Manuale dell'amministratore

Dr.Web Enterprise Security Suite
Versione 10.01.0
Manuale dell'amministratore
11/09/2017

Doctor Web, Sede centrale in Russia

125040

Russia, Mosca

3° via Yamskogo polya, 2, 12A

Sito web: http://www.drweb.com/

Telefono +7 (495) 789-45-87

Le informazioni sulle rappresentanze regionali e sedi sono ritrovabili sul sito ufficiale della società.

Doctor Web

Doctor Web – uno sviluppatore russo di strumenti di sicurezza delle informazioni.

Doctor Web offre efficaci soluzioni antivirus e antispam sia ad enti statali e grandi aziende che ad utenti privati.

Le soluzioni antivirus Dr.Web esistono a partire dal 1992 e dimostrano immancabilmente eccellenza nel rilevamento di programmi malevoli, soddisfano gli standard di sicurezza internazionali.

I certificati e premi, nonché la vasta geografia degli utenti testimoniano la fiducia eccezionale nei prodotti dell'azienda.

Siamo grati a tutti i nostri clienti per il loro sostegno delle soluzioni Dr.Web!

Sommario

Capitolo 1: Dr.Web Enterprise Security Suite

1.1. Introduzione

1.1.1. Scopo del documento

La documentazione dell'amministratore della rete antivirus Dr.Web Enterprise Security Suite contiene le informazioni che descrivono sia i principi generali che dettagli della realizzazione di una protezione antivirus completa dei computer aziendali tramite Dr.Web Enterprise Security Suite.

La documentazione dell'amministratore della rete antivirus Dr.Web Enterprise Security Suite si compone delle seguenti parti principali:

1. **Guida all'installazione** (file **drweb-esuite-10-install-manual-it.pdf**)
2. **Manuale dell'amministratore** (file **drweb-esuite-10-admin-manual-it.pdf**)

   Il manuale dell'amministratore è indirizzato *all'amministratore della rete antivirus* – dipendente della società che è incaricato della gestione della protezione antivirus dei computer (postazioni e server) di questa rete.

   L'amministratore della rete antivirus deve avere privilegi di amministratore di sistema o collaborare con l'amministratore della rete locale, deve essere conoscente in materia di strategia della protezione antivirus e conoscere in dettaglio i pacchetti antivirus Dr.Web per tutti i sistemi operativi utilizzati nella rete.
3. **Allegati** (file **drweb-esuite-10-appendices-it.pdf**)

Nella documentazione sono presenti i riferimenti incrociati tra i documenti elencati. Se i documenti sono stati scaricati su un computer locale, i riferimenti incrociati saranno operanti solo se i documenti sono situati nella stessa directory e hanno i nomi originali.

Nella documentazione dell'amministratore non vengono descritti i pacchetti antivirus Dr.Web per computer protetti. Le informazioni pertinenti sono consultabili nel **Manuale dell'utente** della soluzione antivirus Dr.Web per il sistema operativo corrispondente.

Prima di leggere i documenti, assicurarsi che questa sia la versione più recente dei Manuali. I manuali vengono aggiornati in continuazione, l'ultima versione può sempre essere reperita sul sito ufficiale della società Doctor Web https://download.drweb.com/doc/.

1.1.2. Segni convenzionali e abbreviazioni

Segni convenzionali

In questo manuale vengono utilizzati i segni convenzionali riportati nella tabella 1-1.

Tabella 1-1. Segni convenzionali

Segno	Commento
	Nota importante o istruzione.
	Avviso di possibili situazioni di errore, nonché di punti importanti cui prestare particolare attenzione.
Rete antivirus	Un nuovo termine o un termine accentato nelle descrizioni.
<*indirizzo_IP*>	Campi in cui nomi di funzione vanno sostituiti con valori effettivi.
Salva	Nomi dei pulsanti di schermo, delle finestre, delle voci di menu e di altri elementi dell'interfaccia del programma.
CTRL	Nomi dei tasti della tastiera.
`C:\Windows\`	Nomi di file e directory, frammenti di codice.
Allegato A	Riferimenti incrociati ai capitoli del documento o collegamenti ipertestuali a risorse esterne.

Abbreviazioni

Nel testo del Manuale vengono utilizzate le seguenti abbreviazioni senza spiegazione:

- ACL – lista di controllo degli accessi (Access Control List),
- CDN – rete di distribuzione di contenuti (Content Delivery Network),
- CPU – processore centrale (Central Processing Unit),
- DFS – file system distribuito (Distributed File System),
- DNS – sistema dei nomi a dominio (Domain Name System),
- GUI – interfaccia utente grafica (Graphical User Interface), versione del programma con la GUI – una versione che utilizza gli strumenti della GUI,
- NAP – Network Access Protection,
- MTU – dimensione massima di un pacchetto dati (Maximum Transmission Unit),
- TTL – tempo di vita pacchetto (Time To Live),

- UDS – socket di dominio UNIX (UNIX Domain Socket),
- DB, DBMS – database, database management system,
- SAM Dr.Web – Sistema di aggiornamento mondiale di Dr.Web,
- LAN – rete locale,
- SO – sistema operativo,
- Software – programmi per computer.

1.2. Sul prodotto

Dr.Web Enterprise Security Suite è progettato per installare e gestire una protezione antivirus completa e affidabile della rete interna aziendale, compresi i dispositivi mobili, e dei computer di casa dei dipendenti.

L'insieme dei computer e dei dispositivi mobili su cui sono installati i componenti interagenti di Dr.Web Enterprise Security Suite costituisce una *rete antivirus* unica.

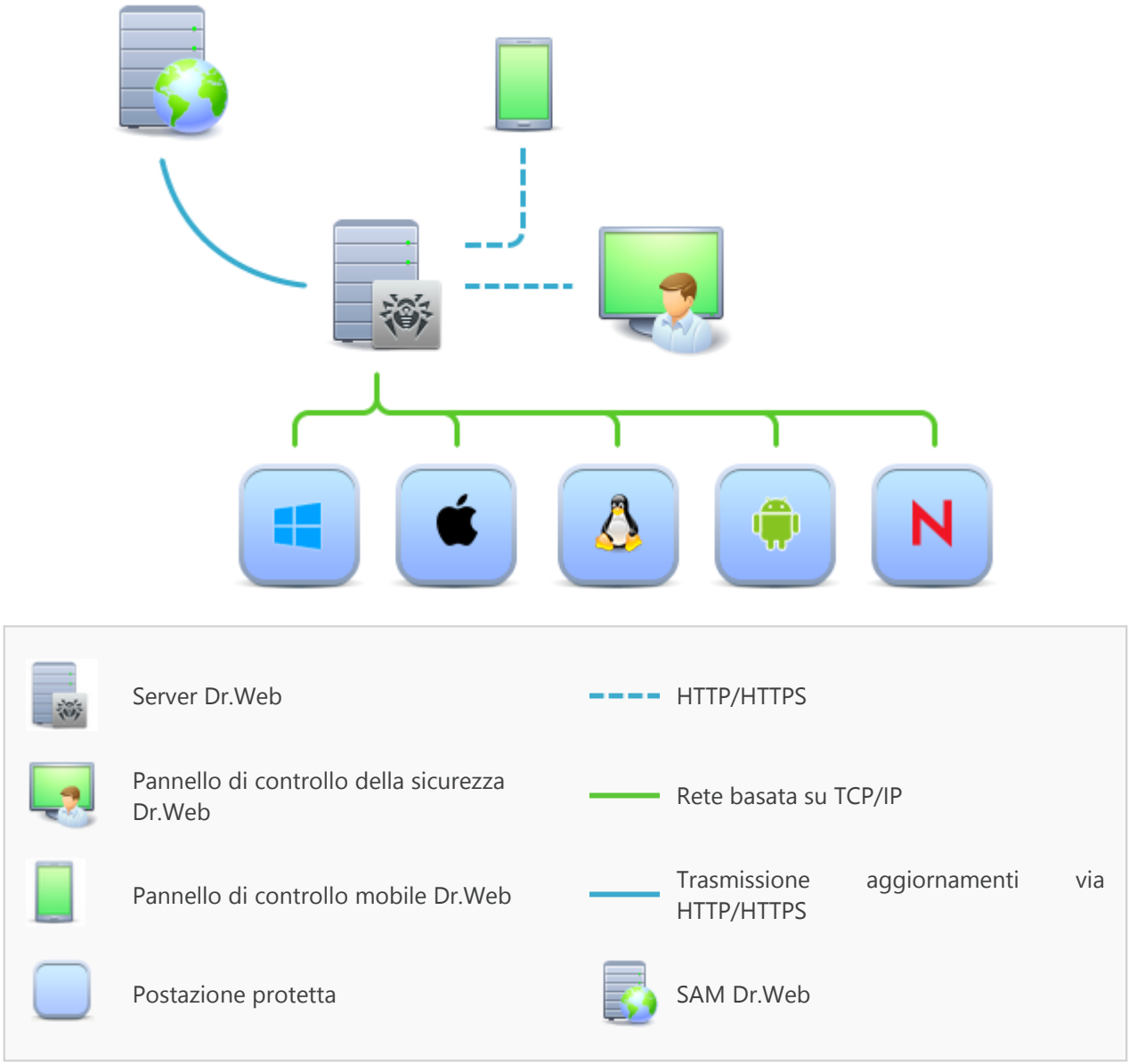


Immagine 1-1. Struttura logica della rete antivirus

La rete antivirus Dr.Web Enterprise Security Suite ha l'architettura *client-server*. I suoi componenti vengono installati sui computer e dispositivi mobili degli utenti e degli amministratori, nonché sui computer che svolgono le funzioni server della rete locale. I componenti della rete antivirus scambiano le informazioni attraverso i protocolli di rete TCP/IP. Si può installare (e successivamente gestire) il software antivirus sulle postazioni protette sia via LAN che via Internet.

Server di protezione centralizzata

Il server di protezione centralizzata viene installato su uno dei computer della rete antivirus, e l'installazione è possibile su qualsiasi computer e non soltanto sul computer che svolge le funzioni server LAN. I requisiti principali di tale computer sono riportati in Requisiti di sistema.

Il carattere multipiattaforma del software server permette di utilizzare come Server un computer gestito dai seguenti sistemi operativi:

- SO Windows®,
- SO della famiglia UNIX® (Linux®, FreeBSD®, Solaris™).

Il server di protezione centralizzata conserva pacchetti antivirus per i diversi SO dei computer protetti, aggiornamenti dei database dei virus e dei pacchetti antivirus, le chiavi di licenza e le impostazioni dei pacchetti dei computer protetti. Il Server riceve gli aggiornamenti dei componenti di protezione antivirus e dei database dei virus tramite Internet dai server del Sistema di aggiornamento mondiale e distribuisce gli aggiornamenti alle postazioni protette.

È possibile creare una struttura gerarchica di diversi Server utilizzati dalle postazioni protette della rete antivirus.

Il Server supporta la funzione backup dei dati critici (database, file di configurazione ecc.).

Il Server registra gli eventi della rete antivirus in un unico log.

Database unico

Il database unico viene collegato al Server di protezione centralizzata e conserva i dati statistici di eventi della rete antivirus, le impostazioni del Server stesso, le impostazioni delle postazioni protette e dei componenti antivirus da installare sulle postazioni protette.

È possibile utilizzare i seguenti tipi di database:

Database incorporato. Vengono fornite due varianti del database incorporato direttamente nel Server di protezione centralizzata:

- SQLite2 (InitDB),
- SQLite3.

Database esterno. Vengono forniti i driver incorporati per la connessione dei seguenti database:

- Oracle,
- PostgreSQL,
- Driver ODBC per la connessione di altri database quali Microsoft SQL Server/Microsoft SQL Server Express.

È possibile utilizzare qualsiasi database che corrisponda alle esigenze dell'azienda. La scelta deve essere basata sulle esigenze che devono essere soddisfatti dal data warehouse, come per esempio: la possibilità di essere utilizzato in una rete antivirus di dimensioni adeguate, le caratteristiche di manutenzione del software del database, le possibilità di amministrazione fornite dal database stesso, nonché i requisiti e gli standard adottati per l'uso nell'azienda.

Pannello di controllo di protezione centralizzata

Il Pannello di controllo di protezione centralizzata viene installato automaticamente insieme al Server e fornisce un'interfaccia web utilizzata per gestire su remoto il Server e la rete antivirus modificando le impostazioni del Server, nonché le impostazioni dei computer protetti, conservate sul Server e sui computer protetti.

Il Pannello di controllo può essere aperto su qualsiasi computer che ha l'accesso di rete al Server. È possibile utilizzare il Pannello di controllo sotto quasi ogni sistema operativo, con l'utilizzo delle complete funzioni sotto i seguenti browser:

- Windows® Internet Explorer®,
- Mozilla® Firefox®,
- Google Chrome®.

L'elenco delle possibili varianti di utilizzo è riportato nel p. Requisiti di sistema.

Il Pannello di controllo di protezione centralizzata fornisce le seguenti possibilità:

- Facilità di installazione di Antivirus su postazioni protette, in particolare è possibile: installare su remoto sulle postazioni SO Windows con un esame preliminare della rete per cercare computer; creare pacchetti con identificatori univoci e con i parametri di connessione al Server per semplificare il processo di installazione di Antivirus da parte dell'amministratore o per consentire agli utenti di installare Antivirus su postazioni in modo autonomo.
- Gestione semplificata delle postazioni della rete antivirus tramite il metodo di gruppi (per maggiori informazioni consultare la sezione Capitolo 6: Gestione integrata delle postazioni).
- Possibilità di gestire pacchetti antivirus delle postazioni in modo centralizzato, in particolare è possibile: rimuovere sia singoli componenti che l'intero Antivirus su postazioni SO Windows; configurare le impostazioni dei componenti dei pacchetti antivirus; assegnare i permessi di configurare e gestire i pacchetti antivirus dei computer protetti agli utenti di questi computer (per maggiori informazioni consultare la sezione Capitolo 7: Gestione delle postazioni).
- Gestione centralizzata della scansione antivirus delle postazioni, in particolare è possibile: avviare la scansione antivirus su remoto sia secondo un calendario prestabilito che su una diretta richiesta dell'amministratore dal Pannello di controllo; configurare in modo centralizzato le impostazioni di scansione antivirus che vengono trasmesse su postazioni per eseguire in seguito una scansione locale con queste impostazioni (per maggiori informazioni consultare la sezione Scansione antivirus delle postazioni).
- Ottenimento delle informazioni statistiche sullo stato delle postazioni protette, delle statistiche di virus, delle informazioni sullo stato del software antivirus installato, sullo stato dei componenti antivirus in esecuzione, nonché dell'elenco degli hardware e dei software della postazione protetta (per maggiori informazioni consultare la sezione Visualizzazione delle statistiche della postazione).
- Flessibile sistema di amministrazione del Server e della rete antivirus grazie alla possibilità di delimitare i permessi di diversi amministratori, nonché la possibilità di connettere

amministratori attraverso sistemi di autenticazione esterni, per esempio Active Directory, LDAP, RADIUS, PAM (per maggiori informazioni consultare la sezione Capitolo 5: Amministratori della rete antivirus).

- Gestione delle licenze di protezione antivirus di postazioni con un complesso sistema di assegnazione delle licenze a postazioni e gruppi di postazioni, nonché trasferimento delle licenze tra diversi Server in caso di una configurazione della rete antivirus con diversi server (per maggiori informazioni consultare la sezione Gestione licenze).
- Una vasta gamma di impostazioni per configurare il Server e i suoi componenti separati, in particolare, è possibile: impostare un calendario di manutenzione del Server; connettere procedure personalizzate; configurare in modo flessibile l'aggiornamento di tutti i componenti della rete antivirus da SAM e la successiva distribuzione degli aggiornamenti sulle postazioni; configurare i sistemi che avvisano l'amministratore degli eventi accaduti nella rete antivirus tramite diversi metodi di consegna di messaggi; configurare le relazioni tra i server in caso di una rete antivirus con diversi server (per maggiori informazioni consultare la sezione Capitolo 8: Configurazione del Server Dr.Web).

Le informazioni dettagliate sulle possibilità dell'installazione della protezione antivirus su postazioni sono riportate nella **Guida all'installazione**.

Fa parte del Pannello di controllo della sicurezza Dr.Web il Web server che viene installato automaticamente insieme al Server. L'obiettivo principale del Web server è assicurare il lavoro con le pagine del Pannello di controllo e con le connessioni di rete client.

Pannello di controllo mobile di protezione centralizzata

Come un componente separato, viene fornito il Pannello di controllo mobile che è progettato per l'installazione e l'esecuzione su dispositivi mobili iOS e SO Android. I requisiti di base per l'applicazione sono riportati in p. Requisiti di sistema.

Il Pannello di controllo mobile viene connesso al Server sulla base delle credenziali dell'amministratore di rete antivirus, anche attraverso il protocollo criptato. Il Pannello di controllo mobile supporta le funzionalità di base del Pannello di controllo:

1. Gestione del repository di Server Dr.Web:
   - visualizzazione dello stato dei prodotti nel repository;
   - avvio dell'aggiornamento di repository da Sistema di aggiornamento mondiale Dr.Web.
2. Gestione delle postazioni su cui un aggiornamento del software antivirus non è riuscito:
   - visualizzazione delle postazioni fallite;
   - aggiornamento dei componenti sulle postazioni fallite.
3. Visualizzazione delle statistiche sullo stato della rete antivirus:
   - numero di postazioni registrate sul Server Dr.Web e il loro stato corrente (online/offline);
   - statistiche di infezioni su postazioni protette.
4. Gestione delle nuove postazioni in attesa di essere collegate al Server Dr.Web:
   - conferma dell'accesso;

- rigetto delle postazioni.

5. Gestione dei componenti antivirus installati su postazioni della rete antivirus:
   - avvio di una scansione rapida o completa sulle postazioni selezionate o su tutte le postazioni dei gruppi selezionati;
   - configurazione della reazione di Scanner Dr.Web al rilevamento di oggetti malevoli;
   - visualizzazione e gestione dei file da Quarantena sulla postazione selezionata o su tutte le postazioni di un gruppo.
6. Gestione delle postazioni e dei gruppi:
   - visualizzazione delle impostazioni;
   - visualizzazione e gestione della lista dei componenti del pacchetto antivirus;
   - rimozione;
   - invio dei messaggi con qualsiasi contenuto sulle postazioni;
   - riavvio delle postazioni SO Windows;
   - aggiunzione alla lista dei preferiti per un rapido accesso.
7. Ricerca delle postazioni e dei gruppi nella rete antivirus secondo vari parametri: nome, indirizzo, ID.
8. Visualizzazione e gestione dei messaggi sugli eventi importanti nella rete antivirus tramite le notifiche interattive Push:
   - visualizzazione di tutte le notifiche sul Server Dr.Web;
   - impostazione delle reazioni agli eventi delle notifiche;
   - ricerca delle notifiche secondo i criteri di filtro impostati;
   - eliminazione delle notifiche;
   - esclusione dell'eliminazione automatica delle notifiche.

Si può scaricare il Pannello di controllo mobile dal Pannello di controllo o direttamente da App Store e Google Play.

Protezione delle postazioni della rete

Sui computer e dispositivi mobili protetti vengono installati il modulo di gestione (Agent) e il pacchetto antivirus corrispondente al sistema operativo in uso.

Il carattere multipiattaforma del software permette di proteggere contro i virus i computer e dispositivi mobili gestiti dai seguenti sistemi operativi:

- SO Windows®,
- SO della famiglia UNIX®,
- OS X®,
- Android,
- SO Novell® NetWare®.

Postazioni protette possono essere sia i computer degli utenti che i server LAN. In particolare, è supportata la protezione antivirus del sistema email Microsoft® Outlook®.

Il modulo di gestione aggiorna regolarmente dal Server i componenti antivirus e i database dei virus, nonché invia al Server informazioni sugli eventi di virus accaduti sul computer protetto.

Se il Server di protezione centralizzata non è disponibile, i database dei virus di postazioni protette possono essere aggiornati direttamente tramite Internet dal Sistema di aggiornamento mondiale.

A seconda del sistema operativo della postazione, vengono fornite le funzioni di protezione corrispondenti, riportate di seguito.

Postazioni SO Windows®

Scansione antivirus

Scansione del computer on demand e secondo il calendario. Inoltre, è supportata la possibilità di avviare la scansione antivirus delle postazioni su remoto dal Pannello di controllo, compresa la scansione alla ricerca dei rootkit.

Monitoraggio di file

Scansione continua del file system in tempo reale. Controlla tutti i processi che vengono avviati e file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

Monitoraggio di email

Scansione di ogni email in entrata e in uscita in client di posta.

Inoltre, è possibile utilizzare il filtro antispam (a condizione che la licenza permetta l'utilizzo di tale funzionalità).

Monitoraggio del web

Controllo di ogni connessione a siti web via HTTP. Neutralizzazione delle minacce nel traffico HTTP (per esempio in file inviati o ricevuti), nonché blocco dell'accesso a siti non attendibili o non corretti.

Office control

Controllo dell'accesso a risorse locali e di rete, in particolare, controllo dell'accesso a siti web. Permette di controllare l'integrità dei file importanti, proteggendoli contro le modifiche accidentali o contro l'infezione dai virus, e vieta ai dipendenti l'accesso alle informazioni indesiderate.

Firewall

Protezione dei computer dall'accesso non autorizzato dall'esterno e prevenzione della fuga di informazioni importanti attraverso Internet. Controllo della connessione e del trasferimento di dati attraverso Internet e blocco delle connessioni sospette a livello di pacchetti e di applicazioni.

Quarantena

Isolamento di oggetti dannosi e sospetti in una directory speciale.

Auto-protezione

Protezione dei file e delle directory Dr.Web Enterprise Security Suite contro la rimozione o la modifica non autorizzata o accidentale da parte dell'utente e contro la rimozione o la modifica da parte del malware. Quando l'auto-protezione è attivata, l'accesso ai file e alle directory Dr.Web Enterprise Security Suite è consentito solamente ai processi Dr.Web.

Protezione preventiva

Prevenzione di potenziali minacce alla sicurezza. Controllo dell'accesso agli oggetti critici del sistema operativo, controllo del caricamento driver, dell'esecuzione automatica programmi e del funzionamento dei servizi di sistema, nonché monitoraggio dei processi in esecuzione e blocco processi se rilevata attività di virus.

Postazioni SO famiglia UNIX®

Scansione antivirus

Scansione del computer on demand e secondo il calendario. Inoltre, è supportata la possibilità di avviare la scansione antivirus delle postazioni su remoto dal Pannello di controllo.

Monitoraggio di file

Scansione continua del file system in tempo reale. Controlla tutti i processi che vengono avviati e file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

Monitoraggio del web

Controllo di ogni connessione a siti web via HTTP. Neutralizzazione delle minacce nel traffico HTTP (per esempio in file inviati o ricevuti), nonché blocco dell'accesso a siti non attendibili o non corretti.

Quarantena

Isolamento di oggetti dannosi e sospetti in una directory speciale.

Postazioni OS X®

Scansione antivirus

Scansione del computer on demand e secondo il calendario. Inoltre, è supportata la possibilità di avviare la scansione antivirus delle postazioni su remoto dal Pannello di controllo.

Monitoraggio di file

Scansione continua del file system in tempo reale. Controlla tutti i processi che vengono avviati e file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

Monitoraggio del web

Controllo di ogni connessione a siti web via HTTP. Neutralizzazione delle minacce nel traffico HTTP (per esempio in file inviati o ricevuti), nonché blocco dell'accesso a siti non attendibili o non corretti.

Quarantena

Isolamento di oggetti dannosi e sospetti in una directory speciale.

Dispositivi mobili SO Android

Scansione antivirus

Scansione del dispositivo mobile on demand e secondo il calendario. Inoltre, è supportata la possibilità di avviare la scansione antivirus delle postazioni su remoto dal Pannello di controllo.

Monitoraggio di file

Scansione continua del file system in tempo reale. Scansione di ogni file al momento quando viene salvato nella memoria del dispositivo mobile.

Filtraggio di chiamate e di messaggi

Il filtraggio di messaggi SMS e di chiamate consente di bloccare messaggi e chiamate indesiderati, per esempio messaggi di pubblicità, nonché chiamate e messaggi provenienti da numeri sconosciuti.

Antifurto

Rilevamento della posizione o blocco istantaneo delle funzioni del dispositivo mobile in caso di smarrimento o furto.

Limitazione dell'accesso a risorse Internet

Il filtraggio URL consente di proteggere l'utente del dispositivo mobile dalle risorse di Internet indesiderate.

Firewall

Protezione del dispositivo mobile dall'accesso non autorizzato dall'esterno e prevenzione della fuga di informazioni importanti attraverso la rete. Controllo della connessione e del trasferimento di dati attraverso Internet e blocco delle connessioni sospette a livello di pacchetti e di applicazioni.

Aiuto nella risoluzione di problemi

Diagnostica ed analisi della sicurezza del dispositivo mobile ed eliminazione di problemi e vulnerabilità rilevati.

Controllo dell'esecuzione di applicazioni

Divieto dell'esecuzione sul dispositivo mobile delle applicazioni non incluse nella lista di quelle consentite dall'amministratore.

Server SO Novell® NetWare®

Scansione antivirus

Scansione del computer on demand e secondo il calendario.

Monitoraggio di file

Scansione continua del file system in tempo reale. Controlla tutti i processi che vengono avviati e file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

Assicurazione della comunicazione tra i componenti della rete antivirus

Per assicurare la comunicazione stabile e sicura tra i componenti della rete antivirus, vengono fornite le seguenti possibilità:

Server proxy Dr.Web

Il Server proxy può essere incluso opzionalmente nella struttura di rete antivirus. L'obiettivo principale del Server proxy è assicurare la comunicazione del Server e delle postazioni protette nel caso non sia possibile organizzare l'accesso diretto, per esempio se il Server e le postazioni protette si trovano nelle reti diverse tra cui non c'è l'instradamento dei pacchetti. Tramite la funzione di memorizzazione in cache è anche possibile ridurre il traffico di rete e il tempo di ottenimento degli aggiornamenti da parte delle postazioni protette.

Compressione del traffico

Vengono forniti gli algoritmi di compressione dei dati per la comunicazione tra i componenti di rete antivirus, il che riduce il traffico di rete al minimo.

Cifratura del traffico

Viene fornita la possibilità di cifrare i dati trasmessi tra i componenti di rete antivirus, il che assicura un ulteriore livello di protezione.

Possibilità addizionali

NAP Validator

NAP Validator viene fornito come un componente addizionale e permette di utilizzare la tecnologia Microsoft Network Access Protection (NAP) per controllare l'operatività del software delle postazioni protette. La sicurezza risultante viene raggiunta tramite la soddisfazione dei requisiti per l'operatività delle postazioni della rete.

Loader di repository

Il Loader di repository Dr.Web, fornito come utility addizionale, permette di scaricare i prodotti Dr.Web Enterprise Security Suite dal Sistema di aggiornamento mondiale. Si può uti-

lizzarlo per scaricare aggiornamenti dei prodotti Dr.Web Enterprise Security Suite per mettere gli aggiornamenti su un Server non connesso a Internet.

1.3. Requisiti di sistema

Per l'installazione e il funzionamento di Dr.Web Enterprise Security Suite occorre:

- che il Server Dr.Web sia installato su un computer connesso a Internet per la ricezione automatica degli aggiornamenti dai server SAM (Sistema di aggiornamento mondiale) Dr.Web;

  È ammissibile la possibilità di distribuire gli aggiornamenti in un altro modo sui Server non connessi a Internet. In particolare, in una rete antivirus con diversi server è possibile che soltanto un Server riceva gli aggiornamenti dal SAM per la successiva distribuzione degli stessi sugli altri Server, oppure si può usare l'utility supplementare Loader di repository Dr.Web che scarica gli aggiornamenti dal SAM attraverso Internet e in seguito gli aggiornamenti vengono distribuiti sui Server.

- che i computer della rete antivirus abbiano accesso al Server Dr.Web o al Server proxy;
- per la comunicazione dei componenti antivirus, sui computer in uso devono essere aperte tutte le seguenti porte:

<table>
<tr><th>Numeri di porte</th><th>Protocolli</th><th>Direzione delle connessioni</th><th>Scopo</th></tr>
<tr><td rowspan="3">2193</td><td>TCP</td><td>• in ingresso, in uscita per il Server e il Server proxy
• in uscita per Agent</td><td rowspan="2">Per la comunicazione dei componenti antivirus con il Server e per le connessioni tra i server.

Tra gli altri scopi, viene utilizzata dal Server proxy per stabilire una connessione con i client.</td></tr>
<tr><td>UDP</td><td>in ingresso, in uscita</td></tr>
<tr><td></td><td></td><td>Per il funzionamento dello Scanner di rete.</td></tr>
<tr><td rowspan="2">139, 445</td><td>TCP</td><td>• in ingresso per il Server
• in ingresso, in uscita per l'Agent
• in uscita per il computer su cui viene aperto il Pannello di controllo</td><td rowspan="2">Per il funzionamento dell'Installer di rete.</td></tr>
<tr><td>UDP</td><td>in ingresso, in uscita</td></tr>
<tr><td>9080</td><td>HTTP</td><td rowspan="3">• in ingresso per il Server
• in uscita per il computer su cui viene aperto il Pannello di controllo</td><td rowspan="2">Per il funzionamento del Pannello di controllo della sicurezza Dr.Web.</td></tr>
<tr><td>9081</td><td>HTTPS</td></tr>
<tr><td>10101</td><td>TCP</td><td>Per il funzionamento dell'utility di diagnostica remota del Server.</td></tr>
</table>

Numeri di porte	Protocolli	Direzione delle connessioni	Scopo
80	HTTP	in uscita	Per ricevere aggiornamenti da SAM.
443	HTTPS		

Notare: nelle versioni Server 4 veniva utilizzata la porta `2371` per la connessione dei componenti antivirus con il Server. Nella versione 10 questa porta non è più supportata.

Per il funzionamento del Server Dr.Web occorre:

Componente	Requisiti

Processore e sistema operativo	Sono supportati i seguenti sistemi operativi installati sui computer con le CPU corrispondenti:
	• CPU con il supporto del set di istruzioni SSE2 e con la frequenza di clock di 1,3 GHz e superiori:
	  ▫ SO Windows;
	  ▫ SO Linux;
	  ▫ SO FreeBSD;
	  ▫ SO Solaris x86.
	• CPU V9 UltraSPARC IIIi e superiori:
	  ▫ SO Solaris Sparc.
	La lista completa degli SO supportati è riportata nel documento **Allegati**, in Allegato A.

Memoria operativa	• Requisiti minimi: 1 GB. • Requisiti consigliati: 2 GB e superiori.
Spazio su disco rigido	almeno 12 GB: fino ai 8 GB per il database incorporato (directory di installazione), fino ai 4 GB nella directory temporanea di sistema (per i file operativi). A seconda delle impostazioni del Server, potrebbe essere necessario spazio addizionale per la conservazione di file temporanei, per esempio di pacchetti di installazione di Agent personali (circa 8,5 MB ognuno) nella sottodirectory `var\installers-cache` della directory di installazione di Server Dr.Web. Per l'installazione del Server è necessario che sul disco di sistema in caso di SO Windows o in `/var/tmp` in caso di SO della famiglia UNIX (oppure in un'altra directory di file temporanei se è stata ridefinita), a prescindere dal luogo di installazione del Server stesso, ci siano almeno 1,2 GB per il pacchetto principale e 2,5 GB di memoria libera per il pacchetto supplementare per l'avvio dell'installer e per l'estrazione di file temporanei.

Componente	Requisiti
Altro	Per l'installazione di Server Dr.Web sotto SO della famiglia UNIX è necessaria la disponibilità delle librerie: `lsb` versione 3 e superiori, `glibc` versione 2.7 e superiori. Per l'utilizzo del DB **PostgreSQL** è necessaria la disponibilità della libreria `libpq`. Per l'utilizzo del DB **Oracle** è necessaria la disponibilità della libreria `libaio`. In aggiunta sotto SO **FreeBSD** è necessaria la disponibilità della libreria `compat-8x`.

Per il funzionamento del Server proxy Dr.Web occorre:

Componente	Requisito
Processore	Intel® Pentium® III frequenza di 667 MHz e superiori.
Memoria operativa	almeno 1 GB.
Spazio su disco rigido	almeno 1 GB.
Sistema operativo	• Windows; • Linux; • FreeBSD; • Solaris. La lista completa degli SO supportati è riportata nel documento **Allegati**, in Allegato A.
Altro	Per l'installazione del Server proxy sotto SO della famiglia UNIX è necessaria la disponibilità delle librerie: `lsb` versione 3 e superiori. In aggiunta sotto SO **FreeBSD** è necessaria la disponibilità della libreria `compat-8x`.

Per il funzionamento del Pannello di controllo della sicurezza Dr.Web occorre:

a) Browser web:

Web browser	Supporto
Windows Internet Explorer 8 e superiori	È supportato
Mozilla Firefox 25 e superiori	
Google Chrome 30 e superiori	

Web browser	Supporto
Opera® 10 e superiori	L'uso è ammissibile, però la possibilità di lavoro non è garantita.
Safari® 4 e superiori	

Se si usa il web browser Windows Internet Explorer, si deve tener conto delle seguenti particolarità:

- Non è garantita la completa operatività del Pannello di controllo sotto il web browser Windows Internet Explorer con la modalità attivata **Enhanced Security Configuration for Windows Internet Explorer**.
- Se il Server viene installato su un computer il cui nome include il carattere "_" (trattino basso), non sarà possibile gestire il Server attraverso il Pannello di controllo nel browser. In questo caso deve essere utilizzato un altro web browser.
- Per il corretto funzionamento del Pannello di controllo, l'indirizzo IP e/o il nome DNS del computer su cui è installato il Server Dr.Web devono essere aggiunti ai siti attendibili del web browser in cui viene aperto il Pannello di controllo.
- Per aprire il Pannello di controllo in modo corretto tramite il menu **Start** in SO Windows 8 e Windows Server 2012 con l'interfaccia delle piastrelle dinamiche, è necessario configurare le seguenti impostazioni del web browser: **Opzioni Internet** → **Programmi** → **Apertura di Internet Explorer** spuntare il flag **Sempre in Internet Explorer in visualizzazione classica**.

b) Per utilizzare le piene funzionalità del Pannello di controllo, è necessario installare l'estensione del Pannello di controllo della sicurezza Dr.Web. L'estensione viene fornita insieme al pacchetto Server e viene installata a richiesta del browser nel processo di utilizzo degli elementi del Pannello di controllo che necessitano del caricamento dell'estensione (per Scanner di rete, per l'installazione remota di componenti antivirus).

L'installazione dell'estensione è possibile nei seguenti browser:

Web browser	Versione minima supportata	Versione massima supportata
Windows Internet Explorer	8	11
Mozilla Firefox	25	50.0.1
Google Chrome	30	44.0.2403

Per il funzionamento dell'Estensione del Pannello di controllo della sicurezza Dr.Web sulla pagina dello Scanner di rete in SO Windows, così come in SO della famiglia GNU/Linux, sono necessari i permessi di amministratore (root).

In caso di utilizzo dei browser Mozilla Firefox e Google Chrome, l'estensione del Pannello di controllo della sicurezza Dr.Web è disponibile soltanto per le versioni sotto SO Windows e SO della famiglia Linux.

c) La risoluzione schermo consigliata per l'utilizzo del Pannello di controllo è 1280x1024 px.

Per il funzionamento del Pannello di controllo mobile Dr.Web occorre:

I requisiti variano a seconda del sistema operativo su cui viene installata l'applicazione:

Sistema operativo	Requisito	
	Versione del sistema operativo	**Dispositivo**
iOS	iOS® 7 e superiori	Apple® iPhone® Apple® iPad®
Android	Android 4.0 e superiori	–

Per il funzionamento di NAP occorre:

Per il server:

- SO Windows Server 2008.

Per gli agent:

- SO Windows XP SP3, SO Windows Vista, SO Windows Server 2008.

Per il funzionamento dell'Agent Dr.Web e del pacchetto antivirus completo occorre:

I requisiti sono diversi a seconda del sistema operativo in cui viene installata la soluzione antivirus (la lista completa dei sistemi operativi supportati è riportata nel documento **Allegati**, in Allegato A. Lista completa delle versioni supportate dei SO):

- SO Windows:

Componente	Requisito
Processore	CPU con la frequenza di clock di 1 GHz e superiori.
Memoria operativa libera	Almeno 512 MB.
Spazio libero su disco rigido	Almeno 1 GB per i file eseguibili + spazio addizionale per i log di funzionamento e per i file temporanei.

Componente	Requisito
Altro	1. Per il corretto funzionamento della guida sensibile al contesto di **Agent Dr.Web per Windows** è necessaria la disponibilità di Windows® Internet Explorer® 6.0 e superiori. 2. Per il plugin Dr.Web per Microsoft Outlook deve essere installato il client Microsoft Outlook di Microsoft Office: • Outlook 2000; • Outlook 2002; • Outlook 2003; • Outlook 2007; • Outlook 2010 SP2; • Outlook 2013; • Outlook 2016.

- SO della famiglia Linux:

Componente	Requisito
Processore	Sono supportati i processori con l'architettura e il set di istruzioni Intel/AMD: 32 bit (IA-32, x86); 64 bit (x86-64, x64, amd64).
Memoria operativa libera	Almeno 512 MB.
Spazio libero su disco rigido	Almeno 400 MB di spazio libero sul volume su cui sono situate le directory di Antivirus.

- OS X, SO Android, SO Novell NetWare: i requisiti di configurazione coincidono con i requisiti di sistema operativo.

Sulle postazioni della rete antivirus gestita tramite Dr.Web non deve essere utilizzato altro software antivirus (neanche altre versioni dei programmi antivirus Dr.Web).

La descrizione delle funzionalità di Agent è riportata nei manuali utente per il sistema operativo corrispondente.

1.4. Contenuto del pacchetto

Il pacchetto Dr.Web Enterprise Security Suite viene fornito a seconda di SO di Server Dr.Web scelto:

1. In caso di UNIX – come file in formato `run`:

Nome del file	Componente
drweb-esuite-server-10.01.0-<*build*>-<*versione_SO*>.run	Pacchetto principale di Server Dr.Web
drweb-esuite-extra-10.01.0-<*build*>-<*versione_SO*>.run	Pacchetto supplementare di Server Dr.Web
drweb-esuite-proxy-10.01.0-<*build*>-<*versione_SO*>.run	Server proxy

2. In caso di Windows – come file eseguibili:

Nome del file	Componente
drweb-esuite-server-10.01.0-<*build*>-<*versione_SO*>.exe	Pacchetto principale di Server Dr.Web
drweb-esuite-extra-10.01.0-<*build*>-<*versione_SO*>.exe	Pacchetto supplementare di Server Dr.Web
drweb-esuite-proxy-10.01.0-<*build*>-<*versione_SO*>.msi	Server proxy
drweb-esuite-agent-activedirectory-10.01.0-<*build*>.msi	Agent Dr.Web per Active Directory
drweb-esuite-modify-ad-schema-10.01.0-<*build*>-<*versione_SO*>.exe	Utility per modificare lo schema Active Directory
drweb-esuite-aduac-10.01.0-<*build*>-<*versione_SO*>.msi	Utility per modificare gli attributi degli oggetti Active Directory
drweb-esuite-napshv-10.01.0-<*build*>-<*versione_SO*>.msi	NAP Validator
drweb-esuite-agent-full-11.00.0-<*versione_build*>-windows.exe	Installer completo di Agent Dr.Web. Anche fa parte del pacchetto supplementare di Server Dr.Web.

Il pacchetto di Server Dr.Web è composto da due pacchetti:

1. *Pacchetto principale* – il pacchetto base per l'installazione di Server Dr.Web. Il pacchetto include le parti analoghe a quelle incluse nel pacchetto delle versioni precedenti di Dr.Web Enterprise Security Suite.

   Il pacchetto principale permette di installare il Server Dr.Web stesso che include i pacchetti di protezione antivirus soltanto per le postazioni Windows.
2. *Pacchetto supplementare (extra)* – include i pacchetti di tutti i prodotti per l'impresa forniti per l'installazione sulle postazioni protette gestite da tutti gli SO supportati.

   Viene installato come un supplemento su un computer su cui è già installato il pacchetto principale di Server Dr.Web.

Il pacchetto supplementare deve essere dello stesso tipo del pacchetto principale.

Il pacchetto principale di Server Dr.Web include i seguenti componenti:

- software di Server Dr.Web per il SO corrispondente,
- software di Agent Dr.Web e di pacchetti antivirus per le postazioni SO Windows,
- software di Pannello di controllo della sicurezza Dr.Web,
- database dei virus,
- Estensione del Pannello di controllo della sicurezza Dr.Web,
- Estensione Dr.Web Server FrontDoor,
- documentazione, moduli ed esempi.

  Oltre al pacchetto, vengono forniti anche i numeri di serie, dopo la registrazione dei quali si ottengono i file con le chiavi di licenza.

Capitolo 2: Concessione delle licenze

Per il funzionamento della soluzione antivirus Dr.Web Enterprise Security Suite è necessaria una licenza.

Il contenuto e il prezzo di una licenza di utilizzo di Dr.Web Enterprise Security Suite dipendono dal numero di postazioni protette, compresi i server che rientrano nella rete di Dr.Web Enterprise Security Suite come postazioni protette.

Queste informazioni si devono obbligatoriamente comunicare al rivenditore della licenza prima dell'acquisto della soluzione Dr.Web Enterprise Security Suite. Il numero di Server Dr.Web in uso non influisce sull'aumento del prezzo della licenza.

File della chiave di licenza

I diritti di utilizzo di Dr.Web Enterprise Security Suite vengono regolati tramite i file della chiave di licenza.

Il formato del file della chiave è protetto da modifica tramite il metodo di firma digitale. La modifica del file lo rende non valido. Per evitare danni accidentali al file della chiave di licenza, non si deve modificarlo e/o salvarlo dopo averlo visualizzato in un editor di testo.

I file della chiave di licenza vengono forniti in un archivio .zip contenente uno o più file della chiave per postazioni protette.

L'utente può ottenere i file della chiave di licenza in uno dei seguenti modi:

- Il file della chiave di licenza fa parte del set antivirus Dr.Web Enterprise Security Suite acquistato, se è stato incluso nel pacchetto software all'assemblaggio. Tuttavia, di regola, vengono forniti solamente i numeri di serie.
- Il file della chiave di licenza viene inviato agli utenti via email dopo la registrazione del numero di serie sul sito web della società Doctor Web sull'indirizzo http://products.drweb.com/register/ , se un altro indirizzo non è indicato nella scheda di registrazione allegata al prodotto. Andare al sito indicato, compilare il modulo con le informazioni sull'acquirente e inserire nel campo indicato il numero di serie di registrazione (è reperibile nella scheda di registrazione). Un archivio con i file della chiave verrà inviato sull'indirizzo email indicato dall'utente. Si potrà inoltre scaricare i file della chiave direttamente dal sito indicato.
- Il file della chiave di licenza può essere fornito su un supporto separato.

Si consiglia di conservare il file della chiave di licenza fino alla scadenza della sua validità e di utilizzarlo per la reinstallazione o per il ripristino dei componenti del programma. In caso di perdita del file della chiave di licenza, si può rifare la procedura di registrazione sul sito indicato e ottenere nuovamente un file della chiave di licenza. A questo scopo occorre indicare lo stesso numero di serie di registrazione e le stesse informazioni sull'acquirente che sono state indicate per la pri-

ma registrazione; soltanto l'indirizzo email può essere diverso. In questo caso il file della chiave di licenza verrà inviato sul nuovo indirizzo email.

Per provare l'Antivirus, è possibile utilizzare i file della chiave demo. Tali file della chiave assicurano le funzionalità complete dei principali componenti antivirus, ma hanno una validità limitata. Per ottenere i file della chiave demo, è necessario compilare un modulo situato sulla pagina https://download.drweb.com/demoreq/biz/. La richiesta verrà valutata su base individuale. Nel caso di decisione positiva, un archivio con i file della chiave di licenza verrà inviato sull'indirizzo email indicato dall'utente.

L'utilizzo dei file della chiave di licenza nel processo di installazione del programma è descritto in **Guida all'installazione**, p. Installazione di Server Dr.Web.

L'utilizzo dei file della chiave di licenza per una rete antivirus già dispiegata è descritto in p. Gestione licenze.

2.1. Caratteristiche delle licenze

1. Server Dr.Web non viene concesso in licenza.

   L'UUID di Server che nelle versioni precedenti di Dr.Web Enterprise Security Suite era memorizzato nella chiave di licenza di Server adesso è memorizzato nel file di configurazione di Server (a partire dalla versione 10).

   - Quando viene installato un nuovo Server, viene generato un nuovo UUID.
   - Quando il Server viene aggiornato dalle versioni precedenti, l'UUID viene preso automaticamente dalla chiave del Server della versione precedente (file `enterprise.key` nella directory `etc` dell'installazione precedente del Server) e viene registrato nel file di configurazione del Server che viene installato.

   Se viene aggiornato un cluster dei Server, il Server responsabile dell'aggiornamento del database riceve la chiave di licenza. Per gli altri Server le chiavi di licenza devono essere aggiunte manualmente.

2. Le chiavi di licenza sono rilevanti soltanto per le postazioni protette. È possibile assegnare licenze sia a singole postazioni, che a gruppi di postazioni: in questo caso una chiave di licenza vale per tutte le postazioni che la ereditano da questo gruppo. Per assegnare un file della chiave contemporaneamente a tutte le postazioni della rete antivirus, cui non sono state assegnate le impostazioni individuali della chiave di licenza, assegnare la chiave di licenza al gruppo **Everyone**.
3. Il file della chiave di licenza può essere impostato durante l'installazione di Server Dr.Web (v. **Guida all'installazione**, p. Installazione di Server Dr.Web).

   È possibile però installare un Server anche senza una chiave di licenza. La licenza può essere aggiunta in seguito sia localmente e sia può essere ricevuta attraverso la comunicazione tra i server.
4. Attraverso la comunicazione tra i server è possibile trasferire un numero opzionale di licenze dalle chiavi conservate su questo Server a un Server adiacente per un determinato periodo.

5. È possibile utilizzare alcune licenze diverse, per esempio licenze con diverse scadenze o con un diverso insieme di componenti antivirus per postazioni protette. Ogni chiave di licenza può essere assegnata contemporaneamente a più oggetti di licenza (gruppi e postazioni). Più chiavi di licenza possono essere assegnate contemporaneamente allo stesso oggetto di licenza.
6. Quando vengono assegnate più chiavi ad un oggetto, prestare attenzione alle seguenti particolarità:
   a) Se diverse chiavi dello stesso oggetto hanno un diverso elenco dei componenti antivirus consentiti, l'elenco dei componenti consentiti per le postazioni viene determinato tramite l'intersezione degli insiemi di componenti nelle chiavi. Per esempio, se a un gruppo di postazioni sono state assegnate una chiave con il supporto di Antispam ed una senza il supporto di Antispam, l'installazione di Antispam sulle postazioni sarà vietata.
   b) Le impostazioni di licenza per un oggetto vengono calcolate sulla base di tutte le chiavi assegnate a quest'oggetto. Se le scadenze delle chiavi di licenza sono diverse, allora dopo che è scaduta una chiave con la validità minima è necessario sostituirla o eliminarla manualmente. Se la chiave scaduta impostava limitazioni all'installazione dei componenti antivirus, è necessario modificare le impostazioni dell'oggetto di licenza nella sezione **Componenti da installare**.
   c) Il numero di licenze di un oggetto viene calcolato dalla somma delle licenze di tutte le chiavi assegnate a quest'oggetto. È inoltre necessario tenere conto della possibilità di trasferimento delle licenze attraverso la comunicazione tra i server su un Server adiacente (v. p. 4). In questo caso, dal numero totale di licenze vengono sottratte le licenze trasferite su un Server adiacente.

Le chiavi di licenza vengono gestite attraverso la Gestione licenze.

Quando una chiave di licenza viene impostata nella Gestione licenze, tutte le informazioni su questa licenza vengono salvate nel database.

2.2. Aggiornamento automatico delle licenze

Una licenza per Dr.Web Enterprise Security Suite può essere aggiornata in maniera automatica.

L'aggiornamento automatico della licenza sottintende i seguenti aspetti:

- Quando scade una chiave di licenza, essa può essere sostituita automaticamente dal programma con una chiave di licenza precedentemente acquistata.
- L'aggiornamento automatico viene eseguito per una chiave di licenza specifica per cui è stato acquistato un rinnovo.
- La chiave di licenza che verrà utilizzata per l'aggiornamento automatico si trova sui server della società Doctor Web fino alla scadenza della chiave di licenza che va rinnovata.
- La verifica della disponibilità dell'aggiornamento automatico (disponibilità di una chiave di licenza sui server della società Doctor Web) e l'aggiornamento stesso vengono eseguiti quando viene eseguito il task **La scadenza della chiave di licenza** dal calendario di Server Dr.Web.

Se il task **La scadenza della chiave di licenza** è disattivato nel calendario di Server, l'aggiornamento automatico della licenza non sarà possibile.

Per avviare il task, è necessario che vengano soddisfatte le seguenti condizioni:

- Sta per scadere la licenza corrente (il numero di giorni mancanti alla scadenza viene impostato nei parametri del task).
- La licenza corrente appartiene a questo Server: al principio è stata aggiunta manualmente od ottenuta attraverso l'aggiornamento automatico. Licenze ottenute dai Server adiacenti attraverso le relazioni tra i server non sono soggette all'aggiornamento automatico tramite un task dal calendario di Server.

Aggiornamento delle licenze automatico programmato

Sono possibili i seguenti risultati dell'esecuzione del task **La scadenza della chiave di licenza**:

1. *L'aggiornamento automatico non è disponibile per la licenza*.

   All'amministratore viene inviato un avviso **La scadenza della chiave di licenza**.

2. *L'aggiornamento automatico è disponibile per la licenza. La lista dei componenti concessi in licenza della chiave corrente è diversa da quella della chiave nuova (nella chiave nuova non c'è qualche componente che c'è in quella corrente) o la chiave di licenza nuova ha un minor numero di licenze rispetto alla chiave di licenza corrente.*

   La nuova licenza viene scaricata dai server Doctor Web, viene aggiunta alla Gestione licenze e al database di Server, ma non viene distribuita sugli oggetti di licenza. In tale situazione è necessario distribuire manualmente la chiave di licenza.

   All'amministratore viene inviato un avviso **Chiave di licenza non può essere aggiornata automaticamente**. Il motivo specifico per cui la chiave non può essere distribuita automaticamente verrà riportato nell'avviso.

3. *L'aggiornamento automatico è disponibile per la licenza. Le liste dei componenti concessi in licenza della chiave corrente e di quella nuova corrispondono (o nella chiave nuova ci sono più componenti concessi in licenza rispetto alla chiave corrente, compresi tutti i componenti della chiave corrente), il numero di licenze della chiave di licenza nuova è superiore o uguale a quello della chiave di licenza corrente.*

   La nuova licenza viene scaricata dai server Doctor Web, viene aggiunta alla Gestione licenze e al database di Server e viene distribuita su tutti gli oggetti di licenza su cui era distribuita la licenza precedente, compresi i Server adiacenti.

   La licenza vecchia verrà rimossa quando non sarà utilizzata da alcun Server subordinato. Pertanto, se al momento dell'aggiornamento automatico un Server subordinato era disconnesso, la licenza vecchia verrà conservata fino a quando questo Server subordinato non si riconnetterà.

   La licenza vecchia verrà conservata fino a quando non verrà rimossa manualmente nei seguenti casi:

   - Se non è possibile distribuire la licenza ottenuta tramite l'aggiornamento automatico su un Server subordinato (il Server è stato disconnesso in modo permanente).

- Se su un Server subordinato viene utilizzata una versione del protocollo che non supporta le funzionalità aggiornamenti automatici. In questo caso licenze verranno trasferite sul Server subordinato, ma non verranno distribuite.

All'amministratore viene inviato un avviso **Chiave di licenza è aggiornata automaticamente**. L'avviso di aggiornamento verrà inviato da ciascun Server su cui verrà distribuita la nuova licenza.

Tutti gli avvisi da essere inviati all'amministratore vengono configurati nella sezione **Amministrazione → Configurazione delle notifiche**.

Dopo l'invio di ciascun avviso viene eseguita la procedura personalizzata **Aggiornamento automatico della chiave di licenza**.

Aggiornamento delle licenze manuale

Se si è acquistata una chiave di licenza per l'aggiornamento automatico della chiave corrente, non è richiesto aggiungere la nuova chiave manualmente nella Gestione licenze. A seconda della situazione (la variante 2 nella procedura sopra) può essere richiesta soltanto la distribuzione manuale sugli oggetti di licenza.

Tuttavia, se prima dell'esecuzione del task **La scadenza della chiave di licenza** si è aggiunta in autonomo attraverso la Gestione licenze la nuova chiave soggetta all'aggiornamento automatico secondo la variante 3 (v. la procedura sopra), allora durante l'esecuzione del task verrà effettuata soltanto la distribuzione della nuova chiave di licenza. In questo caso sono possibili le seguenti varianti:

a) La nuova chiave di licenza è stata distribuita manualmente su tutti gli oggetti su cui era distribuita la chiave precedente (quella che viene aggiornata). In tale caso durante l'esecuzione del task di aggiornamento non verranno apportate alcune modifiche.

b) La nuova chiave di licenza è stata distribuita manualmente su alcuni oggetti di quelli su cui era distribuita la chiave precedente (quella che viene aggiornata). In tale caso durante l'esecuzione del task di aggiornamento la nuova chiave verrà distribuita su tutti gli oggetti rimanenti della chiave precedente che non hanno ancora ricevuto l'aggiornamento.

   Se la nuova chiave di licenza è stata distribuita manualmente su ulteriori oggetti che non c'erano nella lista della chiave precedente, dopo l'esecuzione del task la nuova chiave rimarrà distribuita anche su questi oggetti. In questo caso sono possibili le seguenti varianti:

   - Il numero di licenze è sufficiente a tutti gli oggetti di licenza: a quelli che c'erano nella chiave precedente e a quelli assegnati manualmente alla nuova chiave. Tale situazione è possibile se la nuova chiave contiene un maggior numero di licenze. In tale caso durante l'esecuzione del task di aggiornamento non verranno apportate alcune modifiche.
   - Il numero di licenze non è sufficiente per distribuire licenze su tutti gli oggetti di licenza che c'erano nella chiave precedente perché delle licenze sono state assegnate manualmente ad altri oggetti. L'aggiornamento non verrà eseguito per gli oggetti che non hanno avuto licenze, però la chiave precedente verrà rimossa comunque e gli oggetti rimarranno senza licenze. Quando compariranno licenze libere, tutti gli oggetti che non hanno avuto licenze otter-

ranno la nuova chiave di licenza. In questo caso le azioni dipendono dal tipo di oggetto di licenza:

- Se le licenze dalla nuova chiave non sono bastate a postazioni di questo Server, la verifica di licenze disponibili verrà eseguita ogni volta quando una postazione cercherà di connettersi al Server. Se al momento di una connessione verrà rilevata una licenza liberata, quest'ultima verrà concessa a tale postazione.
- Se le licenze dalla nuova chiave non sono bastate per essere rilasciate ai Server adiacenti, la verifica di licenze disponibili verrà eseguita automaticamente circa una volta al minuto. Quando compariranno licenze libere, verranno date ai Server adiacenti.

File della chiave di licenza

Notare le seguenti caratteristiche dei file della chiave di licenza quando viene eseguito l'aggiornamento automatico:

- Quando viene eseguito l'aggiornamento automatico, la nuova licenza viene scaricata dai server della società Doctor Web, le informazioni su di essa vengono salvate nel database di Server e visualizzate in Gestione licenze. In questo caso non viene creato alcun file della chiave di licenza.
- Per ottenere un file della chiave di licenza, utilizzare l'opzione **Amministrazione** → **Gestione licenze** → **Esporta chiave**. Un file della chiave di licenza può inoltre essere ottenuto con l'esecuzione della procedura personalizzata **Aggiornamento automatico della chiave di licenza**.
- Quando la licenza viene rimossa, le informazioni su di essa vengono rimosse da Gestione licenze e dal database di Server, però il file della chiave di licenza rimane nella directory di Server.

Capitolo 3: Introduzione all'uso

3.1. Creazione della rete antivirus

Brevi istruzioni per l'installazione di una rete antivirus:

1. Preparare uno schema della struttura della rete antivirus, includerci tutti i computer e dispositivi mobili protetti.

   Selezionare il computer che svolgerà le funzioni di Server Dr.Web. In una rete antivirus potrebbero rientrare diversi Server Dr.Web. Le caratteristiche di tale configurazione sono descritte in p. Caratteristiche di una rete con diversi Server Dr.Web.

   > Il Server Dr.Web può essere installato su qualsiasi computer e non soltanto su quello che svolge le funzioni server LAN. I requisiti principali nei confronti di tale computer sono riportati in p. Requisiti di sistema.
   >
   > Su tutte le postazioni protette, compresi i server di rete locale, viene installata la stessa versione di Agent Dr.Web. La differenza sta nella lista dei componenti antivirus che vengono installati, definita in base alle impostazioni sul Server.

   Per installare il Server Dr.Web e l'Agent Dr.Web, è necessario accedere una volta ai relativi computer (fisicamente o utilizzando strumenti di gestione e di avvio programmi su remoto). Tutte le operazioni successive vengono eseguite dalla postazione di lavoro dell'amministratore della rete antivirus (anche probabilmente dall'esterno della rete locale) e non richiedono l'accesso ai Server Dr.Web o alle postazioni.
2. In base allo schema progettato determinare quali prodotti per quali sistemi operativi si dovranno installare sui nodi della rete corrispondenti. Le informazioni dettagliate sui prodotti disponibili sono riportate nella sezione Contenuto del pacchetto.

   Tutti i prodotti richiesti possono essere acquistati come le soluzioni boxed Dr.Web Enterprise Security Suite o scaricati sul sito web della società Doctor Web https://download.drweb.com/.

   > Agent Dr.Web per le postazioni SO Android, SO Linux, OS X possono anche essere installati dai pacchetti di prodotti standalone e successivamente connessi al Server Dr.Web centralizzato. Le relative impostazioni di Agent sono descritte in **Guida all'installazione**, p. Installazione di Agent Dr.Web attraverso il pacchetto d'installazione personale.
3. Installare il pacchetto principale di Server Dr.Web su uno o diversi computer selezionati. L'installazione viene descritta in **Guida all'installazione**, p. Installazione di Server Dr.Web.

   Insieme al Server viene installato il Pannello di controllo della sicurezza Dr.Web.

   Di default, Server Dr.Web viene avviato automaticamente dopo l'installazione e dopo ogni riavvio del sistema operativo.
4. Se la rete antivirus includerà le postazioni protette SO Android, SO Linux, OS X, installare il pacchetto supplementare di Server Dr.Web su tutti i computer su cui è installato il pacchetto principale di Server.

5. Se necessario, installare e configurare il Server proxy. La descrizione viene riportata in **Guida all'installazione**, p. Installazione del Server proxy.
6. Per configurare il Server e il software antivirus su postazioni, è necessario connettersi al Server attraverso il Pannello di controllo della sicurezza Dr.Web.

   > Il Pannello di controllo può essere aperto su qualsiasi computer e non soltanto su quello su cui è installato il Server. Basta che ci sia una connessione di rete con il computer su cui è installato il Server.

   Il Pannello di controllo è disponibile sull'indirizzo:

   `http://<Indirizzo_Server>:9080`

   o

   `https://<Indirizzo_Server>:9081`

   dove come *<Indirizzo_Server>* indicare l'indirizzo IP o il nome a dominio del computer su cui è installato il Server Dr.Web.

   Nella finestra di dialogo di richiesta di autenticazione impostare il nome utente e la password dell'amministratore.

   Il nome di amministratore predefinito è **admin**.

   La password:

   - in caso di SO Windows – la password che è stata impostata quando veniva installato il Server.
   - in caso di SO della famiglia UNIX – **root**.

   > Per il Server sotto SO della famiglia UNIX modificare la password di amministratore predefinita al momento della prima connessione al Server.

   In caso di una connessione riuscita al Server, si apre la finestra principale del Pannello di controllo (per la descrizione dettagliata v. in p. Pannello di controllo della sicurezza Dr.Web).
7. Effettuare la configurazione iniziale di Server (le impostazioni di Server vengono descritte dettagliatamente in Capitolo 8: Configurazione di Server Dr.Web):
   a. Nella sezione Gestione licenze aggiungere uno o più chiavi di licenza e distribuirle ai gruppi corrispondenti, in particolare, al gruppo **Everyone**. Il passaggio è obbligatorio se durante l'installazione di Server la chiave di licenza non è stata impostata.
   b. Nella sezione Configurazione generale del repository impostare quali componenti della rete antivirus verranno aggiornati da SAM Dr.Web. Nella sezione Stato del repository eseguire un aggiornamento dei prodotti nel repository di Server. L'aggiornamento può richiedere un lungo tempo. Attendere fino a quando il processo di aggiornamento non sarà terminato prima di proseguire con la successiva configurazione.
   c. Sulla pagina **Amministrazione** → **Server Dr.Web** sono riportate le informazioni sulla versione di Server. Se è disponibile una nuova versione, aggiornare Server, come descritto in p. Aggiornamento di Server Dr.Web e ripristino da copia di backup.
   d. Se necessario, configurare Connessioni di rete per modificare le impostazioni di rete di default utilizzate per l'interazione di tutti i componenti della rete antivirus.

e. Se necessario, configurare la lista degli amministratori di Server. Inoltre, è disponibile l'autenticazione di amministratori esterna. Per maggiori informazioni v. Capitolo 5: Amministratori della rete antivirus.

f. Prima di iniziare ad utilizzare il software antivirus, è consigliabile modificare l'impostazione della directory per il backup dei dati critici del Server (v. p. Configurazione del calendario di Server Dr.Web). È preferibile collocare questa directory su un altro disco locale per ridurre la probabilità di una perdita simultanea dei file del software Server e della copia di backup.

8. Configurare il software antivirus per le postazioni (la configurazione dei gruppi e delle postazioni viene descritta dettagliatamente in Capitolo 6 e Capitolo 7):

   a. Se necessario, creare gruppi di postazioni personalizzati.

   b. Configurare il gruppo **Everyone** e i gruppi personalizzati creati. In particolare, configurare la sezione dei componenti da installare.

9. Installare il software Agent Dr.Web sulle postazioni.

   Nella sezione File di installazione controllare l'elenco dei file disponibili per l'installazione di Agent. Selezionare la variante di installazione adatta, basandosi sul sistema operativo della postazione, sulla possibilità di installazione su remoto, sulla variante di configurazione delle impostazioni di Server nel corso dell'installazione di Agent ecc. Per esempio:

   - Se gli utenti installano l'antivirus in autonomo, utilizzare pacchetti di installazione personali che vengono creati attraverso il Pannello di controllo separatamente per ciascuna postazione. Questo tipo di pacchetti può inoltre essere inviato agli utenti via email direttamente dal Pannello di controllo. Dopo l'installazione le postazioni si connettono al Server in modo automatico.
   - Per un'installazione remota attraverso la rete allo stesso tempo su una o più postazioni (soltanto per le postazioni SO Windows) utilizzare l'installer di rete. L'antivirus viene installato attraverso il Pannello di controllo con l'impiego di una determinata estensione del browser.
   - Inoltre, è possibile installare l'antivirus in remoto attraverso la rete su una o più postazioni, utilizzando il servizio Active Directory. A tale scopo si usa l'installer di Agent Dr.Web per le reti con Active Directory che viene fornito insieme al pacchetto Dr.Web Enterprise Security Suite, ma separatamente dall'installer di Server.
   - Se nel processo dell'installazione è necessario ridurre il carico sul canale di comunicazione tra Server e postazioni, è possibile utilizzare l'installer completo che installa contemporaneamente Agent e i componenti di protezione.
   - L'installazione su postazioni Android, Linux, OS X può essere eseguita localmente secondo le regole generali. Inoltre, un prodotto standalone già installato può connettersi al Server sulla base della configurazione corrispondente.

10. Non appena installati sui computer, gli Agent si connettono automaticamente al Server. Le postazioni antivirus vengono autenticate sul Server a seconda dei criteri scelti (v. p. Criteri di approvazione delle postazioni):

    a. In caso di installazione dai pacchetti di installazione e inoltre in caso di configurazione di conferma automatica sul Server, le postazioni vengono registrate automaticamente al momento della prima connessione al Server e non è richiesta alcuna ulteriore conferma.

    b. In caso di installazione dagli installer e di configurazione di conferma di accesso manuale, l'amministratore deve confermare manualmente le nuove postazioni in modo da registrarle

sul Server. In questo caso, le nuove postazioni non vengono connesse automaticamente, ma vengono messe dal Server nel gruppo dei nuovi arrivi.

11. Dopo che la postazione si è connessa al Server e ha ottenuto le impostazioni, su di essa viene installato il relativo set di componenti del pacchetto antivirus, definito nelle impostazioni del gruppo primario della postazione.

   Per completare l'installazione dei componenti della postazione, sarà necessario il riavvio del computer.

12. È possibile configurare le postazioni e il software antivirus anche dopo l'installazione (la descrizione dettagliata viene riportata in Capitolo 7).

3.2. Configurazione delle connessioni di rete

Informazioni generali

Al Server Dr.Web si connettono i seguenti client:

- Agent Dr.Web,
- Installer di Agent Dr.Web,
- altri Server Dr.Web.

Una connessione viene sempre stabilita da parte del client.

Sono disponibili i seguenti modi di connessione dei client al Server:

1. Tramite le connessioni dirette.

   Questo approccio ha tanti vantaggi, ma non è sempre preferibile (ci sono perfino delle situazioni quando non si deve utilizzarlo).

