

]HackingTeam[

RCS 9.6

The hacking suite for governmental interception

Manuale dell'amministratore di sistema



Proprietà delle informazioni

© COPYRIGHT 2015, HT S.r.l.

Tutti i diritti sono riservati in tutti i paesi.

Nessuna parte di questo manuale può essere tradotta in altra lingua e/o adattata e/o riprodotta in altra forma e/o mezzo meccanico, elettronico, per fotocopie, registrazioni o altro, senza una precedente autorizzazione scritta da parte di HackingTeam.

Tutte le società e i nomi di prodotti possono essere marchi legali o marchi registrati delle rispettive società la cui proprietà viene qui riconosciuta. In particolare Internet Explorer™ è un marchio registrato dalla Microsoft Corporation.

L'elaborazione del testo e delle immagini è stata vagliata con la massima cura, nonostante ciò HackingTeam si riserva il diritto di modificare e/o aggiornare le informazioni qui contenute per correggere errori tipografici e/o imprecisioni, senza preavviso o alcun impegno da parte della stessa.

Qualsiasi riferimento a nomi, dati e indirizzi di altre società non facenti parte di HackingTeam è casuale e, salvo diversa indicazione, è riportato a titolo puramente esemplificativo, allo scopo di chiarire meglio l'utilizzo del prodotto.

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

Introduzione a questa Guida	1
Informazioni utili sulla Guida	1
Obiettivi del manuale	1
Novità della guida	1
Documentazione fornita	3
Convenzioni tipografiche per le segnalazioni	4
Convenzioni tipografiche per la formattazione	4
Destinatari del prodotto e di questa guida	5
Dati di identificazione dell'autore del software	6
RCS (Remote Control System)	7
Architettura di un sistema RCS	8
Introduzione	8
Schema architettura	8
Componenti architettura	8
Cose da sapere su RCS	10
Funzionamento	10
Flusso e protezione dei dati	10
Continuità della registrazione dei dati	10
Certificati digitali	10
Decodifica dei dati	11
Architetture di più sistemi RCS	11
Introduzione	11
Schema architettura uno-molti	12
Schema architettura molti-uno	13
Sistemi RCS mittenti	13
Sistemi RCS riceventi	13
Struttura dei dati ricevuti	14
Installazione dei sistemi RCS riceventi	14
Introduzione all'installazione	15
Contenuto della confezione	16
Contenuto della confezione	16
Contenuto pacchetto di installazione (CD o sito web)	16

Chiave USB con licenza d'uso	16
Chiavi USB di protezione	17
Requisiti minimi di sistema	17
Porte da aprire nel firewall	17
Procedure dell'Amministratore di sistema	18
Introduzione	18
Installare RCS e configurarne i componenti	18
Mantenere e aggiornare il sistema	18
Monitorare il sistema	18
Installazione di RCS	19
Cose da sapere sull'installazione di RCS	20
Privilegi di accesso	20
Utente admin e utente Amministratore di sistema	20
Installazione server RCS	20
Introduzione	20
Prerequisiti all'installazione	21
Sequenza di installazione	21
Installazione del Master Node	21
Installazione del Collector	24
Verifica dell'avviamento dei servizi	26
Verifica dei log di installazione	26
Verificare gli indirizzi IP	26
Disinstallazione	26
Modulo OCR	26
Introduzione	26
Installazione	26
Funzionamento del modulo OCR	27
Occupazione di spazio nel database dei testi indicizzati	27
Carico di lavoro di un modulo OCR	27
Sintomi di carico eccessivo	27
Verificare il corretto funzionamento del modulo OCR	27
Disabilitare o riabilitare il modulo OCR	28
Elenco dei servizi RCS	28
Servizi ambiente front end	28

Servizi ambiente backend (Master Node)	28
Servizi ambiente backend (Shard)	29
Per saperne di più	29
Installazione RCS Console	29
Introduzione	29
Prerequisiti	29
Sequenza di installazione	29
Installazione di Adobe AIR	29
Installazione RCS Console	30
Disinstallazione di RCS Console	31
Creazione dell'utente Amministratore	31
File installati al termine dell'installazione	32
File installati	32
Installazione componenti aggiuntivi	34
Cose da sapere sugli Anonymizer	35
Introduzione	35
Stati dell'Anonymizer	35
Comunicazione tra Anonymizer e Collector	36
Anonymizer malfunzionante	37
Installazione e configurazione degli Anonymizer	37
Prerequisito all'installazione	37
Installazione	37
Dati di un Anonymizer	38
Verifica dell'avviamento	39
Verifica degli indirizzi IP	39
Modifica alla configurazione	39
Disinstallazione	39
Cose da sapere su Network Injector Appliance	40
Introduzione	40
Funzioni principali	40
Connessioni alla rete	40
Chiave di autenticazione	40
Schema di collegamento standard	40
Schema di collegamento come segmento intra-switch	41

Sniffing dei dati tramite TAP, porta SPAN	41
Installazione di Network Injector Appliance	42
Introduzione	42
Contenuto della confezione	42
Sequenza di installazione	42
Descrizione del pannello posteriore	42
Connessioni alla rete	43
Installazione e configurazione del sistema operativo	44
Verifica dell'indirizzo IP	46
Modifica dell'indirizzo IP	46
Disinstallazione	46
Cose da sapere su Tactical Network Injector	47
Introduzione	47
Funzioni principali	47
Connessioni alla rete	47
Chiave di autenticazione	47
Schema di collegamento standard	47
Schema di collegamento in emulazione Access Point	48
Installazione di Tactical Network Injector	49
Introduzione	49
Contenuto della confezione	49
Sequenza di installazione	49
Installazione e configurazione del sistema operativo	49
Verifica dell'indirizzo IP	51
Modifica dell'indirizzo IP	52
Disinstallazione	52
Altri applicativi installati sui Network Injector	52
Introduzione	52
Applicativi	52
Comandi Tactical Control Center e Appliance Control Center	53
Introduzione	53
Comandi	53
Prima sincronizzazione dei Network Injector con il server RCS	54
Introduzione	54

Sincronizzare un Network Injector con il server RCS	54
Verifica dello stato dei Network Injector	55
Introduzione	55
Individuare quando il Network Injector è sincronizzato	55
Visualizzare i log dei Network Injector	55
Installazione componenti aggiuntivi	56
Introduzione	56
Prerequisiti all'installazione di componenti aggiuntivi	56
Sequenza di installazione	56
Installazione del database Shard aggiuntivo	56
Installazione di Collector aggiuntivi	58
Verifica dell'avviamento dei servizi	60
Verifica dei log di installazione	60
Verificare gli indirizzi IP	60
Disinstallazione	61
Manutenzione ordinaria e aggiornamenti software	62
Cose da sapere sulla manutenzione di RCS	63
Ricezione degli aggiornamenti	63
Comportamento delle macchine in aggiornamento	63
Procedure di manutenzione ordinaria	63
Introduzione	63
Controllo e eliminazione dei file di log	63
Controllo dello spazio disponibile sul disco di backup	63
Aggiornamenti sistemi operativi Linux	63
Aggiornamento del server RCS	63
Prerequisiti all'aggiornamento	63
Modalità di aggiornamento	64
Aggiornamento del/dei server RCS	64
Aggiornamento di RCS Console	64
Prerequisiti all'aggiornamento	64
Aggiornamento di RCS Console	64
Aggiornamento degli Anonymizer	64
Prerequisiti all'aggiornamento	64
Aggiornamento degli Anonymizer	65

Aggiornamento Network Injector Appliance	65
Introduzione	65
Aggiornamento totale di Network Injector Appliance	65
Aggiornamento parziale con infezione in corso	66
Aggiornamento parziale senza infezione in corso	66
Aggiornamento Tactical Network Injector	67
Introduzione	67
Aggiornamento completo Tactical Network Injector	68
Aggiornamento parziale	68
Modifica alla configurazione di Master Node e Collector	70
Cose da sapere sulla configurazione	71
Cosa è possibile modificare	71
Quando cambiare la configurazione	71
Ordine di modifica della configurazione	71
Impostazione del server di posta	71
Utility per la configurazione	71
Le utility di RCS	71
Sintassi dei comandi delle utility	72
Altre opzioni	72
Modifica alla configurazione di Master Node	72
Modifica alla configurazione di Collector	73
Verifica della configurazione	74
Introduzione	74
Esempio output verifica configurazione	74
Risoluzione dei problemi	75
Malfunzionamenti possibili	76
Possibili problemi durante l'installazione	76
Possibili problemi con i server	76
Possibili problemi con i backup	77
Per saperne di più	77
I log di sistema	77
Introduzione	77
Utilità dell'analisi dei log	77
Esempio file di log	78

File di log di RCS	78
Visualizzazione rapida dei log	78
Contenuto di un file di log	79
Procedure di verifica stato componenti	79
Introduzione	79
Verifica delle licenze installate	79
Verifica dello stato del Master Node	79
Verifica dello stato dei servizi Worker	80
Verifica dello stato degli agent tramite il Collector	80
Verifica dell'avviamento del Network Injector	80
Verifica dei componenti del sistema	80
Creazione file per assistenza	81
Per saperne di più	81
Procedure per riavviamento dei servizi	81
Introduzione	81
Procedure di intervento sui componenti hardware	82
Introduzione	82
Sostituzione chiave di protezione	82
Sostituzione del Master Node	83
Sostituzione di uno Shard	83
Sostituzione del Collector	83
Sostituzione di un Anonymizer	83
Sostituzione di un Network Injector Appliance	84
Sostituzione di un Tactical Network Injector	84
RCS Console per l'Amministratore di sistema	85
Avvio di RCS Console	86
Introduzione	86
Riabilitare utenti disabilitati per inserimento password errata	86
Come si presenta la pagina di login	86
Accedere a RCS Console	87
Descrizione della homepage	87
Introduzione	87
Come si presenta	87
Descrizione dei wizard da homepage	88

Introduzione	88
Come si presenta	89
Archiviazione Rapida	89
Elementi e azioni comuni dell'interfaccia	90
Introduzione	90
Come si presenta RCS Console	90
Cambiare la lingua dell'interfaccia o la propria password	92
Convertire le date-ora di RCS Console al proprio fuso orario	92
Azioni sulle tabelle	93
Gestione dei front end	95
Scopo della funzione	95
Come si presenta la funzione	95
Per saperne di più	97
Aggiungere un Anonymizer alla configurazione	97
Modificare la configurazione di un Anonymizer	97
Dati del File Manager	97
Gestione dei back end	97
Scopo della funzione	97
Come si presenta la funzione	97
Per saperne di più	98
Dati significativi di un database Shard	98
Cose da sapere sui backup	100
Responsabilità di gestione	100
Modalità di backup	100
Backup tipo Metadata	100
Backup tipo Full	100
Backup tipo Operation	100
Backup tipo Target	100
Backup incrementale	101
Ripristino dei backup per cause gravi	101
Ripristino dati da backup	101
Backup completo per cause gravi	102
Introduzione	102
Eseguire il backup	102

Ripristinare il backup	102
Gestione dei backup	102
Scopo della funzione	102
Come si presenta la funzione	102
Dati significativi di un processo di backup	104
Gestione dei connettori	104
Scopo della funzione	104
Come si presenta la funzione	105
Per saperne di più	105
Dati significativi di una regola di connessione	105
Gestione dei Network Injector	106
Scopo	106
Cosa è possibile fare	106
Per saperne di più	108
Aggiornare il software di gestione del Network Injector	108
Dati dei Network Injector	108
Monitoraggio del sistema (Monitor)	109
Scopo	109
Come si presenta la funzione	109
Per saperne di più	110
Eliminare un componente da monitorare	110
Dati del monitoraggio del sistema (Monitor)	110
Glossario dei termini	113

Elenco delle figure

<i>Figura 2.1: Architettura RCS: schema logico</i>	8
<i>Figura 2.1: Architettura RCS uno a molti: schema logico</i>	12
<i>Figura 2.2: Architettura RCS molti a uno: schema logico</i>	13
<i>Figura 4.1: Servizi Master Node e loro dipendenze</i>	28
<i>Figura 4.2: Servizi Shard e loro dipendenze</i>	29
<i>Figura 5.1: Esempio catena di Anonymizer</i>	35
<i>Figura 5.2: Flusso informazioni tra Anonymizer e Collector</i>	36
<i>Figura 5.3: Flusso informazioni tra Anonymizer e Collector con un Anonymizer malfunzionante</i>	37
<i>Figura 5.1: Network Injector Appliance: schema fisico</i>	41
<i>Figura 5.2: Network Injector Appliance con TAP: schema fisico</i>	41
<i>Figura 5.1: Tactical Network Injector: schema di collegamento standard</i>	48
<i>Figura 5.2: Tactical Network Injector: schema in emulazione di access point</i>	48

Introduzione a questa Guida

Informazioni utili sulla Guida

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

Novità della guida

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

<i>Data rilascio</i>	<i>Codice</i>	<i>Versione software</i>	<i>Descrizione</i>
15 Marzo 2015	Manuale dell'amministratore di sistema 1.9 MAR-2015	9.6	Aggiornata procedura per l'installazione del server RCS, del Collector e dello Shard, vedi " Installazione server RCS " a pagina 20 e " Installazione componenti aggiuntivi " a pagina 56. Aggiunta disabilitazione automatica per inserimento password errata e procedure di riabilitazione, vedi " Avvio di RCS Console " a pagina 86.
24 Novembre 2014	Manuale dell'amministratore di sistema 1.9 MAR-2015	9.5	Aggiornata modalità di comunicazione tra Network Injector e server RCS, vedi " Architettura di un sistema RCS " a pagina 8. Aggiornata procedura per sincronizzare la prima volta Network Injector e il server RCS vedi " Prima sincronizzazione dei Network Injector con il server RCS " a pagina 54.

Data rilascio	Codice	Versione software	Descrizione
20 Settembre 2014	Manuale dell'amministratore di sistema 1.7 SET-2014	9.4	<p>Aggiornata modalità di comunicazione tra Collector e Anonymizer, vedi "Architettura di un sistema RCS" a pagina 8 e "Cose da sapere sugli Anonymizer" a pagina 35.</p> <p>Aggiunto servizio RCSMonitor del Master Node, vedi "Architettura di un sistema RCS" a pagina 8 e "Elenco dei servizi RCS" a pagina 28.</p>
23 Giugno 2014	Manuale dell'amministratore di sistema 1.6 GIU-2014	9.3	<p>Aggiunto elenco applicativi di terze parti installati su Network Injector, vedi "Altri applicativi installati sui Network Injector" a pagina 52.</p> <p>Rimossa la tipologia di architettura All-in-one.</p> <p>Aggiunte architetture più sistemi RCS, vedi "Architetture di più sistemi RCS" a pagina 11.</p> <p>Aggiunte nuove utility per verifica e diagnostica dei componenti di RCS, vedi "Procedure di verifica stato componenti" a pagina 79</p> <p>Introdotte dipendenze tra i servizi RCS, vedi "Elenco dei servizi RCS" a pagina 28 vedi "Elenco dei servizi RCS" a pagina 28</p> <p>"Aggiornamento del server RCS" a pagina 63</p>

Data rilascio	Codice	Versione software	Descrizione
19 Febbraio 2014	Manuale dell'amministratore di sistema 1.5 FEB-2014	9.2	<p>Aggiornata gestione installazione e aggiornamento degli Anonymizer, vedi "Installazione e configurazione degli Anonymizer" a pagina 37, "Aggiornamento degli Anonymizer" a pagina 64.</p> <p>Aggiunta gestione del servizio Carrier del Collector, vedi "Cose da sapere su RCS" a pagina 10</p> <p>Modificati comandi per verifica stato dei componenti, vedi "Procedure di verifica stato componenti" a pagina 79.</p> <p>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 53</p>
30 Settembre 2013	Manuale dell'amministratore di sistema 1.4 SET - 2013	9	<p>Aggiornata documentazione installazione, aggiornamento e gestione dei Network Injector, vedi "Installazione componenti aggiuntivi" a pagina 34, "Manutenzione ordinaria e aggiornamenti software" a pagina 62, "Gestione dei Network Injector" a pagina 106.</p> <p>Aggiornata documentazione sui connettori, vedi "Gestione dei connettori" a pagina 104.</p> <p>Aggiornata documentazione per migliorie apportate all'interfaccia utente.</p>

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 1.9 MAR-2015	PDF
Manuale dell'amministratore	Amministratori	Manuale dell'amministratore 1.7 MAR-2015	PDF

<i>Manuale</i>	<i>Destinatari</i>	<i>Codice</i>	<i>Formato di distribuzione</i>
Manuale del tecnico	Tecnici	Manuale del tecnico 2.0 MAR-2015	PDF
Manuale dell'analista	Analisti	Manuale dell'analista 1.9 MAR-2015	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:

<i>Esempio</i>	<i>Stile</i>	<i>Descrizione</i>
Vedi " Dati degli utenti "	<i>corsivo</i>	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.

