

RCS 8.0

The hacking suite for governmental interception

Manuale dell'amministratore

Proprietà delle informazioni

© COPYRIGHT 2012, HT S.r.l.

Tutti i diritti 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 tipografi ci 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 meglio chiarire l’utilizzo del prodotto.

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

HT S.r.l.

via della Moscova, 13

20121 Milano (MI)

Italy

Tel.: + 39 02 29 060 603

Fax: + 39 02 63 118 946

e-mail: info@hackingteam.com

Sommario

[Glossario dei termini 5](#_Toc321317370)

[Introduzione a questa Guida 8](#_Toc321317371)

[Novità della guida 8](#_Toc321317372)

[Documentazione fornita 8](#_Toc321317373)

[Convenzioni tipografiche per le segnalazioni 2](#_Toc321317374)

[Convenzioni tipografiche per la formattazione 2](#_Toc321317375)

[Destinatari del prodotto e di questa guida 3](#_Toc321317376)

[Dati di identificazione dell'autore del software 4](#_Toc321317377)

[RCS (Remote Control System) 4](#_Toc321317378)

[Differenze rispetto alle versioni precedenti 4](#_Toc321317379)

[RCS Console per l'Amministratore 5](#_Toc321317380)

[Ruolo dell'Amministratore 5](#_Toc321317381)

[Funzioni abilitate per l'Amministratore 5](#_Toc321317382)

[Avvio di RCS Console 5](#_Toc321317383)

[Come si presenta la pagina di login 5](#_Toc321317384)

[Accedere a RCS Console 6](#_Toc321317385)

[Descrizione della homepage 6](#_Toc321317386)

[Introduzione 7](#_Toc321317387)

[Come si presenta 7](#_Toc321317388)

[Elementi e azioni comuni dell'interfaccia 8](#_Toc321317389)

[Come si presenta RCS Console 8](#_Toc321317390)

[Azioni sempre disponibili sull'interfaccia 12](#_Toc321317391)

[Procedure dell'Amministratore 14](#_Toc321317392)

[Introduzione 14](#_Toc321317393)

[Procedure 14](#_Toc321317394)

[Utenti e gruppi 15](#_Toc321317395)

[Gestione degli utenti 16](#_Toc321317396)

[Scopo 16](#_Toc321317397)

[Passi successivi 16](#_Toc321317398)

[Gestione dei gruppi 19](#_Toc321317399)

[Scopo 19](#_Toc321317400)

[Cose da sapere su utenti e gruppi 21](#_Toc321317401)

[Introduzione 21](#_Toc321317402)

[Privilegi di accesso 21](#_Toc321317403)

[Funzioni abilitate per il singolo ruolo 21](#_Toc321317404)

[Gruppi di utenti per ogni operation 22](#_Toc321317405)

[Gruppi di utenti per gli allarmi di sistema 22](#_Toc321317406)

[Dati degli utenti 22](#_Toc321317407)

[Gestione delle operation 23](#_Toc321317408)

[Scopo 23](#_Toc321317409)

[Passi successivi 24](#_Toc321317410)

[Cose da sapere sulle operation 26](#_Toc321317411)

[Cos'è un'operation 26](#_Toc321317412)

[Assegnare l'operation a un gruppo di utenti 26](#_Toc321317413)

[Cosa avviene quando si crea una nuova operation 26](#_Toc321317414)

[Cosa avviene quando si chiude un'operation 27](#_Toc321317415)

[Dati delle operation 27](#_Toc321317416)

[Operation: gestire i target 27](#_Toc321317417)

[Scopo 27](#_Toc321317418)

[Cose da sapere sui target 30](#_Toc321317419)

[Cos'è un target 30](#_Toc321317420)

[Compiti dell'Amministratore 30](#_Toc321317421)

[Cosa avviene quando si crea un target 30](#_Toc321317422)

[Cosa avviene quando si chiude un target 30](#_Toc321317423)

[Apertura e chiusura di una indagine 31](#_Toc321317424)

[Dati dei target 31](#_Toc321317425)

[Monitoraggio utenti (Audit) 31](#_Toc321317426)

[Scopo 31](#_Toc321317427)

[Cosa è possibile fare 32](#_Toc321317428)

[Cose da sapere sul monitoraggio utenti (Audit) 34](#_Toc321317429)

[Cos'è il monitoraggio utenti 34](#_Toc321317430)

[Come si leggono le azioni segnalate 34](#_Toc321317431)

[La selezione delle azioni interessanti tramite i filtri 35](#_Toc321317432)

[Dati esportabili 35](#_Toc321317433)

[Dati del monitoraggio utenti (Audit) 35](#_Toc321317434)

[Monitoraggio del sistema (Monitor) 36](#_Toc321317435)

[Scopo 36](#_Toc321317436)

[Dati del monitoraggio del sistema (Monitor) 38](#_Toc321317437)

[Dati di monitoraggio dei componenti del sistema 38](#_Toc321317438)

[Dati di monitoraggio delle licenze 38](#_Toc321317439)

Glossario dei termini

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

Accounting

Sezione di RCS Console dedicata alla gestione degli accessi a RCS.

Agent

Sonde software installate sui dispositivi sotto monitoraggio. Sono deputati a intercettare i dati e comunicarli a un Anonymizer o, in assenza di questo, direttamente al Collector.

Alerting

Sezione di RCS 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 intercettazioni in essere, gli obiettivi delle intercettazioni e il tipo di dati da rilevare.

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 l'attività di intercettazione.

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 di RCS Console dedicata al controllo delle azioni dei vari utenti.

avvisi da Evidence

segnalazioni che generano Email verso gli analisti che informano quando è stata intercettata una prova importante (Evidence)

back end

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

BRAS

(Broadband Remote Access Server) instrada il traffico da/a dal DSLAM verso la rete dell'ISP.

Collector

Riceve i dati inviati dagli Agent, direttamente o tramite la catena di Anonymizer.

Console

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

Dashboard

Sezione di RCS Console dedicata all'Analista. Qui è possibile inserire Operation, Target e Agent che si vogliono tenere sotto controllo.

DSLAM

(Digital Subscriber Line Access Multiplexer) apparato elettronico di trasmissione di rete che esplica le funzioni di multiplazione/demultiplazione di linea di accesso numerica e modulazione da e verso il doppino dell'utente finale, cioè nella rete di accesso.

Evidence

Dati di una intercettazione che costituiscono una prova. Il formato dipende dalla configurazione dell’ Agent installato (es.: immagine).