2. Tramite il Servizio di rilevamento Server.

   Di default (se non configurati diversamente), i client utilizzano proprio questo Servizio.

   Questo approccio è da utilizzare se è necessaria la riconfigurazione di tutto il sistema, in particolare, se si deve trasferire il Server Dr.Web su altro computer o cambiare l'indirizzo IP del computer su cui è installato il Server.

3. Tramite il protocollo SRV.

   Questo approccio permette di cercare il Server per nome del computer e/o del servizio Server sulla base dei record SRV su server DNS.

Se nelle impostazioni della rete antivirus Dr.Web Enterprise Security Suite è indicato l'utilizzo di connessioni dirette, il Servizio di rilevamento Server può essere disattivato. Per farlo, nella descrizione dei trasporti (**Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Rete** → scheda **Trasporto**) si deve lasciare vuoto il campo **Gruppo multicast**.

Configurazione del firewall

Per l'interazione dei componenti della rete antivirus è necessario che tutte le porte ed interfacce utilizzate siano aperte su tutti i computer che fanno parte della rete antivirus.

Durante l'installazione di Server l'installer aggiunge automaticamente le porte e le interfacce di Server alle eccezioni del firewall SO Windows.

Se sul computer viene utilizzato un firewall diverso da quello SO Windows, l'amministratore della rete antivirus deve configuralo manualmente in modo opportuno.

3.2.1. Connessioni dirette

Configurazione del Server Dr.Web

Nelle impostazioni di Server deve essere indicato l'indirizzo (v. documento **Allegati**, p. Allegato E. Specifica di indirizzo di rete) su cui il Server deve essere "in ascolto" per la ricezione delle connessioni TCP in arrivo.

Questo parametro viene indicato nelle impostazioni del Server **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Rete** → scheda **Trasporto** → campo **Indirizzo**.

Di default, viene impostato che il Server "è in ascolto" con i seguenti parametri:

- **Indirizzo**: valore vuoto – utilizza *tutte le interfacce di rete* per questo computer su cui è installato Server.
- **Porta**: `2193` – utilizza la porta `2193` assegnata a Dr.Web Enterprise Security Suite in IANA.

> Notare: nelle versioni Server 4 veniva utilizzata la porta `2371`. Nella versione 10 questa porta non è più supportata.

Per il funzionamento corretto di tutto il sistema Dr.Web Enterprise Security Suite, è sufficiente che il Server "sia in ascolto" di almeno una porta TCP che deve essere conosciuta da tutti i client.

Configurazione dell'Agent Dr.Web

Durante l'installazione dell'Agent, l'indirizzo del Server (indirizzo IP o nome DNS del computer su cui è avviato il Server Dr.Web) può essere esplicitamente indicato nei parametri di installazione:

`drwinst` <*Indirizzo_Server*>

Durante l'installazione dell'Agent, è consigliabile utilizzare il nome del Server registrato nel servizio DNS. Questo semplifica il processo di configurazione della rete antivirus nel caso si dovrà reinstallare il Server Dr.Web su un altro computer.

Di default, il comando `drwinst` eseguito senza parametri scansiona la rete alla ricerca dei Server Dr.Web e tenta di installare l'Agent dal primo Server rilevato nella rete (modalità *Multicasting* con utilizzo di Servizio di rilevamento Server).

In questo modo, l'indirizzo del Server Dr.Web diventa conosciuto dall'Agent durante l'installazione.

In seguito, l'indirizzo del Server può essere modificato manualmente nelle impostazioni dell'Agent.

3.2.2. Servizio di rilevamento di Server Dr.Web

Con questo metodo di connessione, il client non conosce inizialmente l'indirizzo del Server. Ogni volta prima di stabilire la connessione, il client cerca il Server nella rete. Per farlo, il client invia nella rete una richiesta broadcast e aspetta una risposta dal Server in cui è indicato il suo indirizzo. Dopo aver ricevuto la risposta, il client stabilisce una connessione al Server.

Per questo fine, il Server deve rimanere "in ascolto" di tali richieste sulla rete.

Sono possibili diverse varianti di configurazione di questo modo. L'importante è che il metodo di ricerca del Server, impostato per i client, corrisponda alle impostazioni della parte relativa del Server.

In Dr.Web Enterprise Security Suite di default viene utilizzata la modalità *Multicast over UDP*:

1. Il Server viene registrato in un gruppo multicast con l'indirizzo indicato nelle impostazioni del Server.
2. Gli Agent, cercando il Server, inviano nella rete le richieste multicast sull'indirizzo di gruppo definito nel punto 1.

Di default per "l'ascolto" da parte del Server viene impostato (come per le connessioni dirette): `udp/231.0.0.1:2193`.

> Notare: nei Server versione 4 veniva utilizzata la porta `2371`. Nella versione 10 questa porta non è più supportata.

Questo parametro viene configurato nelle impostazioni del Pannello di controllo **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Rete** → scheda **Trasporto** → campo **Gruppo multicast**.

3.2.3. Utilizzo del protocollo SRV

I client SO Windows supportano il protocollo di rete del client *SRV* (la descrizione del formato è riportata nel documento **Allegati**, p. Allegato E. Specifica di indirizzo di rete).

Un client può connettersi al Server tramite i record SRV nel seguente modo:

1. Durante l'installazione del Server, viene configurata la registrazione in dominio Active Directory, e l'installer inserisce il record SRV corrispondente su server DNS.

   Il record SRV viene inserito su server DNS in conformità a RFC2782 (v. http://tools.ietf.org/html/rfc2782).

2. Quando viene richiesta una connessione a Server, l'utente imposta la comunicazione attraverso il protocollo `srv`.

   Per esempio, l'esecuzione dell'installer di Agent:

   - con l'esplicita indicazione del nome del servizio `myservice`:
     `drwinst /server "srv/myservice"`
   - senza l'esplicita indicazione del nome del servizio. In tale caso nei record SRV verrà cercato il nome di default – `drwcs`
     `drwinst /server "srv/"`

3. Il client utilizza le funzioni del protocollo SRV in modo trasparente all'utente per la comunicazione con Server.

   Se per la connessione, il Server non è indicato in modo esplicito, come il nome del servizio predefinito viene utilizzato `drwcs`.

Capitolo 4: Componenti della rete antivirus e la loro interfaccia

4.1. Server Dr.Web

La rete antivirus deve includere almeno un Server Dr.Web.

Per aumentare l'affidabilità e la produttività della rete antivirus, nonché per bilanciare il carico, Dr.Web Enterprise Security Suite consente di creare una rete antivirus con diversi Server. In tale caso, il software server viene installato su più computer contemporaneamente.

Server Dr.Web è un servizio residente in memoria operativa. Il software Server Dr.Web è progettato per diversi SO (l'elenco completo degli SO supportati è disponibile in documento **Allegati**, in Allegato A).

Funzioni principali

Il Server Dr.Web svolge le seguenti funzioni:

- avviare un'installazione dei pacchetti antivirus su un computer selezionato o in un gruppo di computer selezionato,
- domandare il numero della versione del pacchetto antivirus, nonché i dati di creazione e i numeri delle versioni dei database dei virus ad ogni computer protetto,
- aggiornare contenuti della directory di installazione centralizzata e della directory di aggiornamento,
- aggiornare i database dei virus e i file eseguibili dei pacchetti antivirus, nonché i file eseguibili dei componenti di rete antivirus sui computer protetti.

Raccolta delle informazioni sullo stato di rete antivirus

Il Server Dr.Web permette di raccogliere e di registrare nel log le informazioni circa il funzionamento dei pacchetti antivirus, trasmesse su di esso dal software sui computer protetti (dagli Agent Dr.Web, per maggiori informazioni v. sotto). Le informazioni vengono registrate nel log generale di eventi realizzato nel formato di database. In una rete di piccola dimensione (non più di 200-300 computer), il database interno può essere utilizzato per la registrazione dati nel log generale di eventi. Per reti grandi , è prevista la possibilità di utilizzare database esterni.

Il database incorporato può essere utilizzato se al Server sono connesse non più di 200-300 postazioni. Se lo permettono la configurazione dell'hardware del computer su cui è installato il Server Dr.Web e il carico di altri processi eseguiti su questo computer, è possibile connettere fino a 1000 postazioni.

Altrimenti, si deve utilizzare un database esterno.

Se viene utilizzato un database esterno e se al Server sono connesse più di 10000 postazioni, sono consigliabili i seguenti requisiti minimi:

- processore con velocità 3GHz,
- memoria operativa a partire dai 4 GB per il Server Dr.Web, a partire dai 8 GB per il server del database,
- SO della famiglia UNIX.

Devono essere raccolte e registrate nel log generale di eventi le seguenti informazioni:

- versione dei pacchetti antivirus su computer protetti,
- ora e data di installazione e di aggiornamento del software di postazione antivirus, nonché la versione del software,
- ora e data di aggiornamento dei database dei virus, nonché le sue versioni,
- versione dell'SO installato su computer protetti, tipo di processore, posizione delle directory di sistema dell'SO ecc.,
- configurazione e modalità di funzionamento dei pacchetti antivirus (utilizzo dei metodi euristici, lista dei tipi di file scansionati, azioni in caso di rilevamento di virus informatici ecc.),
- eventi dei virus: nome del virus informatico rilevato, data di rilevamento, azioni eseguite, il risultato di trattamento ecc.

Il Server Dr.Web avvisa l'amministratore della rete antivirus se si sono verificati degli eventi relativi al funzionamento della rete antivirus attraverso email o gli strumenti broadcast standard dei sistemi operativi Windows. La configurazione degli eventi che provocano l'invio degli avvisi e degli altri parametri di avviso è descritta in p. Configurazione degli avvisi.

Web server

Il Web server fa parte del Pannello di controllo della sicurezza Dr.Web e svolge le seguenti funzioni principali:

- autenticazione e autorizzazione di amministratori nel Pannello di controllo;
- automatizzazione del funzionamento delle pagine del Pannello di controllo;
- supporto di pagine dinamicamente generate del Pannello di controllo;
- supporto di connessi sicure HTTPS con i client.

4.1.1. Gestione del Server Dr.Web sotto SO Windows®

Interfaccia e gestione del Server Dr.Web

Server Dr.Web non ha interfaccia incorporata. Generalmente, Server Dr.Web viene gestito tramite il Pannello di controllo che funge da interfaccia esterna del Server.

Quando il Server viene installato, nel menu principale del SO Windows **Programmi** viene collocata la directory **Dr.Web Server** contenente i seguenti elementi di configurare e di gestione base del Server:

- La directory **Gestione del server** – contiene i comandi di avvio, di riavvio e di arresto del Server, nonché i comandi di configurazione di registrazione del log e gli altri comandi del Server descritti in dettaglio nel documento **Allegati**, p. H4. Server Dr.Web.
- La voce **Interfaccia web** – per aprire il Pannello di controllo e per connettersi al Server installato sul questo computer (sull'indirizzo http://localhost:9080).
- La voce **Documentazione** – per aprire la documentazione dell'amministratore in formato HTML.

La directory di installazione di Server Dr.Web ha la seguente struttura:

- `bin` – file eseguibili di Server Dr.Web.
- `etc` – file di configurazione principali dei componenti di rete antivirus.
- `Installer` – programma che permette di installare l'Antivirus sul computer protetto e chiave di cifratura pubblica (`drwcsd.pub`).
- `update-db` – script necessari per aggiornare la struttura dei database del Server.
- `var` – la directory contiene le sottodirectory:
  - `es-dl-cache` – pacchetti d'installazione personali degli utenti entro due settimane dopo la creazione;
  - `backup` – backup dei database e degli altri dati critici;
  - `extensions` – script di procedure personalizzate, ideati per automatizzare l'esecuzione di determinati task;
  - `repository` – directory di repository in cui vengono messi gli aggiornamenti attuali dei database dei virus, dei file di pacchetti antivirus e dei componenti di rete antivirus. La directory include sottodirectory per singoli componenti del software dentro cui si trovano sottodirectory per singoli SO. La directory deve essere scrivibile per l'utente sotto il cui account viene avviato il Server (di regola, è l'utente **LocalSystem**);
  - `templates` – moduli dei resoconti.
- `webmin` – elementi del Pannello di controllo della sicurezza Dr.Web: documentazione, icone, moduli.

I contenuti della directory di aggiornamento `\var\repository` vengono scaricati dal server di aggiornamento tramite il protocollo HTTP/HTTPS automaticamente, secondo il calendario impostato per il Server; inoltre l'amministratore della rete antivirus può mettere manualmente gli aggiornamenti in queste directory.

File di configurazione principali

File	Descrizione	Directory predefinita
`agent.key` (il nome può essere diverso)	chiave di licenza di Agent	`etc`
`certificate.pem`	certificato per SSL	
`download.conf`	impostazioni di rete per la generazione dei pacchetti d'installazione di Agent	
`drwcsd.conf` (il nome può essere diverso)	file di configurazione del Server	
`drwcsd.conf.distr`	template del file di configurazione di Server con i parametri di default	
`drwcsd.pri`	chiave di cifratura privata	
`enterprise.key` (il nome può essere diverso)	chiave di licenza di Server. Viene mantenuta soltanto se era presente dopo l'aggiornamento dalle versioni precedenti. Quando viene installato il nuovo Server 10, è assente	
`frontdoor.conf`	file di configurazione per l'utility di diagnostica remota di Server	
`http-alerter-certs.pem`	certificati per la verifica dell'host apple-notify.drweb.com in caso di invio delle notifiche push	
`private-key.pem`	chiave privata RSA	
`webmin.conf`	file di configurazione del Pannello di controllo	
`auth-ads.xml`	file di configurazione per l'autenticazione esterna degli amministratori attraverso Active Directory	
`auth-ldap.xml`	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP	
`auth-radius.xml`	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS	
`database.sqlite`	database incorporato	`var`
`drwcsd.pub`	chiave di cifratura pubblica	• `Installer` • `webmin\install`

Avvio e arresto del Server Dr.Web

Di default, Server Dr.Web viene avviato automaticamente dopo l'installazione e dopo ogni riavvio del sistema operativo.

Inoltre, si può avviare, riavviare o arrestare il Server Dr.Web in uno dei seguenti modi:

- Caso generale:
  - Tramite il comando corrispondente locato nel menu **Start** → **Programmi** → **Server Dr.Web**.
  - Tramite gli strumenti di gestione dei servizi nella sezione **Amministrazione** del **Pannello di controllo** del SO Windows.
- Arresto e riavvio tramite il Pannello di controllo:

  Nella sezione **Amministrazione**: riavvio con l'ausilio del pulsante  , arresto con l'ausilio del pulsante  .
- Tramite i comandi console eseguiti dalla sottocartella `bin` della cartella di installazione del Server (v. anche il documento **Allegati**, p. H4. Server Dr.Web):
  - `drwcsd start` – avvio del Server.
  - `drwcsd restart` – riavvio completo del servizio Server.
  - `drwcsd stop` – arresto normale del Server.

> Notare: affinché il Server legga le variabili di ambiente, è necessario riavviare il servizio tramite gli strumenti di gestione dei servizi o tramite il comando console.

4.1.2. Gestione del Server Dr.Web sotto SO della famiglia UNIX®

Interfaccia e gestione del Server Dr.Web

Server Dr.Web non ha interfaccia incorporata. Generalmente, Server Dr.Web viene gestito tramite il Pannello di controllo che funge da interfaccia esterna del Server.

La directory di installazione di Server Dr.Web ha la seguente struttura:

`/opt/drwcs/` in caso di OS Linux, OS Solaris e `/usr/local/drwcs` in caso di OS FreeBSD:

- `bin` – file eseguibili di Server Dr.Web.
- `doc` – file di contratti di licenza.
- `ds-modules`
- `fonts` – tipi di carattere per l'interfaccia del Pannello di controllo.
- `Installer` – installer di rete e chiave di cifratura pubblica per installare l'Antivirus su computer protetti.
- `lib` – set di librerie per il funzionamento del Server.

- `update-db` – script necessari per aggiornare la struttura dei database del Server.
- `webmin` – tutti gli elementi del Pannello di controllo della sicurezza Dr.Web.

`/var/opt/drwcs/` in caso di SO Linux, SO Solaris e `/var/drwcs` in caso di SO FreeBSD:

- `backup` – backup dei database e degli altri dati critici.
- `bases` – database dei virus decompressi per la compatibilità all'indietro con le versioni precedenti degli Agent Dr.Web.
- `coredump` – crash dump del Server.
- `database.sqlite` – database incorporato del Server.
- `etc` – file delle impostazioni principali dei componenti della rete antivirus.
- `extensions` – script personalizzati ideati per automatizzare l'esecuzione di determinati task.
- `installers-cache` – cache degli installer dell'Agent. Viene utilizzato per memorizzare pacchetti di installazione dell'Agent durante la creazione delle postazioni nel Pannello di controllo.
- `log` – file di log del Server.
- `object` – cache degli oggetti del Pannello di controllo.
- `reports` – directory temporanea utilizzata per generare e memorizzare resoconti.
- `repository` – directory di aggiornamenti in cui vengono messi gli aggiornamenti attuali dei database dei virus, dei file di pacchetti antivirus e dei componenti di rete antivirus. La directory include sottodirectory per singoli componenti del software dentro cui si trovano sottodirectory per singoli SO. La directory deve essere scrivibile per l'utente sotto il cui account viene avviato il Server (di regola, è l'utente **drwcs**).
- `run` – PID del processo del Server.
- `sessions` – sessioni del Pannello di controllo.
- `upload` – directory di caricamento dei file temporanei che vengono impostati tramite il Pannello di controllo (chiavi ecc.).

`/etc/opt/drweb.com/` per l'SO Linux (solo in caso di installazione tramite pacchetti generic `*.tar.gz.run`) e `/usr/local/etc/opt/` per l'SO FreeBSD:

- `software/drweb-esuite.remove` – script di rimozione del Server.
- + eventuali file e directory addizionali.

`/usr/local/etc/rc.d/` per l'SO FreeBSD:

- `drwcsd.sh` – script di avvio e arresto del Server.

`/var/tmp/drwcs` – backup dopo la rimozione del Server.

File di configurazione principali

File	Descrizione	Directory predefinita
`agent.key` (il nome può essere diverso)	chiave di licenza di Agent	• in caso di SO Linux e SO Solaris: `/var/opt/drwcs/etc` • in caso di SO FreeBSD: `/var/drwcs/etc`
`certificate.pem`	certificato per SSL	
`common.conf`	file di configurazione (per alcuni SO della famiglia UNIX)	
`download.conf`	impostazioni di rete per la generazione dei pacchetti d'installazione di Agent	
`drwcsd.conf` (il nome può essere diverso)	file di configurazione del Server	
`drwcsd.conf.distr`	template del file di configurazione di Server con i parametri di default	
`drwcsd.pri`	chiave di cifratura privata	
`enterprise.key` (il nome può essere diverso)	chiave di licenza di Server. Viene mantenuta soltanto se era presente dopo l'aggiornamento dalle versioni precedenti. Quando viene installato il nuovo Server 10, è assente	
`frontdoor.conf`	file di configurazione per l'utility di diagnostica remota di Server	
`http-alerter-certs.pem`	certificati per la verifica dell'host apple-notify.drweb.com in caso di invio delle notifiche push	
`private-key.pem`	chiave privata RSA	
`webmin.conf`	file di configurazione del Pannello di controllo	
`auth-ldap.xml`	file di configurazione per l'autenticazione esterna degli amministratori attraverso LDAP	
`auth-pam.xml`	file di configurazione per l'autenticazione esterna degli amministratori attraverso PAM	
`auth-radius.xml`	file di configurazione per l'autenticazione esterna degli amministratori attraverso RADIUS	
`database.sqlite`	database incorporato	• in caso di SO Linux e SO Solaris: `/var/opt/drwcs`

File	Descrizione	Directory predefinita
		• in caso di SO FreeBSD: `/var/drwcs`
`drwcsd.pub`	chiave di cifratura pubblica	• in caso di SO Linux e SO Solaris: `/opt/drwcs/Installer` `/opt/drwcs/webmin/install` • in caso di SO FreeBSD: `/usr/local/drwcs/Installer` `/usr/local/drwcs/webmin/install`

Avvio e arresto del Server Dr.Web

Di default, Server Dr.Web viene avviato automaticamente dopo l'installazione e dopo ogni riavvio del sistema operativo.

Inoltre, si può avviare, riavviare o arrestare il Server Dr.Web in uno dei seguenti modi:

- Arresto e riavvio tramite il Pannello di controllo:

  Nella sezione **Amministrazione**: riavvio con l'ausilio del pulsante  , arresto con l'ausilio del pulsante  (non è disponibile nella versione per l'SO Solaris).
- Tramite il relativo comando console (v. anche il documento Allegati, p. H4. Server Dr.Web):
  - Avvio:
    - in caso di SO FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh start
      ```
    - in caso di SO Linux e SO Solaris:
      ```
      # /etc/init.d/drwcsd start
      ```
  - Riavvio:
    - in caso di SO FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh restart
      ```
    - in caso di SO Linux e SO Solaris:
      ```
      # /etc/init.d/drwcsd restart
      ```
  - Arresto:
    - in caso di SO FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh stop
      ```
    - Per l'SO Linux e per l'SO Solaris:
      ```
      # /etc/init.d/drwcsd stop
      ```

Notare: affinché il Server legga le variabili di ambiente, è necessario riavviare il servizio tramite il comando console.

4.2. Protezione delle postazioni

Le impostazioni dei componenti antivirus, configurabili attraverso il Pannello di controllo, sono descritte dettagliatamente nel **Manuale dell'amministratore** per la gestione delle postazioni per il sistema operativo corrispondente.

Un computer protetto tramite un pacchetto antivirus installato, in conformità con le sue funzioni nella rete antivirus, viene denominato *postazione* della rete antivirus. Va ricordato che a seconda delle sue funzioni svolte nella rete locale tale computer può essere sia una postazione o un dispositivo mobile che un server della rete locale.

Le postazioni vengono protette tramite i pacchetti antivirus Dr.Web progettati per i sistemi operativi corrispondenti.

I pacchetti antivirus si installano su postazioni protette e si connettono a un Server Dr.Web. Ciascuna postazione fa parte di uno o più gruppi registrati su questo Server (per maggiori informazioni v. p. Gruppi di sistema e custom). Le informazioni vengono trasmesse tra la postazione e il Server attraverso il protocollo utilizzato nella rete locale (TCP/IP versione 4 o 6).

Installazione

Un pacchetto antivirus può essere installato su una postazione in uno dei seguenti modi:

1. Localmente. L'installazione locale viene eseguita direttamente sul computer o sul dispositivo mobile dell'utente. Può essere eseguita sia dall'amministratore che dall'utente.
2. Su remoto. L'installazione remota è disponibile soltanto per le postazioni SO Windows e viene eseguita nel Pannello di controllo attraverso la rete locale. Viene eseguita dall'amministratore della rete antivirus. L'intervento dell'utente in tale caso non è richiesto.

Le procedure di installazione dei pacchetti antivirus su postazioni vengono descritte nel dettaglio nella **Guida all'installazione**.

Gestione

Se la postazione è connessa con il Server Dr.Web, all'amministratore sono disponibili le seguenti funzioni realizzate dal pacchetto antivirus sulla postazione:

- Configurazione centralizzata di Antivirus sulle postazioni tramite il Pannello di controllo.

  L'amministratore può vietare all'utente o lasciargli la possibilità di modificare in autonomo le impostazioni di Antivirus sulla postazione.
- Configurazione del calendario di scansioni antivirus e di altri task eseguibili sulla postazione.
- Ottenimento delle statistiche di scansione e di altre informazioni sul funzionamento dei componenti antivirus e sullo stato della postazione.
- Avvio e arresto di una scansione antivirus ecc.

L'avvio remoto dello Scanner è possibile soltanto sulle postazioni SO Windows, SO della famiglia UNIX e OS X.

Aggiornamento

Server Dr.Web scarica gli aggiornamenti e li distribuisce sulle postazioni connesse. In questo modo l'ottimale strategia per la protezione dalle minacce viene stabilita, mantenuta e regolata automaticamente a prescindere dal livello di qualifica degli utenti delle postazioni.

Nel caso di una disconnessione provvisoria di una postazione dalla rete antivirus, Antivirus sulla postazione utilizza la copia locale delle configurazioni, la protezione antivirus sulla postazione rimane operativa (durante un periodo che non supera il periodo di validità della licenza di utente), ma il software non viene aggiornato. Se per la postazione è consentito il funzionamento in *Modalità mobile*, quando la postazione si disconnette dal Server, alla postazione sarà disponibile l'aggiornamento dei database dei virus direttamente dai server SAM.

Il principio di funzionamento delle postazioni in modalità mobile è descritto in p. Aggiornamento di Agent Dr.Web mobile.

4.3. Pannello di controllo della sicurezza Dr.Web

Per la gestione della rete antivirus in generale (compresa la modifica dei suoi contenuti e della sua struttura) e di tutti i suoi componenti, nonché per la configurazione di Server Dr.Web, si utilizza il Pannello di controllo della sicurezza Dr.Web.

Affinché il Pannello di controllo possa funzionare in maniera corretta nel web browser Windows Internet Explorer, è necessario aggiungere l'indirizzo del Pannello di controllo all'area attendibile nelle impostazioni del browser: **Servizio** → **Opzioni Internet** → **Sicurezza** → **Siti attendibili**.

Affinché il Pannello di controllo possa funzionare in maniera corretta nel web browser Chrome, è necessario attivare i cookies nelle impostazioni del browser.

Connessione al Server Dr.Web

Su qualunque computer che abbia una connessione di rete con il Server Dr.Web, il Pannello di controllo è disponibile sull'indirizzo:

`http://`<*Indirizzo_Server*>`:9080`

o

`https://`<*Indirizzo_Server*>`:9081`

dove come <*Indirizzo_Server*> indicare l'indirizzo IP o il nome a dominio del computer su cui è installato il Server Dr.Web.

> I numeri di porta sono diversi per le connessioni http e per le connessioni protette https: rispettivamente 9080 e 9081.

Nella finestra di dialogo di richiesta di autenticazione inserire il nome e la password dell'amministratore (il nome dell'amministratore con i permessi completi di default è **admin**, la password è la password che è stata impostata quando si installava il Server).

In caso di caricamento su HTTPS (connessione sicura SSL), il browser richiede una conferma del certificato utilizzato dal Server. La richiesta della conferma potrebbe essere accompagnata dalle supposizioni che il certificato sia inattendibile o invalido. Il browser visualizza queste informazioni perché il certificato è sconosciuto. Per caricare il Pannello di controllo è necessario accettare il certificato proposto. Altrimenti, il caricamento non sarà possibile.

> In alcune versioni dei browser, per esempio, in **FireFox 3** e superiori, in caso di connessione via https, viene restituito un errore, e il Pannello di controllo non viene caricato. In questo caso sulla pagina di errore si deve selezionare la voce **Aggiungi sito alla lista esclusioni** (sotto il messaggio di errore). Dopo questo, l'accesso al Pannello di controllo sarà consentito.

Interfaccia del Pannello di controllo della sicurezza Dr.Web

La finestra del Pannello di controllo (v. immagine 4-1) è suddivisa in *intestazione del menu principale* e in *area operativa*.

Area operativa

Tramite l'area operativa si può accedere alle funzionalità principali del Pannello di controllo. È costituita da due o tre pannelli, a seconda delle azioni che vengono eseguite. Le funzionalità dei pannelli sono nidificate da sinistra a destra:

- *menu di gestione* è sempre situato nella parte sinistra della finestra,
- a seconda della voce selezionata nel menu di gestione, vengono visualizzati uno o due pannelli supplementari. Nell'ultimo caso, nella parte destra vengono mostrate le proprietà o le impostazioni degli elementi visualizzati nel pannello centrale.

La lingua dell'interfaccia viene impostata separatamente per ciascun account amministratore (v. p. Gestione degli account amministratori).

Menu principale

Nel menu principale del Pannello di controllo sono disponibili le seguenti voci:

- sezione Amministrazione,
- sezione Rete antivirus,

- sezione Relazioni,
- Barra di ricerca,
- l'account amministratore sotto cui si è accessi al Pannello di controllo. Inoltre può essere disponibile il menu delle relazioni tra i server,
- sezione Eventi,
- sezione Impostazioni,
- sezione Guida,
- pulsante **Esci** per terminare la corrente sessione di lavoro con il Pannello di controllo.

Se nel Pannello di controllo è attiva l'autenticazione automatica, dopo che si è fatto clic sul pulsante **Esci**, le informazioni circa il nome e la password dell'amministratore vengono eliminate.

Quando si entrerà successivamente nel Pannello di controllo, si dovrà ripetere la procedura standard di autenticazione, indicando il nome e la password. In questo caso, se è attiva l'autenticazione automatica, il nome e la password indicati vengono salvati in questo browser, e l'autenticazione nel Pannello di controllo verrà eseguita automaticamente (senza inserire il nome e la password) fino a quando non si farà clic di nuovo sul pulsante **Esci**.

Immagine 4-1. Finestra del Pannello di controllo della sicurezza Dr.Web. Fare clic su una voce del menu principale per andare alla descrizione

Menu delle relazioni tra i server

Le informazioni relative all'organizzazione di una rete antivirus con diversi server e alla configurazione delle reazioni tra i server vengono riportate nella sezione Caratteristiche di una rete con diversi Server Dr.Web.

Se ci sono le relazioni del tipo "tra i server" con altri Server Dr.Web, le seguenti funzioni vengono aggiunte per il nome utente amministratore al menu principale:

- Accanto al nome amministratore viene visualizzato il nome del Server Dr.Web corrente.
- Quando si fa clic sul nome amministratore, si apre una lista a discesa dei Server interrelati. Se per una relazione non è impostato il nome, viene visualizzato l'identificatore.

  Quando si fa clic su una relazione, sono possibili due varianti delle azioni:

  - Si apre il Pannello di controllo del Server interrelato se nella configurazione della relazione si è indicato l'indirizzo IP del Pannello di controllo.
    L'azione è uguale a quella del pulsante nella barra degli strumenti nella sezione **Relazioni** del menu principale.
  - Se l'indirizzo del Pannello di controllo del Server adiacente non è impostato per questa relazione, si apre la configurazione della sezione **Relazioni** in modo che sia possibile impostare l'indirizzo IP.

4.3.1. Amministrazione

Dal menu principale del Pannello di controllo selezionare la voce **Amministrazione**. Per visualizzare e modificare le informazioni nella finestra che si è aperta, utilizzare il menu di gestione situato sul lato sinistro della finestra.

Il menu di gestione contiene le seguenti voci:

1. **Amministrazione**

   - **Server Dr.Web** – apre un pannello tramite cui è possibile visualizzare le informazioni principali su Server, nonché riavviarlo tramite il pulsante o arrestarlo tramite il pulsante (non disponibile nella versione per SO Solaris) locati nella parte superiore destra del pannello. Inoltre, se sono disponibili aggiornamenti scaricati di Server Dr.Web, da questa sezione è disponibile la sezione Aggiornamenti di Server Dr.Web con una lista delle versioni di Server per l'aggiornamento e il backup.
   - Gestione licenze – consente di gestire i file della chiave di licenza.
   - **Chiavi di crittografia** – consente di esportare (salvare localmente) le chiavi di crittografia pubblica e privata.

2. **Logs**

   - Log di verifica – consente di visualizzare la lista degli eventi e delle modifiche apportate tramite i sottosistemi di gestione di Dr.Web Enterprise Security Suite.
   - **Log di esecuzione dei task** – contiene l'elenco dei task impostati sul Server con l'annotazione di esecuzione e con commenti.
   - Log del Server Dr.Web – contiene l'elenco dei log di eventi relativi al funzionamento del Server.
   - Log di aggiornamento del repository – contiene un elenco di aggiornamenti da SAM che include informazioni dettagliate sulle revisioni aggiornate dei prodotti.

3. **Configurazione**

   - Amministratori – apre il pannello di gestione degli account amministratori di rete antivirus.
   - Autenticazione – apre il pannello di gestione dell'autenticazione degli amministratori nel Pannello di controllo.
   - Configurazione del Server Dr.Web – apre il pannello delle impostazioni principali del Server.
   - Accesso remoto al Server Dr.Web – contiene le impostazioni per la connessione dell'utility di diagnostica remota del Server.
   - Scheduler del Server Dr.Web – apre il pannello di configurazione del calendario dei task del Server.
   - Configurazione del web server – apre il pannello delle impostazioni principali del Web server.
   - Procedure personalizzate.

4. **Installazione**

   - Scanner di rete – permette di impostare una lista delle reti e scansionare le reti, cercando il software antivirus installato, determinando lo stato di protezione dei computer, nonché di installare il software antivirus.
   - **Installazione via rete** – permette di semplificare l'installazione del software Agent su concrete postazioni (v. **Guida all'installazione**, p. Installazione di Agent Dr.Web tramite il Pannello di controllo della sicurezza Dr.Web).

5. **Avvisi**

   - Notifiche nella console web – permette di visualizzare e gestire gli avvisi dell'amministratore ricevuti tramite il metodo **Web console**.
   - Notifiche non inviate – permette di tracciare e gestire gli avvisi all'amministratore che non sono stati inviati secondo le impostazioni della sezione **Configurazione degli avvisi**.
   - Configurazione delle notifiche – permette di configurare gli avvisi all'amministratore su eventi nella rete antivirus.

6. **Repository**

- Stato del repository – permette di controllare lo stato del repository: data di ultimo aggiornamento dei componenti del repository e il loro stato. E inoltre permette di aggiornare il repository da SAM.
- Aggiornamenti differiti – contiene una lista dei prodotti per cui gli aggiornamenti dei prodotti sono stati vietati temporaneamente nella sezione **Configurazione dettagliata del repository**.
- Configurazione generale del repository – apre la finestra di configurazione della connessione a SAM e dell'aggiornamento del repository per tutti i prodotti.
- Configurazione dettagliata del repository – consente di configurare le revisioni separatamente per ogni prodotto nel repository.
- Contenuti del repository – consente di visualizzare e gestire i contenuti correnti del repository a livello di directory e file del repository.

7. **Possibilità addizionali**

- Gestione del database – consente di fare la manutenzione diretta del database con cui interagisce Server Dr.Web.
- Statistiche del Server Dr.Web – contiene le statistiche del funzionamento di questo Server.
- **Console SQL** – dà la possibilità di eseguire query SQL al database utilizzato dal Server Dr.Web.
- **Console Lua** – dà la possibilità di eseguire script LUA, sia quelli digitati direttamente nella console che quelli caricati da file.

Con l'accesso alla console lua l'amministratore ottiene l'accesso a tutto il file system all'interno del directory di Server e ad alcuni comandi di sistema sul computer su cui Server è installato.

Per vietare l'accesso alla console lua, disattivare il permesso **Possibilità addizionali** per il relativo amministratore (v. p. Amministratori e gruppi di amministratori).

- **Utility** – apre una sezione per il caricamento delle utility supplementari per l'interazione con Dr.Web Enterprise Security Suite:
  - Loader di repository Dr.Web per il download dei prodotti Dr.Web Enterprise Security Suite da Sistema di aggiornamento mondiale. La versione grafica del Loader di repository Dr.Web è disponibile solo in SO Windows.
  - Utility di diagnostica remota del Server Dr.Web consente di connettersi al Server Dr.Web su remoto per effettuare la gestione base e visualizzare le statistiche di funzionamento. V. inoltre p. Accesso remoto al Server Dr.Web.
  - Pannello di controllo mobile Dr.Web per l'amministrazione di una rete antivirus costruita sulla base di Dr.Web Enterprise Security Suite. Può essere installato e avviato sui dispositivi mobili iOS e SO Android.

4.3.2. Rete antivirus

Nel menu principale del Pannello di controllo selezionare la voce **Rete antivirus**.

Menu di gestione

Per visualizzare e modificare le informazioni nella finestra che si è aperta, si utilizza il menu di gestione situato nella parte sinistra della finestra.

Il menu di gestione contiene le seguenti voci:

1. **Generali**
   - Grafici
   - Componenti in esecuzione
   - Componenti installati
   - Quarantena
   - Comparazione di hardware e software (in caso di selezione di un gruppo o di diverse postazioni)
   - **Sessioni degli utenti**
   - **Postazioni non attive**
   - Hardware e software (in caso di selezione di una postazione)
   - Proprietà
   - Regole di appartenenza al gruppo (in caso di selezione di un gruppo definito dall'utente)
2. Statistiche
3. **Configurazione**
   - Permessi
   - Scheduler
   - Componenti da installare
   - Limitazioni degli aggiornamenti
   - Lista dei componenti antivirus adatti per il sistema operativo della postazione selezionata o riportati per liste dei sistemi operativi in caso di selezione di un gruppo.

> Le impostazioni dei componenti antivirus, configurabili attraverso il Pannello di controllo, sono descritte dettagliatamente nel **Manuale dell'amministratore** per la gestione delle postazioni per il sistema operativo corrispondente.

Lista gerarchica della rete antivirus

Nella parte centrale della finestra si trova la lista gerarchica della rete antivirus. La lista gerarchica visualizza la struttura ad albero degli elementi della rete antivirus. I nodi di questa struttura sono i gruppi e le postazioni che ne fanno parte.

Si possono eseguire le seguenti azioni con gli elementi della lista:

- fare clic con il tasto sinistro del mouse sul nome di un gruppo o di una postazione per visualizzare il menu di gestione del rispettivo elemento (nella parte sinistra della finestra) o le informazioni riepilogative su postazione nella barra delle proprietà (nella parte destra della finestra);
- fare clic con il tasto sinistro del mouse sull'icona di un gruppo per mostrare o nascondere i contenuti del gruppo;
- fare clic con il tasto sinistro del mouse sull'icona di una postazione per andare alla sezione delle proprietà di questa postazione.

> Per selezionare più postazioni o gruppi dalla lista gerarchica, utilizzare il mouse tenendo premuti i tasti CTRL o MAIUSCOLO.

L'aspetto dell'icona di un elemento della lista dipende dal tipo o dallo stato di questo elemento (v. tabella 4-1).

Tabella 4-1. Icone degli elementi della lista gerarchica

Icona	Descrizione
Gruppi. Icone principali	
	Gruppi visualizzati sempre nella lista gerarchica.
	I gruppi non verranno visualizzati nella lista gerarchica se: • ai gruppi è stata applicata l'azione **Imposta la visibilità del gruppo** → **Nascondi se vuoto** e al momento i gruppi non includono postazioni, • ai gruppi è stata applicata l'azione **Imposta la visibilità del gruppo** → **Nascondi** e in un dato momento nella sezione **Impostazioni della vista albero** è deselezionato il flag **Mostra gruppi nascosti**.
Postazioni. Icone principali	
	Postazione disponibile con il software antivirus installato.
	Postazione non disponibile.
	Software antivirus su postazione è disinstallato.

Icona	Descrizione
	Stato della postazione in caso dell'installazione remota di Agent attraverso la rete. La postazione è in tale stato dal momento di un'installazione riuscita di Agent su questa postazione fino al momento della prima connessione della postazione al Server.
	Icone addizionali
	L'icona delle impostazioni individuali viene visualizzata sopra le icone principali delle postazioni e dei gruppi per cui le impostazioni individuali sono state definite (in caso dei gruppi anche quando il gruppo include postazioni con le impostazioni individuali). Per visualizzare l'icona, selezionare la voce **Impostazioni della vista albero** nella barra degli strumenti e spuntare il flag **Mostra l'icona di impostazioni personalizzate**. Per esempio, se le impostazioni individuali sono definite su una postazione con il software antivirus installato, che al momento è online, la sua icona avrà il seguente aspetto: .
	L'icona dell'errore di aggiornamento viene visualizzata accanto alle icone principali delle postazioni sulle quali alcuni errori si sono verificati durante l'aggiornamento del software antivirus. Per visualizzare l'icona, selezionare la voce **Impostazioni della vista albero** nella barra degli strumenti e spuntare il flag **Mostra l'icona di errore di aggiornamento**. Per esempio, se è occorso un errore di aggiornamento del software antivirus su una postazione che al momento è online, la sua icona avrà il seguente aspetto: .
	L'icona delle regole dell'appartenenza ai gruppi viene visualizzata accanto alle icone principali delle postazioni per le quali sono state stabilite le regole della sistemazione automatica delle postazioni. Per visualizzare l'icona, selezionare la voce **Impostazioni della vista albero** nella barra degli strumenti e spuntare il flag **Mostra l'icona di regole di appartenenza**. Per esempio, se per un gruppo visualizzato sempre nella lista gerarchica, sono state impostate le regole dell'appartenenza, la sua icona avrà il seguente aspetto: .

Gli elementi della lista gerarchica della rete antivirus vengono gestiti attraverso la barra degli strumenti.

Barra degli strumenti

La barra degli strumenti della lista gerarchica contiene i seguenti elementi:

Generali. Consente di gestire parametri generali della lista gerarchica. Selezionare la voce opportuna dalla lista a cascata:

Modifica. Apre la barra delle proprietà della postazione o del gruppo nella parte destra della finestra del Pannello di controllo.

Rimuovi gli oggetti selezionati. Consente di rimuovere oggetti della lista gerarchica. Per farlo, selezionare uno o più oggetti dalla lista e fare clic su **Rimuovi gli oggetti selezionati**.

Rimuovi le regole di appartenenza. Consente di rimuovere le regole della sistemazione automatica delle postazioni in gruppi.

Imposta questo gruppo come primario. Consente di impostare come primario un gruppo scelto nella lista gerarchica per tutte le postazioni che ne fanno parte.

Imposta il gruppo primario per le postazioni. Consente di impostare gruppo primario per le postazioni selezionate nella lista gerarchica. Se un gruppo è selezionato nella lista gerarchica, a tutte le postazioni che ne fanno parte, verrà assegnato il gruppo primario scelto.

Unisci le postazioni. Consente di unire le postazioni sotto un singolo account nella lista gerarchica. Si può utilizzare questa funzione quando la stessa postazione è stata registrata sotto diversi account.

Rimuovi le impostazioni personalizzate. Consente di rimuovere le impostazioni personalizzate dell'oggetto selezionato dalla lista. In tale caso, l'oggetto eredita le impostazioni del gruppo primario. Se un gruppo è selezionato nella lista gerarchica, anche le impostazioni di tutte le postazioni che ne fanno parte vengono rimosse.

Invia il messaggio alle postazioni. Consente di inviare un messaggio con qualsiasi contenuto agli utenti.

Resetta la password. Consente di cancellare la password utente di accesso alle impostazioni dei componenti antivirus sulle postazioni selezionate. L'opzione è disponibile soltanto per le postazioni SO Windows.

Riavvia la postazione. Consente di lanciare su remoto il processo di riavvio di una postazione.

Disinstalla Agent Dr.Web. Rimuove l'Agent e il software antivirus dalla postazione o da un gruppo di postazioni selezionate.

Installa Agent Dr.Web. Apre Scanner di rete per installare Agent sulle postazioni selezionate. Questa voce è attiva soltanto se vengono selezionate postazioni nuove approvate o postazioni su cui Agent è stato disinstallato in precedenza.

Recupera le postazioni rimosse. Consente di recuperare le postazioni rimosse in precedenza. Questa voce è attiva soltanto se postazioni vengono selezionate dal sottogruppo **Deleted** del gruppo **Status**.

Invia file di installazione. Consente di inviare i file di installazione per le postazioni selezionate dalla lista agli indirizzi di posta elettronica definiti nelle impostazioni di questa sezione.

Aggiungi una postazione o un gruppo. Consente di creare un nuovo elemento della rete antivirus. Per farlo, selezionare la voce opportuna dalla lista a cascata:

Crea una postazione. Consente di creare una nuova postazione (v. **Guida all'installazione**, p. Creazione di un nuovo account).

Crea gruppo. Consente di creare un nuovo gruppo di postazioni.

Esporta dati:

Salva in formato CSV – per registrare i dati generali delle postazioni selezionate della rete antivirus in un file in formato CSV.

Salva in formato HTML – per registrare i dati generali delle postazioni selezionate della rete antivirus in un file in formato HTML.

Salva in formato XML – per registrare i dati generali delle postazioni selezionate della rete antivirus in un file in formato XML.

Salva in formato PDF – per registrare i dati generali delle postazioni selezionate della rete antivirus in un file in formato PDF.

> Quando vengono selezionate le opzioni sopraelencate dalla sezione **Esporta dati**, verranno esportate le informazioni soltanto circa le postazioni selezionate e le postazioni che fanno parte dei gruppi selezionati.

Esporta la configurazione – per salvare in file la configurazione di un oggetto selezionato della rete antivirus. Per questa opzione verrà offerto di selezionare le sezioni di configurazione da salvare.

Importa la configurazione – per caricare da file la configurazione di un oggetto selezionato della rete antivirus. Per questa opzione verrà offerto di selezionare un file da cui verrà caricata la configurazione e inoltre le sezioni di configurazione da caricare.

Propaga la configurazione – per propagare la configurazione di un oggetto selezionato verso altri oggetti della rete antivirus. Per questa opzione verrà offerto di selezionare oggetti su cui verrà propagata la configurazione e inoltre le sezioni di configurazione da propagare.

Imposta la visibilità del gruppo. Consente di modificare i parametri di visualizzazione dei gruppi. Per farlo, selezionare un gruppo dalla lista gerarchica ed indicare nella lista a cascata una delle seguenti varianti (l'icona del gruppo cambierà, v. tabella 4-1):

Nascondi – significa che la visualizzazione del gruppo nella lista gerarchica è sempre disattivata.

Nascondi se vuoto – significa che la visualizzazione del gruppo nella lista gerarchica è disattivata se il gruppo è vuoto (non contiene postazioni).

Mostra – significa che il gruppo è sempre visualizzato nella lista gerarchica.

Gestione dei componenti. Consente di gestire i componenti antivirus sulle postazioni. Per farlo, selezionare dalla lista a cascata una delle seguenti varianti:

Aggiorna i componenti falliti. Comanda di sincronizzare forzatamente i componenti di cui l'aggiornamento non è riuscito.

Aggiorna tutti i componenti. Comanda di aggiornare tutti i componenti antivirus installati, per esempio se l'Agent non si connette al Server da molto tempo ecc. (v. p. Aggiornamento manuale dei componenti Dr.Web Enterprise Security Suite).

Interrompi i componenti in esecuzione. Comanda di fermare il funzionamento dei componenti antivirus in esecuzione sulla postazione.

Scansiona. Consente di eseguire la scansione sulla postazione in una delle modalità da selezionare dalla lista a cascata:

Scanner Dr.Web. Scansione rapida. In questa modalità Dr.Web Agent Scanner esegue la scansione dei seguenti oggetti:

- memoria operativa,

- settori di avvio di tutti i dischi,
- oggetti in esecuzione automatica,
- directory radice del disco di avvio,
- directory radice del disco di installazione di SO Windows,
- directory di sistema di SO Windows,
- cartella `Documenti`,
- directory temporanea di sistema,
- directory temporanea dell'utente.

 **Scanner Dr.Web. Scansione completa**. In questa modalità Dr.Web Agent Scanner esegue la scansione completa di tutti i dischi rigidi e supporti rimovibili (inclusi i settori di avvio).

 **Scanner Dr.Web. Scansione personalizzata**. In questa modalità è possibile selezionare cartelle e file per la successiva scansione tramite Dr.Web Agent Scanner.

 **Postazioni non confermate**. Consente di gestire la lista dei nuovi arrivi – postazioni la cui registrazione non è stata ancora confermata (per maggiori informazioni consultare la sezione Criteri di approvazione delle postazioni). Questa voce è attiva soltanto se le postazioni vengono selezionate dal sottogruppo **Newbies** del gruppo **Status**. Quando la registrazione verrà confermata o l'accesso a Server verrà negato, le postazioni verranno cancellate automaticamente dal sottogruppo predefinito **Newbies**. Per gestire i nuovi arrivi, selezionare dalla lista a cascata una delle seguenti varianti:

 **Consenti alle postazioni selezionate di accedere e imposta gruppo primario**. Comanda di confermare l'accesso al Server per la postazione e di assegnarle un gruppo primario dall'elenco proposto.

 **Annulla l'azione da eseguire al momento di connessione**. Comanda di annullare l'azione che deve essere eseguita con una postazione non confermata e che è stata impostata in precedenza per essere eseguita al momento della connessione della postazione al Server.

 **Proibisci alle postazioni selezionate di accedere**. Comanda di negare alla postazione l'accesso al Server.

 **Impostazioni della vista albero**. Permettono di modificare l'aspetto dell'albero della rete antivirus. Per attivare il parametro, impostare i flag corrispondenti nel menu a discesa:

- per i gruppi:
  - **Appartenenza a tutti i gruppi** – per duplicare la visualizzazione della postazione nella lista se fa parte contemporaneamente di diversi gruppi (soltanto per i gruppi con l'icona di cartella bianca – v. tabella 4-1). Se il flag è selezionato, la postazione viene visualizzata in tutti i gruppi di cui fa parte. Se il flag è deselezionato, la postazione viene visualizzata nella lista una volta.
  - **Mostra gruppi nascosti** – per visualizzare tutti i gruppi inclusi nella rete antivirus. Se questo flag viene tolto, i gruppi vuoti (che non contengono postazioni) saranno nascosti. Questo può essere utile per escludere le informazioni eccessive, per esempio se ci sono tanti gruppi vuoti.
- per le postazioni:

- **Mostra identificatori delle postazioni** – per visualizzare gli identificatori unici delle postazioni nella lista gerarchica.
- **Mostra nomi delle postazioni** – per visualizzare i nomi delle postazioni.

> Non è possibile disattivare contemporaneamente la visualizzazione degli identificatori e dei nomi delle postazioni. Uno dei parametri **Mostra identificatori delle postazioni** e **Mostra nomi delle postazioni** sarà sempre selezionato.

- **Mostra indirizzi delle postazioni** – per visualizzare gli indirizzi IP delle postazioni nella lista gerarchica.
- **Mostra i server delle postazioni** – per visualizzare i nomi o gli indirizzi IP dei Server antivirus a cui sono connesse le postazioni.
- **Mostra l'icona di errore di aggiornamento** – per visualizzare un indicatore sulle icone delle postazioni su cui l'ultimo aggiornamento non è riuscito.

- per tutti gli elementi:
  - **Mostra l'icona di impostazioni personalizzate** – per visualizzare sulle icone delle postazioni e dei gruppi un indicatore che segnala la presenza delle impostazioni individuali.
  - **Mostra descrizioni** – per visualizzare le descrizioni dei gruppi e delle postazioni (le descrizioni vengono impostate nelle proprietà di un elemento).
  - **Mostra il numero di postazioni** – per visualizzare il numero di postazioni per tutti i gruppi della rete antivirus.
  - **Mostra l'icona di regole di appartenenza** – per visualizzare un indicatore sulle icone delle postazioni che sono state aggiunte a un gruppo in modo automatico secondo le regole di appartenenza, nonché sulle icone dei gruppi a cui le postazioni sono state aggiunte in modo automatico.

Impostazioni di ordinamento delle postazioni. Permettono di modificare il parametro in base a cui vengono ordinate le postazioni e di metterle in ordine crescente o decrescente nell'albero della rete antivirus.

- Per selezionare il parametro in base a cui verranno ordinate le postazioni, impostare uno dei seguenti flag (è possibile selezionare solo un parametro):
  - **Identificatore** – per ordinare in base agli identificatori unici delle postazioni.
  - **Nome** – per ordinare in base ai nomi delle postazioni.
  - **Indirizzo** – per ordinare in base agli indirizzi di rete delle postazioni. Le postazioni che non hanno un indirizzo di rete verranno visualizzate in ordine casuale senza essere ordinate.
  - **Data di creazione** – per ordinare in base alla data di creazione dell'account di postazione sul Server.
- Per selezionare la direzione di ordinamento, impostare uno dei seguenti flag:
  - **Ordina crescente**.
  - **Ordina decrescente**.

Le sezioni **Impostazioni della vista albero** e **Impostazioni di ordinamento delle postazioni** sono interdipendenti:

- Se viene selezionato un parametro di ordinamento nella sezione **Impostazioni di ordinamento delle postazioni**, la visualizzazione di questo parametro viene attivata automaticamente nella sezione **Impostazioni della vista albero**, se era disattivata.
- Se nella sezione **Impostazioni della vista albero** viene disattivata la visualizzazione del parametro di ordinamento selezionato nella sezione **Impostazioni di ordinamento delle postazioni**, l'ordinamento in base a questo parametro cambia automaticamente nell'ordinamento in base ai nomi delle postazioni. Se in questo caso la visualizzazione dei nomi delle postazioni è disattivata, l'ordinamento cambia in quello per identificatore delle postazioni (non possono essere disattivati contemporaneamente il nome e l'identificatore).

Barra delle proprietà

La barra delle proprietà serve a visualizzare le proprietà e le impostazioni delle postazioni e dei gruppi.

Per visualizzare la barra delle proprietà:

1. Nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
2. Nella parte destra della finestra del Pannello di controllo si apre la barra contenente le proprietà del gruppo o della postazione selezionata. Queste impostazioni sono descritte in modo dettagliata in p. Modifica dei gruppi e Proprietà della postazione.

4.3.3. Relazioni

Nel menu principale del Pannello di controllo selezionare la voce **Relazioni**. Per scegliere le informazioni da visualizzare, utilizzare il menu di gestione situato nella parte sinistra della finestra.

Amministrazione

La sezione **Amministrazione** del menu di gestione contiene la voce **Relazioni** che si utilizza per gestire le relazioni tra i Server in una rete antivirus con diversi server (v. p. Caratteristiche di una rete con diversi Server Dr.Web).

Nella lista gerarchica sono riportati tutti i Server Dr.Web connessi con questo Server.

La creazione delle nuove relazioni tra i server è descritta nella sezione Configurazione delle relazioni tra i Server Dr.Web.

Tabelle

Nella sezione **Tabelle** del menu di gestione sono riportate le informazioni su funzionamento della rete antivirus, ricevute da altri Server (v. p. Caratteristiche di una rete con diversi Server Dr.Web).

Per visualizzare le tabelle riassuntive contenenti dati degli altri Server, fare clic sulla voce corrispondente della sezione **Tabelle**.

4.3.4. Barra di ricerca

Per semplificare la ricerca di un elemento richiesto, si utilizza la *barra di ricerca* locata sul bordo destro del menu principale del Pannello di controllo. La barra permette di cercare sia gruppi che singole postazioni sulla base dei parametri indicati.

Per cercare postazioni o gruppi di postazioni:

1. Nella lista a cascata della barra di ricerca, scegliere il criterio di ricerca:
   - **Postazione** – per cercare postazioni per nome,
   - **Gruppo** – per cercare gruppi per nome,
   - **ID** – per cercare gruppi e postazioni per identificatore unico,
   - **Descrizione** – per cercare gruppi e postazioni per descrizione,
   - **Nome utente** – per cercare postazioni per nome utente sulla postazione,
   - **Indirizzo IP** – per cercare postazioni per indirizzo IP,
   - **Hardware** – per cercare postazioni per nome o categoria dell'hardware della postazione,
   - **Programma** – per cercare postazioni per nome del software installato su postazione.
2. Inserire una stringa sulla base della quale verrà eseguita la ricerca. Si può utilizzare:
   - una stringa specifica per la completa corrispondenza con il parametro di ricerca,
   - una maschera della stringa di ricerca: sono consentiti i caratteri `*` e `?`.
3. Premere il tasto INVIO per far partire la ricerca. Si apre la barra di ricerca avanzata e l'albero della rete antivirus.
4. Nell'albero della rete antivirus saranno visualizzati tutti gli elementi trovati secondo i parametri di ricerca, in particolare:
   - se si è cercata una postazione, sarà visualizzata l'appartenenza della postazione a tutti i gruppi di cui fa parte,
   - se nessun elemento è stato trovato nel corso della ricerca, sarà visualizzata una lista gerarchica vuota con il messaggio **Nessun risultato della ricerca**.

4.3.5. Eventi

Per avvisare l'amministratore di eventi che richiedono attenzione, si usa la sezione visualizzata nel menu principale tramite l'icona **Eventi**.

L'icona può essere nei seguenti stati:

– non ci sono avvisi di eventi nella rete.

– ci sono nuovi avvisi di eventi minori.

– ci sono nuovi avvisi di eventi importanti che richiedono l'intervento dell'amministratore.

Per la lista degli eventi sono possibili le seguenti azioni:

1. Con un clic sull'icona si apre una lista a discesa degli eventi della rete antivirus. L'icona cambia automaticamente in .
2. Quando si fa clic sulla riga dell'avviso di un evento, si passa alla sezione del Pannello di controllo responsabile delle funzionalità corrispondenti.
3. La costola di ogni avviso nella lista degli avvisi è contrassegnata da un colore che corrisponde all'importanza dell'evento (nello stesso modo dell'icona). Quando si passa alla sezione responsabile delle funzionalità dell'avviso, l'avviso viene considerato come letto e la costola cambia colore al grigio.

Tabella 4-2. La lista dei possibili avvisi di eventi della rete antivirus

Evento	Importanza	Sezione del Pannello di controllo	Descrizione
Installa l'estensione di browser per il Pannello di controllo della sicurezza Dr.Web	minore	La pagina di download dell'estensione del Pannello di controllo della sicurezza Dr.Web	È necessario installare l'estensione del Pannello di controllo della sicurezza Dr.Web.
Notizie non lette	minore	**Guida → Notizie**	Sono disponibili notizie della società Doctor Web non lette.
Nuovi avvisi	minore	**Amministrazione → Notifiche della web console**	Sono disponibili nuovi avvisi dell'amministratore ricevuti tramite **Web console**.
Avvisi critici	importante		
Sono disponibili aggiornamenti del Server	importante	**Amministrazione → Server Dr.Web**	L'aggiornamento del Server Dr.Web è stato caricato nel repository ed è disponibile per l'installazione.
La configurazione del Server è stata modificata. È necessario riavviare il Server.	importante	**Amministrazione → Configurazione del Server Dr.Web**	Le impostazioni del file di configurazione del Server sono state modificate dopo l'avvio del Server. È ne-

Evento	Importanza	Sezione del Pannello di controllo	Descrizione
			cessario riavviare il Server per accettare le nuove impostazioni.
La configurazione del web server è stata modificata. È necessario riavviare il Server.	importante	**Amministrazione → Configurazione del web server**	Le impostazioni del file di configurazione del web server sono state modificate dopo l'avvio del Server. È necessario riavviare il Server per accettare le nuove impostazioni.

4.3.6. Impostazioni

Per passare alla sezione delle impostazioni del Pannello di controllo, nel menu principale fare clic sul pulsante **Impostazioni**.

> Tutte le impostazioni di questa sezione sono valide solo per l'account amministratore corrente.

Il menu di gestione locato nella parte sinistra della finestra contiene i seguenti elementi:

- **Il mio account**.
- **Interfaccia**.
- **Abbonamento**.

Il mio account

Tramite questa sezione viene gestito l'account amministratore della rete antivirus corrente (v. anche Amministratori e gruppi di amministratori).

Generali

> I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

Se necessario, modificare i seguenti parametri:

- **Nome utente** dell'amministratore – login per accedere al Pannello di controllo.
- Nome e cognome dell'amministratore.
- **Lingua dell'interfaccia** utilizzata da questo amministratore.
- **Formato della data** utilizzato da questo amministratore nella modifica delle impostazioni contenenti una data. Sono disponibili i seguenti formati:
  - europeo: `DD-MM-YYYY HH:MM:SS`

  - americano: `MM/DD/YYYY HH:MM:SS`
- **Descrizione** dell'account.
- Per cambiare la password, premere il pulsante **Cambia password** nella barra degli strumenti.

I seguenti parametri sono di sola lettura:

- Data della creazione account e dell'ultima modifica parametri,
- **Ultimo indirizzo** – visualizza l'indirizzo di rete dell'ultima connessione sotto questo account.

Permessi

I permessi amministratore e la modifica degli stessi sono descritti nella sezione Modifica degli amministratori.

Dopo aver modificato i parametri, fare clic sul pulsante **Salva**.

Interfaccia

Impostazioni della vista albero

I parametri di questa sottosezione permettono di modificare l'aspetto della lista e sono simili alle impostazioni locate nella barra degli strumenti della voce **Impostazioni della vista albero** nella sezione del menu principale **Rete antivirus**:

- per i gruppi:
  - **Appartenenza a tutti i gruppi** – per duplicare la visualizzazione della postazione nella lista se fa parte contemporaneamente di diversi gruppi (soltanto per i gruppi con l'icona di cartella bianca – v. tabella 4-1). Se il flag è selezionato, la postazione viene visualizzata in tutti i gruppi di cui fa parte. Se il flag è deselezionato, la postazione viene visualizzata nella lista una volta.
  - **Mostra gruppi nascosti** – per visualizzare tutti i gruppi inclusi nella rete antivirus. Se questo flag viene tolto, i gruppi vuoti (che non contengono postazioni) saranno nascosti. Questo può essere utile per escludere le informazioni eccessive, per esempio se ci sono tanti gruppi vuoti.
- per le postazioni:
  - **Mostra identificatori delle postazioni** – per visualizzare gli identificatori unici delle postazioni nella lista gerarchica.
  - **Mostra nomi delle postazioni** – per visualizzare i nomi delle postazioni.

> Non è possibile disattivare contemporaneamente la visualizzazione degli identificatori e dei nomi delle postazioni. Uno dei parametri **Mostra identificatori delle postazioni** e **Mostra nomi delle postazioni** sarà sempre selezionato.

- **Mostra indirizzi delle postazioni** – per visualizzare gli indirizzi IP delle postazioni nella lista gerarchica.
- **Mostra i server delle postazioni** – per visualizzare i nomi o gli indirizzi IP dei Server antivirus a cui sono connesse le postazioni.
- **Mostra l'icona di errore di aggiornamento** – per visualizzare un indicatore sulle icone delle postazioni su cui l'ultimo aggiornamento non è riuscito.

- per tutti gli elementi:
  - **Mostra l'icona di impostazioni personalizzate** – per visualizzare sulle icone delle postazioni e dei gruppi un indicatore che segnala la presenza delle impostazioni individuali.
  - **Mostra descrizioni** – per visualizzare le descrizioni dei gruppi e delle postazioni (le descrizioni vengono impostate nelle proprietà di un elemento).
  - **Mostra il numero di postazioni** – per visualizzare il numero di postazioni per tutti i gruppi della rete antivirus.
  - **Mostra l'icona di regole di appartenenza** – per visualizzare un indicatore sulle icone delle postazioni che sono state aggiunte a un gruppo in modo automatico secondo le regole di appartenenza, nonché sulle icone dei gruppi a cui le postazioni sono state aggiunte in modo automatico.

Scanner di rete

Per il funzionamento di Scanner di rete è necessario che sia installata l'estensione del Pannello di controllo della sicurezza Dr.Web.

I parametri di questa sottosezione permettono di definire le impostazioni di default dello Scanner di rete.

Per avviare lo Scanner di rete, nel menu principale del Pannello di controllo selezionare la voce **Amministrazione**, nel menu di gestione selezionare la voce **Scanner di rete**.

Impostare i seguenti parametri dello Scanner di rete:

1. Nel campo di input **Reti** impostare una lista delle reti nel formato:
   - separati da trattino (per esempio, `10.4.0.1-10.4.0.10`),
   - separati da virgola e spazio (per esempio, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`),
   - con il prefisso di rete (per esempio, `10.4.0.0/24`).
2. Se necessario, modificare la **Porta** e il valore del parametro **Timeout (s)**.
3. Per salvare i valori di default, fare clic sul pulsante **Salva**. In seguito, quando verrà utilizzato Scanner di rete, questi parametri verranno impostati automaticamente.

Intervallo di tempo

In questa sottosezione viene configurato l'intervallo di tempo entro cui vengono visualizzati i dati statistici (v. p. Visualizzazione delle statistiche della postazione):

- Nella lista a cascata **Intervallo predefinito per la visualizzazione delle statistiche** viene impostato l'intervallo di tempo predefinito per tutte le sezioni dei dati statistici.

  Alla prima apertura della pagina, le statistiche verranno visualizzate per l'intervallo di tempo indicato. Se necessario, si può modificare l'intervallo di tempo direttamente nelle sezioni delle statistiche.
- Affinché nelle sezioni delle statistiche venga salvato l'ultimo intervallo impostato, mettere il flag **Salva l'ultimo intervallo di visualizzazione delle statistiche**.

  Se il flag è selezionato, alla prima apertura della pagina, verranno visualizzate le statistiche per l'ultimo periodo scelto nel browser.

  Se il flag è deselezionato, alla prima apertura della pagina, verranno visualizzate le statistiche per il periodo impostato nella lista **Intervallo predefinito per la visualizzazione delle statistiche**.

Autenticazione

Spuntare il flag **Autenticazione automatica** per consentire nel browser corrente l'autenticazione automatica in tutti i Pannelli di controllo Dr.Web con questi nome utente e password amministratore.

Dopo che il flag è stato selezionato, verranno salvati tramite l'estensione del Pannello di controllo della sicurezza Dr.Web il nome utente e la password che l'amministratore indica durante l'autenticazione successiva nel Pannello di controllo.

Per il funzionamento dell'autenticazione automatica è necessario che sia installata l'estensione del Pannello di controllo della sicurezza Dr.Web.

In seguito, se si apre un Pannello di controllo della sicurezza Dr.Web in questo browser, l'autenticazione verrà eseguita automaticamente se sul Server è disponibile un utente con questi nome utente e password. Se il nome utente e la password non corrispondono (per esempio, tale utente non esiste o l'utente con questo nome ha un'altra password), si aprirà la finestra standard di autenticazione del Pannello di controllo.

Se si fa clic sul pulsante **Esci** nel menu principale dell'interfaccia del Pannello di controllo, vengono eliminate le informazioni su nome utente e password dell'amministratore.