<i>Esempio</i>	<i>Stile</i>	<i>Descrizione</i>
<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	prima lettera maiuscola	indica il nome di un tasto 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:

<i>Destinatario</i>	<i>Attività</i>	<i>Competenze</i>
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.	Tecnico di reti esperto
	 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.	
Amministratore	Crea gli account e i gruppi autorizzati. Crea operation e target. Controlla lo stato del sistema e delle licenze.	Responsabile dell'indagine

<i>Destinatario</i>	<i>Attività</i>	<i>Competenze</i>
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

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:

Architettura di un sistema RCS	8
Cose da sapere su RCS	10
Architetture di più sistemi RCS	11

Architettura di un sistema RCS

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.

Schema architettura

I componenti software sono installati su più server. Di seguito lo schema dell'architettura:

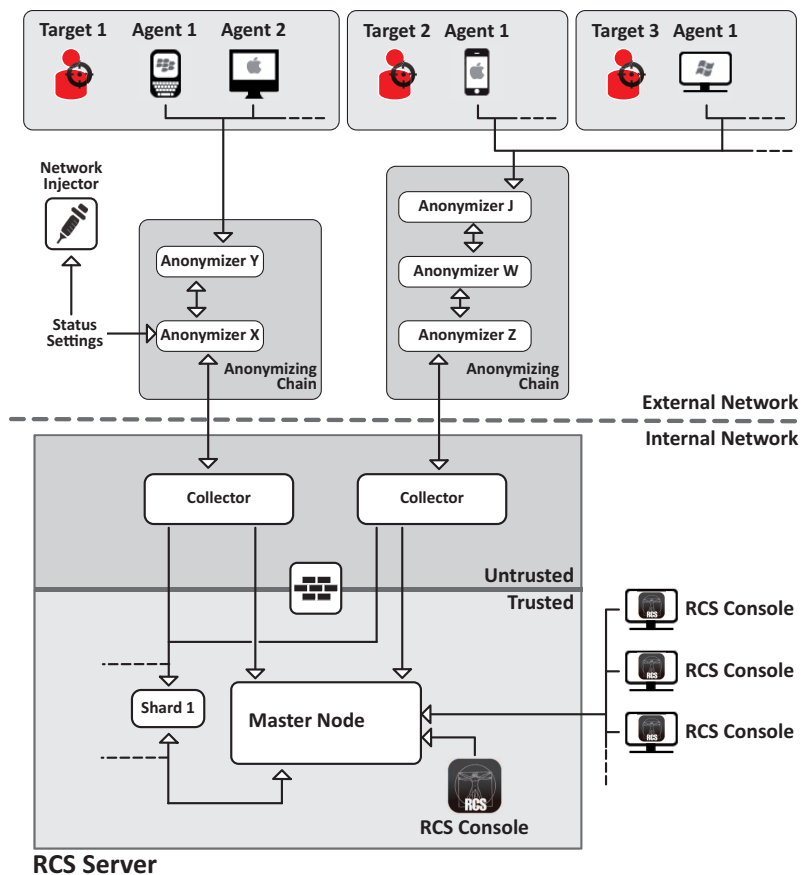


Figura 2.1: Architettura RCS: schema logico

Componenti architettura

Di seguito i componenti dell'architettura:

Componente	Funzione	Installazione
Agent	Cimice software, intercetta e comunica dati e informazioni del target dell'investigazione a un Anonymizer.	<ul style="list-style-type: none"> • 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 e dei Network Injector ai server. È possibile configurare più Anonymizer in catena per aumentare il livello della protezione. Ciascuna catena fa capo a un Collector.	VPS (Virtual Private Server)
Collector	<p>Uno per ogni Anonymizing Chain. In ognuno sono installati tre servizi:</p> <ul style="list-style-type: none"> • Collector: raccoglie i dati degli agent inviati all'ultimo Anonymizer della catena e dei Network Injector inviati all'Anonymizer configurato. • Carrier: invia i dati agli Shard e al Master Node • Network Controller: riceve lo stato e i log degli Anonymizer e invia loro gli aggiornamenti e le nuove configurazioni. <p>Sottoposto a singola licenza.</p>	uno o più server in ambiente front end
Firewall	Opzionale, ma fortemente suggerito, protegge l'ambiente <i>trusted</i> (dove vengono elaborati e memorizzati i dati) dall'ambiente <i>untrusted</i> (dove i dati vengono raccolti).	server RCS
RCS console	Console di configurazione, monitoraggio e analisi a uso degli operatori della centrale operativa.	<ul style="list-style-type: none"> • 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 e il servizio Monitor per il monitoraggio di tutti i componenti dell'architettura, compreso il Master Node stesso e l'invio di e-mail in caso di allarmi.	server RCS
Network Injector	(opzionale) Componente hardware fisso (Appliance) o portatile (Tactical), esegue operazioni di sniffing e infezione sulle connessioni HTTP del target. Comunica con il Collector tramite un Anonymizer (ed eventuale sua catena) per inviare dati e ricevere regole e configurazioni.	<ul style="list-style-type: none"> • ISP • LAN Wired o Wireless (abitazioni, hotel)

Componente	Funzione	Installazione
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 il loro inserimento nel database.	uno o più server in ambiente back end
Target	Bersagli dell'investigazione. Ogni dispositivo in possesso del target rappresenta una sorgente di prove e può essere monitorato da un agent.	-

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, reindirizzati per proteggere l'identità del destinatario (Voi) e passati a un collettore di informazioni (Collector) e inviati all'ambiente *trusted* tramite un servizio specifico (Carrier). La verifica dello stato e la configurazione delle entità esterne viene demandata a un servizio specifico della macchina Collector (Network Controller).

In ambiente *trusted* invece, avviene la vera gestione, la configurazione e il 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 "[Architettura di un sistema RCS](#)" a pagina 8.

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.

Certificati digitali

Il Master Node utilizza dei certificati digitali HTTPS che garantiscono la sicurezza della comunicazione tra Master Node, Collector e 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 32

Decodifica dei dati

Il servizio Worker viene installato insieme a ogni Shard e si occupa della decodifica dei dati prima che questi siano 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.

Architetture di più sistemi RCS

Introduzione

RCS può essere configurato per comunicare con altri sistemi RCS per trasferire o ricevere le prove ricevute dagli agent.

Sono previsti due possibili scenari di comunicazione:

- uno a molti: un sistema RCS riceve tutte le prove dagli agent e le smista a più sistemi RCS che visualizzano ed elaborano solo le prove di loro competenza. Per esempio se le prove sono raccolte da un unico ente centrale ma le indagini sono svolte da diverse procure locali.
- molti a uno: diversi sistemi RCS ricevono le prove dagli agent e le inviano a un unico sistema RCS che le visualizza e le elabora tutte. Per esempio se le prove sono raccolte ed elaborate dall'ente locale di competenza ma esiste un ente centrale che monitora i diversi enti locali e svolge indagini globali.

Schema architettura uno-molti

Di seguito lo schema dell'architettura uno-molti:

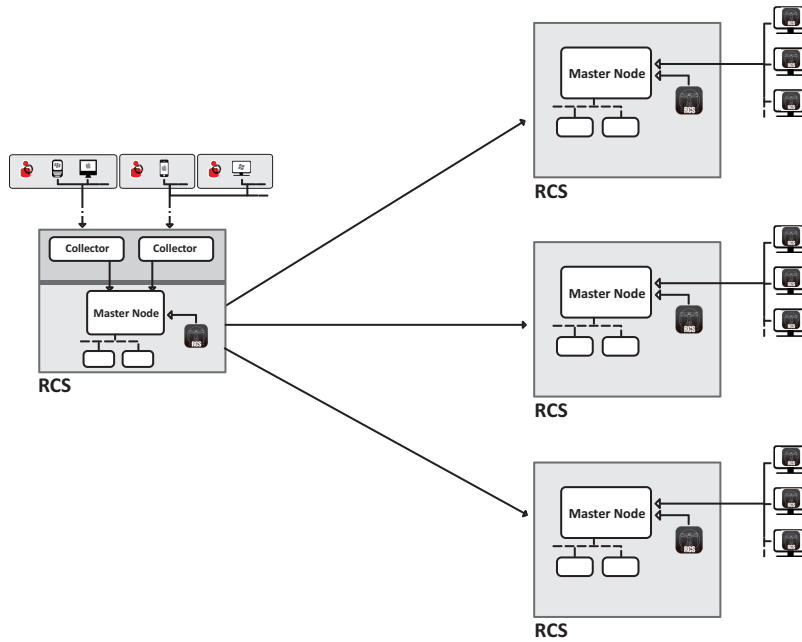


Figura 2.1: Architettura RCS uno a molti: schema logico

Schema architettura multi-uno

Di seguito lo schema dell'architettura multi-uno:

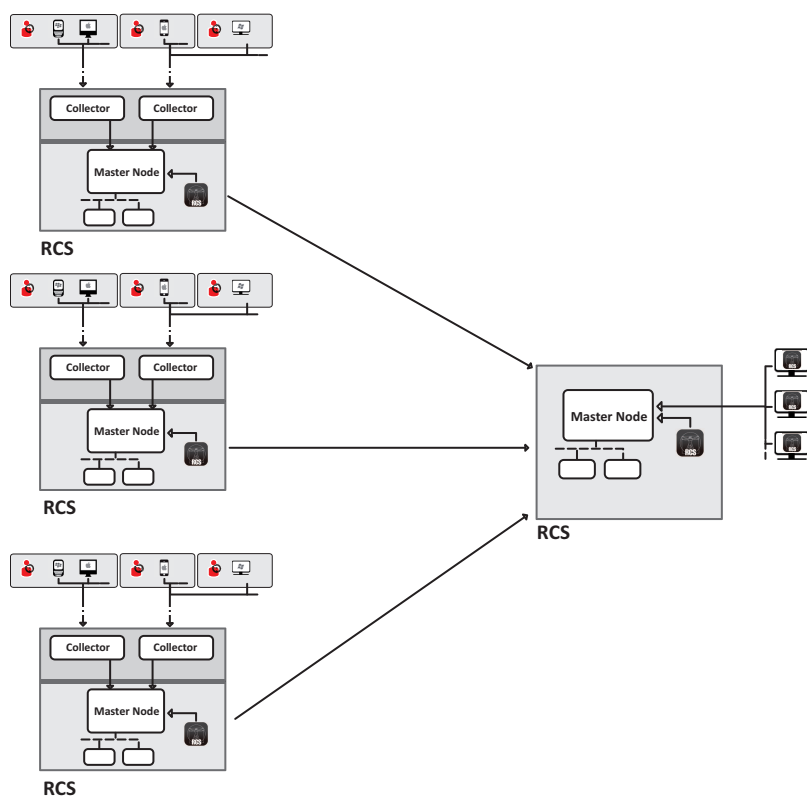


Figura 2.2: Architettura RCS molti a uno: schema logico

Sistemi RCS mittenti

Un sistema RCS mittente (sia per l'architettura uno-molti che multi-uno) è un sistema RCS completo. Prevede l'installazione di Collector ed eventuali altri componenti aggiuntivi e opzionali che gli permettono di ricevere le prove dagli agent installati nei dispositivi dei target. Vedi ["Architettura di un sistema RCS"](#) a pagina 8

Il trasferimento dei dati verso uno o più RCS ricevente/i viene configurato con RCS Console tramite le regole di connessione, vedi ["Gestione dei connettori"](#) a pagina 104.

Sistemi RCS riceventi

La funzione principale di un sistema RCS ricevente (sia per l'architettura uno-molti che multi-uno) è quella di visualizzare ed elaborare le prove. Le prove in suo possesso sono ricevute unicamente da uno o più sistemi RCS mittenti, mai direttamente dagli agent.

Le principali operazioni abilitate in RCS Console sono quelle relative alla gestione ed elaborazione delle prove. Invece, la gestione e configurazione degli agent è demandata completamente al sistema RCS mittente. I componenti principali sono il Master Node, RCS Console ed eventuali shard aggiuntivi.



NOTA: se si ricevono i dati da un unico sistema RCS, le uniche prove che si vedono e possono essere elaborate sono quelle delle indagini di propria competenza. Se si ricevono dati da più sistemi RCS, si vedono tutte le prove e si possono fare elaborazioni trasversali a più indagini.

Struttura dei dati ricevuti

I dati vengono ricevuti organizzati e nominati come definito nella RCS Console del sistema mittente. Tuttavia, i nomi possono essere modificati per essere meglio interpretati senza creare problemi di comunicazione tra i sistemi.

Se si ricevono dati da più sistemi RCS, i dati arrivano con associato un identificativo del sistema RCS mittente.

Installazione dei sistemi RCS riceventi



NOTA: i sistemi RCS riceventi richiedono licenza d'uso specifica.

Di seguito la sequenza completa d'installazione:

Passo	Azione	Vedi
1	Installare il Master Node.	<i>"Installazione server RCS" a pagina 20</i>
2	Verificare i log di installazione.	
3	Verificare l'avviamento dei servizi del Master Node.	
4	Installare RCS Console.	<i>"Installazione RCS Console" a pagina 29</i>
5	Installare eventuali shard aggiuntivi.	<i>"Installazione componenti aggiuntivi" a pagina 56</i>

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 17



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

Contenuti

Questa sezione include i seguenti argomenti:

Contenuto della confezione	16
Procedure dell'Amministratore di sistema	18

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	Guide all'installazione e all'uso di RCS. Ogni guida è destinata a un ruolo specifico dell'utente. <ul style="list-style-type: none"> • x.x: versione di RCS . • y.y: versione della guida. • Lingua: lingua di distribuzione.
	RCS_x.x_Analyst_y.y_Lingua.PDF	
	RCS_x.x_SysAdmin_y.y_Lingua.PDF	
	RCS_x.x_Technician_y.y_Lingua.PDF	
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.

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 Master Node per permettere il funzionamento di tutti i servizi RCS. La disconnessione della chiave comporta una 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:

<i>Macchina</i>	<i>Componente</i>	<i>Requisito</i>
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:

<i>Dal...</i>	<i>Al...</i>	<i>Porta da aprire</i>
Anonymizer	Collector	80
Collector	Master Node	443
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.

Installare RCS e configurarne i componenti

Di seguito la procedura per installare i componenti dell'architettura RCS:

Passo Azione

- 1** Predisporre l'ambiente di installazione.
Vedi "[Introduzione all'installazione](#)" a pagina 15.
- 2** Installare il server RCS.
Vedi "[Installazione di RCS](#)" a pagina 19.
- 3** Installare le RCS Console.
Vedi "[Installazione RCS Console](#)" a pagina 29.
- 4** Installare e configurare gli Anonymizer.
Vedi "[Installazione e configurazione degli Anonymizer](#)" a pagina 37
- 5** (opzionale) Installare database Shard e Collector aggiuntivi.
Vedi "[Installazione componenti aggiuntivi](#)" a pagina 56.
- 6** (opzionale) Installare i Network Injector.
Vedi "[Cose da sapere su Network Injector Appliance](#)" a pagina 40.
Vedi "[Cose da sapere su Tactical Network Injector](#)" a pagina 47.

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 62.
- Vedi "[Modifica alla configurazione di Master Node e Collector](#)" a pagina 70.
- Vedi "[Risoluzione dei problemi](#)" a pagina 75.

Monitorare il sistema

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

- Vedi "[RCS Console per l'Amministratore di sistema](#)" a pagina 85

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	20
Installazione server RCS	20
Modulo OCR	26
Elenco dei servizi RCS	28
Installazione RCS Console	29
File installati al termine dell'installazione	32

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 agent di intercettazione
-  Analista: responsabile dell'analisi dei dati



Suggerimento: a 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

Introduzione

I componenti sono installati tipicamente 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 permette diverse espansioni. Verificare con l'assistenza tecnica HackingTeam.



NOTA: RCS Console viene installata con una procedura a parte, sullo stesso server o su un altro computer remoto. Vedi "[Installazione RCS Console](#)" a pagina 29

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 17

Sequenza di installazione

Di seguito la sequenza completa di installazione:

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

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

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 **Master Node**.