Factory

È un template per la configurazione e compilazione degli Agent in base al vettore di infezione scelto.

front end

Ambiente destinato a comunicare con la rete esterna, raccogliere le informazioni e controllare e configurare le entità remote di intercettazione. In architettura distribuita include il Collector e il Network Controller.

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.

Monitor

Sezione di RCS Console dedicata alle segnalazioni degli stati dei componenti e delle licenze.

Network Controller

Componente che controlla lo stato dei Network Injectore e degli Anonymizer, spedendo loro le nuove configurazioni o aggiornamenti software.

Network Injector

Componente hardware. Può essere installato presso un ISP (Internet Service Provider) in versione fissa, oppure può essere collegato ad un hotspot WiFi o ad una rete wired locale in versione portatile.

Network Injector Appliance

Versione appliance di Network Injector. Unità rack per installazione presso ISP. Cfr.: Tactical Network Injector.

Operation

Indagine composta da uno o più Target, a loro volta a loro volta associati ad uno o più Agent.

RCS

(Remote Control System) il sistema di monitoraggio in oggetto.

RCS Console

Software dedicato all'interazione con RCS Server.

RCS Server

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

regole di allerta

Regole che permettono di essere avvisati all'arrivo di prove particolari.

Regole di injection

Parametri che permettono la selezione del traffico HTTP originato dai dispositivi del Target e la successiva infezione delle risorse visualizzate e scaricate.

Sequenze di intercettazione

Insieme di eventi, azioni e moduli di registrazione complessi che costituiscono la configurazione avanzata di un Agent.

SSH

(Secure SHell) protocollo di comunicazione per stabilire una sessione remota cifrata.

System

Sezione di RCS Console dedicata alla gestione del sistema.

Tactical Network Injector

Versione portatile di Nework 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 da sottoporre a intercettazione attiva o passiva.

Tecnico

Colui che su mandato dell'Amministratore crea e gestisce gli Agent di intercettazione.

VPS

(Virtual Private Server) server remoto su cui installare l'Anonymizer. Disponibili come servizio a noleggio.

Introduzione a questa Guida

Presentazione

Obiettivi del manuale

Questo manuale guida l'Amministratore a utilizzare RCS Console per:

* creare gli utenti e i gruppi di lavoro
* aprire e chiudere indagini
* fare il monitoraggio degli utenti di RCS
* fare il monitoraggio del sistema

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

Contenuti

Questa sezione include i seguenti argomenti:

Novità della guida

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

| Data rilascio | Codice | Versione software | Descrizione |
| --- | --- | --- | --- |
| 16 Aprile 2012 | Manuale dell'amministratore  1.0 FEB/2012  Administrator's Guide  1.0 FEB/2012 | 8.0 | Prima pubblicazione |

Documentazione fornita

A corredo del software RCS sono forniti i seguenti manuali:

| Manuale | Destinatari | Codice | Formato di distribuzione |
| --- | --- | --- | --- |
| Manuale dell'amministratore di sistema | Amministratore di sistema | Manuale dell'amministratore di sistema - 1.0 FEB/2012 | PDF |
| Manuale dell'amministratore (questo manuale) | Amministratori | Manuale dell'amministratore - 1.0 FEB/2012 | PDF |
| Manuale del tecnico | Tecnici | Manuale del tecnico - 1.0 FEB/2012 | PDF |
| Manuale dell'analista | Analisti | Manuale dell'analista - 1.0 FEB/2012 | 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.

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

Convenzioni tipografiche per la formattazione

Di seguito la legenda di alcune convenzioni tipografiche:

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

Destinatari del prodotto e di questa guida

Di seguito le figure professionali che interagiscono con RCS.

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

Dati di identificazione dell'autore del software

HT S.r.l.

via della Moscova, 13

20121 Milano (MI)

Italy

Tel.: + 39 02 29 060 603

Fax: + 39 02 63 118 946

e-mail: info@hackingteam.com

RCS (Remote Control System)

Presentazione

Introduzione

RCS (Remote Control System) è uno strumento a supporto delle investigazioni che attua intercettazioni attive e passive di dati e informazioni relative alle attività 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:

Differenze rispetto alle versioni precedenti

Di seguito le differenze rispetto alla versione RCS 7.6.

Terminologia

| RCS v. 7.6 | RCS 8.0 e successive |
| --- | --- |
| Activity | Operation |
| Agente | Module |
| Anonymizer chain | Anonymizing chain |
| Backdoor | Agent |
| Backdoor Class | Factory |
| Collection Node (ASP) | Collector |
| Injection Proxy Appliance (IPA) | Network Injector Appliance |
| Log Repository (RCSDB) | Master Node e Shard aggiuntivi |
| Mobile Collection Node (RSSM) | Collector |
| RCSAnon | Anonymizer |

RCS Console per l'Amministratore

Presentazione

Ruolo dell'Amministratore

Il ruolo dell'Amministratore è:

* gestire l'accesso al sistema attribuendo ai diversi utenti i ruoli previsti dall'applicazione
* avviare e chiudere le indagini
* definire i target coinvolti
* indicare all'utente Tecnico i tipi di prove da intercettare
* controllare le azioni svolte dagli utenti
* controllare le licenze disponibili per i componenti di RCS

Funzioni abilitate per l'Amministratore

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

* Accounting
* Operation
* Audit
* Monitor

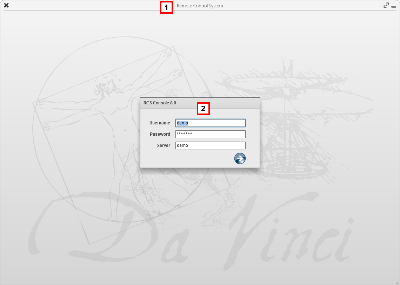
Questa sezione include i seguenti argomenti:

Avvio di RCS Console

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

Come si presenta la pagina di login

Ecco come viene visualizzata la pagina di login:



| Area | Descrizione |
| --- | --- |
| 1 | Barra del titolo con pulsanti di comando:  Uscita da RCS e 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 | Fare clic su : si presenta l'homepage con i menu abilitati in base ai privilegi del proprio account. Vedi "Descrizione della homepage". |

Descrizione della homepage

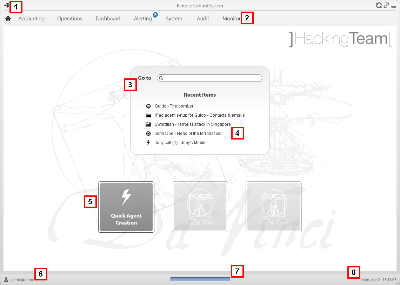
|  |  |
| --- | --- |
| Per visualizzare l'homepage: | * fare clic su |

Introduzione

RCS Console presenta all'avvio questa homepage. L'homepage è identica per tutti gli utenti. Solo i menu abilitati dipendono dai ruoli assegnati al proprio account.