Quando si accederà successivamente al Pannello di controllo, si dovrà ripetere la procedura standard di autenticazione, indicando il nome utente e la password. Se è attivata l'autenticazione automatica, le credenziali indicate vengono memorizzate in questo browser, e l'autenticazione nel Pannello di controllo verrà eseguita automaticamente (senza dover inserire il nome utente e la password) fino allo successivo clic sul pulsante **Esci**.

Dalla lista a cascata **Durata della sessione** selezionare un periodo dopo cui una sessione di utilizzo del Pannello di controllo nel browser si interrompe automaticamente.

Esportazione in PDF

In questa sottosezione viene configurato il testo utilizzato nell'esportazione dei dati statistici in formato PDF:

- Dalla lista a cascata **Tipo carattere dei report**, si può selezionare il tipo di carattere da utilizzare nell'esportazione dei report in formato PDF.
- Nel campo **Dimensione carattere dei report** si può impostare la dimensione dei caratteri del testo principale delle tabelle statistiche da utilizzare nell'esportazione dei report in formato PDF.

Report

In questa sottosezione si configura la visualizzazione delle statistiche nella sezione **Report** del Pannello di controllo:

- Nel campo **Numero di righe per pagina** viene impostato il numero massimo di righe su una pagina del report per la visualizzazione delle statistiche divisa in pagine.
- Spuntare il flag **Mostra grafici** per visualizzare diagrammi sulle pagine dei report statistici. Se il flag è tolto, la visualizzazione dei grafici è disattivata.

Abbonamento

In questa sottosezione si configura l'abbonamento alle notizie della società Doctor Web.

Spuntare il flag **Abbonamento automatico alle nuove sezioni** per attivare l'aggiunzione automatica di nuove sezioni alla sezione di notizie nel Pannello di controllo.

4.3.7. Guida

Per passare alla sezione guida del Pannello di controllo, nel menu principale fare clic sul pulsante **Guida**.

Il menu di gestione locato nella parte sinistra della finestra contiene i seguenti elementi:

1. **Generali**
   - **Forum** – per passare al forum della società Doctor Web.
   - **Notizie** – per passare alla pagina delle notizie della società Doctor Web.
   - **Contatta il servizio di supporto tecnico** – per passare alla pagina del supporto tecnico Doctor Web.
   - **Spedisci un file sospetto** – per aprire il modulo di invio di un virus al laboratorio Doctor Web.

- **Wikipedia Doctor Web** – per passare alla pagina di Wikipedia – un database delle informazioni dedicate ai prodotti della società Doctor Web.
- **Segnala un falso positivo di Office control** – per aprire un formulario tramite il quale si può inviare un messaggio di un falso positivo o di un mancato riconoscimento dei link malevoli da parte del modulo Office control.

2. **Documentazione dell'amministratore**
   - **Manuale dell'amministratore** – per aprire il manuale dell'amministratore in formato HTML.
   - **Guida all'installazione** – per aprire la guida all'installazione di Dr.Web Enterprise Security Suite in formato HTML.
   - **Istruzioni per l'installazione di una rete antivirus** – per aprire le brevi istruzioni per l'installazione di una rete antivirus in formato HTML. Si raccomanda di leggere queste istruzioni prima di dispiegare una rete antivirus, di installare e configurare componenti.
   - **Allegati** – per aprire gli allegati al manuale dell'amministratore in formato HTML.
   - **Guida a Web API** – per aprire la documentazione dell'amministratore su Web API (v. inoltre il documento **Allegati**, p. Allegato L. Integrazione di Web API e di Dr.Web Enterprise Security Suite) in formato HTML.
   - **Note di release** – per aprire la sezione dei commenti al rilascio di Dr.Web Enterprise Security Suite per la versione installata.
3. **Documentazione dell'utente** – per aprire la documentazione dell'utente in formato HTML per il sistema operativo corrispondente, riportato nell'elenco.

4.4. Componenti del Pannello di controllo della sicurezza Dr.Web

4.4.1. Scanner di rete

Una parte di Server Dr.Web è Scanner di rete.

Non si consiglia di avviare Scanner di rete sotto SO Windows 2000 e inferiori: la panoramica della rete può essere incompleta.

Il funzionamento di Scanner di rete è garantito sotto SO della famiglia UNIX o sotto SO Windows XP e superiori.

Per il funzionamento di Scanner di rete è necessario che sia installata l'estensione del Pannello di controllo della sicurezza Dr.Web.

Affinché Scanner di rete possa funzionare in maniera corretta nel web browser Windows Internet Explorer, è necessario aggiungere l'indirizzo del Pannello di controllo, in cui viene avviato Scanner di rete, all'area attendibile nelle impostazioni del browser: **Servizio** → **Opzioni Internet** → **Sicurezza** → **Siti attendibili**.

Scanner di rete svolge le seguenti funzioni:

- Scansione (visualizzazione) della rete per rilevare postazioni.
- Determina la disponibilità di Agent Dr.Web su postazioni.
- Installazione di Agent Dr.Web su postazioni rilevate su comando dell'amministratore. L'installazione di Agent Dr.Web è descritta dettagliatamente nella **Guida all'installazione**, p. Installazione di Agent Dr.Web tramite il Pannello di controllo della sicurezza Dr.Web.

Per scansionare (visualizzare) la rete, eseguire le seguenti azioni:

1. Aprire la finestra di Scanner di rete. Per farlo, selezionare la voce **Amministrazione** del menu principale del Pannello di controllo, nella finestra che si è aperta, selezionare la voce del menu di gestione **Scanner di rete**. Si apre la finestra di Scanner di rete.
2. Spuntare il flag **Ricerca per indirizzo IP** per cercare postazioni nella rete a seconda degli indirizzi IP impostati. Nel campo **Reti** specificare una lista delle reti nel formato:
   - separati da trattino (per esempio, `10.4.0.1-10.4.0.10`),
   - separati da virgola e spazio (per esempio, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`),
   - con il prefisso di rete (per esempio, `10.4.0.0/24`).
3. In caso di SO Windows: spuntare il flag **Cerca le postazioni nel dominio di Active Directory** per cercare le postazioni nel dominio di Active Directory. Inoltre, impostare i seguenti parametri:
   - **Domini** – lista dei domini in cui verranno cercate le postazioni. Utilizzare una virgola come separatore per diversi domini.
   - **Controller di Active Directory** – controller di Active Directory, ad esempio, dc.example.com.

   > ⚠ Per cercare postazioni in un dominio di Active Directory per mezzo di Scanner di rete, è necessario che il web browser, in cui è aperto il Pannello di controllo, sia avviato da un utente di dominio con i permessi di ricerca di oggetti in Active Directory.

4. In caso di SO della famiglia UNIX: spuntare il flag **Ricerca LDAP** per cercare le postazioni attraverso LDAP. Inoltre, impostare i seguenti parametri:
   - **Domini** – lista dei domini in cui verranno cercate le postazioni. Utilizzare una virgola come separatore per diversi domini.
   - **Server LDAP** – server LDAP, ad esempio, ldap://ldap.example.com.
   - **Nome utente** – nome dell'utente di LDAP.
   - **Password** – password dell'utente di LDAP.
5. Nel campo **Porta** indicare il numero di porta per la connessione attraverso il protocollo UDP agli Agent durante una ricerca.
6. Se necessario, nel campo **Time-out (s)** modificare il valore di timeout in secondi per l'attesa di una risposta dalle postazioni.

7. Spuntare il flag **Mostra il nome della postazione** per visualizzare non soltanto l'indirizzo IP dei computer trovati nella rete, ma anche il nome a dominio.

   Se una postazione non è registrata sul server DNS, viene visualizzato solo il suo indirizzo IP.

8. Spuntare il flag **Correla con la lista di postazioni dal database** per attivare la sincronizzazione dei risultati della ricerca di Scanner di rete con la lista di postazioni salvata nel database del Server. Se il flag è spuntato, nella lista delle postazioni trovate nella rete verranno visualizzate anche quelle postazioni che sono presenti nel database del Server, ma non sono state rilevate da Scanner di rete nel corso della ricerca corrente, per esempio se su queste postazioni è installato un firewall che blocca la trasmissione di pacchetti per la connessione TCP.

   Quando i risultati della ricerca fatta da Scanner di rete vengono sincronizzati con le informazioni dal database del Server, la priorità è data alle informazioni dal database del Server. Cioè, se lo status di postazione rilevato nel corso della ricerca non corrisponde a quello registrato nel database, verrà assegnato lo status registrato nel database.

9. Fare clic sul pulsante **Scansiona**. A questo punto inizia la scansione della rete.

10. Durante la scansione di rete nella finestra viene caricata una directory (lista gerarchica) dei computer con l'indicazione della disponibilità degli Agent Dr.Web.

    Espandere gli elementi della directory corrispondenti ai gruppi di lavoro (domini). Tutti gli elementi della directory, corrispondenti ai gruppi di lavoro e a singole postazioni, sono contrassegnati da varie icone, il cui significato è riportato di seguito.

Tabella 4-3. Possibili tipi di icone

Icona	Descrizione
Gruppi di lavoro	
	Gruppi di lavoro che, tra gli altri computer, comprendono computer su cui si può installare Dr.Web Enterprise Security Suite.
	Altri gruppi che comprendono computer con il software antivirus installato o computer non disponibili via rete.
Postazioni	
	La postazione trovata è registrata nel database ed è attiva (postazioni attive con il software antivirus installato).
	La postazione trovata è registrata nel database nella tabella di postazioni eliminate.
	La postazione trovata non è registrata nel database (sul computer non è installato il software antivirus).
	La postazione trovata non è registrata nel database (la postazione è connessa a un altro Server).
	La postazione trovata è registrata nel database, non è attiva, e la porta è chiusa.

Si possono espandere inoltre gli elementi della directory corrispondenti alle postazioni con le icone  o  per visualizzare una lista dei componenti installati.

Interazione con gli Agent Dr.Web

Lo strumento **Scanner di rete** fa parte di Dr.Web Enterprise Security Suite a partire dalla versione 4.44.

Scanner di rete può rilevare su una postazione la disponibilità dell'Agent soltanto delle versioni 4.44 e superiori, ma non può interagire con gli Agent delle versioni precedenti.

Un Agent versioni 4.44 e superiori, installato su una postazione, processa le richieste di Scanner di rete arrivate su una determinata porta. Di default, si usa la porta `udp/2193`, però, per assicurare la compatibilità con il software delle versioni precedenti, è supportata anche la porta `udp/2372`. Di conseguenza, anche Scanner di rete usa di default queste porte. Scanner di rete conclude che l'Agent è disponibile o non disponibile su una postazione, basandosi sulla possibilità di scambiarsi informazioni (richiesta-risposta) sulla porta sopraccitata.

Se su una postazione la ricezione di pacchetti su `udp/2193` è proibita (per esempio tramite il firewall), Agent non può essere rilevato e quindi Scanner di rete ritiene che Agent non sia installato sulla postazione.

4.4.2. Gestione licenze

Per maggiori informazioni circa i principi e le caratteristiche della concessione delle licenze Dr.Web Enterprise Security Suite consultare la sezione Capitolo 2: Concessione delle licenze.

Interfaccia della Gestione licenze

La Gestione licenze fa parte del Pannello di controllo. Questo componente si utilizza per gestire le licenze degli oggetti della rete antivirus.

Per aprire la finestra Gestione licenze, nel menu principale del Pannello di controllo selezionare la voce **Amministrazione**, nella finestra che si è aperta selezionare la voce del menu di gestione **Gestione licenze**.

Lista gerarchica delle chiavi

La finestra principale Gestione licenze contiene l'albero delle chiavi – una lista gerarchica i cui nodi sono le chiavi di licenza, nonché le postazioni e i gruppi a cui sono state assegnate le chiavi di licenza.

La barra degli strumenti contiene i seguenti elementi di gestione:

Opzione	Descrizione	A seconda degli oggetti nell'albero delle chiavi
Aggiungi chiave	Per aggiungere un nuovo record di una chiave di licenza.	L'opzione è sempre disponibile. Le funzioni dipendono da ciò se l'oggetto è selezionato o meno nell'albero delle chiavi (v. Aggiunzione della nuova chiave di licenza).
Rimuovi gli oggetti selezionati	Per cancellare la correlazione tra una chiave e un oggetto di licenza.	L'opzione è disponibile se nell'albero sono selezionati un oggetto di licenza (postazione o gruppo) o una chiave di licenza.
Propaga la chiave verso i gruppi e le postazioni	Per sostituire una chiave con la chiave selezionata o per aggiungere la chiave selezionata ad un oggetto di licenza.	L'opzione è disponibile se nell'albero è selezionata una chiave di licenza.
Esporta chiave	Per salvare una copia locale del file della chiave di licenza.	
Propaga la chiave verso i Server adiacenti	Per trasferire le licenze dalla chiave selezionata ai Server adiacenti.	

Le Impostazioni della vista albero consentono di modificare l'aspetto dell'albero gerarchico:

- Il flag **Mostra il numero di licenze** attiva/disattiva la visualizzazione nell'albero del numero totale di licenze erogate dai file della chiave.
- Per modificare la struttura dell'albero, utilizzare le seguenti opzioni:
  - L'opzione **Chiavi** comanda di visualizzare tutte le chiavi di licenza della rete antivirus come nodi radice dell'albero gerarchico. Elementi nidificati delle chiavi di licenza sono tutti i gruppi e tutte le postazioni a cui queste chiavi sono state assegnate. Questa vista ad albero è quella base e consente di gestire gli oggetti di licenza e le chiavi di licenza.
  - L'opzione **Gruppi** comanda di visualizzare come nodi radice dell'albero gerarchico quei gruppi a cui le chiavi di licenza sono state assegnate direttamente. Elementi nidificati dei gruppi sono le postazioni incluse in questi gruppi e le chiavi di licenza assegnate a questi gruppi. Questa vista ad albero si utilizza per visualizzare le informazioni sulla licenza in un modo più comodo e non consente di gestire gli oggetti dell'albero.

Gestione delle licenze

Tramite la Gestione licenze, si possono eseguire le seguenti azioni con le chiavi di licenza:

1. Visualizzare le informazioni sulla licenza.
2. Aggiungere una nuova chiave di licenza.
3. Aggiornare una chiave di licenza.
4. Sostituire una chiave di licenza.
5. Ampliare la lista delle chiavi di licenza di un oggetto.
6. Eliminare una chiave di licenza e cancellare l'oggetto dalla lista delle licenze.
7. Trasferire licenze su un Server adiacente.
8. Modificare le licenze trasferite su un Server adiacente.

Visualizzare le informazioni sulla licenza

Per visualizzare le informazioni riassuntive su una chiave di licenza, nella finestra principale Gestione licenze selezionare l'account della chiave di cui si vogliono visualizzare le informazioni (fare clic sul nome dell'account della chiave). Il pannello che si è aperto contiene le informazioni quali:

- utente della licenza,
- venditore da cui è stata acquistata la licenza,
- identificatore e numero di serie della licenza,
- scadenza della licenza,
- viene indicato se la licenza comprende il supporto del modulo Antispam,
- numero di postazioni indicato nel file della chiave per cui è stata concessa la licenza,
- MD5 hash della chiave di licenza,
- lista dei componenti antivirus che la licenza consente di utilizzare.

Aggiungere una nuova chiave di licenza

Per aggiungere una nuova chiave di licenza:

1. Nella finestra principale della Gestione licenze premere il pulsante **Aggiungi chiave** nella barra degli strumenti.
2. Nel pannello che si è aperto, fare clic sul pulsante e selezionare un file della chiave di licenza.
3. Premere il pulsante **Salva**.
4. La chiave di licenza viene aggiunta all'albero delle chiavi, però non viene associata ad alcun oggetto. In questo caso, per impostare gli oggetti di licenza, eseguire le procedure personaliz-

zate Sostituire una chiave di licenza o Ampliare la lista delle chiavi di licenza di un oggetto descritte sotto.

Aggiornare una chiave di licenza

In caso di aggiornamento di una chiave di licenza, la nuova chiave di licenza verrà assegnata agli stessi oggetti di licenza per i quali valeva la chiave che viene aggiornata.

Adoperare la procedura di aggiornamento chiave per sostituire una chiave scaduta o per sostituire una chiave con un'altra che ha un altro elenco dei componenti da installare, mentre la struttura dell'albero delle chiavi si mantiene.

Per aggiornare una chiave di licenza:

1. Nella finestra principale Gestione licenze nell'albero delle chiavi selezionare la chiave che si vuole aggiornare.
2. Nel pannello delle proprietà della chiave, che si è aperto, fare clic sul pulsante  e selezionare il file della chiave di licenza.
3. Fare clic sul pulsante **Salva**. Si apre la finestra delle impostazioni dei componenti da installare, descritta nella sottosezione Impostazioni per la sostituzione della chiave di licenza.
4. Fare clic sul pulsante **Salva** per aggiornare la chiave di licenza.

Sostituire una chiave di licenza

In caso di sostituzione della chiave di licenza, tutte le chiavi di licenza correnti dell'oggetto di licenza vengono cancellate e la nuova chiave viene aggiunta.

Per sostituire la chiave di licenza corrente:

1. Nella finestra principale Gestione licenze nell'albero delle chiavi selezionare la chiave che si vuole assegnare a un oggetto di licenza.
2. Nella barra degli strumenti fare clic sul pulsante  **Propaga la chiave verso i gruppi e le postazioni**. Si apre la finestra con la lista gerarchica delle postazioni e dei gruppi della rete antivirus.
3. Selezionare dalla lista gli oggetti di licenza. Per selezionare più postazioni e gruppi, utilizzare i tasti CTRL e MAIUSCOLO.
4. Fare clic sul pulsante **Sostituisci la chiave**. Si apre la finestra delle impostazioni dei componenti da installare, descritta nella sottosezione Impostazioni per la sostituzione della chiave di licenza.
5. Fare clic sul pulsante **Salva** per sostituire la chiave di licenza.

Ampliare la lista delle chiavi di licenza di un oggetto

In caso di aggiunta di una chiave di licenza, tutte le chiavi correnti dell'oggetto di licenza vengono preservate e la nuova chiave di licenza viene aggiunta alla lista delle chiavi.

Per aggiungere una chiave di licenza all'elenco delle chiavi di licenza dell'oggetto:

1. Nella finestra principale Gestione licenze nell'albero delle chiavi selezionare la chiave che si vuole aggiungere all'elenco delle chiavi dell'oggetto.
2. Nella barra degli strumenti fare clic sul pulsante **Propaga la chiave verso i gruppi e le postazioni**. Si apre la finestra con la lista gerarchica delle postazioni e dei gruppi della rete antivirus.
3. Selezionare dalla lista gli oggetti di licenza. Per selezionare più postazioni e gruppi, utilizzare i tasti CTRL e MAIUSCOLO.
4. Fare clic sul pulsante **Aggiungi chiave**. Si apre la finestra delle impostazioni dei componenti da installare, descritta nella sottosezione Impostazioni per l'aggiunta di una chiave di licenza alla lista della chiavi.
5. Fare clic sul pulsante **Salva** per aggiungere la chiave di licenza.

Eliminare una chiave di licenza e cancellare l'oggetto dalla lista delle licenze

Non è possibile cancellare l'ultimo account della chiave del gruppo **Everyone**.

Per cancellare una chiave di licenza o un oggetto dalla lista delle licenze:

1. Nella finestra principale Gestione licenze selezionare la chiave che si vuole cancellare o selezionare l'oggetto (postazione o gruppo) a cui è stata assegnata questa chiave e fare clic sul pulsante **Rimuovi gli oggetti selezionati** nella barra degli strumenti. Tenere presente che:
   - Se è stato selezionato un oggetto di licenza, esso viene cancellato dalla lista degli oggetti a cui è assegnata la stessa chiave. Se la chiave è stata assegnata come l'impostazione individuale a un oggetto, l'oggetto eredita la chiave di licenza dal gruppo.
   - Se è stata selezionata una chiave di licenza, l'account della chiave viene rimosso dalla rete antivirus. Tutti gli oggetti a cui è stata assegnata questa chiave ereditano la chiave di licenza dal gruppo.
2. Si apre la finestra delle impostazioni dei componenti da installare, descritta nella sottosezione Impostazioni per la sostituzione della chiave di licenza.
3. Fare clic sul pulsante **Salva** per cancellare l'oggetto selezionato e per attivare l'ereditarietà della chiave.

Trasferire licenze su un Server adiacente

Se una parte delle licenze libere nella chiave di licenza su un Server viene trasferita su un Server adiacente, il numero di licenze trasferito sarà non disponibile per l'uso su questo Server fino alla fine del periodo di distribuzione di queste licenze.

Per trasferire licenze su un Server adiacente:

1. Nella finestra principale Gestione licenze nell'albero delle chiavi selezionare la chiave di cui le licenze libere si vogliono trasferire su un Server adiacente.
2. Nella barra degli strumenti fare clic sul pulsante **Propaga la chiave verso i Server adiacenti**. Si apre la finestra con la lista gerarchica dei Server adiacenti.
3. Selezionare dalla lista i Server su cui si vogliono distribuire le licenze.
4. Di fronte a ciascun Server, configurare i seguenti parametri:
   - **Numero di licenze** – numero di licenze libere che si vuole trasferire da questa chiave su un Server adiacente.
   - **Data della scadenza della licenza** – periodo per cui vengono trasferite le licenze. Dopo il periodo indicato, tutte le licenze verranno richiamate dal Server adiacente e tornano nella lista delle licenze libere di questa chiave di licenza.
5. Fare clic su uno dei pulsanti:
   - **Aggiungi chiave** – per aggiungere le licenze alla lista delle licenze disponibili dei Server adiacenti. Si apre la finestra delle impostazioni dei componenti da installare, descritta nella sottosezione Impostazioni per l'aggiunta di una chiave di licenza alla lista delle chiavi.
   - **Sostituisci la chiave** – per cancellare le licenze correnti dei Server adiacenti e per assegnare ad essi soltanto le licenze che vengono distribuite. Si apre la finestra delle impostazioni dei componenti da installare, descritta nella sottosezione Impostazioni per la sostituzione della chiave di licenza.
6. Fare clic sul pulsante **Salva** per distribuire le licenze sui Server adiacenti.

Modificare le licenze trasferite su un Server adiacente

Per modificare le licenze distribuite su un Server adiacente:

1. Nella finestra principale Gestione licenze nell'albero delle chiavi selezionare il Server adiacente su cui sono state distribuite le licenze.
2. Nel pannello delle proprietà che si è aperto, modificare i seguenti parametri:
   - **Numero di licenze** – numero di licenze libere trasferite dalla chiave di questo Server sul Server adiacente.
   - **Data della scadenza della licenza** – periodo per cui vengono trasferite le licenze. Dopo il periodo indicato, tutte le licenze verranno ritirate da questo Server e ritorneranno nella lista delle licenze libere della chiave di licenza corrispondente.

3. Fare clic sul pulsante **Salva** per aggiornare le informazioni sulle licenze distribuite.

Modificare la lista dei componenti da installare

Impostazioni per la sostituzione della chiave di licenza

In questa sottosezione, è descritta la configurazione dei componenti da installare quando vengono eseguite le procedure:

- Aggiornare una chiave di licenza.
- Sostituire una chiave di licenza.
- Cancellare una chiave di licenza.
- Trasferire licenze su un Server adiacente sostituendone la chiave.

Nell'esecuzione di queste procedure, per configurare i componenti da installare:

1. Nella finestra di configurazione dei componenti da installare nella lista degli oggetti sono riportati:
   - Postazioni e gruppi con i suoi elenchi dei componenti da installare.
   - Nella colonna **Chiave corrente** sono riportate la lista delle chiavi dell'oggetto e le impostazioni dei componenti da installare che attualmente valgono per l'oggetto.
   - Nella colonna **Chiave che viene assegnata** sono riportate la chiave e le impostazioni dei componenti da installare, definite nella chiave che verrà assegnata agli oggetti selezionati.
   - Se necessario, spuntare il flag **Mostra soltanto ciò che differisce** affinché nella lista vengano visualizzati soltanto quei componenti le cui impostazioni sono diverse nella chiave corrente e in quella che viene assegnata.
2. Per configurare la lista dei componenti da installare:
   a) Nella colonna **Chiave che viene assegnata** si può configurare una lista riassuntiva dei componenti da installare.
      - Le impostazioni dei componenti da installare nella colonna **Chiave che viene assegnata** vengono calcolate sulla base di ciò se l'utilizzo di un componente è consentito (+) o non è consentito (–) nelle impostazioni correnti e nella chiave nuova nel seguente modo:

Impostazioni correnti	Impostazioni della chiave che viene assegnata	Impostazioni risultanti
+	+	+
–	+	+
+	–	–
–	–	–

- Si possono modificare le impostazioni dei componenti da installare (abbassare i permessi di installazione) solo se nelle impostazioni calcolate nella colonna **Chiave che viene assegnata** l'utilizzo di questo componente è consentito.

b) Spuntare i flag corrispondenti a quegli oggetti (postazioni e gruppi) per cui l'ereditarietà delle impostazioni verrà disattivata e verranno assegnate come individuali le impostazioni dei componenti da installare dalla colonna **Chiave che viene assegnata**. Per gli altri oggetti (per cui i flag non sono messi) verrà assegnata l'ereditarietà delle impostazioni originali dalla colonna **Chiave che viene assegnata**.

Impostazioni per l'aggiunta di una chiave di licenza alla lista della chiavi

In questa sottosezione, è descritta la configurazione dei componenti da installare quando vengono eseguite le procedure:

- Ampliare la lista delle chiavi di licenza di un oggetto.
- Trasferire licenze su un Server adiacente aggiungendo la chiave.

Nell'esecuzione di queste procedure, per configurare i componenti da installare:

1. Nella finestra di configurazione dei componenti da installare nella lista degli oggetti sono riportati:
   - Postazioni e gruppi con i suoi elenchi dei componenti da installare.
   - Nella colonna **Chiave corrente** sono riportate la lista delle chiavi dell'oggetto e le impostazioni dei componenti da installare che attualmente valgono per l'oggetto.
   - Nella colonna **Chiave che viene assegnata** sono riportate la chiave e le impostazioni dei componenti da installare, definite nella chiave che si vuole aggiungere per gli oggetti selezionati.
2. Se necessario, spuntare il flag **Mostra soltanto ciò che differisce** affinché nella lista vengano visualizzati soltanto quei componenti le cui impostazioni sono diverse nella chiave corrente e in quella che viene ereditata. Notare che nella sezione **Chiave che viene assegnata** sono riportate non le impostazioni della chiave che viene assegnata, ma le impostazioni risultanti dei componenti da installare.
3. Per configurare la lista dei componenti da installare:
   a) Nella colonna **Chiave che viene assegnata** si può configurare una lista riassuntiva dei componenti da installare.
      - Le impostazioni dei componenti da installare nella colonna **Chiave che viene assegnata** vengono calcolate sulla base di ciò se l'utilizzo di un componente è consentito (+) o non è consentito (–) nelle impostazioni correnti e nella chiave nuova nel seguente modo:

Impostazioni correnti	Impostazioni della chiave che viene assegnata	Impostazioni risultanti
+	+	+
–	+	–

Impostazioni correnti	Impostazioni della chiave che viene assegnata	Impostazioni risultanti
+	–	–
–	–	–

- Si possono modificare le impostazioni dei componenti da installare (abbassare i permessi di installazione) solo se nelle impostazioni calcolate nella colonna Chiave che viene assegnata l'utilizzo di questo componente è consentito.

b) Spuntare i flag corrispondenti a quegli oggetti (postazioni e gruppi) per cui l'ereditarietà delle impostazioni verrà disattivata e verranno assegnate le impostazioni dei componenti da installare dalla colonna **Chiave che viene assegnata** come quelle individuali. Per gli altri oggetti (per cui i flag non sono messi) verrà assegnata l'ereditarietà delle impostazioni dalla colonna **Chiave che viene assegnata**.

4.5. Schema interazione dei componenti della rete antivirus

In immagine 4-2 è rappresentato lo schema generale di un frammento di rete antivirus.

Questo schema visualizza una rete antivirus che include soltanto un Server. In grandi aziende, è preferibile installare una rete antivirus con diversi Server per il bilanciamento di carico tra di essi.

In questo esempio la rete antivirus è stata implementata in una rete locale, però per l'installazione e il funzionamento di Dr.Web Enterprise Security Suite e dei pacchetti antivirus non è necessario che i computer si trovino in una rete locale, è sufficiente l'accesso Internet.

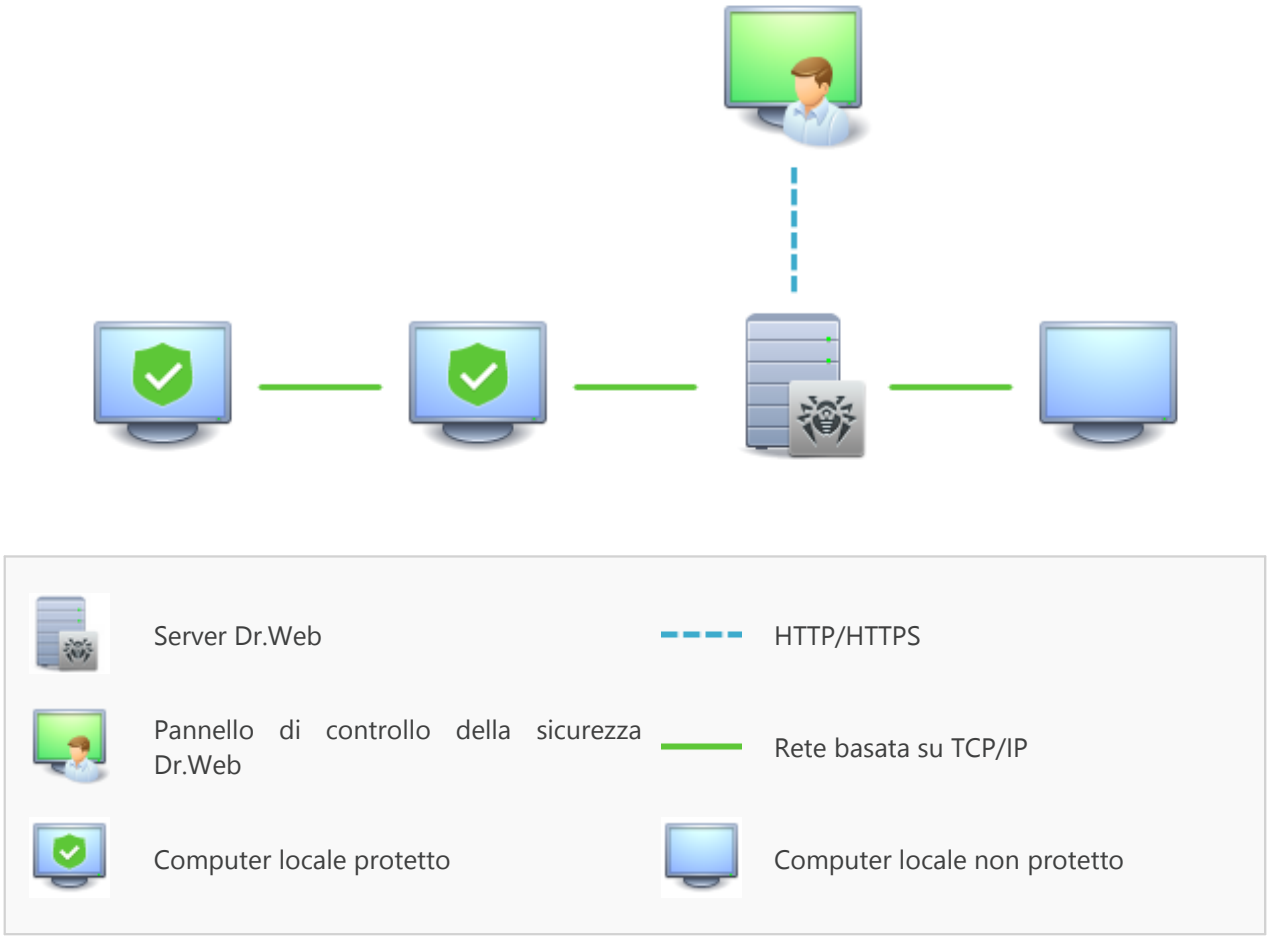


Immagine 4-2. Struttura della rete antivirus

Quando il Server Dr.Webviene eseguita la seguente sequenza di azioni:

1. Vengono caricati i file di Server Dr.Web dalla directory bin.
2. Viene caricato lo Scheduler del Server.
3. Vengono caricate la directory di installazione centralizzata e la directory di aggiornamento, viene avviato il sistema di informazione di segnalazione (sistema di avvisi).
4. Viene controllata l'integrità del database del Server.
5. Vengono eseguiti i task dello Scheduler del Server.
6. Attesa delle informazioni dagli Agent Dr.Web e dei comandi dai Pannelli di controllo.

L'intero flusso dei comandi, dei dati e delle informazioni statistiche nella rete antivirus passa necessariamente attraverso il Server Dr.Web. Anche il Pannello di controllo scambia informazioni solamente con il Server; il Server modifica la configurazione di una postazione e manda comandi all'Agent Dr.Web sulla base dei comandi del Pannello di controllo.

Così, il frammento della rete antivirus ha una struttura logica illustrata in immagine 4-3.

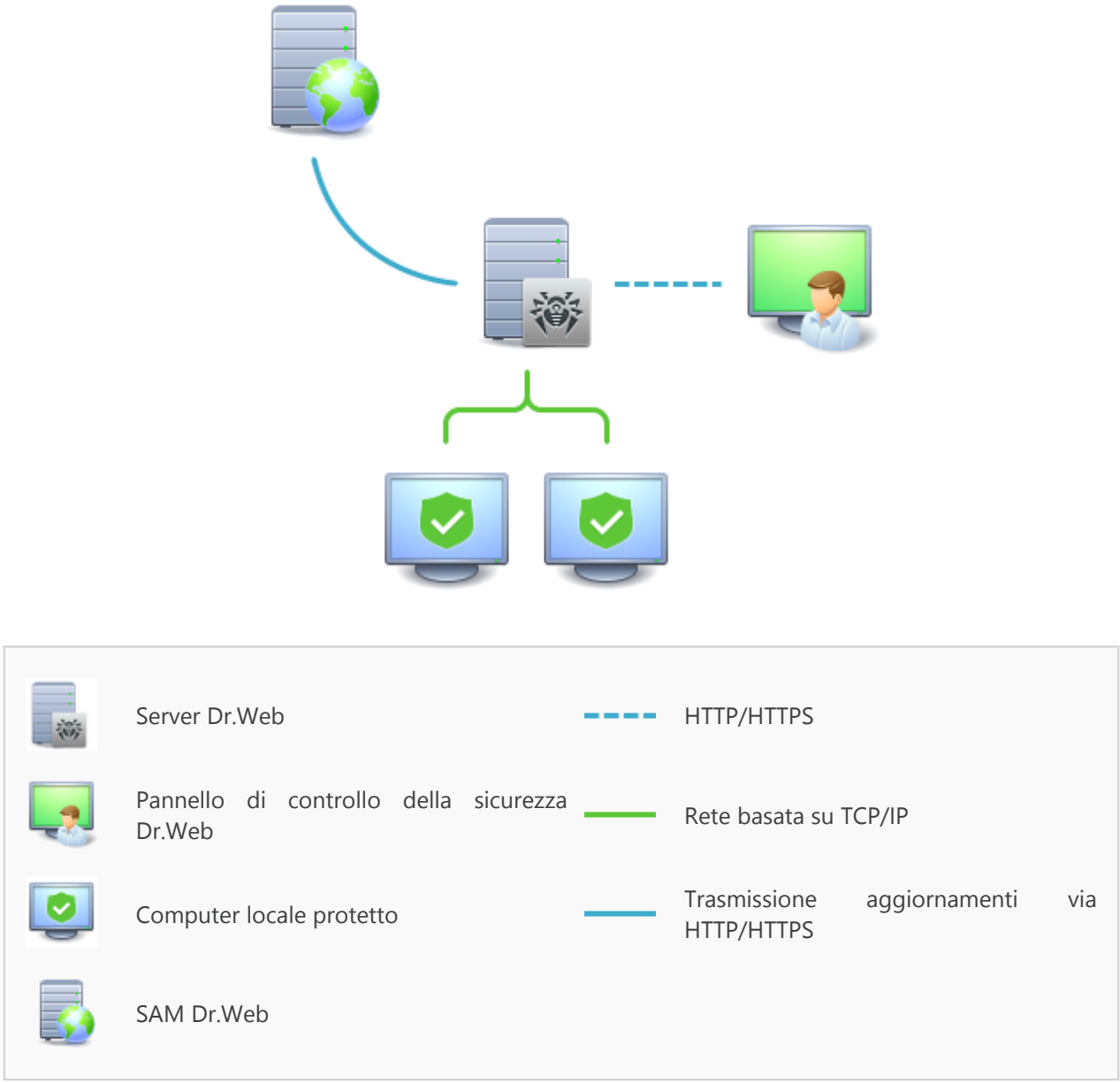


Immagine 4-3. Struttura logica della rete antivirus

Tra il Server e le postazioni (una linea continua sottile in immagine 4-3) vengono trasmessi:

- le query dell'Agent per ottenere il calendario centralizzato e il calendario centralizzato di questa postazione,
- le impostazioni dell'Agent e del pacchetto antivirus,
- le query per ottenere i task ordinari da eseguire (scansione, aggiornamento dei database dei virus ecc),
- i file dei pacchetti antivirus – quando l'Agent ha ricevuto il task di installazione,
- gli aggiornamenti del software e dei database dei virus – nel corso dell'esecuzione del task di aggiornamento,
- gli avvisi dell'Agent sulla configurazione della postazione,

- le statistiche del funzionamento dell'Agent e dei pacchetti antivirus che verranno incluse nel log centralizzato,
- gli avvisi su eventi dei virus e su altri eventi da registrare.

A seconda delle impostazioni e dalla quantità di postazioni, il volume di traffico tra le postazioni e il Server può essere abbastanza grande. La rete antivirus Dr.Web Enterprise Security Suite prevede la possibilità di compressione di traffico. L'utilizzo di questa modalità opzionale è descritta sotto v. p. Utilizzo della codifica e della compressione di traffico.

Il traffico tra il Server e la postazione può essere codificato. Consente di evitare la divulgazione delle informazioni trasmesse via il canale descritto e la sostituzione del software che viene caricato sulle postazioni. Di default, questa possibilità è attivata. L'utilizzo di questa modalità è descritta sotto v. p. Utilizzo della codifica e della compressione di traffico.

Dal server web di aggiornamenti a Server Dr.Web (linea continua spessa in immagine 4-3) attraverso il protocollo HTTP vengono trasmessi i file necessari per la replica delle directory centralizzate di installazione e di aggiornamento, nonché le informazioni di servizio sullo stato di tale processo. L'integrità delle informazioni trasmesse (dei file del software Dr.Web Enterprise Security Suite e dei pacchetti antivirus) è assicurata dall'utilizzo del metodo checksum: un file danneggiato o sostituito durante la trasmissione non sarà accettato dal Server.

Tra il Server e il Pannello di controllo (linea tratteggiata in immagine 4-3) vengono trasmesse le informazioni sulla configurazione del Server (comprese le informazioni sulla topologia di rete) e le impostazioni delle postazioni. Queste informazioni vengono visualizzate nel Pannello di controllo e se qualche impostazione è stata modificata dall'utente (dall'amministratore della rete antivirus), le informazioni sulle modifiche apportate vengono trasmesse sul Server.

La connessione del Pannello di controllo con il Server selezionato viene stabilita soltanto dopo che l'amministratore di rete antivirus si è autenticato, inserendo il nome di registrazione e la password su tale Server.

Capitolo 5: Amministratori della rete antivirus

Si consiglia di nominare amministratore della rete antivirus un dipendente affidabile, qualificato, con esperienza in amministrazione di una rete locale e con buone conoscenze della protezione antivirus. Tale dipendente deve avere l'accesso completo alle directory di installazione di Server Dr.Web. A seconda dei criteri di sicurezza della società e della disponibilità del personale, l'amministratore della rete antivirus deve avere i privilegi di amministratore di rete locale o deve lavorare a stretto contatto con tale amministratore.

Per la gestione operativa della rete antivirus, all'amministratore della rete antivirus non sono necessari i privilegi di amministratore sui computer inclusi in questa rete antivirus. Tuttavia, l'installazione e la disinstallazione remota del software Agent sono possibili soltanto in una rete locale e richiedono i privilegi di amministratore in questa rete, il debugging di Server Dr.Web richiede l'accesso completo alla directory d'installazione server.

5.1. Autenticazione di amministratori

Per connettersi al Server Dr.Web, gli amministratori possono autenticarsi nei seguenti modi:

1. Salvando le informazioni sugli amministratori nel database del Server.
2. Tramite Active Directory (nelle versioni del Server per SO Windows).
3. Utilizzando il protocollo LDAP.
4. Utilizzando il protocollo RADIUS.
5. Utilizzando PAM (solo nei SO della famiglia UNIX).

I modi di autenticazione vengono utilizzati consecutivamente secondo i seguenti principi:

1. L'ordine di utilizzo dei modi di autenticazione dipende dall'ordine in cui essi sono elencati nelle impostazioni definite tramite il Pannello di controllo.
2. Per primo viene eseguito il tentativo di autenticazione amministratore dal database del Server.
3. Come seconda, di default, viene utilizzata l'autenticazione tramite LDAP, come terza – quella tramite Active Directory, come quarta – quella tramite RADIUS. Negli SO della famiglia UNIX come quinta viene utilizzata l'autenticazione PAM.
4. Nelle impostazioni del Server i modi di autenticazione tramite LDAP, Active Directory e RADIUS possono essere scambiati di posto, ma all'inizio viene sempre utilizzato il tentativo di autenticazione dal database.
5. Di default, i modi di autenticazione tramite LDAP, Active Directory e RADIUS sono sempre disattivati.

Per modificare l'ordine di utilizzo dei metodi di autenticazione:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nel menu di gestione selezionare la sezione **Autenticazione**.
3. Nella finestra che si è aperta, viene riportata la lista dei tipi di autenticazione nell'ordine in cui vengono utilizzati. Per modificare la sequenza, trascinare (drag'n'drop) i modi di autenticazione nella lista e metterli nell'ordine in cui si desidera utilizzarli.
4. Per rendere effettive le modifiche apportate, riavviare il Server.

Il nome utente amministratore deve essere unico.

Non è possibile connettere un amministratore tramite i sistemi di autenticazione esterni se sul Server esiste già un amministratore con lo stesso nome utente.

Ogni volta che si salvano modifiche della sezione **Autenticazione**, viene automaticamente salvato un backup della versione precedente del file di configurazione con i parametri di autenticazione degli amministratori. Vengono conservati gli ultimi 10 backup.

I backup si trovano nella stessa directory del file di configurazione e vengono denominati nel seguente formato:

<nome_di_file>;<ora_di_creazione>

dove *<nome_di_file>* dipende dal sistema di autenticazione: `auth-ads.xml`, `auth-ldap.xml`, `auth-radius.xml`, `auth-pam.xml`.

È possibile utilizzare i backup creati, in particolare, per ripristinare il file di configurazione se l'interfaccia del Pannello di controllo non è disponibile.

5.1.1. Autenticazione di amministratori dal database del Server

Il modo di autenticazione che salva i dati di amministratori nel database del Server viene utilizzato di default.

Per gestire la lista degli amministratori:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nel menu di gestione selezionare la sezione **Amministratori**. Si apre la lista di tutti gli amministratori del Server.

   Per maggiori informazioni v. Amministratori e gruppi di amministratori.

5.1.2. Autenticazione con utilizzo di Active Directory

Per attivare l'autenticazione tramite Active Directory:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.

2. Nel menu di gestione selezionare la sezione **Autenticazione**.
3. Nella finestra che si è aperta, entrare nella sezione **Microsoft Active Directory**.
4. Spuntare il flag **Utilizza autenticazione Microsoft Active Directory**.
5. Premere **Salva**.
6. Per rendere effettive le modifiche apportate, riavviare il Server.

Se viene utilizzata l'autenticazione di amministratori tramite Active Directory, nel Pannello di controllo viene impostato solo il permesso di utilizzo di questo modo di autenticazione.

Le proprietà di amministratori di Active Directory vengono modificate manualmente sul server Active Directory.

Per modificare gli amministratori di Active Directory:

> Le seguenti operazioni vengono eseguite su un computer che ha lo snap-in per l'amministrazione di Active Directory.

1. Per poter modificare i parametri di amministratori, è necessario eseguire le seguenti azioni:
   a) Per modificare lo schema di Active Directory, avviare l'utility `drweb-esuite-modify-ad-schema-xxxxxxxxxxxxxxx-windows-nt-xYY.exe` (fa parte del pacchetto Server Dr.Web).
   La modifica dello schema di Active Directory può richiedere un certo tempo. A seconda della configurazione del dominio, ci vogliono fino ai 5 minuti o più per sincronizzare e per applicare lo schema modificato.

   > Se in precedenza lo schema di Active Directory è stato modificato con utilizzo di questa utility dalla 6° versione del Server, non è necessario modificarlo di nuovo con utilizzo dell'utility dalla 10 versione del Server.

   b) Per registrare lo snap-in Active Directory Schema (lo Schema di Active Directory), eseguire con i permessi di amministratore il comando `regsvr32 schmmgmt.dll`, dopodiché avviare `mmc` e aggiungere lo snap-in **Active Directory Schema**.
   c) Utilizzando lo snap-in Active Directory Schema, aggiungere alla classe **User** e (se necessario) alla classe **Group** la classe ausiliaria **DrWebEnterpriseUser**.

   > Se l'applicazione di schema modificato non è ancora finita, la classe **DrWebEnterpriseUser** potrebbe risultare non trovata. In questo caso aspettare per un tempo e ripetere il tentativo secondo il punto **c)**.

   d) Con i permessi di amministratore avviare il file `drweb-esuite-aduac-xxxxxxxxxxxx-xx-windows-nt-xYY.msi` (fa parte del pacchetto Dr.Web Enterprise Security Suite 10) e aspettare il compimento dell'installazione.
2. L'interfaccia grafica per la modifica degli attributi è disponibile nel pannello di controllo **Active Directory Users and Computers** → nella sezione **Users** → nella finestra di modifica delle proprietà dell'utente selezionato **Administrator Properties** → nella scheda **Dr.Web Authentication**.

3. Per la modifica è disponibile il seguente parametro (il valore di attributo può essere **yes**, **no** o **not set**):

   User is administrator – indica che l'utente è un amministratore con i permessi completi.

   Gli algoritmi di principio di funzionamento e di analisi degli attributi di autenticazione sono riportati nel documento **Allegati**, in Allegato C1.

5.1.3. Autenticazione con utilizzo di LDAP

Per attivare l'autenticazione tramite LDAP:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nel menu di gestione selezionare la sezione **Autenticazione**.
3. Nella finestra che si è aperta, entrare nella sezione **Autenticazione LDAP**.
4. Spuntare il flag **Utilizza autenticazione LDAP**.
5. Premere **Salva**.
6. Per rendere effettive le modifiche apportate, riavviare il Server.

Si può configurare l'autenticazione tramite il protocollo LDAP su qualsiasi server LDAP. Inoltre, con utilizzo dello stesso meccanismo, si può configurare il Server sotto SO della famiglia UNIX per l'autenticazione in Active Directory tramite il controller di dominio.

Le impostazioni di autenticazione LDAP vengono salvate nel file di configurazione `auth-ldap.xml`.

I principali attributi xml di autenticazione sono descritti nel documento **Allegati**, in Allegato C2.

A differenza di Active Directory, si può configurare il meccanismo per qualsiasi schema LDAP. Di default, si tenta di utilizzare gli attributi del Dr.Web Enterprise Security Suite definiti per Active Directory.

Il processo di autenticazione tramite LDAP consiste nel seguente:

1. L'indirizzo del server LDAP viene impostato attraverso il Pannello di controllo o nel file di configurazione xml.
2. Per il nome utente impostato vengono eseguite le seguenti azioni:
   - Il nome utente viene convertito in DN (Distinguished Name) tramite maschere simili a DOS (con utilizzo del carattere *), se sono impostate regole.
   - Il nome utente viene convertito in DN con utilizzo di espressioni regolari, se sono impostate regole.
   - Viene utilizzato uno script custom di conversione di nomi in DN, se è specificato nelle impostazioni.

- Se non è adatta nessuna delle regole di conversione, il nome utente impostato viene utilizzato così com'è.

> Il formato di impostazione di nome utente non viene definito o fissato in nessun modo – può essere lo stesso utilizzato dalla società, cioè non è richiesta la modifica coattiva dello schema LDAP. La conversione per tale schema viene eseguita con utilizzo di regole di conversione di nomi in LDAP DN.

3. Come in caso di autenticazione tramite Active Directory, dopo la conversione, si tenta di registrare questo utente sul server LDAP indicato con utilizzo del DN ottenuto e di una password inserita.
4. In seguito, così come in Active Directory, vengono letti gli attributi dell'oggetto LDAP per il DN ottenuto. Si possono ridefinire gli attributi e i valori possibili nel file di configurazione.
5. Se i valori di alcuni attributi dell'amministratore non sono stati definiti, se viene impostata l'ereditarietà (nel file di configurazione), la ricerca di attributi richiesti nei gruppi, di cui l'utente fa parte, viene eseguita così come nel caso quando viene utilizzato Active Directory.

5.1.4. Autenticazione con utilizzo di RADIUS

Per attivare l'autenticazione tramite RADIUS:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nel menu di gestione selezionare la sezione **Autenticazione**.
3. Nella finestra che si è aperta, entrare nella sezione **Autenticazione RADIUS**.
4. Spuntare il flag **Utilizza autenticazione RADIUS**.
5. Premere **Salva**.
6. Per rendere effettive le modifiche apportate, riavviare il Server.

Per utilizzare il protocollo di autenticazione RADIUS, è necessario installare un server che mette in pratica questo protocollo, per esempio freeradius (per maggiori informazioni consultare http://freeradius.org/).

Nel Pannello di controllo vengono configurati i seguenti parametri dell'utilizzo di server RADIUS:

- **Server**, **Porta**, **Password** – parametri di connessione al server RADIUS: rispettivamente l'indirizzo IP/il nome DNS, il numero di porta, la password (segreta).
- **Timeout** – tempo di attesa di una risposta del server RADIUS, in secondi.
- **Numero di tentativi** – numero di tentativi di connessione al server RADIUS.

Inoltre, per configurare i parametri addizionali di RADIUS, si possono utilizzare:

- File di configurazione `auth-radius.xml` situato nella directory etc Server.

  Oltre ai parametri configurati tramite il Pannello di controllo, nel file di configurazione si può impostare il valore dell'identificatore NAS. Secondo la specifica RFC 2865, questo identificatore può essere utilizzato invece dell'indirizzo IP/del nome DNS come l'identificatore del client che

si connette al server RADIUS. Nel file di configurazione l'identificatore si conserva nella seguente forma:

```
<!-- NAS identifier, optional, default - hostname -->
<nas-id value="drwcs"/>
```

- Dizionario `dictionary.drweb` situato nella directory `etc` del Server.

  Il dizionario conserva un set di attributi di RADIUS della società Doctor Web (VSA - Vendor-Specific Attributes).

5.1.5. Autenticazione con utilizzo di PAM

Per attivare l'autenticazione tramite PAM:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nel menu di gestione selezionare la sezione **Autenticazione**.
3. Nella finestra che si è aperta, entrare nella sezione **Autenticazione PAM**.
4. Spuntare il flag **Utilizza autenticazione PAM**.
5. Premere **Salva**.
6. Per rendere effettive le modifiche apportate, riavviare il Server.

Nei sistemi operativi UNIX, l'autenticazione PAM viene effettuata tramite dei plugin di autenticazione.

Per configurare i parametri dell'autenticazione PAM, è possibile utilizzare i seguenti metodi:

- Configurare il metodo di autenticazione attraverso il Pannello di controllo: nella sezione **Amministrazione** → **Autenticazione** → **Autenticazione PAM**.
- File di configurazione `auth-pam.xml`, situato nella directory `etc` del Server. Esempio di file di configurazione:

```
...
<!-- Enable this authorization module -->
  <enabled value="no" />
<!-- This authorization module number in the stack -->
  <order value="50" />
<!-- PAM service name>" -->
  <service name="drwcs" />
<!-- PAM data to be queried: PAM stack must return INT zero/non-zero -->
  <admin-flag mandatory="no" name="DrWeb_ESuite_Admin" />
...
```

Descrizione dei parametri dell'autenticazione PAM che vengono configurati sul lato Dr.Web Enterprise Security Suite

Elemento di Pannello di controllo	Elementi del file auth-pam.xml			Descrizione
	Blocco	Parametro	Valori ammissibili	
Flag **Utilizza autenticazione PAM**	`<enabled>`	`value`	yes | no	Il flag che determina se verrà utilizzato il metodo di autenticazione PAM.
Utilizzare Drag and Drop	`<order>`	`value`	valore di numero intero concordato con i valori degli altri metodi	Il numero di sequenza dell'autenticazione PAM se vengono utilizzati più metodi di autenticazione.
Campo **Nome del servizio**	`<service>`	`name`	-	Il nome del servizio che verrà utilizzato per creare un contesto di PAM. PAM può leggere i criteri per questo servizio da `/etc/pam.d/<nome servizio>` o da `/etc/pam.conf` se il file non esiste. Se il parametro non è impostato (il tag `<service>` non c'è nel file di configurazione), di default, viene utilizzato il nome `drwcs`.
Flag **Il flag di controllo è obbligatorio**	`<admin-flag>`	`mandatory`	yes | no	Il parametro che determina se il file di controllo è obbligatorio per l'identificazione di un utente come amministratore. Di default, è `yes`.
Campo **Nome del flag di controllo**	`<admin-flag>`	`name`	-	Stringa chiave in base alla quale verrà letto il flag dei moduli PAM. Di default, è `DrWeb_ESuite_Admin`.

Quando si configurano i moduli di autenticazione PAM, utilizzare i parametri impostati sul lato Dr.Web Enterprise Security Suite e anche tenere presenti i valori che vengono attribuiti di default anche se nessun parametro è stato impostato.

5.2. Amministratori e gruppi di amministratori

Per aprire la sezione di gestione degli account amministratori, selezionare la voce **Amministrazione** del menu principale del Pannello di controllo, e nella finestra che si è aperta selezionare la voce del menu di gestione **Amministratori**.

La sezione **Amministratori** è disponibile a tutti gli amministratori del Pannello di controllo. Tuttavia, l'intero albero gerarchico degli amministratori è disponibile soltanto agli amministratori appartenenti al gruppo **Administrators** a cui è consentito il permesso di **Visualizzazione delle proprietà e della configurazione dei gruppi di amministratori**. Per gli altri amministratori l'albero gerarchico rispecchia soltanto il loro gruppo e i sottogruppi con gli account che ne fanno parte.

5.2.1. Lista gerarchica degli amministratori

La lista gerarchica degli amministratori rispecchia una struttura ad albero dei gruppi di amministratori e degli account amministratori. Nodi di questa struttura sono i gruppi di amministratori e gli amministratori che ne fanno parte. Ciascun amministratore fa parte di solo un gruppo. Il livello di nidificazione di gruppi non è limitato.

Gruppi predefiniti

Dopo l'installazione del Server, due gruppi vengono creati in modo automatico:

- **Administrators**. Inizialmente nel gruppo rientra solo un amministratore **admin** con il completo set di permessi che viene creato automaticamente all'installazione del Server (v. sotto).
- **Newbies**. Inizialmente il gruppo è vuoto. In questo gruppo vengono messi automaticamente gli amministratori che utilizzano il tipo di autenticazione esterno tramite LDAP, Active Directory e RADIUS.

  Di default, agli amministratori appartenenti al gruppo **Newbies** vengono assegnati i permessi di sola lettura.

Amministratori predefiniti

Dopo l'installazione del Server, un account amministratore viene creato in modo automatico:

Parametro	Valore
Nome utente	**admin**
Password	Viene impostata all'installazione del Server (passo 9 nella procedura di installazione).
Permessi	Completo set di permessi.
Modifica dell'account	I permessi dell'amministratore non possono essere modificati, l'amministratore non può essere rimosso.

Visualizzazione di liste gerarchiche

- Nella lista gerarchica della rete antivirus: un amministratore vede soltanto quei gruppi custom che sono consentiti nel premesso **Visualizza le proprietà dei gruppi di postazioni**. Anche tut-

ti i gruppi di sistema vengono visualizzati nell'albero della rete antivirus, ma in essi sono visibili soltanto le postazioni appartenenti ai gruppi custom dalla lista indicata.

- Nella lista gerarchica degli amministratori: un amministratore dal gruppo **Newbies** vede un albero di cui la radice è il gruppo in cui si trova, cioè vede gli amministratori dal suo gruppo e dai sottogruppi dello stesso. Un amministratore dal gruppo **Administrators** vede tutti gli amministratori a prescindere dai loro gruppi.

5.2.2. Permessi degli amministratori

Tutte le azioni degli amministratori nel Pannello di controllo vengono limitate da un set di permessi che può essere definito sia per un singolo account che per un gruppo di amministratori.

Il sistema dei permessi degli amministratore include le seguenti possibilità di gestione dei permessi:

- **Assegnazione dei permessi**

  I permessi vengono assegnati durante la creazione di un amministratore o di un gruppo di amministratori. Un account o un gruppo eredita permessi dal gruppo padre in cui viene messo quando viene creato. Durante la creazione non vi è la possibilità di modificare i permessi.

- **Ereditarietà dei permessi**

  Di default, amministratori o gruppi di amministratori ereditano permessi dal gruppo padre, ma l'ereditarietà può essere disattivata.

  - Se l'ereditarietà è disattivata, un amministratore utilizza un set indipendente di permessi individuali, che viene impostato direttamente per il suo account. I permessi del gruppo padre non si applicano.
  - Se un amministratore o un gruppo eredita permessi, i permessi non vengono sostituiti con quelli del gruppo padre, ma piuttosto il permesso assegnato viene ricalcolato sulla base di tutti i permessi dei gruppi padre che si trovano più in alto nell'albero gerarchico. La tabella di calcolo del permesso risultante di un oggetto a seconda dei permessi assegnati e dei permessi del gruppo padre è riportata in p. Unione dei permessi.

- **Modifica dei permessi**

  Quando vengono creati amministratori e gruppi di amministratori, non vi è la possibilità di modificarne i permessi. È possibile soltanto modificare i permessi degli oggetti già creati nella sezione delle impostazioni dell'account o del gruppo. Modificando le proprie impostazioni, si possono soltanto abbassare i permessi. Non è possibile modificare i permessi dell'amministratore predefinito **admin** e dei gruppi predefiniti **Administrators** e **Newbies**.

  La procedura di modifica dei permessi è riportata nella sezione Modifica dei permessi.

Modifica dei permessi

Per modificare i permessi di un amministratore o di un gruppo di amministratori:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Amministratori**.
2. Dalla lista degli amministratori, selezionare l'account che si vuole modificare. Si apre la sezione di modifica delle proprietà.
3. Nella sottosezione **Permessi** è possibile modificare la lista delle azioni consentite per l'amministratore o il gruppo amministrativo selezionato.
4. Per gestire l'ereditarietà dei permessi dell'oggetto selezionato dal gruppo padre, utilizzare il pulsante di opzione:

    **Ereditarietà attivata**

    **Ereditarietà disattivata**
5. Le impostazioni principali vengono definite nella tabella dei permessi:
   a) La prima colonna riporta i nomi dei permessi. L'intestazione della colonna dipende dalla specifica sezione che unisce i permessi per tipo.

   I permessi di amministratori e le sezioni del Pannello di controllo di cui sono responsabili gli specifici permessi sono descritti nel documento **Allegati**, in Allegato C3.

   b) La colonna **Permessi** riporta le impostazioni relative ai permessi dalla prima colonna.

Oggetti di gestione	**Lista delle impostazioni nella colonna Permessi**	**Principio di impostazione del permesso**
Il permesso viene impostato per tutti gli oggetti		
Il permesso non implica la divisione in gruppi per oggetto di gestione.	Può essere riportato uno dei seguenti tipi di permessi: • **Individuale** – per questo oggetto sono configurate le sue impostazioni individuali. • **Ereditato** – le impostazioni sono ereditate dal gruppo padre.	Selezionare / deselezionare il flag **Concedi** nella riga del permesso corrispondente.
Un permesso viene impostato per una lista di oggetti (postazioni, amministratori o gruppi)		
• *Concesso tutto* – il permesso è concesso per tutti gli oggetti di gestione. • *Vietato tutto* – il permesso è vietato per tutti gli oggetti di gestione.	In caso dell'unione delle impostazioni vengono riportati allo stesso tempo i seguenti tipi di permessi:	Premere la lista degli oggetti (anche in caso in cui è impostata la variante **Tutto**). Si apre una finestra con l'albero della rete antivirus, l'albero dei gruppi di amministratori o l'albero delle tariffe a seconda del permesso

Oggetti di gestione	Lista delle impostazioni nella colonna Permessi	Principio di impostazione del permesso
• *Concesso per alcuni oggetti*. Deve essere impostata una lista di oggetti per cui questo permesso è concesso. Per tutti gli altri oggetti il permesso è considerato vietato. • *Vietato per alcuni oggetti*. Deve essere impostata una lista di oggetti per cui questo permesso è vietato. Per tutti gli altri oggetti il permesso è considerato concesso.	• **Individuale** – le impostazioni individuali configurate per questo oggetto. • **Risultante** – il risultato della fusione del permesso individuale dell'oggetto e del permesso del gruppo padre. In caso dell'ereditarietà delle impostazioni viene riportato soltanto il tipo di permesso **Ereditato**.	che viene modificato. Selezionare gli oggetti richiesti nell'albero. Per selezionare più oggetti, utilizzare i tasti CTRL o MAIUSCOLO. Se necessario, spuntare il flag **Per tutti i permessi della sezione** per applicare queste impostazioni per tutti i permessi riportati nella stessa sezione del permesso che viene modificato. Premere il pulsante: • **Concedi** per consentire il permesso nei confronti degli oggetti selezionati. • **Vieta** per vietare il permesso nei confronti degli oggetti selezionati.

Per uno e lo stesso permesso che viene impostato nei confronti di una lista di oggetti non è possibile impostare allo stesso tempo le liste di oggetti vietati e consenti. Questi concetti si escludono a vicenda.

c) Nella colonna **Ereditarietà** è riflesso lo stato di questo permesso relativamente al gruppo padre:
   - **Ereditarietà dal gruppo** – è attivata l'ereditarietà dal gruppo padre indicato, i permessi individuali non sono impostati.
   - **Impostazioni individuali** – è disattivata l'ereditarietà dal gruppo padre, sono impostati i permessi individuali.
   - **Unione con il gruppo** – è attivata l'ereditarietà dal gruppo padre indicato, sono impostati i permessi individuali. Il permesso risultante dell'oggetto è stato calcolato tramite l'unione dei permessi del gruppo padre e dei permessi individuali (v. p. Unione dei permessi).
     In questo caso è possibile rimuovere i permessi individuali dell'oggetto. Per farlo, premere il pulsante nella colonna **Ereditarietà**. Dopo la rimozione dei permessi individuali verrà impostata l'opzione **Ereditarietà dal gruppo**.

Unione dei permessi

Il calcolo del permesso risultante di un oggetto (un amministratore o un gruppo di amministratori), se l'ereditarietà è abilitata, dipende dai permessi dei gruppi padre e dai permessi assegnati all'oggetto stesso. La tabella sotto descrive il principio di ottenimento del permesso risultante di un oggetto:

Permesso del gruppo padre	**Permesso del discendente sotto considerazione**	**Permesso risultante**
Concesso tutto	Concesso per alcuni oggetti	Concesso per gli oggetti del discendente
Concesso per alcuni oggetti	Concesso per alcuni oggetti	Le liste di oggetti consentiti si uniscono
Concesso per alcuni oggetti	Concesso tutto	Concesso tutto
I permessi del padre e del discendente sono quelli di divieto e uno di loro vieta tutto		Vietato tutto
Vietato per alcuni oggetti	Vietato per alcuni oggetti	Le liste di oggetti vietati si uniscono
Vietato tutto	Concesso tutto	Concesso tutto
Vietato per alcuni oggetti	Concesso tutto	Vietato per gli oggetti del padre
Vietato per alcuni oggetti	Concesso per alcuni oggetti	Dagli oggetti vietati vengono sottratti gli oggetti consentiti. Se dopo questo la lista di oggetti vietati non è vuota, il risultato è che sono vietati gli oggetti rimanenti. Altrimenti, il risultato è che sono consentiti tutti gli oggetti del discendente
Concesso per alcuni oggetti	Vietato tutto	Vietato tutto
Concesso tutto	Vietato per alcuni oggetti	Vietato per gli oggetti del discendente
Concesso per alcuni oggetti	Vietato per alcuni oggetti	Dagli oggetti consentiti vengono sottratti gli oggetti vietati. Se dopo questo la lista di oggetti consentiti è vuota, il risultato è che è vietato tutto. Altrimenti, il risultato è che sono consentiti gli oggetti rimanenti.

5.3. Gestione degli account amministratori e dei gruppi di amministratori

5.3.1. Creazione ed eliminazione degli account amministratori e di gruppi

Il nome utente amministratore deve essere unico.

Non è possibile connettere un amministratore tramite i sistemi di autenticazione esterni se sul Server esiste già un amministratore con lo stesso nome utente.

Aggiunzione di amministratori

Per poter creare nuovi account amministratori, si deve avere il permesso di **Creazione degli amministratori, dei gruppi di amministratori**.