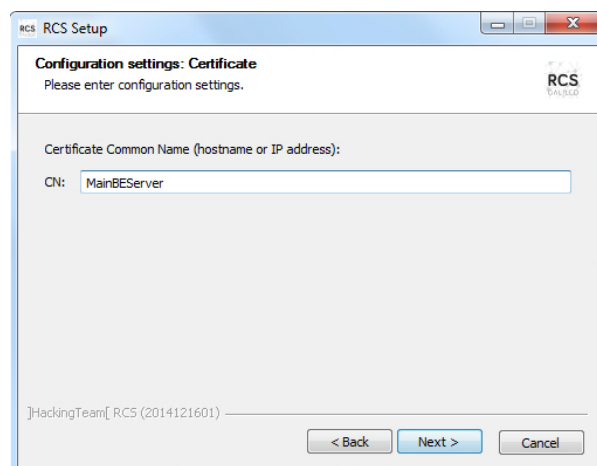
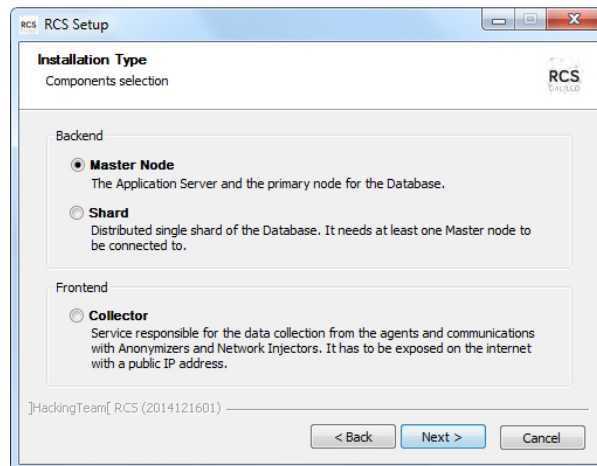
5. Fare clic su **Next**.

6. Inserire il nome o indirizzo IP del server su cui si sta installando il software e che sarà indicato alla login della RCS Console (es.: MainBEServer).



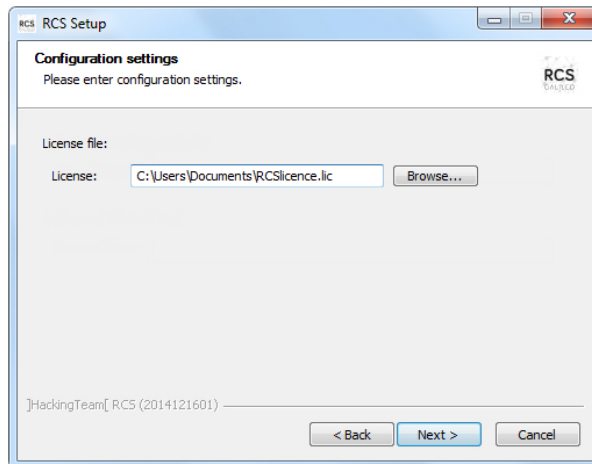
IMPORTANTE: il nome e l'indirizzo IP devono essere univoci.

7. Fare clic su **Next**.

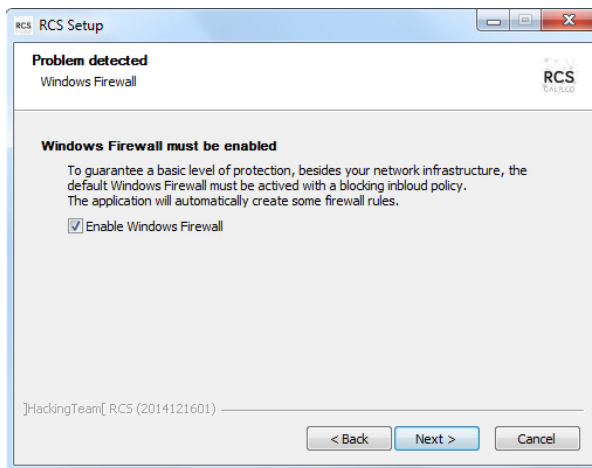
Risultato

Passi

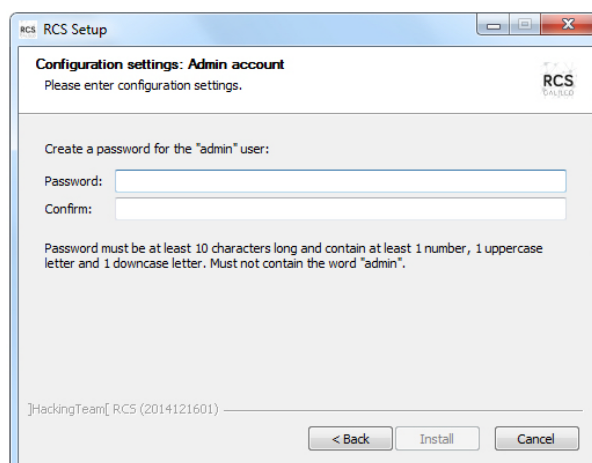
8. Selezionare il file della licenza.
9. Fare clic su **Next**.

Risultato

10. Se il sistema rileva che i firewall di Windows non sono abilitati, richiede di abilitarli. Selezionare **Enable Windows Firewall** e fare clic su **Next**.



11. Inserire la password per l'Amministratore di sistema.
12. Fare clic su **Install**: 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 l'indirizzo IP del server successivamente all'installazione vedi "[Modifica alla configurazione di Master Node](#)" a pagina 72.

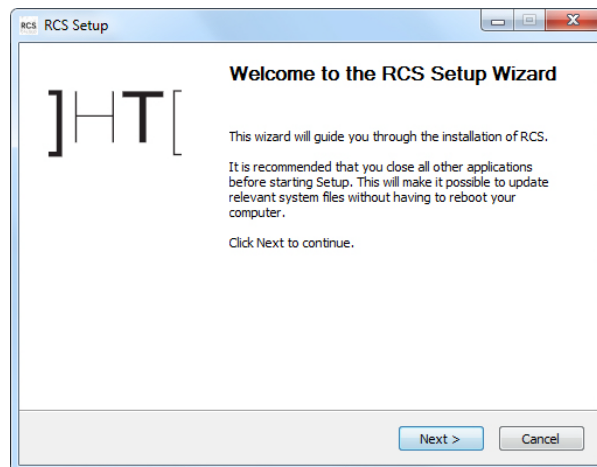
Installazione del Collector

Per installare il/i Collector in ambiente front end:

Passi

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**.

Risultato

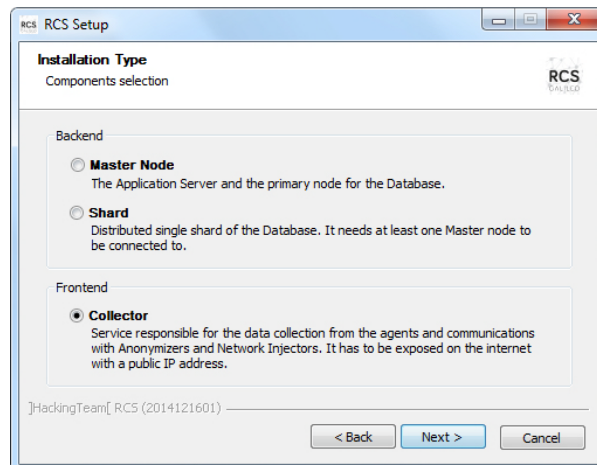


3. Selezionare **Collector**.



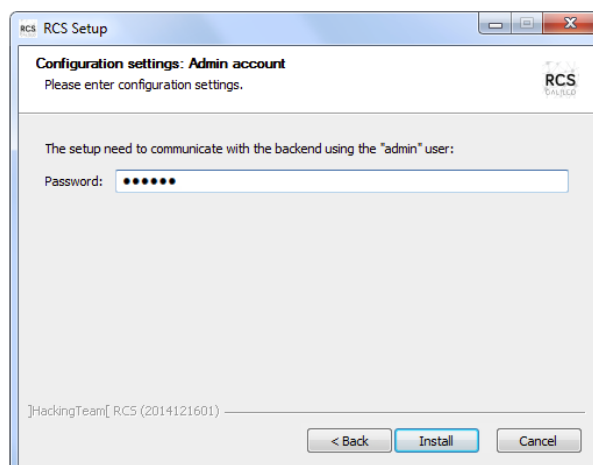
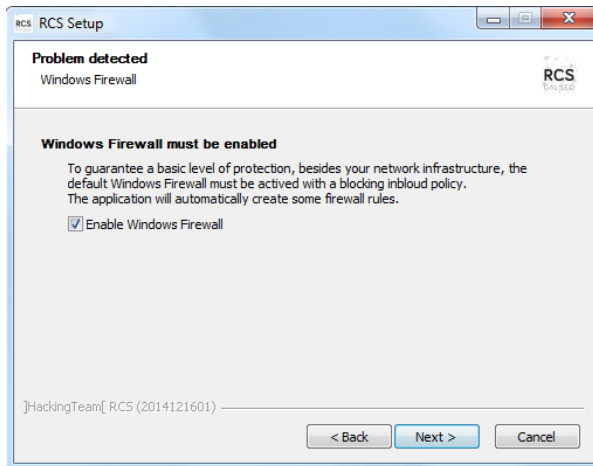
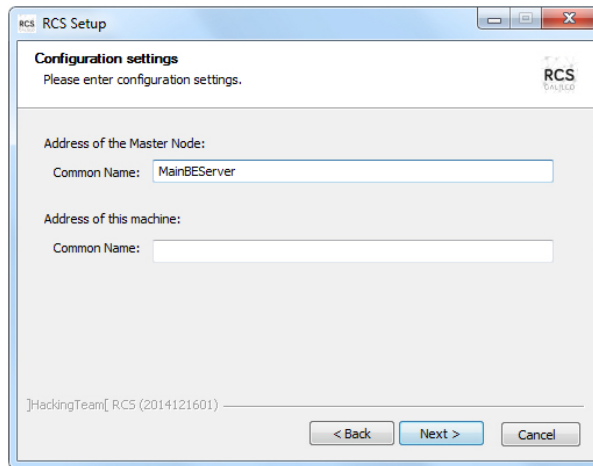
NOTA: vengono installati automaticamente tutti i servizi del Collector.

4. Fare clic su **Next**.



Passi

5. Inserire il nome o indirizzo IP del server del Master Node (es.: MainBEServer) e della macchina dove si sta installando il Collector (es.: ServerB).
6. Fare clic su **Next**: 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.
7. Se il sistema rileva che i firewall di Windows non sono abilitati, richiede di abilitarli. Selezionare **Enable Windows Firewall** e fare clic su **Next**.
8. Inserire la password dell'Amministratore di sistema indicata nell'installazione del Master Node.
9. Fare clic su **Install**: l'installazione viene avviata.

Risultato

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. Vedi "[Elenco dei servizi RCS](#)" a pagina 28.



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

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 77

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 37

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 102.



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

Modulo OCR

Introduzione

Il modulo OCR è un modulo che indicizza tutti i contenuti (es.: oltre a tutti i formati dei documenti tradizionali anche immagini, audio, video) per la ricerca full-text. Inoltre, si occupa di effettuare il "face-detection" nelle immagini per supportare l'intelligence nella creazione dei profili dei target.



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

Installazione

Il modulo OCR è installato e abilitato automaticamente con l'installazione del Master node e di eventuali shard aggiuntivi.



NOTA: il modulo è abilitato solo se previsto da licenza.

Funzionamento del modulo OCR

Di seguito la descrizione del funzionamento del modulo OCR:

Fase Descrizione

- 1 Le immagini di evidence di tipo screenshot e tutti i tipi di documenti, 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 o il documento e li 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 o documento 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.

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 è necessario aggiungere uno shard all'installazione attuale.

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

Verificare il corretto funzionamento del modulo OCR

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

Disabilitare o riabilitare il modulo OCR

Per disabilitare o riabilitare il modulo OCR, dal prompt dei comandi di Windows del Master node, eseguire rispettivamente i seguenti comandi:

- > rcs-db-config --disable-ocr
- > rcs-db-config --enable-ocr

Risultato: il modulo OCR è disabilitato/riabilitato contemporaneamente su tutti gli shard.



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

Elenco dei servizi RCS

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.

Servizi ambiente front end

I servizi dei server in ambiente front end sono:

- RCSCollector
- RCSCarrier
- RCSController

Servizi ambiente backend (Master Node)

I servizi del Master Node e le loro dipendenze sono rappresentati nello schema di seguito. Per esempio, il servizio **RCSDB** dipende sia dal servizio **RCSMasterRouter** che dal servizio **RCSMonitor**.

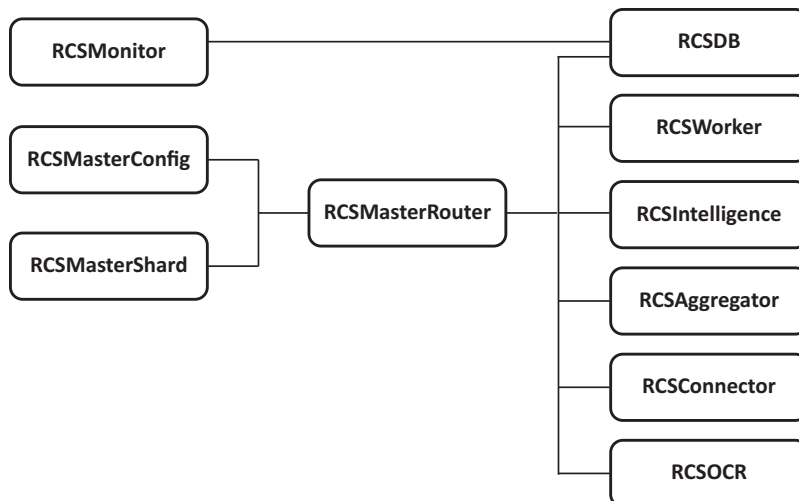


Figura 4.1: Servizi Master Node e loro dipendenze

Servizi ambiente backend (Shard)

I servizi dello Shard e le loro dipendenze sono rappresentati nello schema di seguito.

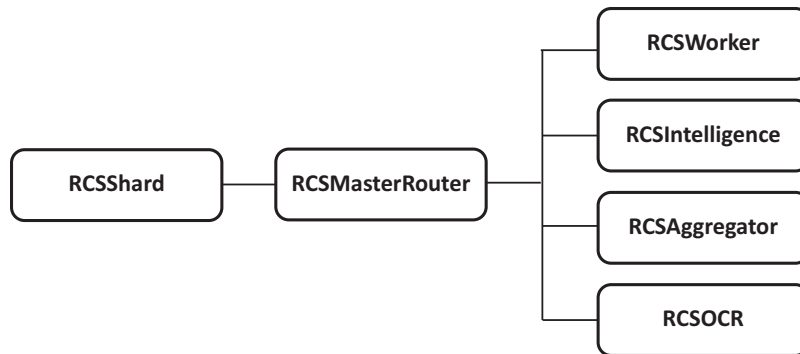


Figura 4.2: Servizi Shard e loro dipendenze

Per saperne di più

Per riavviare eventuali servizi fermi vedi "[Procedure per riavviamento dei servizi](#)" a pagina 81.

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 a uso di tutto il personale coinvolto nell'installazione di RCS.

Prerequisiti

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

- avere installato il/i server RCS
- preparare il nome o l'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:

<i>Passo</i>	<i>Azione</i>
1	Installare Adobe AIR.
2	Installare RCS Console.

Installazione di Adobe AIR

Per installare Adobe AIR:

Passi

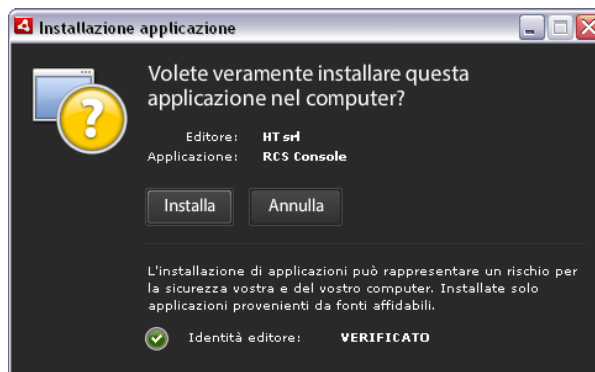
1. Installare Adobe AIR: nessuna icona compare sul desktop al termine dell'installazione.

Risultato**Installazione RCS Console**

Per installare RCS Console:

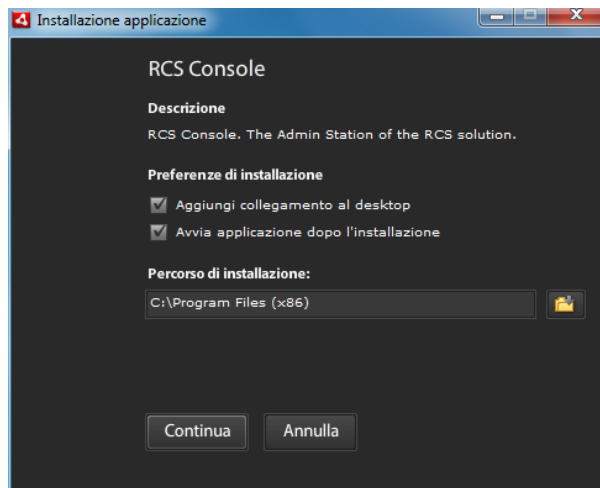
Passi

1. Eseguire il file RCSconsole-version.air.
2. Fare clic su **Installa**.

Risultato

Passi

3. Impostare eventuali preferenze.
4. Fare clic su **Continua**: RCS Console viene installata sul computer.

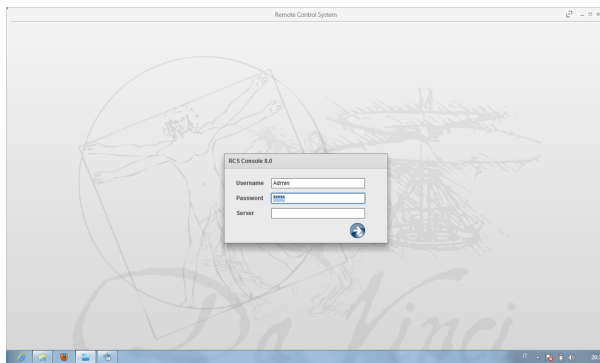
Risultato

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 a un altro uso. 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 **Nuovo utente**.