Come si presenta

Ecco come viene visualizzata l'homepage con già presente una cronologia. 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. |
| 4 | Collegamenti agli ultimi cinque elementi aperti (operation, target e agent). |
| 5 | Pulsanti per avvio del Wizard. |
| 6 | Utente connesso con possibilità di cambiare la lingua e la password. |
| 7 | Area download con possibilità durante l'esportazione o una compilazione di vedere lo stato di avanzamento. |
| 8 | Data e ora attuale con possibilità di cambio fuso orario. |

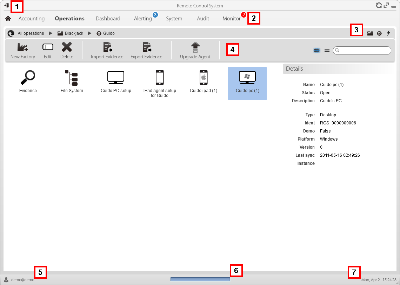
Elementi e azioni comuni dell'interfaccia

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

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

Come si presenta RCS Console

Ecco come viene visualizzata una pagina tipica di RCS Console, in questo esempio la pagina di un target:



| Area | Descrizione |
| --- | --- |
| 1 | Barra del titolo con pulsanti di comando:  Logout da RCS.  Pulsante di aggiornamento della pagina.  Pulsante di ingrandimento della finestra.  Pulsante di riduzione a icona della finestra. |
| 2 | * Pulsante per tornare alla homepage  * Menu di RCS con le funzioni abilitate per l'utente |
| 3 | Barra di navigazione per l'operation. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Torna indietro di un livello | |  | Mostra la pagina dell'operation | |  | Mostra la pagina del target | |  | Mostra la pagina della factory | |  | Mostra la pagina dell'agent | |
| 4 | Pulsanti per visualizzare tutti gli elementi indipendentemente dalla loro appartenenza. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Mostra tutte le operation | |  | Mostra tutti i target | |  | Mostra tutti gli agent | |
| 5 | Barra con i pulsanti della finestra. |
| 6 | Pulsanti e casella di ricerca:   | Oggetto | Descrizione | | --- | --- | |  | Casella di testo con ricerca. Inserendo parte del nome compare l'elenco degli elementi che contengono le lettere inserite. | |  | Visualizza gli elementi in una tabella | |  | Visualizza gli elementi con le icone | |
| 7 | Utente connesso con possibilità di cambiare la lingua e la password |
| 8 | Area download con possibilità durante un'esportazione o una compilazione di vedere lo stato di avanzamento. I file sono scaricati sul desktop nella cartella RCS\_download.   * barra superiore: percentuale generazione sul server. * barra inferiore: percentuale download dal server su RCS Console. |
| 9 | Data e ora attuale con possibilità di cambio fuso orario. |

Azioni sempre disponibili sull'interfaccia

Cambiare la lingua dell'interfaccia o la propria password

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

| Passo | Azione |
| --- | --- |
| 1 | Fare clic su [6] compare una finestra di dialogo con i dati dell'utente. |
| 2 | Cambiare lingua o password e fare clic su 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 [8] compare una finestra di dialogo con la data-ora attuale:  Ora UTC: data-ora di Greenwitch (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 per confermare e uscire: tutte le date-ora visualizzate sono convertite come richiesto. |

Altre azioni comuni

Di seguito la descrizione delle azioni su oggetti di interfaccia, comuni a più funzioni:

| Azione | Descrizione |
| --- | --- |
| Per ordinare una tabella | Fare clic sull'intestazione della tabella. |
| Per cambiare dimensione delle colonne | Selezionare il bordo della colonna e trascinarlo. |

Procedure dell'Amministratore

Introduzione

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

Procedure

Predisporre RCS all'uso di altri utenze

Di seguito le procedure tipiche per predisporre RCS all'uso da parte di altre persone:

| Passo | Azione |
| --- | --- |
| 1 | Nella sezione Accounting, Users definire le persone che avranno accesso a RCS.  Vedi "Gestione degli utenti" |
| 2 | Nella sezione Accounting, Groups creare un gruppo di utenti (tipicamente amministratori di sistema, non associati a operation) cui destinare le mail di segnalazione di sistema in allarme  Vedi "Gestione dei gruppi" |
| 3 | Nella sezione Monitor selezionare il gruppo destinato a ricevere email di segnalazione di sistema in allarme.  Vedi "Monitoraggio del sistema (Monitor)" |

Aprire un'indagine

Di seguito le procedure tipiche per aprire un'indagine:

| Passo | Azione |
| --- | --- |
| 1 | Nella sezione Accounting, Users definire le persone che faranno parte della squadra coinvolta nell'indagine e i loro ruoli.  Vedi "Gestione degli utenti" |
| 2 | Nella sezione Accounting, Groups definire la squadra abilitata a vedere i dati dell'indagine e a ricevere gli allarmi di sistema.  Vedi "Gestione dei gruppi" |
| 3 | Nella sezione Operation aprire l'indagine e associarvi uno o più gruppi.  Vedi "Gestione delle operation"e "Operation: gestire i target" |
| 4 | Comunicare al Tecnico di RCS i tipi di prove da intercettare. |
| 5 | Nella sezione Audit controllare l'accesso al sistema da parte della squadra e verificare le loro azioni.  Vedi "Monitoraggio utenti (Audit)" |

Chiudere un'indagine

Di seguito la procedura tipica per chiudere un'indagine:

| Passo | Azione |
| --- | --- |
| 1 | Nella sezione Operation chiudere l'indagine.  Vedi "Gestione delle Operation" |
| 2 | Se necessario richiedere all'Amministratore di sistema il salvataggio delle evidence in un Backup. |

Monitorare il sistema

Di seguito le procedure tipiche per monitorare l'utilizzo di RCS:

| Passo | Azione |
| --- | --- |
| 1 | Nella sezione Monitor controllare eventuali segnalazioni del sistema e controllare le licenze utilizzate rispetto alle licenze acquistate.  Vedi "Monitoraggio del sistema (Monitor)" |
| 2 | Nella sezione Audit controllare le azioni compiute da Tecnici, Analisti e altri Amministratori.  Vedi "Monitoraggio utenti (Audit)" |

Utenti e gruppi

Presentazione

Introduzione

La gestione degli utenti e dei gruppi è fondamentale per garantire la riservatezza e la sicurezza dei dati.