Per aggiungere un nuovo account amministratore:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Amministratori**.
2. Nella barra degli strumenti premere l'icona **Crea account**. Si apre la finestra delle impostazioni dell'account che viene creato.
3. Nella sottosezione **Generali**, impostare i seguenti parametri:
   - Nel campo **Nome utente** indicare il nome utente amministratore da utilizzare per accedere al Pannello di controllo. Sono permesse le minuscole (a-z), le maiuscole (A-Z), le cifre (0-9), i caratteri "_" e ".".
   - Nell'elenco **Tipo di autenticazione** selezionare una delle varianti:
     - **Interna** – l'amministratore si autentica nel Pannello di controllo sulla base delle credenziali salvate nel database del Server Dr.Web.
     - **Esterna** – l'amministratore si autentica nel Pannello di controllo tramite i sistemi esterni LDAP, Active Directory, RADIUS o PAM.

Per maggiori informazioni consultare la sezione Autenticazione di amministratori.

   - Nei campi **Password** e **Digitare di nuovo la password** impostare la password di accesso al Server e al Pannello di controllo.

Nella password amministratore non possono essere utilizzati i caratteri di alfabeto nazionale.

I campi per l'impostazione della password sono attivi soltanto per gli amministratori con l'autenticazione interna.

Non hanno importanza i valori di questi campi, impostati nel Pannello di controllo per gli amministratori con l'autenticazione esterna.

- Nei campi **Cognome**, **Nome** e **Patronimico** si possono indicare i dati personali dell'amministratore.
- Dalla lista a cascata **Lingua interfaccia** selezionare la lingua dell'interfaccia del Pannello di controllo, che verrà utilizzata dall'amministratore che viene creato (di default, è la lingua impostata nel browser o l'inglese).
- Dalla lista a cascata **Formato della data** selezionare il formato che verrà utilizzato da questo amministratore quando modifica impostazioni che contengono date. Sono disponibili i seguenti formati:
  - europeo: `DD-MM-YYYY HH:MM:SS`
  - americano: `MM/DD/YYYY HH:MM:SS`
- Nel campo **Descrizione** si può impostare una descrizione dell'account.

I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

4. Nella sottosezione **Gruppi** viene impostato il gruppo padre di amministratori. Nella lista sono riportati i gruppi disponibili a cui si può assegnare l'amministratore. Un flag è spuntato di fronte al gruppo a cui verrà assegnato l'amministratore che viene creato. Di default, gli amministratori che vengono creati vengono messi nel gruppo padre dell'amministratore corrente. Per cambiare il gruppo impostato, spuntare il flag di fronte al gruppo desiderato.

   Ciascun amministratore può rientrare in solo un gruppo.

   L'amministratore eredita i permessi dal gruppo padre (v. p. Permessi degli amministratori).
5. Una volta impostati tutti i parametri necessari, premere il pulsante **Salva** per creare l'account amministratore.

Aggiunzione di gruppi di amministratori

Per poter creare gruppi di amministratori, si deve avere il permesso di **Creazione degli amministratori, dei gruppi di amministratori**.

Per aggiungere un nuovo account del gruppo di amministratori:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Amministratori**.
2. Nella barra degli strumenti premere l'icona **Crea gruppo**. Si apre la finestra delle impostazioni del gruppo che viene creato.
3. Nella sottosezione **Generali**, impostare i seguenti parametri:

- Nel campo **Gruppo** impostare il nome del gruppo di amministratori. Sono permesse le minuscole (a-z), le maiuscole (A-Z), le cifre (0-9), i caratteri "_" e ".".
- Nel campo **Descrizione** si può impostare una descrizione del gruppo.

4. Nella sottosezione **Gruppi** viene impostato il gruppo padre di amministratori. Nella lista sono riportati i gruppi disponibili che possono essere assegnati come gruppo padre. Di fronte al gruppo, di cui farà parte il gruppo che viene creato, è spuntato un flag. Di default, i gruppi che vengono creati vengono messi nel gruppo padre dell'amministratore corrente. Per cambiare il gruppo impostato, spuntare il flag di fronte al gruppo desiderato.

   Può essere assegnato solo un gruppo padre.

   Il gruppo di amministratori eredita i permessi dal gruppo padre (v. p. Permessi degli amministratori).
5. Una volta impostati tutti i parametri necessari, premere il pulsante **Salva** per creare il gruppo di amministratori.

Eliminazione di amministratori e di gruppi di amministratori

Per poter eliminare account amministratori e gruppi di amministratori, si devono avere i permessi rispettivi di **Rimozione degli account amministratori** e di **Modifica delle proprietà e della configurazione dei gruppi di amministratori**.

Per eliminare un account amministratore o un gruppo:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Amministratori**.
2. Nella lista gerarchica degli amministratori, selezionare l'account amministratore o il gruppo di amministratori che si vuole eliminare.
3. Nella barra degli strumenti premere l'icona  **Rimuovi gli oggetti selezionati**.

5.3.2. Modifica degli account amministratori e dei gruppi

Per poter modificare gli account amministratori e i gruppi di amministratori, si devono avere i permessi rispettivamente di **Modifica degli account amministratori** e di **Modifica delle proprietà e della configurazione dei gruppi di amministratori**.

Per poter modificare il proprio account, si deve avere il permesso **Modifica delle proprie impostazioni**.

I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

Modifica degli amministratori

Per modificare un account amministratore:

1. Dalla lista degli amministratori, selezionare l'account che si vuole modificare. Si apre la sezione di modifica delle proprietà.
2. Nella sottosezione **Generali** è possibile modificare i parametri che sono stati impostati durante la creazione, in particolare:
   a) Per modificare la password di accesso all'account amministratore, nella barra degli strumenti selezionare l'icona **Cambia password**.

   L'amministratore che ha i relativi permessi può modificare le password di tutti gli altri amministratori.

   Nel nome utente amministratore non possono essere utilizzati i caratteri di alfabeto nazionale.

   b) I seguenti parametri dell'amministratore sono di sola lettura:
      - Data della creazione account e dell'ultima modifica parametri,
      - **Stato** – visualizza l'indirizzo di rete dell'ultima connessione sotto questo account.
3. Nella sottosezione **Gruppi** si può cambiare il gruppo di amministratori. Nella lista sono riportati i gruppi disponibili a cui può essere assegnato l'amministratore. Un flag è spuntato di fronte al gruppo padre corrente dell'amministratore. Per cambiare il gruppo impostato, spuntare il flag di fronte al gruppo desiderato.

   Il gruppo padre deve essere assegnato obbligatoriamente a un amministratore. Ciascun amministratore può rientrare in solo un gruppo. L'amministratore eredita permessi dal gruppo padre impostato.

   V. inoltre la sottosezione Modifica dell'appartenenza.
4. Nella sottosezione **Permessi** è possibile modificare la lista delle azioni consentite per l'amministratore selezionato.

   La procedura di modifica dei permessi è riportata nella sottosezione Modifica dei permessi.
5. Per rendere effettive le modifiche apportate, premere il pulsante **Salva**.

Modifica dei gruppi di amministratori

Per modificare un gruppo di amministratori:

1. Dalla lista degli amministratori, selezionare il gruppo che si vuole modificare. Si apre la sezione di modifica delle proprietà.
2. Nella sottosezione **Generali** è possibile modificare i parametri che sono stati impostati durante la creazione.

3. Nella sottosezione **Gruppi** si può cambiare il gruppo padre. Nella lista sono riportati i gruppi disponibili che possono essere assegnati come gruppo padre. Un flag è spuntato di fronte al gruppo padre corrente. Per cambiare il gruppo impostato, spuntare il flag di fronte al gruppo desiderato.

   Il gruppo padre deve essere assegnato obbligatoriamente a un gruppo di amministratori. Il gruppo eredita permessi dal gruppo padre impostato.

   V. inoltre la sottosezione Modifica dell'appartenenza.
4. Nella sottosezione **Permessi** è possibile modificare la lista delle azioni consentite per il gruppo di amministratori selezionato.

   La procedura di modifica dei permessi è riportata nella sottosezione Modifica dei permessi.
5. Per rendere effettive le modifiche apportate, premere il pulsante **Salva**.

Modifica dell'appartenenza

Vi sono diversi modi di assegnazione del gruppo padre agli amministratori e ai gruppi di amministratori:

1. Si possono modificare le impostazioni dell'amministratore o del gruppo secondo il modo descritto sopra.
2. Si può trascinare (drag'n'drop) un amministratore o un gruppo di amministratori nella lista gerarchica sopra il gruppo il quale si desidera assegnare come gruppo padre.

Capitolo 6: Gestione integrata delle postazioni

Il metodo di gruppi è progettato per la semplificazione della gestione delle postazioni della rete antivirus.

Il raggruppamento di postazioni può servire ai seguenti scopi:

- Applicare operazioni di gruppo a tutte le postazioni che fanno parte di tale gruppo.

  Sia per un gruppo singolo che per diversi gruppi selezionati si possono avviare, visualizzare e terminare task di scansione delle postazioni che fanno parte di tale gruppo. Si possono inoltre visualizzare le statistiche (tra l'altro, infezioni, virus, avvio/terminazione, errori scansione e di installazione ecc.) e le statistiche complessive di tutte le postazioni di un gruppo o di più gruppi.
- Configurare impostazioni comuni delle postazioni attraverso il gruppo di cui fanno parte (v. p. Utilizzo dei gruppi per configurare postazioni).
- Sistemare (strutturare) la lista delle postazioni.

Si possono creare anche gruppi nidificati.

6.1. Gruppi di sistema e custom

Gruppi di sistema

Inizialmente Dr.Web Enterprise Security Suite contiene un set di gruppi di sistema predefiniti. Questi gruppi vengono creati durante l'installazione del Server Dr.Web e non possono essere eliminati. Tuttavia, se necessario, l'amministratore può nascondere la loro visualizzazione.

Ogni gruppo di sistema (salvo il gruppo **Everyone**) contiene un set di sottogruppi raggruppati secondo un determinato criterio.

Dopo che il Server è stato installato e fino a quando le postazioni non si connetteranno ad esso, soltanto il gruppo **Everyone** viene visualizzato nella lista dei gruppi di sistema. Per visualizzare tutti i gruppi di sistema, utilizzare l'opzione **Mostra gruppi nascosti** nella sezione **Impostazioni della vista albero** nella barra degli strumenti.

Everyone

Il gruppo che comprende tutte le postazioni conosciute dal Server Dr.Web. Il gruppo **Everyone** contiene le impostazioni predefinite di ogni postazione e gruppo.

Configured

Il gruppo contiene le postazioni per cui sono state definite le impostazioni individuali.

Operating system

Questa categoria dei sottogruppi visualizza i sistemi operativi attuali delle postazioni. Questi gruppi non sono virtuali e possono contenere impostazioni di postazioni ed essere gruppi primari.

- I sottogruppi della famiglia **Android**. Questa famiglia include un set dei gruppi che corrispondono ad una versione concreta del sistema operativo mobile Android.
- I sottogruppi della famiglia **OS X**. Questa famiglia include un set dei gruppi che corrispondono ad una versione concreta del sistema operativo OS X.
- Il sottogruppo **Netware**. Questo sottogruppo include le postazioni con il sistema operativo Novell NetWare.
- I sottogruppi della famiglia **UNIX**. Questa famiglia include una serie di gruppi che corrispondono agli sistemi operativi della famiglia UNIX, per esempio, Linux, FreeBSD, Solaris ecc.
- I sottogruppi della famiglia **Windows**. Questa famiglia include una serie di gruppi che corrispondono a una specifica versione del sistema operativo Windows.

Status

Il gruppo **Status** contiene gruppi nidificati che visualizzano lo stato corrente delle postazioni: se al momento sono connesse o meno al Server, nonché lo stato del software antivirus: se il software è rimosso o il periodo di utilizzo è scaduto. Questi gruppi sono virtuali e non possono contenere impostazioni od essere gruppi primari.

- Il gruppo **Deinstalled**. Non appena rimosso da una postazione il software Agent Dr.Web, la postazione viene trasferita automaticamente nel gruppo **Deinstalled**.
- Il gruppo **Deleted**. Contiene le postazioni che l'amministratore ha rimosso dal Server. È possibile recuperare queste postazioni (v. p. Rimozione e recupero della postazione).
- Il gruppo **New**. Contiene le postazioni nuove create dall'amministratore attraverso il Pannello di controllo, ma l'Agent non è ancora stato installato su di esse.
- Il gruppo **Newbies**. Contiene tutte le postazioni non confermate di cui la registrazione sul Server per il momento non è ancora stata confermata. Dopo che la registrazione verrà confermata oppure verrà negato l'accesso al Server, le postazioni verranno escluse automaticamente da questo gruppo (per dettagli v. la sezione Criteri di approvazione delle postazioni).
- Il gruppo **Offline**. Contiene tutte le postazioni non connesse al momento.
- Il gruppo **Online**. Contiene tutte le postazioni connesse al momento (che rispondono alle richieste del Server).
- Il gruppo **Update Errors**. Contiene le postazioni sui cui l'aggiornamento del software antivirus non è riuscito.

Transport

Questi sottogruppi definiscono il protocollo attraverso cui le postazioni al momento sono connesse al Server. Questi sottogruppi sono virtuali e non possono contenere impostazioni od essere gruppi primari.

- Il gruppo **TCP/IP**. Il gruppo contiene le postazioni connesse al momento attraverso il protocollo TCP/IP versione 4.
- Il gruppo **TCP/IP Version 6**. Il gruppo contiene le postazioni connesse al momento attraverso il protocollo TCP/IP versione 6.

Ungrouped

Questo gruppo contiene le postazioni che non fanno parte di nessuno dei gruppi custom.

Gruppi custom

Sono gruppi creati dall'amministratore della rete antivirus per le proprie esigenze. L'amministratore può creare propri gruppi, nonché gruppi nidificati, e può aggiungerci postazioni. Dr.Web Enterprise Security Suite non impone alcuna restrizione sui contenuti o sui nomi di tali gruppi.

Per comodità, la tabella 6-1 riassume tutti i gruppi possibili e i tipi di gruppo, nonché i parametri supportati (+) o non supportati (–) da questi gruppi.

Vengono considerati i seguenti parametri:

- **Appartenenza automatica**. Il parametro determina se è possibile includere automaticamente postazioni nel gruppo (supporto dell'appartenenza automatica), nonché se è possibile cambiare automaticamente gli elementi del gruppo nel corso del funzionamento del Server.
- **Gestione dell'appartenenza**. Il parametro determina se l'amministratore può gestire l'appartenenza al gruppo: aggiunzione o cancellazione di postazioni dal gruppo.
- **Gruppo primario**. Il parametro determina se questo gruppo può essere primario per la postazione.
- **Inclusione di impostazioni**. Il parametro determina se il gruppo può contenere impostazioni di componenti antivirus (affinché le postazioni possano ereditarle).

Tabella 6-1. Gruppi e parametri supportati

Gruppo/tipo gruppo	Parametro			
	Appartenenza automatica	Gestione dell'appartenenza	Gruppo primario	Impostazioni
Everyone	+	–	+	+

Gruppo/tipo gruppo	Parametro			
	Appartenenza automatica	Gestione dell'apparte-nenza	Gruppo pri-mario	Impostazioni
Configured	+	–	–	–
Operating System	+	–	+	+
Status	+	–	–	–
Transport	+	–	–	–
Ungrouped	+	–	–	–
Gruppi custom	–	+	+	+

Quando si utilizza un account *amministratore del gruppo*, il gruppo custom gestito da quest'amministratore viene visualizzato nella radice dell'albero gerarchico, anche se effettivamente abbia gruppo padre. In tale caso saranno disponibili tutti i gruppi figlio del gruppo gestito dall'amministratore.

6.2. Gestione dei gruppi

6.2.1. Creazione ed eliminazione di gruppi

Creazione del gruppo

Per creare un nuovo gruppo:

1. Selezionare la voce **Aggiungi una postazione o un gruppo** nella barra degli strumenti, quindi dal sottomenu selezionare la voce **Crea un gruppo**.

   Si apre la finestra di creazione del gruppo.
2. Il campo di input **Identificatore** viene riempito in modo automatico. Se necessario, si può modificarlo durante la creazione. L'identificatore non deve includere spazi. In seguito, non si può modificare l'identificatore.
3. Inserire nel campo **Nome** il nome del gruppo.
4. Per gruppi nidificati, nel campo **Gruppo padre** selezionare dalla lista a cascata un gruppo da assegnare come il gruppo padre dal quale il nuovo gruppo eredita la configurazione, se non sono indicate le impostazioni personalizzate. Per un gruppo radice (che non ha padre) lasciare questo campo vuoto, il gruppo viene aggiunto alla radice della lista gerarchica. In questo caso, il gruppo eredita le impostazioni dal gruppo **Everyone**.
5. Inserire un commento nel campo **Descrizione**.

6. Premere il pulsante **Salva**.

I gruppi creati sono inizialmente vuoti. La procedura di aggiunzione di postazioni ai gruppi è descritta nella sezione Inserimento delle postazioni in gruppi custom.

Eliminazione del gruppo

Per eliminare un gruppo esistente:

1. Selezionare il gruppo custom nella lista gerarchica del Pannello di controllo.
2. Nella barra degli strumenti premere **Generali** → **Rimuovi gli oggetti selezionati**.

> I gruppi predefiniti non si possono eliminare.

6.2.2. Modifica dei gruppi

Per modificare le impostazioni dei gruppi:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica selezionare un gruppo.
2. Aprire la sezione delle impostazioni del gruppo in uno dei seguenti modi:
   a) Fare clic sul nome di un gruppo nella lista gerarchica della rete antivirus. Nella parte destra della finestra del Pannello di controllo si apre automaticamente una sezione con le proprietà del gruppo.
   b) Selezionare la voce **Proprietà** del menu di gestione. Si apre la finestra con le proprietà del gruppo.
3. La finestra delle proprietà del gruppo contiene le schede **Generali** e **Configurazione**. I contenuti e la configurazione delle schede sono descritti sotto.

> Se si aprono le proprietà del gruppo nella parte destra della finestra del Pannello di controllo (v. punto **2.a)**) è inoltre disponibile la sezione **Informazioni sulle postazioni** in cui si trovano le informazioni generali sulle postazioni che fanno parte di tale gruppo.

4. Per salvare le modifiche apportate, premere il pulsante **Salva**.

Generali

Nella sezione **Generali** vengono riportate le seguenti informazioni:

- **Identificatore** – l'identificatore unico del gruppo. Non è modificabile.
- **Nome** – il nome del gruppo. Se necessario, si può modificare il nome di un gruppo personalizzato. Per i gruppi predefiniti il campo **Nome** non è modificabile.

- **Gruppo padre** – il gruppo padre in cui rientra questo gruppo e da cui eredita la sua configurazione, se non sono configurate le impostazioni individuali. Se nessun gruppo padre è assegnato, il gruppo eredita le impostazioni dal gruppo **Everyone**.
- **Descrizione** – un campo non obbligatorio per la descrizione del gruppo.

Informazioni sulle postazioni

Nella sezione **Informazioni sulle postazioni** vengono riportate le seguenti informazioni:

- **Postazioni** – numero totale di postazioni nel gruppo.
- **Gruppo primario per** – numero di postazioni per cui questo gruppo è primario.
- **Postazioni online** – numero di postazioni in questo gruppo che sono attualmente in rete (online).

Configurazione

Per le informazioni dettagliate su ereditarietà di impostazioni dei gruppi da parte delle postazioni per cui tale gruppo è primario, v. sezione Utilizzo dei gruppi per configurare postazioni.

Nella sezione **Configurazione** si può modificare la configurazione dei gruppi che include:

Icona	Impostazioni	Sezione con la descrizione
	Permessi degli utenti delle postazioni che ereditano quest'impostazione dal gruppo se è primario. I permessi dei gruppi vengono configurati nello stesso modo dei permessi di singole postazioni.	Permessi dell'utente della postazione
	Calendario centralizzato per l'esecuzione di task sulle postazioni che ereditano quest'impostazione dal gruppo se è primario. Il calendario dei gruppi viene configurato nello stesso modo del calendario di singole postazioni.	Calendario dei task della postazione
	Chiavi di licenza per le postazioni per cui questo gruppo è primario.	Gestione licenze
	Restrizioni di distribuzione di aggiornamenti di software antivirus sulle postazioni che ereditano quest'impostazione dal gruppo se è primario.	Limitazione degli aggiornamenti delle postazioni
	Lista dei componenti da installare sulle postazioni che ereditano questa impostazione dal gruppo se è primario. La lista di componenti per i gruppi viene modificata nello stesso modo della lista di componenti per le postazioni.	Componenti da installare del pacchetto antivirus
	Configurazione della sistemazione automatica di postazioni in tale gruppo. È disponibile solo per i gruppi custom.	Configurazione dell'appartenenza

Icona	Impostazioni	Sezione con la descrizione
		automatica a un gruppo
	Configurazioni dei componenti di pacchetto antivirus. I componenti di pacchetto antivirus per il gruppo vengono configurati nello stesso modo dei componenti per una postazione.	Configurazione dei componenti antivirus

Per i gruppi in cui sono definite impostazioni individuali nella sezione **Configurazione** viene indicato il numero di gruppi nidificati con l'ereditarietà interrotta e con le proprie impostazioni individuali, se ci sono. Quando si fa clic su questa opzione, si apre una finestra con una lista dei gruppi per cui sono indicati i loro nomi e identificatori.

6.3. Inserimento delle postazioni in gruppi custom

Dr.Web Enterprise Security Suite mette a disposizione i seguenti modi per sistemare postazioni in gruppi custom:

1. Inserimento manuale delle postazioni in gruppi.
2. Utilizzo delle regole di appartenenza automatica a un gruppo.

6.3.1. Inserimento manuale delle postazioni in gruppi

Vi sono diversi modi per aggiungere postazioni manualmente ai gruppi personalizzati:

1. Modificare le impostazioni della postazione.
2. Trascinare le postazioni nella lista gerarchica (drag-and-drop).

Per modificare la lista dei gruppi, di cui fa parte la postazione, tramite le impostazioni della postazione:

1. Selezionare la voce **Rete antivirus**del menu principale, nella finestra che si è aperta nella lista gerarchica premere il nome della postazione.
2. Si apre la barra delle proprietà della postazione. Inoltre, si può aprire la sezione delle proprietà della postazione selezionando nel menu di gestione la voce **Proprietà**.
3. Nel pannello **Proprietà della postazione** che si è aperto, passare alla sezione **Gruppi**.

   Nella lista **Appartenenza** sono elencati tutti i gruppi di cui la postazione fa parte e in cui essa può essere inclusa.
4. Per aggiungere la postazione a un gruppo custom, spuntare il flag di fronte a questo gruppo nella lista **Appartenenza**.
5. Per eliminare la postazione da un gruppo custom, togliere il flag di fronte a questo gruppo nella lista **Appartenenza**.

Non è possibile eliminare postazioni dai gruppi predefiniti.

6. Per salvare le modifiche apportate, premere il pulsante **Salva**.

Inoltre nella sezione **Proprietà** della postazione, è possibile assegnare il gruppo primario alla postazione (per maggiori informazioni v. Ereditarietà della configurazione da parte della postazione. Gruppi primari).

Per modificare la lista dei gruppi, di cui fa parte la postazione, tramite la lista gerarchica:

1. Selezionare la voce **Rete antivirus** del menu principale e aprire la lista gerarchica dei gruppi e delle postazioni.
2. Per aggiungere una postazione a un gruppo custom, premere e tenere premuto il tasto CTRL e trascinare la postazione con il mouse nel gruppo necessario (drag'n'drop).
3. Per spostare la postazione da un gruppo custom in un altro, trascinarla con il mouse (drag'n'drop) dal gruppo custom da cui la postazione viene eliminata nel gruppo custom a cui la postazione viene aggiunta.

Se la postazione viene trascinata da un gruppo predefinito secondo la voce 2 o 3, essa viene aggiunta al gruppo custom e non viene eliminata dal gruppo predefinito.

6.3.2. Configurazione dell'appartenenza automatica a un gruppo

Dr.Web Enterprise Security Suite dà la possibilità di configurare le regole di inclusione automatica di postazioni in gruppi.

Per configurare le regole di inclusione automatica di postazioni in un gruppo:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo.
2. Dalla lista gerarchica della rete antivirus selezionare il gruppo custom per cui si vogliono creare regole di appartenenza.
3. Passare nella sezione di modifica delle regole di appartenenza in uno dei seguenti modi:
   - Nella barra delle proprietà del gruppo nella parte destra della finestra nella sezione **Configurazione** premere **Regole di appartenenza al gruppo**.
   - Nel menu di gestione, nella sezione **Generali** selezionare la voce **Regole di appartenenza al gruppo**.
   - Nel menu di gestione, nella sezione **Generali** selezionare la voce **Proprietà**, passare alla scheda **Configurazione**, premere **Regole di appartenenza al gruppo**.
4. Nella finestra che si è aperta, impostare una lista delle condizioni, verificate le quali, le postazioni verranno inserite in questo gruppo:
   a) Se per un gruppo prima non sono state impostate le regole di appartenenza, premere **Aggiungi regola**.

b) Spuntare il flag **Imposta il gruppo come primario** affinché il gruppo per cui viene creata la regola venga impostato automaticamente come il gruppo primario per tutte le postazioni che verranno trasferite in questo gruppo in base a questa regola.

c) Per ciascun blocco delle regoli definire le seguenti impostazioni:

- Selezionare una delle opzioni che imposta il principio di unione delle regole nel blocco: **Soddisfa tutte le condizioni**, **Soddisfa qualsiasi delle condizioni**, **Non soddisfa alcuna delle condizioni**.
- Dalle liste a cascata delle condizioni selezionare: uno dei parametri della postazione che verrà controllato per la corrispondenza alle condizioni; il principio di corrispondenza a questa condizione e, se il parametro della postazione lo sottintende, inserire la stringa della condizione.

Se viene impostato il parametro **Piattaforma della postazione**, è necessario selezionare dalla lista il nome completo finale della piattaforma che si trova all'ultimo livello della gerarchia della vista ad albero. Tutti i livelli più alti sono solo per la convenienza del raggruppamento della lista delle piattaforme e di per sé non sono valori del parametro **Piattaforma della postazione**.

Per esempio: **Windows** e **Windows 7** non sono valori validi del parametro. La scelta corretta sarà **Windows 7 Professional Edition**.

Se viene impostato il parametro **LDAP DN da Active Directory**, è necessario:

1. Attivare il task **Sincronizzazione con Active Directory** nel calendario di Server (sezione **Amministrazione** → **Scheduler di Server Dr.Web**).
2. Nelle regole di appartenenza come la stringa della condizione per il parametro **LDAP DN da Active Directory** impostare il valore DN richiesto, per esempio:
   `OU=OrgUnit,DC=Department,DC=domain,DC=com`

- Per aggiungere un'altra condizione a questo blocco, premere  a desta della stringa della condizione.

d) Per aggiungere un nuovo blocco di regole, premere  a destra del blocco. Inoltre, impostare il principio di unione di questo blocco di condizioni con gli altri blocchi:

- **E** – le condizioni dei blocchi devono essere soddisfatte allo stesso tempo.
- **O** – devono essere soddisfatte le condizioni di almeno uno dei blocchi.

Nell'impostare della stringa di condizioni è possibile utilizzare espressioni regolari.

L'utilizzo delle espressioni regolari è descritto in breve nel documento **Allegati**, sezione Allegato J. Utilizzo di espressioni regolari in Dr.Web Enterprise Security Suite.

Notare: quando si utilizzano i parametri del filtro **inizia con** e **finisce con**, la stringa di condizione viene integrata automaticamente con i seguenti caratteri di controllo rispettivamente: `^` (la stringa inizia con la sequenza dei caratteri indicati) o `$` (la stringa finisce con la sequenza dei caratteri indicati).

Per fare pieno uso delle espressioni regolari, è consigliato selezionare il parametro del filtro **contiene**.

5. Per salvare ed applicare le regole impostate, premere uno dei seguenti pulsanti:
   - **Applica adesso** – per salvare le regole di appartenenza impostate e per applicare queste regole allo stesso tempo a tutte le postazioni registrate su questo Server. In caso di un grande numero di postazioni connesse al Server, l'esecuzione di quest'azione potrebbe richiedere un certo tempo. Le regole di nuovo raggruppamento di postazioni vengono applicate a tutte le postazioni già registrate subito quando viene impostata l'azione e verranno applicate a tutte le postazioni, anche a quelle che verranno registrate sul Server per la prima volta, al momento della loro connessione.
   - **Applica alla connessione delle postazioni** – per salvare le regole di appartenenza impostate e per applicare queste regole alle postazioni al momento quando si connettono al Server. Le regole di nuovo raggruppamento di postazioni vengono applicate a tutte le postazioni già registrate al momento della loro successiva connessione al Server e verranno applicate a tutte le postazioni che vengono registrate sul Server per la prima volta al momento della loro prima connessione.
6. Quando vengono impostate le regole di appartenenza automatica per un gruppo custom, nella lista gerarchica della rete antivirus accanto all'icona di questo gruppo compare l'icona , a condizione che sia spuntato il flag **Mostra l'icona di regole appartenenza al gruppo** nella lista **Impostazioni della vista albero** nella barra degli strumenti.

Se una postazione è stata trasferita in un gruppo custom sulla base delle regole di appartenenza in modo automatico, è inutile eliminare manualmente la postazione da questo gruppo in quanto al momento della successiva connessione al Server la postazione verrà restituita automaticamente a questo gruppo.

Per eliminare le regole di inclusione automatica di postazioni in un gruppo:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo.
2. Dalla lista gerarchica della rete antivirus selezionare il gruppo custom per cui si vogliono eliminare le regole di appartenenza.
3. Eseguire una delle seguenti azioni:
   - Nella barra degli strumenti premere il pulsante **Rimuovi le regole di appartenenza**.

- Nella barra delle proprietà del gruppo nella parte destra della finestra nella sezione **Configurazione** premere **Rimuovi le regole di appartenenza**.
- Nel menu di gestione, nella sezione **Generali** selezionare la voce **Proprietà**, passare alla scheda **Configurazione**, premere **Rimuovi le regole di appartenenza**.

4. Dopo la rimozione delle regole di appartenenza del gruppo, tutte le postazioni sistemate in questo gruppo sulla base delle regole di appartenenza verranno eliminate da questo gruppo. Se ad alcune delle postazioni questo gruppo è stato assegnato dall'amministratore come il gruppo primario, al momento dell'eliminazione delle postazioni dal gruppo ad esse verrà assegnato come primario il gruppo **Everyone**.

6.4. Utilizzo dei gruppi per configurare postazioni

Le postazioni possono avere impostazioni:

1. Ereditate dal gruppo primario.
2. Definite in modo individuale.

Ereditarietà delle impostazioni

Quando viene creato un nuovo gruppo, esso eredita le impostazioni dal gruppo padre o dal gruppo **Everyone** se il gruppo padre non è assegnato.

Quando viene creata una nuova postazione, essa eredita le impostazioni dal gruppo primario.

> Per maggiori informazioni v. p. Ereditarietà della configurazione da parte della postazione. Gruppi primari.

Quando vengono visualizzate o modificate le impostazioni di una postazione, ereditate dal gruppo primario, nelle relative finestre viene segnalato che tali impostazioni sono ereditate dal gruppo primario.

Si possono impostare varie configurazioni per vari gruppi e postazioni, modificando le impostazioni corrispondenti.

Impostazioni individuali

Per configurare in modo individuale una postazione, modificare la relativa sezione delle impostazioni (v. p. Proprietà della postazione – Configurazione). In tale caso nella sezione delle impostazioni verrà mostrato che questa impostazione è configurata individualmente per questa postazione.

Se una postazione ha delle impostazioni personalizzate, le impostazioni del gruppo primario ed eventuali modifiche non valgono per la postazione.

È possibile tornare alla configurazione ereditata dal gruppo primario. Per farlo, premere il pulsante **Rimuovi le impostazioni personalizzate** nella barra degli strumenti del Pannello di controllo nella sezione delle impostazioni corrispondenti o nella sezione delle proprietà della postazione.

6.4.1. Ereditarietà della configurazione da parte della postazione

Principio di ereditarietà delle impostazioni

Quando viene creata una postazione nuova, essa eredita la sua configurazione da uno dei gruppi di cui fa parte. Tale gruppo si chiama primario.

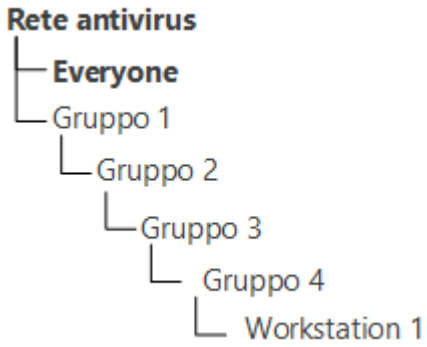
Se vengono modificate le impostazioni del gruppo primario, le postazioni che fanno parte del gruppo ereditano le modifiche, salvo i casi in cui le postazioni hanno impostazioni individuali. Quando viene creata una postazione, è possibile indicare quale gruppo verrà considerato come primario. Di default, il gruppo primario è **Everyone**.

> Se il gruppo primario non è **Everyone** e se il gruppo primario assegnato, che è un nodo radice della lista gerarchica della rete antivirus, non ha impostazioni personalizzate, la nuova postazione eredita le impostazioni del gruppo **Everyone**.

Se ci sono dei gruppi nidificati, se per la postazione non sono state definite impostazioni personalizzate, essa eredita la configurazione secondo la struttura dei gruppi nidificati. La ricerca viene eseguita dal basso in alto dell'albero gerarchico, partendo dal gruppo primario della postazione, dal suo gruppo padre e così via fino all'elemento radice dell'albero. Se durante la ricerca non sono state scoperte impostazioni personalizzate, la postazione eredita le impostazioni del gruppo **Everyone**.

Per esempio:

La struttura della lista gerarchica è il seguente albero:



Il Gruppo `Group4` è primario per la postazione `Station1`. Quando la postazione `Station1` eredita impostazioni, la ricerca delle impostazioni viene eseguita nel seguente ordine: `Workstation 1 → Gruppo 4 → Gruppo 3 → Gruppo 2 → Gruppo 1 → Everyone`.

Di default, la struttura di rete è presentata in modo tale da dimostrare l'appartenenza della postazione a tutti i gruppi di cui fa parte. Se si vuole visualizzare nella directory di rete l'appartenenza della postazione solo ai gruppi primari, nella barra degli strumenti del Pannello di controllo nella voce **Impostazioni della vista albero** togliere il flag **Appartenenza a tutti i gruppi**.

Assegnazione del gruppo primario

Vi sono diversi modi per assegnare il gruppo primario alla postazione e a un gruppo di postazioni.

Per assegnare il gruppo primario a una postazione:

1. Selezionare la voce **Rete antivirus** del menu principale, nella finestra che si è aperta nella lista gerarchica premere il nome della postazione.
2. Si apre la barra delle proprietà della postazione. Inoltre, si può aprire la sezione delle proprietà della postazione selezionando nel menu di gestione la voce **Proprietà**. Nella finestra che si è aperta passare alla sottosezione **Gruppi**.
3. Se è necessario cambiare il gruppo primario, premere l'icona del gruppo richiesto nella sezione Appartenenza. Dopo questo, sull'icona del gruppo compare **1**.
4. Premere il pulsante **Salva**.

Per assegnare il gruppo primario a diverse postazioni:

1. Selezionare la voce **Rete antivirus** del menu principale, nella finestra che si è aperta nella lista gerarchica premere i nomi delle postazioni (si possono selezionare anche gruppi – in tale caso l'azione verrà applicata a tutte le postazioni che ne fanno parte) a cui si desidera assegnare un gruppo primario. Per selezionare diverse postazioni o gruppi, si può utilizzare la selezione con il mouse, premendo i tasti della tastiera CTRL o MAIUSCOLO.
2. Nella barra degli strumenti premere **Generali** → **Imposta il gruppo primario per le postazioni**. Si apre la finestra con una lista dei gruppi che possono essere assegnati come primari a queste postazioni.
3. Per indicare il gruppo primario, premere il nome del gruppo.

Si può impostare il gruppo come primario per tutte le postazioni che ne fanno parte. Per farlo, selezionare il gruppo richiesto nella lista gerarchica, dopodiché nella barra degli strumenti del Pannello di controllo premere **Generali** → **Imposta questo gruppo come primario**.

6.4.2. Copiatura delle impostazioni in altri gruppi/postazioni

Le impostazioni riguardanti i componenti antivirus, calendari, permessi degli utenti e le altre impostazioni di un gruppo o di una postazione possono essere copiate (propagate) in uno o più gruppi e postazioni.

Per copiare le impostazioni:

1. Premere il pulsante **Propaga queste impostazioni verso un altro oggetto**:
    nella finestra di modifica della configurazione del componente antivirus,
    nella finestra di modifica del calendario,
    nella finestra di configurazione delle limitazioni degli aggiornamenti,
    nella finestra dei componenti da installare,
    nella finestra di configurazione dei permessi degli utenti della postazione.
   Si apre la finestra con la lista gerarchica della rete antivirus.
2. Selezionare nella lista i gruppi e le postazioni verso cui si desidera propagare le impostazioni.
3. Per poter apportare le modifiche alla configurazione di questi gruppi, premere il pulsante **Salva**.

6.5. Comparazione delle postazioni e dei gruppi

Si possono comparare le postazioni e i gruppi secondo i parametri principali.

Per comparare diversi oggetti della rete antivirus:

1. Selezionare la voce **Rete antivirus** del menu principale, nella finestra che si è aperta nella lista gerarchica selezionare oggetti da confrontare. Per farlo, utilizzare i tasti della tastiera CTRL e SHIFT. Sono possibili le seguenti varianti:
   - scelta di diverse postazioni – per comparare le postazioni selezionate;
   - scelta di diversi gruppi – per comparare i gruppi selezionati e tutti i gruppi nidificati;
   - scelta di diverse postazioni e gruppi – per comparare tutte le postazioni: sia quelle selezionate direttamente nella lista gerarchica che quelle che fanno parte dei gruppi selezionati e dei relativi gruppi nidificati.
2. Nel menu di gestione premere la voce **Comparazione**.
3. Si apre una tabella comparativa per gli oggetti selezionati.
   - Parametri di confronto per i gruppi:
     - **Postazioni** – numero totale di postazioni nel gruppo.
     - **Postazioni online** – numero di postazioni attive al momento.
     - **Gruppo primario per** – numero di postazioni per cui il gruppo selezionato è quello primario.
     - **Configurazione individuale** – una lista dei componenti che hanno le impostazioni individuali, non ereditate dal gruppo padre.
   - Parametri di confronto per le postazioni:
     - **Data di creazione** della postazione.
     - **Gruppo primario** per la postazione.

- **Configurazione individuale** – una lista dei componenti che hanno le impostazioni individuali, non ereditate dal gruppo primario.
- **Componenti installati** – una lista dei componenti antivirus installati sulla postazione.

Capitolo 7: Gestione delle postazioni

La rete antivirus gestita tramite Dr.Web Enterprise Security Suite consente di configurare in maniera centralizzata i pacchetti antivirus sulle postazioni. Dr.Web Enterprise Security Suite consente di:

- configurare le impostazioni degli elementi antivirus,
- configurare il calendario di esecuzione dei task di scansione,
- avviare singoli task su postazioni a prescindere dalle impostazioni del calendario,
- avviare il processo di aggiornamento di postazioni, anche dopo un errore di aggiornamento con il resettaggio dello stato di errore.

In particolare, l'amministratore della rete antivirus può lasciare all'utente di postazione i permessi per la configurazione indipendente del software antivirus e per l'avvio dei task, può proibire tali attività o limitarle in gran parte.

Le modifiche nella configurazione di una postazione si possono apportare perfino quando la postazione non è disponibile al Server. Queste modifiche verranno accettate dalla postazione non appena si riconnetterà al Server.

7.1. Gestione degli account di postazioni

7.1.1. Criteri di approvazione delle postazioni

> La procedura di creazione della postazione attraverso il Pannello di controllo è descritta nella **Guida all'installazione**, p. Creazione di nuovo account.

La possibilità di gestire l'autenticazione delle postazioni su Server Dr.Web dipende dai seguenti parametri:

1. Se quando l'Agent veniva installato su postazione, il flag **Autenticazione manuale sul server** era deselezionato, la modalità di accesso delle postazioni al Server viene determinata sulla base delle impostazioni definite sul Server (si usa di default), v. sotto.
2. Se quando l'Agent veniva installato su postazione, il flag **Autenticazione manuale sul server** era selezionato ed erano impostati i parametri **Identificatore** e **Password**, quando la postazione si connette al Server, viene autenticata automaticamente a prescindere dalle impostazioni del Server (si usa di default nell'installazione di Agent mediante il pacchetto di installazione `drweb-esuite-install` – v. **Guida all'installazione**, p. File di installazione).

> Come configurare il tipo di autenticazione dell'Agent al momento dell'installazione viene descritto nel **Manuale dell'utente**.

Per modificare la modalità di accesso delle postazioni al Server Dr.Web:

1. Aprire le impostazioni di Server. Per farlo, selezionare la voce **Amministrazione** del menu principale, nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione del Server Dr.Web**.
2. Nella scheda **Generali** nella lista a cascata **Modalità di registrazione dei nuovi arrivi** selezionare uno dei seguenti valori:
   - **Conferma l'accesso manualmente** (modalità predefinita, se non modificata durante l'installazione del Server),
   - **Sempre nega l'accesso**,
   - **Consenti l'accesso automaticamente**.

Conferma manuale dell'accesso

In modalità **Conferma l'accesso manualmente** le nuove postazioni vengono inserite nel sottogruppo di sistema **Newbies** del gruppo **Status** e ci restano fino a quando non verranno considerate dall'amministratore.

Per gestire l'accesso delle postazioni non confermate:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo. Selezionare postazioni nell'albero di rete antivirus nel gruppo **Status** → **Newbies**.

   Il gruppo **Status** → **Newbies** è disponibile nell'albero di rete antivirus soltanto se sono soddisfatte le seguenti condizioni:

   1. Nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Generali** per il parametro **Modalità di registrazione dei nuovi arrivi** è impostato il valore **Conferma l'accesso manualmente**.
   2. All'amministratore è concesso il permesso **Approvazione di nuovi arrivi**.

2. Per configurare l'accesso al Server, nella barra degli strumenti nella sezione **Postazioni non confermate** impostare l'azione che verrà applicata alle postazioni selezionate:

   Consenti alle postazioni selezionate di accedere e imposta gruppo primario – per confermare l'accesso della postazione al Server e per assegnarle un gruppo primario dalla lista proposta.

   Annulla l'azione da eseguire al momento di connessione – per annullare l'operazione con una postazione non confermata, che è stata precedentemente impostata per essere eseguita al momento quando la postazione si connetterà al Server.

   Proibisci alle postazioni selezionate di accedere – per proibire alla postazione di accedere al Server.

Negazione di accesso automatica

In modalità **Sempre nega l'accesso** il Server nega l'accesso se riceve le richieste di nuove postazioni. L'amministratore deve creare gli account di postazioni manualmente e assegnare loro le password di accesso.

Consenti l'accesso automaticamente

In modalità **Consenti l'accesso automaticamente** tutte le postazioni che richiedono l'accesso al Server vengono approvate automaticamente senza ulteriori richieste inviate all'amministratore. In questo caso come gruppo primario viene assegnato il gruppo impostato nella lista a cascata **Gruppo primario** nella sezione **Configurazione del Server Dr.Web** nella scheda **Generali**.

7.1.2. Rimozione e recupero della postazione

Rimozione di postazioni

Per rimuovere l'account di una postazione:

1. Selezionare la voce del menu principale **Rete antivirus**, nella finestra che si è aperta, nella barra degli strumenti fare clic su **Generali** → **Rimuovi gli oggetti selezionati**.
2. Si apre la finestra di conferma della rimozione della postazione. Fare clic su **OK**.

Dopo la rimozione delle postazioni dalla lista gerarchica, esse vengono collocate nella tabella delle postazioni rimosse, da cui è possibile recuperare oggetti attraverso il Pannello di controllo.

Recupero di postazioni

Per recuperare l'account di una postazione:

1. Selezionare la voce **Rete antivirus** del menu principale, nella finestra che si è aperta, nella lista gerarchica selezionare la postazione rimossa o alcune postazioni che si vogliono recuperare.

   Tutte le postazioni rimosse si trovano nel sottogruppo **Deleted** del gruppo **Status**.

2. Nella barra degli strumenti selezionare la voce **Generali** → **Recupera le postazioni rimosse**.
3. Si apre la sezione di recupero di postazioni rimosse. Si possono impostare i seguenti parametri di postazione che verranno assegnati alla postazione recuperata:
   - **Gruppo primario** – selezionare il gruppo primario a cui verrà aggiunta la postazione recuperata. Di default, è selezionato il gruppo primario impostato per la postazione prima della rimozione.

Se vengono recuperate più postazioni simultaneamente, di default è selezionata l'opzione **Ex gruppo primario** che significa che per ciascuna postazione recuperata verrà impostato il gruppo primario a cui apparteneva prima della rimozione. Se viene selezionato un determinato gruppo, per tutte le postazioni recuperate verrà impostato lo stesso gruppo.

- Nella sezione **Appartenenza** si può modificare l'elenco dei gruppi di cui la postazione farà parte. Di default, è impostato l'elenco dei gruppi a cui la postazione apparteneva prima della rimozione. Nella lista **Appartenenza** è riportato l'elenco dei gruppi in cui si può includere la postazione. Spuntare i flag accanto ai gruppi in cui si desidera includere la postazione.

4. Per recuperare la postazione con i parametri impostati, fare clic sul pulsante **Recupera**.

7.1.3. Unione delle postazioni

Quando vengono eseguite operazioni con il database o viene reinstallato il software di postazioni antivirus, nella lista gerarchica della rete antivirus potrebbero comparire diverse postazioni con lo stesso nome (solo uno di questi sarà correlato con la postazione antivirus corrispondente).

Per eliminare i nomi duplicati di postazioni:

1. Selezionare tutti i nomi duplicati della stessa postazione. Per farlo, utilizzare il tasto CTRL.
2. Nella barra degli strumenti selezionare **Generali** → **Unisci le postazioni**.
3. Nella colonna scegliere la postazione che verrà considerata master. Tutte le altre postazioni verranno eliminate, e i loro dati verranno attribuiti a quella scelta.
4. Nella colonna scegliere la postazione, le cui configurazioni verranno impostate per la postazione master scelta.
5. Premere **Salva**.

7.2. Impostazioni generali della postazione

7.2.1. Proprietà della postazione

Proprietà della postazione

Per visualizzare e per modificare le proprietà di una postazione:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica selezionare una postazione.
2. Aprire la sezione delle impostazioni della postazione in uno dei seguenti modi:
   a) Premere il nome della postazione nella lista gerarchica della rete antivirus. Nella parte destra della finestra del Pannello di controllo si apre automaticamente una sezione con le proprietà della postazione.

b) Selezionare la voce **Proprietà** del menu di gestione. Si apre la finestra con le proprietà della postazione.

3. La finestra delle proprietà della postazione contiene i seguenti gruppi di parametri: **Generali**, **Configurazione**, **Gruppi**, **Sicurezza**, **Posizione**. I loro contenuti e la loro configurazione sono descritti sotto.
4. Per salvare le modifiche apportate, premere il pulsante **Salva**.

Eliminazione delle impostazioni individuali della postazione

Per eliminare le impostazioni individuali di una postazione:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica selezionare una postazione e nella barra degli strumenti premere **Generali** → **Rimuovi le impostazioni personalizzate**. Si apre l'elenco delle impostazioni di questa postazione, le impostazioni individuali sono contrassegnate con dei flag.
2. Lasciare le spunte ai flag accanto alle impostazioni individuali che si vogliono rimuovere. Togliere le spunte ai flag accanto alle impostazioni che si vogliono mantenere individuali. Premere **Rimuovi**. Per le impostazioni contrassegnate con i flag verrà ripristinata l'ereditarietà dal gruppo primario.

7.2.1.1. Generali

Nella sezione **Generali** vengono riportati i seguenti campi di sola lettura:

- **Identificatore** – identificatore unico della postazione.
- **Nome** – nome della postazione.
- **Data di creazione** – data di creazione della postazione sul Server.
- **Ultimo accesso** – data dell'ultima connessione di questa postazione a Server.

Inoltre, si possono impostare o modificare i valori dei seguenti campi:

- Nel campo **Password** impostare una password per l'autenticazione della postazione sul Server (è necessario ripetere la stessa password nel campo **Digita di nuovo la password**). Quando la password viene cambiata, affinché l'Agent possa connettersi, è necessario fare la stessa procedura nelle impostazioni della connessione dell'Agent sulla postazione.
- Nel campo **Descrizione** si possono inserire le informazioni supplementari circa la postazione.

> I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

Inoltre, in questa sezione sono riportati i seguenti link:

- Nella voce **File di installazione** – un link per il download dell'installer di Agent per questa postazione.

Subito dopo la creazione della postazione fino al momento quando verrà impostato il sistema operativo della postazione, nella sezione di download del pacchetto, i link sono riportati separatamente per tutti i SO supportati da Dr.Web Enterprise Security Suite.

- Nella voce **File di configurazione** – un link per il download del file con le impostazioni di connessione al Server Dr.Web per le postazioni Android, OS X e Linux.

7.2.1.2. Configurazione

Nella sezione **Configurazione** si può modificare la configurazione delle postazioni, che include:

Icona	Impostazioni	Sezione con la descrizione
	Permessi dell'utente della postazione	Permessi dell'utente della postazione
	Orario centralizzato dell'avvio dei task sulla postazione	Calendario dei task della postazione
	Chiavi di licenza per la postazione	Gestione licenze
	Limitazioni di propagazione degli aggiornamenti del software antivirus	Limitazione degli aggiornamenti delle postazioni
	Lista dei componenti da installare	Componenti da installare del pacchetto antivirus
	Impostazioni dei componenti di pacchetto antivirus per questa postazione	Configurazione dei componenti antivirus

Inoltre, nel Pannello di controllo sono disponibili i pulsanti di eliminazione di impostazioni individuali. Si trovano a destra dei relativi pulsanti di configurazione. Quando viene eliminata la configurazione individuale di una postazione, viene ristabilita la configurazione ereditata dal gruppo primario.

Se vengono modificate le impostazioni di SpIDer Gate e/o di Office control, si deve tenere presente che le impostazioni di questi componenti sono interrelate, dunque se le impostazioni individuali di uno di essi sono state rimosse tramite il pulsante  **Rimuovi le impostazioni personalizzate**, le impostazioni dell'altro componente anche verranno rimosse (viene impostata l'ereditarietà delle impostazioni dal gruppo padre).

7.2.1.3. Gruppi

Nella sezione **Gruppi** viene configurata una lista dei gruppi di cui fa parte questa postazione. Nella lista **Appartenenza** sono elencati tutti i gruppi di cui la postazione fa parte e in cui essa può essere inclusa.

Per gestire l'appartenenza di una postazione, è necessario:

1. Per aggiungere la postazione a un gruppo custom, spuntare il flag di fronte a questo gruppo nella lista **Appartenenza**.
2. Per eliminare la postazione da un gruppo custom, togliere il flag di fronte a questo gruppo nella lista **Appartenenza**.

   Non è possibile eliminare postazioni dai gruppi predefiniti.

3. Se è necessario assegnare un altro gruppo primario, premere l'icona del gruppo desiderato nella sezione Appartenenza. Dopo questo, sull'icona del gruppo compare **1**.

7.2.1.4. Sicurezza

Nella sezione **Sicurezza** vengono impostate le restrizioni sugli indirizzi di rete da cui l'Agent installato su questa postazione può accedere al Server.

Per consentire tutte le connessioni, togliere il flag da **Usa questa lista di accesso**. Per impostare liste di indirizzi consentiti o bloccati, spuntare questo flag.

Per consentire l'accesso da un determinato indirizzo TCP, includerlo nella lista **TCP: Consentito** o **TCPv6: Consentito**.

Per proibire qualche indirizzo TCP, includerlo nella lista **TCP: Negato** o **TCPv6: Negato**.

Per modificare gli indirizzi nella lista:

1. Inserire un indirizzo di rete nel relativo campo nel seguente formato: <*indirizzo IP*>/[<*prefisso rete*>].
2. Per aggiungere un nuovo campo di indirizzo, premere il pulsante  della sezione corrispondente.
3. Per eliminare un campo, premere il pulsante  di fronte all'indirizzo da eliminare.
4. Per applicare le impostazioni, premere il pulsante **Salva**.

Esempio di utilizzo del prefisso:

1. Il prefisso 24 sta per la maschera di rete: `255.255.255.0`

   Contiene 254 indirizzi.

Gli indirizzi di host in queste reti sono del tipo: `195.136.12.*`

2. Il prefisso 8 sta per la maschera di rete `255.0.0.0`

   Contiene fino a 16387064 indirizzi (256*256*256).

   Gli indirizzi di host in queste reti sono del tipo: `125.*.*.*`

Inoltre, si possono eliminare gli indirizzi dalla lista e modificare gli indirizzi inseriti nella lista.

Gli indirizzi non inclusi in nessuna lista vengono consentiti o proibiti a seconda della selezione del flag **Priorità di negazione**. Se il flag è selezionato, la lista **Negato** ha la precedenza rispetto alla lista **Consentito**. Gli indirizzi non inclusi in nessuna lista o inclusi in tutte e due vengono proibiti. Vengono consentiti soltanto gli indirizzi che sono inclusi nella lista **Consentito** e non sono inclusi nella lista **Negato**.

7.2.1.5. Posizione

Nella scheda **Posizione** si possono indicare le informazioni supplementari circa la posizione fisica della postazione.

Inoltre, in questa scheda su può visualizzare la posizione della postazione su una mappa.

Per visualizzare la posizione della postazione sulla mappa:

1. Inserire nei campi **Latitudine** e **Longitudine** le coordinate geografiche della postazione nel formato gradi decimali (Decimal Degrees).
2. Premere il pulsante **Salva** per memorizzare i dati inseriti.
3. Nella scheda **Posizione** viene visualizzata l'anteprima della mappa OpenStreetMaps con un'etichetta corrispondente alle coordinate inserite.

   Se l'anteprima non può essere caricata, viene visualizzato il testo **Mostra sulla mappa**.
4. Per visualizzare la mappa di grandezza piena, fare clic sull'anteprima o sul testo **Mostra sulla mappa**.

7.2.2. Componenti installati del pacchetto antivirus

Componenti

Per scoprire quali componenti del pacchetto antivirus sono installati su una postazione:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
2. Dal menu di gestione che si è aperto selezionare dalla sottosezione **Generali** la voce **Componenti installati**.

3. Si apre la finestra con le informazioni circa i componenti installati: nome del componente; tempo di installazione; indirizzo del Server da cui è stato installato questo componente; directory di installazione del componente sulla postazione.

L'elenco dei componenti installati dipende da:

- Componenti il cui utilizzo è consentito dalla chiave di licenza.
- SO della postazione.
- Impostazioni definite dall'amministratore sul Server della rete antivirus. L'amministratore può cambiare l'elenco dei componenti del pacchetto antivirus sulla postazione sia prima dell'installazione dell'Agent che in qualsiasi momento dopo l'installazione (v. Componenti da installare del pacchetto antivirus).

Sui server che svolgono le funzioni di rete critiche (controller di dominio, server di distribuzione licenze ecc.), non è consigliabile installare i componenti SpIDer Gate, SpIDer Mail e Firewall Dr.Web per evitare eventuali conflitti dei servizi di rete e dei componenti interni dell'antivirus Dr.Web.

Database dei virus

Per scoprire quali database dei virus sono installati su una postazione:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione.
2. Dal menu di gestione che si è aperto selezionare dalla sottosezione **Statistiche** la voce **Database dei virus**.
3. Si apre la finestra con le informazioni circa i database dei virus installati: nome del file di un concreto database dei virus; versione del database dei virus; data di creazione del database dei virus; numero di record nel database dei virus.

Se la visualizzazione della voce **Database dei virus** è disattivata, per attivarla, selezionare la voce **Amministrazione** del menu principale, nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione del Server Dr.Web**. Nella scheda **Statistiche** spuntare i flag **Stato dei database dei virus** e **Stato delle postazioni**, dopodiché riavviare il Server.

7.2.3. Hardware e software sulle postazioni SO Windows®

Dr.Web Enterprise Security Suite consente di accumulare e di visualizzare informazioni circa gli hardware e i software delle postazioni SO Windows protette.

Per raccogliere le informazioni circa gli hardware e i software delle postazioni:

1. Attivare la raccolta delle statistiche sul Server:
   a) Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
   b) Selezionare la voce del menu di gestione **Configurazione del Server Dr.Web**.

c) Nelle impostazioni del Server aprire la scheda **Statistiche** e spuntare il flag **Elenco di hardware e software**, se la spunta è tolta.

d) Per accettare le modifiche apportate, premere **Salva** e riavviare il Server.

2. Consentire la raccolta delle statistiche sulle postazioni:

a) Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo.

b) Nella lista gerarchica della rete antivirus, selezionare una postazione o un gruppo di postazioni per cui si vuole consentire la raccolta delle statistiche. Quando si seleziona un gruppo di postazioni, prestare attenzione all'ereditarietà di impostazioni: se alle postazioni del gruppo selezionato sono assegnate impostazioni individuali, la modifica delle impostazioni del gruppo non porterà alla modifica delle impostazioni della postazione.

c) Nel menu di gestione, nella sezione **Configurazione** → **Windows** selezionare la voce **Agent Dr.Web**.

d) Nelle impostazioni dell'Agent, nella scheda **Generali** spuntare il flag **Raccogli le informazioni sulle postazioni**, se è deselezionato. Se necessario, modificare il valore del parametro **Periodo di raccolta delle informazioni delle postazioni (min)**.

e) Per accettare le modifiche apportate, premere **Salva**. Le impostazioni verranno trasferite sulle postazioni.

Per visualizzare gli hardware e i software delle postazioni:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo.
2. Nella lista gerarchica della rete antivirus, selezionare la postazione desiderata.
3. Nel menu di gestione, nella sezione **Generali** selezionare la voce **Hardware e software**.
4. Nella finestra che si è aperta viene riportato l'albero con l'elenco di hardware e software che contiene le seguenti informazioni circa questa postazione:
   - **Application** – elenco dei prodotti software installati sulla postazione.
   - **Hardware** – elenco degli hardware della postazione.
   - **Operating System** – informazioni sul sistema operativo della postazione.
   - **Windows Management Instrumentation** – informazioni sugli strumenti di gestione di SO Windows.
5. Per filtrare i parametri visualizzati di hardware e software di una postazione, nella sezione **Impostazioni della vista albero** impostare le opzioni appropriate:
   - **Nascondi componenti di sistema** – per nascondere la visualizzazione delle applicazioni di sistema dalla sezione **Application**. Se il flag è selezionato, verrà visualizzato un elenco con tutte le altre applicazioni tranne quelle di sistema. Se il flag è deselezionato, nell'elenco, oltre agli altri, verranno visualizzati anche i componenti di sistema.
   - **Nascondi informazioni estese** – per visualizzare soltanto il set di componenti minimo che consentirà di avere un'idea generale della postazione. Questo set viene determinato da una serie di filtri predefiniti e non può essere modificato dall'utente. Se il flag è selezionato, verranno visualizzati soltanto i componenti principali. Se il flag è deselezionato, verranno visualizzati tutti i componenti.

6. Per visualizzare informazioni dettagliate su uno specifico hardware o software, selezionare l'oggetto desiderato nell'albero.
7. Se necessario, è possibile esportare in un file i dati su hardware e software di una postazione. È possibile esportare i dati visualizzati al momento nell'albero secondo le impostazioni definite (v. p 5).

   Per esportare i dati, fare clic su uno dei seguenti pulsanti nella barra degli strumenti:

   Registra le informazioni in file CSV,

   Registra le informazioni in file HTML,

   Registra le informazioni in file XML,

   Registra le informazioni in file PDF.

Per confrontare gli hardware e i software di diverse postazioni:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo.
2. Nella lista gerarchica della rete antivirus, selezionare diverse postazioni o gruppi di postazioni. Per visualizzare una pagina di confronto, si devono selezionare due o più postazioni SO Windows.
3. Nel menu di gestione, nella sezione **Generali** selezionare la voce **Comparazione di hardware e software**.
4. Nella finestra che si è aperta sono disponibili le seguenti informazioni:
   - l'albero con l'elenco degli hardware e dei software;
   - una tabella di confronto delle postazioni selezionate.
5. Per visualizzare i dati confrontati, selezionare l'elemento desiderato nell'albero degli hardware e dei software. Tutti i valori disponibili dell'elemento selezionato verranno visualizzati nell'albero di comparazione.

7.3. Configurazione delle impostazioni della postazione

7.3.1. Permessi dell'utente della postazione

Per configurare i permessi dell'utente di postazione tramite il Pannello di controllo della sicurezza Dr.Web:

1. Selezionare la voce **Rete antivirus** del menu principale, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione. Nel menu di gestione che si è aperto selezionare la voce **Permessi**. Si apre la finestra di configurazione dei permessi.
2. I permessi vengono modificati nelle schede che corrispondono al sistema operativo della postazione. Per modificare (concedere o togliere) un permesso, selezionare o deselezionare il flag di questo permesso.
3. I permessi per le postazioni SO Windows, OS X, Linux e Android vengono modificati nelle seguenti schede:

- **Componenti** – vengono configurati i permessi per la gestione dei componenti antivirus. Di default, l'utente è autorizzato ad avviare ciascun componente, però gli è vietato modificare la configurazione dei componenti e arrestare i componenti.
- **Generali** – vengono configurati i permessi per la gestione dell'Agent Dr.Web e delle sue funzioni:

Flag della sezione Permessi	Azione del flag	Il risultato sulla postazione se il flag è deselezionato
Postazioni SO Windows		
Avvio in modalità mobile	Spuntare il flag per permettere agli utenti su postazione di passare alla modalità mobile e di ricevere aggiornamenti direttamente dal Sistema d'aggiornamento mondiale Dr.Web se non è disponibile una connessione con il Server Dr.Web.	Nelle impostazioni di Agent, nella sezione **Generali** → **Modalità** non è disponibile l'impostazione **Utilizza la Modalità mobile se non è disponibile la connessione al server**.
Cambio della modalità di funzionamento	Spuntare il flag per permettere agli utenti su postazione di impostare le modalità di funzionamento di Agent Dr.Web.	Nelle impostazioni di Agent, nella sezione **Generali** → **Modalità** non sono disponibili le seguenti impostazioni: • **Accetta aggiornamenti dal server**, • **Accetta task dal server**, • **Accumula eventi**.
Modifica della configurazione di Agent Dr.Web	Spuntare il flag per permettere agli utenti su postazione di modificare le impostazioni di Agent Dr.Web.	Nelle impostazioni di Agent, nella sezione **Generali** non sono disponibili le impostazioni delle seguenti sezioni: • **Avvisi**: tutte le impostazioni non sono disponibili. • **Modalità**: non sono disponibili le impostazioni di connessione al Server e il flag **Sincronizza l'ora del sistema con l'ora del server**. • **Auto-protezione**: non sono disponibili le impostazioni **Impedisci la modifica della data e dell'ora di sistema**, **Proibisci l'emulazione delle azioni dell'utente**. • **Avanzate**: nelle impostazioni della sottosezione **Log** non sono disponibili le voci **Aggiornamento di Dr.Web**, **Servizi Dr.Web**, **Crea memory dump in caso di errori di scansione**.
Disattivazione dell'auto-protezione	Spuntare il flag per permettere agli utenti su postazione di arre-	Nelle impostazioni di Agent, nella sezione **Principali** → **Auto-protezione** non è

Flag della sezione Permessi	Azione del flag	Il risultato sulla postazione se il flag è deselezionato
	stare l'auto-protezione.	disponibile l'impostazione **Attiva l'auto-protezione** e l'impostazione **Attiva la virtualizzazione hardware**.
Disinstallazione di Agent Dr.Web	Spuntare il flag per permettere agli utenti su postazione di disinstallare l'Agent Dr.Web.	Vieta la rimozione dell'Agent su postazione tramite l'installer e tramite i mezzi standard del SO Windows. In questo caso, la rimozione dell'Agent è possibile soltanto tramite la voce **Generali** → **Disinstalla Agent Dr.Web** nella barra degli strumenti del Pannello di controllo.
Postazioni OS X		
Avvio in modalità mobile	Spuntare il flag per permettere agli utenti su postazione di passare alla modalità mobile e di ricevere aggiornamenti direttamente dal Sistema d'aggiornamento mondiale Dr.Web se non è disponibile una connessione con il Server Dr.Web.	Nella finestra principale dell'applicazione la sezione **Aggiornamento** non è disponibile.
Postazioni SO famiglia Linux		
Avvio in modalità mobile	Spuntare il flag per permettere agli utenti su postazione di passare alla modalità mobile e di ricevere aggiornamenti direttamente dal Sistema d'aggiornamento mondiale Dr.Web se non è disponibile una connessione con il Server Dr.Web.	Per la modalità di funzionamento console dell'applicazione: il comando `drweb-ctl update` di aggiornamento dei database dei virus da SAM non è disponibile.
Postazioni SO Android		
Avvio in modalità mobile	Spuntare il flag per permettere agli utenti di dispositivi mobili di passare alla modalità mobile e di ricevere aggiornamenti direttamente dal Sistema d'aggiornamento mondiale Dr.Web se non è disponibile una connessione con il Server Dr.Web.	Nella schermata principale dell'applicazione, avviata su un dispositivo mobile, la sezione **Aggiornamento** non è disponibile.

Quando viene disattivata un'impostazione responsabile per la modifica della configurazione dell'Agent, verrà utilizzato il valore assegnato a quest'impostazione per l'ultima volta prima

della disattivazione.

Le azioni eseguite dalle relative voci del menu sono descritte nella documentazione **Dr.Web per Windows. Manuale dell'utente**.

