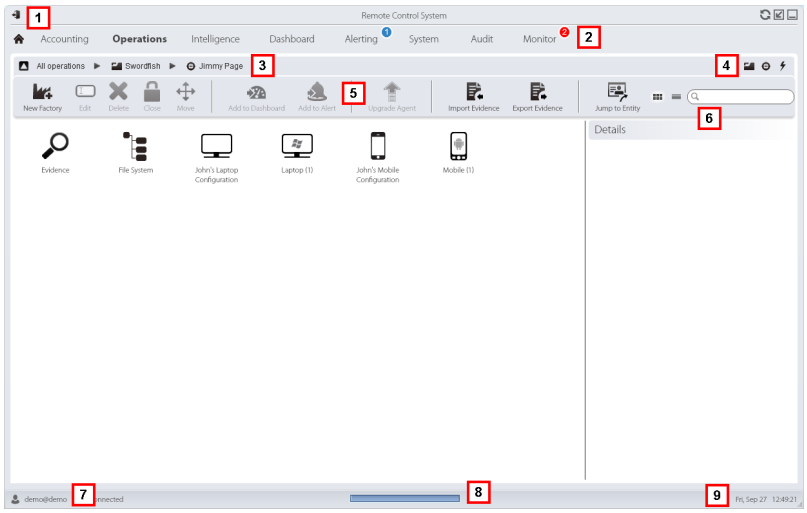
Elementi e azioni comuni dell'interfaccia

Ogni pagina del programma utilizza elementi comuni e permette azioni simili tra loro.

Per facilitare la consultazione di questo manuale, sono stati descritti in questo capitolo elementi e azioni comuni ad alcune le funzioni.

Come si presenta RCS Console

Ecco come viene visualizzata una pagina tipica di RCS Console. In questo esempio mostriamo la pagina di un target:



Area	*Descrizione*
1	Barra del titolo con pulsanti di comando: Logout da RCS. Pulsante di aggiornamento della pagina. Pulsante di ingrandimento della finestra. Pulsante di riduzione a icona della finestra.
2	• Pulsante per tornare alla homepage • Menu di RCS con le funzioni abilitate per l'utente
3	Barra di navigazione per l'operation. Di seguito la descrizione:

Icona	*Descrizione*
	Torna al livello superiore.
	Mostra la pagina dell'operation (sezione Operations).
	Mostra la pagina del target.
	Mostra la pagina della factory.
	Mostra la pagina dell'agent.
	Mostra la pagina dell'operation (sezione Intelligence).
	Mostra la pagina dell'entità.

Area	*Descrizione*
4	Pulsanti per visualizzare tutti gli elementi indipendentemente dalla loro appartenenza. Di seguito la descrizione:

Icona	*Descrizione*
	Mostra tutte le operation.
	Mostra tutti i target.
	Mostra tutti gli agent.
	Mostra tutte le entità.

5 Barre con i pulsanti della finestra.

6 Pulsanti e casella di ricerca:

Oggetto	*Descrizione*
John Doe	Casella di ricerca. Inserendo parte del nome compare l'elenco degli elementi che contengono le lettere inserite.
	Visualizza gli elementi in una tabella.
	Visualizza gli elementi come icone.

7 Utente connesso con possibilità di cambiare la lingua e la password.

8 Area download con possibilità durante un'esportazione o una compilazione di vedere lo stato di avanzamento. I file sono scaricati sul desktop nella cartella RCS Download.

- barra superiore: percentuale generazione sul server.
- barra inferiore: percentuale download dal server su RCS Console.

9 Data e ora attuale con possibilità di cambio fuso orario.

Azioni sempre disponibili sull'interfaccia

Cambiare la lingua dell'interfaccia o la propria password

Per cambiare la lingua dell'interfaccia o la propria password:

Passo	*Azione*
1	Fare clic su **[7]** compare una finestra di dialogo con i dati dell'utente.
2	Cambiare lingua o password e fare clic su **Save** per confermare e uscire.