<i>Passo</i>	<i>Azione</i>
2	<p>Compilare i dati richiesti, selezionando il ruolo Amministratore e fare clic su</p> <p>Salva: 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.</p>

File installati al termine dell'installazione

File installati

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

Cartella *File contenuti*

backup	<p>La cartella contiene i file con i dati registrati nei database. Vedi "Gestione dei backup" a pagina 102</p> <p> 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.</p> <p>Percorso: C:\RCS\DB\backup</p>
bin	<p>La cartella contiene le utility (es.: rcs-db-config) per configurare i componenti di RCS. Vedi "Utility per la configurazione" a pagina 71</p> <p>Percorso: C:\RCS\DB\bin C:\RCS\Collector\bin</p>
certs	<p>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 72</p> <p>Percorso: \RCS\DB\config\certs</p>
config	<p>La cartella contiene numerosi file di configurazione del sistema. Percorso: C:\RCS\DB\config C:\RCS\Collector\config</p>

Cartella *File contenuti*

log File di log dei componenti di RCS.
Vedi "[I log di sistema](#)" a pagina 77
Percorso:
C:\RCS\DB\log
C:\RCS\Collector\log

Installazione componenti aggiuntivi

Presentazione

Introduzione

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

- Anonymizer
- Network Injector
- Database Shard
- Collector

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sugli Anonymizer	35
Installazione e configurazione degli Anonymizer	37
Cose da sapere su Network Injector Appliance	40
Installazione di Network Injector Appliance	42
Cose da sapere su Tactical Network Injector	47
Installazione di Tactical Network Injector	49
Altri applicativi installati sui Network Injector	52
Comandi Tactical Control Center e Appliance Control Center	53
Prima sincronizzazione dei Network Injector con il server RCS	54
Verifica dello stato dei Network Injector	55
Installazione componenti aggiuntivi	56

Cose da sapere sugli Anonymizer

Introduzione

Un Anonymizer serve a reindirizzare i dati di un gruppo di agent e dei Network Injector. 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.

È possibile configurare più Anonymizer in catena per aumentare il livello della protezione. Ciascuna catena fa capo a un Collector.

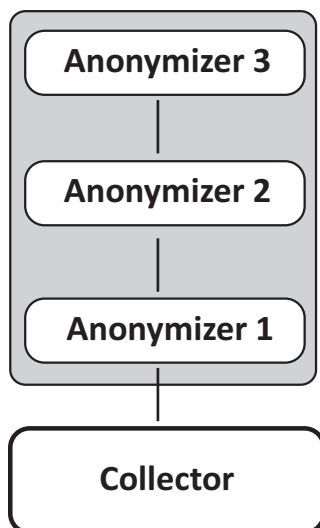


Figura 5.1: Esempio catena di Anonymizer

Stati dell'Anonymizer

Un Anonymizer può assumere diversi stati:

Stato	Simbolo in RCS Console, System, Frontend
In catena funzionante	
Non in catena	
Disabilitato	

Stato**Simbolo in RCS Console,
System, Frontend**

Anonymizer non riconosciuto perchè non entrato ancora in contatto con il Collector



Anonymizer con malfunzionamenti

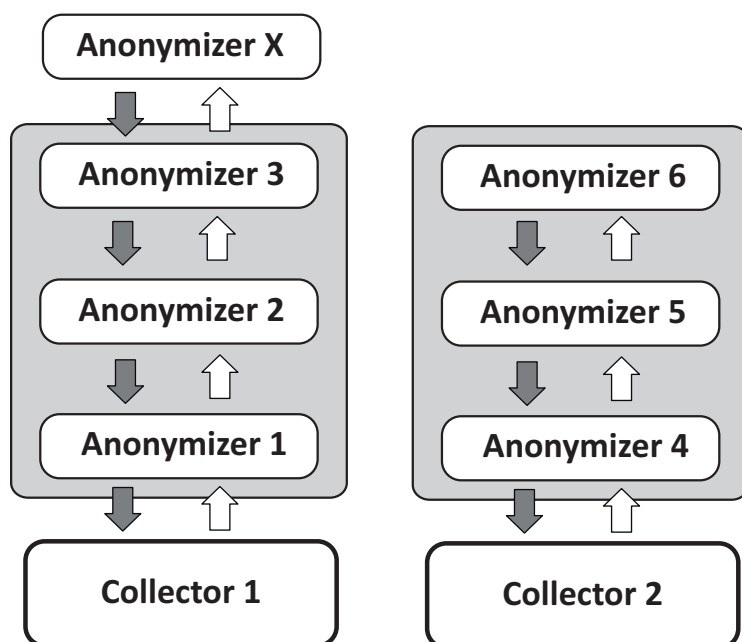
**Comunicazione tra Anonymizer e Collector**

Figura 5.2: Flusso informazioni tra Anonymizer e Collector

Una volta installato e configurato, l'Anonymizer invia lo stato e i log al Collector e riceve configurazioni e aggiornamenti dal Collector tramite la catena di Anonymizer. Per esempio, l'**Anonymizer 2** invia il suo stato all'**Anonymizer 1** che lo invia al **Collector 1**.



NOTA: se un Anonymizer non appartiene ad alcuna catena (es.: **Anonymizer X** nello schema), utilizza la prima catena di Anonymizer della configurazione per comunicare con il Collector.



NOTA: per escludere un Anonymizer da ogni comunicazione, è sufficiente disabilitarlo.

Anonymizer malfunzionante

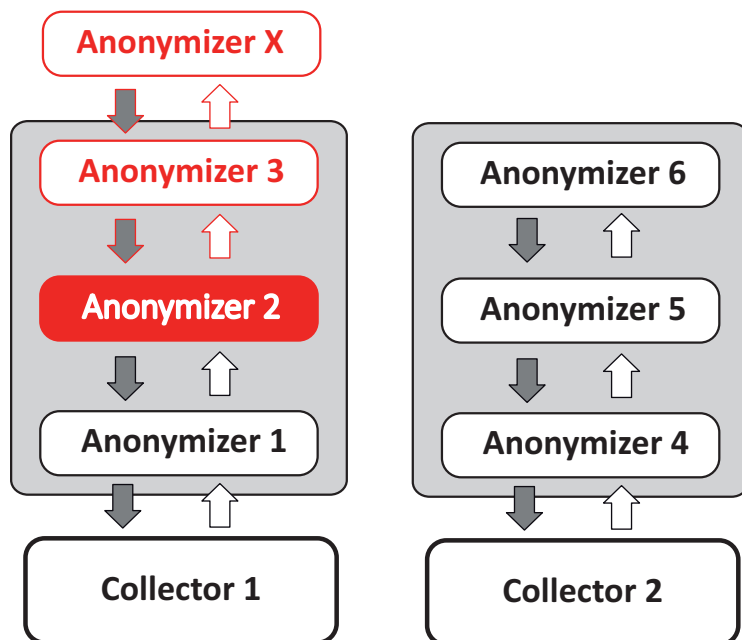


Figura 5.3: Flusso informazioni tra Anonymizer e Collector con un Anonymizer malfunzionante

Un Anonymizer malfunzionante (es. **Anonymizer 2** nello schema) interrompe la comunicazione tra il Collector e gli Anonymizer di quella catena, che quindi risultano malfunzionanti. Per continuare a lavorare con gli altri Anonymizer della catena, spostare l'Anonymizer malfunzionante fuori dalla catena e aggiornare la configurazione.

Installazione e configurazione degli Anonymizer

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 17

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**.

Passo Azione

- 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.

- 4 Fare clic su **Scarica 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.

- 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.

- 7 Da **RCS Console**, nella sezione **System, Frontend**, selezionare l'Anonymizer e fare clic su **Applica configurazione**: la nuova configurazione viene inviata all'Anonymizer dal Collector tramite la catena di Anonymizer.

Dati di un Anonymizer

Di seguito la descrizione dei dati dell'Anonymizer selezionato:

<i>Dato</i>	<i>Descrizione</i>
Nome	Nome dell'Anonymizer.
Descrizione	Descrizione libera.
Versione	Versione software. Per vedere le versioni software di tutti i componenti vedi la sezione Monitor .
Indirizzo	Indirizzo IP del VPS dove è stato installato l'Anonymizer.
Abilitato	Se abilitato, l'Anonymizer viene contattato per aggiornamenti e nuove configurazioni. Disabilitare la funzione per evitare connessioni verso Anonymizer posti in ambienti untrusted o verso Anonymizer fuori servizio.
Log	Ultimi messaggi registrati nei log. Per vedere il contenuto dei file di log vedi " I log di sistema " a pagina 77

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 64

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 **Salva**.
Risultato: lo schema viene aggiornato.
- 3 Verificare lo stato dell'Anonymizer nella sezione **Monitor**.
- 4 Fare clic su **Applica configurazione**.
Risultato: RCS si collega all'Anonymizer e trasferisce la nuova configurazione tramite la catena di Anonymizer.

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 segmento access switch o 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 nei 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.

Funzioni principali

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

Network Injector Appliance comunica con RCS tramite un Anonymizer (ed eventualmente la sua catena, vedi "[Cose da sapere sugli Anonymizer](#)" a pagina 35). La comunicazione avviene ogni 30 secondi per ricevere le regole di identificazione e di infezione e inviare lo stato e i log.

Il suo software di gestione Appliance Control Center è configurabile per l'accesso da remoto.

Connessioni alla rete

Network Injector Appliance richiede due connessioni alla rete: una per intercettare il traffico del target, l'altra per fare l'infezione con gli 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 le strette indicazioni di connessione, lasciando all'assistenza tecnica tutti quegli aspetti strategici da definire in fase di start-up e consegna.

Chiave di autenticazione

Per comunicare in sicurezza con il server RCS, sul Network Injector deve essere installata una chiave di autenticazione. La chiave deve essere generata quando si crea l'oggetto Network Injector sulla RCS Console e installata tramite Appliance Control Center alla prima sincronizzazione del Network Injector con RCS, vedi "[Prima sincronizzazione dei Network Injector con il server RCS](#)" a pagina 54.

Schema di collegamento standard

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

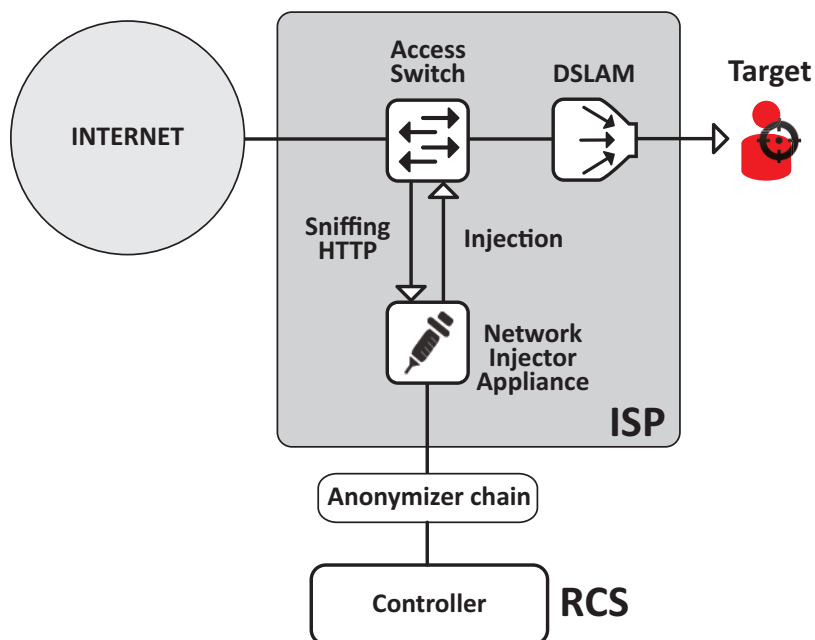


Figura 5.1: Network Injector Appliance: schema fisico

Schema di collegamento come segmento intra-switch

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

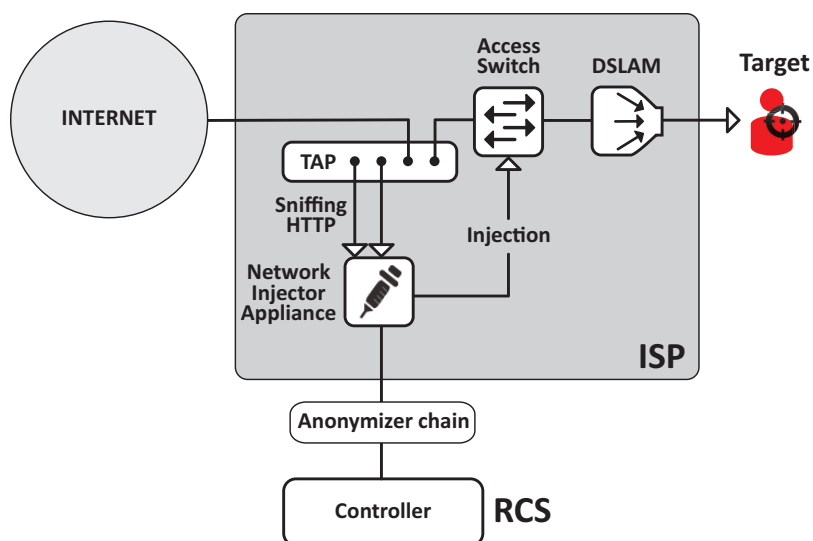


Figura 5.2: Network Injector Appliance con TAP: schema fisico

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 di installazione:


<i>Passo</i>	<i>Azione</i>	<i>Paragrafo</i>
1	Collegare Network Injector Appliance alla propria rete.	<i>"Connessioni alla rete" alla pagina successiva</i>
2	Installare il sistema operativo Network Appliance.  NOTA: all'acquisto il sistema operativo è già installato.	<i>"Installazione e configurazione del sistema operativo" a pagina 44</i>
3	Sincronizzare il Network Injector al server RCS.	<i>"Prima sincronizzazione dei Network Injector con il server RCS" a pagina 54</i>
4	Verificare lo stato del Network Injector.	<i>"Verifica dello stato dei Network Injector" a pagina 55</i>
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.
2	Scheda madre	Uscite standard PC per collegare monitor e tastiera per lanciare l'utility <code>sysconf</code> o gli eventuali aggiornamenti totali da CD di installazione. Vedi " Procedure di manutenzione ordinaria " a pagina 63
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'infezione del traffico.

Connessioni alla rete



Suggerimento: preparare Network Injector Appliance collegandolo alla propria rete e impostando i parametri prima di trasferirlo 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 infezione (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 con un disco di ripristino.

Di seguito la procedura:

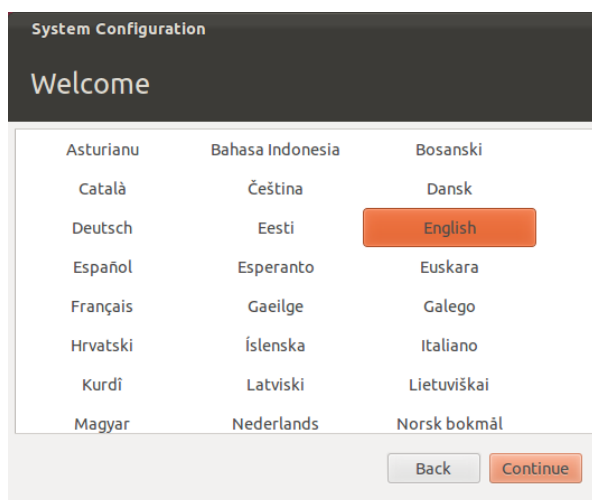
Passi

Risultato

1. Collegare in rete il computer tramite un cavo Ethernet e inserire il CD di installazione. -
2. Scegliere di installare la versione Network Appliance per server: viene avviata l'installazione del sistema operativo e al termine il computer si spegne. -
3. Riavviare il portatile. -
4. Compare la prima finestra del setup.
5. Selezionare la lingua.

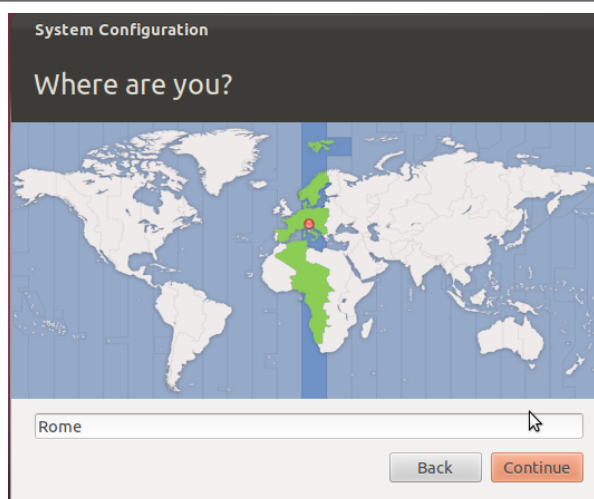


IMPORTANTE: la connessione alla rete Internet deve durare per tutta l'installazione.