4. Si possono propagare queste impostazioni ad un altro oggetto, premendo il pulsante **Propaga queste impostazioni verso un altro oggetto**.
5. Per esportare queste impostazioni in file, fare clic su **Esporta impostazioni da questa sezione in file**.
6. Per importare queste impostazioni da file, fare clic su **Importa impostazioni in questa sezione da file**.
7. Per accettare le modifiche fatte, premere il pulsante **Salva**.

Se al momento della modifica delle impostazioni, la postazione non è connessa al Server, le impostazioni verranno accettate non appena l'Agent si riconnetterà al Server.

7.3.2. Calendario dei task della postazione

Dr.Web Enterprise Security Suite fornisce la possibilità di tenere un *calendario dei task centralizzato* che viene creato dall'amministratore di rete antivirus ed è aderente a tutte le regole di ereditarietà delle configurazioni.

Calendario dei task – un elenco delle attività che vengono eseguite automaticamente su postazioni all'ora stabilita. I calendari vengono utilizzati principalmente per eseguire le scansioni antivirus delle postazioni al momento più conveniente per gli utenti senza la necessità dell'avvio manuale di Scanner. Inoltre, Agent Dr.Web consente di eseguire alcuni altri tipi di azioni che vengono descritti di seguito.

Il calendario centralizzato di esecuzione regolare dei task di postazioni e gruppi specifici viene modificato tramite il Pannello di controllo della sicurezza Dr.Web.

Agli utenti sulla postazione non è disponibile la possibilità di visualizzare e modificare i task del calendario centralizzato.

I risultati di esecuzione dei task del calendario centralizzato non vengono registrati nei dati statistici sul lato Agent, ma vengono inviati sul Server e vengono conservati nei dati statistici del Server.

Per modificare il calendario centralizzato, eseguire le seguenti azioni:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo. Nel menu di gestione che si è aperto selezionare la voce **Scheduler**. Si apre una lista dei task per le postazioni.

Di default, per le postazioni SO Windows il calendario contiene il task **Daily scan** – scansione quotidiana di postazione (vietata).

2. Per gestire il calendario, vengono utilizzati gli elementi corrispondenti nella barra degli strumenti:

   a) Gli elementi generali della barra degli strumenti vengono utilizzati per creare nuovi task e per gestire la sezione calendario in generale. Questi strumenti sono sempre disponibili nella barra degli strumenti.

    **Crea task** – per aggiungere un nuovo task. Questa azione viene descritta in dettaglio qui sotto nella sottosezione Editor dei task.

    **Propaga queste impostazioni verso un altro oggetto** – per copiare i task dal calendario in altri oggetti – postazioni o gruppi. Per maggiori informazioni consultare la sezione Copiatura delle impostazioni in altri gruppi/postazioni.

    **Esporta impostazioni da questa sezione in file** – per esportare il calendario in un file di formato specifico.

    **Importa impostazioni in questa sezione da file** – per importare il calendario da un file di formato specifico.

   b) Per gestire i task esistenti, spuntare i flag di fronte ai task richiesti oppure il flag nell'intestazione della tabella se si vogliono selezionare tutti i task nella lista. Con questo diventano disponibili gli elementi della barra degli strumenti utilizzati per la gestione dei task selezionati.

Impostazione		Azione
Stato	**Permetti l'esecuzione**	Attivare l'esecuzione dei task selezionati secondo il calendario impostato se erano proibiti.
	Proibisci l'esecuzione	Proibire l'esecuzione dei task selezionati. I task saranno presenti nella lista ma non verranno eseguiti.
L'impostazione simile viene definita nell'editor del task nella scheda **Generali** tramite il flag **Permetti l'esecuzione**.		
Importanza	**Rendi critico**	Eseguire il task in modo straordinario al successivo avvio di Agent Dr.Web se l'esecuzione di questo task è stata omessa nell'ora programmata.
	Rendi non critico	Eseguire il task solo nell'ora programmata, indipendentemente dall'omissione o dall'esecuzione del task.
L'impostazione simile viene definita nell'editor del task nella scheda **Generali** tramite il flag **Task critico**.		
Duplica le impostazioni		Duplicare i task selezionati nella lista del calendario corrente. Tramite l'azione **Duplicare le impostazioni** vengono creati nuovi ta-

Impostazione	Azione
	sk che hanno le impostazioni uguali a quelle dei task selezionati.
Programma un'altra esecuzione dei task	Per i task per cui è impostata l'esecuzione singola: eseguire il task ancora una volta secondo le impostazioni di ora (ciò come cambiare la frequenza di esecuzione del task è descritto sotto nella sottosezione Editor dei task).
Rimuovi i task selezionati	Rimuovere dal calendario il task selezionato.

3. Per modificare i parametri di un task, selezionarlo dalla lista dei task. Si apre la finestra **Editor dei task** descritta sotto.
4. Dopo aver finito di modificare il calendario, fare clic su **Salva** per accettare le modifiche.

> Se come risultato della modifica viene creato un calendario vuoto (che non contiene task), il Pannello di controllo chiede se si vuole utilizzare il calendario ereditato dai gruppi o il calendario vuoto. Si deve impostare il calendario vuoto se si vuole rifiutare il calendario ereditato dai gruppi.

Editor dei task

Tramite l'editor dei task si possono definire le impostazioni per:

1. Creare un nuovo task.

   A questo fine fare clic sul pulsante **Crea task nella barra degli strumenti**.
2. Modificare un task esistente.

   A questo fine fare clic sul nome di uno dei task nella lista dei task.

Si apre la finestra di modifica dei parametri dei task. Le impostazioni di task per la modifica di un task esistente sono simili alle impostazioni per la creazione di un task nuovo.

> I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

Per modificare i parametri di un task:

1. Nella scheda **Generali** vengono impostati i seguenti parametri:
   - Nel campo **Nome** viene definito il nome del task sotto cui verrà visualizzato nel calendario.
   - Spuntare il flag **Permetti l'esecuzione** per attivare l'esecuzione del task. Se il flag non è selezionato, il task sarà presente nella lista ma non verrà eseguito.

> L'impostazione simile viene definita nella finestra principale di Scheduler tramite l'elemento della barra degli strumenti **Stato**.

- Spuntare il flag **Task critico** per eseguire il task in modo straordinario al prossimo avvio di Agent Dr.Web, se l'esecuzione di tale task è stata persa nell'ora programmata (Agent Dr.Web è disattivato al momento dell'esecuzione del task). Se al momento dell'avvio il task è stato perso diverse volte, verrà eseguito solo 1 volta.

L'impostazione simile viene definita nella finestra principale di Scheduler tramite l'elemento della barra degli strumenti **Importanza**.

Se in tale caso sono da eseguire diversi task di scansione, ne verrà eseguito solamente uno – il primo nella coda.

Per esempio, se è consentito il task **Daily scan** ed è stata rinviata la scansione critica tramite Agent Scanner, verrà eseguito **Daily scan**, e la scansione critica rinviata non potrà essere eseguita.

Nella scheda **Azione** selezionare il tipo di task dalla lista a cascata **Azione** e configurare i parametri del task, richiesti per l'esecuzione:

Tipo di task	Parametri e descrizione
Registrazione nel file di log	**Stringa** – testo del messaggio da registrare nel file di log.
Avvio del programma	Impostare i seguenti parametri: • Nel campo **Percorso –** nome completo (con il percorso) del file eseguibile del programma da avviare. • Nel campo **Argomenti** – parametri da riga di comando per il programma da avviare. • Spuntare il flag **Attendi che il programma venga completato** per l'attesa di completamento del programma avviato da questo task. In questo caso Agent registra nel log l'avvio del programma, il codice restituito e l'ora di completamento del programma. Se il flag **Attendi che il programma venga completato** è deselezionato, il task è considerato completato subito dopo l'avvio del programma ed Agent registra nel log soltanto l'avvio del programma.
Scanner Dr.Web. Scansione rapida	I parametri di configurazione della scansione sono descritti nel p. Configurazione di Scanner.
Scanner Dr.Web. Scansione personalizzata	
Scanner Dr.Web. Scansione completa	

L'avvio remoto dello Scanner è possibile soltanto sulle postazioni SO Windows, SO della famiglia UNIX e OS X.

2. Nella scheda **Tempo**:

- Dalla lista a cascata **Periodicità** selezionare la modalità di avvio del task e impostare il tempo secondo la periodicità scelta:

Modalità di avvio	Parametri e descrizione
Iniziale	Il task verrà eseguito all'avvio di Agent. Viene avviato senza parametri supplementari.
Tra N minuti dopo il task iniziale	Dalla lista a cascata **Task iniziale** è necessario selezionate il task relativamente al quale viene impostato il tempo di esecuzione del task che viene creato. Nel campo **Minuto** impostare o selezionare dalla lista il numero di minuti da aspettare dopo l'esecuzione del task iniziale prima che venga avviato il task corrente.
Ogni giorno	È necessario inserire l'ora e il minuto — il task verrà avviato ogni giorno all'ora indicata.
Ogni mese	È necessario selezionare un giorno (giorno del mese), immettere l'ora e il minuto — il task verrà avviato nel giorno del mese selezionato all'ora indicata.
Ogni settimana	È necessario selezionare un giorno della settimana, immettere l'ora e il minuto — il task verrà avviato nel giorno della settimana selezionato all'ora indicata.
Ogni ora	È necessario immettere un numero dallo 0 ai 59 che indica il minuto di ogni ora in cui il task verrà avviato.
Ogni N minuti	È necessario immettere il valore **N** per definire l'intervallo di tempo dell'esecuzione del task. Se **N** è pari ai `60` o superiore, il task verrà avviato ogni **N** minuti. Se **N** è inferiore ai `60`, il task verrà avviato ogni minuto dell'ora multiplo di **N**.

- Spuntare il flag **Proibisci dopo la prima esecuzione** per eseguire il task soltanto una volta secondo l'ora impostata. Se il flag è tolto, il task verrà eseguito molte volte con la periodicità selezionata.
  Per ripetere l'esecuzione di un task la cui esecuzione è definita come singola e che è già stato eseguito, utilizzare il pulsante  **Programma un`altra esecuzione dei task** che si trova nella barra degli strumenti della sezione calendario.
- Spuntare il flag **Avvia il task secondo l'UTC** per avviare il task secondo l'ora mondiale (il fuso orario UTC+0). Se il flag è deselezionato, il task verrà avviato secondo l'ora locale sulla postazione.

3. Finite le modifiche dei parametri del task, fare clic sul pulsante **Salva** per accettare le modifiche dei parametri del task, se veniva modificato un task esistente, oppure per creare un nuovo task con i parametri impostati, se veniva creato un nuovo task.

7.3.3. Componenti da installare del pacchetto antivirus

Per configurare la lista dei componenti da installare del pacchetto antivirus:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica selezionare una postazione o un gruppo. Nel menu di gestione che si è aperto, selezionare la voce **Componenti da installare**.
2. Per i componenti richiesti, dalla lista a cascata selezionare una delle opzioni:
   - **Deve essere installato** – comanda la disponibilità obbligatoria del componente sulla postazione. Quando viene creata una nuova postazione, il componente viene incluso obbligatoriamente nel pacchetto antivirus da installare. Quando il valore **Deve essere installato** viene impostato per una postazione già esistente, il componente viene aggiunto al pacchetto antivirus disponibile.
   - **Può essere installato** – determina la possibilità di installare il componente antivirus. L'utente decide se vuole installare il componente quando installa l'Agent.
   - **Non può essere installato** – vieta la disponibilità del componente sulla postazione. Quando viene creata una nuova postazione, il componente non viene incluso nel pacchetto antivirus da installare. Quando il valore **Non può essere installato** viene impostato per una postazione già esistente, il componente viene rimosso dal pacchetto antivirus.

   Nella tabella 7-1 è indicato se il componente verrà installato su una postazione (+) a seconda delle impostazioni configurate dall'utente e di quelle configurate dall'amministratore sul Server.

Tabella 7–1.

Definito dall'utente	Parametri impostati sul Server		
	Deve	Può	Non può
Installa	+	+	
Non installare	+		

3. Fare clic sul pulsante **Salva** per salvare le impostazioni e la relativa modifica della lista dei componenti del pacchetto antivirus sulla postazione.

7.4. Configurazione dei componenti antivirus

Le impostazioni dei componenti antivirus, configurabili attraverso il Pannello di controllo, sono descritte dettagliatamente nel **Manuale dell'amministratore** per la gestione delle postazioni per il sistema operativo corrispondente.

7.4.1. Componenti

A seconda del sistema operativo della postazione, vengono fornite le funzioni di protezione corrispondenti, riportate di seguito.

Postazioni SO Windows®

Scanner Dr.Web, Dr.Web Agent Scanner

Scansione del computer on demand e secondo il calendario. Inoltre, è supportata la possibilità di avviare la scansione antivirus delle postazioni su remoto dal Pannello di controllo, compresa la scansione alla ricerca dei rootkit.

SpIDer Guard

Scansione continua del file system in tempo reale. Controlla tutti i processi che vengono avviati e file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

SpIDer Mail

Scansione di ogni email in entrata e in uscita in client di posta.

Inoltre, è possibile utilizzare il filtro antispam (a condizione che la licenza permetta l'utilizzo di tale funzionalità).

SpIDer Gate

Controllo di ogni connessione a siti web via HTTP. Neutralizzazione delle minacce nel traffico HTTP (per esempio in file inviati o ricevuti), nonché blocco dell'accesso a siti non attendibili o non corretti.

Office control

Controllo dell'accesso a risorse locali e di rete, in particolare, controllo dell'accesso a siti web. Permette di controllare l'integrità dei file importanti, proteggendoli contro le modifiche accidentali o contro l'infezione dai virus, e vieta ai dipendenti l'accesso alle informazioni indesiderate.

Firewall

Protezione dei computer dall'accesso non autorizzato dall'esterno e prevenzione della fuga di informazioni importanti attraverso Internet. Controllo della connessione e del trasferimento di dati attraverso Internet e blocco delle connessioni sospette a livello di pacchetti e di applicazioni.

Quarantena

Isolamento di oggetti dannosi e sospetti in una directory speciale.

Auto-protezione

Protezione dei file e delle directory Dr.Web Enterprise Security Suite contro la rimozione o la modifica non autorizzata o accidentale da parte dell'utente e contro la rimozione o la

modifica da parte del malware. Quando l'auto-protezione è attivata, l'accesso ai file e alle directory Dr.Web Enterprise Security Suite è consentito solamente ai processi Dr.Web.

Protezione preventiva (le impostazioni sono disponibili nelle impostazioni dell'Agent Dr.Web)

Prevenzione di potenziali minacce alla sicurezza. Controllo dell'accesso agli oggetti critici del sistema operativo, controllo del caricamento driver, dell'esecuzione automatica programmi e del funzionamento dei servizi di sistema, nonché monitoraggio dei processi in esecuzione e blocco processi se rilevata attività di virus.

Postazioni SO famiglia UNIX®

Scanner Dr.Web, Dr.Web Agent Scanner

Scansione del computer on demand e secondo il calendario. Inoltre, è supportata la possibilità di avviare la scansione antivirus delle postazioni su remoto dal Pannello di controllo.

SpIDer Guard

Scansione continua del file system in tempo reale. Controlla tutti i processi che vengono avviati e file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

SpIDer Gate

Controllo di ogni connessione a siti web via HTTP. Neutralizzazione delle minacce nel traffico HTTP (per esempio in file inviati o ricevuti), nonché blocco dell'accesso a siti non attendibili o non corretti.

Quarantena

Isolamento di oggetti dannosi e sospetti in una directory speciale.

Gli altri componenti, di cui le impostazioni sono riportate nel Pannello di controllo per le postazioni SO della famiglia UNIX, sono aggiuntivi e servono per la configurazione interna del funzionamento del software antivirus.

Postazioni OS X®

Scanner Dr.Web, Dr.Web Agent Scanner

Scansione del computer on demand e secondo il calendario. Inoltre, è supportata la possibilità di avviare la scansione antivirus delle postazioni su remoto dal Pannello di controllo.

SpIDer Guard

Scansione continua del file system in tempo reale. Controlla tutti i processi che vengono avviati e file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

SpIDer Gate (le impostazioni sono disponibili soltanto sulla postazione)

Controllo di ogni connessione a siti web via HTTP. Neutralizzazione delle minacce nel traffico HTTP (per esempio in file inviati o ricevuti), nonché blocco dell'accesso a siti non attendibili o non corretti.

Quarantena

Isolamento di oggetti dannosi e sospetti in una directory speciale.

Dispositivi mobili SO Android

Scanner Dr.Web, Dr.Web Agent Scanner

Scansione del dispositivo mobile on demand e secondo il calendario. Inoltre, è supportata la possibilità di avviare la scansione antivirus delle postazioni su remoto dal Pannello di controllo.

SpIDer Guard

Scansione continua del file system in tempo reale. Scansione di ogni file al momento quando viene salvato nella memoria del dispositivo mobile.

Filtraggio di chiamate e di messaggi

Il filtraggio di messaggi SMS e di chiamate consente di bloccare messaggi e chiamate indesiderati, per esempio messaggi di pubblicità, nonché chiamate e messaggi provenienti da numeri sconosciuti.

Antifurto

Rilevamento della posizione o blocco istantaneo delle funzioni del dispositivo mobile in caso di smarrimento o furto.

Cloud Checker

Il filtraggio URL consente di proteggere l'utente del dispositivo mobile dalle risorse di Internet indesiderate.

Firewall (le impostazioni sono disponibili soltanto sul dispositivo mobile)

Protezione del dispositivo mobile dall'accesso non autorizzato dall'esterno e prevenzione della fuga di informazioni importanti attraverso la rete. Controllo della connessione e del trasferimento di dati attraverso Internet e blocco delle connessioni sospette a livello di pacchetti e di applicazioni.

Auditor della sicurezza (le impostazioni sono disponibili soltanto sul dispositivo mobile)

Diagnostica ed analisi della sicurezza del dispositivo mobile ed eliminazione di problemi e vulnerabilità rilevati.

Filtro delle applicazioni

Divieto dell'esecuzione sul dispositivo mobile delle applicazioni non incluse nella lista di quelle consentite dall'amministratore.

Server SO Novell® NetWare®

Scanner Dr.Web

Scansione del computer on demand e secondo il calendario.

SpIDer Guard

Scansione continua del file system in tempo reale. Controlla tutti i processi che vengono avviati e file che vengono creati su dischi rigidi e vengono aperti su supporti rimovibili.

7.5. Scansione antivirus delle postazioni

L'utente della postazione può eseguire la scansione antivirus da solo, utilizzando il componente Scanner Dr.Web per Windows. L'icona di avvio di questo componente viene messa sul desktop al momento dell'installazione del software antivirus. Scanner può essere avviato e può funzionare anche se Agent non è operativo, anche in modalità provvisoria del SO Windows.

Tramite il Pannello di controllo è possibile:

- Visualizzare la lista di tutti i componenti antivirus in esecuzione al momento.
- Interrompere l'esecuzione di componenti antivirus per tipo.
- Avviare i task di scansione antivirus con la configurazione dei parametri di scansione.

7.5.1. Visualizzazione ed interruzione dell'esecuzione dei componenti

Per visualizzare una lista dei componenti avviati e per interromperne l'esecuzione:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo. Nel menu di gestione che si è aperto selezionare la voce **Componenti in esecuzione**.

   Si apre una lista di tutti i componenti attivi al momento, sia di quelli avviati tramite il Pannello di controllo manualmente dall'amministratore o secondo il calendario, che di quelli avviati dall'utente sulla postazione.
2. Se è necessario interrompere l'esecuzione di uno dei componenti, spuntare il flag di fronte a questo componente, dopo di che nella barra degli strumenti premere il pulsante **Interrompi**. Il componente viene arrestato e viene eliminato dalla lista dei componenti in esecuzione.

Quando viene utilizzata questa opzione, le scansioni in corso vengono interrotte, lo Scanner viene arrestato, il funzionamento dei monitor in esecuzione viene sospeso.

Attenzione! Non è possibile avviare i monitor SpIDer Guard, SpIDer Mail e SpIDer Gate dal Pannello di controllo.

7.5.2. Interruzione di componenti in esecuzione per tipo

Quando viene utilizzata questa opzione, le scansioni in corso vengono interrotte, lo Scanner viene arrestato, il funzionamento dei monitor in esecuzione viene sospeso.

Attenzione! Non è possibile avviare i monitor SpIDer Guard, SpIDer Mail e SpIDer Gate dal Pannello di controllo.

Per interrompere l'esecuzione di tutti i componenti di un determinato tipo, avviati su postazioni:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica selezionare il gruppo richiesto o singole postazioni.
2. Nella barra degli strumenti della directory della rete antivirus premere **Gestione dei componenti**. Dalla lista a cascata selezionare la voce **Interrompi i componenti in esecuzione**.
3. Nel pannello che si è aperto spuntare i flag di fronte ai tipi di componenti da interrompere immediatamente:
   - **Interrompi Dr.Web Agent Scanner avviato dallo Scheduler** – per arrestare una scansione attiva tramite Dr.Web Agent Scanner, che è stata avviata secondo i task del calendario centralizzato.
   - **Interrompi Dr.Web Agent Scanner avviato dall'amministratore** – per arrestare una scansione attiva tramite Dr.Web Agent Scanner, che è stata avviata manualmente dall'amministratore tramite il Pannello di controllo.
   - **Interrompi Scanner Dr.Web avviato dall'utente** – per arrestare una scansione attiva tramite Scanner Dr.Web, che è stata avviata dall'utente sulla postazione.
   - **Interrompi SpIDer Guard, SpIDer Mail, SpIDer Gate, Office control, Firewall, Auto-protezione e Protezione preventiva** – per sospendere l'operazione dei rispettivi componenti.

   Per selezionare tutti i tipi di componenti da arrestare, spuntare il flag di fronte all'intestazione del pannello **Interruzione dei componenti in esecuzione**.
4. Premere il pulsante **Interrompi**.

7.5.3. Avvio della scansione della postazione

Per avviare la scansione antivirus delle postazioni:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.

3. Nella barra degli strumenti premere sulla voce **Scansiona**. Nella lista che si è aperta nella barra degli strumenti selezionare una delle modalità di scansione:

   Scanner Dr.Web. Scansione rapida. In questa modalità vengono scansionati i seguenti oggetti:

   - memoria operativa,
   - settori di avvio di tutti i dischi,
   - oggetti in esecuzione automatica,
   - directory radice del disco di avvio,
   - directory radice del disco di installazione di SO Windows,
   - directory di sistema di SO Windows,
   - cartella `Documenti`,
   - directory temporanea di sistema,
   - directory temporanea utente.

   Scanner Dr.Web. Scansione completa. In questa modalità viene eseguita la scansione completa di tutti i dischi rigidi e supporti rimovibili (inclusi i settori di avvio).

   Scanner Dr.Web. Scansione personalizzata. Questa modalità permette di scegliere qualsiasi directory o file per la successiva scansione, nonché di configurare le impostazioni avanzate di scansione.

   > L'avvio remoto dello Scanner è possibile soltanto se vengono selezionate le postazioni attive gestite da un sistema operativo che consente l'avvio dello Scanner: SO Windows, SO della famiglia UNIX e OS X.

4. Dopo che è stata scelta una variante di scansione, si apre la finestra delle impostazioni dello Scanner. Se necessario, modificare le impostazioni di scansione (v. sezione Configurazione dei parametri di Scanner).
5. Premere il pulsante **Scansiona** per avviare il processo di scansione sulle postazioni selezionate.

   > La scansione della postazione tramite Dr.Web Agent Scanner avviato su remoto viene eseguita in modalità silenziosa senza visualizzare gli avvisi all'utente della postazione.

7.5.4. Configurazione di Scanner

Tramite il Pannello di controllo si possono configurare le seguenti impostazioni di scansione antivirus:

- Impostazioni di Scanner Dr.Web. Questo Scanner viene avviato dagli utenti su postazioni e non può essere avviato su remoto tramite il Pannello di controllo. Tuttavia, l'amministratore può modificarne le impostazioni in modo centralizzato che verranno trasmesse e salvate successivamente sulle postazioni.

- Impostazioni di Dr.Web Agent Scanner. Questo Scanner viene avviato su remoto tramite il Pannello di controllo ed esegue la scansione antivirus della postazione in un modo simile a Scanner Dr.Web. Le impostazioni di Dr.Web Agent Scanner sono impostazioni estese di Scanner Dr.Web e vengono configurate quando viene avviata la scansione antivirus delle postazioni.

Configurazione di Scanner Dr.Web

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
3. Nel menu di gestione che si è aperto, nella sezione **Configurazione** nella sottosezione del sistema operativo richiesto, selezionare la voce **Scanner**. Si apre la finestra di configurazione di Scanner.
4. Impostare i parametri di scansione richiesti. I parametri di Scanner Dr.Web sono descritti nel **Manuale dell'utente** per il sistema operativo corrispondente.
5. Fare clic sul pulsante **Salva**. Le impostazioni verranno salvate nel Pannello di controllo e verranno trasferite sulle postazioni corrispondenti.

Configurazione di Dr.Web Agent Scanner

Le impostazioni di Dr.Web Agent Scanner vengono configurate quando viene avviata la scansione delle postazioni, come è descritto in p. Avvio della scansione di postazioni.

La lista delle sezioni delle impostazioni di Scanner che saranno disponibili (+) o non disponibili (–) dipende dalla variante di avvio della scansione di postazioni ed è riportata nella tabella sotto.

Tabella 7–2. Lista delle sezioni delle impostazioni dello scanner a seconda della variate di avvio

Variante di avvio della scansione	Sezioni delle impostazioni			
	Generali	Azioni	Limitazioni	Esclusioni
Scanner Dr.Web. Scansione personalizzata	+	+	+	+
Scanner Dr.Web. Scansione rapida	–	+	+	–
Scanner Dr.Web. Scansione completa	–	+	+	–

A seconda del sistema operativo della postazione su cui viene avviata la scansione remota, sarà disponibile solo quella parte delle impostazioni di Scanner che è supportata dal sistema operativo della postazione.

Le impostazioni che non sono supportate per la scansione delle postazioni SO della famiglia UNIX e OS X sono racchiuse tra parentesi quadre **[ ]**.

7.5.4.1. Generali

Le impostazioni che non sono supportate per la scansione delle postazioni SO della famiglia UNIX e OS X sono racchiuse tra parentesi quadre **[ ]**.

Nella sezione **Generali** si possono configurare le seguenti impostazioni della scansione antivirus:

- Spuntare il flag **Utilizza l'analisi euristica** affinché Scanner cerchi virus sconosciuti, utilizzando l'analisi euristica. In questa modalità sono possibili falsi positivi di Scanner.
- Spuntare il flag **Controlla settori di avvio** affinché Scanner scansioni i settori di avvio. Vengono scansionati sia i settori di avvio dei dischi logici, che i master boot record dei dischi fisici.
- Spuntare il flag **[Controlla programmi avviati automaticamente]** per scansionare programmi eseguiti automaticamente alla partenza del sistema operativo.
- Spuntare il flag **Segui collegamenti simbolici** affinché la scansione segua collegamenti simbolici.
- Spuntare il flag **[Controlla programmi e moduli in esecuzione]** per scansionare i processi in esecuzione nella memoria operativa.
- Spuntare il flag **[Scansione alla ricerca di rootkit]** per abilitare la ricerca dei programmi malevoli che nascondono la propria presenza nel sistema operativo.
- Spuntare il flag **[Sospendi la scansione se computer passa all'alimentazione a batteria]** per sospendere la scansione antivirus se il computer dell'utente passa all'alimentazione a batteria.
- La lista a cascata **Priorità di scansione** determina la priorità del processo di scansione relativamente alle risorse di elaborazione del sistema operativo.
- Spuntare il flag **[Livello del consumo delle risorse del computer]** per limitare l'utilizzo delle risorse del computer da parte della scansione, e dalla lista a cascata selezionare il tasso massimo di utilizzo delle risorse da parte di Scanner. In assenza di altri processi attivi, le risorse del computer verranno utilizzate nel grado massimo.

  L'opzione **Livello del consumo delle risorse del computer** non influisce sul valore effettivo del consumo delle risorse se la scansione viene eseguita in un sistema a singolo processore con un core.

- La lista a cascata **Azioni dopo la scansione** imposta l'esecuzione automatica di un'azione subito dopo la fine della scansione:
  - **non fare nulla** – dopo la fine della scansione non intraprendere alcun'azione con il computer dell'utente.
  - **[spegni la postazione]** – dopo la fine della scansione spegni il computer dell'utente. Prima di spegnere il computer, Scanner applicherà alle minacce rilevate le azioni impostate.
  - **riavvia la postazione** – dopo la fine della scansione riavvia il computer dell'utente. Prima di riavviare il computer, Scanner applicherà alle minacce rilevate le azioni impostate.

- **trasferisci la postazione in modalità standby**.
- **trasferisci la postazione in modalità sleep**.

- Spuntare il flag **Disattiva rete durante la scansione** per scollegare il computer dalla rete locale e da Internet per il tempo della scansione.
- Spuntare il flag **Controlla dischi fissi** per scansionare le unità dischi fissi (hard drive ecc.).
- Spuntare il flag **Controlla oggetti nei dispositivi rimovibili** per scansionare tutte le unità dispositivi rimovibili, per esempio unità dischi magnetici (dischetti), dischi CD/DVD, dispositivi flash ecc.
- Nel campo **Percorsi da scansionare** impostare una lista dei percorsi da scansionare (il metodo di impostazione è descritto sotto).
  - Per aggiungere una nuova riga alla lista, fare clic sul pulsante  e nella riga che si è aperta inserire il percorso richiesto.
  - Per eliminare un elemento dalla lista, fare clic sul pulsante  di fronte alla riga corrispondente.

  Se viene spuntato il flag **Percorsi da scansionare**, vengono scansionati soltanto i percorsi indicati. Se il flag è tolto, vengono scansionati tutti i dischi.

7.5.4.2. Azioni

Le impostazioni che non sono supportate per la scansione delle postazioni SO della famiglia UNIX e OS X sono racchiuse tra parentesi quadre **[ ]**.

Nella sezione **Azioni** viene impostata la reazione di Scanner al rilevamento di file infetti o sospetti, programmi malevoli e archivi infetti.

Dr.Web Agent Scanner applica automaticamente le azioni impostate per gli oggetti malevoli rilevati.

Sono previste le seguenti azioni da applicare alle minacce rilevate:

- **Cura** – per ripristinare l'oggetto infetto allo stato precedente all'infezione. Se l'oggetto è incurabile o se il tentativo di cura non è riuscito, viene applicata l'azione impostata per gli oggetti incurabili.

  Quest'azione è disponibile solo per gli oggetti infettati da un virus conosciuto curabile, esclusi i trojan e i file infetti all'interno di oggetti complessi (archivi compressi, file di email o container di file).
- **Rimuovi** – per rimuovere gli oggetti infetti.
- **Sposta in quarantena** – per trasferire gli oggetti infetti nella directory di Quarantena su postazione.
- **Informa** – per inviare nel Pannello di controllo un avviso di rilevamento di un virus (per la configurazione di modalità avvisi v. p. Configurazione delle notifiche).

- **Ignora** – per saltare l'oggetto senza eseguire alcun'azione, neanche inviando i relativi avvisi nelle statistiche di scansione.

Tabella 7–3. Azioni di Scanner applicate a oggetti malevoli rilevati

Oggetto	Azione				
	Cura	Rimuovi	Sposta in quarantena	Informa	Ignora
Infetti	+/*	+	+		
Sospetti		+	+/*		+
Incurabili		+	+/*		
Container		+	+/*		
Archivi compressi		+	+/*		
File di email			+/*		+
Settori di avvio	+/*			+	
Adware		+	+/*		+
Dialer		+	+/*		+
Joke		+	+/*		+
Riskware		+	+/*		+
Hacktool		+	+/*		+

Segni convenzionali

+	azione consentita per questo tipo di oggetti
+/*	azione predefinita per questo tipo di oggetti

Per impostare le azioni da applicare a minacce rilevate, si utilizzano le seguenti impostazioni:

- La lista a cascata **Infetti** imposta la reazione di Scanner al rilevamento di un file infettato da un virus conosciuto.
- La lista a cascata **Sospetti** imposta la reazione di Scanner al rilevamento di un file presumibilmente infettato da un virus (tale file è stato rilevato tramite l'analisi euristica).

Se nella scansione è inclusa la directory di installazione di SO, si consiglia di selezionare per i file sospetti la reazione **Informa**.

- La lista a cascata **Incurabili** imposta la reazione di Scanner al rilevamento di un file infettato da un virus conosciuto incurabile, nonché per i casi quando il tentativo di cura non è riuscito.
- La lista a cascata **Container infetti** imposta la reazione di Scanner al rilevamento di un file infettato o sospetto incluso in un container di file.
- La lista a cascata **Archivi infetti** imposta la reazione di Scanner al rilevamento di un file infettato o sospetto incluso in un archivio di file.
- La lista a cascata **File di email infetti** imposta la reazione di Scanner al rilevamento di un file infettato o sospetto nel formato di email.

> Se un virus o un codice sospetto vengono rilevati dentro oggetti complessi (archivi compressi, file di email o container di file), le azioni da applicare alle minacce in tali oggetti vengono eseguite con l'intero oggetto e non soltanto con la parte infetta. Di default, in tutti questi casi è prevista l'azione "Informa".

- La lista a cascata **Settori di avvio infetti** imposta la reazione di Scanner al rilevamento di un virus o di un codice sospetto nell'area dei settori di avvio.
- Le seguenti liste a cascata impostano la reazione di Scanner al rilevamento dei corrispondenti tipi di malware:
  - **Adware**;
  - **Dialer**;
  - **Joke**;
  - **Riskware**;
  - **Hacktool**.

> Se viene impostata l'azione **Ignora**, nessuna azione verrà eseguita: nessun avviso verrà spedito nel Pannello di controllo diversamente dal caso quando l'opzione **Informa** è attivata per il rilevamento dei virus.

Spuntare il flag **[Riavvia il computer automaticamente]** per riavviare il computer dell'utente automaticamente dopo la fine della scansione se durante la scansione sono stati rilevati gli oggetti infetti per cui, per completarne la cura, occorre il riavvio del sistema operativo. Se il flag è deselezionato, il computer dell'utente non verrà riavviato. Nelle statistiche della scansione della postazione, ricevute dal Pannello di controllo, viene segnalata la necessità di riavviare la postazione per completare la cura. Le informazioni sullo stato che richiede il riavvio vengono visualizzate nella tabella Stati. Se necessario, l'amministratore può riavviare la postazione dal Pannello di controllo (v. sezione Rete antivirus).

Spuntare il flag **Mostra il progresso della scansione** per visualizzare nel Pannello di controllo l'indicatore e la barra di stato del processo di scansione della postazione.

7.5.4.3. Limitazioni

> Le impostazioni che non sono supportate per la scansione delle postazioni SO della famiglia UNIX e OS X sono racchiuse tra parentesi quadre **[ ]**.

Nella sezione **Limitazioni** sono disponibili le seguenti configurazioni di scansione antivirus:

- **Tempo massimo di scansione (ms)** – tempo massimo in millisecondi di scansione di un oggetto. Dopo il tempo indicato, la scansione dell'oggetto viene arrestata.
- **Livello di annidamento massimo di un archivio** – numero massimo di archivi annidati. Se un archivio ha un livello di annidamento che supera il limite impostato, la scansione viene eseguita solo fino al livello di annidamento indicato.
- **[Dimensione massima di un archivio (KB)]** – dimensione massima in kilobyte di un archivio da controllare. Se la dimensione dell'archivio eccede il limite indicato, la decompressione e la scansione non vengono eseguite.
- **Rapporto di compressione massimo** – se Scanner determina che il rapporto di compressione di un archivio eccede il limite indicato, la decompressione e la scansione non vengono eseguite.
- **[Dimensione massima di un oggetto decompresso (KB)]** – dimensione massima in kilobyte di un file da decomprimere. Se Scanner determina che dopo la decompressione la dimensione dei file dell'archivio eccede il limite indicato, la decompressione e la scansione non vengono eseguite.
- **[Valore soglia per il controllo del grado di compressione (KB)]** – dimensione minima in kilobyte di un file all'interno dell'archivio, a partire dalla quale viene controllato il rapporto di compressione.

7.5.4.4. Esclusioni

Nella sezione **Esclusioni** viene impostata una lista delle directory e dei file da escludere dalla scansione antivirus.

Per modificare le liste dei percorsi e dei file da escludere:

1. Inserire il percorso del file o della directory richiesta nella riga **Percorsi e file da escludere**.
2. Per aggiungere una nuova riga alla lista, fare clic sul pulsante  e nella riga che si è aperta inserire il percorso richiesto.
3. Per eliminare un elemento dalla lista, fare clic sul pulsante  di fronte alla riga corrispondente.

La lista degli oggetti esclusi può contenere elementi dei seguenti tipi:

1. Percorso diretto esplicito dell'oggetto da escludere. In questo caso:
   - Carattere \ o / – viene escluso dalla scansione tutto il disco su cui si trova la directory di installazione di SO Windows,
   - Percorso che finisce con il carattere \ – questa directory viene esclusa dalla scansione,
   - Percorso che non finisce con il carattere \ – viene esclusa dalla scansione qualsiasi sottodirectory, il percorso della quale inizia con la riga indicata.

   Per esempio: `C:\Windows` – non scansionare file della directory `C:\Windows` e tutte le sottodirectory.

2. Le maschere di oggetti esclusi dalla scansione. Per impostare le maschere si possono utilizzare i caratteri `?` e `*`.

   Per esempio: `C:\Windows\*\*.dll` – non scansionare tutti i file con l'estensione `dll` che si trovano in tutte le sottodirectory della directory `C:\Windows`.

3. Espressione regolare. I percorsi si possono impostare con le espressioni regolari. Inoltre, qualsiasi file, il cui nome completo (con il percorso) corrisponde a un'espressione regolare, viene escluso dalla scansione.

> Prima di avviare il processo di scansione antivirus, consultare le raccomandazioni sull'utilizzo dei programmi antivirus sui computer Windows Server 2003 e Windows XP. L'articolo che contiene le informazioni necessarie si trova sull'indirizzo – http://support.microsoft.com/kb/822158/it. Il materiale di questo articolo è progettato per aiutare ad ottimizzare le prestazioni del sistema.

La sintassi delle espressioni regolari utilizzate per trascrivere percorsi esclusi è la seguente:

```
qr{espressione}flag
```

Spesso come flag si utilizza il carattere `i`, questo flag significa "non prendere in considerazione differenza di maiuscole e minuscole".

Esempi di trascrizione in espressioni regolari di percorsi e file da escludere

Espressione regolare	Valore
`qr{\\pagefile\.sys$}i`	non scansionare file di swap di SO Windows NT
`qr{\\notepad\.exe$}i`	non scansionare file `notepad.exe`
`qr{^C:}i`	non scansionare proprio niente sul disco `C`
`qr{^.:\\WINNT\\}i`	non scansionare niente nelle directory `WINNT` su tutti i dischi
`qr{(^C:)|(^.:\\WINNT\\)}i`	unione di due casi precedenti
`qr{^C:\\dir1\\dir2\\file\.ext$}i`	non scansionare il file `c:\dir1\dir2\file.ext`
`qr{^C:\\dir1\\dir2\\(.+\\)?file\.ext$}i`	non scansionare il file `file.ext` se si trova nella directory `c:\dir1\dir2` e nelle sottodirectory
`qr{^C:\\dir1\\dir2\\}i`	non scansionare la directory `c:\dir1\dir2` e le sottodirectory
`qr{dir\\[^\\]+}i`	non scansionare la sottodirectory `dir` che si trova in qualsiasi directory, ma scansiona le sottodirectory
`qr{dir\\}i`	non scansionare la sottodirectory `dir` che si trova in qualsiasi directory e le sottodirectory

L'utilizzo delle espressioni regolari è descritto in breve nel documento **Allegati**, sezione Allegato J. Utilizzo di espressioni regolari in Dr.Web Enterprise Security Suite.

Nella sottosezione **Controllare i contenuti dei seguenti file**, si può disattivare la scansione di oggetti compositi. Per farlo, togliere i seguenti flag:

- Il flag **Archivi** comanda a Scanner di cercare virus nei file compressi in archivi di file.
- Il flag **File di email** comanda di scansionare caselle di email.
- Il flag **Pacchetti d'installazione** comanda a Scanner di controllare pacchetti di installazione di programmi.

7.6. Visualizzazione delle statistiche della postazione

Tramite il menu di gestione della sezione **Rete antivirus** si possono visualizzare le seguenti informazioni:

- Statistiche – le statistiche del funzionamento di elementi antivirus su postazione, dello stato di postazioni e di elementi antivirus, per visualizzare e salvare i report che includono le statistiche riepilogative o riassunti selezionati per tipo di tabella.
- Grafici – i grafici con le informazioni su infezioni rilevate su postazioni.
- Quarantena – un accesso su remoto ai contenuti della Quarantena su postazione.

7.6.1. Statistiche

Inoltre, è possibile configurare la creazione automatica di un report statistico che include tabelle statistiche richieste. Questo report in formato selezionato può essere non soltanto salvato su Server, ma anche inviato via email.

Per farlo, configurare il task **Creazione di resoconto statistico** nel calendario di Server.

Per visualizzare le tabelle:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
2. Nel menu di gestione che si è aperto, selezionare la voce richiesta dalla sottosezione **Statistiche**.

La sezione di menu **Statistiche** contiene le seguenti voci:

- **Statistiche complessive** – per ottenere le statistiche riepilogative senza suddividerle per sessioni.
- Dati complessivi – per visualizzare e salvare i report che contengono tutte le statistiche riepilogative o i riassunti selezionati per tipo di tabella impostato. Non è disponibile nel menu se sono nascoste tutte le altre voci di menu nella sezione **Statistiche**.

- **Minacce** – per visualizzare le informazioni sulle minacce rilevate alla sicurezza delle postazioni protette: un elenco degli oggetti infetti, la posizione per postazione, i nomi delle minacce, le azioni dell'antivirus ecc.
- **Errori** – per visualizzare una lista di errori di scansione sulla postazione selezionata per un determinato periodo.
- Statistiche di scansione – per ottenere le statistiche di funzionamento degli elementi antivirus su postazione.
- **Avvio/Arresto** – per visualizzare una lista dei componenti che erano avviati su postazione.
- **Statistiche delle minacce** – per visualizzare le informazioni sul rilevamento delle minacce alla sicurezza delle postazioni protette, raggruppate per tipo di minaccia e per quantità di minacce su postazioni.
- Stato – per visualizzare le informazioni su uno stato insolito delle postazioni, che probabilmente richiede l'intervento.
- **Task** – per visualizzare una lista dei task assegnati alla postazione in un determinato periodo.
- **Prodotti** – per visualizzare le informazioni sui prodotti installati su postazioni selezionate. "Prodotti" in questo caso si riferisce ai prodotti del repository del Server.
- **Database dei virus** – per visualizzare le informazioni circa i database dei virus installati: nome del file che contiene un database dei virus specifico; versione del database dei virus; numero di record nel database dei virus; data di creazione del database dei virus. Questa voce è disponibile solo se vengono selezionate postazioni.
- **Moduli** – per visualizzare le informazioni dettagliate su tutti i moduli dell'antivirus Dr.Web: descrizione del modulo: il suo nome di funzione; il file che determina un modulo separato del prodotto; la versione completa del modulo ecc. Questa voce è disponibile solo se vengono selezionate postazioni.
- **Installazioni di Agent** – per visualizzare una lista delle installazioni del software Agent su una postazione o un gruppo di postazioni.
- **Disinstallazioni di Agent** – per visualizzare una lista delle postazioni da cui il software antivirus Dr.Web è stato rimosso.

Per visualizzare le voci nascoste della sezione **Statistiche**, selezionare la voce del menu principale **Amministrazione**, nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione del Server Dr.Web**. Nella scheda **Statistiche** spuntare i flag corrispondenti (v. di seguito), dopodiché premere **Salva** e riavviare il Server.

Tabella 7-4. Corrispondenza delle voci della sezione Statistiche e dei flag della sezione Statistiche nella configurazione del Server

Voci della sezione Statistiche	Flag della sezione Statistiche nella configurazione del Server
Statistiche complessive	Statistiche di scansione
Minacce	Minacce alla sicurezza rilevate

Voci della sezione Statistiche	Flag della sezione Statistiche nella configurazione del Server
Errori	Errori di scansione
Statistiche di scansione	Statistiche di scansione
Avvio/Arresto	Avvio/arresto dei componenti
Statistiche delle minacce	Minacce alla sicurezza rilevate
Stato	Stato delle postazioni
Task	Log di esecuzione di task su postazioni
Database dei virus	Stato delle postazioni Monitoraggio dei database dei virus Log di esecuzione di task su postazioni
Moduli	Lista dei moduli delle postazioni
Installazioni di Agent	Installazioni di Agent

Le finestre in cui vengono visualizzati i risultati del funzionamento di vari componenti e le statistiche riepilogative della postazione hanno l'interfaccia uguale e le azioni per l'ottenimento delle informazioni dettagliate che loro forniscono sono uguali.

Di seguito vengono riportati alcuni esempi della visualizzazione di statistiche riepilogative tramite il Pannello di controllo.

7.6.1.1. Dati riepilogativi

Per visualizzare i dati riepilogativi:

1. Nella lista gerarchica selezionare una postazione o un gruppo.
2. Nel menu di gestione nella sezione **Statistiche** selezionare la voce **Dati complessivi**.
3. Si apre la finestra che contiene i dati di tabella di report. Per includere nel report determinate statistiche, premere il pulsante **Dati complessivi** nella barra degli strumenti e selezionare i tipi richiesti dalla lista a cascata: **Statistiche di scansione**, **Minacce**, **Task**, **Avvio/Arresto**, **Errori**. Le statistiche che vengono incluse in queste sezioni del report corrispondono alle statistiche contenute nei punti corrispondenti della sezione **Tabelle**. Per visualizzare il report con le tabelle selezionate, premere il pulsante **Aggiorna**.
4. Per visualizzare le informazioni per un determinato periodo, indicare un periodo relativamente al giorno odierno nella lista a cascata o impostare un intervallo di tempo nella barra degli strumenti. Per impostare un intervallo di tempo, inserire le date richieste o premere le icone

del calendario accanto ai campi di date.Per visualizzare le informazioni, premere il pulsante **Aggiorna**.

5. Se occorre salvare il report in modo da stamparlo o da elaborarlo in seguito, premere uno dei pulsanti:

   Registra le informazioni in file CSV,

   Registra le informazioni in file HTML,

   Registra le informazioni in file XML,

   Registra le informazioni in file PDF.

7.6.1.2. Statistiche di scansione

Per ottenere le statistiche del funzionamento degli elementi antivirus su postazione:

1. Nella lista gerarchica selezionare una postazione o un gruppo.

   Se è necessario visualizzare le statistiche per diverse postazioni o gruppi, si possono selezionare le postazioni richieste utilizzando i tasti MAIUSCOLO o CTRL.

2. Nel menu di gestione nella sezione **Statistiche** selezionare la voce **Statistiche di scansione**.
3. Si apre la finestra delle statistiche. Di default vengono visualizzate le statistiche per le ultime ventiquattro ore.
4. Per visualizzare le informazioni per un determinato periodo, indicare un periodo relativamente al giorno odierno nella lista a cascata o impostare un intervallo di tempo nella barra degli strumenti. Per impostare un intervallo di tempo, inserire le date richieste o premere sulle icone del calendario accanto ai campi di date.Per visualizzare le informazioni, premere il pulsante **Aggiorna**. Nella finestra verranno caricate le tabelle con i dati statistici.
5. Nella sezione **Statistiche complessive** vengono riportati i dati riepilogativi:
   - se sono selezionate postazioni – per le postazioni selezionate;
   - se sono selezionati gruppi – per i gruppi selezionati. Se sono stati selezionati diversi gruppi, vengono visualizzati soltanto i gruppi che contengono postazioni;
   - se sono selezionate contemporaneamente postazioni e gruppi – separatamente per tutte le postazioni, comprese quelle inclusi nei gruppi non vuoti selezionati.
6. Per visualizzare le statistiche dettagliate del funzionamento di elementi antivirus specifici, premere sul nome di postazione nella tabella. Se sono stati selezionati dei gruppi, premere sul nome di gruppo nella tabella delle statistiche generali e quindi sul nome di postazione nella tabella visualizzata. Si apre una finestra (o una sezione della finestra attuale) contenente una tabella con le statistiche dettagliate.
7. Dalla tabella con le statistiche del funzionamento di elementi antivirus della postazione o del gruppo, si può aprire la finestra di configurazione di un componente antivirus concreto. Per farlo, premere sul nome del relativo componente nella tabella delle statistiche.
8. Per ordinare i dati di una colonna della tabella, premere la freccia corrispondente (ordine decrescente o crescente) nell'intestazione della colonna corrispondente.

9. Se occorre salvare un report in modo da stamparlo o elaborarlo in seguito, premere uno dei pulsanti:

   Registra le informazioni in file CSV,

   Registra le informazioni in file HTML,

   Registra le informazioni in file XML,

   Registra le informazioni in file PDF.

10. Per ottenere le statistiche riepilogative senza suddividerle per sessioni, premere la voce **Statistiche complessive** nel menu di gestione. Si apre una finestra con le statistiche complessive.
11. Per visualizzare le statistiche di eventi di virus nel formato dei diagrammi, nel menu di gestione selezionare la voce **Grafici**. Si apre la finestra di visualizzazione dei diagrammi statistici (per la descrizione dettagliata v. sotto).

7.6.1.3. Stato

Per visualizzare le informazioni circa lo stato delle postazioni:

1. Nella lista gerarchica selezionare una postazione o un gruppo.
2. Nel menu di gestione nella sezione **Statistiche** selezionare la voce **Stato**.
3. Le informazioni circa lo stato delle postazioni vengono visualizzate in base ai parametri del filtro. Nella barra degli strumenti sono disponibili i seguenti parametri del filtro:
   - Nella lista a cascata **Periodo** selezionare il periodo durante cui si è verificato un evento. Nel campo del periodo viene visualizzato il numero di giorni corrispondente al valore selezionato: nella lista verranno visualizzate le postazioni su cui gli eventi si sono verificati durante il tempo impostato.
   - Nella lista **Gravità** impostare un'opzione per selezionare il livello minimo di importanza dei messaggi: la lista dei messaggi sullo stato includerà i messaggi con il livello selezionato e superiori.
   - Nella lista **Fonte** spuntare i flag per le fonti di comparsa di eventi che dovranno essere visualizzate nella lista:
     - **Agent** – per visualizzare gli eventi arrivati dagli Agent Dr.Web connessi a questo Server.
     - **Server** – per visualizzare gli eventi arrivati da questo Server Dr.Web.
     - **Online** – per visualizzare gli eventi per le postazioni che sono connesse a questo Server e sono attualmente in rete (online).
     - **Offline** – per visualizzare gli eventi per le postazioni che sono connesse a questo Server e non sono attualmente in rete (offline).
     - **Disinstallati** – per visualizzare l'ultimo evento per le postazioni su cui il software antivirus Dr.Web è stato rimosso.
4. Premere il pulsante **Aggiorna** per applicare le impostazioni di filtraggio selezionate e visualizzare i dati corrispondenti.
5. Le informazioni di questa tabella possono essere visualizzate ed elaborate nel modo uguale a quello descritto sopra per la tabella delle statistiche della scansione.

Inoltre, si possono visualizzare i risultati del funzionamento e le statistiche di diverse postazioni. Per farlo, occorre selezionare queste postazioni nella lista gerarchica della rete.

6. Se occorre salvare un report in modo da stamparlo o elaborarlo in seguito, premere uno dei pulsanti:

   Registra le informazioni in file CSV,

   Registra le informazioni in file HTML,

   Registra le informazioni in file XML,

   Registra le informazioni in file PDF.

7.6.2. Grafici

Grafici delle infezioni

Per visualizzare grafici generali con informazioni sulle infezioni rilevate:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo. Nel menu di gestione che si è aperto nella sezione **Generali** selezionare la voce **Grafici**.
2. Si apre una finestra che contiene le seguenti informazioni grafici:
   - **Attività di virus** – nel grafico viene visualizzato il numero totale di oggetti malevoli trovati entro ogni intervallo di tempo per tutte le postazioni e gruppi selezionati. Il grafico viene visualizzato se è stato impostato un periodo di tempo superiore a ventiquattro ore.
   - **Le minacce più diffuse** – viene riportata una lista di dieci minacce riscontrate nel più grande numero di file. Nel grafico vengono visualizzati i dati numerici degli oggetti corrispondenti a una particolare minaccia.
   - **Classi delle minacce** – viene riportata una lista delle minacce in base alla classificazione degli oggetti malevoli. Un diagramma circolare mostra la percentuale di tutte le minacce rilevate.
   - **Le postazioni più infette** – viene riportata una lista delle postazioni su cui sono state rilevate delle minacce alla sicurezza. Il grafico mostra il numero totale di minacce per ciascuna postazione.
   - **Azioni eseguite** – viene riportata una lista delle azioni eseguite sugli oggetti malevoli rilevati. Un diagramma circolare mostra la percentuale di tutte le azioni eseguite.
3. Per visualizzare le informazioni grafiche per un determinato periodo, selezionare un intervallo di tempo da una lista a cascata nella barra degli strumenti: report per un determinato giorno o mese. Oppure si può impostare un intervallo di tempo, per farlo inserire le date richieste o selezionare le date dai calendari a discesa. Per visualizzare le informazioni, premere il pulsante **Aggiorna**.
4. Per escludere una voce dalla visualizzazione nel grafico (salvo il grafico **Attività di virus**), premere il nome di questa voce nella legenda sotto il grafico.

Grafici delle statistiche complessive

I dati grafici vengono riportati nella voce **Grafici** della sezione **Generali** e in alcune voci della sezione **Statistiche** del menu di gestione. La tabella sottostante riporta una lista dei possibili grafici e le sezioni del menu di gestione in cui questi grafici vengono visualizzati.

Tabella 7-5. Corrispondenza dei grafici alle sezioni del menu di gestione

Grafici	Sezioni
Attività di virus	Grafici
Le minacce più diffuse	Grafici Minacce Statistiche delle minacce
Classi delle minacce	Grafici Statistiche delle minacce
Le postazioni più infette	Grafici
Azioni eseguite	Grafici Minacce
Numero di errori per postazione	Errori
Numero di errori per componente	Errori
Minacce per componente	Avvio/Arresto
Errori per componente	Avvio/Arresto

- **Numero di errori per postazione** – viene riportata una lista delle postazioni su cui si verificavano errori nel funzionamento dei componenti antivirus. Il grafico mostra il numero totale di errori per ciascuna postazione.
- **Numero di errori per componente** – viene riportata una lista dei componenti antivirus nel cui funzionamento si verificavano degli errori. Un diagramma circolare mostra la percentuale di errori di tutti i componenti.
- **Minacce per componente** – viene riportata una lista dei componenti antivirus che hanno rilevato le minacce. Il grafico mostra il numero totale di minacce rilevate da ciascuno componente.
- **Errori per componente** – viene riportata una lista dei componenti antivirus nel cui funzionamento si verificavano degli errori. Il grafico mostra il numero totale di errori di ciascuno componente.

7.6.3. Quarantena

Contenuti di Quarantena

File possono essere aggiunti a Quarantena da uno dei componenti antivirus, per esempio da Scanner.

L'utente può scansionare nuovamente in autonomo i file che si trovano in Quarantena, utilizzano il Pannello di controllo o la gestione di Quarantena sulla postazione.

Per visualizzare e modificare i contenuti di Quarantena nel Pannello di controllo:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo. Nel menu di gestione nella sezione **Generali** selezionare la voce **Quarantena**.
2. Si apre una finestra che contiene i dati tabulari sullo stato corrente di Quarantena.

   Se è stata selezionata una postazione, viene visualizzata una tabella con gli oggetti che si trovano in Quarantena su questa postazione.

   Se sono state selezionate diverse postazioni o un gruppo o diversi gruppi, viene visualizzato un set di tabelle che contengono gli oggetti di quarantena separatamente per ciascuna postazione.

   Le statistiche su una scansione ripetuta di un oggetto in Quarantena, riportate nella colonna **Informazioni**, tengono conto soltanto di una scansione ripetuta avviata attraverso il Pannello di controllo.

   Se per un oggetto in Quarantena è dichiarato lo status **non è infetto**, questo significa che dopo lo spostamento in Quarantena di questo oggetto classificato come una minaccia è stata eseguita una scansione ripetuta e all'oggetto è stato attribuito lo status di un oggetto sicuro.

   È possibile ripristinare oggetti da Quarantena soltanto manualmente.
3. Per visualizzare i file che sono stati messi in Quarantena in un determinato periodo di tempo, specificare il periodo richiesto nella barra degli strumenti e premere il pulsante **Aggiorna**.
4. Per gestire i file in Quarantena, spuntare il flag che corrisponde a un file, a un gruppo di file o a tutti i file in Quarantena (nell'intestazione della tabella). Nella barra degli strumenti selezionare una delle seguenti azioni:
   - **Recupera files** – per ripristinare i file da Quarantena.

     Utilizzare questa funzione soltanto se si è sicuri che l'oggetto è innocuo.

     Dal menu a cascata selezionare una delle opzioni:

     a) **Recupera files** – per far tornare il file alla sua posizione originale sul computer (ripristinare il file nella cartella dove era prima dello spostamento in Quarantena).

b) **Recupera files al percorso indicato** – per trasferire il file nella cartella indicata dall'amministratore.

- **Rimuovere files** – per rimuovere i file selezionati da Quarantena e dal sistema.
- **Scansiona files** – per eseguire un'altra scansione dei file selezionati in Quarantena.
- **Esportazione** – per copiare e salvare i file selezionati in Quarantena.

Dopo che i file sospetti sono stati messi nella Quarantena locale sul computer dell'utente, si possono copiare questi file tramite il Pannello di controllo e salvarli tramite il browser web, per esempio per il fine di mandarli successivamente per analisi al laboratorio antivirus Doctor Web. Per il salvataggio, spuntare i flag di fronte ai file richiesti e premere il pulsante **Esportazione**.

- Esportare i dati sullo stato di Quarantena in un file in uno dei seguenti formati:
  - **Registra le informazioni in file CSV**,
  - **Registra le informazioni in file HTML**,
  - **Registra le informazioni in file XML**,
  - **Registra le informazioni in file PDF**.

7.7. Invio dei file d'installazione

Quando viene creato un nuovo account di postazione, nel Pannello di controllo viene generato un pacchetto di installazione di Agent Dr.Web personale. Il pacchetto di installazione include l'installer di Agent Dr.Web e un set di impostazioni per la connessione al Server Dr.Web e per l'approvazione della postazione sul Server Dr.Web (il pacchetto di installazione e il relativo processo di installazione di Agent sono descritti nella **Guida all'installazione**, nella sezione Installazione locale di Agent Dr.Web).

Dopo aver creato i pacchetti di installazione, per la comodità della loro distribuzione, si possono inviare pacchetti di installazione specifici sugli indirizzi email degli utenti.

Quando i pacchetti d'installazione vengono inviati via email, i contenuti dell'email vengono formati nel seguente modo:

1. Il sistema operativo della postazione è conosciuto:
   a) SO Windows: all'email viene allegato il pacchetto d'installazione di Agent Dr.Web per Windows.
   b) Linux, OS X, Android: all'email viene allegato il file d'installazione di Agent Dr.Web per il rispettivo sistema operativo e il file di configurazione con le impostazioni per la connessione al Server Dr.Web.
2. Il sistema operativo della postazione non è conosciuto – un nuovo account di postazione, l'Agent non è ancora installato:
   a) Se sul Server non vi sono pacchetti per le postazioni Linux, OS X, Android (in particolare, sul Server non è installato il pacchetto supplementare (extra)): all'email viene allegato il pacchetto d'installazione di Agent Dr.Web per Windows e il file di configurazione con le impostazioni per la connessione al Server Dr.Web per le postazioni Linux, OS X, Android.

b) Se sul Server vi è almeno un pacchetto oltre al pacchetto per le postazioni SO Windows: all'email viene allegato il pacchetto d'installazione di Agent Dr.Web per Windows, il file di configurazione con le impostazioni per la connessione al Server Dr.Web per le postazioni Linux, OS X, Android, nonché un link al download dei file d'installazione per le postazioni Linux, OS X, Android.

Per inviare pacchetti d'installazione via email:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica selezionare i seguenti oggetti:
   - selezionare una postazione per inviare via email il pacchetto d'installazione generato per questa postazione.
   - selezionare un gruppo di postazioni per inviare via email i pacchetti d'installazione generati per le postazioni di questo gruppo.

   Per selezionare più oggetti alla volta, utilizzare i tasti CTRL o SHIFT.
2. Nella barra degli strumenti premere **Generali** → **Invia i file di installazione**.
3. Nella sezione **Invio dei file di installazione** che si è aperta, impostare i seguenti parametri:
   - Nella sezione **E-mail dei destinatari** impostare l'indirizzo email su cui verrà inviato il pacchetto di installazione. Se sono state selezionate diverse postazioni o gruppi, impostare per ciascuna postazione separatamente di fronte al nome di questa postazione gli indirizzi email per l'invio del pacchetto di installazione.
   - Nella sezione **Avanzate** spuntare il flag **Comprimi in archivio zip** per comprimere i file dei pacchetti di installazione in un archivio zip. La compressione in archivio può essere utile se sul lato utente ci sono filtri email che bloccano la trasmissione di file eseguibili in allegati ai messaggi email.
   - Nella sezione **Mittente** indicare l'indirizzo email che verrà indicato come il mittente dell'email con i file d'installazione.
   - Nella sezione **Impostazioni del server SMTP** si impostano i parametri del server SMTP che verrà utilizzato per l'invio delle email. Se i parametri sono conosciuti, per esempio sono già stati impostati in precedenza, questa sezione è ridotta e si può espanderla e si possono modificare i parametri impostati, se necessario. Quando i pacchetti d'installazione vengono inviati per la prima volta, nella sezione che si è aperta, è necessario impostare i seguenti parametri:
     - **Indirizzo** – indirizzo del server SMTP che verrà utilizzato per l'invio delle email.
     - **Porta** – porta per la connessione al server SMTP. Di default è la porta 465 se viene aperta una connessione TLS protetta separata, altrimenti è la porta 25.
     - **Utente**, **Password** – se necessario, impostare il nome utente e la password dell'utente del server SMTP se il server SMTP richiede l'autenticazione.
     - Spuntare il flag **Crittografia STARTTLS** per lo scambio di dati crittografati. In tale caso il programma passa alla connessione protetta attraverso il comando `STARTTLS`. Di default per la connessione è previsto l'utilizzo della porta 25.

- Spuntare il flag **Crittografia SSL** per lo scambio di dati crittografati. In tale caso verrà aperta una connessione TLS protetta separata. Di default per la connessione è previsto l'utilizzo della porta 465.
- Spuntare il flag **Utilizza l'autenticazione CRAM-MD5** per utilizzare *l'autenticazione* CRAM-MD5 sul mail server.
- Spuntare il flag **Utilizza l'autenticazione DIGEST-MD5** per utilizzare *l'autenticazione* DIGEST-MD5 sul mail server.
- Spuntare il flag **Utilizza l'autenticazione Plain** per utilizzare l'autenticazione *plain text* sul mail server.
- Spuntare il flag **Utilizza l'autenticazione LOGIN** per utilizzare *l'autenticazione* LOGIN sul mail server.
- Spuntare il flag **Verifica se il certificato SSL del server è corretto** per controllare la correttezza del certificato SSL del mail server.
- Spuntare il flag **Modalità debug** per ottenere un log dettagliato di sessione SMTP.Premere il pulsante **Invia**.

7.8. Invio di messaggi alle postazioni

L'amministratore di sistema può inviare agli utenti messaggi informativi con qualsiasi contenuto che includono:

- testo del messaggio;
- link alle risorse Internet;
- logotipo della società (o qualsiasi immagine grafica);
- nella testata della finestra inoltre viene indicata la data precisa di ricezione del messaggio.

Tali messaggi vengono visualizzati sul lato utente come finestre pop-up (v. immagine 7-1).

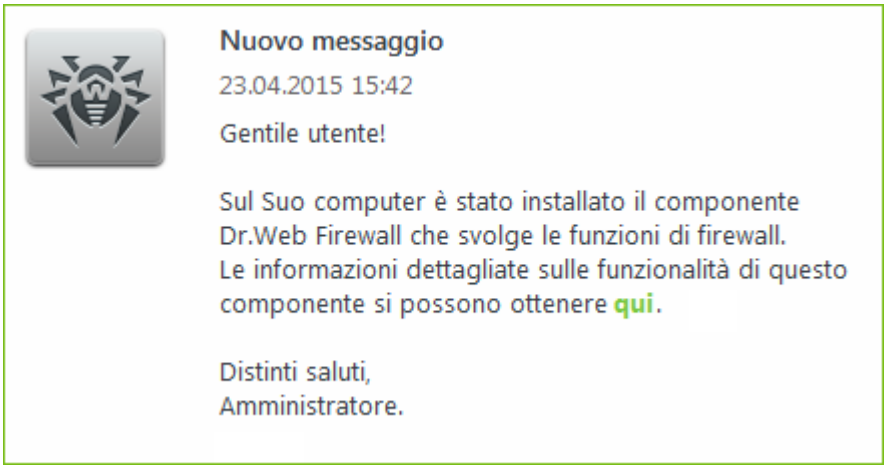


Immagine 7-1. Una finestra di messaggio su una postazione SO Windows

Per inviare un messaggio all'utente:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo.