Convertire le date-ora di RCS Console al proprio fuso orario

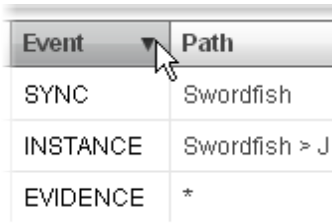
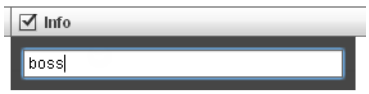
Per convertire tutte le date-ora al proprio fuso orario:

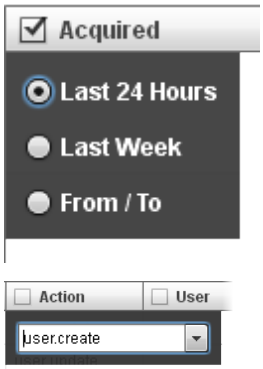
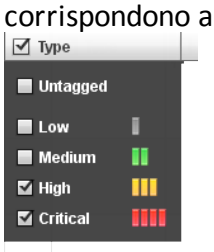
Passo	*Azione*
1	Fare clic su **[9]** compare una finestra di dialogo con la data-ora attuale: **UTC Time**: data-ora di Greenwitch (GMT) **Local Time**: data-ora dove è installato il server RCS **Console Time**: data-ora della console da cui si sta lavorando e che può essere convertita.
2	Cambiare il fuso orario e fare clic su **Save** per confermare e uscire: tutte le date-ora visualizzate sono convertite come richiesto.

Azioni sulle tabelle

RCS Console mostra diversi dati in forma di tabella. Le tabelle permettono di:

- ordinare i dati per colonna in ordine crescente/decrescente
- filtrare i dati per ogni colonna

Azione	*Descrizione*
Ordinare per colonna	Fare clic sull'intestazione per ottenere l'ordine per quella colonna, crescente o decrescente. 
Filtrare un testo	Inserire parte del testo che si sta cercando: compaiono solo gli elementi che contengono il testo digitato.  L'esempio mostrerà elementi con descrizioni tipo: • "my**boss**" • "**boss**anova"

Azione	*Descrizione*
Filtrare in base a un'opzione	Selezionare un'opzione: compaiono gli elementi che corrispondono all'opzione scelta. 
Filtrare in base a più opzioni	Selezionare una o più opzioni: compaiono gli elementi che corrispondono a tutte le opzioni scelte. 
Cambiare la dimensione delle colonne	Selezionare il bordo della colonna e trascinarlo.

Gestione dei frontend

Per gestire i frontend: • **sezione System, Frontend**

Scopo della funzione

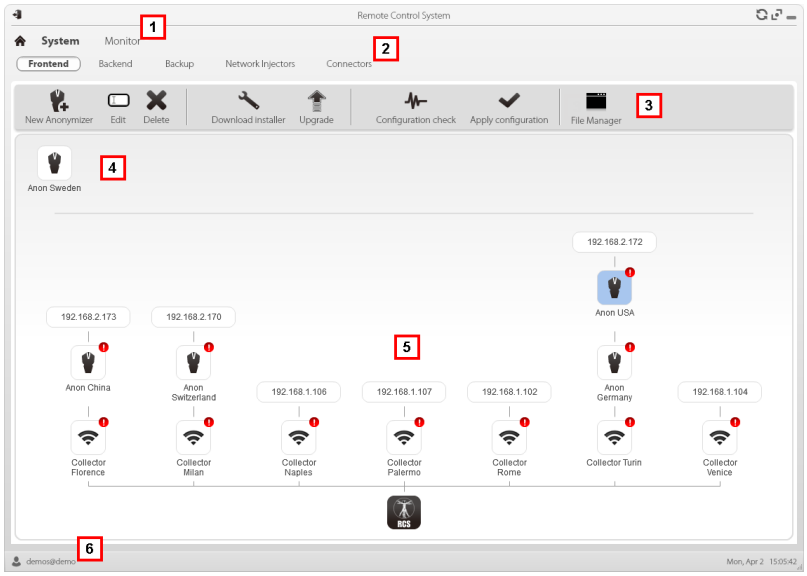
Durante il funzionamento di RCS, questa funzione permette di verificare lo stato di Anonymizer e Collector, modificare la configurazione degli Anonymizer e delle catene e aggiornare i VPS.

In fase di installazione, questa funzione permette di creare un nuovo "oggetto" Anonymizer che funziona da collegamento logico tra RCS Console e la singola componente software da installare su un VPS.