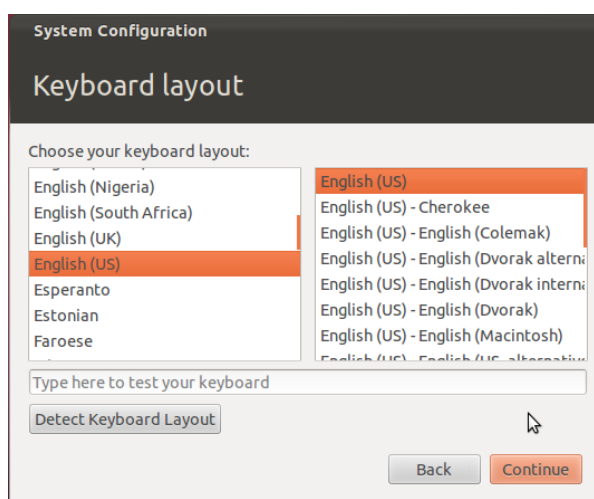


Passi

6. Selezionare il fuso orario appropriato.

Risultato

7. Viene rilevato il layout della tastiera. Cambiarlo solo se necessario.



Passi

8. Inserire i dati utente: si avvia il setup del sistema operativo.

Risultato



System Configuration

Who are you?

Your name:

Your computer's name:
The name it uses when it talks to other computers.

Pick a username:

Choose a password:

Confirm your password:

Log in automatically

Require my password to log in

Encrypt my home folder

Back Continue

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.

Verifica dell'indirizzo IP

Per verificare gli indirizzi IP del Network Injector, aprire RCS Console, sezione **Monitor**: nella colonna **Indirizzo** corrispondente al Network Injector di interesse è riportato il suo indirizzo IP.

Modifica dell'indirizzo IP

Se l'indirizzo IP dell'apparato del Network Injector cambia, nella sezione **Monitor** di RCS Console viene visualizzato un nuovo elemento. Saranno quindi presenti due elementi per quel Network Injector: uno con il nuovo indirizzo in stato verde (componente funzionante), e uno con il vecchio indirizzo in stato rosso. Eliminare l'elemento con l'indirizzo vecchio.

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 106

Cose da sapere su Tactical Network Injector

Introduzione

Tactical Network Injector è un computer portatile per installazioni tattiche in LAN o reti WiFi. Inoltre, può essere utilizzato per sbloccare la password del sistema operativo del computer del target e permettere così infezioni fisiche (es.: tramite Silent Installer).

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 principali

Tactical Network Injector identifica i dispositivi presenti in una rete WiFi o cablata e vi inietta gli agent. Opera sulle base delle regole di identificazione (automatica o manuale) e di infezione definite in RCS Console. Può inoltre collegarsi a reti WiFi protette, emulare Access Point di una rete WiFi e sbloccare la password di sistemi operativi.

Tactical Network Injector comunica con RCS tramite un Anonymizer (ed eventualmente la sua catena, vedi "[Cose da sapere sugli Anonymizer](#)" a pagina 35). La comunicazione avviene ogni 30 secondi per ricevere le regole di identificazione e di infezione e inviare lo stato e i log.

Il suo software di gestione Tactical Control Center è configurabile per l'accesso da remoto.

Connessioni alla rete

Tactical Network Injector richiede due connessioni alla rete: una per intercettare il traffico del target, l'altra per fare infezione 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).

Chiave di autenticazione

Per comunicare in sicurezza con il server RCS, sul Network Injector deve essere installata una chiave di autenticazione. La chiave deve essere generata quando si crea l'oggetto Network Injector sulla RCS Console e installata tramite Tactical Control Center alla prima sincronizzazione del Network Injector con RCS, vedi "[Prima sincronizzazione dei Network Injector con il server RCS](#)" a pagina 54.

Schema di collegamento standard

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

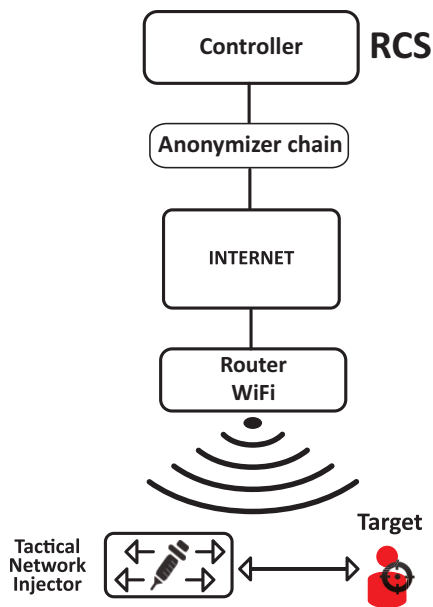


Figura 5.1: Tactical Network Injector: schema di collegamento standard

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:

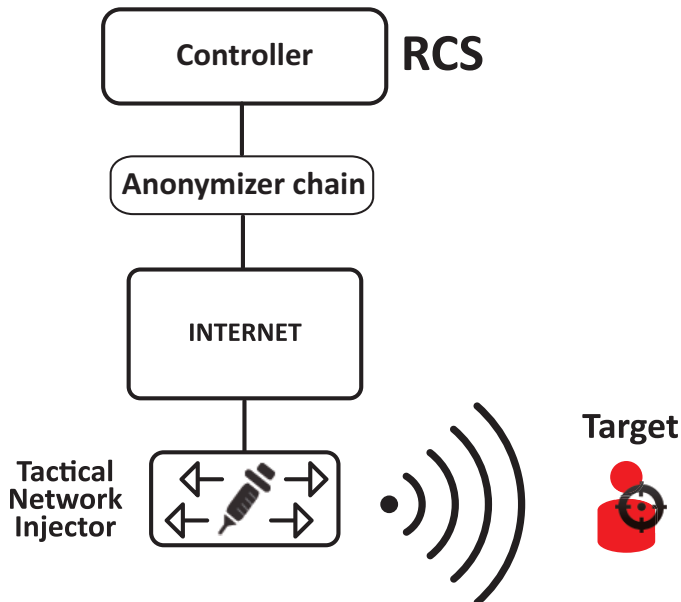


Figura 5.2: Tactical Network Injector: schema in emulazione di access point

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 di installazione:

<i>Passo</i>	<i>Azione</i>	<i>Paragrafo</i>
1	Installare il sistema operativo Tactical Device.	<i>"Installazione e configurazione del sistema operativo" nel seguito</i>
	 NOTA: all'acquisto il sistema operativo è già installato.	
2	Sincronizzare il Network Injector al server RCS.	<i>"Prima sincronizzazione dei Network Injector con il server RCS" a pagina 54</i>
3	Verificare lo stato del Network Injector.	<i>"Verifica dello stato dei Network Injector" a pagina 55</i>

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 con un disco di ripristino.

Di seguito la procedura:

<i>Passi</i>	<i>Risultato</i>
1. Collegare in rete il portatile tramite un cavo Ethernet e inserire il CD di installazione.	-

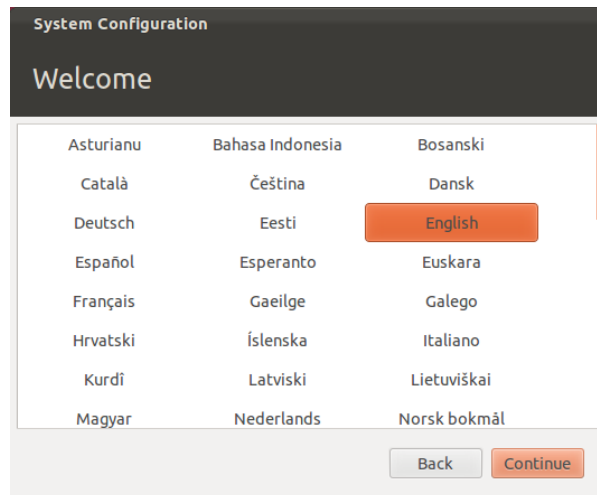
Passi

- Scegliere di installare la versione Tactical Device per pc portatili: viene avviata l'installazione del sistema operativo e al termine il computer si spegne.

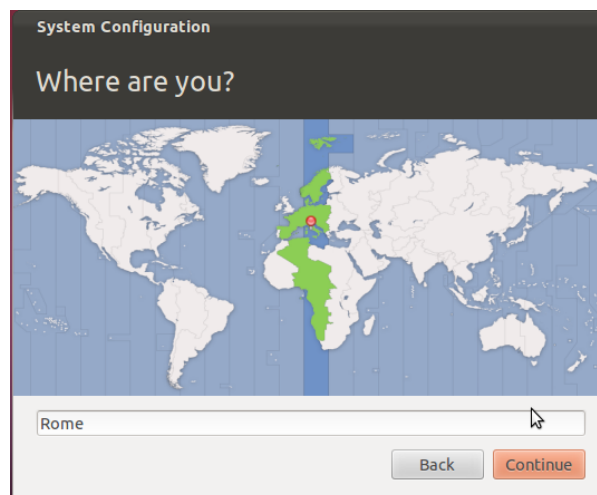


IMPORTANTE: la connessione alla rete Internet deve durare per tutta l'installazione.

- Riavviare il portatile: inserire la *passphrase* per sbloccare il disco cifrato. Al primo avvio la passphrase è "firstboot".
- Compare la prima finestra del setup.
- Selezionare la lingua.

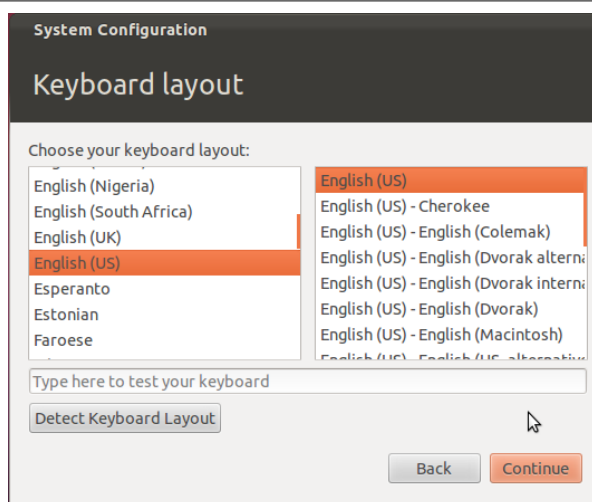
Risultato

- Selezionare il fuso orario appropriato.



Passi

7. Viene rilevato il layout della tastiera. Cambiarlo solo se necessario.

Risultato

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.

Verifica dell'indirizzo IP

Per verificare gli indirizzi IP del Network Injector, aprire RCS Console, sezione **Monitor**: nella colonna **Indirizzo** corrispondente al Network Injector di interesse è riportato il suo indirizzo IP.

Modifica dell'indirizzo IP

Se l'indirizzo IP dell'apparato del Network Injector cambia, nella sezione **Monitor** di RCS Console viene visualizzato un nuovo elemento. Saranno quindi presenti due elementi per quel Network Injector: uno con il nuovo indirizzo in stato verde (componente funzionante), e uno con il vecchio indirizzo in stato rosso. Eliminare l'elemento con l'indirizzo vecchio.

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 106

Altri applicativi installati sui Network Injector

Introduzione

I Network Injector sono forniti con installati alcuni utili applicativi realizzati da altri produttori.

Applicativi

Di seguito gli applicativi installati su Tactical Network Injector e su Network Injector Appliance:



NOTA: per istruzioni di utilizzo degli applicativi fare riferimento alla documentazione rilasciata dal produttore dell'applicativo.

<i>Nome applicativo</i>	<i>Descrizione</i>
Disniff	Pacchetto di strumenti per intercettare il traffico di rete insicuro
hping3	Generatore di traffico di rete
Kismet	Strumento di monitoraggio per reti Wireless 802.11b
Macchanger	Strumento per manipolare l'indirizzo MAC delle interfacce di rete
Nbtscan	Scanner di reti per informazioni sui nomi NetBIOS
Netdiscover	Scanner di indirizzo di rete attivo/passivo utilizzando richieste ARP
Ngrep	Grep per il traffico di rete
Nmap	Network Mapper
P0f	Strumento passivo di OS fingerprinting
Sslsniff	Strumento di attacco man-in-the-middle per traffico di rete SSL/TLS
Sslstrip	Strumento di attacco man-in-the-middle e hijacking per traffico di rete SSL/TLS

Nome applicativo	Descrizione
Tcpdump	Analizzatore di traffico di rete da riga di comando
Wireshark	Analizzatore di traffico di rete
Xprobe	Strumento remoto per l'identificazione di OS

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
<code>tactical</code>	<code>appliance</code>	Avvia l'applicativo.
<code>tactical -d oppure tactical --desync</code>	<code>appliance -d oppure appliance --desync</code>	Dissocia il sistema dal server RCS con cui è attualmente sincronizzato.
<code>tactical -l oppure tactical --log</code>	<code>appliance -l oppure appliance --log</code>	Visualizza i log del processo di infezione in corso.
		NOTA: la finestra dell'applicativo deve essere aperta.
<code>tactical -s oppure tactical --show-logs</code>	<code>appliance -s oppure appliance --show-logs</code>	Visualizza tutti i file di log salvati nel file system.
<code>tactical -r oppure tactical --report</code>	<code>appliance -r oppure appliance --report</code>	Crea un report del sistema e lo salva nella cartella Home dell'utente.

Comando Tactical Control Center	Comando Appliance Control Center	Funzione
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 la comunicazione tra il Network Injector e il server RCS e di creare e inviare le regole di sniffing e infezione. Una volta installato e sincronizzato, Network Injector interroga il server ogni 30 secondi.

Sincronizzare un Network Injector con il server RCS

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



NOTA: l'installazione della chiave di autenticazione è necessaria solo per la prima sincronizzazione.

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

Passo Azione

- 1** Da RCS Console, nella sezione **System, Network Injector** fare clic su **Nuovo Injector**.
- 2** Compilare i dati richiesti e fare clic su **Salva**.
Vedi "Dati dei Network Injector" a pagina 108
Risultato: il Network Injector compare nell'elenco e nella sezione Monitor viene aggiunto il nuovo oggetto da monitorare.
- 3** Selezionare il Network Injector appena creato e fare clic su **Esporta Chiave**
Risultato: viene generato un file .zip contenente la chiave di autenticazione.
- 4** Salvare il file .zip generato.
- 5** Da Appliance Control Center o Tactical Control Center, nella scheda **System Management**, nella sezione **Server Management**, inserire l'indirizzo IP dell'Anonymizer e la porta di comunicazione.



NOTA: la porta di comunicazione di default è la 80.

Passo Azione

- 6 Fare clic su **Import key** e selezionare il file .zip generato da RCS Console e precedentemente salvato.
- 7 Fare clic su **Configure**.
Risultato: il Network Injector inizia a comunicare con l'Anonymizer.
- 8 Da RCS Console, 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 infezione 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 richiede scambio di dati.
- nella sezione **System, Network Injectors**: 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 **Stato**: 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 **Configure**, l'operatore manualmente ha richiesto di verificare la presenza di regole nuove o aggiornamenti;
 - è stato premuto il tasto **Start** o comunque è in corso una 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 Injectors**, selezionare il Network Injector che si vuole analizzare, fare doppio clic o fare clic su **Modifica**.

Risultato: si apre la finestra con i dati del Network Injector e i log registrati.
Vedi "[Dati dei Network Injector](#)" a pagina 108



NOTA: i log vengono ricevuti e visualizzati solo se il Network Injector è sincronizzato.

Installazione componenti aggiuntivi

Introduzione

È possibile aggiungere database Shard (per grossi volumi di dati) e ulteriori Collector (uno per ogni catena di Anonymizer).



Richiede assistenza: la progettazione dell'architettura 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](#)" a pagina 20.

Sequenza di installazione

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

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

Installazione del database Shard aggiuntivo

Per installare un ulteriore database Shard in ambiente back end:

Passi

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.