2. Nella finestra che si è aperta nella lista gerarchica selezionare una postazione o un gruppo e nella barra degli strumenti premere **Generali** → **Invia il messaggio alle postazioni**.
3. Nella finestra che si è aperta, riempire i seguenti campi:
   - **Testo del messaggio** – campo obbligatorio. Contiene direttamente il messaggio stesso.
   - Spuntare il flag **Visualizza il logo nel messaggio** per visualizzare un oggetto grafico nella barra del titolo del messaggio. Impostare i seguenti parametri del logotipo:
     - Spuntare il flag **Utilizza trasparenza** per utilizzare la trasparenza nell'immagine del logo (v. Formato del file di logo, p. 4).
     - Nel campo **URL** si può indicare il link alla pagina web che si apre quando si preme sul logo e sulla testata della finestra.
     - Nel campo **Intestazione del messaggio** si può inserire un'intestazione del messaggio, per esempio il nome della società. Tale testo verrà visualizzato nella testata della finestra del messaggio a destra del logo. Se questo campo rimane vuoto, invece dell'intestazione nella finestra di messaggio verranno visualizzate le informazioni sul messaggio.
     - A destra del campo **File del logo** premere il pulsante per caricare il file di logo da risorsa locale e selezionare l'oggetto desiderato in esplora risorse di file system (v. Formato del file di logo).

   Se il logotipo non è impostato, o la dimensione del logotipo eccede la dimensione massima ammissibile (v. Formato del file di logo, p. 3), invece del logotipo nella finestra di messaggio verrà visualizzata l'icona di Agent Dr.Web.
   - Spuntare il flag **Mostra link nel messaggio** per includere nel messaggio un link a risorse web.

   Per aggiungere un link:
   1. Nel campo **URL** impostare un link ad una risorsa Internet.
   2. Nel campo **Testo** indicare il nome del link – il testo che verrà visualizzato invece del link nel messaggio.
   3. Nel campo **Testo del messaggio** aggiungere il marcatore `{link}` ovunque è necessario aggiungere il link. Nel messaggio risultante, invece di esso viene inserito il link con i parametri indicati. Il numero di tag `{link}` nel testo non è limitato, però ogni tag ha gli stessi parametri dai campi **URL** e **Testo**.
   - Spuntare il flag **Invia soltanto alle postazioni online** per inviare il messaggio soltanto alle postazioni online. Se il flag è spuntato, il messaggio non verrà inviato alle postazioni offline. Se il flag è tolto, l'invio del messaggio alle postazioni offline verrà rinviato fino al momento della loro connessione.
   - Spuntare il flag **Mostra lo stato dell'invio** per visualizzare un avviso con lo stato dell'invio del messaggio.
4. Premere il pulsante **Invia**.

Formato del file di logo

Il file con un'immagine grafica (logotipo), che viene incluso nel messaggio, deve soddisfare le seguenti condizioni:

1. Formato di file grafico: BMP, JPG, PNG, GIF, SVG.
2. La dimensione del file di logo non deve eccedere 512 KB.
3. Le dimensioni d'ingombro dell'immagine sono di 72x72 pixel. Le immagini di altre dimensioni verranno ridimensionate per l'invio fino alla dimensione predefinita.
4. La profondità di colore (bit depth) è qualsiasi (8 – 24 bit).
5. Se all'invio del messaggio, è spuntato il flag **Utilizza trasparenza**, il primo pixel nella posizione (0,0) viene dichiarato trasparente. Tutti i pixel che hanno lo stesso colore diventano trasparenti, e invece di essi viene visualizzato lo sfondo della finestra di messaggio.

   Se si utilizza l'opzione **Utilizza trasparenza** per un logotipo rettangolare, è consigliabile fare una cornice rettangolare per evitare che i pixel dell'immagine di logo stessa vengano impostati come trasparenti in modo sbagliato.

   L'utilizzo dell'opzione **Utilizza trasparenza** è utile nel caso di una forma non standard (non rettangolare) del logo per escludere lo sfondo indesiderabile che completa la parte informativa per renderla rettangolare. Per esempio se si utilizza come il logo l'immagine riportata nella figura 7-2, lo sfondo viola viene escluso (diventa trasparente).

Immagine 7-2. Logotipo di una forma non standard

Se si vuole utilizzare nel messaggio un logo con lo sfondo trasparente, utilizzare i file nel formato PNG o GIF.

Prima di inviare il messaggio all'utente (soprattutto su molteplici indirizzi), si consiglia di inviarlo preliminarmente a qualsiasi computer con l'Agent installato per controllare la correttezza del risultato.

Esempio dell'invio del messaggio

Per avviare il messaggio riportato nell'immagine 7-1 sono stati impostati i seguenti parametri:

Testo del messaggio:

```
Gentile utente!



Sul Suo computer è stato installato il componente Dr.Web Firewall che svolge
le funzioni di firewall.

Le informazioni dettagliate sulle funzionalità di questo componente si pos-
sono ottenere {link}.



Distinti saluti,

Amministratore.
```

URL: `http://drweb.com/`

Testo: `qui`

Capitolo 8: Configurazione del Server Dr.Web

In questo capitolo vengono descritte le seguenti possibilità di gestione dei parametri di funzionamento della rete antivirus e del Server Dr.Web:

- Logging – per visualizzare e gestire i log di funzionamento del Server, per visualizzare le informazioni statistiche dettagliate sul funzionamento del Server;
- Configurazione del Server Dr.Web – per configurare i parametri di funzionamento del Server;
- Configurazione del calendario di Server Dr.Web – per configurare un calendario dei task per la manutenzione del Server;
- Configurazione del web server – per configurare i parametri di funzionamento del web server;
- Procedure personalizzate – per collegare e configurare procedure personalizzate;
- Configurazione degli avvisi – per configurare il sistema di avviso che notifica l'amministratore su eventi della rete antivirus e fornisce diversi modi per consegnare messaggi;
- Gestione del repository di Server Dr.Web – per configurare il repository per l'aggiornamento di tutti i componenti della rete antivirus da SAM e per la successiva distribuzione degli aggiornamenti su postazioni;
- Gestione del database – per la manutenzione diretta del database di Server;
- Caratteristiche di una rete con diversi Server Dr.Web – per configurare una rete antivirus con diversi server e per configurare le reazioni tra i server.

8.1. Log

8.1.1. Log di verifica

Il log di verifica consente di visualizzare la lista degli eventi e delle modifiche apportate tramite i sottosistemi di gestione di Dr.Web Enterprise Security Suite.

Per visualizzare il log di verifica:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Log di verifica**.
3. Si apre una finestra con una tabella delle azioni registrate. Per configurare la visualizzazione del log, impostare nella barra degli strumenti un periodo durante cui sono state eseguite le azioni. Per farlo, si può selezionare dalla lista a discesa uno dei periodi proposti o impostare qualsiasi data nei calendari che vengono aperti quando si fa clic sui campi delle date. Premere **Aggiorna** per visualizzare il log per le date selezionate.
4. La tabella del log contiene le seguenti informazioni:
   - **Data** – la data e l'ora quando è stata eseguita l'azione.

- **Nome utente** – il nome utente dell'amministratore di Server. Viene specificato se l'azione è stata avviata direttamente dall'amministratore o in caso di una connessione al Server secondo le credenziali dell'amministratore.
- **Indirizzo** – l'indirizzo IP da cui è stata avviata l'esecuzione di quest'azione. Viene indicato soltanto in caso di una connessione esterna al Server, in particolare attraverso il Pannello di controllo o attraverso Web API.
- **Sottosistema** – il nome del sottosistema da cui o attraverso cui è stata avviata l'azione. Il log di verifica viene registrato per i seguenti sottosistemi:
  - **Pannello di controllo** – l'azione è stata eseguita attraverso il Pannello di controllo della sicurezza Dr.Web, in particolare dall'amministratore.
  - **Web API** – l'azione è stata eseguita attraverso Web API, per esempio da un'applicazione esterna connessa in base alle credenziali dell'amministratore (v. inoltre il documento **Allegati**, p. Allegato L. Integrazione di Web API e di Dr.Web Enterprise Security Suite).
  - **Server** – l'azione è stata eseguita dal Server Dr.Web, per esempio secondo il suo calendario.
  - **Utility** – l'azione è stata avviata attraverso le utility esterne, in particolare attraverso l'utility di diagnostica remota di Server.
- **Risultato** – il breve risultato dell'esecuzione dell'azione:
  - **OK** – l'operazione è stata eseguita con successo.
  - **non riuscito** – un errore è occorso durante l'esecuzione dell'operazione. L'operazione non è stata eseguita.
  - **cominciato** – l'esecuzione dell'operazione è stata avviata. Il risultato dell'esecuzione dell'operazione sarà noto soltanto dopo il suo completamento.
  - **non ci sono permessi** – l'amministratore che ha avviato l'esecuzione dell'operazione non ha i permessi per la sua esecuzione.
  - **differito** – l'esecuzione dell'azione è stata rinviata fino al verificarsi di un determinato termine o evento.
  - **impossibile** – l'esecuzione dell'azione richiesta è vietata. Per esempio, l'eliminazione dei gruppi di sistema.

Per le azioni fallite (il valore **non riuscito** nella colonna **Risultato**) le righe vengono marcate in rosso.

- **Operazione** – una descrizione dell'azione.

5. Se necessario, è possibile esportare in file le informazioni per un periodo selezionato. Per farlo, nella barra degli strumenti premere uno dei seguenti pulsanti:

 **Registra le informazioni in file CSV**,

 **Registra le informazioni in file HTML**,

 **Registra le informazioni in file XML**,

 **Registra le informazioni in file PDF**.

8.1.2. Log di funzionamento di Server Dr.Web

Il Server Dr.Web registra in un log gli eventi relativi al suo funzionamento.

> Il log di Server viene utilizzato per il debugging e per l'eliminazione di inconvenienti in caso di funzionamento non corretto dei componenti della rete antivirus.

Di default, il file di log si chiama `drwcsd.log` e si trova in:

- In SO **UNIX**:
  - in caso di SO Linux e SO Solaris: `/var/opt/drwcs/log/drwcsd.log`;
  - in caso di SO FreeBSD: `/var/drwcs/log/drwcsd.log`.
- In SO **Windows**: nella sottodirectory `var` della directory di installazione di Server.

Il file è di formato di testo semplice (v. il documento **Allegati**, sezione Allegato K. Formato dei file di log).

Per visualizzare il log di funzionamento di Server tramite il Pannello di controllo:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Log del Server Dr.Web**.
3. Si apre una finestra con l'elenco dei log di funzionamento del Server. Secondo le impostazioni della modalità di rotazione, viene utilizzato il seguente formato dei nomi dei file di log di Server: <*file_name*>.<*N*>.`log` o <*file_name*>.<*N*>.`log.gz`, dove <*N*> – un numero progressivo: 1, 2, ecc. Per esempio, se il file ha il nome `drwcsd`, l'elenco dei file di log di funzionamento sarà il seguente:
   - `drwcsd.log` – file corrente (in cui le informazioni vengono registrate al momento),
   - `drwcsd.1.log.gz` – file precedente,
   - `drwcsd.2.log.gz` e così via, più alto è il numero, più vecchia è la versione del file.
4. Per gestire i file di log, spuntare i flag accanto al file o diversi file richiesti. Per selezionare tutti i file di log, spuntare il flag nell'intestazione della tabella. Nella barra degli strumenti saranno disponibili i seguenti pulsanti:

   Esporta i file di log selezionati – per salvare una copia locale dei file di log selezionati. Si può usare il salvataggio di copia di log, per esempio per visualizzare i contenuti del file di log da un computer remoto.

   Rimuovi i file di log selezionati – per rimuovere i file di log selezionati senza la possibilità di recupero.

Configurazione del log di funzionamento per UNIX

I Server Dr.Web sotto gli SO della famiglia UNIX includono la possibilità di configurare la registrazione del log di funzionamento di Server attraverso un file di configurazione separato:

- in caso di SO Linux e SO Solaris: `/var/opt/drwcs/etc/local.conf`;
- in caso di SO FreeBSD: `/var/drwcs/etc/local.conf`.

Contenuti del file `local.conf`:

```
# Log level.

DRWCS_LEV=trace3

# Log rotation.

DRWCS_ROT=10,10m
```

I valori dei parametri corrispondono ai valori delle opzioni della riga di comando per l'avvio di Server:

- `-verbosity=`<*livello_di_dettaglio*> – livello di dettaglio del log di funzionamento di Server.
- `-rotate=`<*N*><*f*>`,`<*M*><*u*> – modalità di rotazione del log di funzionamento di Server.

La descrizione dettagliata delle opzioni è riportata nel documento **Allegati**, sezione H4.8.

> Se il file `local.conf` è stato modificato nel processo del funzionamento di Server, è necessario riavviare Server di modo che abbiano effetto le modifiche nelle impostazioni della registrazione del log. Il riavvio deve essere eseguito dal sistema operativo.

Se Server viene aggiornato o rimosso, viene eseguito il backup del file `local.conf`, il che consente di controllare il livello di registrazione del log in caso di un aggiornamento batch di Server.

8.1.3. Log di aggiornamento del repository

Il log di aggiornamento del repository contiene un elenco degli aggiornamenti da SAM che include le informazioni dettagliate su revisioni aggiornate dei prodotti.

Per visualizzare il log di aggiornamento del repository:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Log di aggiornamento del repository**.
3. Si apre una finestra con una tabella delle azioni registrate. Per configurare la visualizzazione del log, impostare nella barra degli strumenti un periodo durante cui sono state eseguite le azioni. Per farlo, si può selezionare dalla lista a discesa uno dei periodi proposti o impostare

qualsiasi data nei calendari che vengono aperti quando si fa clic sui campi delle date. Premere **Aggiorna** per visualizzare il log per le date selezionate.

4. La tabella del log contiene le seguenti informazioni:
   - **Inizio** – la data e l'ora di inizio del caricamento degli aggiornamenti di un prodotto specifico da SAM.
   - **Terminazione** – la data e l'ora di fine del caricamento degli aggiornamenti di un prodotto specifico da SAM.
   - **Nome del prodotto** – il nome del prodotto di repository che è stato caricato o di cui il caricamento è stato richiesto.
   - **Risultato dell'aggiornamento** – il risultato dell'aggiornamento del repository. Contiene le brevi informazioni sul completamento di aggiornamento riuscito o la causa dell'errore.

     Per le azioni fallite le celle **Risultato dell'aggiornamento** vengono marcate in rosso.

   - **Revisione iniziale** – il numero della revisione (le revisioni vengono numerate in base alla data di creazione) che è stata l'ultima per questo prodotto prima dell'inizio del processo di aggiornamento.
   - **Revisione dall'aggiornamento** - il numero della revisione (le revisioni vengono numerate in base alla data di creazione) che è stata caricata nel corso dell'aggiornamento.
   - **File aggiornati** – un riepilogo dei file modificati. Viene riportato nel formato: <*numero di file*> – <*azione eseguita con i file*>.
   - **Iniziatore** – il sistema che ha avviato il processo di aggiornamento:
     - **Avviato dalla riga di comando** – l'aggiornamento è stato avviato dall'amministratore tramite il comando di console corrispondente.
     - **Avviato dallo Scheduler** – l'aggiornamento è stato avviato secondo un task nel calendario del Server Dr.Web.
     - **Aggiornamento tra i server** – l'aggiornamento è stato ricevuto attraverso la comunicazione tra i server dal Server principale. Questo tipo di iniziatore è presente soltanto nel caso di una configurazione di rete antivirus con diversi server con la distribuzione degli aggiornamenti attraverso la comunicazione tra i server.
     - **Avviato dal Pannello di controllo** – l'aggiornamento è stato avviato dall'amministratore tramite il Pannello di controllo della sicurezza Dr.Web, nella sezione Stato del repository.
     - **Importazione del repository** – l'aggiornamento è stato caricato dall'amministratore attraverso la sezione Contenuti del repository del Pannello di controllo.
   - **Amministratore** – il nome utente dell'amministratore di Server. È presente se l'azione è stata avviata direttamente dall'amministratore.
   - **Indirizzo di rete** – l'indirizzo IP da cui è stata avviata l'esecuzione di quest'azione. È presente soltanto nel caso di una connessione esterna al Server, in particolare attraverso il Pannello di controllo o attraverso Web API.
   - **Directory nel repository** – il nome della directory di repository di Server che è stata modificata secondo il processo di aggiornamento.

5. Per visualizzare le informazioni dettagliate su un aggiornamento concreto, premere la riga di questo aggiornamento. Si apre una finestra con una tabella delle informazioni sui file del prodotto modificati durante l'aggiornamento selezionato. Per ciascun file vengono riportate le seguenti informazioni: **Nome del file**, **Hash del file**, **Dimensione** e **Stato**.
6. Se necessario, è possibile esportare in file le informazioni per un periodo selezionato. Per farlo, nella barra degli strumenti premere uno dei seguenti pulsanti:

   Registra le informazioni in file CSV,

   Registra le informazioni in file HTML,

   Registra le informazioni in file XML,

   Registra le informazioni in file PDF.

8.2. Configurazione del Server Dr.Web

Ogni volta che si salvano modifiche della sezione **Configurazione del Server Dr.Web**, viene automaticamente salvato un backup della versione precedente del file di configurazione del Server. Vengono conservati gli ultimi 10 backup.

I backup si trovano nella stessa directory del file di configurazione e vengono denominati nel seguente formato:

`drwcsd.conf;<ora_di_creazione>`

È possibile utilizzare i backup creati, in particolare, per ripristinare il file di configurazione se l'interfaccia del Pannello di controllo non è disponibile.

Per configurare il Server Dr.Web:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Configurazione del Server Dr.Web**. Si apre la finestra di configurazione di Server.

   I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

3. Nella barra degli strumenti sono disponibili i seguenti pulsanti per gestire le impostazioni della sezione:

   Riavvia Server Dr.Web – per riavviare il Server al fine di accettare le modifiche apportate in questa sezione. Il pulsante diventa attivo dopo che si sono apportate delle modifiche nelle impostazioni della sezione e si è premuto il pulsante **Salva**.

   Recupera la configurazione da copia di backup – una lista a cascata che include le copie salvate delle impostazioni dell'intera sezione a cui si può ritornare dopo aver apportato delle modifiche. Il pulsante diventa attivo dopo che si sono apportate delle modifiche nelle impostazioni della sezione e si è premuto il pulsante **Salva**.

Resetta tutti i parametri ai valori iniziali – per ripristinare tutti i parametri di questa sezione ai valori che avevano prima della modifica corrente (ultimi valori salvati).

Resetta tutti i parametri ai valori default – per ripristinare tutti i parametri di questa sezione ai valori di default.

4. Per accettare le modifiche apportate nelle impostazioni della sezione, premere il pulsante **Salva**, dopodiché sarà necessario riavviare il Server. Per farlo, premere il pulsante **Riavvia Server Dr.Web** nella barra degli strumenti di questa sezione.

8.2.1. Generali

Nella scheda **Generali** vengono configurate le seguenti impostazioni del funzionamento di Server:

- **Nome di Server Dr.Web** – il nome di questo Server. Se il valore del campo non è impostato, viene utilizzato il nome del computer su cui è installato il Server Dr.Web.
- **Lingua del Server** – la lingua che viene utilizzata di default dai componenti e sistemi di Server Dr.Web, se non è stato possibile ottenere le impostazioni di lingua dal database di Server. In particolare, si usa per il Pannello di controllo della sicurezza Dr.Web e il sistema di avviso dell'amministratore, se il database è stato danneggiato e non è possibile ottenere le impostazioni di lingua.
- **Numero di richieste parallele dai client** – il numero di flussi per l'elaborazione dei dati che arrivano dai client: Agent, installer di Agent, Server adiacenti. Questo parametro influisce sulle prestazioni del Server. Si consiglia di modificare il valore predefinito soltanto dopo l'approvazione da parte del servizio di supporto tecnico.
- **Numero di connessioni al database** – il numero di connessioni di Server al database. Si consiglia di modificare il valore predefinito soltanto dopo l'approvazione da parte del servizio di supporto tecnico.

A partire dalla versione 10, non viene più fornita la possibilità di modificare il parametro **Coda di autenticazione** attraverso il Pannello di controllo.

Di default, quando viene installato il nuovo Server, questo parametro viene impostato pari a 50. Se il server viene aggiornato da una versione precedente e viene mantenuto il file di configurazione, il valore di coda di autenticazione viene mantenuto dalla configurazione della versione precedente.

Se è necessario modificare la lunghezza della coda di autenticazione, modificare il valore del seguente parametro nel file di configurazione di Server:

```
<!-- Maximun authorization queue length -->
<maximum-authorization-queue size='50'/>
```

- Spuntare il flag **Limita il volume del traffico dati degli aggiornamenti** per limitare il traffico dati di rete quando gli aggiornamenti vengono trasmessi tra il Server e gli Agent.

  Se il flag è spuntato, inserire nel campo **Velocità di trasmissione massima (KB/s)** un valore della velocità massima di trasmissione degli aggiornamenti. Gli aggiornamenti verranno trasmessi entro la larghezza di banda impostata per il traffico dati cumulativo degli aggiornamenti

di tutti gli Agent.

Se la spunta al flag è tolta, gli aggiornamenti vengono trasmessi agli Agent senza la limitazione della larghezza di banda.

- Nella lista a cascata **Modalità di registrazione dei nuovi arrivi** viene definito il criterio di ammissione delle nuove postazioni (v p. Criteri di approvazione delle postazioni).
  - La lista a cascata **Gruppo primario predefinito** definisce il gruppo primario in cui le postazioni verranno messe se l'accesso delle postazioni al Server viene approvato in maniera automatica.
- Spuntare il flag **Trasferisci le postazioni non autenticate in nuovi arrivi** per resettare per le postazioni non autenticate i parametri con cui possono ottenere l'accesso a Server. Questa opzione potrebbe essere utile in caso di modifica delle impostazioni del Server (quali, per esempio, la chiave di cifratura pubblica) o in caso di cambio del database. In tali casi le postazioni non potranno connettersi e dovranno ricevere le nuove impostazioni di accesso al Server.
- Dalla lista a cascata **Crittografia** viene selezionato il criterio di codifica dei dati trasmessi attraverso il canale di comunicazione tra il Server Dr.Web e i client connessi: Agent, Server adiacenti, Installer di rete.

  Per maggiori informazioni su questi parametri v. p. Utilizzo di cifratura e di compressione di traffico.
- Dalla lista a cascata **Compressione** viene selezionato il criterio di compressione dei dati trasmessi attraverso il canale di comunicazione tra il Server Dr.Web e i client connessi: Agent, Server adiacenti, Installer di rete. Per maggiori informazioni su questi parametri v. p. Utilizzo di cifratura e di compressione di traffico.
  - Se vengono selezionati i valori **Sì** e **Possibile** per la compressione del traffico dati, diventa disponibile la lista a cascata **Grado di compressione**. Da questa lista si può selezionare un grado di compressione dei dati da 1 a 9, dove 1 è il grado minimo e 9 è il grado massimo di compressione.
- Nel campo **Differenza ammissibile tra l'ora del Server e dell'Agent** viene definita la differenza ammissibile in minuti tra l'ora di sistema sul Server Dr.Web e sugli Agent. Se la differenza è maggiore del valore specificato, ciò verrà segnalato nello stato della postazione sul Server Dr.Web. Di default, è ammissibile la differenza di 3 minuti. Il valore 0 significa che il controllo non verrà eseguito.
- Spuntare il flag **Sostituisci gli indirizzi IP** per sostituire gli indirizzi IP con i nomi DNS dei computer nel file di log di Server Dr.Web.
- Spuntare il flag **Sostituisci i nomi NetBIOS** affinché nella directory rete antivirus del Pannello di controllo vengano visualizzati i nomi DNS delle postazioni invece dei nomi NetBIOS (se un nome a dominio non può essere determinato, viene visualizzato l'indirizzo IP).

Di default, entrambi i flag **Sostituisci gli indirizzi IP** e **Sostituisci i nomi NetBIOS** sono deselezionati. In caso di configurazione scorretta del servizio DNS, l'attivazione di queste possibilità potrebbe rallentare notevolmente il funzionamento del Server. Se viene attivata una di queste modalità, si consiglia di consentire la memorizzazione dei nomi nella cache su server DNS.

Se il flag **Sostituisci i nomi NetBIOS** è selezionato, e nella rete antivirus viene utilizzato un Server proxy, per tutte le postazioni connesse al Server attraverso il Server proxy nel Pannello di controllo come i nomi di postazioni verrà visualizzato il nome del computer su cui è installato il Server proxy.

- Spuntare il flag **Sincronizza le descrizioni delle postazioni** per sincronizzare la descrizione del computer dell'utente con la descrizione della rispettiva postazione nel Pannello di controllo (campo Computer description sulla pagina System properties). Se la descrizione della postazione non è disponibile nel Pannello di controllo, in questo campo verrà scritta la descrizione del computer disponibile sul lato utente. Se le descrizioni sono diverse, i dati nel Pannello di controllo verranno sostituiti con quelli dell'utente.
- Spuntare il flag **Segui epidemie** per attivare la modalità di avviso con cui l'amministratore viene notificato su casi di epidemie di virus. Se il flag è tolto, gli avvisi di infezioni di virus vengono spediti in modalità normale. Se il flag è spuntato, si possono inoltre impostare i seguenti parametri di monitoraggio di epidemie di virus:
  - **Periodo (s)** – il periodo in secondi in cui deve arrivare il numero impostato di avvisi di infezione affinché il Server Dr.Web mandi all'amministratore un singolo avviso di epidemia racchiudente tutti i casi di infezione.
  - **Numero di avvisi** – il numero di avvisi di infezione che devono arrivare nel periodo impostato affinché il Server Dr.Web mandi all'amministratore un singolo avviso di epidemia racchiudente tutti i casi di infezione.
- Spuntare il flag **Sincronizza la posizione geografica** per attivare la sincronizzazione della posizione geografica delle postazioni tra i Server Dr.Web in una rete antivirus con diversi server. Se il flag è spuntato, si può inoltre impostare il seguente parametro:
  - **Sincronizzazione iniziale** – numero di postazioni senza coordinate geografiche, le informazioni su cui vengono richieste quando viene stabilita una connessione tra i Server Dr.Web.

8.2.1.1. Utilizzo di cifratura e di compressione di traffico

La rete antivirus di Dr.Web Enterprise Security Suite permette di cifrare il traffico dei dati trasmessi tra il Server e le postazioni (Agent Dr.Web), tra i Server Dr.Web (se la configurazione della rete include diversi server), nonché tra il Server e gli Installer di rete. Questa modalità viene utilizzata per evitare l'eventuale divulgazione delle chiavi di utenti, nonché delle informazioni su hardware e utenti della rete antivirus nel corso della comunicazione dei componenti.

La rete antivirus Dr.Web Enterprise Security Suite utilizza i mezzi di firma digitale e di crittografia forte, basati sul concetto di coppie delle chiavi pubbliche e private.

Il criterio di utilizzo di cifratura viene impostato separatamente su ogni componente della rete antivirus, e le impostazioni di altri componenti devono corrispondere alle impostazioni del Server.

Visto che il traffico dei dati trasmessi tra i componenti, in particolare tra i Server può essere abbastanza grande, la rete antivirus permette di impostare la compressione di tale traffico. La configurazione di criterio di compressione e la compatibilità di queste impostazioni su vari componenti sono uguali alle impostazioni di cifratura.

Quando si impostano la cifratura e la compressione sul lato Server prestare attenzione alle caratteristiche dei client che si pianifica di connettere a questo Server. Non tutti i client supportano la cifratura e la compressione del traffico (per esempio, l'Antivirus Dr.Web per Android e l'Antivirus Dr.Web per OS X non supportano né la cifratura né la compressione). Non sarà possibile connettere al Server tali client se è impostato il valore **Sì** per la cifratura e/o compressione sul lato Server.

Per impostare i criteri di compressione e di cifratura per il Server Dr.Web:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Configurazione** del **Server Dr.Web**.
3. Nella scheda **Generali** selezionare dalle liste a cascata **Crittografia** e **Compressione** una delle varianti:
   - **Sì** – è obbligatoria la cifratura (o la compressione) del traffico dati scambiati con tutti i componenti (valore predefinito per la cifratura se durante l'installazione del Server non è stato impostato altrimenti),
   - **Possibile** – la cifratura (o la compressione) viene eseguita per il traffico dei dati scambiati con i componenti, le cui impostazioni non lo bloccano,
   - **No** – la cifratura (o la compressione) non è supportata (valore predefinito per la compressione se durante l'installazione del Server non è stato impostato altrimenti).

Quando vengono coordinate le impostazioni di criterio di cifratura e di compressione sul Server e su un altro componente (Agent o Installer di rete), si deve tenere presente che alcune combinazioni di impostazioni non sono ammissibili e la loro scelta porterà all'impossibilità di stabilire una connessione tra il Server e il componente.

Nella tabella 8-1 sono riportate le informazioni su ciò con quali impostazioni la connessione tra il Server e un componente è cifrata/compressa (+), con quali è non cifrata/non compressa (–), e quali combinazioni non sono ammissibili (**Errore**).

Tabella 8-1. Compatibilità delle impostazioni di criteri di cifratura e di compressione

Impostazioni del componente	Impostazioni del Server		
	Sì	Possibile	No
Sì	+	+	Errore
Possibile	+	+	–
No	Errore	–	–

L'utilizzo della cifratura di traffico dati crea un notevole carico di elaborazione sui computer con le prestazioni minime ammissibili per i componenti installati. Se la cifratura di traffico dati non è richiesta per assicurare la sicurezza supplementare, si può rinunciare all'utilizzo di que-

sta modalità. Inoltre, la cifratura di traffico dati non è consigliabile nelle reti grandi (più di 2000 client).

Per disattivare la modalità di cifratura, conviene prima cambiare consecutivamente il Server e i componenti a modalità **Possibile**, non lasciando che vengano create coppie incompatibili Installer di rete-Server e Agent-Server. Se questa regola non viene osservata, ciò può portare alla perdita di controllo sul componente e alla necessità di reinstallarlo.

L'utilizzo della compressione diminuisce il traffico dati ma aumenta notevolmente il carico di elaborazione dei dati sui computer, più della cifratura.

Il valore **Possibile**, impostato sul lato Agent Dr.Web, significa che di default la cifratura/compressione viene eseguita ma può essere annullata con la modifica delle impostazioni di Server Dr.Web senza dover modificare le impostazioni sul lato Agent.

8.2.2. Rete

8.2.2.1. DNS

Nella scheda **DNS** vengono impostati i parametri delle query inviate al server DNS:

- **Timeout per query DNS (secondi)** – il timeout in secondi per la risoluzione delle query DNS dirette/inverse. Impostare 0 per non limitare il tempo di attesa della fine della risoluzione di una query DNS.
- **Numero di query DNS ripetute** – il numero massimo di query DNS ripetute in caso di una risoluzione di query DNS non riuscita.
- Spuntare il flag **Imposta il tempo di conservazione delle risposte del server DNS** per impostare il tempo di conservazione di risposte del server DNS nella cache (TTL).
  - **Per le risposte positive (minuti)** – il tempo in minuti per cui le risposte positive del server DNS si conservano nella memoria cache (TTL).
  - **Per le risposte negative (minuti)** – il tempo in minuti per cui le risposte negative del server DNS si conservano nella memoria cache (TTL).
- **Server DNS** – una lista dei server DNS che sostituisce la lista di sistema predefinita.
- **Domini DNS** – una lista dei domini DNS che sostituisce la lista di sistema predefinita.

8.2.2.2. Proxy

Nella scheda **Server proxy** vengono impostati i parametri del server proxy.

Spuntare il flag **Utilizza server proxy** per configurare le connessioni di Server Dr.Web attraverso il server proxy. In questo caso, diventano disponibili le seguenti impostazioni:

- **Server proxy** – indirizzo IP o nome DNS del server proxy.

- Per utilizzare l'autenticazione per l'accesso al server proxy secondo i metodi impostati, spuntare il flag **Utilizza autenticazione** e definire i seguenti parametri:
  - Compilare i campi **Utente del proxy** e **Password dell'utente del proxy**.
  - Selezionare uno dei metodi di autenticazione:

Opzione		Descrizione
Qualsiasi metodo da quelli supportati		Utilizzare qualsiasi metodo di autenticazione supportato dal proxy. Se il proxy supporta più metodi di autenticazione, verrà utilizzato il più affidabile.
Qualsiasi metodo sicuro da quelli supportati		Utilizzare qualsiasi metodo di autenticazione sicuro supportato dal proxy. In questa modalità l'autenticazione Basic non si usa. Se il proxy supporta più metodi di autenticazione, verrà utilizzato il più affidabile.
Metodi elencati sotto:	Autenticazione Basic	Utilizza l'autenticazione Basic. Non è consigliabile utilizzare questo metodo perché il trasferimento di credenziali di autenticazione non viene criptato.
	Autenticazione Digest	Utilizza l'autenticazione Digest. Metodo di autenticazione crittografica.
	Autenticazione NTLM	Utilizza l'autenticazione NTLM. Metodo di autenticazione crittografica. Per l'autenticazione viene utilizzato il protocollo NTLM di Microsoft.
	Autenticazione GSS-Negotiate	Utilizza l'autenticazione GSS-Negotiate. Metodo di autenticazione crittografica.

8.2.2.3. Trasporto

Nella scheda **Trasporto** si impostano i parametri dei protocolli di trasporto utilizzati dal Server per la comunicazione con i client.

Nella sottosezione **TCP/IP** vengono configurati i parametri delle connessioni con il Server attraverso i protocolli TCP/IP:

- **Indirizzo** e **Porta** – rispettivamente l'indirizzo IP e il numero di porta dell'interfaccia di rete a cui viene associato questo protocollo di trasporto. Sull'interfaccia che ha le impostazioni indicate il Server è in ascolto per la comunicazione con gli Agent installati su postazioni.
- **Nome** – nome di Server Dr.Web. Se non è indicato, viene utilizzato il nome impostato nella scheda **Generali** (v. sopra, in particolare, se nella scheda non è impostato nessun nome, viene utilizzato il nome di computer). Se per il protocollo è impostato un nome diverso da quello definito nella scheda **Generali**, viene utilizzato il nome definito nella descrizione del protocollo. Questo nome viene utilizzato dal servizio di rilevamento per la ricerca del Server da parte degli Agent ecc.
- Spuntare il flag **Rilevamento** per abilitare il servizio di rilevamento del Server.

- Spuntare il flag **Multicasting** per utilizzare la modalità *Multicast over UDP* per il rilevamento del Server.
- **Gruppo Multicast** – indirizzo IP del gruppo multicast in cui è registrato il Server. Viene utilizzato per la comunicazione con gli Agent e gli Installer di rete durante la ricerca dei Server Dr.Web attivi nella rete. Se il valore di questo campo non è impostato, di default viene utilizzato il gruppo `231.0.0.1`.
- Soltanto nei SO della famiglia UNIX: nel campo **Percorso** viene impostato il percorso del socket, per esempio per la connessione con Agent.

Per maggiori informazioni consultare la sezione Configurazione delle connessioni di rete.

Questi parametri vengono impostati nel formato di indirizzo di rete riportato nel documento **Allegati,** nella sezione Allegato E. Specifica indirizzo di rete.

8.2.2.4. Cluster

Nella scheda **Cluster** vengono impostati i parametri di cluster dei Server Dr.Web per lo scambio delle informazioni in una configurazione di rete antivirus con diversi server.

Per utilizzare il cluster, impostare i seguenti parametri:

- **Gruppo multicast** – l'indirizzo IP del gruppo multicast attraverso cui i Server si scambieranno le informazioni.
- **Porta** – il numero di porta dell'interfaccia di rete a cui è associato il protocollo di trasporto per la trasmissione delle informazioni nel gruppo multicast.
- **Interfaccia** – l'indirizzo IP dell'interfaccia di rete a cui è associato il protocollo di trasporto per la trasmissione delle informazioni nel gruppo multicast.

Le caratteristiche della creazione di un cluster dei Server Dr.Web sono riportate nella sezione Cluster dei Server Dr.Web.

8.2.2.5. Download

Nella scheda **Download** vengono configurati i parametri del Server utilizzati nella generazione dei file di installazione di Agent per le postazioni della rete antivirus. In seguito, questi parametri vengono utilizzati quando l'installer di Agent si connette al Server:

- **Indirizzo di Server Dr.Web** – l'indirizzo IP o il nome DNS del Server Dr.Web.

  Se l'indirizzo di Server non è impostato, viene utilizzato il nome del computer restituito dal sistema operativo.
- **Porta** – il numero di porta da utilizzare per la connessione dell'installer di Agent al Server.

  Se il numero di porta non è impostato, di default viene utilizzata la porta 2193 (viene configurata nel Pannello di controllo nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Rete** → scheda **Trasporto**).

Le impostazioni della sezione **Download** vengono memorizzate nel file di configurazione `download.conf` (v. documento **Allegati**, p. G3. File di configurazione download.conf).

8.2.2.6. Aggiornamenti per gruppi

Nella scheda **Aggiornamenti per gruppi** viene configurata la trasmissione degli aggiornamenti per gruppi alle postazioni attraverso il protocollo multicast.

Per attivare la trasmissione degli aggiornamenti alle postazioni attraverso il protocollo multicast, spuntare il flag **Attiva gli aggiornamenti per gruppi**, in tale caso:

- Se gli aggiornamenti per gruppi sono disattivati, l'aggiornamento su tutte le postazioni viene eseguito soltanto nel modo regolare – attraverso il protocollo TCP.
- Se gli aggiornamenti per gruppi sono attivati, su tutte le postazioni connesse a questo Server l'aggiornamento si svolgerà in due fasi:
  1. Aggiornamento attraverso il protocollo multicast.
  2. Aggiornamento standard attraverso il protocollo TCP.

Per configurare gli aggiornamenti per gruppi, utilizzare i seguenti parametri:

- **Dimensione del datagramma UDP (byte)** – dimensione in byte dei datagrammi UDP utilizzati dal protocollo multicast.

  L'intervallo ammissibile è 512 – 8192. Per evitare frammentazione, si consiglia di impostare un valore inferiore all'MTU (Maximum Transmission Unit) della rete in uso.
- **Tempo di trasmissione del file (ms)** – nel periodo definito viene trasmesso un file di aggiornamento, dopo di che il Server inizia a trasmettere il file successivo.

  Tutti i file che non sono stati trasmessi in fase dell'aggiornamento tramite il protocollo multicast verranno trasmessi durante l'aggiornamento standard tramite il protocollo TCP.
- **Durata degli aggiornamenti per gruppi (ms)** – durata del processo di aggiornamento attraverso il protocollo multicast.

  Tutti i file che non sono stati trasmessi in fase dell'aggiornamento tramite il protocollo multicast verranno trasmessi durante l'aggiornamento standard tramite il protocollo TCP.
- **Intervallo di trasmissione pacchetti (ms)** – intervallo di trasmissione dei pacchetti al gruppo multicast.

  Un valore piccolo di intervallo potrebbe causare notevoli perdite durante la trasmissione dei pacchetti e sovraccaricare la rete. Si raccomanda di non modificare questa impostazione.
- **Intervallo tra le richieste di ritrasmissione (ms)** – con questo intervallo gli Agent inviano le richieste di ritrasmissione dei pacchetti persi.

  Il Server Dr.Web accumula queste query, dopodiché trasmette i blocchi persi.
- **Intervallo "di silenzio" su linea (ms)** – se la trasmissione di un file è finita prima della scadenza del tempo assegnato e se nel tempo "di silenzio" impostato nessuna richiesta di trasmissione ripetuta di pacchetti persi è arrivata dagli Agent, il Server Dr.Web ritiene che tutti gli Agent abbiano ottenuto con successo i file di aggiornamento e inizia a trasmettere il file successivo.

- **Intervallo per accumulare richieste di ritrasmissione (ms)** – durante questo intervallo il Server accumula le richieste degli Agent per la ritrasmissione dei pacchetti persi.

  Gli Agent chiedono l'invio ripetuto dei pacchetti persi. Il Server accumula queste richieste entro il tempo specificato, dopodiché trasmette i blocchi persi.

Per configurare una lista dei gruppi multicast, attraverso i quali l'aggiornamento per gruppi sarà disponibile, impostare i seguenti parametri nella sottosezione **Gruppi multicast**:

- **Gruppo multicast** – l'indirizzo IP del gruppo multicast attraverso cui le postazioni riceveranno gli aggiornamenti per gruppi.
- **Porta** – il numero di porta dell'interfaccia di rete del Server Dr.Web a cui è associato il protocollo di trasporto multicast per la trasmissione degli aggiornamenti.

> Per gli aggiornamenti per gruppi, è necessario impostare qualsiasi porta libera, in particolare, una che è diversa dalla porta assegnata nelle impostazioni al funzionamento del protocollo di trasporto del Server stesso.

- **Interfaccia** - l'indirizzo IP dell'interfaccia di rete del Server Dr.Web a cui è associato il protocollo di trasporto multicast per la trasmissione degli aggiornamenti.

  In ciascuna riga vengono configurate le impostazioni di un gruppo multicast. Per aggiungere un altro gruppo multicast, fare clic su  .

Se vengono impostati diversi gruppi multicast, prestare attenzione alle seguenti caratteristiche:

- Per diversi Server Dr.Web che spediranno gli aggiornamenti per gruppi, devono essere impostati diversi gruppi multicast.
- Per diversi Server Dr.Web che spediranno gli aggiornamenti per gruppi, devono essere impostati diversi parametri **Interfaccia** e **Porta**.
- Se vengono impostati diversi gruppi multicast, i set delle postazioni che rientrano in questi gruppi non devono intersecarsi. Pertanto, ciascuna postazione della rete antivirus può far parte soltanto di un gruppo multicast.

8.2.3. Statistiche

Nella scheda **Statistiche** vengono definite le informazioni statistiche che verranno registrate nel log e salvate nel database del Server.

Per registrare e aggiungere al database il rispettivo tipo d'informazione, spuntare i seguenti flag:

- **Stato della quarantena** – abilita il monitoraggio dello stato della Quarantena su postazioni e la registrazione delle informazioni nel database.
- **Elenco di hardware e software** – abilita il monitoraggio dell'elenco di hardware e software su postazioni e la registrazione delle informazioni nel database.
- **Elenco di moduli di postazioni** – abilita il monitoraggio della lista dei moduli di Antivirus installati su postazioni e la registrazione delle informazioni nel database.

- **Elenco di componenti installati** – abilita il monitoraggio della lista dei componenti di Antivirus (Scanner, i monitor ecc.) installati sulla postazione e la registrazione delle informazioni nel database.
- **Sessioni degli utenti di postazioni** – abilita il monitoraggio delle sessioni degli utenti di postazioni e la registrazione nel database dei nomi utente degli utenti entrati nel sistema da computer con Agent installato.
- **Avvio/arresto dei componenti** – abilita il monitoraggio delle informazioni su avvio e arresto dei componenti di Antivirus (Scanner, i monitor ecc.) su postazioni e la registrazione delle informazioni nel database.
- **Minacce alla sicurezza rilevate** – abilita il monitoraggio del rilevamento delle minacce alla sicurezza delle postazioni e la registrazione delle informazioni nel database.

  Se il flag **Minacce alla sicurezza rilevate** è spuntato, è inoltre possibile configurare le impostazioni addizionali delle statistiche su minacce.

  Per abilitare l'invio delle statistiche sulle minacce alla sicurezza di postazioni rilevate alla società Doctor Web, spuntare il flag Invia le statistiche a Doctor Web. Diventano disponibili i seguenti campi:

  - **Intervallo** – intervallo in minuti di invio delle statistiche;
  - **Identificatore** – chiave MD5 (si trova nel file di configurazione del Server).

  È obbligatorio soltanto il campo **Intervallo** di invio delle statistiche.
- **Errori di scansione** – abilita il monitoraggio del rilevamento di errori di scansione su postazioni e la registrazione delle informazioni nel database.
- **Statistiche di scansione** – abilita il monitoraggio dei risultati di scansione su postazioni e la registrazione delle informazioni nel database.
- **Installazioni di Agent** – abilita il monitoraggio delle informazioni sulle installazioni di Agent su postazioni e la registrazione delle informazioni nel database.
- **Log di esecuzione di task su postazioni** – abilita il monitoraggio dei risultati dell'esecuzione di un task su postazioni e la registrazione delle informazioni nel database.
- **Stato delle postazioni** – abilita il monitoraggio dei cambiamenti di stato delle postazioni e la registrazione delle informazioni nel database.
  - **Stato dei database dei virus** – abilita il monitoraggio dello stato (componenti, modifiche) dei database dei virus su postazione e la registrazione delle informazioni nel database. Il flag è disponibile soltanto se è spuntato il flag **Stato delle postazioni**.

Per visualizzare le informazioni statistiche:

1. Selezionare la voce del menu principale **Rete antivirus**.
2. Nella lista gerarchica selezionare una postazione o un gruppo.
3. Aprire la sezione corrispondente del menu di gestione (v. tabella sotto).

La descrizione dettagliata delle informazioni statistiche è riportata nella sezione Visualizzazione delle statistiche della postazione.

Nella tabella sottostante è riportata la corrispondenza dei flag della sezione **Statistiche** nelle impostazioni di Server e delle voci del menu di gestione sulla pagina **Rete antivirus**.

Se vengono deselezionati i flag nella scheda **Statistiche**, saranno nascoste le voci corrispondenti nel menu di gestione.

Tabella 8-2. Corrispondenza delle impostazioni del Server e delle voci del menu di gestione

Impostazioni del Server	Voci del menu
Stato della quarantena	Generali → Quarantena Configurazione → Windows → Agent Dr.Web → flag Consenti la gestione remota della quarantena
Elenco di hardware e software	Generali → Hardware e software Generali → Comparazione di hardware e software
Elenco di moduli di postazioni	Statistiche → Moduli
Elenco di componenti installati	Generali → Componenti installati
Sessioni degli utenti di postazioni	Generali → Sessioni degli utenti
Avvio/arresto dei componenti	Statistiche → Avvio/Arresto
Minacce alla sicurezza rilevate	Statistiche → Minacce Statistiche → Statistiche delle minacce
Errori di scansione	Statistiche → Errori
Statistiche di scansione	Statistiche → Statistiche di scansione Tabelle → Statistiche riassuntive
Installazioni di Agent	Statistiche → Installazioni di Agent
Log di esecuzione dei task sulla postazione	Statistiche → Task Statistiche → Database dei virus
Stato delle postazioni	Statistiche → Stato Statistiche → Database dei virus
Stato dei database dei virus	Statistiche → Database dei virus

8.2.4. Sicurezza

Nella scheda **Sicurezza** vengono impostate le limitazioni riguardanti gli indirizzi di rete da cui gli Agent, gli installer di rete e gli altri Server Dr.Web (adiacenti) possono accedere a questo Server.

Il log di verifica del Server viene gestito tramite i seguenti flag:

- **Verifica delle operazioni dell'amministratore** consente di registrare nel log di verifica le informazioni sulle operazioni eseguite dall'amministratore con il Pannello di controllo e di registrare il log nel database.
- **Verifica delle operazioni interne del server** consente di registrare nel log di verifica le informazioni sulle operazioni interne del Server Dr.Web e di registrare il log nel database.
- **Verifica delle operazioni Web API** consente di registrare nel log di verifica le informazioni sulle operazioni tramite XML API e di registrare il log nel database.

Si può visualizzare il log di verifica selezionando nel menu principale **Amministrazione** la voce **Log di verifica**.

Nella scheda **Sicurezza** sono incluse schede supplementari in cui vengono impostate le limitazioni per i tipi di connessione corrispondenti:

- **Agent** – una lista delle limitazioni agli indirizzi IP da cui gli Agent Dr.Web possono connettersi a questo Server.
- **Installer** – una lista delle limitazioni agli indirizzi IP da cui gli installer di Agent Dr.Web possono connettersi a questo Server.
- **Adiacenti** – una lista delle limitazioni agli indirizzi IP da cui i Server Dr.Web adiacenti possono connettersi a questo Server.
- **Servizio di rilevamento** – una lista delle limitazioni agli indirizzi IP da cui le richieste broadcast vengono accettate dal servizio di rilevamento del Server.

Per impostare la limitazione di accesso per qualche tipo di connessione:

1. Passare alla scheda corrispondente (**Agent**, **Installazioni**, **Adiacenti** o **Servizio di rilevamento**).
2. Per consentire tutte le connessioni, togliere la spunta dal flag **Usa questa lista di controllo di accesso**.
3. Per impostare liste degli indirizzi consentiti o proibiti, spuntare il flag **Usa questa lista di controllo di accesso**.
4. Per consentire l'accesso da un determinato indirizzo TCP, includerlo nella lista **TCP: Consentito** o **TCPv6: Consentito**.
5. Per proibire qualche indirizzo TCP, includerlo nella lista **TCP: Negato** o **TCPv6: Negato**.

Per modificare una lista degli indirizzi:

1. Inserire l'indirizzo di rete nel campo corrispondente e premere il pulsante **Salva**.

2. Per aggiungere un nuovo campo di indirizzo, premere il pulsante  della sezione corrispondente.
3. Per eliminare un campo, premere il pulsante  .

   Indirizzo di rete viene definito come: <*indirizzo-IP*>/[<*prefisso*>].

> Le liste per inserire gli indirizzi TCPv6 saranno visualizzate solo se sul computer è installata l'interfaccia IPv6.

Esempio di utilizzo del prefisso:

1. Il prefisso 24 sta per la maschera di rete: `255.255.255.0`

   Contiene 254 indirizzi

   Gli indirizzi di host in queste reti sono del tipo: `195.136.12.*`
2. Il prefisso 8 sta per la maschera di rete 255.0.0.0

   Contiene fino a 16387064 indirizzi (256*256*256)

   Gli indirizzi di host in queste reti sono del tipo: `125.*.*.*`

Gli indirizzi non inclusi in nessuna lista vengono consentiti o proibiti a seconda della selezione del flag **Priorità di negazione**. Se il flag è selezionato, la lista **Negato** ha la precedenza rispetto alla lista **Consentito**. Gli indirizzi non inclusi in nessuna lista o inclusi in tutte e due vengono proibiti. Vengono consentiti soltanto gli indirizzi che sono inclusi nella lista **Consentito** e non sono inclusi nella lista **Negato**.

8.2.5. Cache

Nella scheda **Cache** vengono configurati i parametri della cancellazione della cache di server:

- **Periodicità di pulizia della cache** – periodicità della cancellazione completa della cache.
- **File in quarantena** – periodicità dell'eliminazione di file conservati in Quarantena sul lato Server.
- **File del repository** – periodicità dell'eliminazione di file conservati nel repository.
- **Pacchetti di installazione** – periodicità dell'eliminazione dei pacchetti di installazione individuali.

> Impostando valori numerici, prestare attenzione alle liste a cascata con le unità di misura di periodicità.

8.2.6. Database

Nella scheda **Database** viene selezionato il DBMS necessario per il funzionamento del Server Dr.Web.

Si può ottenere la struttura del database di Server Dr.Web sulla base dello script `sql init.sql` locato nella sottodirectory etc della directory di installazione di Server Dr.Web.

1. Dalla lista a cascata **Database** selezionare il tipo di database:
   - **IntDB** – database incorporato SQLite2 (un componente di Server Dr.Web),
   - **ODBC** – per utilizzare un database esterno tramite la connessione ODBC,

     Se si verificano avvisi o errori nel funzionamento di Server Dr.Web con il DBMS Microsoft SQL Server attraverso ODBC, è necessario assicurarsi che sia utilizzata l'ultima versione disponibile del DBMS per questa edizione.

     Per scoprire come determinare se ci sono service pack, consultare la seguente pagina Microsoft: https://support.microsoft.com/en-us/kb/321185.

   - **Oracle** – database esterno per le piattaforme ad eccezione di FreeBSD,

     Se viene utilizzato il **DBMS Oracle** esterno tramite la connessione ODBC, è necessario installare l'ultima versione del driver ODBC, fornita insieme a questo DBMS. L'utilizzo del driver ODBC per Oracle, fornito da Microsoft, è fortemente sconsigliato.

   - **PostgreSQL** – database esterno,
   - **SQLite3** – database incorporato (un componente di Server Dr.Web). È la variante consigliata se viene utilizzato il database incorporato.
2. Configurare le impostazioni necessarie di utilizzo del database:
   - Per i database incorporati, se necessario, inserire nel campo **Nome del file** il percorso completo del file di database ed impostare la dimensione della memoria cache e la modalità di registrazione dei dati.
   - I parametri per i database esterni sono descritti nel documento **Allegati**, nella sezione Allegato B. Impostazioni necessarie per l'utilizzo di DBMS. Parametri dei driver per DBMS.
3. Per rendere effettive le impostazioni, fare clic su **Salva**.

Il pacchetto di Server Dr.Web contiene client incorporati dei DBMS supportati dunque:

- Se si intende utilizzare i client del DBMS incorporati, forniti insieme a Server Dr.Web, durante l'installazione (l'aggiornamento) di Server nelle impostazioni dell'installer controllare che l'installazione del relativo client del DBMS sia consentita nella sezione **Supporto dei database**.
- Se si intende utilizzare database esterni attraverso la connessione ODBC, durante l'installazione (l'aggiornamento) di Server, nelle impostazioni di installer annullare l'installazione del relativo client del DBMS nella sezione **Supporto dei database**.
  Altrimenti, l'utilizzo del database attraverso ODBC non sarà possibile per conflitto delle librerie.

L'installer del Server supporta la modalità di modifica di prodotto. Per aggiungere o rimuovere singoli componenti, per esempio driver per la gestione dei database, basta avviare l'installer del Server e selezionare l'opzione **Modifica**.

Di default, è impostato l'utilizzo del DBMS incorporato. La scelta di questa modalità impegna molte risorse di elaborazione di dati del Server. Se la rete antivirus è di una dimensione significativa, si consiglia di utilizzare un DBMS esterno. La procedura di cambio del tipo di DBMS viene descritta nel documento **Allegati**, nella sezione Cambio del tipo di DBMS di Dr.Web Enterprise Security Suite.

Il database incorporato può essere utilizzato se al Server sono connesse non più di 200-300 postazioni. Se lo permettono la configurazione dell'hardware del computer su cui è installato il Server Dr.Web e il carico di altri processi eseguiti su questo computer, è possibile connettere fino a 1000 postazioni.

Altrimenti, si deve utilizzare un database esterno.

Se viene utilizzato un database esterno e se al Server sono connesse più di 10000 postazioni, sono consigliabili i seguenti requisiti minimi:

- processore con velocità 3GHz,
- memoria operativa a partire dai 4 GB per il Server Dr.Web, a partire dai 8 GB per il server del database,
- SO della famiglia UNIX.

È prevista la possibilità di eseguire le operazioni di pulizia del database utilizzato dal Server Dr.Web, in particolare: eliminazione dei record di eventi e delle informazioni su postazioni che non si sono connesse al Server per un determinato periodo. Per ripulire il database, passare alla sezione del calendario del Server e creare un task corrispondente.

8.2.7. Moduli

Nella scheda **Moduli** viene configurata la modalità di interazione di Server Dr.Web con gli altri componenti di Dr.Web Enterprise Security Suite:

- Spuntare il flag **Estensione del Pannello di controllo della sicurezza Dr.Web** per poter utilizzare l'Estensione del Pannello di controllo della sicurezza Dr.Web per gestire il Server e la rete antivirus tramite il Pannello di controllo.

  Se è tolto il flag **Estensione del Pannello di controllo della sicurezza Dr.Web**, dopo il riavvio del Server Dr.Web non sarà disponibile il Pannello di controllo della sicurezza Dr.Web. In questo caso il Server e la rete antivirus possono essere gestiti soltanto tramite l'utility di diagnostica remota, a condizione che sia spuntato il flag **Estensione Dr.Web Server FrontDoor**.

- Spuntare il flag **Estensione Dr.Web Server FrontDoor** per poter utilizzare l'estensione Dr.Web Server FrontDoor che abilita la connessione dell'utility di diagnostica remota di Server (v. inoltre p. Accesso remoto al Server Dr.Web).
- Spuntare il flag **Protocollo di Agent Dr.Web** per attivare il protocollo di interazione del Server con gli Agent Dr.Web.
- Spuntare il flag **Protocollo Microsoft NAP Health Validator** per attivare il protocollo di interazione di Server con il componente di verifica di integrità di sistema Microsoft NAP Validator.

- Spuntare il flag **Protocollo di installer di Agent Dr.Web** per attivare il protocollo di interazione del Server con gli installer di Agent Dr.Web.
- Spuntare il flag **Protocollo di cluster dei Server Dr.Web** per attivare il protocollo di interazione dei Server in un sistema a cluster.
- Spuntare il flag **Protocollo di Server Dr.Web** per attivare il protocollo di interazione del Server Dr.Web con gli altri Server Dr.Web. Di default, il protocollo è disattivato. Se viene configurata una rete con diversi server (v. p. Caratteristiche di una rete con diversi Server Dr.Web), attivare questo protocollo, spuntando il flag **Protocollo di Server Dr.Web**.

8.2.8. Posizione

Nella scheda **Posizione** si può indicare le informazioni supplementari circa la posizione fisica del computer su cui è installato il software Server Dr.Web.

Inoltre, in questa scheda su può visualizzare la posizione del Server su una mappa.

Per visualizzare la posizione della postazione del Server sulla mappa:

1. Nei campi **Latitudine** e **Longitudine** inserire le coordinate geografiche del Server nel formato gradi decimali (Decimal Degrees).
2. Premere il pulsante **Salva** per memorizzare i dati immessi nel file di configurazione del Server.

   Non è necessario riavviare il Server per visualizzare la mappa. Tuttavia, sarà necessario riavviare il Server per applicare le coordinate geografiche modificate.
3. Nella scheda **Posizione** viene visualizzata l'anteprima della mappa OpenStreetMaps con un'etichetta corrispondente alle coordinate inserite.

   Se l'anteprima non può essere caricata, viene visualizzato il testo **Mostra sulla mappa**.
4. Per visualizzare la mappa di grandezza piena, fare clic sull'anteprima o sul testo **Mostra sulla mappa**.

8.2.9. Licenze

Nella scheda **Licenze** viene configurata la distribuzione di licenze tra i Server Dr.Web:

- **Periodo di validità delle licenze rilasciate** – periodo di tempo per cui vengono rilasciate le licenze dalla chiave su questo Server. L'impostazione viene utilizzata se questo Server rilascia licenze ai Server adiacenti.
- **Periodo per il rinnovo delle licenze ricevute** – il periodo fino alla scadenza di una licenza, a partire da cui questo Server richiede il rinnovo della licenza ricevuta da un Server adiacente. L'impostazione viene utilizzata se questo Server riceve licenze dai Server adiacenti.
- **Periodo di sincronizzazione delle licenze** – la periodicità della sincronizzazione delle informazioni su licenze rilasciate tra i Server.

Per maggiori informazioni su distribuzione di licenze tra i Server, consultare la sezione Gestione licenze.

8.3. Accesso remoto al Server Dr.Web

Per connettere l'utility di diagnostica remota del Server, è necessario attivare Dr.Web Server FrontDoor Plug-in. Per farlo, nella sezione **Configurazione del Server Dr.Web**, nella scheda Moduli spuntare il flag **Estensione Dr.Web Server FrontDoor**.

Per connettere l'utility di diagnostica remota del Server è necessario che per l'amministratore che si connette attraverso l'utility sia consentito il permesso **Utilizzo delle funzioni addizionali**. Altrimenti, sarà negato l'accesso al Server attraverso l'utility di diagnostica remota.

Per configurare i parametri di connessione dell'utility di diagnostica remota del Server:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Accesso remoto al Server Dr.Web**.
2. Configurare il protocollo di connessione:
   - Spuntare il flag **Utilizza SSL** per consentire la connessione dell'utility di diagnostica remota a Server Dr.Web tramite il protocollo SSL. Se il flag è deselezionato, la connessione sarà possibile solo tramite il protocollo TCP.
     Per una connessione tramite il protocollo SSL, configurare le seguenti impostazioni:
     - **Certificato SSL** – il file del certificato SSL che verrà controllato al momento della connessione. Nella lista a cascata sono elencati i certificati disponibili dalla directory di Server.
     - **Chiave privata SSL** – il file della chiave privata SSL che verrà controllata al momento della connessione. Nella lista a cascata sono elencate le chiavi private disponibili dalla directory di Server.
3. Configurare le impostazioni dei nodi della connessione:
   - **Indirizzo** – l'indirizzo da cui è consentita la connessione dell'utility di diagnostica remota del Server.
   - **Porta** – la porta per la connessione dell'utility di diagnostica remota del Server. Di default, si usa la porta 10101.

   Per aggiungere un altro indirizzo consentito, premere  e configurare i valori dei campi aggiunti.

   Per vietare la connessione da un indirizzo consentito, cancellare questo indirizzo dalla lista, premendo  di fronte alla riga con questo indirizzo.
4. Premere **Salva**.

L'utilizzo della versione console dell'utility di diagnostica remota di Server è descritto nel documento **Allegati**, nella sezione H10. Utility di diagnostica remota del Server Dr.Web.

8.4. Configurazione del calendario di Server Dr.Web

Per configurare il calendario di esecuzione dei task di Server Dr.Web:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Scheduler del Server Dr.Web**. Si apre una lista dei task del Server.
2. Per gestire il calendario, vengono utilizzati gli elementi corrispondenti nella barra degli strumenti:
   a) Gli elementi generali della barra degli strumenti vengono utilizzati per creare nuovi task e per gestire la sezione calendario in generale. Questi strumenti sono sempre disponibili nella barra degli strumenti.

    **Crea task** – per aggiungere un nuovo task. Questa azione viene descritta in dettaglio qui sotto nella sottosezione Editor dei task.

    **Esporta impostazioni da questa sezione in file** – per esportare il calendario in un file di formato specifico.

    **Importa impostazioni in questa sezione da file** – per importare il calendario da un file di formato specifico.

   b) Per gestire i task esistenti, spuntare i flag di fronte ai task richiesti oppure il flag nell'intestazione della tabella se si vogliono selezionare tutti i task nella lista. Con questo diventano disponibili gli elementi della barra degli strumenti utilizzati per la gestione dei task selezionati.

Impostazione		Azione
Stato	**Permetti l'esecuzione**	Attivare l'esecuzione dei task selezionati secondo il calendario impostato se erano proibiti.
	Proibisci l'esecuzione	Proibire l'esecuzione dei task selezionati. I task saranno presenti nella lista ma non verranno eseguiti.
 L'impostazione simile viene definita nell'editor del task nella scheda **Generali** tramite il flag **Permetti l'esecuzione**.		
Importanza	**Rendi critico**	Eseguire il task in modo straordinario se l'esecuzione di questo task è stata persa nell'ora programmata.
	Rendi non critico	Eseguire il task solo nell'ora programmata, nonostante l'omissione o l'esecuzione del task.
 L'impostazione simile viene definita nell'editor del task nella scheda **Generali** tramite il flag **Task critico**.		

Impostazione	Azione
Duplica le impostazioni	Duplicare i task selezionati nella lista del calendario corrente. Tramite l'azione **Duplicare le impostazioni** vengono creati nuovi task che hanno le impostazioni uguali a quelle dei task selezionati.
Programma un'altra esecuzione dei task	Per i task per cui è impostata l'esecuzione singola: eseguire il task ancora una volta secondo le impostazioni di ora (ciò come cambiare la frequenza di esecuzione del task è descritto sotto nella sottosezione Editor dei task).
Rimuovi i task selezionati	Rimuovere dal calendario il task selezionato.

3. Per modificare i parametri di un task, selezionarlo dalla lista dei task. Si apre la finestra **Editor dei task** descritta sotto.
4. Dopo aver finito di modificare il calendario, fare clic su **Salva** per accettare le modifiche.

Editor dei task

Tramite l'editor dei task si possono definire le impostazioni per:

1. Creare un nuovo task.

   A questo fine fare clic sul pulsante **Crea task nella barra degli strumenti**.
2. Modificare un task esistente.

   A questo fine fare clic sul nome del task nella lista dei task.

Si apre la finestra di modifica dei parametri dei task. Le impostazioni di task per la modifica di un task esistente sono simili alle impostazioni per la creazione di un task nuovo.

I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

Per modificare i parametri di un task:

1. Nella scheda **Generali** vengono impostati i seguenti parametri:
   - Nel campo **Nome** viene definito il nome del task sotto cui verrà visualizzato nel calendario.
   - Spuntare il flag **Permetti l'esecuzione** per attivare l'esecuzione del task. Se il flag non è selezionato, il task sarà presente nella lista ma non verrà eseguito.

     L'impostazione simile viene definita nella finestra principale di Scheduler tramite l'elemento della barra degli strumenti **Stato**.
   - Spuntare il flag **Task critico** per eseguire il task in modo straordinario se l'esecuzione di questo task è stata persa nell'ora programmata per qualsiasi motivo. Scheduler controlla ogni minuto l'elenco dei task e se scopre un task critico perso, lo avvia. Se al momento dell'avvio il task è stato perso diverse volte, verrà eseguito solo 1 volta.

L'impostazione simile viene definita nella finestra principale di Scheduler tramite l'elemento della barra degli strumenti **Importanza**.