Contenuti

Questa sezione include i seguenti argomenti:

Gestione degli utenti

|  |  |
| --- | --- |
| Per gestire  gli utenti: | * sezione Accounting, Users |

Scopo

Questa funzione permette di:

* registrare un utente e permettergli l'accesso a determinate funzioni di RCS. Da quel momento l'utente potrà collegarsi e vedere le funzioni in base ai ruoli assegnati
* disabilitare temporaneamente l'utente all'accesso, per esempio in caso di assenza prolungata
* disconnettere immediatamente l'utente da RCS, per esempio in caso di sospetto di accesso illegale a RCS
* controllare la data-ora e l'indirizzo IP dell'ultima connessione dell'utente a RCS e altri suoi dati

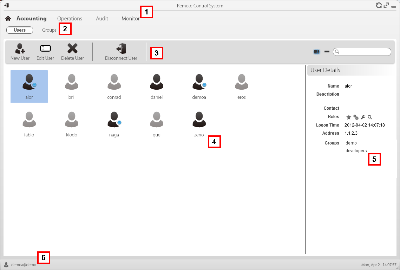
Per bloccare un utente e impedirgli un qualsiasi accesso a RCS si suggerisce di disconnetterlo immediatamente (se è connesso) e subito disabilitarlo.

Passi successivi

È possibile associare più utenti a un gruppo di lavoro, per assegnare loro solo specifiche operation o per destinare eventuali allarmi di sistema. Vedi "Gestione dei gruppi"

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 2 | Menu Accounting |
| 3 | Barra con i pulsanti della finestra. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Aggiunge un utente. | |  | Modifica l'utente selezionato. | |  | Elimina l'utente selezionato. | |  | Disconnette l'utente selezionato. | |
| 4 | Area di lavoro principale con elenco degli utenti registrati:  Utente registrato e connesso attualmente a RCS  Utente registrato ma non connesso attualmente a RCS  Utente registrato ma non abilitato al login. L'utente non può avere accesso a RCS |
| 5 | Dati dell'utente selezionato |
| 6 | Barra di stato di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |

Registrare e abilitare un utente all'accesso a RCS

Per registrare un nuovo utente:

| Passo | Azione |
| --- | --- |
| 1 | Fare clic su New user: compaiono i dati da compilare |
| 2 | Compilare i dati richiesti e assicurarsi che la casella Enabled sia selezionata se si desidera che l'utente possa già accedere a RCS |
| 3 | Fare clic su Save: nell'area di lavoro principale compare il nuovo utente con l'icona |

Abilitare/disabilitare un utente

Per abilitare o disabilitare un utente ad accedere a RCS:

| Passo | Azione |
| --- | --- |
| 1 | Fare doppio clic su un utente: compaiono i suoi dati |
| 2 | Fare clic su Enabled per abilitare o disabilitare |
| 3 | Fare clic su Save: nell'area di lavoro principale il nuovo utente compare con l'icona (abilitato) o (disabilitato).  IMPORTANTE: se l'utente è connesso continuerà a lavorare ma il successivo accesso gli sarà negato. Per disconnetterlo vedi "**Gestione degli utenti**". |

Disconnettere un utente immediatamente

Per disconnettere immediatamente un utente connesso:

| Passo | Azione |
| --- | --- |
| 1 | Fare clic su un utente e fare clic su Disconnect user: nell'area di lavoro principale l'utente compare con l'icona .  IMPORTANTE: se l'utente è connesso verrà immediatamente disconnesso. Ma il successivo accesso gli sarà permesso a meno che non lo si disabiliti. Per disabilitarlovedi "**Gestione degli utenti**".Fare riferimento a "**Abilitare/disabilitare un utente**" |

Modificare i dati di un utente

Per modificare i dati di un utente:

| Passo | Azione |
| --- | --- |
| 1 | Fare doppio clic su un utente: compaiono i suoi dati |
| 2 | Modificare i dati e fare clic su Save: i dati vengono considerati a partire da successive login o da successivi messaggi di avviso |

Da sapere

Cose da sapere su utenti e gruppi 21

Azioni correlate

Procedure dell'Amministratore 14

Dati di riferimento

Dati degli utenti 22

Gestione dei gruppi

|  |  |
| --- | --- |
| Per gestire  i gruppi: | * sezione Accounting, Gruppi |

Scopo

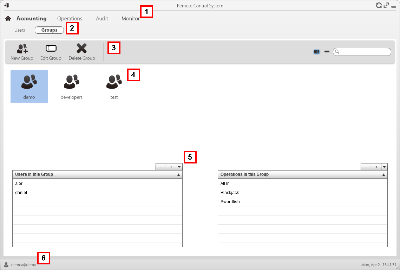
Questa funzione permette di:

* organizzare gli utenti in gruppi di lavoroper assegnare loro specifiche operation
* creare un gruppo di alerting, che riceverà le email di allarmi del sistema

Suggerimento: per rendere più semplice e immediato raggruppare e gestire gli utenti destinati a ricevere gli allarmi di RCS creare un gruppo "di alerting" senza associarlo a un'operation ma contenente tutti quegli utenti da avvertire in caso di allarme. Vedi "Gestione degli utenti"

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS.  Vedi "Descrizione della homepage" |
| 2 | Menu Accounting |
| 3 | Barra con i pulsanti della finestra. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Aggiunge un gruppo. | |  | Modifica il gruppo selezionato. | |  | Elimina il gruppo selezionato. | |
| 4 | Elenco dei gruppi. |
| 5 | Utenti e operation assegnati al gruppo selezionato. |
| 6 | Barra di stato di RCS.  Vedi "Descrizione della homepage" |

Creare un gruppo e associarvi utenti e operation

Per creare un nuovo gruppo:

| Passo | Azione |
| --- | --- |
| 1 | Fare clic su New group: viene richiesto il nome da assegnare al gruppo |
| 2 | Compilare i dati richiesti e fare clic su Save: nell'area di lavoro principale compare il nuovo gruppo |
| 3 | Nella tabella Users in this Group fare clic su per aggiungere gli utenti al gruppo |
| 4 | Nella tabella Operations in this Group fare clic su per aggiungere le operation al gruppo: alla successiva login gli utenti appartenenti al gruppo vedranno solo le operation in elenco.  Se si associa una operation a un utente attualmente connesso, quell'utente potrà vedere l'operation solo dalla successiva login. |

Modificare i dati di un gruppo e disassociare utenti e operation

Per modificare i dati di un gruppo:

| Passo | Azione |
| --- | --- |
| 1 | Fare doppio clic su un gruppo |
| 2 | Modificarne il nome e fare clic su Save |
| 3 | Nella tabellaUsers in this Group fare clic su per escludere utenti dal gruppo |
| 4 | Nella tabella Operations in this Group fare clic su per escludere le operation visibili al gruppo: alla successiva login gli utenti appartenenti al gruppo non vedranno più le operation escluse.  Se si esclude una operation da un utente attualmente connesso, quell'utente non vedrà l'operation solo dalla successiva login. |

Da sapere

Cose da sapere su utenti e gruppi 21

Cose da sapere su utenti e gruppi

Introduzione

Per garantire la massima riservatezza e sicurezza dei dati RCS offre all'Amministratore la possibilità di assegnare privilegi di accesso ad ogni suo utente e raccogliere gli utenti in gruppi di lavoro cui affidare specifiche operation. La struttura si adatta sia alle realtà dove i compiti sono molto frammentati sia alle realtà dove tutti i compiti ricadono su poche persone.