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Frontend management**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Menu **System.**

Area	*Descrizione*
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Descrizione*
	Crea un nuovo Anonymizer.
	Modifica i dati dell'Anonymizer. Dopo la modifica fare clic su **Apply configuration**. Mostra gli ultimi log.  Suggerimento: fare doppio clic su un Anonymizer per vedere/modificarne i dati.
	Elimina un Anonymizer. Questa operazione non elimina l'Anonymizer installato sul VPS.
	Genera l'installer per la prima installazione dell'Anonymizer e lo salva sul desktop. Copiare il file via SSH sul VPS remoto ed eseguirlo.
	Aggiorna la versione del software dell'Anonymizer da remoto.
	Simula il comportamento di un agent. Si connette quindi a ogni Anonymizer di una catena fino al Collector di ingresso, e restituisce il risultato della connessione.
	Aggiorna la configurazione di tutti gli Anonymizer. Questo comando viene utilizzato dopo aver aggiunto, rimosso o modificato la catena di Anonymizer in uso.
	Mostra i pacchetti creati automaticamente sul Collector dai vettori **Exploit, WAP Push e QR Code** e resi disponibili per il dispositivo target. È possibile eliminare i file non più utilizzati.  ***PRUDENZA: l'eliminazione anticipata dei file può vanificare l'infezione operata dai vettori.***  NOTA: non compaiono eventuali file copiati manualmente nella cartella.

4	Anonymizer configurati non ancora inclusi in una catena.

Area	*Descrizione*
5	Catene di Anonymizer sul sistema con l'indirizzo IP dell'ultimo elemento. Possibili stati:  : Anonymizer non in catena.  : Anonymizer in catena e funzionante.  : Anonymizer non monitorato da Network Controller.  : Anonymizer con malfunzionamenti.  : Collector in funzione.  : Collector non funzionante.
6	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 96* .

Per le procedure di installazione, modifica, eliminazione di un Anonymizer *vedi "**Installazione e configurazione degli Anonymizer**" a pagina 42* .

Aggiungere un Anonymizer alla configurazione

Per aggiungere un Anonymizer *vedi "**Installazione e configurazione degli Anonymizer**" a pagina 42*

Modificare la configurazione di un Anonymizer

Per modificare la configurazione di un Anonymizer *vedi "**Installazione e configurazione degli Anonymizer**" a pagina 42* .

Dati del File Manager

Di seguito la descrizione:

Campo	*Descrizione*
Time	Data-ora dell'installazione dei vettori sul dispositivo.

Campo	*Descrizione*
Name	Nome del file creato dall'installer.
Factory	Factory da cui è stato generato l'installer.
User	Utente che ha creato l'installer.

Gestione dei back end

Per gestire i back end:	• sezione System, Backend

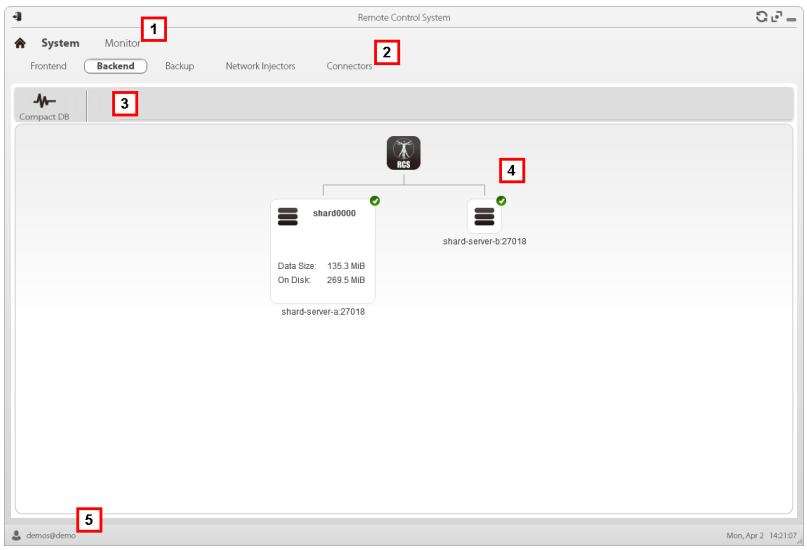
Scopo della funzione

Durante il funzionamento di RCS, questa funzione permette di verificare lo stato dei database e controllare lo spazio su disco disponibile.

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Backend management**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Menu **System.**

Area	*Descrizione*
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Descrizione*
	Compatta il database.