Nella scheda **Azione** selezionare il tipo di task dalla lista a cascata **Azione** e configurare i parametri del task, richiesti per l'esecuzione:

Tipo di task	Parametri e descrizione
Esecuzione di procedura	Il task è studiato per eseguire le procedure personalizzate (per maggiori informazioni v. p. Procedure personalizzate). È necessario impostare i seguenti parametri: • **Gruppo di procedure personalizzate** – gruppo di procedure personalizzate per cui verrà eseguita la procedura. • **Procedura** – nome della procedura personalizzata specifica dal gruppo selezionato nell'elenco **Gruppo di procedure personalizzate**, che verrà eseguita. • Spuntare il flag **Esegui in tutti i gruppi di procedure personalizzate** affinché la procedura personalizzata selezionata venga eseguita in tutti i gruppi di procedure nelle quali è impostata. In questo caso per ciascun gruppo verrà eseguita quella procedura che è impostata proprio per questo gruppo.
Esecuzione dello script	Il task è studiato per eseguire lo script Lua riportato nel campo **Script**. L'esecuzione simultanea del tipo di task **Esecuzione dello script** su diversi Server che utilizzano l'unico database potrebbe portare agli errori nell'esecuzione di questo task. Eseguendo script lua, l'amministratore ottiene l'accesso a tutto il file system all'interno del directory di Server e ad alcuni comandi di sistema sul computer su cui Server è installato. Per vietare l'accesso al calendario, disattivare il permesso **Modifica del calendario del Server** per il relativo amministratore (v. p. Amministratori e gruppi di amministratori).
Sostituzione della chiave di cifratura	Il task è studiato per la sostituzione periodica delle chiavi di cifratura: • della chiave privata `drwcsd.pri` su Server, • della chiave pubblica `drwcsd.pub` su postazioni. Siccome alcune postazioni potrebbero essere spente al momento di sostituzione, la procedura si articola in due fasi. Devono essere creati due task per l'esecuzione di ciascuna di queste fasi, e si consiglia di eseguire la seconda fase qualche tempo dopo la prima, in cui le postazioni di sicuro si connetteranno al Server. Creando un task, selezionare dalla lista a cascata la fase corrispondente di sostituzione della chiave:

Tipo di task	Parametri e descrizione
	• **Aggiunzione della nuova chiave** – è la prima fase della procedura in cui viene creata una nuova coppia non attiva di chiavi di cifratura. Le postazioni avranno la nuova chiave pubblica quando si connetteranno al Server. • **Rimozione della chiave vecchia e passaggio alla chiave nuova** – è la seconda fase in cui le postazioni vengono informate del passaggio alle nuove chiavi di cifratura, dopo di che le chiavi correnti vengono sostituite con quelle nuove: le chiavi pubbliche sulle postazioni e la chiave privata sul Server. Le postazioni che per qualche ragione non hanno ricevuto la nuova chiave pubblica non potranno connettersi al Server. Per risolvere questo problema, sono possibili le seguenti varianti di azioni: • Mettere manualmente la nuova chiave pubblica sulla postazione (si può consultare la procedura di sostituzione di chiave su postazione nel documento **Allegati**, nella sezione Connessione di Agent Dr.Web ad un altro Server Dr.Web). • Consentire agli Agent di essere autenticati sul Server con una chiave pubblica non valida (v. p. **Rete** nelle impostazioni di Agent).
Registrazione nel file di log	Il task è studiato per registrare la stringa impostata nel file di log di Server. **Stringa** – testo del messaggio da registrare nel file di log.
Avvio del programma	Il task è studiato per avviare un programma. I programmi avviati tramite questo task vengono eseguiti in background. È necessario impostare i seguenti parametri: • Nel campo **Percorso** – nome completo (con il percorso) del file eseguibile del programma da avviare. • Nel campo **Argomenti** – parametri da riga di comando per il programma da avviare. • Spuntare il flag **Attendi che il programma venga completato** per l'attesa di completamento del programma avviato da questo task. In questo caso Server registra nel log l'avvio del programma, il codice restituito e l'ora di completamento del programma. Se il flag **Attendi che il programma venga completato** è deselezionato, il task è considerato completato subito dopo l'avvio del programma e Server registra nel log soltanto l'avvio del programma.
Promemoria sulla scadenza della licenza	Il task è studiato per visualizzare un avviso di scadenza della licenza del prodotto Dr.Web. È necessario impostare un periodo prima di scadenza a partire dal quale verranno visualizzati gli avvisi promemoria.
Aggiornamento del repository	Le informazioni su questo task sono riportate nella sezione Aggiornamenti programmati.

Tipo di task	Parametri e descrizione
Arresto di Server Dr.Web	Il task è studiato per interrompere il funzionamento di Server. Viene avviato senza parametri supplementari.
Invio del messaggio sulla postazione	Il task è studiato per mandare un messaggio personalizzabile agli utenti della postazione o del gruppo di postazioni. Le impostazioni del messaggio sono riportate nella sezione Invio di messaggi alle postazioni.
Pulizia del database	Il task è studiato per raccogliere e cancellare i record non utilizzati nel database del Server tramite l'esecuzione del comando `vacuum`. Viene avviato senza parametri supplementari.
Rimozione degli eventi non inviati	Il task è studiato per cancellare dal database gli eventi non inviati. È necessario impostare il tempo di conservazione degli eventi non inviati, dopo il quale saranno cancellati. Qui sono sottintesi gli eventi trasmessi dal Server subordinato al Server principale. Se la trasmissione di un evento non è riuscita, quest'ultimo viene registrato nell'elenco degli eventi non inviati. Il Server subordinato con una periodicità fa i tentativi di trasmissione. Quando viene eseguito il task **Rimozione degli eventi non inviati**, vengono rimossi tutti gli eventi, di cui la durata di conservazione ha raggiunto o superato il periodo impostato.
Rimozione delle registrazioni vecchie	Il task è studiato per cancellare dal database le informazioni obsolete riguardanti le postazioni. È necessario impostare il numero di giorni dopo cui le informazioni statistiche su postazioni (però non le postazioni stesse) vengono considerate obsolete e vengono cancellate dal Server. Il periodo di rimozione di dati statistici viene impostato separatamente per ciascun tipo di registrazione.
Rimozione delle postazioni vecchie	Il task è studiato per cancellare dal database le postazioni obsolete. È necessario impostare un periodo di tempo (di default è di 90 giorni), e le postazioni che non si collegavano al Server durante tale periodo vengono considerate obsolete e vengono cancellate dal Server.

Le informazioni vecchie vengono rimosse dal database automaticamente al fine di risparmiare spazio su disco. Di default, per i task **Rimozione delle registrazioni vecchie** e **Rimozione delle postazioni vecchie** il periodo è di 90 giorni. Con la diminuzione di questo parametro, le informazioni statistiche sui componenti di rete antivirus accumulate diventano meno rappresentative. Con l'aumento di questo parametro, potrebbe aumentare notevolmente il volume delle risorse consumate dal Server.

Tipo di task	Parametri e descrizione
Rimozione dei messaggi obsoleti	Il task è studiato per cancellare dal database i seguenti messaggi: • avvisi degli agent, • avvisi per la console web, • report generati secondo il calendario. Vengono rimossi i messaggi contrassegnati come obsoleti, cioè i messaggi di cui è scaduto il periodo di conservazione che può essere configurato: • per gli avvisi: durante la creazione degli avvisi per il metodo di invio corrispondente (v. p. Configurazione degli avvisi). • per i report: nel task di generazione dei report. Il task viene avviato senza parametri supplementari.
Riavvio del Server Dr.Web	Il task è studiato per il riavvio del Server. Viene avviato senza parametri supplementari.
Risveglio delle postazioni	Il task è studiato per accendere le postazioni, per esempio, prima di avviare il task di scansione. Le postazioni da accendere vengono impostate tramite i seguenti parametri del task: • **Sveglia tutte le postazioni** – prescrive di accendere tutte le postazioni connesse a questo Server. • **Sveglia le postazioni secondo i parametri specificati** – prescrive di accendere soltanto le postazioni che corrispondono ai parametri indicati di seguito: ▫ **Indirizzi IP** – una lista degli indirizzi IP delle postazioni da accendere. Viene impostato nel formato: 10.3.0.127, 10.4.0.1-10.4.0.5, 10.5.0.1/30. Compilando la lista degli indirizzi, usare virgola o nuova riga come separatore. Inoltre, gli indirizzi IP possono essere sostituiti con i nomi DNS dei computer. ▫ **Indirizzi MAC** – una lista degli indirizzi MAC delle postazioni da accendere. Gli ottetti dell'indirizzo MAC vengono separati dal carattere ':'. Compilando la lista degli indirizzi, usare virgola o nuova riga come separatore. ▫ **Gruppi** – una lista dei gruppi le cui postazioni sono da accendere. Per selezionare diversi gruppi, utilizzare i tasti CTRL e MAIUSCOLO.  Per l'esecuzione di questo task è necessario che sulle postazioni da accendere siano installate le schede di rete con il supporto dell'opzione Wake-on-LAN. Si può controllare la disponibilità del supporto dell'opzione Wake-on-LAN nella documentazione o nelle proprietà della scheda di rete (**Pannello di controllo** → **Rete ed Internet** → **Connessioni di rete** → **Configura connessione** → **Configura** → **Avanzate**).

Tipo di task	Parametri e descrizione
Backup dei dati critici del server	Il task è studiato per il backup dei seguenti dati critici del Server: • database, • file della chiave di licenza, • chiave di cifratura privata. È necessario impostare i seguenti parametri: • **Percorso** – percorso della directory in cui verranno salvati i dati (il percorso vuoto significa la directory predefinita). • **Numero massimo di copie –** numero massimo di copie di backup (il valore 0 significa l'annullamento di questa limitazione). Per maggiori informazioni v. documento **Allegati**, p. Allegato H4.5. ⚠ La directory per il backup deve essere vuota. Altrimenti, il contenuto della directory verrà rimosso nel corso dell'esecuzione di un backup.

Backup del repository	Il task è studiato per il salvataggio periodico delle copie di backup del repository.
	È necessario impostare i seguenti parametri:
	• **Percorso** – percorso completo della directory in cui verrà salvata la copia di backup.
	• **Numero massimo di copie** – numero massimo di copie di backup del repository che il task salva nella directory indicata. Quando viene raggiunto il numero massimo di copie del repository, per salvare una nuova copia, viene rimossa la copia più vecchia tra quelle a disposizione.
	• **Area del repository** determina quale blocco delle informazioni sul componente antivirus verrà salvato:
	  ▫ **Tutto il repository** – vengono salvate tutte le revisioni dal repository, per i componenti selezionati nella lista sotto.
	  ▫ **Soltanto le revisioni importanti** – vengono salvate soltanto le revisioni contrassegnate come importanti, per i componenti selezionati nella lista sotto.
	  ▫ **Soltanto i file di configurazione** – vengono salvati soltanto i file di configurazione dei componenti selezionati nella lista sotto.
	• Contrassegnare con i flag i componenti le cui aree selezionate verranno salvate.
	⚠ La directory per il backup deve essere vuota. Altrimenti, il contenuto della directory verrà rimosso nel corso dell'esecuzione di un backup.

Sincronizzazione con Active Directory	Il task è studiato per sincronizzare la struttura della rete: i container di Active Directory che contengono computer diventano gruppi della rete antivirus in cui vengono messe le postazioni.

Tipo di task	Parametri e descrizione
	Viene avviato senza parametri supplementari. Di default, questo task è disattivato. Per attivare l'esecuzione del task, impostare l'opzione **Permetti l'esecuzione** nelle impostazioni del task o nella barra degli strumenti, come è descritto sopra.
Il server adiacente non si connette da molto tempo	Il task è studiato per visualizzare l'avviso su ciò che i Server adiacenti non si collegano a questo Server da molto tempo. La visualizzazione dell'avviso viene configurata nella sezione Configurazione degli avvisi tramite la voce **Il server adiacente non si connette da molto tempo**. Nei campi **Ore** e **Minuti** impostare un periodo, dopo il quale il Server adiacente verrà considerato un server che non si collega da molto tempo.
La postazione non si connette da molto tempo	Il task è studiato per visualizzare l'avviso su ciò che alcune postazioni non si collegano a questo Server da molto tempo. La visualizzazione dell'avviso viene configurata nella sezione Configurazione degli avvisi tramite la voce **La postazione non si connette al server da molto tempo**. Nel campo **Giorni** impostare un periodo, dopo il quale la postazione verrà considerata una postazione che non si collega da molto tempo.
Creazione del report statistico	Il task è studiato per creare un report con le informazioni statistiche della rete antivirus. Per poter creare un report, è necessario che sia attivo l'avviso **Report periodico** (v. p. Configurazione degli avvisi). Il report creato viene salvato sul computer su cui è installato il Server. L'ottenimento del report dipende dal tipo di avviso: • In caso del metodo di invio di messaggio **E-mail**: sull'indirizzo e-mail impostato nella configurazione dell'avviso viene inviato un messaggio con un link del percorso del report e con il report stesso in allegato. • In caso di ogni altro metodo di invio: viene inviato l'avviso congruo che contiene il link al percorso del report. Per creare il task, nel calendario si devono definire i seguenti parametri: • **Profili di notifiche** – nome del gruppo di avvisi con le impostazioni, secondo cui verrà generato il report. L'intestazione viene configurata durante la creazione di un nuovo gruppo di avvisi. • **Lingua del resoconto** – lingua in cui le informazioni saranno presentate nel report. • **Formato della data** – formato in cui verranno presentate le informazioni statistiche che contengono date. Sono disponibili i seguenti formati: ▫ europeo: `DD-MM-YYYY HH:MM:SS` ▫ americano: `MM/DD/YYYY HH:MM:SS`

Tipo di task	Parametri e descrizione
	• **Formato del resoconto** – formato di file in cui verrà salvato il report statistico. • **Periodo di riferimento** – periodo di tempo, per cui le statistiche verranno incluse nel report. • **Gruppi** – lista dei gruppi di postazioni di rete antivirus, le informazioni su cui verranno incluse nel report. Per selezionare diversi gruppi, utilizzare i tasti CTRL o MAIUSCOLO. • **Tabelle del resoconto** – lista delle tabelle statistiche, le informazioni da cui verranno incluse nel report. Per selezionare diverse tabelle, utilizzare i tasti CTRL o MAIUSCOLO. • **Tempo di conservazione del resoconto** – periodo per la conservazione del report sul computer con il Server installato, cominciando dal momento della creazione del report.

2. Nella scheda **Tempo**:
   - Dalla lista a cascata **Periodicità** selezionare la modalità di avvio del task e impostare il tempo secondo la periodicità scelta:

Modalità di avvio	Parametri e descrizione
Finale	Il task verrà eseguito ad arresto di Server. Viene avviato senza parametri supplementari.
Iniziale	Il task verrà eseguito ad avvio di Server. Viene avviato senza parametri supplementari.
Tra N minuti dopo il task iniziale	Dalla lista a cascata **Task iniziale** è necessario selezionate il task relativamente al quale viene impostato il tempo di esecuzione del task che viene creato. Nel campo **Minuto** impostare o selezionare dalla lista il numero di minuti da aspettare dopo l'esecuzione del task iniziale prima che venga avviato il task corrente.
Ogni giorno	È necessario inserire l'ora e il minuto — il task verrà avviato ogni giorno all'ora indicata.
Ogni mese	È necessario selezionare un giorno (giorno del mese), immettere l'ora e il minuto — il task verrà avviato nel giorno del mese selezionato all'ora indicata.
Ogni settimana	È necessario selezionare un giorno della settimana, immettere l'ora e il minuto — il task verrà avviato nel giorno della settimana selezionato all'ora indicata.
Ogni ora	È necessario immettere un numero dallo 0 ai 59 che indica il minuto di ogni ora in cui il task verrà avviato.
Ogni N minuti	È necessario immettere il valore **N** per definire l'intervallo di tempo dell'esecuzione del task.

Modalità di avvio	Parametri e descrizione
	Se **N** è pari ai `60` o superiore, il task verrà avviato ogni **N** minuti. Se **N** è inferiore ai `60`, il task verrà avviato ogni minuto dell'ora multiplo di **N**.

- Spuntare il flag **Proibisci dopo la prima esecuzione** per eseguire il task soltanto una volta secondo l'ora impostata. Se il flag è tolto, il task verrà eseguito molte volte con la periodicità selezionata.

Per ripetere l'esecuzione di un task la cui esecuzione è definita come singola e che è già stato eseguito, utilizzare il pulsante **Programma un`altra esecuzione dei task** che si trova nella barra degli strumenti della sezione calendario.

3. Finite le modifiche dei parametri del task, fare clic sul pulsante **Salva** per accettare le modifiche dei parametri del task, se veniva modificato un task esistente, oppure per creare un nuovo task con i parametri impostati, se veniva creato un nuovo task.

8.5. Configurazione del web server

Ogni volta che si salvano modifiche della sezione **Configurazione del web server**, viene automaticamente salvato un backup della versione precedente del file di configurazione del web server. Vengono conservati gli ultimi 10 backup.

I backup si trovano nella stessa directory del file di configurazione e vengono denominati nel seguente formato:

`webmin.conf;`*<ora_di_creazione>*

È possibile utilizzare i backup creati, in particolare, per ripristinare il file di configurazione se l'interfaccia del Pannello di controllo non è disponibile.

Per configurare il web server:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Configurazione del web server**. Si apre la finestra di configurazione di web server.

I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

3. Nella barra degli strumenti sono disponibili i seguenti pulsanti per gestire le impostazioni della sezione:

Riavvia Server Dr.Web – per riavviare il Server al fine di accettare le modifiche apportate in questa sezione. Il pulsante diventa attivo dopo che si sono apportate delle modifiche nelle impostazioni della sezione e si è premuto il pulsante **Salva**.

Recupera la configurazione da copia di backup – una lista a cascata che include le copie salvate delle impostazioni dell'intera sezione a cui si può ritornare dopo aver apportato

delle modifiche. Il pulsante diventa attivo dopo che si sono apportate delle modifiche nelle impostazioni della sezione e si è premuto il pulsante **Salva**.

Resetta tutti i parametri ai valori iniziali – per ripristinare tutti i parametri di questa sezione ai valori che avevano prima della modifica corrente (ultimi valori salvati).

Resetta tutti i parametri ai valori default – per ripristinare tutti i parametri di questa sezione ai valori di default.

4. Per accettare le modifiche apportate nelle impostazioni della sezione, premere il pulsante **Salva**, dopodiché sarà necessario riavviare il Server. Per farlo, premere il pulsante **Riavvia Server Dr.Web** nella barra degli strumenti di questa sezione.

8.5.1. Generali

Nella scheda **Generali** vengono configurate le seguenti impostazioni del funzionamento del web server:

- **Indirizzo di Server Dr.Web** – l'indirizzo IP o il nome DNS del Server Dr.Web.

  Viene impostato nel formato:

  <Indirizzo IP o nome DNS del Server> [**:** *<porta>*]

  Se l'indirizzo del Server non è impostato, viene utilizzato il nome di computer restituito dal sistema operativo o l'indirizzo di rete del Server: il nome DNS, se disponibile, altrimenti l'indirizzo IP.

  Se il numero di porta non è impostato, viene utilizzata la porta impostata nella richiesta (per esempio in caso di connessione al Server dal Pannello di controllo o attraverso **Web API**). In particolare, in caso di una richiesta dal Pannello di controllo è la porta specificata nella barra degli indirizzi per la connessione del Pannello di controllo al Server.

  Valore è memorizzato nel parametro `<server-name />` nel file di configurazione `webmin.conf`.

  Il valore del parametro viene utilizzato anche quando vengono generati i link per il download del file d'installazione di Agent per le postazioni della rete antivirus.
- **Numero di richieste parallele** – numero di richieste parallele elaborate dal web server. Questo parametro influisce sulle prestazioni del server. Non è consigliabile modificarne il valore senza necessità.
- **Numero di threads input/output** – numero di flussi che elaborano i dati trasmessi in rete. Questo parametro influisce sulle prestazioni del Server. Non è consigliabile modificarne il valore senza necessità.
- **Time-out (sec)** – time-out di una sessione HTTP. In caso di connessioni permanenti, il Server interrompe la connessione se entro il periodo indicato non arrivano richieste dal client.
- **Velocità di invio minima (B/s)** – velocità minima dell'invio dei dati. Se la velocità di trasmissione in uscita nella rete è più bassa di questo valore, la connessione sarà rifiutata. Impostare il valore 0 per togliere questa limitazione.
- **Velocità di ricezione minima (B/s)** – velocità minima della ricezione dei dati. Se la velocità di trasmissione in arrivo nella rete è più bassa di questo valore, la connessione sarà rifiutata. Impostare il valore 0 per togliere questa limitazione.

- **Dimensione del buffer di invio (KB)** – dimensione dei buffer utilizzati per l'invio dei dati. Questo parametro influisce sulle prestazioni del Server. Non è consigliabile modificarne il valore senza necessità.
- **Dimensione del buffer di ricezione (KB)** – dimensione dei buffer utilizzati per la ricezione dei dati. Questo parametro influisce sulle prestazioni del Server. Non è consigliabile modificarne il valore senza necessità.
- **Lunghezza massima di una query (KB)** – lunghezza massima ammissibile di una richiesta HTTP.
- **Utilizza compressione** – spuntare il flag per utilizzare la compressione per i dati trasmessi attraverso il canale di comunicazione con il web server tramite HTTP/HTTPS.
  - Se il flag è spuntato, è disponibile la lista a cascata **Livello di compressione**. Da questa lista si può selezionare un livello di compressione dei dati da 1 a 9, dove 1 è il grado minimo e 9 è il grado massimo di compressione.
- **Sostituisci gli indirizzi IP** – spuntare il flag per sostituire gli indirizzi IP con i nomi DNS dei computer nel file di log del Server.
- **Mantieni attiva la sessione SSL** – spuntare il flag per utilizzare una connessione permanente per SSL. Le versioni superate dei browser potrebbero gestire in modo scorretto le connessioni permanenti SSL. In caso di problemi con l'utilizzo del protocollo SSL, disattivare questo parametro.
- **Certificato SSL** – percorso del file di certificato SSL. Nella lista a cascata sono elencati i certificati disponibili dalla directory di Server.
- **Chiave privata SSL** – percorso del file della chiave privata SSL. Nella lista a cascata sono elencate le chiavi private disponibili dalla directory di Server.

8.5.2. Avanzate

Nella scheda **Addizionali** vengono configurate le seguenti impostazioni del funzionamento del web server:

- Spuntare il flag **Mostra errori degli script** per visualizzare errori degli script nel browser. Questo parametro si usa dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza necessità.
- Spuntare il flag **Rintraccia gli script** per attivare il rintracciamento degli script. Questo parametro si usa dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza necessità.
- Spuntare il flag **Consenti l'interruzione degli script** per consentire l'interruzione degli script. Questo parametro si usa dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza necessità.

8.5.3. Trasporto

Nella scheda **Trasporto** vengono configurati gli indirizzi di rete "in ascolto" da cui il web server accetta le connessioni in entrata, per esempio per la connessione del Pannello di controllo o per l'esecuzione di richieste attraverso Web API:

- Nella sezione **Indirizzi ascoltati tramite HTTP**, viene configurata una lista delle interfacce su cui il server è in ascolto per accettare connessioni attraverso il protocollo HTTP:

  Nei campi **Indirizzo** e **Porta** è necessario indicare rispettivamente l'indirizzo IP e il numero di porta dell'interfaccia di rete da cui è consentito accettare le connessioni attraverso il protocollo HTTP.

  Di default, per "l'ascolto" da parte del web server vengono impostati:

  - **Indirizzo**: `0.0.0.0` – utilizza "tutte le interfacce di rete" per questa macchina su cui è installato il web server.
  - **Porta**: `9080` – utilizza la porta standard `9080` per il protocollo HTTP.
- Nella sezione **Indirizzi ascoltati tramite HTTPS**, viene configurata una lista delle interfacce su cui il server è in ascolto per accettare connessioni attraverso il protocollo HTTPS:

  Nei campi **Indirizzo** e **Porta** è necessario indicare rispettivamente l'indirizzo IP e il numero di porta dell'interfaccia di rete da cui è consentito accettare le connessioni attraverso il protocollo HTTPS.

  Di default, per "l'ascolto" da parte del web server vengono impostati:

  - **Indirizzo**: `0.0.0.0` – utilizza "tutte le interfacce di rete" per questa macchina su cui è installato il web server.
  - **Porta**: `9081` – utilizza la porta standard `9081` per il protocollo HTTPS.

Per aggiungere un nuovo campo di indirizzo, premere il pulsante  della sezione corrispondente. Per eliminare un campo, premere il pulsante  accanto al campo da eliminare.

8.5.4. Sicurezza

Nella scheda **Sicurezza** vengono impostate le limitazioni riguardanti gli indirizzi di rete da cui il web server accetta le richieste HTTP e HTTPS.

Per impostare le limitazione di accesso per un tipo di connessione:

1. Per consentire l'accesso attraverso HTTP o HTTPS da determinati indirizzi, includerli nelle liste rispettive **HTTP: Consentito** o **HTTPS: Consentito**.
2. Per vietare l'accesso attraverso HTTP o HTTPS da determinati indirizzi, includerli nelle liste rispettive **HTTP: Negato** o **HTTPS: Negato**.
3. Gli indirizzi non inclusi in nessuna lista vengono consentiti o proibiti a seconda della selezione dei flag **Priorità di negazione per HTTP** e **Priorità di negazione per HTTPS**: se il flag è selezionato, gli indirizzi non inclusi in nessuna lista (o inclusi in tutte e due) vengono proibiti. In caso contrario, tali indirizzi vengono consentiti.

Per modificare una lista degli indirizzi:

1. Inserire l'indirizzo di rete nel campo corrispondente e premere il pulsante **Salva**.
2. Indirizzo di rete viene definito come: <*indirizzo-IP*>/[<*prefisso*>].

   Le liste per inserire gli indirizzi TCPv6 saranno visualizzate solo se sul computer è installata l'interfaccia IPv6.

3. Per aggiungere un nuovo campo di indirizzo, premere il pulsante  della sezione corrispondente.
4. Per eliminare un campo, premere il pulsante  .

Esempio di utilizzo del prefisso:

1. Il prefisso 24 sta per la maschera di rete: `255.255.255.0`

   Contiene 254 indirizzi.

   Gli indirizzi di host in queste reti sono del tipo: `195.136.12.*`
2. Il prefisso 8 sta per la maschera di rete `255.0.0.0`

   Contiene fino a 16387064 indirizzi (256*256*256).

   Gli indirizzi di host in queste reti sono del tipo: `125.*.*.*`

8.6. Procedure personalizzate

Eseguendo script lua, l'amministratore ottiene l'accesso a tutto il file system all'interno del directory di Server e ad alcuni comandi di sistema sul computer su cui Server è installato.

Per vietare l'accesso alle procedure personalizzate, disattivare il permesso **Modifica della configurazione del Server e di quella del repository** per il relativo amministratore (v. p. Amministratori e gruppi di amministratori).

Per semplificare e automatizzare l'esecuzione di determinati task di Server Dr.Web, si possono utilizzare delle procedure personalizzate realizzate come gli script lua.

Le procedure personalizzate si trovano nella seguente sottodirectory della directory d'installazione di Server:

- in caso di SO Windows: `var\extensions`
- in caso di SO FreeBSD: `/var/drwcs/extensions`
- per i SO Linux e Solaris: `/var/opt/drwcs/extensions`

Dopo l'installazione di Server, in questa sottodirectory si trovano le procedure personalizzate predefinite.

Si consiglia di modificare procedure personalizzate attraverso il Pannello di controllo.

Per configurare l'esecuzione delle procedure personalizzate:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Procedure personalizzate**. Si apre la finestra di configurazione delle procedure personalizzate.

Albero delle procedure

La lista gerarchica delle procedure riflette una struttura ad albero, i nodi della quale sono i gruppi di procedure e le procedure che ne fanno parte.

Inizialmente nell'albero delle procedure sono presenti i seguenti gruppi predefiniti:

- **Examples of the hooks** – contiene i template di tutte le procedure personalizzate disponibili. Sulla base di questi template, si possono creare le proprie procedure personalizzate.
- **IBM Tivoli integration** – contiene i template delle procedure personalizzate utilizzate per l'integrazione con il sistema IBM Tivoli.

L'icona di un elemento dell'albero dipende dal tipo o dallo stato di questo elemento (v. tabella 8-6).

Tabella 8-6. Le icone degli elementi dell'albero delle procedure

Icona	Descrizione
Gruppi di procedure	
	Gruppo di procedure per cui è consentita l'esecuzione delle procedure.
	Gruppo di procedure per cui è proibita l'esecuzione delle procedure.
Procedure	
	Procedura per cui è consentita l'esecuzione.
	Procedura per cui è proibita l'esecuzione.

Gestione dell'albero delle procedure

Per gestire oggetti nell'albero delle procedure, si usano i seguenti elementi della barra degli strumenti:

 – lista a cascata che si usa per aggiungere un elemento all'albero delle procedure:

 **Aggiungi procedura personalizzata** – per aggiungere una nuova procedura personalizzata.

 **Aggiungi gruppo di procedure personalizzate** – per creare un nuovo gruppo custom in cui verranno messe le procedure.

Rimuovi gli oggetti selezionati – per rimuovere una procedura personalizzata o un gruppo selezionato nell'albero delle procedure.

Consenti l'esecuzione della procedura personalizzata – l'azione simile si esegue tramite l'editor delle procedure selezionando il flag **Consenti l'esecuzione della procedura personalizzata**. V. inoltre Attivazione delle procedure.

Proibisci l'esecuzione della procedura personalizzata – l'azione simile si esegue tramite l'editor delle procedure togliendo la spunta alla voce **Consenti l'esecuzione della procedura personalizzata**. V. inoltre Attivazione delle procedure.

Gestione dei gruppi di procedure

Per creare un nuovo gruppo:

1. Nella barra degli strumenti selezionare → **Aggiungi gruppo di procedure personalizzate**.
2. Nella finestra che si è aperta, impostare i seguenti parametri:
   - Spuntare il flag **Consenti l'esecuzione della procedura personalizzata** per attivare le procedure che faranno parte di questo gruppo. V. inoltre Attivazione delle procedure.
   - Nel campo **Nome del gruppo** specificare un nome per il gruppo che viene creato.
3. Premere il pulsante **Salva**.

Per modificare l'ordine di utilizzo dei gruppi:

1. Nell'albero delle procedure trascinare (drag and drop) un gruppo di procedure e metterlo nel giusto ordine rispetto agli altri gruppi.
2. L'ordine di utilizzo delle procedure cambierà automaticamente quando viene modificato l'ordine dei gruppi: per prime verranno eseguite le procedure dai gruppi che si trovano più in alto nell'albero delle procedure.

Per spostare una procedura in un altro gruppo:

1. Nell'albero delle procedure selezionare la procedura che si desidera spostare.
2. Nella barra delle proprietà aperta dalla lista a cascata **Gruppo padre** selezionare il gruppo in cui si vuole spostare la procedura.
3. Premere il pulsante **Salva**.

Gestione delle procedure

Per aggiungere una nuova procedura:

1. Nella barra degli strumenti selezionare → **Aggiungi procedura personalizzata**.
2. Nella finestra che si è aperta, impostare i seguenti parametri:

- Spuntare il flag **Consenti l'esecuzione della procedura personalizzata** per attivare la procedura che viene creata. V. inoltre Attivazione delle procedure.
- Dalla lista a cascata **Gruppo padre** selezionare il gruppo in cui sarà situata la procedura che viene creata. In seguito sarà possibile spostare la procedura in un altro gruppo – v. sopra.
- Dalla lista a cascata **Procedura personalizzata** selezionare il tipo di procedura. Il tipo di procedura definisce l'azione per cui verrà invocata questa procedura.
- Nel campo **Testo della procedura personalizzata** immettere lo script lua che verrà eseguito quando verrà invocata questa procedura.
  Nella sottosezione **Informazioni sulla procedura** viene riportato l'evento per cui verrà invocata questa procedura; viene indicato se per questa procedura è disponibile il database di Server; nonché vengono riportate liste dei parametri di input e dei valori restituiti per questo tipo di procedura.

3. Premere il pulsante **Salva**.

Per modificare una procedura:

1. Nell'albero delle procedure selezionare la procedura che si desidera modificare.
2. Nella parte destra della finestra si apre automaticamente la barra delle proprietà di questa procedura. Possono essere modificati tutti i parametri che venivano impostati durante la creazione della procedura, ad eccezione del parametro **Procedura personalizzata**. Questo parametro definisce l'evento per cui viene invocata questa procedura e non può essere modificato dopo la creazione della procedura.
3. Premere il pulsante **Salva**.

Attivazione delle procedure

L'attivazione delle procedure e dei gruppi di procedure definisce se le procedure verranno eseguite o meno al verificarsi degli eventi corrispondenti.

Per attivare una procedura o un gruppo di procedure:

1. Nell'albero delle procedure selezionare la procedura o il gruppo che si desidera attivare.
2. Eseguire una delle seguenti azioni:
   - Nella barra degli strumenti premere il pulsante **Consenti l'esecuzione della procedura personalizzata**.
   - Nella parte destra della finestra nella barra delle proprietà dell'oggetto selezionato spuntare il flag **Consenti l'esecuzione della procedura personalizzata** se la spunta è tolta. Premere il pulsante **Salva**.

Caratteristiche dell'attivazione delle procedure:

Affinché una procedura venga eseguita al verificarsi dell'evento corrispondente, è necessario quanto segue:

a) la procedura deve essere attivata;

b) deve essere attivato il gruppo in cui rientra questa procedura.

> Se un gruppo di procedure è disattivato, le procedure che ne fanno parte non verranno eseguite anche se loro stesse sono attivate.
>
> Quando viene attivato un gruppo, verranno eseguite soltanto quelle procedure contenute che sono attivate.

8.7. Configurazione degli avvisi

Dr.Web Enterprise Security Suite supporta la possibilità di inviare gli avvisi su attacchi dei virus, su stato dei componenti della rete antivirus e su altri eventi agli amministratori della rete antivirus Dr.Web Enterprise Security Suite.

8.7.1. Configurazione degli avvisi

Per configurare gli avvisi su eventi nella rete antivirus:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo. Nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione delle notifiche**.
2. Quando si configurano gli avvisi per la prima volta, la lista degli avvisi deve essere vuota. Premere **Aggiungi avviso**.
3. Per abilitare l'invio di avvisi, mettere il controllo a sinistra dell'intestazione di un blocco nella posizione appropriata:

    – l'invio di avvisi per questo blocco è abilitato.

    – gli avvisi di questo blocco non verranno inviati.
4. In questa sezione, si possono creare alcuni blocchi (profili) degli avvisi, per esempio a seconda di vari modi di invio. Per aggiungere un altro blocco, premere  a destra delle impostazioni del blocco di avvisi. In fondo alla pagina verrà aggiunto un altro blocco di avvisi. Diversi blocchi di avvisi e testi dei template vengono configurati in modo indipendente.
5. Nel campo **Intestazione** impostare il nome del blocco di avvisi aggiunto. Questo nome verrà utilizzato, per esempio nella configurazione del task **Report statistici** nel calendario del Server. Per la modifica successiva dell'intestazione, premerla con il tasto sinistro del mouse e digitare il nome richiesto. Se ci sono più di un blocco di avvisi, quando si fa clic sul testo dell'intestazione, viene visualizzata una lista a cascata con le intestazioni dei blocchi di avvisi esistenti.

6. Per configurare l'invio delle notifiche, selezionare il modo di invio richiesto dalla lista a cascata **Metodo di invio notifiche**:
   - Console web – per inviare gli avvisi che verranno visualizzati nella Console web.
   - E-mail – per inviare gli avvisi via posta elettronica.
   - SNMP – per inviare gli avvisi attraverso il protocollo SNMP.
   - Notifiche push – per inviare gli avvisi push sul Pannello di controllo della sicurezza mobile Dr.Web. Questa voce diventa disponibile nella lista a cascata **Metodo di invio notifiche** soltanto dopo che il Pannello di controllo della sicurezza mobile Dr.Web viene connesso a questo Server Dr.Web.
   - Windows Message – per inviare avvisi mediante **Windows Messenger** (solo per i Server SO Windows).

   Le impostazioni di ciascuno dei tipi di invio di notifiche sono descritte di seguito in questa sezione.
7. Per inviare avvisi, si può utilizzare un set di avvisi predefiniti del Server.

   Gli avvisi predefiniti e i loro parametri vengono descritti nel documento **Allegati**, in Allegato D1. Descrizione degli avvisi predefiniti.

   Per configurare avvisi concreti, è necessario:

   a) Nella lista degli avvisi, spuntare i flag di fronte agli avvisi che verranno inviati in conformità al metodo di invio del blocco di avvisi corrente.

   b) Per modificare le impostazioni degli avvisi, premere ⚙ di fronte all'avviso che viene modificato. Si apre il template dell'avviso. Se necessario, modificare il testo dell'avviso che verrà inviato. Nel testo di avviso, si possono utilizzare le variabili di template (tra parentesi graffe). Per aggiungere le variabili, sono disponibili liste a cascata nell'intestazione del messaggio. Quando un messaggio viene preparato, il sistema di avviso sostituisce le variabili di template con un testo specifico che dipende dalle sue impostazioni correnti. La lista delle variabili disponibili viene riportata nel documento **Allegati**, in Allegato D3. Parametri dei template del sistema di avviso.

   c) Per gli avvisi via email viene fornita la possibilità di aggiungere campi personalizzati nella sezione aggiuntiva **Intestazioni** nell'editor dei template per ciascun avviso (v. p. **b)**). Le intestazioni devono essere formate in conformità con gli standard RFC 822, RFC 2822 e non devono intersecarsi con i campi definiti negli standard per messaggi di posta elettronica. In particolare, lo standard RFC 822 garantisce l'assenza nella specifica delle intestazioni che iniziano con `X-` perciò è consigliabile impostare nomi in formato `X-`<*nome-intestazione*>. Per esempio: `X-Template-Language: Italian`.

   d) In caso degli avvisi della sottosezione **Postazione** è inoltre possibile impostare una lista delle postazioni circa le cui eventi verranno spediti gli avvisi. Nella finestra di modifica del template nell'albero **Gruppi di postazioni monitorate** selezionare gruppi di postazioni per cui verranno tracciati gli eventi e verranno spediti gli avvisi corrispondenti. Per selezionare diversi gruppi, utilizzare i tasti CTRL o MAIUSCOLO.

In caso del metodo di invio **SNMP** i template di avvisi vengono impostati sul lato destinatario (*postazione di comando* secondo RFC 1067). Tramite il Pannello di controllo, sottosezione **Postazione** si può impostare soltanto una lista delle postazioni sugli eventi sulle quali verranno spediti gli avvisi.

8. Dopo aver finito di modificare le impostazioni, premere il pulsante **Salva** per salvare tutte le modifiche apportate.

Avvisi che vengono visualizzati nella Web console

Per gli avvisi che vengono visualizzati nella Web console, impostare i seguenti parametri:

- **Numero di tentativi di invio** – numero di tentativi di invio del messaggio in caso di un invio non riuscito. Il numero predefinito è 10.
- **Time-out del tentativo di invio** – periodo in secondi, finito il quale viene fatto un tentativo ripetuto di invio dell'avviso. Il time-out predefinito è di 300 secondi.
- **Tempo di conservazione di una notifica** – tempo per il quale deve essere conservato un avviso dal momento della ricezione. Il tempo predefinito è di 1 giorno. Dopo il tempo specificato, l'avviso viene contrassegnato come obsoleto e viene eliminato secondo il task **Rimozione dei messaggi obsoleti** impostato nel calendario del Server.

  Per gli avvisi ricevuti tramite questo metodo di invio, si può impostare un tempo illimitato di conservazione nella sezione Notifiche della web console.
- **Invia un messaggio di test** – per inviare un avviso di test in conformità alle impostazioni del sistema di avviso. Il testo di tale avviso viene specificato nei template di avvisi.

Avvisi via email

Per gli avvisi via email, impostare i seguenti parametri:

- **Numero di tentativi di invio** – numero di tentativi di invio del messaggio in caso di un invio non riuscito. Il numero predefinito è 10.
- **Time-out del tentativo di invio** – periodo in secondi, finito il quale viene fatto un tentativo ripetuto di invio dell'avviso. Il time-out predefinito è di 300 secondi.
- **Indirizzo e-mail del mittente** – indirizzo di posta elettronica del mittente degli avvisi.
- **Indirizzi e-mail dei destinatari** – indirizzi di posta elettronica dei destinatari dei messaggi. In ciascun campo si può inserire soltanto un indirizzo di posta elettronica di destinatario. Per aggiungere un altro campo di destinatario, premere il pulsante  . Per rimuovere un campo, premere il pulsante  .
- Nella sezione **Impostazioni del server SMTP**, impostare i seguenti parametri:
  - **Indirizzo** – indirizzo del server SMTP che verrà utilizzato per l'invio delle email.
  - **Porta** – porta per la connessione al server SMTP. Di default è la porta 465 se viene aperta una connessione TLS protetta separata, altrimenti è la porta 25.
  - **Utente**, **Password** – se necessario, impostare il nome utente e la password dell'utente del server SMTP se il server SMTP richiede l'autenticazione.

- Spuntare il flag **Crittografia STARTTLS** per lo scambio di dati crittografati. In tale caso il programma passa alla connessione protetta attraverso il comando `STARTTLS`. Di default per la connessione è previsto l'utilizzo della porta 25.
- Spuntare il flag **Crittografia SSL** per lo scambio di dati crittografati. In tale caso verrà aperta una connessione TLS protetta separata. Di default per la connessione è previsto l'utilizzo della porta 465.
- Spuntare il flag **Utilizza l'autenticazione CRAM-MD5** per utilizzare *l'autenticazione* CRAM-MD5 sul mail server.
- Spuntare il flag **Utilizza l'autenticazione DIGEST-MD5** per utilizzare *l'autenticazione* DIGEST-MD5 sul mail server.
- Spuntare il flag **Utilizza l'autenticazione Plain** per utilizzare l'autenticazione *plain text* sul mail server.
- Spuntare il flag **Utilizza l'autenticazione LOGIN** per utilizzare *l'autenticazione* LOGIN sul mail server.
- Spuntare il flag **Verifica se il certificato SSL del server è corretto** per controllare la correttezza del certificato *SSL* del mail server.
- Spuntare il flag **Modalità debug** per ottenere un log dettagliato di sessione SMTP.

- **Invia un messaggio di test** – per inviare un avviso di test in conformità alle impostazioni del sistema di avviso. Il testo di tale avviso viene specificato nei template di avvisi.

Avvisi attraverso il protocollo SNMP

Per gli avvisi attraverso il protocollo SNMP, impostare i seguenti parametri:

- **Numero di tentativi di invio** – numero di tentativi di invio del messaggio in caso di un invio non riuscito. Il numero predefinito è 10.
- **Time-out del tentativo di invio** – periodo in secondi, finito il quale viene fatto un tentativo ripetuto di invio dell'avviso. Il time-out predefinito è di 300 secondi.
- **Destinatario** – entità che riceve una query SNMP. Per esempio, un indirizzo IP o il nome DNS di un computer. In ciascun campo si può inserire soltanto un destinatario. Per aggiungere un altro campo di destinatario, premere il pulsante  . Per rimuovere un campo, premere il pulsante  .
- **Mittente** – entità che invia una query SNMP. Per esempio, un indirizzo IP o un nome DNS di computer (deve essere riconosciuto dal server DNS).

  Se il mittente non è impostato, di default si usa `"localhost"` per SO Windows e `""` per SO della famiglia UNIX.
- **Community** – community SNMP o contesto. Di default è `public`.
- **Invia un messaggio di test** – per inviare un avviso di test in conformità alle impostazioni del sistema di avviso. Il testo di tale avviso viene specificato nei template di avvisi.

Avvisi Push

Per gli avvisi Push che vengono mandati sul Pannello di controllo mobile, impostare i seguenti parametri:

- **Numero di tentativi di invio** – numero di tentativi di invio del messaggio in caso di un invio non riuscito. Il numero predefinito è 10.
- **Time-out del tentativo di invio** – periodo in secondi, finito il quale viene fatto un tentativo ripetuto di invio dell'avviso. Il time-out predefinito è di 300 secondi.
- **Invia un messaggio di test** – per inviare un avviso di test in conformità alle impostazioni del sistema di avviso. Il testo di tale avviso viene specificato nei template di avvisi.

Avvisi di rete di Windows

Il sistema di avviso di rete Windows funziona solamente nel SO Windows con il supporto del servizio Windows Messenger (Net Send).

SO Windows Vista e superiori non supportano il servizio Windows Messenger.

Per i messaggi di rete di SO Windows, impostare i seguenti parametri:

- **Numero di tentativi di invio** – numero di tentativi di invio del messaggio in caso di un invio non riuscito. Il numero predefinito è 10.
- **Time-out del tentativo di invio** – periodo in secondi, finito il quale viene fatto un tentativo ripetuto di invio dell'avviso. Il time-out predefinito è di 300 secondi.
- **Destinatario** – lista dei nomi dei computer su cui si ricevono i messaggi. In ciascun campo si può inserire soltanto un nome di computer. Per aggiungere un altro campo di destinatario, premere il pulsante  Per rimuovere un campo, premere il pulsante  .
- **Invia un messaggio di test** – per inviare un avviso di test in conformità alle impostazioni del sistema di avviso. Il testo di tale avviso viene specificato nei template di avvisi.

8.7.2. Avvisi nella console web

Tramite il Pannello di controllo, è possibile visualizzare e gestire gli avvisi all'amministratore, ricevuti tramite il metodo **Web console** (l'invio di avvisi all'amministratore è descritto nella sezione Configurazione degli avvisi).

Per visualizzare e gestire gli avvisi:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo. Nella finestra che si è aperta selezionare la voce del menu di gestione **Notifiche della web console**. Si apre un elenco degli avvisi inviati sulla Web console.
2. Per visualizzare un avviso, premere la riga corrispondente della tabella. Si apre una finestra con il testo dell'avviso. L'avviso verrà contrassegnato automaticamente come letto.

3. Per gestire la lista degli avvisi, utilizzare i seguenti elementi:

   a) Gli elementi generali della barra degli strumenti vengono utilizzati per gestire la sezione degli avvisi in generale. Questi strumenti sono sempre disponibili nella barra degli strumenti:

Impostazione		Azione
Gravità	**Massima**	Per visualizzare soltanto gli avvisi con la gravità **Massima**
	Alta	Per visualizzare gli avvisi con la gravità da **Alta** a **Massima**
	Media	Per visualizzare gli avvisi con la gravità da **Media** a **Massima**
	Bassa	Per visualizzare gli avvisi con la gravità da **Bassa** a **Massima**
	Minima	Per visualizzare tutti gli avvisi con la gravità da **Minima** a **Massima**
Fonte	**Agent**	Per visualizzare gli avvisi relativi ad eventi su postazioni
	Server	Per visualizzare gli avvisi relativi ad eventi su Server

   Per visualizzare gli avvisi ricevuti entro un determinato intervallo di tempo, utilizzare uno dei seguenti metodi:

   - Nella lista a cascata nella barra degli strumenti selezionare uno degli intervalli di tempo predefiniti.
   - Nei calendari a cascata selezionare le date di inizio e di fine di un intervallo di tempo.

   Dopo aver modificato i valori di queste impostazioni, premere il pulsante **Aggiorna** per visualizzare l'elenco degli avvisi in conformità alle impostazioni definite.

   b) Per gestire singoli avvisi, spuntare i flag di fronte agli avvisi richiesti oppure il flag generale nell'intestazione della tabella se si vogliono selezionare tutti gli avvisi nella lista. Con questo diventano disponibili gli elementi della barra degli strumenti utilizzati per la gestione di avvisi selezionati:

   Elimina avvisi – per eliminare definitivamente tutti gli avvisi selezionati senza la possibilità di recupero.

   Contrassegna avvisi come letti – per contrassegnare come letti tutti gli avvisi selezionati.

   c) Spuntare la casella **Conserva il messaggio senza rimozione automatica** nell'elenco degli avvisi di fronte agli avvisi che non devono essere eliminati dopo la fine del periodo di conservazione (il periodo di conservazione viene impostato prima dell'invio di avvisi nella sezione Configurazione delle notifiche nelle impostazioni del metodo di invio **Console web**). Tali avvisi verranno conservati fino a quando non verranno rimossi manualmente nella sezione **Notifiche della web console** oppure non verrà deselezionata la casella di fronte a questi avvisi.

8.7.3. Avvisi non inviati

Tramite il Pannello di controllo, è possibile tracciare e gestire gli avvisi all'amministratore che non sono stati inviati secondo le impostazioni della sezione Configurazione delle notifiche.

Per visualizzare e gestire gli avvisi non inviati:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo. Nella finestra che si è aperta selezionare la voce del menu di gestione **Notifiche non inviate**. Si apre l'elenco delle notifiche non inviate di questo Server.
2. Nell'elenco delle notifiche non inviate vengono elencati gli avvisi di cui l'invio non è riuscito, ma il numero di tentativi di invio, determinato nelle impostazioni di quest'avviso, non si è ancora esaurito.
3. La tabella di avvisi non inviati contiene le seguenti informazioni:
   - **Notifica** – nome di avviso dall'elenco degli avvisi predefiniti.
   - **Intestazione** – nome del blocco di avvisi, secondo le impostazioni di cui viene inviato questo avviso.
   - **Tentativi di invio rimanenti** – numero di tentativi rimanenti di invio dell'avviso se un invio non è riuscito. Il numero iniziale di tentativi di invio ripetuto viene impostato quando si configurano gli avvisi nella sezione Configurazione delle notifiche. Dopo che un avviso è stato inviato, non è possibile modificare il numero di tentativi di invio ripetuto di questo avviso.
   - **Tempo del successivo tentativo di invio** – data e ora del successivo tentativo di invio dell'avviso. La periodicità con cui si ripetono i tentativi di invio dell'avviso viene impostata quando si configurano gli avvisi nella sezione Configurazione delle notifiche. Dopo che un avviso è stato inviato, non è possibile modificare la periodicità di tentativi ripetuti di invio di questo avviso.
   - **Destinatario** – indirizzi dei destinatari dell'avviso.
   - **Errore** – errore per cui non è stato possibile inviare l'avviso.
4. Per gestire gli avvisi non inviati:
   a) Spuntare i flag di fronte a concreti avvisi oppure il flag nell'intestazione della tabella per selezionare tutti gli avvisi nella lista.
   b) Utilizzare i seguenti pulsanti nella barra degli strumenti:

      Rispedisci – per inviare subito gli avvisi selezionati. Verrà effettuato un tentativo straordinario di invio dell'avviso. Se l'invio non sarà riuscito, il numero di tentativi rimanenti diminuirà di uno, e il tempo del successivo tentativo verrà conteggiato dal momento dell'invio corrente con la periodicità impostata nella sezione Configurazione delle notifiche.

      Rimuovi – per eliminare definitivamente tutti gli avvisi non inviati selezionati senza la possibilità di recupero.
5. Gli avvisi non inviati vengono cancellati dalla lista nei seguenti casi:
   a) L'avviso è stato mandato con successo al destinatario.

b) L'avviso è stato cancellato dall'amministratore manualmente tramite il pulsante **Rimuovi** nella barra degli strumenti.

c) Si è esaurito il numero di tentativi di invio ripetuto e la notifica non è stata inviata.

d) Nella sezione Configurazione delle notifiche è stato eliminato il blocco di avvisi, secondo le cui impostazioni venivano inviati questi avvisi.

8.8. Gestione del repository di Server Dr.Web

Il repository di Server Dr.Web è studiato per conservare i campioni modello del software e per aggiornarli dai server SAM.

Per questo fine, il repository utilizza un set dei file che vengono chiamati *prodotti*. Ciascun prodotto si trova in una sottodirectory separata della directory di `repository` che si trova nella directory `var` che con l'installazione di default è una sottodirectory della directory radice di Server. Le funzioni di repository, nonché la gestione delle funzioni, vengono effettuate indipendentemente per ciascun prodotto.

Per gestire il repository, si utilizza il concetto *revisione* di un prodotto. Una revisione è lo stato dei file di un prodotto, corretto per un determinato momento (comprende nomi dei file e checksum), essa è caratterizzata da un numero unico.

Il repository sincronizza le revisioni di un prodotto nelle seguenti direzioni:

a) su Server Dr.Web dal sito di aggiornamento del prodotto (via protocollo HTTP),

b) tra vari Server Dr.Web nella configurazione con diversi server (secondo il criterio di scambio impostato),

c) da Server Dr.Web su postazioni.

Il repository permette all'Amministratore della rete antivirus di impostare i seguenti parametri:

- lista dei siti di aggiornamento nelle operazioni del tipo **a)**;
- limitare la lista dei prodotti che richiedono la sincronizzazione del tipo **a)** (in questo modo, l'utente ha la possibilità di tracciare solamente le modifiche necessarie di singole categorie di prodotti);
- limitare la lista delle parti dei prodotti che richiedono la sincronizzazione del tipo **c)** (l'utente può scegliere che cosa concretamente è da installare su postazioni);
- controllare il passaggio alle revisioni nuove (si possono testare i prodotti per conto proprio prima dell'implementazione);
- aggiungere propri componenti ai prodotti;
- creare indipendentemente degli nuovi prodotti per cui anche viene eseguita la sincronizzazione.

Attualmente nella fornitura sono compresi i seguenti prodotti:

- Server Dr.Web,

- Agent Dr.Web (software Agent, software antivirus postazione per i sistemi operativi corrispondenti),
- Server proxy Dr.Web,
- Database dei virus Dr.Web,
- Database di SpIDer Gate,
- Database di Antispam Dr.Web,
- Notizie di Doctor Web.

8.8.1. Stato del repository

Per controllare lo stato attuale del repository o per aggiornare i componenti della rete antivirus:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Stato del repository**.
2. La finestra che si è aperta visualizza una lista dei prodotti del repository, la data della revisione utilizzata al momento, la data della revisione ultima scaricata e lo stato dei prodotti.

   Nella colonna **Stato** è indicato lo stato dei prodotti nel repository di Server al momento dell'ultimo aggiornamento.

3. Per gestire i contenuti del repository, utilizzare i seguenti pulsanti:
   - Premere il pulsante **Verifica aggiornamenti** per verificare la disponibilità degli aggiornamenti di tutti i prodotti su SAM e per scaricare gli aggiornamenti disponibili dai server SAM.
   - Premere il pulsante **Ricarica il repository da disco** per ricaricare la versione corrente del repository da disco.

   Quando viene avviato, il Server carica i contenuti del repository nella memoria, e se durante l'operazione del Server i contenuti del repository sono stati modificati dall'amministratore in un modo diverso da quello fornito dal Pannello di controllo, ad esempio, i contenuti del repository sono stati aggiornati tramite un'utility esterna o manualmente, per cominciare ad utilizzare la versione caricata su disco, è necessario riavviare il repository.

8.8.2. Aggiornamenti differiti

La sezione **Aggiornamenti differiti** contiene una lista dei prodotti per cui gli aggiornamenti di prodotti sono stati vietati temporaneamente nella sezione **Configurazione dettagliata del repository** → <*Prodotto*> → Aggiornamenti differiti. Una revisione differita è considerata *congelata*.

La tabella dei prodotti congelati contiene le seguenti informazioni:

- **Directory nel repository** – nome della directory del prodotto congelato nel repository:
  - 10-drwgatedb – database di SpIDer Gate,
  - 10-drwspamdb – database di AntiSpam,

- 20-drwagent – Agent Dr.Web per Windows,
- 20-drwandroid – Agent Dr.Web per Android,
- 20-drwcs – Server Dr.Web,
- 20-drwunix – Agent Dr.Web per UNIX,
- 80-drwnews – notizie di Doctor Web.

- **Revisione** – numero della revisione congelata.
- **Differito fino al** – tempo fino a cui sono stati differiti gli aggiornamenti di questo prodotto.

Quando si fa clic su una riga della tabella dei prodotti congelati, si apre una tabella con le informazioni dettagliate sulla revisione congelata di questo prodotto.

Le funzioni di aggiornamenti differiti possono essere utilizzate se è necessario annullare temporaneamente la distribuzione di ultima revisione di un prodotto su tutte le postazioni della rete antivirus, per esempio se è necessario prima provare questa revisione su un numero limitato di postazioni.

Per utilizzare le funzioni di aggiornamenti differiti, eseguire le azioni descritte nella sezione **Configurazione dettagliata del repository** → Aggiornamenti differiti.

Per gestire gli aggiornamenti differiti:

1. Spuntare il flag di fronte ai prodotti per cui si vuole impostare un'azione da applicare agli aggiornamenti differiti. Per selezionare tutti i prodotti, spuntare il flag nell'intestazione della tabella dei prodotti congelati.
2. Nella barra degli strumenti selezionare l'azione richiesta:

   Esegui subito – per annullare la congelazione del prodotto e per includere questa revisione nell'elenco delle revisioni con la distribuzione su postazioni secondo la procedura generale.

   Annulla l'aggiornamento – per annullare la congelazione del prodotto e vietare questa revisione. Si riprende il processo di ottenimento di aggiornamenti da SAM. La revisione scongelata verrà cancellata dall'elenco delle revisioni del prodotto. Quando arriverà la prossima revisione, la revisione scongelata verrà cancellata anche dal disco.

   Cambia il tempo di differimento degli aggiornamenti – per impostare il tempo per cui la revisione di questo prodotto viene rinviata. Il tempo di inizio di congelazione viene conteggiato dal momento della ricezione della revisione da SAM.
3. Se per un prodotto congelato non è stata impostata un'azione da applicare dopo lo scongelamento, una volta finito il tempo impostato nell'elenco **Tempo di differimento degli aggiornamenti**, la revisione verrà scongelata automaticamente e verrà inclusa nell'elenco delle revisioni per essere distribuita su postazioni secondo la procedura generale.

8.8.3. Configurazione generale del repository

La sezione **Configurazione generale del repository** consente di impostare i parametri della connessione a SAM e dell'aggiornamento del repository per tutti i prodotti.

Per modificare la configurazione del repository:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nella finestra che si è aperta selezionare la voce del menu di gestione **Configurazione generale del repository**.
3. Configurare tutti i parametri necessari dell'aggiornamento da SAM descritti di seguito.
4. Se modificando i parametri, si devono annullare tutte le modifiche apportate, utilizzare i seguenti pulsanti nella barra degli strumenti:

   Resetta tutti i parametri ai valori iniziali – per ripristinare tutti i parametri di questa sezione nei valori che avevano prima della modifica corrente. Per applicare la stessa azione ai singoli parametri, utilizzare i pulsanti di fronte a ciascun parametro.

   Resetta tutti i parametri ai valori default – per ripristinare tutti i parametri di questa sezione nei valori salvati nel file di configurazione di Server. Per applicare la stessa azione ai singoli parametri, utilizzare i pulsanti di fronte a ciascun parametro.
5. Fare clic su uno dei pulsanti nella barra degli strumenti:
   - **Salva e sincronizza di nuovo** – per salvare tutte le modifiche apportate e per eseguire un aggiornamento del repository da SAM secondo le nuove impostazioni.
   - **Salva e ricarica da disco** – per salvare tutte le modifiche apportate senza aggiornare il repository da SAM. In questo caso la versione di repository corrente viene ricaricata da disco (v. inoltre la sezione Stato del repository).

Configurazione si SAM Dr.Web

Nella scheda **SAM Dr.Web** vengono configurati i parametri della connessione al Sistema di aggiornamento mondiale Dr.Web.

Per modificare i parametri della connessione a SAM, si utilizzano le seguenti impostazioni:

- **URI di base** – la directory sui server di aggiornamento che contiene gli aggiornamenti dei prodotti Dr.Web.
- Spuntare il flag **Utilizza CDN** per consentire l'utilizzo di Content Delivery Network per il caricamento del repository.
- Spuntare il flag **Utilizza SSL** per caricare il repository attraverso la connessione sicura SSL.

  In questo caso dalla lista a cascata **Certificati validi** selezionare il tipo di certificati SSL da accettare automaticamente.
- Se necessario, modificare la lista dei server SAM da cui viene aggiornato il repository, nella sezione **Lista dei server del Sistema di aggiornamento mondiale Dr.Web**:
  - Per aggiungere un server SAM alla lista dei server utilizzati per l'aggiornamento, premere il pulsante ed inserire l'indirizzo del server SAM nel campo aggiunto.
  - Per cancellare un server SAM dalla lista dei server utilizzati, premere il pulsante di fronte al server che si vuole cancellare.

- L'ordine dei server SAM nella lista determina l'ordine di connessione del Server Dr.Web durante l'aggiornamento del repository. Per modificare l'ordine dei server SAM trascinare il server richiesto, tenendo premuto la riga del server alla matrice a sinistra.

Quando viene installato il Server Dr.Web, la lista contiene soltanto i server di aggiornamento della società Doctor Web. Se necessario, è possibile configurare le proprie zone di aggiornamento ed inserirle nella lista dei server per la ricezione degli aggiornamenti.

Configurazione degli aggiornamenti di Agent Dr.Web

L'aggiornamento di repository per il software Agent e per il pacchetto antivirus viene configurato separatamente per le varie versioni dei SO su cui verrà installato tale software:

- Nella scheda **Agent Dr.Web per Windows** nel gruppo di pulsanti di scelta, indicare se è necessario aggiornare tutti i componenti installati su postazioni SO Windows o soltanto i database dei virus.
- Nella scheda **Agent Dr.Web per UNIX** indicare per quali SO della famiglia UNIX è necessario aggiornare i componenti installati su postazioni.

Per disattivare completamente la ricezione di aggiornamenti da SAM per Agent per UNIX, passare alla sezione **Configurazione dettagliata del repository**, voce **Agent Dr.Web per UNIX**, e nella scheda **Sincronizzazione** spuntare il flag **Disattiva l'aggiornamento del prodotto**.

Configurazione degli aggiornamenti di Server Dr.Web

Nella scheda **Server Dr.Web** indicare per quali SO verrà eseguito l'aggiornamento dei file di Server:

- Per ricevere gli aggiornamenti per i Server sotto tutti gli SO supportati, spuntare il flag **Aggiorna tutte le piattaforme disponibili su SAM**.
- Per ricevere gli aggiornamenti per il Server soltanto sotto alcuni degli SO supportati, spuntare i flag solo accanto a questi SO.

Per disattivare completamente la ricezione di aggiornamenti da SAM per Server, passare alla sezione **Configurazione dettagliata del repository**, voce **Server Dr.Web**, e nella scheda **Sincronizzazione** spuntare il flag **Disattiva l'aggiornamento del prodotto**.

Notizie di Doctor Web

Nella scheda **Notizie della società Doctor Web** impostare una lista delle lingue in cui verranno scaricate le notizie.

L'iscrizione alle sezioni di notizie viene configurata nella sezione Impostazioni → **Abbonamento**.

Si possono leggere le notizie di Doctor Web nella sezione del menu principale del Pannello di controllo **Guida** → **Notizie**.

Lingue di Agent Dr.Web per Windows

Nella scheda **Lingue di Agent Dr.Web per Windows** impostare una lista delle lingue dell'interfaccia di Agent e di pacchetto antivirus per SO Windows che verranno scaricate da SAM.

8.8.4. Configurazione dettagliata del repository

La sezione **Configurazione dettagliata del repository** consente di configurare le revisioni separatamente per ogni prodotto nel repository.

Per modificare la configurazione del repository:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nella finestra che si è aperta nella sottosezione del menu di gestione **Configurazione dettagliata del repository** selezionare la voce che corrisponde al prodotto che si vuole modificare.
3. Configurare tutti i parametri di repository necessari del prodotto selezionato, che vengono descritti di seguito.
4. Nella barra degli strumenti premere il pulsante **Salva e ricarica da disco** per salvare tutte le modifiche apportate. In questo caso la versione di repository corrente viene ricaricata da disco (v. inoltre la sezione Stato del repository).

Lista delle revisioni

Nella scheda **Lista delle revisioni** vengono riportate le informazioni su tutte le revisioni di questo prodotto disponibili su questo Server.

La tabella delle revisioni contiene le seguenti colonne:

Nome di colonna	Descrizione dei contenuti
Distribuita	Il marcatore automatico in questa colonna definisce lo stato delle revisioni del prodotto. Nella colonna possono esserci due tipi di marcatore: – *Revisione distribuita*. La revisione viene utilizzata per aggiornare gli Agent e il software antivirus su postazioni. La revisione da distribuire viene selezionata nel seguente modo: 1. Viene distribuita la revisione che è contrassegnata dal marcatore nella colonna **Corrente**. Può essere contrassegnata soltanto una revisione. Per il prodotto **Agent Dr.Web**

Nome di colonna	Descrizione dei contenuti
	per Windows non esiste la possibilità di contrassegnare dal marcatore una revisione che è stata ricevuta prima della revisione che viene distribuita al momento. 2. Se nella colonna **Corrente** nessuna revisione è contrassegnata, viene distribuita l'ultima revisione contrassegnata dal marcatore nella colonna **Conservata**. 3. Se nelle colonne **Corrente** e **Conservata** non è contrassegnata alcuna revisione, viene distribuita la revisione più recente. Il marcatore automatico sempre indica la revisione che viene distribuita. – *Revisione congelata*. Questa revisione non viene distribuita su postazioni, le nuove revisioni non vengono scaricate dal Server. Per le azioni applicabili in caso di congelazione della revisione, consultare la sottosezione Aggiornamenti differiti. Se c'è una revisione congelata, la revisione da distribuire viene selezionata nel seguente modo: 1. Se è impostato il marcatore nella colonna **Corrente**, su postazioni viene distribuita la revisione corrente. 2. Se non è impostato il marcatore nella colonna **Corrente**, su postazioni viene distribuita la revisione precedente a quella congelata.
Corrente	Impostare il marcatore per indicare la revisione di prodotto da utilizzare per l'aggiornamento degli Agent e del software antivirus su postazioni. Può essere impostata soltanto una revisione corrente. Il marcatore che indica la revisione corrente può anche essere non impostato.
Conservata	Impostare il marcatore per conservare questa revisione quando il repository viene cancellato in automatico. Il marcatore può essere impostato per più revisioni alla volta. Il marcatore può anche essere non impostato. Il Server conserva su disco un determinato numero di revisioni di prodotto, che viene impostato nella scheda **Sincronizzazione**. Quando viene raggiunto il numero massimo di revisioni conservate temporaneamente, per salvare una nuova revisione scaricata da SAM, la revisione più vecchia conservata temporaneamente viene rimossa. Quando il repository viene cancellato in automatico, non vengono rimosse le seguenti revisioni: • Le revisioni contrassegnati dal marcatore nella colonna **Conservata**. • La revisione contrassegnata dal marcatore nella colonna **Corrente**. Se una revisione di prodotto funziona in modo stabile, si può contrassegnarla come conservata, e qualora da SAM arrivi una revisione non stabile, si può eseguire il rollback a quella precedente.