Con la gestione degli utenti l'Amministratore può inoltre disconnettere rapidamente un utente sospetto e disabilitarlo temporaneamente dall'accesso a RCS.

Privilegi di accesso

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

* Amministratore di sistema: responsabile esclusivo dell'installazione hardware e software e dei backup



* Amministratore: responsabile di tutti gli accessi al sistema, delle indagini e degli obiettivi dell'indagine



* Tecnico: responsabile della configurazione e dell'installazione degli agenti di intercettazione



* Analista: responsabile dell'analisi dei dati



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

Funzioni abilitate per il singolo ruolo

Di seguito l'elenco delle funzioni di RCS il cui accesso è previsto solo per gli utenti in possesso di quel ruolo:

| Ruolo | Funzioni abilitate |
| --- | --- |
| Amministratore di sistema | * System * Monitor |
| Amministratore | * Accounting * Operation * Audit * Monitor |
| Tecnico | * Operation * System * Monitor |
| Analista | * Operation * Dashboard * Alerting * Monitor |

Gruppi di utenti per ogni operation

I gruppi permettono di raggruppare più utenti per assegnare loro operation specifiche. In questo modo è possibile gestire più operation contemporaneamente garantendo la massima riservatezza dei dati tra i gruppi di lavoro.

Vedi "Gestione delle operation"

IMPORTANTE: le assegnazioni delle operation a un gruppo di lavoro saranno effettive alla successiva login dell'utente che appartiene al gruppo.

Gruppi di utenti per gli allarmi di sistema

È possibile creare un gruppo di utenti esclusivamente destinato a ricevere una email nel caso di allarmi di sistema.

In questo modo è possibile garantire interventi rapidi degli Amministratori di sistema in caso di malfunzionamenti gravi.

Vedi "Monitoraggio del sistema (Monitor)"

Azioni correlate

Procedure dell'Amministratore 14

Dati di riferimento

Dati degli utenti 22

Dati degli utenti

Di seguito la descrizione dei dati dell'utente selezionato:

| Dato | Descrizione |
| --- | --- |
| Enabled | Selezionare per abilitare l'utente alla connessione a RCS. Non selezionare per lasciare l'utente registrato ma non permettergli l'accesso a RCS |
| Name | Nome utilizzato per accedere a RCS |
| Description | Descrizione libera |
| Contact | Email dell'utente.  Se l'utente ha i privilegi di Analista questa è l'email dove l'utente riceverà gli avvisi delle evidence. L'email non può essere cambiata dall'utente. |
| Password | Password dell'utente. L'utente potrà successivamente modificarla dalla barra di stato. Vedi "Elementi e azioni comuni dell'interfaccia" |
| Roles | Privilegi assegnati all'utente:  Amministratore di sistema  Amministratore  Tecnico  Analista  Per la descrizione dettagliata dei privilegi vedi "Cose da sapere su utenti e gruppi" |
| Language | Lingua dell'interfaccia di RCS Console. L'utente potrà successivamente modificarla dalla barra di stato. Vedi "Descrizione della homepage"Fare riferimento a "Elementi e azioni comuni dell'interfaccia" |
| Console Timezone | Fuso orario per la rappresentazione degli orari in RCS Console. Vedi "Descrizione della homepage"Fare riferimento a "Elementi e azioni comuni dell'interfaccia"Vedi "Descrizione della homepage" |
| Groups | Gruppi cui appartiene l'utente. L'utente potrà vedere solo le operation assegnate al gruppo. Vedi "Gestione dei gruppi" |

Da sapere

Cose da sapere su utenti e gruppi 21

Azioni correlate

Procedure dell'Amministratore 14

Gestione delle operation

|  |  |
| --- | --- |
| Per gestire  le operation: | * sezione Operations |

Scopo

Questa funzione permette di:

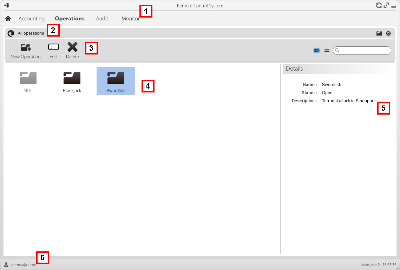
* creare una nuova operation
* assegnare l'operation a un gruppo di utenti
* visualizzare e gestire i target associati a una operation

Passi successivi

Uno o più target devono essere associati all'operation. Vedi "Operation: gestire i target".

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia" |
| 2 | Barra di navigazione. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 3 | Barra con i pulsanti della finestra. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Aggiunge un'operation | |  | Modifica l'operation selezionata. | |  | Elimina l'operation selezionata. | |
| 4 | Elenco delle operation create:  Operation aperta. Se sono stati definiti dei target e sono stati installati correttamente degli agent, si ricevono i dati di interesse.  Operation chiusa. Tutti i target sono chiusi e gli agent disinstallati. È comunque possibile vedere tutti i suoi target e tutte le sue evidence. |
| 5 | Dati dell'operation selezionata |
| 6 | Barra di stato di RCS.  Vedi "Descrizione della homepage" |

Creare un'operation

Per creare una nuova operation:

| Passo | Azione |
| --- | --- |
| 1 | Fare clic su New Operation: compaiono i dati da compilare |
| 2 | Selezionare il gruppo (o i gruppi) da assegnare all’operation.  NOTA: E’ necessario che almeno uno dei gruppi associati contenga l’utente che sta creando l’operation |
| 3 | Compilare i dati richiesti e fare clic su Save: nell'area di lavoro principale compare la nuova operation in stato Aperta. |