4	Struttura dei database Shard con loro stato, spazio su disco occupato e disponibile.
	 NOTA: il database 0 è quello incluso in MasterNode.
5	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 96* .

Per saperne di più sui backup *vedi "**Cose da sapere sui backup**" nel seguito* .

Dati significativi di un database Shard

Di seguito la descrizione dei dati del database Shard selezionato:

Campo	*Descrizione*
Data Size	Spazio occupato.
On Disk	Spazio totale unità Shard.
nomeServer:porta	Porta del server Shard

Cose da sapere sui backup

Responsabilità di gestione

L'Amministratore di sistema deve salvaguardare i dati registrati e decidere la frequenza dei backup di varia tipologia.

Modalità di backup

RCS salva tutti i dati contenuti nei database nella cartella specificata in fase di modifica alla configurazione di RCS. *Vedi "**Modifica alla configurazione di Master Node**" a pagina 77*

Un backup può salvare uno o più tipi di dati. I tipi di backup sono:

- metadata
- full
- operation
- target

Backup tipo Metadata

Il backup tipo metadata è rapido e salva tutta la configurazione del sistema, permettendo un rapido ripristino del normale funzionamento del sistema in caso di problemi. Questo tipo di backup non include le evidence raccolte. Si consiglia di effettuare un backup giornaliero.

AVVERTENZA: l'assenza di un backup metadati recenti può causare la perdita degli agent installati sui vari dispositivi.

NOTA: il job che comanda il backup dei metadata settimanale è già impostato di default e abilitato ad ogni riavvio del sistema. Non è possibile eliminare il job di default.

Backup tipo Full

Il backup **full** contiene tutte le evidence, pertanto può richiedere molto tempo. Visto che può essere ripristinato successivamente ad un eventuale backup di tipo metadata, si consiglia di effettuarlo una volta al mese.

Backup tipo Operation

Il backup **operation** salva tutte le operation aperte e chiuse. Visto che può essere ripristinato successivamente ad un eventuale backup di tipo metadata, si consiglia di effettuarlo una volta al mese.

Backup tipo Target

Il backup **target** salva i dati di tutti i target aperti e chiusi. Visto che può essere ripristinato successivamente ad un eventuale backup di tipo metadata, si consiglia di effettuarlo una volta al mese.

Backup incrementale

I backup di tipo **full**, **operation** e **target** possono essere anche incrementali. In questo modo il sistema salva i dati generati a partire dalla data-ora dell'ultimo backup. Il primo backup incrementale è sempre un backup completo (full, operation o target). Sono solo i successivi backup ad essere incrementali.

NOTA: se si toglie l'opzione incrementale a un job e poi la si riapplica, il primo backup di quel job sarà comunque completo.

Suggerimento: nominare il job in modo da poter successivamente riconoscere che si tratta di un backup incrementale (es.: "Increm_lastWeek").

Si suggerisce di fare un backup completo (full, operation o target) ogni mese e un backup incrementale ogni settimana.

Ripristino dei backup per cause gravi

PRUDENZA: il ripristino di un backup deve essere considerato solo in situazioni gravi quali la sostituzione di un database.

Il ripristino di un backup deve essere usato per tutte le sostituzioni dei server.

Ripristino dati da backup

IMPORTANTE: il ripristino di un backup non è mai distruttivo. Per questo motivo il ripristino non deve essere usato per recuperare elementi che sono stati modificati inavvertitamente.

Di seguito alcuni esempi:

Se dopo l'ultimo backup	*Allora il ripristino*
si è cancellato un elemento	recupera l'elemento cancellato.
si è modificato un elemento	lascia l'elemento modificato.
si è aggiunto un nuovo elemento	lascia l'elemento modificato.

IMPORTANTE: il backup non recupera le informazioni di operation che sono state chiuse (eliminate) per errore.

IMPORTANTE: per ripristinare i backup incrementali occorre ripristinarli tutti a partire dal più vecchio.