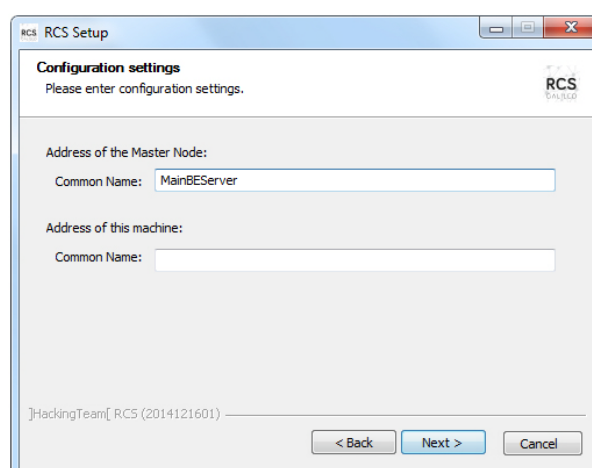
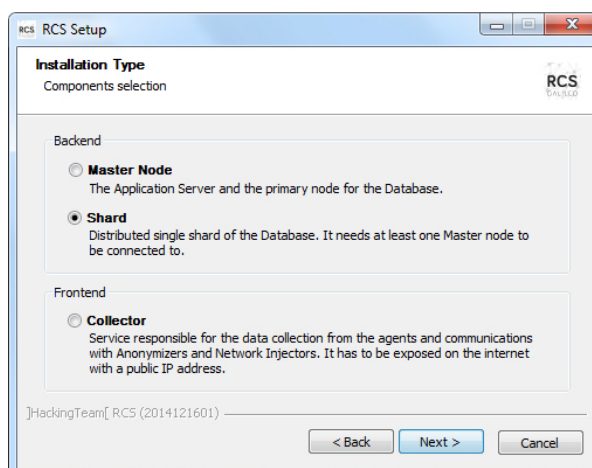
2. Fare clic su **Next**.

3. Selezionare **Shard**.

4. Fare clic su **Next**.

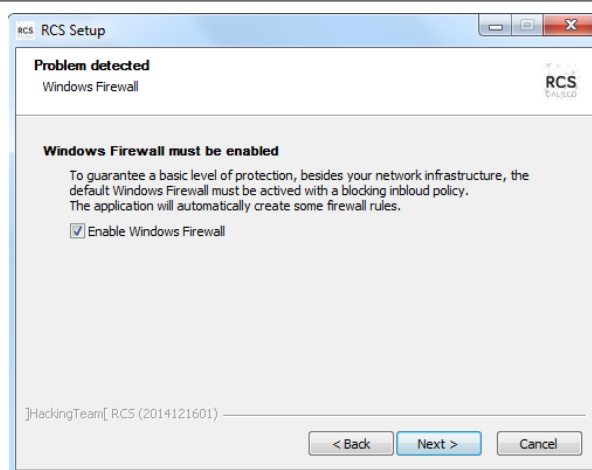
5. Inserire il nome o indirizzo IP del server del Master Node (es.: MainBEServer) e della macchina dove si sta installando lo Shard.

6. Fare clic su **Next**: 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.

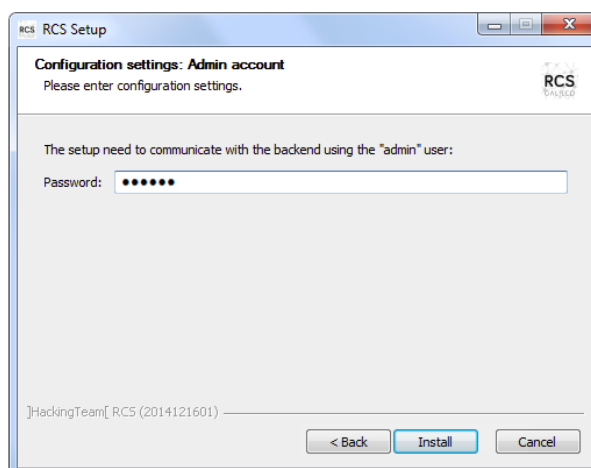
Risultato

Passi

7. Se il sistema rileva che i firewall di Windows non sono abilitati, richiede di abilitarli. Selezionare **Enable Windows Firewall** e fare clic su **Next**.

Risultato

8. Inserire la password dell'Amministratore di sistema.
9. Fare clic su **Install**: 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 72.

Installazione di Collector aggiuntivi

Per installare più Collector in ambiente front end:

Passi

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**.

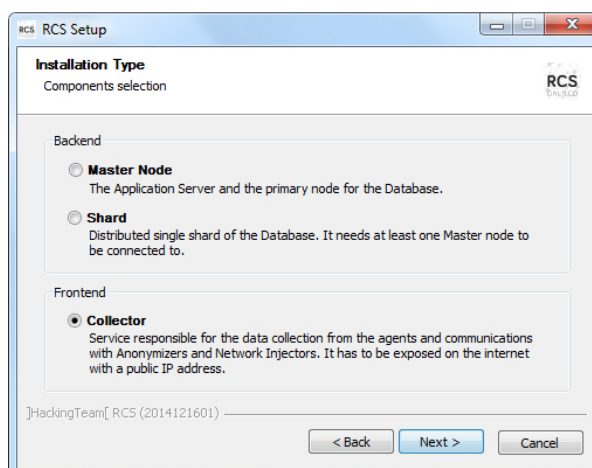
Risultato

3. Selezionare **Collector**.

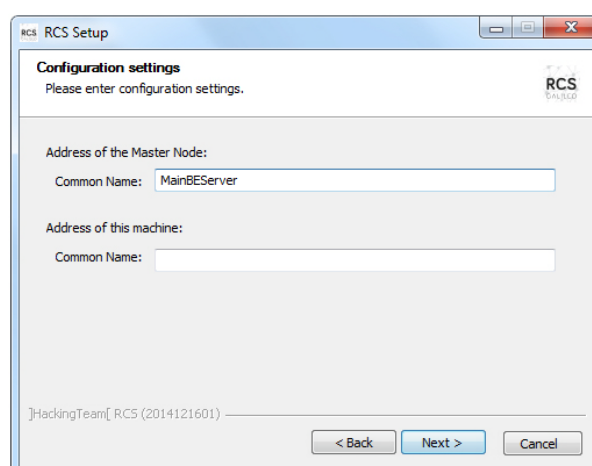


NOTA: vengono installati automaticamente tutti i servizi del Collector.

4. Fare clic su **Next**.

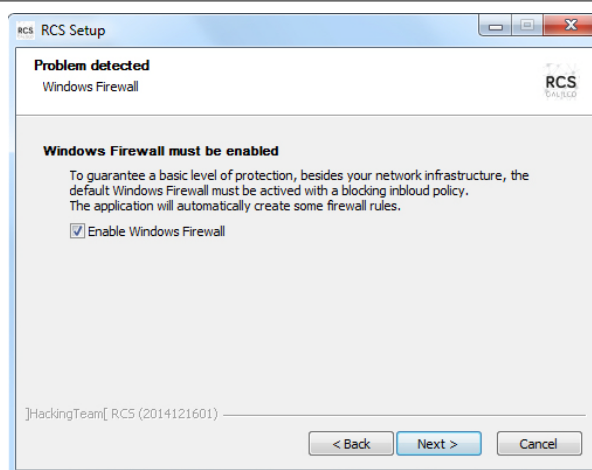


5. Inserire il nome o indirizzo IP del server del Master Noder (es.: MainBEServer) e della macchina dove si sta installando il Collector.
6. Fare clic su **Next**: al termine dell'installazione i servizi si avviano e cercano di comunicare con Master Node. Il server in ambiente back end è protetto e qualsiasi accesso esterno è reindirizzato.

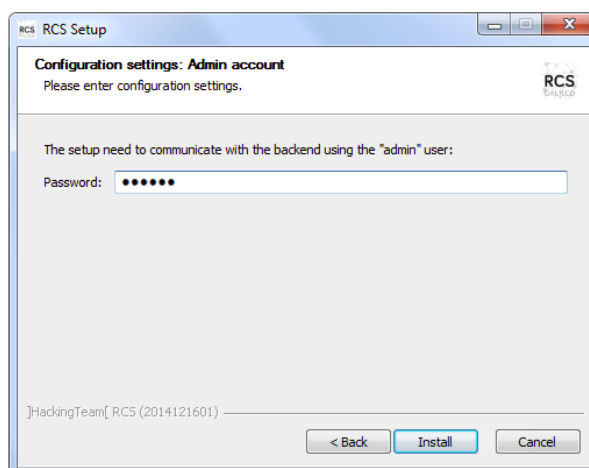


Passi

7. Se il sistema rileva che i firewall di Windows non sono abilitati, richiede di abilitarli. Selezionare **Enable Windows Firewall** e fare clic su **Next**.

Risultato

8. Inserire la password dell'Amministratore di sistema indicata nell'installazione del Master Node.
9. Fare clic su **Install**: l'installazione viene avviata.

**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. Vedi "[Elenco dei servizi RCS](#)" a pagina 28.



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

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 77

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 37

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 102.*



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

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	63
Procedure di manutenzione ordinaria	63
Aggiornamento del server RCS	63
Aggiornamento di RCS Console	64
Aggiornamento degli Anonymizer	64
Aggiornamento Network Injector Appliance	65
Aggiornamento Tactical Network Injector	67

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 a 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 alla frequenza dei backup previsti in **RCS Console** sezione **System**.

Frequenza suggerita: dipende dalla frequenza e dalla 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

A scopo precauzionale, prima di aggiornare il server RCS, eseguire i seguenti passaggi:

Passo Azione

- 1 Arrestare tutti i servizi RCS. Vedi "[Elenco dei servizi RCS](#)" a pagina 28.
- 2 Creare una copia dell'intero contenuto della cartella C:\RCS\ sia del Master Node che degli eventuali Shard aggiuntivi.
- 3 A copia ultimata, riavviare i servizi RCS.

Modalità di aggiornamento

Una volta avviato l'installer, questo identifica i componenti presenti sulla macchina e invita all'aggiornamento automatico.

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**.
- 2 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 29

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 37

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 una 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 operativo e fare il boot da CD: il contenuto del disco viene cancellato e vengono reinstallati 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 una 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 54



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

Fase Descrizione

- | Fase | Descrizione |
|------|---|
| 1 | Da RCS Console , nella sezione System, Network Injectors selezionare il Network Injector che si vuole aggiornare e fare clic su Aggiorna . |
| 2 | Alla successiva richiesta di comunicazione del Network Injector, l'Anonymizer incaricato invierà l'aggiornamento che verrà installato automaticamente. |



NOTA: il tempo di attesa per la comunicazione del Network Injector sarà massimo di un minuto. Nell'area download di RCS Console è possibile verificare lo stato di l'avanzamento dell'operazione.



NOTA: la fase di installazione inizia solo se la finestra dell'applicativo Appliance Control Center è chiusa.

Ad aggiornamento concluso, sarà 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 una infezione:



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

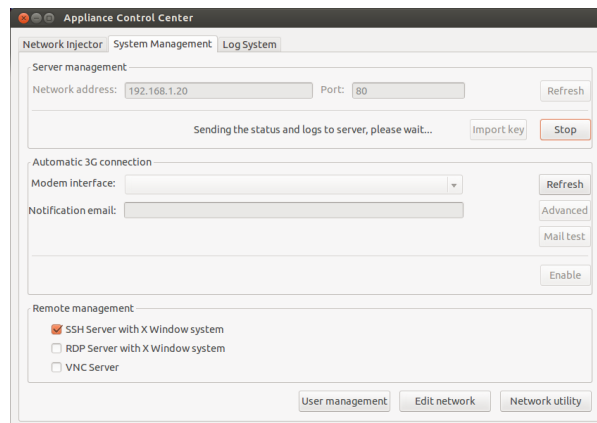
Passo

Azione

- | | |
|--|---|
| 1. Da RCS Console, nella sezione System, Network Injectors selezionare il Network Injector che si vuole aggiornare e fare clic su Aggiorna . | |
| 2. Aprire Appliance Control Center . | - |

Passo**Azione**

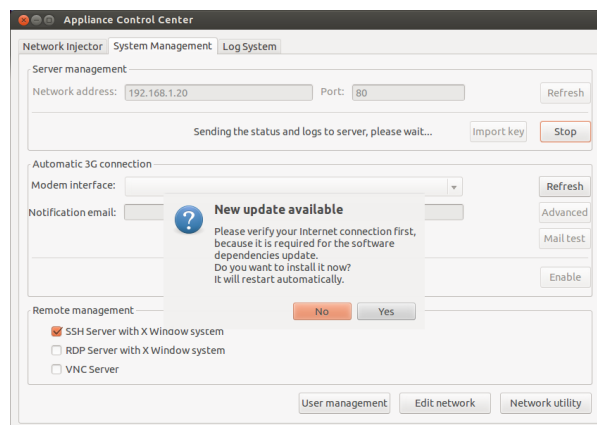
3. Nella scheda **System Management** fare clic sul pulsante **Configure**: la sincronizzazione viene abilitata.



4. Durante la sincronizzazione, Network Injector interroga RCS 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 al successivo avvio di una infezione, oppure comparirà una richiesta di autorizzazione 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](#)" nella pagina di fronte
- parzialmente vedi "[Aggiornamento parziale](#)" nella pagina di fronte

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 fare il boot da CD: il contenuto del disco viene cancellato e vengono reinstallati 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 a Internet per scaricare eventuali pacchetti aggiuntivi necessari all'aggiornamento.

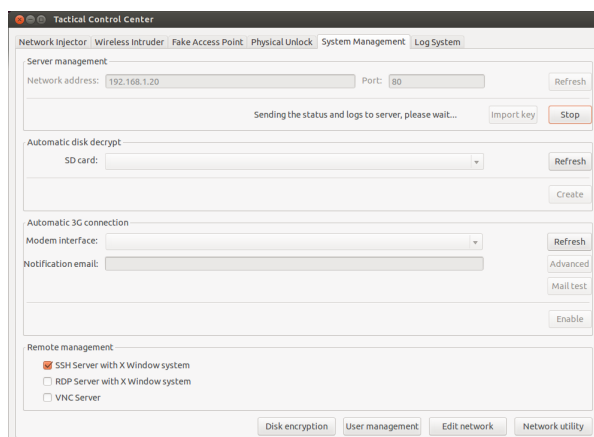
Passo

Azione

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

Passo**Azione**

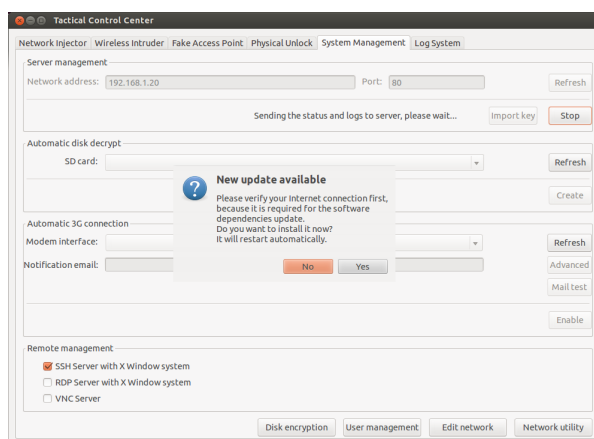
3. Nella scheda **System Management** fare clic su **Configure**: la sincronizzazione viene abilitata.



4. Durante la sincronizzazione, Network Injector interroga RCS 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.

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	71
Utility per la configurazione	71
Modifica alla configurazione di Master Node	72
Modifica alla configurazione di Collector	73
Verifica della configurazione	74

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 del 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 cartella C:\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: **rscs-db-config**
- per Collector: **rscs-collector-config**

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 > rcs-db-config -n *Nome* -g

IP del Master oppure

Node

```
> 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

la password di un > rcs-db-config -R *Username*

utente del sistema **Risultato:** viene richiesta la nuova password che viene poi salvata nel database. Questa operazione rinnova automaticamente la scadenza della password.

Per modificare... Digitare...

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:

Per...

comunicare il nuovo
nome/indirizzo IP del Master
Node

Digitare...

```
> 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

Introduzione

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"}
```

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	76
I log di sistema	77
Procedure di verifica stato componenti	79
Procedure per riavviamento dei servizi	81
Procedure di intervento sui componenti hardware	82

Malfunzionamenti possibili

Possibili problemi durante l'installazione

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

<i>Se...</i>	<i>Allora...</i>
l'installazione non avanza	controllare la presenza della chiave di protezione e inserirla correttamente.
RCS console non riesce a connettersi al server	<ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • controllare i file di log del Master Node per verificare eventuali errori.

Possibili problemi con i server

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

<i>Se...</i>	<i>E...</i>	<i>Allora...</i>
non è possibile connettersi al Master Node	la chiave di protezione è correttamente inserita, ma il servizio Master Node non è avviato	<ul style="list-style-type: none"> • controllare lo stato dei servizi del Master Node. • richiedere la sostituzione della 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	<ul style="list-style-type: none"> • 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 abilitato	controllare l'effettivo rallentamento nel log del modulo e installare un altro modulo OCR.

<i>Se...</i>	<i>E...</i>	<i>Allora...</i>
il Collector non è disponibile	-	riavviare il servizio RCS Collector.
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, e dei servizi da cui dipende.
Network Controller riporta un errore	-	collegarsi sulla macchina Collector interessata 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 le azioni suggerite:

<i>Se...</i>	<i>Allora...</i>
lo stato di un backup è error	controllare lo spazio disponibile sul 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 79*

Per riavviare i servizi *Vedi " [Procedure per riavviamento dei servizi](#) " a pagina 81*

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 per passo le operazioni di RCS e comprendere eventuali cause di malfunzionamenti (es.: servizio avviato, ma subito fermato).

Utilità dell'analisi dei log

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

<i>Componente</i>	<i>Motivazione analisi</i>
Master Node	Verificare problemi con RCS Console.
Collector	Verificare la ricezione dei dati dagli agent.

<i>Componente</i>	<i>Motivazione analisi</i>
Carrier	Verificare l'invio dei dati agli shard e al Master Node.
Modulo OCR	Verificare eventuali rallentamenti nell'indicizzazione dei contenuti estratti.
Modulo Translate	Verificare eventuali rallentamenti nella traduzione dei contenuti.
Network Controller	Verificare lo stato dei Network Injector o degli Anonymizer.
Network Injector	Verificare le operazioni effettuate.
Anonymizer	Verificare il flusso dei 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:

<i>Componente</i>	<i>Cartella</i>
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:

<i>Livello gravità</i>	<i>Descrizione</i>
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 rende 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 **racs-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 **racs-db-queue**.

Risultato: di seguito un esempio.