Modificare i dati di un'operation

Per modificare i dati di un'operation:

| Passo | Azione |
| --- | --- |
| 1 | Selezionare un'operation, quindi fare clic su Edit: compaiono i suoi dati |
| 2 | Modificare i dati e fare clic su Save |

Chiudere un'operation

Per chiudere un'operation e attivare la disinstallazione degli agent su tutti i target:

| Passo | Azione |
| --- | --- |
| 1 | Selezionare un'operation, quindi fare clic su Edit: compaiono i suoi dati |
| 2 | In Status selezionare CLOSED |
| 3 | Fare clic su Save: vengono chiusi tutti i target e viene richiesta la disinstallazione degli agent. I dati restano disponibili sul database.  PRUDENZA: la chiusura dell'operation è irreversibile, Vedi "**Cose da sapere sulle operation**" |



Visualizzare i target di un'operation

Per visualizzare i target di un'operation:

| Passo | Azione |
| --- | --- |
| 1 | Fare doppio clic su un'operation: si apre la pagina per la gestione dei target.  Vedi "Operation: gestire i target" |

Eliminare un'operation

Per eliminare un'operation:

| Passo | Azione |
| --- | --- |
| 1 | Selezionare un'operation, quindi fare clic su Delete. |
| 2 | Confermare l'azione facendo clic su OK: vengono eliminati dai database i dati dell'operation, dei target, degli agent e tutte le evidence. |

PRUDENZA: eliminare un'operation è un'azione irreversibile e causa la perdita dei dati associati a quella operation.

Cose da sapere sulle operation

Cos'è un'operation

L'operation rappresenta l'indagine da eseguire. Un'operation contiene uno o più target, ovvero le persone fisiche da intercettare. A un target il Tecnico assegnerà uno o più agent, di tipo desktop o mobile, ovvero agent che possono essere installati su un computer o su un telefono cellulare.

Assegnare l'operation a un gruppo di utenti

Per garantire il massimo della riservatezza dei dati si suggerisce di associare un'operation solo agli utenti di RCS incaricati dell'indagine. Utenti non associati all'operation non vedranno alcun dato dell'operation e delle evidence raccolte; **per questo motivo è necessario che chi crea un operation faccia parte di almeno uno dei gruppi associati ad essa al momento della creazione**

Cosa avviene quando si crea una nuova operation

Quando un'operation viene creata è già dichiarata aperta, quindi è possibile creare i target dell'operation e chiedere al Tecnico la generazione e l'installazione degli agent. Ad operation aperta gli agent iniziano a raccogliere i dati e a inviarli a RCS.

Cosa avviene quando si chiude un'operation

La chiusura di un operation deve avvenire alla chiusura effettiva dell'indagine, quando si è sicuri che tutti gli agent hanno già scaricato tutte le informazioni necessarie ai fini dell'indagine.

La chiusura provoca automaticamente la chiusura dei target e la chiusura degli agent. La chiusura di ogni agent provoca la sua disinstallazione alla prima sincronizzazione, lasciando così pulito il dispositivo dove era stato installato.

Un'operation chiusa non può più essere riaperta. Solo i dati dell'operation stessa e quelli già inviati dagli agent restano nel database.

PRUDENZA: in caso di sincronizzazioni non frequenti, per esempio ogni quattro giorni, attendere l'ultima sincronizzazione utile prima di chiudere l'operation.

Dati delle operation

Di seguito la descrizione dei dati dell'operation selezionata:

| Dato | Descrizione |
| --- | --- |
| Name | Nome dell'operation |
| Description | Descrizione libera |
| Contact | Campo descrittivo per definire, ad esempio, il nome di un referente (Giudice, Magistrato, etc.) |
| Status | Stato di un'operation e comando di chiusura:  OPEN: l'operation è aperta. Se sono stati definiti dei target e sono stati installati correttamente degli agent, RCS riceve i dati di interesse.  CLOSED: l'operation è chiusa, senza più possibilità di riaprirla. Gli agent non inviano più i dati, ma è possibile consultare le evidence.  PRUDENZA: chiudere un'operation è un'azione irreversibile.Vedi "**Cose da sapere sulle operation**" |
| Groups | Gruppi abilitati a visualizzare l'operation.  Vedi "Gestione dei gruppi" |

Operation: gestire i target

|  |  |
| --- | --- |
| Per entrare in una operation: | * sezione Operation, entrare in una operation |

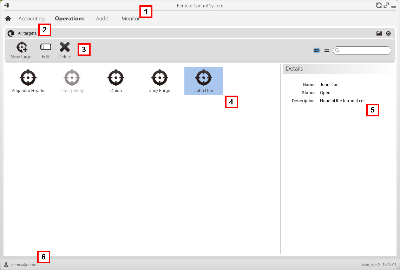
Scopo

Questa funzione permette di:

* creare uno o più target da intercettare durante un'operation
* gestire l'attivazione/disattivazione di un target.

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 2 | Barra di navigazione. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 3 | Barra con i pulsanti della finestra. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Aggiunge un target. | |  | Modifica il target selezionato. | |  | Elimina il target selezionato. | |
| 4 | Elenco dei target:  target Aperto  target Chiuso |
| 5 | Dati del target selezionato |
| 6 | Barra di stato di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |

Creare un target

Per creare un nuovo target:

| Passo | Azione |
| --- | --- |
| 1 | Fare clic su New Target: compaiono i dati da compilare |
| 2 | Compilare i dati richiesti e fare clic su Save: nell'area di lavoro principale compare il nuovo target in stato Aperto, ovvero pronto per essere utilizzato da un Tecnico |

Chiudere un target

Per chiudere un target e attivare la disinstallazione dei suoi agent:

| Passo | Azione |
| --- | --- |
| 1 | Selezionare un target, quindi fare clic su Edit: compaiono i suoi dati |
| 2 | In Status selezionare CLOSED |
| 3 | Fare clic su Save: viene chiuso il target e viene automaticamente avviata la disinstallazione dei suoi agent. I dati restano disponibili sul database.  PRUDENZA: la chiusura del target è irreversibile, Vedi "**Cose da sapere sui target**" |

Modificare i dati di un target

Per modificare i dati di un target:

| Passo | Azione |
| --- | --- |
| 1 | Selezionare un target, quindi fare clic su Edit: compaiono i suoi dati |
| 2 | Modificare i dati e fare clic su Save |

Eliminare un target

Per eliminare un target:

| Passo | Azione |
| --- | --- |
| 1 | Selezionare un target, quindi fare clic su Delete. |
| 2 | Confermare l'azione facendo clic su OK: vengono eliminati dai database i dati del target, dei suoi agent e tutte le evidence. |

PRUDENZA: eliminare un target è un'azione irreversibile e causa la perdita dei dati associati a quel target.