Gestione dei backup

Per gestire i backup: • **sezione System, Backup**

Scopo della funzione

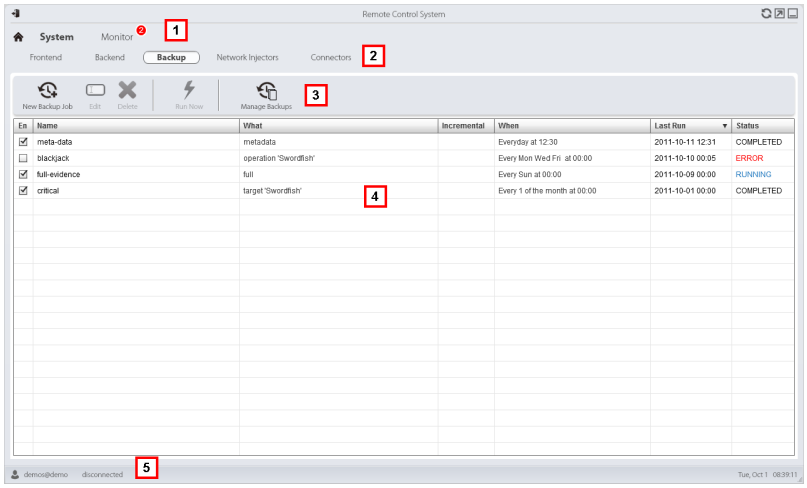
Durante il funzionamento di RCS, questa funzione permette di verificare lo stato dell'ultimo backup, creare dei nuovi processi di backup o eseguire un backup istantaneamente.

In fase di manutenzione di RCS, questa funzione permette ripristinare dati danneggiati recuperandoli da un backup esistente.

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **System Backup&Restore**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Menu **System.**

Area	*Descrizione*
3	Barra con i pulsanti dedicati ai processi di backup. Di seguito la descrizione:

Icona	*Descrizione*
	Aggiunge un processo di backup.
	Modifica un processo di backup per esempio per disabilitarlo o cambiarne la frequenza.  **IMPORTANTE: non usare questa funzione per cambiare la tipologia dei dati trattati. Meglio disabilitare il processo e crearne uno nuovo con un nome coerente.**
	Elimina un processo di backup. Non elimina i backup generati dal processo.
	Esegue il backup anche se disabilitato.
	Visualizza elenco dei backup eseguiti. Di seguito la descrizione dei pulsanti:  ripristina i dati del backup selezionato.  ***PRUDENZA: il ripristino dei dati è un'operazione delicata. Assicuratevi di aver compreso bene il meccanismo di ripristino operato da RCS.Vedi "Cose da sapere sui backup" a pagina 105***  elimina il backup selezionato.

4	Elenco processi di backup programmati (abilitati e non) con lo stato dell'ultimo backup.
5	Barra di stato di RCS.

Dati significativi di un processo di backup

Di seguito la descrizione dei dati del processo di backup selezionato:

Campo	*Descrizione*
Abilitato	Abilita/disabilita il processo di backup. Utilizzare per disabilitare temporaneamente il processo, per esempio in caso di sostituzione dell'unità di backup.  Suggerimento: per abilitare/disabilitare rapidamente un processo selezionare la casella nella colonna **En** dell'elenco.
What	Dati da includere nel backup. **metadata**: tutta la configurazione del sistema: database, Collector, Network Injector, Anonymizer, agent. Ovvero il minimo indispensabile per ripristinare il sistema in caso di disastro. Tutte le informazioni necessarie per proseguire la raccolta informazioni dagli agent sono contenuti in questo tipo di backup. **full**: backup completo della configurazione di sistema e dei dati di intercettazione (operation e target). Può richiedere diverso tempo di esecuzione. **operation**: backup dell'operation indicata, dati inclusi. **target**: backup del target indicato, dati inclusi.
When	Cadenza del backup. **UTC**: fuso orario.
Name	Nome da assegnare al backup.