```

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

```

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 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_47170c3e047b6a910e7ecc2e987060db2ff06cd81 | WINDOWS | 2012-02-03 15:44:54 UTC | IDLE | 0 | 0 B |
|RCS_00000000771_47170c3e047b6a910e7ecc2e987060db2ff06cd81 | 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 decremerà 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.

Verifica dei componenti del sistema

Verificare lo stato dei componenti del sistema e visualizzare la topologia dei componenti front end e back end.

Comando

Nella cartella C:\RCS\DB\bin digitare **rcs-db-status**. Di seguito il comando per conoscere la corretta sintassi e la descrizione di tutte le opzioni:

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

Creazione file per assistenza

Creare un file .zip con tutte le informazioni necessarie per il supporto dell'assistenza tecnica.

Comando

Nella cartella C:\RCS\DB\bin o C:\RCS\Collector\bin digitare rispettivamente **rcs-db-diagnostic** o **rcs-collector-diagnostic**. Di seguito il comando per conoscere la corretta sintassi e la descrizione di tutte le opzioni:

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

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

Per esempio, l'opzione `--hide-addresses` permette di cancellare ogni riferimento agli indirizzi IP o ai nomi di dominio contenuti nei file.

Per saperne di più

Per la visualizzazione dei log vedi "[I log di sistema](#)" a pagina 77

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.



IMPORTANTE: per riavviare i servizi e per identificare la causa di anomalia, tenere conto della gerarchia di dipendenza tra i servizi. Vedi "[Elenco dei servizi RCS](#)" a pagina 28.

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

Servizio	Comandi
RCSDB	<ul style="list-style-type: none"> • > rcs-db-service start • > rcs-db-service stop • > rcs-db-service restart
MongoDB	<ul style="list-style-type: none"> • > rcs-db-mongo-service start • > rcs-db-mongo-service stop • > rcs-db-mongo-service restart
Collector	<ul style="list-style-type: none"> • > rcs-collector-service start • > rcs-collector-service stop • > rcs-collector-service restart
Carrier	<ul style="list-style-type: none"> • > rcs-carrier-service start • > rcs-carrier-service stop • > rcs-carrier-service restart

<i>Servizio</i>	<i>Comandi</i>
Network Controller	<ul style="list-style-type: none"> • > <code>rcs-controller-service start</code> • > <code>rcs-controller-service stop</code> • > <code>rcs-controller-service restart</code>
Worker	<ul style="list-style-type: none"> • > <code>rcs-worker-service start</code> • > <code>rcs-worker-service stop</code> • > <code>rcs-worker-service restart</code>
Network Injector	 PRUDENZA: utilizzare il protocollo SSH per tutte le operazioni di installazione, configurazione e trasferimento dati verso le entità remote.
<p>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.</p>	
Anonymizer	 PRUDENZA: utilizzare il protocollo SSH per tutte le operazioni di installazione, configurazione e trasferimento dati verso le entità remote.
<p>Per riavviare il servizio digitare il seguente comando:</p> <pre># /etc/init.d/bbproxy restart</pre> <p>Per fermare il servizio digitare il seguente comando:</p> <pre># /etc/init.d/bbproxy stop</pre>	
 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:

<i>Fase</i>	<i>Chi</i>	<i>Fa cosa</i>
1	Il cliente	<i>segnala a HackingTeam il guasto.</i>

Fase	Chi	Fa cosa
2	HackingTeam	<i>invia un nuovo file di licenza associato alla chiave di protezione di backup.</i>
3	Il cliente	<i>sostituisce la chiave principale con quella di backup e avvia la procedura per l'assegnazione del nuovo file di licenza.</i>
4	Il cliente	<i>invia la chiave guasta ad HackingTeam.</i>
5	HackingTeam	<i>sostituisce la chiave guasta con una nuova chiave di backup e la invia al cliente.</i>

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](#)" a pagina 20
- 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 100

Sostituzione di uno Shard

Di seguito la procedura suggerita:

Passo Azione

- 1 Rieseguire tutta la procedura di installazione.
Vedi "[Installazione server RCS](#)" a pagina 20
- 2 Ripristinare l'ultimo backup full.
Vedi "[Gestione dei backup](#)" a pagina 102

Sostituzione del Collector

Rieseguire tutta la procedura di installazione.

Vedi "[Installazione server RCS](#)" a pagina 20

Sostituzione di un Anonymizer

Rieseguire tutta la procedura di installazione.

Vedi "[Installazione e configurazione degli Anonymizer](#)" a pagina 37

Sostituzione di un Network Injector Appliance

Rieseguire tutta la procedura di installazione.

Vedi "[Installazione di Network Injector Appliance](#)" a pagina 42

Sostituzione di un Tactical Network Injector

Rieseguire tutta la procedura di installazione.

Vedi "[Installazione di Tactical Network Injector](#)" a pagina 49

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, e risolvere eventuali problemi
- aggiornare i componenti di sistema
- gestire i backup

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	86
Descrizione della homepage	87
Descrizione dei wizard da homepage	88
Elementi e azioni comuni dell'interfaccia	90
Gestione dei front end	95
Gestione dei back end	97
Cose da sapere sui backup	100
Backup completo per cause gravi	102
Gestione dei backup	102
Gestione dei connettori	104
Gestione dei Network Injector	106
Monitoraggio del sistema (Monitor)	109

Avvio di RCS Console

Introduzione

All'avvio, RCS Console chiede di inserire le proprie credenziali (nome utente e password) precedentemente impostate dall'Amministratore.



IMPORTANTE: se viene inserita per cinque volte consecutive la password sbagliata, l'utente viene disabilitato automaticamente dal sistema e non può più accedere a RCS Console. Rivolgersi all'Amministratore.

Riabilitare utenti disabilitati per inserimento password errata

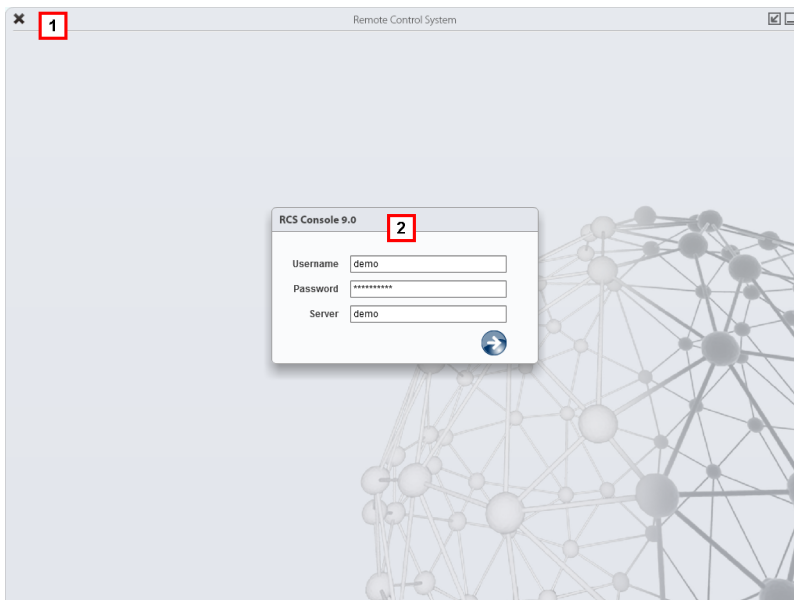
Per riabilitare un utente, sul server dal prompt dei comandi di Windows, eseguire il comando:

```
> rcs-db-config -R Username
```




Risultato: viene richiesta una nuova password, successivamente salvata nel database. Questa operazione riabilita automaticamente l'utente.

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.
- 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

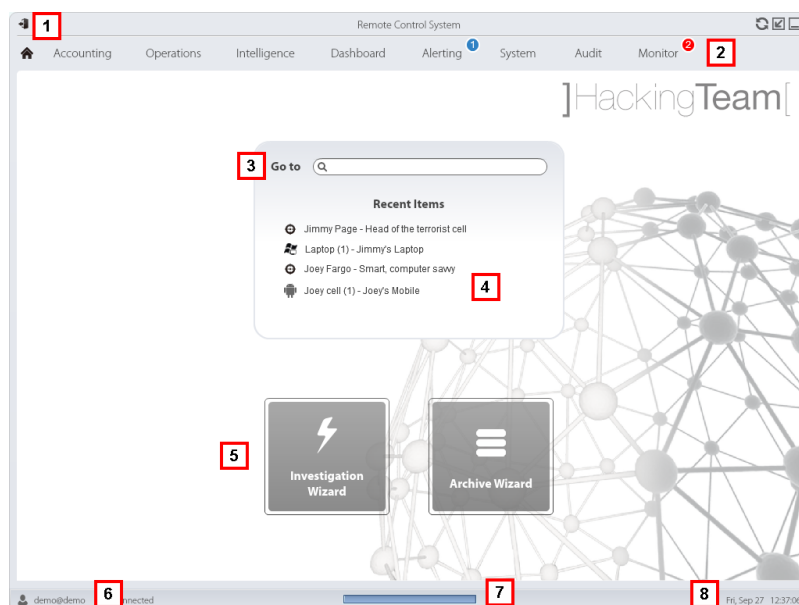
Per visualizzare l'homepage: | • fare clic su 

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

Descrizione dei wizard da homepage

Per visualizzare l'homepage:

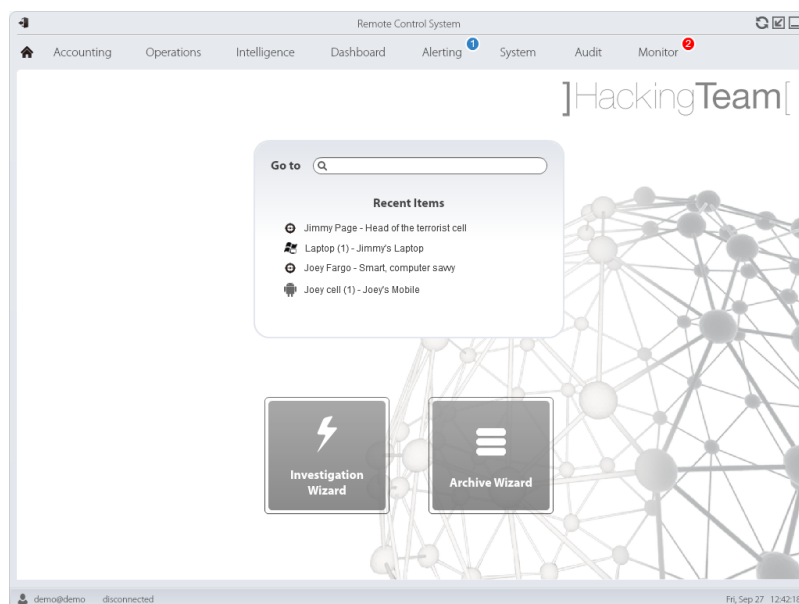
- fare clic su 

Introduzione

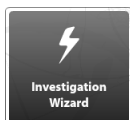
Per utenti con certi privilegi RCS Console presenta dei pulsanti che attivano dei wizard.

Come si presenta

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



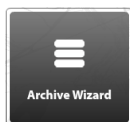
Pulsante **Funzione**



Aprire il wizard per la creazione rapida di un agent.



NOTA: pulsante abilitato solo per utenti con privilegi di Amministratore e di Tecnico.



Aprire 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.

Archiviazione Rapida

Questo wizard permette di gestire rapidamente i dati di operation o target aperti allo scopo di archivarli ed 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**

Archivia tutti i dati nel 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.

<i>Opzione</i>	<i>Descrizione</i>
Rimuovi tutti i dati dal sistema	<p>Elimina dal database tutte le evidenze dell'operation o del target selezionato. L'operation o il target restano aperti e funzionanti. Solo il database viene ridotto di dimensione.</p> <p> PRUDENZA: se combinate questa opzione con il backup istantaneo date un nome particolare al backup in modo che sia evidente che le evidenze corrispondenti sono stati eliminate dal sistema.</p>
Chiudi l'oggetto	<p>Chiude l'operation o il target selezionati.</p> <p> 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 evidenze già ricevute.</p>
Elimina l'oggetto dal sistema	<p>Elimina tutti i dati dell'operation o del target selezionati. Vengono eliminati dai database i dati dell'operation, dei target, degli agent e tutte le evidenze.</p> <p> PRUDENZA: eliminare una operation/target è un'azione irreversibile e causa la perdita dei dati associati a quella operation/target.</p>

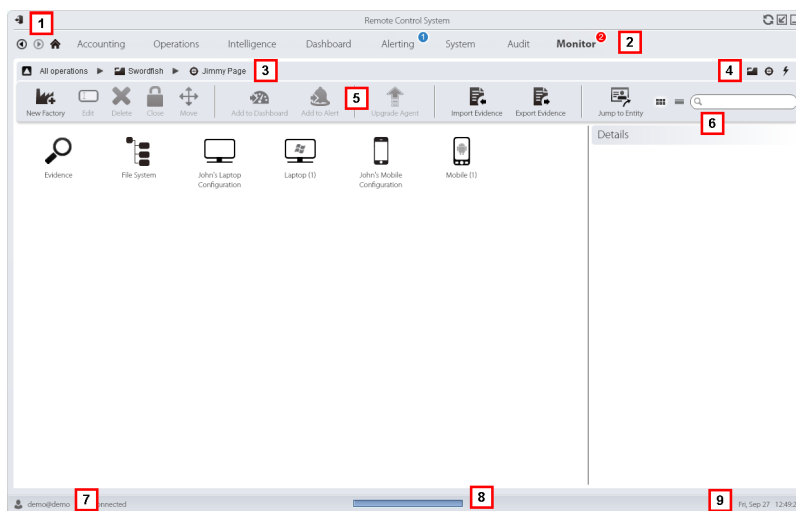
Elementi e azioni comuni dell'interfaccia

Introduzione

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 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 indietro nella cronologia di navigazione



Pulsante per andare avanti nella cronologia di navigazione



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:



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:
-  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:
-  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 una esportazione o una compilazione di vedere lo stato di avanzamento. I file sono scaricati sul desktop nella cartella RCS Download.
- Barra superiore: percentuale di generazione sul server.
 - Barra inferiore: percentuale di download dal server su RCS Console.
- 9** Data e ora attuale con la possibilità di cambiare il fuso orario.

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 **Salva** 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.
Ora UTC: data-ora di Greenwich (GMT)
Ora Locale: data-ora dove è installato il server RCS
Ora Console: data-ora della console da cui si sta lavorando e che può essere convertita
- 2 Cambiare il fuso orario e fare clic su **Salva** 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.

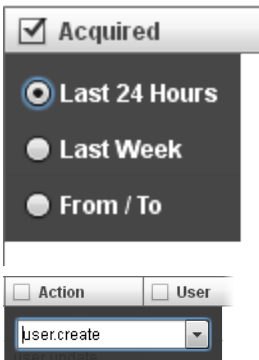
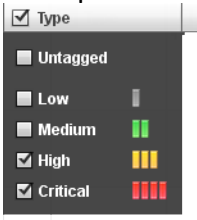
Event	Path
SYNC	Swordfish
INSTANCE	Swordfish > J
EVIDENCE	*

Filtrare un testo

Inserire parte del testo che si sta cercando: compaiono solo gli elementi che contengono il testo digitato.

L'esempio mostra elementi con descrizioni tipo:

- "my**boss**"
- "**boss**anova"

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

Gestione dei front end


Per gestire i frontend:

- sezione System, Frontend

Scopo della funzione

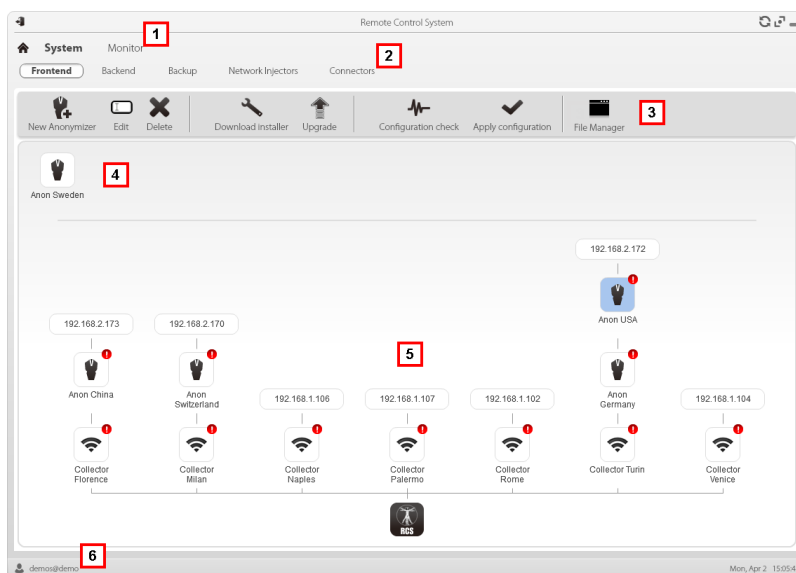
Durante il funzionamento di RCS, questa funzione permette di verificare lo stato di Anonymizer e Collector, modificare la configurazione degli Anonymizer e delle catene e aggiornare i VPS.

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 **Gestione front end**.

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:
-  Crea un nuovo Anonymizer.
 -  Modifica i dati dell'Anonymizer. Dopo la modifica fare clic su **Ricarica Log**. 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 d'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.
- 5** Catene di Anonymizer sul sistema con l'indirizzo IP dell'ultimo elemento.
-  Anonymizer (per il significato dei diversi simboli, vedi "[Cose da sapere sugli Anonymizer](#)" a pagina 35
 -  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 90.

Per le procedure di installazione, modifica, eliminazione di un Anonymizer vedi "[Installazione e configurazione degli Anonymizer](#)" a pagina 37.

Aggiungere un Anonymizer alla configurazione

Per aggiungere un Anonymizer vedi "[Installazione e configurazione degli Anonymizer](#)" a pagina 37

Modificare la configurazione di un Anonymizer

Per modificare la configurazione di un Anonymizer vedi "[Installazione e configurazione degli Anonymizer](#)" a pagina 37.

Dati del File Manager

Di seguito la descrizione:

<i>Campo</i>	<i>Descrizione</i>
Ora	Data-ora dell'installazione dei vettori sul dispositivo.
Nome	Nome del file creato dall'installer.
Factory	Factory da cui è stato generato l'installer.
Utente	Utente che ha creato l'installer.

Gestione dei back end

Per gestire i back end:  sezione System, Backend

Scopo della funzione

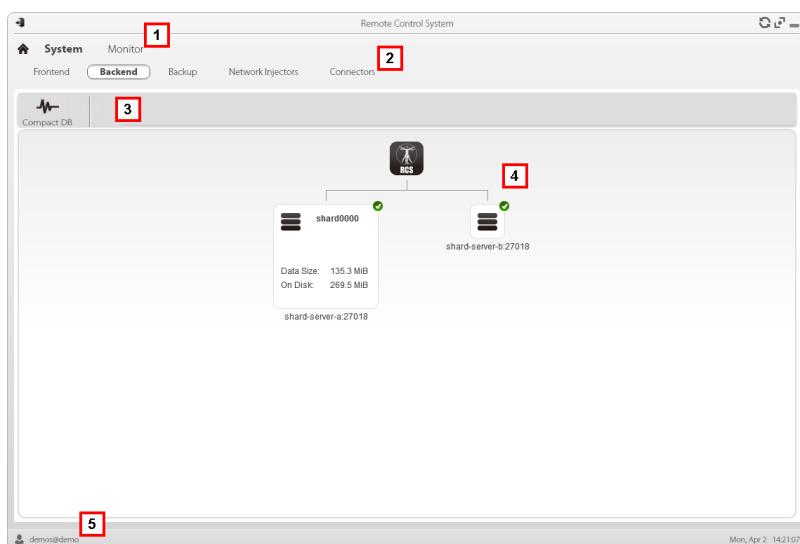
Durante il funzionamento di RCS, questa funzione permette di verificare lo stato dei database e controllare lo spazio disponibile sul disco .





NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Gestione back end**.

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:
 Compatta il database.
- 4 Struttura dei database Shard con il loro stato, lo spazio occupato sul disco e quello disponibile.
 NOTA: il database 0 è quello incluso in Master Node.
- 5 Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi dell'interfaccia vedi "[Elementi e azioni comuni dell'interfaccia](#)" a pagina 90.

Per saperne di più sui backup vedi "[Cose da sapere sui backup](#)" a pagina 100.

Dati significativi di un database Shard

Di seguito la descrizione dei dati del database Shard selezionato:

<i>Campo</i>	<i>Descrizione</i>
Spazio occupato	Spazio occupato.

<i>Campo</i>	<i>Descrizione</i>
Spazio totale	Spazio totale unità Shard.
<i>nomeServer.porta</i>	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 vario tipo.

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 72

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 evidenze raccolte. Si consiglia di effettuare un backup giornaliero.



AVVERTENZA: l'assenza di un backup metadata 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 a ogni riavvio del sistema. Non è possibile eliminare il job di default.

Backup tipo Full

Il backup **full** contiene tutte le evidenze, quindi può richiedere molto tempo. Visto che può essere ripristinato successivamente a 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 a 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 a 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). Solo i successivi possono 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").



Suggerimento: 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.

Backup completo per cause gravi

Introduzione

In casi estremi (es.: migrazione server su altro hardware, ripristino dati corrotti) è necessario eseguire un backup completo.

Eeguire il backup

Di seguito la procedura per eseguire il backup:

Passo Azione

- 1 Arrestare tutti i servizi RCS.
- 2 Creare una copia dell'intero contenuto della cartella C:\RCS\.

Ripristinare il backup

Di seguito la procedura per eseguire il ripristino:

Passo Azione

- 1 Installare un sistema RCS come fosse nuovo.
- 2 Arrestare tutti i servizi RCS.
- 3 Sostituire la nuova cartella C:\RCS\ con quella copiata precedentemente.
- 4 Riavviare i servizi.

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 istantaneo.

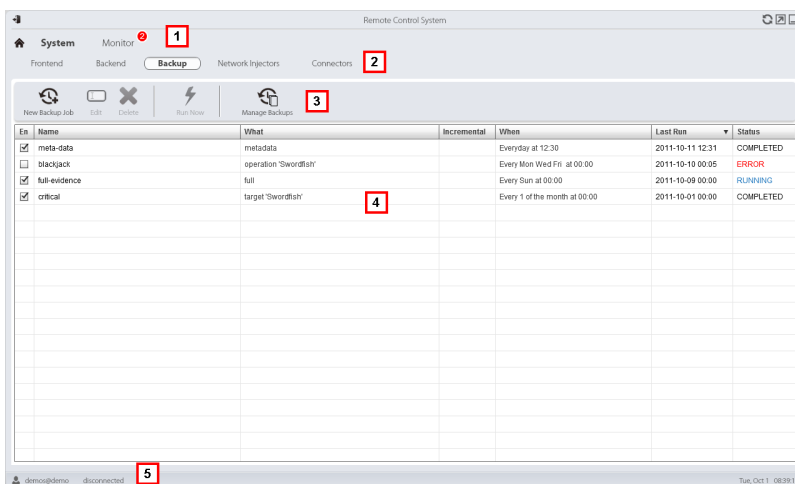
In fase di manutenzione di RCS, questa funzione permette di ripristinare dati danneggiati recuperandoli da un backup esistente.



NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Backup e ripristino sistema**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area Descrizione

- 1 Menu di RCS.
- 2 Menu **System**.
- 3 Barra con i pulsanti dedicati ai processi di backup. Di seguito la 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 l'elenco dei backup eseguiti. Di seguito la descrizione dei pulsanti:



Ripristina i dati del backup selezionato.



PRUDENZA: il ripristino dei dati è una operazione delicata. Assicuratevi di aver compreso bene il meccanismo di ripristino operato da RCS. Vedi "Cose da sapere sui backup" a pagina 100



Elimina il backup selezionato.

Area	Descrizione
------	-------------

- | | |
|---|--|
| 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 **Ab** dell'elenco.

Cosa	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 di informazioni dagli agent sono contenute 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.
-------------	---

Quando	Cadenza del backup. UTC : fuso orario.
---------------	--

Nome	Nome da assegnare al backup.
-------------	------------------------------

Gestione dei connettori



Per gestire i connettori: [sezione System, Connettori](#)

Scopo della funzione

Questa funzione permette creare delle regole di connessione con altri server RCS installati con licenze specifiche o con software di terze parti. Le evidenze ricevute da RCS saranno smistate secondo queste regole.



IMPORTANTE: questa funzione è sottoposta a licenza.

Campo	Descrizione
Percorso	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.
Tipo	Tipo di archiviazione delle evidence: <ul style="list-style-type: none"> • Local: le evidence vengono inviate a una cartella locale. • Remote: le evidence vengono inviate a sistema RCS.
Formato	Formato delle evidence. <ul style="list-style-type: none"> • JSON, XML per tipo Local • RCS per tipo Remote
Conserva l'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.
Destinazione	Percorso della cartella locale dove consegnare le evidence (es.: "C:\RCSevidence") o indirizzo IP del server RCS.  NOTA: le evidence possono essere inviate solo a server RCS con specifica licenza d'uso. Nel file di configurazione del sistema è possibile definire l'identificativo che sarà associato alle evidence inviate.

Gestione dei Network Injector

Per gestire i Network Injector: | • sezione System, Network Injectors

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
- esportare la chiave di autenticazione da installare sul Network Injector per abilitare la comunicazione con RCS Console



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

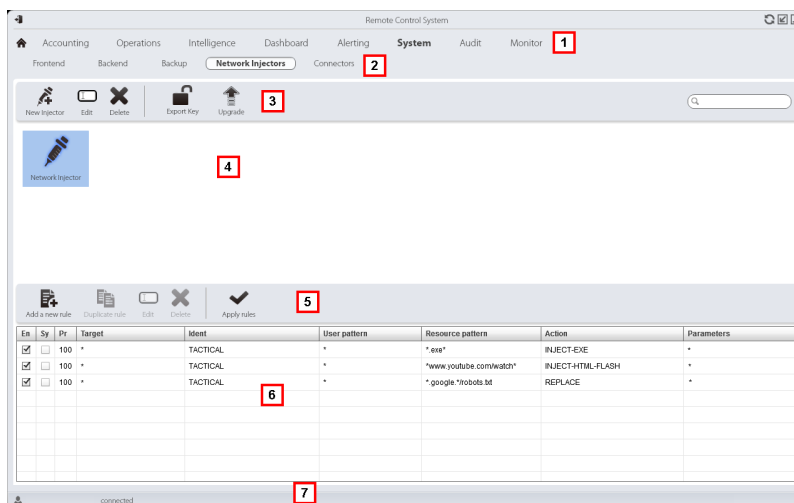
Cosa è possibile fare

Con questa funzione è possibile:

- creare un nuovo Network Injector
- esportare la chiave di autenticazione del 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**.
- 3 Barra con i pulsanti dedicati ai Network Injector. Di seguito la descrizione:



Aggiunge un nuovo Network Injector.



Modifica i dati del Network Injector e visualizza i log.



Elimina il Network Injector selezionato.




Genera un file .zip con la chiave di autenticazione del 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 65, "[Aggiornamento Tactical Network Injector](#)" a pagina 67

- 4 Elenco dei Network Injector.

Area Descrizione

- 5 Barra con i pulsanti dedicati alle regole di infezione.
Di seguito la descrizione:
 -  Apre la finestra con i dati della regola.
- 6 Elenco delle regole del Network Injector selezionato.
- 7 Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi dell'interfaccia vedi "[Elementi e azioni comuni dell'interfaccia](#)" a pagina 90.

Per saperne di più sull'installazione di un Network Injector Appliance vedi "[Installazione di Network Injector Appliance](#)" a pagina 42

Per saperne di più sull'installazione di un Tactical Network Injector vedi "[Installazione di Tactical Network Injector](#)" a pagina 49

Per saperne di più sui dati di un Network Injector vedi "[Dati dei Network Injector](#)" nel seguito

Aggiornare il software di gestione del Network Injector

Per aggiornare un Network Injector:

Passo Azione

- 1
 - Selezionare il Network Injector
 - Fare clic su **Aggiorna**: 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 55

Dati dei Network Injector

Di seguito la descrizione dei dati del Network Injector:

<i>Dato</i>	<i>Descrizione</i>
Nome	Nome del Network Injector.
Descrizione	Descrizioni libera.
Versione	Versione del software. Per vedere le versioni del software di tutti i componenti vedi " Monitoraggio del sistema (Monitor) " nella pagina di fronte.

Dato	Descrizione
Log	<p>Ultimi messaggi registrati nei log.</p> <p> NOTA: l'aggiornamento dei log del Tactical Network Injector dipendono dalla frequenza con cui l'operatore abilita la sincronizzazione.</p> <p>Per vedere il contenuto dei file di log vedi "<i>I log di sistema</i>" a pagina 77.</p> <p> Aggiorna l'elenco.</p> <p> Elimina i log visualizzati.</p>

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:

Type	Name	Address	Last contact	Status	CPU Proc	CPU Host	Disk Free
Satellite	127.0.0.1	2014-05-30 11:57:21	✓	70%	15%	20%	
Master	127.0.0.1	2014-05-30 11:57:21	✓	70%	15%	20%	
Intelligence	172.20.20.1	2014-05-30 11:57:21	✓	90%	70%	70%	
Money	172.20.20.1	2014-05-30 11:57:21	✓	90%	70%	70%	
Or	172.20.20.1	2014-05-30 11:57:21	✓	90%	70%	70%	
Anonymizer	172.20.20.1	2014-05-30 11:57:21	✓	90%	70%	70%	
Anonymizer	172.20.20.2	2014-05-30 11:57:21	✓	90%	70%	70%	
Anonymizer	172.20.20.3	2014-05-30 11:57:21	✓	90%	70%	70%	
Anonymizer	172.20.20.4	2014-05-30 11:57:21	✓	90%	70%	70%	
Anonymizer	172.20.20.5	2014-05-30 11:57:21	✓	90%	70%	70%	

Area Descrizione

1 Menu di RCS.

 **Monitor**: indica la quantità di allarmi di sistema in corso.

2 Barre con i pulsanti della finestra.

Di seguito la 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 Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi dell'interfaccia vedi "[Elementi e azioni comuni dell'interfaccia](#)" a pagina 90.

Per la descrizione dei dati presenti sulla finestra vedi "[Dati del monitoraggio del sistema \(Monitor\)](#)" nel seguito.

Eliminare un componente da monitorare

Per eliminare un componente eventualmente dismesso:

Passo Azione

1 Selezionare il componente.

2 Fare clic su **Cancella**: 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
Tipo	Tipo e nome del componente controllato.
Nome	Di seguito alcuni esempi:  Anonymizer  Carrier  Collector  Database  Network Controller
Indirizzo	Indirizzo IP del componente.
Ultimo contatto	Data-ora ultima sincronizzazione.
Stato	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 Proc	% utilizzo CPU del singolo processo.
CPU Host	% utilizzo CPU del server.
Disco libero	% 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.

<i>Dato</i>	<i>Descrizione</i>
Tipo di licenza	<p>Tipo di licenza attualmente in uso per gli agent.</p> <p>reusable: è possibile riutilizzare la licenza di un agent dopo la sua disinstallazione.</p> <p>oneshot: la licenza di un agent ha validità solo per una installazione.</p> <p> NOTA: è possibile aggiornare la licenza solo se si è in possesso dell'autorizzazione Modifica licenza.</p>
Utenti	Quantità di utenti attualmente usati dal sistema e quantità massima ammessa.
Agent	Quantità di agent attualmente usati dal sistema e quantità massima ammessa.
Desktop Mobile	Rispettivamente quantità di agent desktop e di agent mobile attualmente usati dal sistema e quantità massima ammessa.
Server distribuiti	Quantità di database attualmente usati dal sistema e quantità massima ammessa.
Collectors	Quantità di Collector attualmente usati dal sistema e quantità massima ammessa.
Anonymizers	Quantità di Anonymizer attualmente usati dal sistema e quantità massima ammessa.

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

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

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.

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. 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. Include i Collector.

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 mittente

Sistema RCS che riceve le evidence dagli agent e li trasferisce ad altri sistemi RCS riceventi (vedi) tramite le regole di connessione. È un sistema RCS completo.

RCS ricevente

Sistema RCS che riceve le evidence da un altro sistema RCS mittente (vedi) e non direttamente dagli agent. Rispetto a RCS nella sua forma completa, RCS ricevente offre solo le funzioni per elaborare le evidence.

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.

]HackingTeam[

RCS 9.6 Manuale dell'amministratore di sistema
Manuale dell'amministratore di sistema 1.9 MAR-2015
© COPYRIGHT 2015
info@hackingteam.com

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