Cose da sapere sui target

Cos'è un target

Il target rappresenta la persona fisica da intercettare. A un target il Tecnico assegna uno o più agent, di tipo desktop o mobile, ovvero agent che possono essere installati su un computer o su un telefono cellulare.

Il ruolo dell'Amministratore nella gestione dei target è a un livello di organizzazione generale; è compito del Tecnico configurare e lavorare operativamente sui target secondo le disposizioni dell'Amministratore.

L'Amministratore ha il compito di:

* creare un nuovo target all'interno di un'operation
* dare disposizioni al Tecnico sulle tempistiche di attivazione e la tipologia delle prove da raccogliere attraverso gli agent di un determinato target, in base alle caratteristiche del mandato ricevuto dall'autorità giudiziaria
* target

Cosa avviene quando si crea un target

Quando un target viene creato è già dichiarato aperto, quindi è possibile chiedere al Tecnico la generazione e l'installazione degli agent.

Cosa avviene quando si chiude un target

È possibile chiudere un target di un'operation, per esempio alla chiusura effettiva dell'indagine per quel target, quando si è sicuri che tutti gli agent hanno già scaricato tutte le informazioni necessarie ai fini dell'indagine.

La chiusura provoca automaticamente la chiusura degli agent. La chiusura di ogni agent provoca la sua disinstallazione alla prima sincronizzazione, lasciando così pulito il dispositivo dove era stato installato.

Un target chiuso non può più essere riaperto. Solo i dati del target stesso e quelli già inviati dagli agent restano nel database.

PRUDENZA: quando si chiude un target, si disinstallano automaticamente tutti gli agent associati.

target.

Chiudere un target solo quando si è sicuri che gli agent hanno già scaricato tutte le informazioni di cui si ha bisogno.

Apertura e chiusura di una indagine

Nel caso di chiusura di una indagine, tutti i target associati sono irrevocabilmente chiusi, e tutti gli agent disinstallati. Vedi "Cose da sapere sulle operation".

Dati dei target

Di seguito la descrizione dei dati del target selezionato:

| Dato | Descrizione |
| --- | --- |
| Name | Nome del target |
| Description | Descrizione libera |
| Status | Definisce lo stato di un target:  il target è aperto. Se il Tecnico ha installato correttamente degli agent, RCS riceve i dati di interesse  il target è chiuso, senza più possibilità di riaprirlo. Vengono automaticamente disinstallati tutti gli agent. Un target chiuso resta presente nel database ed è quindi possibile vedere tutti i suoi agent e tutte le sue evidence.  PRUDENZA: chiudere un target è un'azione irreversibile. Vedi "**Operation: gestire i target**" |

Monitoraggio utenti (Audit)

|  |  |
| --- | --- |
| Per monitorare gli utenti: | * sezione Audit |

Scopo

Questa funzione permette di controllare le azioni in RCS di Amministratori, Tecnici e Analisti. Per esempio è possibile verificare il corretto svolgimento di un'operation, il rispetto delle tempistiche di attivazione/disattivazione di un target, l'applicazione corretta da parte del Tecnico delle tipologie di agent autorizzate per una specifica operation.

Cosa è possibile fare

È possibile selezionare solo le azioni svolte in un certo periodo e applicare dei filtri per ricercare, per esempio, informazioni dettagliate su specifiche operation o di specifici utenti. In caso di necessità, è possibile esportare le azioni in un file in formato CSV.

IMPORTANTE: se la pagina viene tenuta aperta, è necessario aggiornarla per ottenere le azioni più recenti.Vedi "**Descrizione della homepage**"

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione | |
| --- | --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". | |
| 2 | Barra con i pulsanti della finestra. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Esporta le azioni visualizzate in un file in formato CSV (importabile in Excel) | |  | Rimuove tutti i filtri applicati ai dati della tabella | | |
| 3 | Elenco azioni svolte dagli utenti di RCS. Per la descrizione Vedi "Dati del monitoraggio utenti (Audit)" | |
| 4 | Barra di stato di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". | |

Selezionare le azioni di un periodo di tempo

Per visualizzare solo le azioni di un periodo dei tempo:

| Passo | Azione |
| --- | --- |
| 1 | Selezionare la colonna Date |
| 2 | * Selezionare l’intervallo di tempo di interesse |
|  |  |

NOTA: il filtro sulla data è sempre attivo, impostato sulle azioni delle ultime 24 ore. È possibile solo modificarne i criteri.

Selezionare le azioni in base ai dati proposti

Per aumentare l'accuratezza del risultato :

| Passo | Azione |
| --- | --- |
| 1 | Fare clic sull'intestazione di una o più colonne: compare un campo di ricerca da compilare |
| 2 | Inserire la parola da ricercare e premere il tasto INVIO. Le informazioni all'interno della colonna sono filtrate e ordinate in base alla parola chiave inserita |

Rimuovere uno o più filtri

Per rimuovere un filtro e visualizzare tutti i dati:

| Se volete rimuovere... | Allora... |
| --- | --- |
| un singolo filtro | deselezionare la casella di controllo nell'intestazione della colonna desiderata |
| tutti i filtri contemporaneamente | fare clic su Reset filters |

NOTA: il filtro sulla data è sempre attivo, impostato sulle azioni delle ultime 24 ore. È possibile solo modificarne i criteri.

Esportare le azioni visualizzate

Per esportare le azioni visualizzate:

| Passo | Azione |
| --- | --- |
| 1 | Fare clic su Export: compaiono i dati da compilare |
| 2 | Inserire il nome del file da esportare e fare clic su OK: un indicatore di stato mostra l'avanzamento dell'operazione. Per controllarne l'avanzamento fare clic sulla barra. |

Cose da sapere sul monitoraggio utenti (Audit)

Cos'è il monitoraggio utenti

L'Audit è l'elenco delle azioni intraprese in RCS da tutti gli utenti tipo Amministratori, Tecnici e Analisti. Serve a garantire la correttezza di una indagine, il rispetto delle regole e delle indicazioni dettate da un qualsiasi ente che richiede un'attività investigativa nei confronti di un sospettato.

In questo modo l'Amministratore può controllare l'accesso al sistema da parte di tutti gli utenti abilitati ed eventualmente risalire nel tempo ad azioni particolari, quali per esempio la creazione di un target.

Come si leggono le azioni segnalate

L'Audit riassume in una tabella ogni azione effettuata nel sistema da ogni singolo utente in un certo istante.