Gestione dei connector

Per gestire i connector: • sezione **System, Connectors**

Scopo della funzione

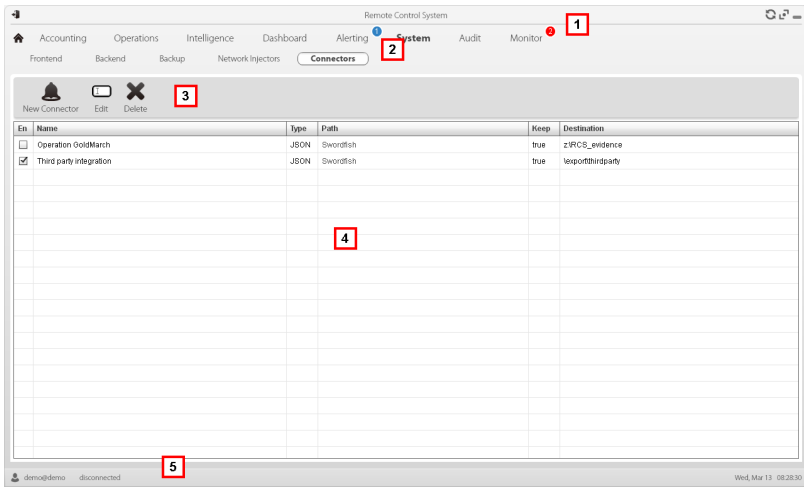
Questa funzione permette creare delle regole di connessione con software di terze parti. Le evidence ricevute da RCS saranno smistate secondo queste regole.

 **IMPORTANTE: questa funzione è sottoposta a licenza.**

 NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Connector management**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Menu **System.**
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Descrizione*
	Aggiunge una regola di connessione.
	Modifica la regola di connessione selezionata.
	Elimina la regola di connessione selezionata.

4	Elenco delle regole di connessione.
5	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 96 .*

Dati significativi di una regola di connessione

Di seguito la descrizione dei dati della regola selezionata:

Campo	*Descrizione*
Path	Nome dell'operation o del target di cui smistare le evidence. Se non si specifica nulla, tutte le operation e tutte le evidence sono consegnate al software di terze parti.
Type	Tipo di archiviazione delle evidence: • **Local**: le evidence vengono inviate a una cartella locale • **Remote**: le evidence vengono inviate a un'installazione RCS con licenza **Archive**  Il sistema RCS con licenza Archive riceve i dati dal sistema centrale ed è abilitato a tutte le funzioni di analisi come se le informazioni le avesse ricevute direttamente dai dispositivi del target; non è però in grado di creare agent e di ricevere nuovi dati direttamente da Collector.
[Formato]	Formato delle evidence. • **JSON, XML** per tipo **Local** • **RCS** per tipo **Remote**
Keep the evidence	Se selezionato, mantiene una copia delle evidence nel database di RCS.  PRUDENZA: se non viene selezionato, non sarà più possibile vedere queste evidence in RCS, né ricevere alert.
Destination	Percorso della cartella locale dove consegnare le evidence (es.: "C:\RCSevidence") o indirizzo IP del server RCS Archive.

Gestione dei Network Injector

Per gestire i Network Injector:	• sezione **System, Network Injector**

Scopo

In fase di installazione, questa funzione permette di creare un nuovo "oggetto" Network Injector che crea il collegamento logico tra RCS Console e il singolo apparato hardware.

 NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Injector management**.

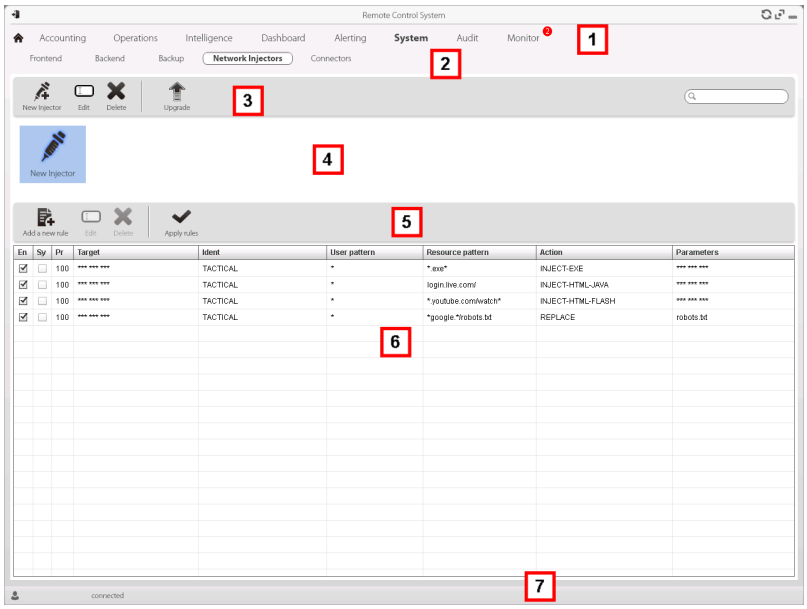
Cosa è possibile fare

Con questa funzione è possibile:

- creare un nuovo Network Injector
- aggiornare il software Appliance Control Center o Tactical Control Center
- visualizzare i log e verificare lo stato del Network Injector

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Menu **System.**

Area	*Descrizione*
3	Barra con i pulsanti dedicati ai Network Injector. Di seguito la descrizione:

Azione	*Funzione*
	Aggiunge un nuovo Network Injector.
	Modifica i dati del Network Injector e visualizza i log.
	Elimina il Network Injector selezionato.
	Aggiorna il software Appliance Control Center o Tactical Control Center. Se il Network Injector è di tipo Appliance alla successiva sincronizzazione si aggiorna automaticamente, basta che ci sia un processo di infezione attivo. Se invece è di tipo Tactical sarà l'operatore a scegliere se aggiornare l'applicativo. *Vedi "**Aggiornamento Network Injector Appliance**" a pagina 70 , "**Aggiornamento Tactical Network Injector**" a pagina 72*

4	Elenco dei Network Injector.
5	Barra con i pulsanti dedicati alle regole di injection.
6	Elenco delle regole del Network Injector selezionato.
7	Barra di stato di RCS. .

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 96* .

Per saperne di più sull'installazione di un Network Injector Appliance *vedi "**Installazione di Network Injector Appliance**" a pagina 46*

Per saperne di più sull'installazione di un Tactical Network Injector *vedi "**Installazione di Tactical Network Injector**" a pagina 53 vedi "**Installazione di Network Injector Appliance**" a pagina 46*

Per saperne di più sui dati di un Network Injector *vedi "**Dati dei Network Injector**" alla pagina successiva*

Aggiornare il software di gestione del Network Injector

Per aggiornare un Network Injector:]

Passo	*Azione*
1	• Selezionare il Network Injector • Fare clic su **Ugrade**: compaiono i dati dell'aggiornamento. • Fare clic su **OK** : RCS ha preso in carico la richiesta di invio dell'aggiornamento al Network Injector. **IMPORTANTE: il Network Injector riceve l'aggiornamento del software solo quando è sincronizzato con il server RCS.** ***Vedi "Verifica dello stato dei Network Injector " a pagina 59***

Dati dei Network Injector

Di seguito la descrizione dei dati del Network Injector:

Dato	*Descrizione*
Name **Description**	Descrizioni libere.
Version	Versione software. Per vedere le versioni software di tutti i componenti *vedi "Monitoraggio del sistema (Monitor)" nella pagina di fronte* .
Address	Indirizzo IP dell'apparato.
Port	443. Per vedere le porte da aprire in caso di firewall*vedi "Porte da aprire nel firewall" a pagina 16*
Monitor via NC	Se abilitato, Network Controller acquisisce lo stato di Network Injector ogni 30 secondi. Se non abilitato, Network Injector continua le sue operazioni di sniffing e injection ma Network Controller non ne verifica lo stato. Usato quando non è possibile per qualsiasi ragione connettersi al Network Injector una volta installato presso l'ISP, o nel caso di utilizzo tattico.
Log	Ultimi messaggi registrati nei log. NOTA: l'aggiornamento dei log del Tactical Network Injector dipendono dalla frequenza con cui l'operatore abilita la sincronizzazione. Per vedere il contenuto dei file di log *vedi "I log di sistema" a pagina 82* . : aggiorna l'elenco. : elimina i log visualizzati.

Monitoraggio del sistema (Monitor)

Per fare il monitoraggio del sistema:	• sezione **Monitor**

Scopo

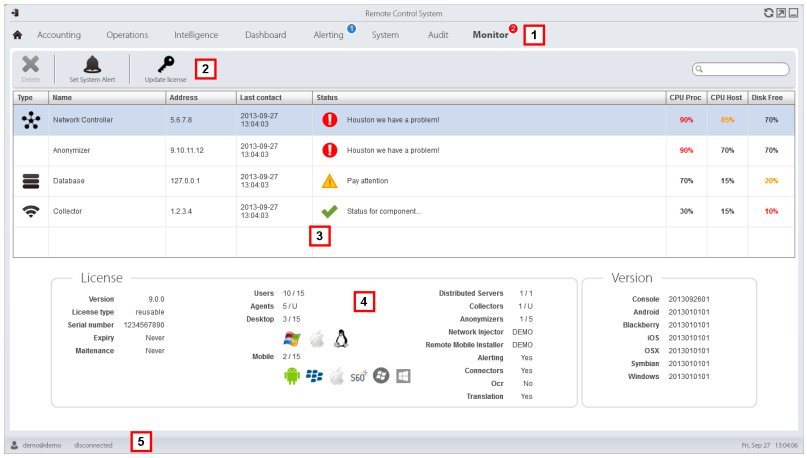
Questa funzione permette di:

- monitorare lo stato del sistema in termini di componenti hardware e software
- eliminare elementi da monitorare che sono stati disinstallati
- monitorare le licenze utilizzate rispetto a quelle acquistate

Richiede assistenza: contattare il vostro Account Manager HackingTeam se sono necessarie licenze aggiuntive.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS. Monitor 1 : indica la quantità di allarmi di sistema in corso.

Area	*Descrizione*
2	Barre con i pulsanti della finestra. Di seguito la descrizione: *Icona* *Descrizione*  Elimina il componente da monitorare.
3	Elenco componenti di RCS con relativo stato:  Allarme (genera l'invio di una e-mail al gruppo di alerting)  Avvertenza  Componente funzionante
4	Stato delle licenze.
5	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 96* .

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati del monitoraggio del sistema (Monitor)**" nella pagina di fronte* .

Eliminare un componente da monitorare

Per eliminare un componente eventualmente dismesso:

Passo	*Azione*
1	Selezionare il componente.
2	Fare clic su **Delete**: RCS non acquisirà più lo stato da quel componente. Solo eventuali successive installazioni di nuovi componenti aggiorneranno l'elenco automaticamente.  NOTA: una cancellazione per errore di un componente ancora installato non è distruttiva. Lo stato del componente ricomparirà al successivo aggiornamento della pagina.

Dati del monitoraggio del sistema (Monitor)

Dati di monitoraggio dei componenti del sistema

Di seguito la descrizione dei dati del monitoraggio di sistema:

Dato	*Descrizione*
Type Name	Tipo e nome del componente controllato:  Anonymizer  Carrier  Collector  Database  Network Controller
Address	Indirizzo IP del componente.
Last contact	Data-ora ultima sincronizzazione.
Status	Stato del componente dall'ultima sincronizzazione:  Allarme: il componente non sta funzionando, contattare il gruppo di alerting per un intervento rapido.  Avvertenza: il componente segnala una situazione di rischio, contattare l'Amministratore di sistema per le verifiche del caso.  Componente funzionante.
CPU	% utilizzo CPU del singolo processo.
CPU Total	% utilizzo CPU del server.
Disk Free	% di unità disco libera.

Dati di monitoraggio delle licenze

Di seguito la descrizione dei dati del monitoraggio delle licenze. Nel caso di licenze limitate il formato è "x/y" dove x è la quantità di licenze attualmente usate dal sistema e y la quantità massima di licenze.

PRUDENZA: se la quantità di licenze si esaurisce, eventuali nuovi agent saranno accodati in attesa che si liberi una licenza o che se ne acquistino di nuove.

Dato	*Descrizione*
License type	Tipo di licenza attualmente in uso per gli agent. **reusable**: è possibile riutilizzare la licenza di un agent dopo la sua disinstallazione. **oneshot**: la licenza di un agent ha validità solo per una installazione. NOTA: è possibile aggiornare la licenza solo se si è in possesso dell'autorizzazione **License modification**.
Users	Quantità di utenti attualmente usati dal sistema e quantità massima ammessa.
Gli agent	Quantità di agent attualmente usati dal sistema e quantità massima ammessa.
Desktop **Mobile**	Rispettivamente quantità agent desktop e mobile attualmente usati dal sistema e quantità massima ammessa.
Distributed server	Quantità database attualmente usati dal sistema e quantità massima ammessa.
Collectors	Quantità Collector attualmente usati dal sistema e quantità massima ammessa.
Anonymizers	Quantità di Anonymizer attualmente usati dal sistema e quantità massima ammessa.

]HackingTeam[

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

RCS 9 Manuale dell'amministratore di sistema
Manuale dell'amministratore di sistema 1.5 FEB-2014

info@hackingteam.com