In ogni azione sono sempre presenti quattro informazioni:

* data-ora dell'evento,
* utente connesso,
* tipo di evento,
* descrizione.

Le altre caselle sono popolate solo in relazione al tipo di azione. Ad esempio, se un utente accede al sistema, l'Audit registra il nome dell'utente in Actor e il tipo di azione "login" in Action.

Se un Tecnico crea degli agent, nell'elenco compare un'azione per ogni agent con il nome dell'utente, il tipo di azione "target.create" , il nome dell'operation, il nome del target e il nome dell'agent.

NOTA: i testi delle azioni sono disponibili solo in lingua inglese.

La selezione delle azioni interessanti tramite i filtri

La funzione mostra normalmente le azioni registrate da RCS nelle ultime 24 ore. Il filtro sulla colonna Date è quindi l'unico filtro che è sempre impostato di default ma che può essere modificato a piacimento cambiando i valori dell'intervallo. Per questo motivo la casella di controllo corrispondente è sempre selezionata.

Per tutte le altre colonne è possibile impostare un filtro per restringere la ricerca. Se la casella di controllo di fianco all'intestazione è selezionata, indica che c'è un filtro attivo su quella colonna.

Ogni intestazione permette quindi di selezionare quali dati visualizzare.

Solo la colonna Description accetta l'inserimento di parte del testo da cercare, per esempio se si inserisce "log" saranno visualizzate tutte le azioni la cui descrizione contiene il testo "log", per esempio:

* "User 'xxx' logged in"
* "Log file created"

Dati esportabili

RCS permette di esportare le azioni registrate per Amministratori, Tecnici e Analisti in file visibili nella cartella RCS Download sul desktop.

Dati del monitoraggio utenti (Audit)

Di seguito la descrizione delle colonne della tabella Audit:

| Colonna | Descrizione |
| --- | --- |
| Date | Data-ora dell'azione |
| Actor | Nome dell'utente connesso che ha causato l'azione |
| Action | Tipo di azione intrapresa dall'utente connesso. L'azione viene rappresentata con "<soggetto>.<azione>", per esempio "user.update" significa che è stato aggiornato un utente. Questo facilita la selezioni di azioni dello stesso tipo. |
| User | Utente interessato dall'azione, per esempio creato da un Amministratore. Da non confondere con il nome in Actor che è l'utente che ha causato l'azione. |
| Group | Gruppo interessato dall'azione, per esempio il gruppo associato a un'operation |
| Operation | Operation interessata dall'azione, per esempio l'operation chiusa da un Amministratore |
| Target | Target interessato dall'azione, per esempio il target chiuso da un Amministratore |
| Agent | Agent interessato dall'azione, per esempio l'agent creato da un Tecnico |
| Description | Breve descrizione esplicativa dell'azione |

NOTA: tutte le azioni sono visualizzate solo in lingua inglese.

Monitoraggio del sistema (Monitor)

|  |  |
| --- | --- |
| Per fare il monitoraggio del sistema: | * sezione Monitor |

Scopo

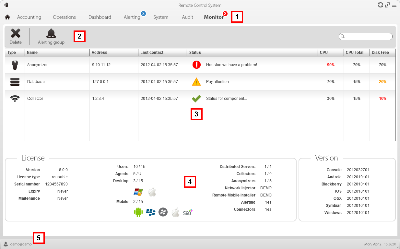
Questa funzione permette di:

* monitorare lo stato del sistema sia in termini di componenti hardware e software
* monitorare le licenze utilizzate rispetto a quelle acquistate
* definire il gruppo di alerting, destinatario delle email di segnalazione nel caso di allarmi di sistema

Contattare l'assistenza tecnica se sono necessarie licenze aggiuntive.

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | | Descrizione | |
| --- | --- | --- | --- |
| 1 | | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia".  : indica la quantità di allarmi di sistema in corso. | |
| 2 | | Barra con i pulsanti della finestra. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Elimina il componente da monitorare. | |  | Definisce il gruppo di alerting. | | |
| 3 | | Elenco componenti di RCS con relativo stato:  Allarme (genera l'invio di una email al gruppo di alerting)  Avvertenza  Componente funzionante | |
| 4 | | Stato delle licenze | |
| 5 | | Barra di stato di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". | |

Definire il gruppo di alerting o disattivarlo/attivarlo temporaneamente

Per selezionare il gruppo di alerting:

| Passo | Azione |
| --- | --- |
| 1 | Fare clic su Alerting Group. |
| 2 | Selezionare No Alert per disattivare le notifiche via email al gruppo di alerting  oppure  Selezionare un gruppo di alerting dal menu a tendina. Il gruppo selezionato riceverà ad ogni allarme di sistema una notifica via email con la descrizione dell'allarme. |

Suggerimento: per rendere più semplice e immediato raggruppare e gestire gli utenti destinati a ricevere gli allarmi di RCS creare un gruppo "di alerting" senza associarlo a un'operation ma contenente tutti quegli utenti da avvertire in caso di allarme. Vedi "Gestione degli utenti"

Dati del monitoraggio del sistema (Monitor)

Dati di monitoraggio dei componenti del sistema

Di seguito la descrizione dei dati del monitoraggio di sistema:

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

Dati di monitoraggio delle licenze

Di seguito la descrizione dei dati del monitoraggio delle licenze:

| Dato | Descrizione |
| --- | --- |
| License type | Indica il tipo di licenziamento attualmente in uso per gli Agent  reusable: è possibile riutilizzare la licenza di un agent dopo la sua disinstallazione  oneshot: la licenza di un agent ha validità solo per una installazione |
| Users | Indica quanti utenti sono attualmente in uso nel sistema e qual’e’ il numero massimo. |
| Agents/Desktop/Mobile | **Agents:** Indica quanti Agent sono attualmente in uso e qual’e’ il numero massimo. **Desktop e Mobile** indicano lo stesso dato suddiviso per Agent di tipo Desktop e Mobile.  **Se il numero di licenze viene esaurito, eventuali nuovi agent finiranno in coda finchè una licenza non viene liberata o non se ne acquistano di nuove.**  Le icone sottostanti indicano su quali piattaforme gli Agent possono essere isntallati (es: Windows, Android, etc.) |
|  |  |
| Distributed Servers | Indica il numero di database utilizzati e utilizzabili |
| Collectors | Indica il numero di Collectors utilizzati e utilizzabili |
| Anonymizers | Indica il numero di Anonymizers utilizzati e utilizzabili |
|  |  |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RCS8.0Manuale dell'amministratore di sistema  Manuale dell'amministratore di sistema 1.0 FEB/2012  © COPYRIGHT 2012  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 | |