Nome di colonna	Descrizione dei contenuti
Revisione	Data di ricezione della revisione di prodotto. Se la revisione è congelata, in questa colonna inoltre viene visualizzato lo stato del blocco.

Sincronizzazione

Nella scheda **Sincronizzazione** vengono configurati i parametri dell'aggiornamento del repository di Server da SAM:

- Nella lista a cascata **Numero di revisioni conservate** si imposta il numero di revisioni di prodotto che sono conservate temporaneamente su disco, senza contare le revisioni contrassegnate in almeno una delle colonne nella scheda **Lista delle revisioni**. Qualora arrivi una revisione nuova e il numero di revisioni di prodotto abbia già raggiunto il massimo impostato, viene eliminata la revisione più vecchia. Le revisioni contrassegnate come **Corrente**, **Conservata** e **Distribuita** non possono essere eliminate.
- Spuntare il flag **Disattiva l'aggiornamento del prodotto** per disattivare la ricezione degli aggiornamenti di questo prodotto dai server SAM. Gli Agent verranno aggiornati alla revisione corrente sul Server (o secondo la procedura della scelta della revisione da distribuire).

Per alcuni prodotti sono inoltre disponibili le seguenti impostazioni:

- Spuntare il flag **Aggiorna soltanto i seguenti file** per ricevere gli aggiornamenti da SAM soltanto per i file indicati di seguito.
- Spuntare il flag **Non aggiornare soltanto i seguenti file** per disattivare l'aggiornamento da SAM soltanto per i file indicati di seguito.

  Le liste dei file vengono impostate nel formato di espressioni regolari.

  Se sono spuntati entrambi i flag, i file vengono selezionati nel seguente modo:

  1. Dalla lista completa dei file di prodotto, vengono selezionati i file secondo le liste **Aggiorna soltanto i seguenti file**.
  2. Dalla lista ottenuta al passo 1, vengono cancellati i file secondo le liste **Non aggiornare soltanto i seguenti file**.
  3. Da SAM vengono aggiornati soltanto i file selezionati al passo 2.

Avvisi

Nella scheda **Notifiche** vengono configurati le notifiche sugli aggiornamenti del repository:

- Spuntare il flag **Non notificare soltanto dei seguenti file**, per disattivare l'invio delle notifiche soltanto degli eventi relativi ai file indicati nella lista di seguito.
- Spuntare il flag **Notifica soltanto dei seguenti file** per inviare le notifiche soltanto degli eventi relativi ai file indicati nella lista di seguito.

Le liste dei file vengono impostate nel formato di espressioni regolari.

Se le liste di eccezioni non sono impostate, verranno inviate tutte le notifiche attivate sulla pagina Configurazione delle notifiche.

Le notifiche su aggiornamenti di repository vengono configurate sulla pagina di configurazione di notifiche nella sottosezione **Repository**.

Aggiornamenti differiti

Nella scheda **Aggiornamenti differiti** è possibile rinviare la distribuzione di aggiornamenti su postazioni per un determinato periodo. Una revisione differita è considerata congelata.

Queste funzioni possono essere utilizzate se è necessario annullare temporaneamente la distribuzione di ultima revisione di un prodotto su tutte le postazioni della rete antivirus, per esempio se è necessario prima provare questa revisione su un numero limitato di postazioni.

Per utilizzare le funzioni di aggiornamenti differiti, eseguire le seguenti azioni:

1. Per il prodotto da congelare, impostare gli aggiornamenti differiti come viene descritto di seguito.
2. Per annullare la distribuzione dell'ultima revisione, impostare come corrente una delle revisioni precedenti nella scheda Lista delle revisioni.
3. Per il gruppo di postazioni su cui verrà distribuita la revisione più recente, spuntare il flag **Ricevi tutti gli aggiornamenti recenti** nella sezione **Rete antivirus** → Limitazione degli aggiornamenti delle postazioni. Sulle altre postazioni verrà distribuita la revisione che è stata contrassegnata come corrente al passaggio 2.
4. La prossima revisione scaricata da SAM, che soddisfa le condizioni dell'opzione **Differisci solo gli aggiornamenti dei seguenti file**, verrà congelata e differita per il tempo selezionato nella lista **Tempo di differimento degli aggiornamenti**.

Per configurare gli aggiornamenti differiti:

1. Spuntare il flag **Differisci gli aggiornamenti** per annullare temporaneamente il caricamento degli aggiornamenti di questo prodotto ricevuti dai server SAM.
2. Nella lista a cascata **Tempo di differimento degli aggiornamenti** selezionare il tempo per il quale il caricamento degli aggiornamenti viene differito contando dal momento della loro ricezione dai server SAM.
3. Se necessario, spuntare il flag **Differisci solo gli aggiornamenti dei seguenti file** per rinviare la distribuzione degli aggiornamenti che contengono i file che corrispondono alle maschere wildcard specificate nella lista sotto. La lista delle maschere viene impostata nel formato di espressioni regolari.

   Se il flag non è spuntato, verranno congelati tutti gli aggiornamenti che arrivano da SAM.

Per annullare la congelazione:

- Nella scheda **Lista delle revisioni** premere **Esegui subito** per annullare la congelazione del prodotto e per includere questa revisione nell'elenco delle revisioni per distribuirla su postazioni secondo la procedura generale.
- Nella scheda **Lista delle revisioni** premere **Annulla l'aggiornamento** per annullare la congelazione del prodotto e per vietare questa revisione. Si riprende il processo dell'ottenimento di aggiornamenti da SAM. La revisione scongelata verrà rimossa dall'elenco delle revisioni del prodotto. Quando arriva la prossima revisione, la revisione scongelata verrà rimossa anche dal disco.
- Una volta finito il tempo impostato nell'elenco **Tempo di differimento degli aggiornamenti**, la revisione verrà scongelata automaticamente e verrà inclusa nell'elenco delle revisioni per essere distribuita su postazioni secondo la procedura generale.

Le revisioni congelate di tutti i prodotti vengono gestite nella sezione Aggiornamenti differiti.

8.8.5. Contenuti del repository

La sezione **Contenuti del repository** consente di visualizzare e gestire i contenuti correnti del repository a livello di directory e di file del repository.

La finestra principale della sezione **Contenuti del repository** contiene l'albero gerarchico dei contenuti del repository, che riflette tutte le directory e file nella versione corrente del repository con l'elenco di tutte le revisioni disponibili di ogni prodotto.

Visualizzazione delle informazioni sul repository

Per visualizzare informazioni sugli oggetti del repository, selezionare un oggetto nell'albero gerarchico dei contenuti del repository. Si apre il pannello delle proprietà con le seguenti informazioni:

- Nella sottosezione **Oggetti selezionati** vengono riportate informazioni dettagliate sull'oggetto selezionato nell'albero dei contenuti del repository: **Tipo**, **Dimensione** (solo per file separati), **Data di creazione** e **Data di modifica**.
- Nella sottosezione **Stato del repository** vengono riportate informazioni generali su tutti gli oggetti del repository: la lista corrente degli oggetti e la data del loro ultimo aggiornamento.

Gestione del repository

Per gestire i contenuti del repository, utilizzare i seguenti pulsanti nella barra degli strumenti:

Esporta i file del repository in archivio,

Importa archivio con i file del repository,

Rimuovi gli oggetti selezionati – per rimuovere gli oggetti selezionati nell'albero dei contenuti del repository, senza la possibilità di recupero.

Dopo aver modificato i contenuti del repository, per esempio dopo aver rimosso o importato oggetti del repository, affinché il Server possa utilizzare i dati modificati, è necessario riavviare il repository.

V. sezione Stato del repository.

Esportazione del repository

Per salvare i file del repository in un archivio .zip, eseguire le seguenti azioni:

1. Nell'albero gerarchico dei contenuti di repository, selezionare un prodotto, una revisione separata di un prodotto o l'intero repository. L'intero repository verrà esportato se nulla è selezionato nell'albero oppure è selezionata l'intestazione dell'albero – **Repository**. Per selezionare diversi oggetti, utilizzare il tasti della tastiera CTRL o MAIUSCOLO.

   Quando si esegue l'esportazione di oggetti del repository, prestare attenzione ai tipi principali di oggetto da esportare:

   a) Archivi Zip dei prodotti del repository. Tali archivi contengono uno dei seguenti tipi di oggetto del repository:
      - L'intero repository.
      - L'intero prodotto.
      - L'intera revisione separata di un prodotto.

   Gli archivi in cui vengono esportati questi oggetti possono essere importati tramite la sezione **Contenuti del repository**. Il nome di tali archivi include il prefisso `repository_`.

   b) Archivi Zip di file separati del repository.

   Gli archivi in cui vengono esportati file e directory separate che si trovano nell'albero gerarchico più in basso degli oggetti dal p. **a)**, non possono essere importati tramite la sezione **Contenuti del repository**. Il nome di tali archivi include il prefisso `files_`.

   Si possono utilizzare tali archivi come backup di file per la sostituzione manuale. Tuttavia, non è consigliato sostituire file del repository manualmente, non utilizzando la sezione **Contenuti del repository**.
2. Premere il pulsante **Esporta i file del repository in archivio** nella barra degli strumenti.
3. Il percorso per il salvataggio dell'archivio .zip con l'oggetto selezionato nel repository viene impostato in conformità alle impostazioni del browser web in cui è aperto il Pannello di controllo.

Importazione del repository

Per caricare i file del repository da un archivio .zip, eseguire le seguenti azioni:

1. Premere il pulsante **Importa archivio con i file del repository** nella barra degli strumenti.

2. Nella finestra che si è aperta nella sezione **Selezionare un file** selezionare un archivio .zip con i file del repository. Per selezionare file, si può utilizzare il pulsante  .

   Possono essere importati soltanto gli archivi .zip in cui è stato esportato uno dei seguenti tipi di oggetti del repository:

   - L'intero repository.
   - L'intero prodotto.
   - L'intera revisione separata di un prodotto.

   I nomi di tali archivi ad esportazione includono il prefisso `repository_`.
3. Nella sezione **Parametri dell`importazione**, impostare i seguenti parametri:
   - **Aggiungi soltanto le revisioni mancanti** – in questa modalità di importazione vengono aggiunte soltanto le revisioni di repository che sono assenti nella versione corrente. Le altre revisioni rimangono invariate.
   - **Sostituisci l'intero repository** – in questa modalità di importazione il repository viene sostituito per intero con quello importato.
   - Spuntare il flag **Importa i file di configurazione** per importare i file di configurazione insieme all'importazione del repository.
4. Premere il pulsante **Importa** per iniziare il processo di importazione.

8.9. Possibilità addizionali

8.9.1. Gestione del database

La sezione **Gestione del database** consente di mantenere il database con cui interagisce il Server Dr.Web.

La sezione **Generali** contiene i seguenti parametri:

- Il campo **Ultima manutenzione del database** – la data dell'ultima esecuzione dei comandi di manutenzione di database da questa sezione.
- Una lista dei comandi per la manutenzione del database, che include:
  - Comandi analoghi ai task dal calendario di Server Dr.Web. I nomi dei comandi corrispondono ai nomi dei task dalla sezione **Azioni** nel calendario di Server (i task corrispondenti del calendario vengono descritti nella tabella Tipi di task e i loro parametri).
  - Il comando **Analisi della base di dati**. È studiato per ottimizzare il database di Server attraverso l'esecuzione del comando `analyze`.

Per eseguire i comandi di manutenzione di database:

1. Nella lista dei comandi spuntare i flag per i comandi che si desidera eseguire.

   Se necessario, modificare i periodi di tempo per i comandi di pulizia di database, trascorsi i quali le informazioni conservate vengono ritenute obsolete e devono essere rimosse dal Server.

2. Premere il pulsante **Applica adesso**. Tutti i comandi selezionati verranno eseguiti immediatamente.

   Per un'esecuzione differita e/o periodica automatica di questi comandi (eccetto il comando **Analisi della base di dati**) utilizzare lo Scheduler del Server.

Per gestire il database, utilizzare i seguenti pulsanti nella barra degli strumenti:

 Importazione,

 Esportazione,

 Copiatura di backup.

Esportazione del database

Per salvare le informazioni dal database in un file, eseguire le seguenti azioni:

1. Premere il pulsante  **Esportazione** nella barra degli strumenti.
2. Nella finestra di configurazione dell'esportazione selezionare una delle opzioni:
   - **Esporta l'intero database** per salvare tutte le informazioni dal database in un archivio gz. Il file XML, ottenuto durante l'esportazione, è analogo al file di esportazione di database che viene ottenuto quando si avvia il file eseguibile di Server dalla riga di comando con l'opzione `xmlexportdb`. Questo file di esportazione può essere importato quando si avvia il file eseguibile di Server dalla riga di comando con l'opzione `xmlimportdb`.
     Una descrizione dettagliata di questi comandi è riportata nel documento **Allegati**, nella sezione H4.3. Comandi di gestione del database.
   - **Esporta le informazioni circa le postazioni e i gruppi** per salvare le informazioni su oggetti della rete antivirus in un archivio zip. Come risultato dell'esecuzione di quest'operazione, in un file di un apposito formato vengono salvate tutte le informazioni sui gruppi di postazioni e sugli account di postazioni della rete antivirus servita da questo Server. Il file di esportazione include le seguenti informazioni su postazioni: proprietà, configurazione dei componenti, permessi, impostazioni delle limitazioni di aggiornamenti, calendario, lista dei componenti da installare, statistiche, informazioni su postazioni rimosse; su gruppi: proprietà, configurazione dei componenti, permessi, impostazioni delle limitazioni di aggiornamenti, calendario, lista dei componenti da installare, identificatore del gruppo padre.
     In seguito il file di esportazione può essere importato attraverso la sezione **Gestione del database**.
3. Premere il pulsante **Esporta**.
4. Il percorso per il salvataggio dell'archivio con il database viene impostato in conformità con le impostazioni del browser web in cui è aperto il Pannello di controllo.

Importazione del database

L'importazione del file di database con le informazioni su oggetti della rete antivirus può essere utilizzata per trasferire le informazioni sia su un Server nuovo che su un Server che già funziona nella rete antivirus, in particolare per unire le liste delle postazioni servite da due Server.

Al Server su cui viene fatta l'importazione potranno connettersi tutte le postazioni, le informazioni su cui vengono importate. Quando si fa l'importazione, prestare attenzione che sul server deve esserci il numero corrispondente di licenze disponibili per connettere le postazioni trasferite. Per esempio, se necessario, nella sezione Gestione licenze aggiungere una chiave di licenza dal Server da cui sono state trasferite le informazioni circa le postazioni.

Per caricare il database da file, eseguire le seguenti azioni:

1. Premere il pulsante **Importazione** nella barra degli strumenti.
2. Nella finestra di importazione impostare un archivio zip con il file di database. Per selezionare file, si può utilizzare il pulsante .

   Possono essere importati soltanto gli archivi .zip che sono stati ottenuti attraverso l'esportazione di database per la variante **Esporta le informazioni circa le postazioni e i gruppi**.
3. Premere il pulsante **Importa** per iniziare il processo di importazione.
4. Se durante l'importazione vengono scoperte postazioni e/o gruppi con identificatori uguali che fanno parte sia delle informazioni importate che del database del Server corrente, si apre la sezione **Collisioni** per impostare le azioni con gli oggetti duplicati.

   Le liste dei gruppi e delle postazioni vengono riportate in tabelle separate.

   Per la rispettiva tabella di oggetti dalla lista a cascata **Modalità di importazione dei gruppi** o **Modalità di importazione delle postazioni** selezionare una variante per risolvere la collisione:

   - **Mantieni i dati dell'importazione per tutti** – per cancellare tutte le informazioni sugli oggetti duplicati dal database del Server corrente e sovrascriverle con le informazioni dal database che viene importato. L'azione viene applicata contemporaneamente a tutti gli oggetti duplicati in questa tabella.
   - **Mantieni i dati correnti per tutti** – per mantenere tutte le informazioni sugli oggetti duplicati dal database del Server corrente. Le informazioni dal database che viene importato verranno ignorate. L'azione viene applicata contemporaneamente a tutti gli oggetti duplicati in questa tabella.
   - **Seleziona manualmente** – per impostare manualmente un'azione a ciascun oggetto duplicato separatamente. In questa modalità la lista degli oggetti duplicati sarà disponibile per la modifica. Impostare le opzioni di fronte agli oggetti che verranno mantenuti.

   Premere **Salva**.

Copiatura di backup

Per creare una copia di backup dei dati critici del Server, premere il pulsante **Copiatura di backup** nella barra degli strumenti. I dati verranno salvati in un archivio gz. I file ottenuti come risultato della copiatura di backup sono analoghi ai file ottenuti quando si avvia il file eseguibile di Server dalla riga di comando con l'opzione `backup`.

Questo comando è descritto in più dettagli nel documento **Allegati**, nella sezione H4.5. Backup dei dati critici del Server Dr.Web.

8.9.2. Statistiche di Server Dr.Web

Tramite il Pannello di controllo è possibile visualizzare le statistiche di funzionamento di Server Dr.Web, riguardanti il consumo delle risorse di sistema del computer su cui è installato il Server Dr.Web e l'interazione via rete con i componenti della rete antivirus e con risorse esterne, in particolare con SAM.

Per visualizzare le statistiche di funzionamento di Server Dr.Web:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo.
2. Nella finestra che si è aperta, selezionare la voce del menu di gestione **Statistiche del Server Dr.Web**.
3. Nella finestra che si è aperta sono riportate le seguenti sezioni delle informazioni statistiche:
   - **Attività dei client** – informazioni sul numero di client connessi a questo Server: Agent Dr.Web, Server Dr.Web adiacenti e installer di Agent Dr.Web.
   - **Traffico di rete** – parametri di traffico di rete in entrata e uscita durante lo scambio di dati con il Server.
   - **Utilizzo delle risorse di sistema** – parametri di consumo delle risorse di sistema del computer su cui è installato il Server.
   - **Microsoft NAP** – parametri di funzionamento di Dr.Web NAP Validator.
   - **Utilizzo del database** – parametri di utilizzo del database di Server.
   - **Utilizzo della cache di file** – parametri di utilizzo della cache di file del computer su cui è installato il Server.
   - **Utilizzo della cache DNS** – parametri di utilizzo della cache delle richieste ai server DNS sul computer su cui è installato il Server.
   - **Avvisi** – parametri di funzionamento del sottosistema che invia avvisi all'amministratore.
   - **Repository** – parametri di comunicazione del repository di Server con i server SAM.
   - **Statistiche web** – parametri di utilizzo di Web server.
   - **Cluster** – parametri di comunicazione attraverso il protocollo di sincronizzazione tra server se viene utilizzato un cluster di Server in una configurazione di rete con diversi server.
4. Per visualizzare le statistiche di una sezione, premere il nome della sezione richiesta.
5. Nell'elenco che si è aperto sono riportate i parametri della sezione con contatori dinamici dei valori.
6. Contemporaneamente con l'apertura della sezione statistica, si attiva la rappresentazione grafica delle modifiche per ciascuno dei parametri. In particolare:
   - Per disattivare la rappresentazione grafica, premere il nome della sezione richiesta. Se la rappresentazione grafica viene disattivata, il valore numerico dei parametri continua ad aggiornarsi in maniera dinamica.
   - Per riattivare la rappresentazione grafica dei dati, premere ancora una volta il nome della sezione richiesta.

- I nomi delle sezioni e i rispettivi parametri, per cui è attivata la rappresentazione grafica, sono evidenziati in grassetto.

7. Per modificare la frequenza dell'aggiornamento dei parametri, servirsi dei seguenti strumenti nella barra di gestione:
   - Dalla lista a cascata **Frequenza dell'aggiornamento** selezionare il periodo richiesto di aggiornamento di dati. Quando cambia il valore dalla lista a cascata, viene applicato automaticamente il periodo di aggiornamento dei dati numerici e grafici.
   - Premere il pulsante **Aggiorna** per aggiornare una volta tutti i valori delle informazioni statistiche nello stesso tempo.
8. Quando il puntatore del mouse passa sopra i dati grafici, viene visualizzato il valore numerico del punto selezionato nella forma:
   - **Abs** – valore assoluto del parametro.
   - **Delta** – aumento del valore del parametro rispetto al valore precedente secondo la frequenza di aggiornamento di dati.
9. Per nascondere i parametri della sezione, premere la freccia a sinistra del nome della sezione. Quando i parametri della sezione vengono nascosti, la rappresentazione grafica viene cancellata, e quando i parametri vengono riaperti, il rendering inizia di nuovo.

8.10. Caratteristiche di una rete con diversi Server Dr.Web

Dr.Web Enterprise Security Suite consente di creare una rete antivirus che includa diversi Server Dr.Web. In questo caso, ciascuna postazione viene registrata su un determinato Server e questo consente di distribuire il carico tra i server.

Le relazioni tra i Server possono avere una struttura gerarchica e questo consente di distribuire in modo ottimale il carico sui Server.

Per lo scambio di informazioni tra i Server viene utilizzato un apposito *protocollo di sincronizzazione interserver*.

Possibilità fornite dal protocollo di sincronizzazione interserver:

- Distribuzione degli aggiornamenti tra i Server all'interno della rete antivirus.
- Trasferimento veloce degli aggiornamenti ricevuti dai server SAM Dr.Web.
- Tra i Server associati vengono trasferite le informazioni sullo stato di postazioni protette.
- Trasferimento delle licenze per postazioni protette tra i Server adiacenti.

8.10.1. Struttura di una rete con diversi Server Dr.Web

In una rete antivirus è possibile installare diversi Server Dr.Web. In questo caso ogni Agent Dr.Web si connette a uno dei Server. Ogni Server insieme alle postazioni antivirus connesse funziona come una rete antivirus separata, come descritto nelle sezioni precedenti.

Dr.Web Enterprise Security Suite permette di connettere tali reti antivirus, organizzando la trasmissione di informazioni tra i Server Dr.Web.

Un Server Dr.Web può trasmettere su un altro Server Dr.Web:

- aggiornamenti del software e dei database dei virus. In questo caso solo uno di essi riceve gli aggiornamenti da SAM Dr.Web;
- informazioni su eventi dei virus, statistiche di operazione ecc.;
- licenze per postazioni protette (il trasferimento di licenza tra i Server viene configurato in Gestione licenze).

Dr.Web Enterprise Security Suite distingue due tipi di relazione tra i Server Dr.Web:

- *relazione del tipo principale-subordinato*, in cui il server principale trasmette a quello subordinato gli aggiornamenti e riceve da esso le informazioni su eventi,
- *relazione tra server paritari*, in cui le direzioni di trasmissione di informazioni e i tipi di informazione vengono configurati in maniera personalizzata.

In immagine 8-1 è rappresentata un esempio della struttura della rete con diversi Server.

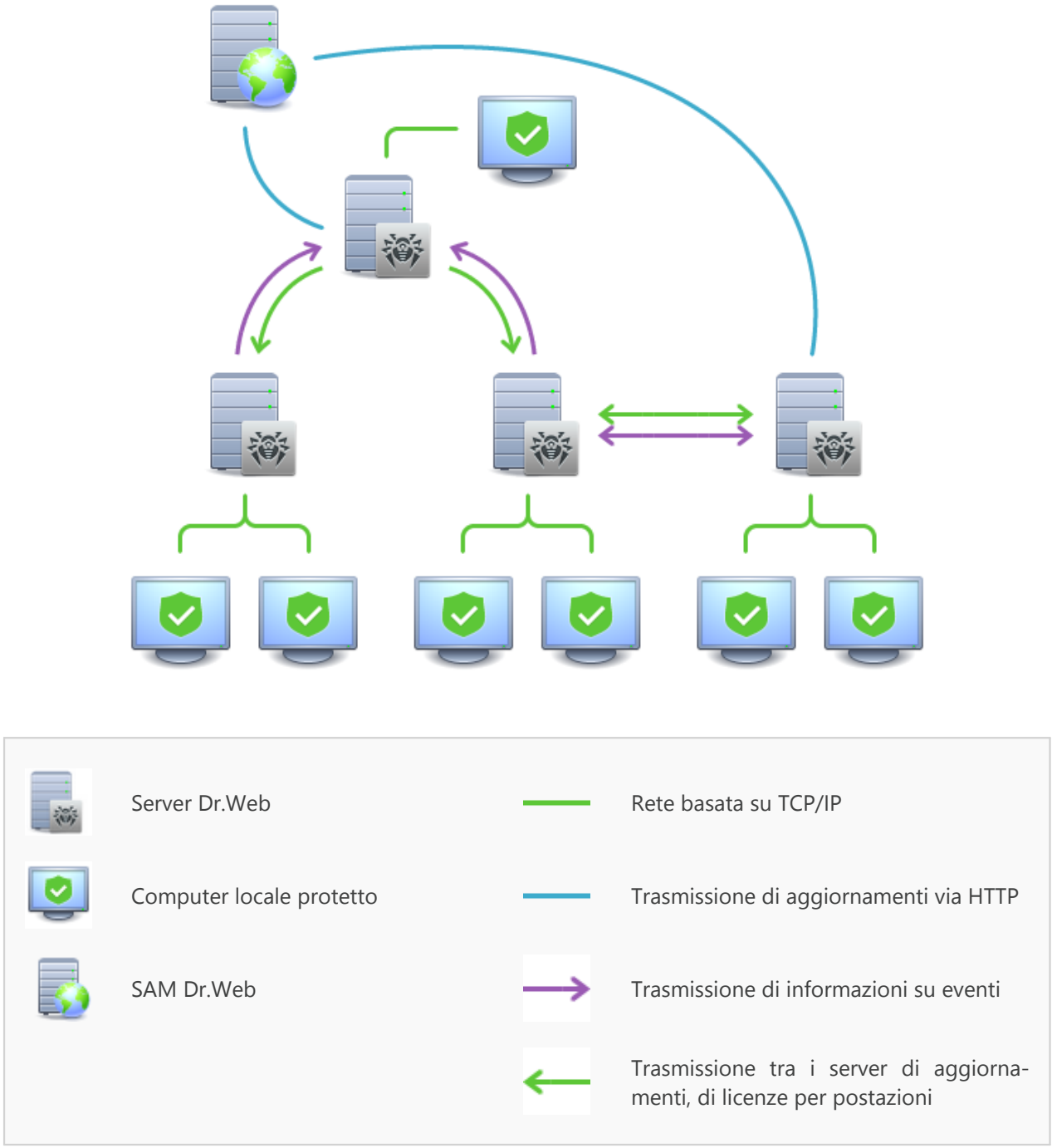


Immagine 8-1. Rete con diversi Server

Alcuni vantaggi di una rete antivirus con diversi Server Dr.Web:

1. Possibilità di ricevere aggiornamenti dai server SAM Dr.Web attraverso un Server Dr.Web con la successiva trasmissione sugli altri Server direttamente attraverso intermediari.

   I Server che ricevono aggiornamenti da un Server principale non ricevono aggiornamenti da SAM, anche se tale task è disponibile nel loro calendario.

Tuttavia, per il caso in cui il Server principale sia temporaneamente non disponibile, si consiglia di lasciare nel calendario del Server subordinato il task di aggiornamento dai server SAM. Questo permetterà agli Agent connessi al Server subordinato di ottenere gli aggiornamenti dei database dei virus e dei moduli di programma (v. anche Configurazione generale del repository).

Nel task di aggiornamento da SAM sul Server principale che distribuisce gli aggiornamenti, è necessario configurare la ricezione degli aggiornamenti del software server per tutti i sistemi operativi installati su tutti i Server subordinati che ricevono gli aggiornamenti da questo Server principale (v. p. Configurazione generale del repository).

2. Possibilità di distribuire le postazioni tra diversi Server diminuendo il carico su ognuno di essi.
3. Unione delle informazioni da diversi Server su uno di essi; possibilità di ottenere le informazioni in forma consolidata in una sessione del Pannello di controllo su questo Server.

Dr.Web Enterprise Security Suite traccia e blocca autonomamente percorsi ciclici di trasmissione delle informazioni.

4. Possibilità di trasferire licenze libere per postazioni su un Server adiacente. In questo caso, la chiave di licenza stessa rimane a disposizione del Server che la distribuisce, le licenze libere vengono rilasciate al Server adiacente per un determinato periodo di tempo, scaduto il quale vengono prese indietro.

8.10.2. Configurazione delle relazioni tra i Server Dr.Web

Per avvalersi le possibilità di utilizzo di diversi Server, si deve configurare le relazioni tra di essi.

Si consiglia di progettare prima la struttura della rete antivirus, contrassegnando tutti i flussi d'informazione attesi e prendendo la decisione quali relazioni saranno "tra i paritari" e quali saranno del tipo "principale-subordinato". Dopo questo per ogni Server che fa parte della rete antivirus occorre configurare le relazioni con i Server adiacenti (i Server adiacenti sono collegati da almeno un flusso d'informazione).

Un esempio della configurazione della comunicazione dei Server Dr.Web principale e subordinato:

I valori dei campi marcati con il carattere * devono essere impostati obbligatoriamente.

1. Assicurarsi che tutti e due Server Dr.Web operano correttamente.
2. A ciascuno dei Server Dr.Web dare un nome "parlante" per non sbagliare quando si configura la connessione tra i Server Dr.Web e quando successivamente si gestiscono i server. Si può farlo nel menu del Pannello di controllo **Amministrazione** → **Configurazione del Server Dr.Web** nella scheda **Generali** nel campo **Nome**. In quest'esempio chiamiamo il Server principale `MAIN` e quello subordinato – `AUXILIARY`.

3. Su entrambi i Server Dr.Web abilitare il protocollo server. Per farlo, nel menu del Pannello di controllo **Amministrazione** → **Configurazione del Server Dr.Web** nella scheda **Moduli** spuntare il flag **Protocollo di Server Dr.Web** (v. p. Moduli).

   Se il protocollo server non è attivo, quando viene creata una nuova relazione nel Pannello di controllo viene visualizzato un avviso di necessità di attivazione di tale protocollo e viene indicato il link alla sezione corrispondente del Pannello di controllo.

4. Riavviare entrambi i Server Dr.Web.
5. Tramite il Pannello di controllo del Server subordinato (`AUXILIARY`) aggiungere il Server principale (`MAIN`) all'elenco dei Server adiacenti. Per farlo, selezionare la voce **Relazioni** dal menu principale. Si apre una finestra che contiene la lista gerarchica dei Server della rete antivirus che sono adiacenti a questo Server. Per aggiungere un Server a questa lista, premere il pulsante **Crea relazione** nella barra degli strumenti.

   Si apre una finestra di descrizione delle relazioni tra il Server attuale e quello che viene aggiunto. Impostare i seguenti parametri:

   - **Tipo** di relazione – **Principale**.
   - **Nome** – nome del Server principale (`MAIN`).
   - **Password*** – password di accesso al Server principale.
   - **Proprie chiavi del Server Dr.Web** – lista delle chiavi di cifratura pubbliche del Server che viene configurato. Premere il pulsante e selezionare la chiave `drwcsd.pub` che corrisponde al Server attuale. Per aggiungere un'altra chiave, premere e aggiungere una chiave nel nuovo campo.
   - **Chiavi del Server Dr.Web adiacente*** – lista delle chiavi di cifratura pubbliche del Server principale che viene collegato. Premere il pulsante e selezionare la chiave `drwcsd.pub` che corrisponde al Server principale. Per aggiungere un'altra chiave, premere e aggiungere una chiave nel nuovo campo.
   - **Indirizzo*** – indirizzo di rete del Server principale e la porta per la connessione. Viene impostato nel formato <*indirizzo_di_Server*>**:**<*porta*>.

   Si può cercare la lista dei Server disponibili in rete. Per farlo:

   a) Premere la freccia a destra del campo **Indirizzo**.
   b) Nella finestra che si è aperta, indicare la lista delle reti nel formato: separate da trattino (per esempio, `10.4.0.1-10.4.0.10`), separate da virgola e spazio (per esempio, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`), utilizzando il prefisso di rete (per esempio, `10.4.0.0/24`).
   c) Premere il pulsante . Inizia una ricerca nella rete dei Server disponibili.
   d) Selezionare un Server nella lista dei Server disponibili. Il suo indirizzo verrà scritto nel campo **Indirizzo** per la creazione di una relazione.

   - **Indirizzo del Pannello di controllo della sicurezza Dr.Web** – si può indicare l'indirizzo della pagina iniziale del Pannello di controllo del Server principale (v. p. Pannello di controllo della sicurezza Dr.Web).

- Nella lista a cascata **Parametri della connessione** viene impostato il principio di connessione dei Server della relazione che viene creata.
- Nelle liste a cascata **Crittografia** e **Compressione** impostare i parametri di cifratura e di compressione di traffico dati tra i Server che vengono collegati (v. p. Utilizzo di cifratura e di compressione di traffico).
- **Periodo di validità delle licenze rilasciate** – periodo per cui vengono rilasciate le licenze dalla chiave sul Server principale. L'impostazione viene utilizzata se il Server principale rilascerà licenze al Server attuale.
- **Periodo per il rinnovo delle licenze ricevute** – l'impostazione non viene utilizzata se viene creata una relazione a Server principale.
- **Periodo di sincronizzazione delle licenze** – la periodicità della sincronizzazione delle informazioni su licenze rilasciate tra i Server.
- I flag nelle sezioni **Licenze**, **Aggiornamenti** e **Eventi** sono spuntati in conformità alla relazione *principale-subordinato* e non possono essere modificati:
  - il Server principale invia licenze sul Server subordinato;
  - il Server principale invia aggiornamenti sul Server subordinato;
  - il Server principale accetta informazioni su eventi dal Server subordinato.
- Nella sezione **Limitazioni degli aggiornamenti** → **Eventi** è possibile impostare un calendario di trasmissione di eventi dal Server attuale su quello principale (la tabella **Limitazioni degli aggiornamenti** viene modificata in modo simile alla modifica della tabella nella sezione Limitazione degli aggiornamenti delle postazioni).

Premere il pulsante **Salva**.

Come risultato, il Server principale (`MAIN`) viene incluso nelle cartelle **Principali** e **Offline** (v. immagine 8-2).

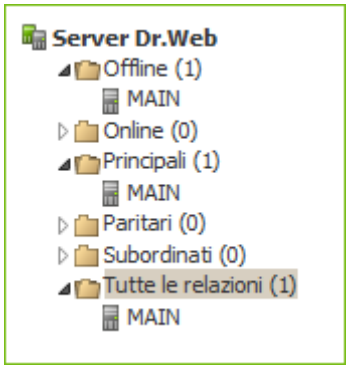


Immagine 8-2.

6. Aprire il Pannello di controllo del Serverprincipale (`MAIN`) e aggiungere il Server subordinato (`AUXILIARY`) all'elenco dei Server adiacenti. Per farlo, selezionare la voce **Relazioni** dal menu principale. Si apre una finestra che contiene la lista gerarchica dei Server della rete antivirus che sono adiacenti a questo. Per aggiungere un Server a questa lista, premere il pulsante **Crea relazione** nella barra degli strumenti.

   Si apre una finestra di descrizione delle relazioni tra il Server attuale e quello che viene aggiunto. Impostare i seguenti parametri:

- **Tipo** di relazione – **Subordinato**.
- **Nome** – nome del Server subordinato (`AUXILIARY`).
- **Password*** – inserire la stessa password che è stata indicata nella voce **5**.
- **Proprie chiavi del Server Dr.Web** – lista delle chiavi di cifratura pubbliche del Server che viene configurato. Premere il pulsante e selezionare la chiave `drwcsd.pub` che corrisponde al Server attuale. Per aggiungere un'altra chiave, premere e aggiungere una chiave nel nuovo campo.
- **Chiavi del Server Dr.Web adiacente*** – lista delle chiavi di cifratura pubbliche del Server subordinato che viene collegato. Premere il pulsante e selezionare la chiave `drwcsd.pub` che corrisponde al Server subordinato. Per aggiungere un'altra chiave, premere e aggiungere una chiave nel nuovo campo.
- **Indirizzo del Pannello di controllo della sicurezza Dr.Web** – si può indicare l'indirizzo della pagina iniziale del Pannello di controllo del Server subordinato (v. p. Pannello di controllo della sicurezza Dr.Web).
- Nella lista a cascata **Parametri della connessione** viene impostato il principio di connessione dei Server della relazione che viene creata.
- Nelle liste a cascata **Crittografia** e **Compressione** impostare i parametri di cifratura e di compressione di traffico dati tra i Server che vengono collegati (v. p. Utilizzo di cifratura e di compressione di traffico).
- **Periodo di validità delle licenze rilasciate** – l'impostazione non viene utilizzata se viene creata una relazione a Server subordinato.
- **Periodo per il rinnovo delle licenze ricevute** – periodo fino alla scadenza di una licenza, a partire da cui il Server subordinato richiede il rinnovo della licenza ricevuta dal Server attuale. L'impostazione viene utilizzata se il Server subordinato riceverà licenze dal Server attuale.
- **Periodo di sincronizzazione delle licenze** – la periodicità della sincronizzazione delle informazioni su licenze rilasciate tra i Server.
- I flag nelle sezioni **Licenze**, **Aggiornamenti** e **Eventi** sono spuntati in conformità alla relazione *principale-subordinato* e non possono essere modificati:
  - il Server subordinato riceve licenze dal Server principale;
  - il Server subordinato riceve aggiornamenti dal Server principale;
  - il Server subordinato invia informazioni su eventi sul Server principale.
- Nella sezione **Limitazioni degli aggiornamenti** → **Aggiornamenti** è possibile impostare un calendario di trasmissione di aggiornamenti dal Server attuale su quello subordinato (la tabella **Limitazioni degli aggiornamenti** viene modificata in modo simile alla modifica della tabella nella sezione Limitazione degli aggiornamenti delle postazioni).

Premere il pulsante **Salva**.

Come risultato, il Server subordinato (`AUXILIARY`) viene incluso nelle cartelle **Subordinati** e **Offline** (v. immagine 8-3).

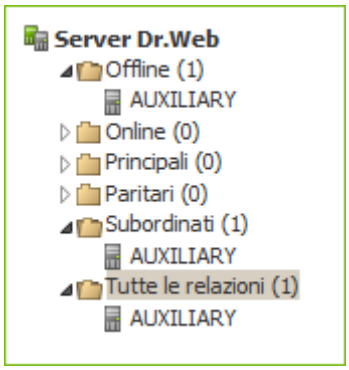


Immagine 8-3.

7. Attendere che viene stabilita una connessione tra i Server (di solito ci vuole meno di un minuto). Per il controllo, aggiornare periodicamente la lista dei Server tramite il tasto F5. Dopo che è stata stabilita la connessione, il Server subordinato (`AUXILIARY`) viene trasferito dalla cartella **Offline** nella cartella **Online** (v. immagine 8-4).

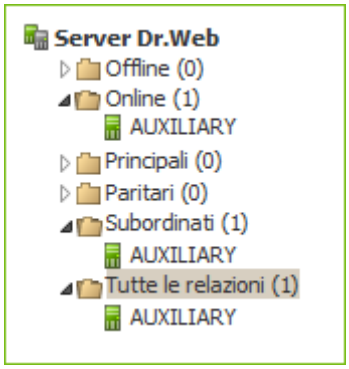


Immagine 8-4.

8. Aprire il Pannello di controllo del Server subordinato (`AUXILIARY`) e assicurarsi che il Server principale (`MAIN`) sia connesso a quello subordinato (`AUXILIARY`) (v. immagine 8-5).

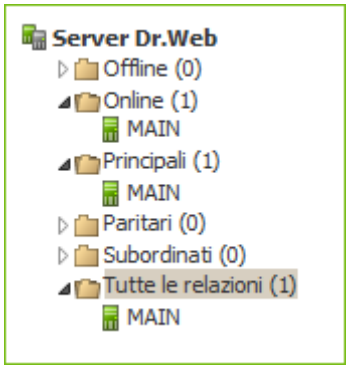


Immagine 8-5.

Non è possibile creare una relazione tra diversi Server con la stessa copia dei parametri: password e chiave di cifratura pubblica `drwcsd.pub`.

Quando viene creata una relazione paritaria tra Server, si consiglia di indicare l'indirizzo del Server che viene connesso soltanto nelle impostazioni di uno di essi.

Questo non influisce su interazione tra i Server, però permette di evitare record del tipo **Link with the same key id is already activated** nel log di funzionamento dei Server.

Non è possibile stabilire una connessione tra i Server Dr.Web nei seguenti casi:

- Problemi di connessioni di rete.
- Quando veniva configurata la relazione, è stato impostato un indirizzo sbagliato del Server principale.
- Sono state impostate chiavi di cifratura pubbliche `drwcsd.pub` non valide su uno dei Server.
- È stata impostata una password di accesso non valida su uno dei Server (sono state impostate le password che non coincidono sui Server che vengono collegati).

8.10.3. Utilizzo di una rete antivirus con diversi Server Dr.Web

Una caratteristica della rete con diversi Server è che dai server SAM Dr.Web gli aggiornamenti vengono ricevuti attraverso una parte dei Server Dr.Web (di regola, da uno o più Server principali). In questo caso solo su questi Server si deve impostare un calendario con il task di aggiornamento (v. p. Configurazione del calendario di Server Dr.Web). Qualsiasi Server che abbia ottenuto gli aggiornamenti dai server SAM Dr.Web oppure da un altro Server li trasmette immediatamente su tutti i Server per cui tale possibilità è configurata su questo server (cioè su tutti i server subordinati e anche su quelli dei server paritari per cui la possibilità di ricezione di aggiornamenti è impostata in modo esplicito).

Dr.Web Enterprise Security Suite traccia automaticamente le situazioni quando, per l'incorretta programmazione della topologia della rete e per l'incorretta configurazione dei Server, un aggiornamento, già ottenuto da un'altra fonte, arriva di nuovo sullo stesso Server, e tale aggiornamento ripetuto non viene eseguito.

L'amministratore può inoltre ottenere le informazioni consuntive sugli eventi di virus più importanti nei segmenti della rete connessi a qualche Server, attraverso le relazioni tra i server (per esempio, nella configurazione descritta sopra "un server principale, altri server subordinati" queste informazioni vengono consolidate sul Server principale).

Per visualizzare le informazioni su eventi di virus su tutti i Server Dr.Web associati a questo Server:

1. Selezionare la voce **Relazioni** del menu principale del Pannello di controllo.
2. Nella finestra che si è aperta nella sezione **Tabelle** del menu di gestione, selezionare la voce **Report di riepilogo** per visualizzare le informazioni sul totale record di eventi sui Server adiacenti. Nella tabella con le statistiche dei Server adiacenti vengono visualizzate le informazioni nelle seguenti sezioni:
   - **Infezioni** – infezioni rilevate sulle postazioni connesse ai Server adiacenti.
   - **Errori** – errori di scansione.
   - **Statistiche** – statistiche delle infezioni rilevate.

- **Avvio/arresto** – avvio e completamento dei task di scansione di postazioni.
- **Stato** – stato del software antivirus su postazioni.
- **Tutte le installazioni di rete** – installazioni di rete di Agent.

3. Per passare alla pagina con la tabella delle informazioni dettagliate su eventi sui Server adiacenti, nella tabella della sezione **Report di riepilogo** premere la cifra del numero di record relativi all'evento richiesto.
4. Inoltre, per passare alla tabella delle informazioni su eventi dei Server adiacenti, selezionare la voce corrispondente (v. passo 2) della sezione **Tabelle** del menu di gestione.
5. Per visualizzare le informazioni per un determinato periodo, indicare un periodo relativamente al giorno odierno nella lista a cascata o impostare un intervallo di tempo nella barra degli strumenti. Per impostare un intervallo di tempo, inserire le date richieste o premere le icone del calendario accanto ai campi di date.Per visualizzare le informazioni, premere il pulsante **Aggiorna**.
6. Se occorre salvare la tabella in modo da stamparla o da elaborarla in seguito, premere nella barra degli strumenti

   Registra le informazioni in file CSV,

   Registra le informazioni in file HTML,

   Registra le informazioni in file XML,

   Registra le informazioni in file PDF.

8.10.4. Cluster dei Server Dr.Web

Conviene aggiornare i Server all'interno di un cluster soltanto da pacchetti d'installazione. In questo caso, occorre arrestare tutti i Server e aggiornarli uno dopo l'altro. Non si deve utilizzare l'aggiornamento tramite il Pannello di controllo (passaggio ad una nuova revisione), in quanto in caso di utilizzo di database comune dopo l'aggiornamento del primo Server tutti gli altri Server non potranno continuare a funzionare e ad aggiornarsi.

Se nella rete antivirus viene creato un cluster di Server Dr.Web, è necessario soddisfare i seguenti requisiti:

1. **File di configurazione uguali**

   Su tutti i Server devono esserci le stesse chiavi di cifratura `drwcsd.pub` e `drwcsd.pri`.

   Se le chiavi di cifratura non erano create precedentemente, allora durante l'installazione del primo Server del cluster le chiavi di cifratura verranno generate automaticamente.

   Le chiavi di cifratura per l'installazione dei successivi Server del cluster possono essere ottenute attraverso il Pannello di controllo: menu **Amministrazione** → **Chiavi di crittografia**. A seconda di quello come il cluster viene installato successivamente, potrebbero essere necessarie entrambe le chiavi o soltanto `drwcsd.pri`:

   - Se la chiave privata `drwcsd.pri` viene impostata durante l'installazione del Server, la chiave pubblica `drwcsd.pub` viene generata automaticamente.

- Se la chiave privata desiderata non viene impostata durante l'installazione di Server, dopo l'installazione è necessario sostituire entrambe le chiavi manualmente.

Il percorso dei file di configurazione è riportato nella sezione Server Dr.Web.

2. **Lo stesso nome del Server**

   Per tutti i Server devono essere impostati gli stessi indirizzo IP o nome DNS di Server utilizzati nella generazione dei file di installazione di Agent per le postazioni della rete antivirus.

   Questo nome viene impostato attraverso il Pannello di controllo: **Amministrazione** → **Configurazione del Server Dr.Web** → scheda **Rete** → scheda Download → il campo **Indirizzo di Server Dr.Web**. Le impostazioni di questa sezione vengono conservate nel file di configurazione `download.conf` (il file viene descritto nel documento **Allegati**, p. G3. File di configurazione download.conf).

3. **Configurazione dell'uso del cluster**

   Sul server DNS in rete è necessario registrare il nome comune di cluster per ogni singolo Server e impostare il metodo di bilanciamento del carico.

   Affinché le impostazioni vengano applicate in modo automatico nel cluster di Server Dr.Web, è necessario utilizzare un apposito protocollo di cluster.

   Per configurare il protocollo di cluster, è necessario per ciascuno dei Server nel Pannello di controllo passare al menu **Amministrazione** → **Configurazione del Server Dr.Web** e configurare le seguenti impostazioni:

   a) Per attivare il protocollo di cluster, nella scheda Moduli spuntare il flag **Protocollo di cluster dei Server Dr.Web**.

   b) Per configurare i parametri di interazione dei Server inclusi nel cluster, nella scheda Cluster configurare le impostazioni relative.

   c) Dopo aver configurato tutti i parametri necessari, premere **Salva** e riavviare i Server.

   Per esempio:

   - Gruppo Multicast: `232.0.0.1`
   - Porta: `11111`
   - Interfaccia: `0.0.0.0`

   In questo esempio per tutti i Server del cluster vengono configurati i trasporti per tutte le interfacce. In altri casi, per esempio quando una delle reti è esterna per il cluster e gli Agent si connettono attraverso di essa e la seconda rete è una all'interno del cluster, è preferibile aprire il protocollo di cluster soltanto per le interfacce della rete interna. In questo caso come le interfacce è necessario impostare gli indirizzi del tipo `192.168.1.1`, ..., `192.168.1.N`.

4. Database unico

Per poter utilizzare un database unico, tutti i Server Dr.Web devono essere della stessa versione.

Tutti i Server Dr.Web all'interno di un cluster devono utilizzare lo stesso database esterno.

Come nel caso di utilizzo di database senza l'organizzazione di un cluster, ciascuno dei Server si connette al database in un modo indipendente, e tutti i dati dei Server vengono conservati separatamente. Ovunque dov'è applicabile, il Server prende dal database soltanto i record associati al suo ID il quale è unico per ciascun Server. L'utilizzo dello stesso database consente ai Server di interagire con gli Agent che inizialmente sono stati registrati sugli altri Server del cluster.

Quando viene creato un cluster dei Server con un unico database, è necessario tenere presente le seguenti caratteristiche:

- Il database può essere installato sia separatamente da tutti i Server che su uno dei computer su cui è installato un Server del cluster.
- Il database deve essere creato prima dell'installazione del primo Server del cluster o prima del momento della connessione del primo Server al database.
- Nel corso dell'aggiunzione di nuovi nodi al cluster (ad eccezione del primo Server), durante l'installazione dei Server non è consigliabile impostare subito il database unico che viene utilizzato in questo cluster. Altrimenti questo potrebbe provocare l'eliminazione delle informazioni già memorizzate nel database. È consigliabile installare inizialmente i Server con il database interno e dopo l'installazione connetterli con il database esterno unico.
  È possibile riconfigurare i Server all'utilizzo del database esterno attraverso il Pannello di controllo: nel menu **Amministrazione** → **Configurazione del Server Dr.Web** → nella scheda Database o attraverso il file di configurazione dei Server `drwcsd.conf`.
- Ad eccezione del primo Server del cluster, non è consigliabile introdurre nel cluster i Server che già sono operativi nella rete antivirus utilizzando un altro database esterno o quello interno. Questo provocherà una perdita dei dati: le informazioni sulle postazioni, statistiche, impostazioni (salvo le impostazioni conservate nei file di configurazione) in quanto i dati nel database vengono eliminati completamente durante l'importazione. In questo caso è possibile soltanto un'importazione parziale di alcune informazioni.

5. Una versione del repository

Su tutti i Server del cluster i repository devono contenere gli aggiornamenti della stessa versione.

È possibile soddisfare questo requisito in uno dei seguenti modi:

- Aggiornare simultaneamente tutti i Server del cluster da SAM. In questo caso tutti i Server avranno la versione più recente degli aggiornamenti. Inoltre è possibile configurare l'aggiornamento dei repository di tutti i Server dalla zona locale degli aggiornamenti da cui verrà distribuita la stessa versione confermata degli aggiornamenti dei prodotti o quella più recente in caso della creazione di un mirror di SAM.

- È possibile creare una struttura ibrida che combina sia un cluster di Server che una struttura gerarchica basata sulle relazioni tra server. In tale caso uno dei Server (potrebbe essere un Server del cluster o uno che non fa parte del cluster) viene nominato principale e riceve gli aggiornamenti da SAM. Gli altri Server del cluster – quelli subordinati – ricevono gli aggiornamenti dal Server principale attraverso la comunicazione tra server.

Se viene configurato che i Server del cluster ricevano gli aggiornamenti dalla zona locale (mirror di SAM) o dal Server principale, è necessario monitorare l'operatività di questa zona o del Server principale. Se il nodo che distribuisce gli aggiornamenti fallisce, è necessario riconfigurare uno degli altri Server al ruolo del Server principale o rispettivamente creare una nuova zona degli aggiornamenti per la ricezione degli aggiornamenti da SAM.

6. Le caratteristiche della distribuzione delle licenze per postazioni

Per distribuire licenze tra i Server del cluster, è possibile utilizzare i seguenti approcci:

a) Creare una struttura ibrida che combina sia un cluster dei Server che una struttura gerarchica basata sulle relazioni tra i server. Tale struttura sarà utile se per l'interazione con gli Agent all'interno di un sistema a cluster dei Server viene utilizzata l'allocazione dinamica delle postazioni tra i Server del cluster. In questo caso il numero necessario di licenze viene propagato dal Server principale (potrebbe essere un Server del cluster o uno che non fa parte del cluster) ai Server subordinati attraverso la comunicazione tra i server direttamente durante il funzionamento.

   In questo modo basta memorizzare sul Server principale un file di licenza con il numero di licenze corrispondente al numero di postazioni e distribuire il numero di licenze necessario sui Server subordinati durante il funzionamento del cluster. L'amministratore della rete antivirus configura manualmente la distribuzione sui Server subordinati del numero di licenze necessario per il periodo necessario.

   Per configurare la distribuzione delle licenze sui Server adiacenti, utilizzare la Gestione licenze.

   Per esempio, è possibile configurare una struttura gerarchica dei Server e allocare il Server principale (potrebbe essere un Server del cluster o uno che non fa parte del cluster) che distribuirà sia gli aggiornamenti del repository che le licenze dal file di licenza a tutti i nodi del cluster.

b) Quando si sceglie di non configurare la struttura gerarchica dei Server, non c'è la possibilità di distribuire licenze dall'unico file di licenza tra tutti i Server. In tale caso è necessario pianificare in anticipo la struttura della rete antivirus tenendo conto della disponibilità di un cluster di Server e utilizzare diversi file di licenza – uno per ciascun Server del cluster. Il numero totale di licenze in tutti i file di licenza è pari al numero totale di postazioni nella rete, però è necessario calcolare in anticipo la distribuzione del numero di licenze per i Server del cluster basandosi sul numero stimato di postazioni che si pianifica di connettere a ciascuno dei Server.

7. I task nel calendario dei Server

Per escludere la duplicazione delle query al database, è consigliabile eseguire soltanto su uno dei Server le seguenti task dal calendario del Server: **Purge Old Data**, **Backup sensitive data**,

Purge old stations, **Purge expired stations**, **Purge unsent IS events**. Per esempio, sul Server che si trova sullo stesso computer del database esterno unico. O sul computer del cluster con le maggiori prestazioni se le configurazioni dei Server sono diverse e il database è installato su un computer separato.

Capitolo 9: Aggiornamento dei componenti di Dr.Web Enterprise Security Suite

Prima di cominciare ad aggiornare Dr.Web Enterprise Security Suite e singoli componenti, si consiglia vivamente di controllare se le impostazioni di accesso ad Internet del protocollo TCP/IP sono corrette. In particolare, il servizio DNS deve essere attivo ed avere le impostazioni corrette.

Si possono aggiornare i database dei virus e il software sia manualmente che attraverso il calendario di task del Server e dell'Agent.

Prima di aggiornare il software, si consiglia di configurare il repository, compreso l'accesso a SAM Dr.Web (v. p. Configurazione generale del repository).

9.1. Aggiornamento di Server Dr.Web e ripristino da copia di backup

Il Pannello di controllo fornisce le seguenti possibilità per la gestione del software Server Dr.Web:

- L'aggiornamento del software Server ad una delle versioni disponibili, caricate da SAM e memorizzate nel repository del Server. Le impostazioni dell'aggiornamento di repository da SAM sono descritte nella sezione Gestione del repository di Server Dr.Web.
- Il rollback del software Server ad una copia di backup salvata. Le copie di backup del Server vengono create automaticamente quando si passa ad una versione nuova nella sezione **Aggiornamenti di Server Dr.Web** (passo 4 della procedura sottostante).

L'aggiornamento di Server all'interno della versione 10 inoltre può essere eseguito tramite il pacchetto di Server. La procedura viene descritta nella **Guida all'installazione**, nella sezione Aggiornamento di Server Dr.Web per SO Windows® o Aggiornamento di Server Dr.Web per SO della famiglia UNIX®.

Non tutti gli aggiornamenti di Server all'interno della versione 10 contengono un file di pacchetto. Alcuni di essi possono essere installati soltanto tramite il Pannello di controllo.

Quando il Server sotto un SO della famiglia UNIX viene aggiornato tramite il Pannello di controllo, la versione di Server in gestore pacchetti del SO non cambia.

Per gestire il software Server Dr.Web:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Server Dr.Web**.
2. Per andare alla lista delle versioni di Server, eseguire una delle seguenti azioni:

- Premere la versione corrente di Server nella finestra principale.
- Premere il pulsante **Elenco delle versioni**.

3. Si apre la sezione **Aggiornamenti di Server Dr.Web** con un elenco degli aggiornamenti e dei backup di Server disponibili. In particolare:
   - Nella lista **Versione corrente** è indicata la versione di Server che viene utilizzata al momento. Nella sezione **Lista delle modifiche** è riportato un breve elenco di nuove funzioni e un elenco degli errori corretti in questa versione rispetto alla versione precedente dell'aggiornamento.
   - Nella lista **Tutte le versioni** è riportata una lista degli aggiornamenti per questo Server, caricati da SAM. Nella sezione **Lista delle modifiche** è riportato un breve elenco di nuove funzioni e di errori corretti per ciascuno degli aggiornamenti.
     Per la versione che corrisponde all'installazione iniziale di Server da pacchetto d'installazione, la sezione **Lista delle modifiche** è vuota.
   - Nella lista **Copie di backup** è riportata una lista delle copie di backup salvate per questo Server. Nella sezione **Data** sono disponibili le informazioni sulla data del backup.
4. Per aggiornare il software Server, selezionare la casella di controllo di fronte alla versione di Server richiesta nella lista **Tutte le versioni** e premere il pulsante **Salva**.

   Il software di Server può essere aggiornato soltanto ad una versione più recente rispetto a quella utilizzata al momento.

   Nel corso dell'aggiornamento del Server, la versione corrente viene salvata come backup (viene messa nella sezione **Copie di backup**) e la versione a cui si aggiorna viene trasferita dalla sezione **Tutte le versioni** nella sezione **Versione corrente**.

   I backup vengono salvati nella seguente directory:

   `var → update_backup_`<*vecchia_versione*>`_`<*nuova_versione*>.

   Nel corso dell'aggiornamento viene creato o completato il file di log `var → dwupdater.log`.
5. Per eseguire il rollback del software Server ad una copia di backup salvata, selezionare la casella di controllo di fronte alla versione di Server richiesta nella lista **Copie di backup** e premere il pulsante **Salva**.

   Nel corso del rollback del software Server, la copia di backup a cui si passa viene messa nella sezione **Versione corrente**.

9.2. Aggiornamento manuale dei componenti di Dr.Web Enterprise Security Suite

Controllo della disponibilità di aggiornamenti in SAM

Per controllare la disponibilità di aggiornamenti di prodotti Dr.Web Enterprise Security Suite sul server di aggiornamento:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Stato del repository**.
2. Nella finestra che si è aperta vengono visualizzate le informazioni su tutti i componenti e inoltre la data dell'ultima revisione e lo stato corrente. Per controllare la disponibilità di aggiornamenti sul server SAM, premere il pulsante **Verifica aggiornamenti**.
3. Se il componente che viene verificato è obsoleto, verrà aggiornato automaticamente nel corso della verifica. L'aggiornamento avviene secondo le impostazioni del repository (v. p. Gestione del repository di Server Dr.Web).

Avvio del processo dell'aggiornamento del software postazione

Per avviare il processo dell'aggiornamento del software postazione:

1. Selezionare la voce **Rete antivirus** del menu principale del Pannello di controllo, nella finestra che si è aperta nella lista gerarchica fare clic sul nome di una postazione o di un gruppo.
2. Nella barra degli strumenti premere il pulsante **Gestione dei componenti**. Nel sottomenu selezionare la voce:

   Aggiorna i componenti falliti per aggiornare soltanto i componenti di cui l'ultimo aggiornamento non è riuscito e per resettare lo stato errore.

   Aggiorna tutti i componenti per avviare l'aggiornamento forzato di tutti i componenti, compresi quelli di cui l'ultima versione è già installata.

   In caso della sincronizzazione forzata di tutti i componenti, sarà necessario riavviare la postazione. Seguire le indicazioni dell'Agent.

9.3. Aggiornamenti programmati

È possibile configurare un calendario di esecuzione di task sul Server per aggiornare il software a cadenze regolari (per maggiori informazioni sul calendario dei task consultare il p. Configurazione del calendario di Server Dr.Web).

Per configurare il calendario di esecuzione di un task di aggiornamento sul Server Dr.Web:

1. Selezionare la voce **Amministrazione** del menu principale del Pannello di controllo, nella finestra che si è aperta selezionare la voce del menu di gestione **Scheduler del Server Dr.Web**. Si apre una lista attuale dei task del Server.
2. Per aggiungere un task alla lista, nella barra degli strumenti premere il pulsante **Crea task** Si apre la finestra di modifica del task.
3. Inserire nel campo **Nome** il nome del task sotto cui verrà visualizzato nel calendario.
4. Passare alla scheda **Azione** e selezionare dalla lista a cascata il tipo di task **Aggiornamento del repository**.
5. Nella lista che si è aperta, spuntare i flag di fronte ai componenti da aggiornare secondo questo task.
6. Passare alla scheda **Tempo** e selezionare dalla lista a cascata la periodicità dell'esecuzione del task, dopodiché configurare il tempo secondo la periodicità selezionata.
7. Per salvare le modifiche, premere il pulsante **Salva**.

9.4. Aggiornamento del repositorio di Server Dr.Web, non connesso a Internet

9.4.1. Copiatura del repository di un altro Server Dr.Web

Se un Server Dr.Web non è connesso a Internet, si può aggiornare il suo repository manualmente, copiando il repository di un altro Server Dr.Web aggiornato.

Questo metodo non è progettato per l'aggiornamento di Server a una nuova versione.

Per trasferire gli aggiornamenti di repository da un altro Server Dr.Web:

1. Aggiornare il repository del Server collegato ad Internet, utilizzando la sezione **Amministrazione** → Stato del repository nel Pannello di controllo.
2. Esportare il repository o una sua parte (i prodotti richiesti) tramite il Pannello di controllo, utilizzando la sezione Contenuti del repository. È necessario esportare soltanto i tipi di oggetti che sono supportati per la successiva importazione.
3. Copiare l'archivio con il repository esportato sul computer con il Server che richiede gli aggiornamenti.

   Importare il repository caricato sul Server tramite il Pannello di controllo, utilizzando la sezione **Amministrazione** → Contenuti del repository.

Se si utilizzano le impostazioni personalizzate del repository, per esempio il congelamento di revisioni o l'aggiornamento di Agent soltanto dalla revisione impostata (diversa da quella ulti-

ma), durante l'importazione del repository è necessario attivare l'opzione **Aggiungi soltanto le revisioni mancanti** e disattivare l'opzione **Importa i file di configurazione**.

9.4.2. Loader di repository Dr.Web

Se non è possibile collegare ad Internet uno dei Server Dr.Web, è possibile scaricare il repository da SAM senza utilizzare il software Server. Per tale scopo viene fornita l'utility standard Loader di repository Dr.Web.

Caratteristiche dell'utilizzo

- Per caricare il repository da SAM, occorre la chiave di licenza di Dr.Web Enterprise Security Suite o il suo hash MD5 che può essere visualizzato nel Pannello di controllo, nella sezione **Amministrazione** → **Gestione licenze**.
- Il Loader di repository Dr.Web è disponibile nelle seguenti versioni:
  - versione dell'utility con interfaccia grafica (soltanto nella versione per il SO Windows),
  - versione console dell'utility.
- Per il caricamento del repository da SAM, è possibile utilizzare un server proxy.

Possibili varianti dell'utilizzo

Caricamento con la sostituzione manuale del repository

1. Caricare da SAM il repository di Server attraverso l'utility Loader di repository Dr.Web.

   Al caricamento creare un archivio di repository:

   a) In caso dell'utility grafica: selezionare la modalità **Carica repository** e spuntare la casella **Archivia il repository** nella finestra principale dell'utility.

   b) In caso dell'utility console: utilizzare l'opzione `--archive`.

2. Copiare l'archivio con il repository caricato sul computer con il Server Dr.Web che richiede gli aggiornamenti.

   Importare il repository caricato sul Server Dr.Web tramite il Pannello di controllo, utilizzando la sezione **Amministrazione** → Contenuti del repository.

Se si utilizzano le impostazioni personalizzate del repository, per esempio il congelamento di revisioni o l'aggiornamento di Agent soltanto dalla revisione impostata (diversa da quella ultima), durante l'importazione del repository è necessario attivare l'opzione **Aggiungi soltanto le revisioni mancanti** e disattivare l'opzione **Importa i file di configurazione**.

La modalità di creazione di mirror di aggiornamento è disponibile soltanto nel loader grafico soltanto dell'ultima versione che può essere scaricata sul sito ufficiale della società nei formati versione x64 e versione x32.

Creazione di un mirror del repository su un server della rete locale

1. Caricare da SAM il repository di Server attraverso l'utility grafica Loader di repository Dr.Web.

   Al caricamento selezionare la modalità **Sincronizza mirror degli aggiornamenti** nella finestra principale dell'utility.
2. Mettere il repository caricato su un web server della propria rete locale, che verrà utilizzato per distribuire gli aggiornamenti del repository.
3. Nella sezione **Amministrazione** → Configurazione generale del repository configurare la ricezione di aggiornamenti da parte del Server Dr.Web dal mirror locale anziché dai server SAM Dr.Web.

Assicurarsi che il mirror si trovi nella directory con il nome `10.01.0`. Il percorso nel campo **URI di base** deve essere indicato fino a questa directory, non compresa la directory stessa.

9.4.2.1. Utility con interfaccia grafica

La versione con interfaccia grafica dell'utility Loader di repository Dr.Web può essere scaricata tramite il Pannello di controllo, nella sezione **Amministrazione** → **Utility**. Questa versione dell'utility può essere eseguita su qualsiasi computer SO Windows con una connessione Internet. Il file eseguibile è `drwreploader-gui-<versione>.exe`.

La modalità di caricamento degli aggiornamenti e alcune altre sezioni dei parametri avanzati sono disponibili soltanto nell'ultima versione del loader, che può essere scaricata sul sito ufficiale della società nei formati versione x64 e versione x32.

Per caricare il repository tramite la versione con interfaccia grafica di Loader di repository Dr.Web:

1. Avviare la versione con interfaccia grafica di Loader di repository Dr.Web.
2. Nella finestra principale dell'utility, impostare i seguenti parametri:
   a) **Chiave di licenza o MD5 della chiave** – specificare il file della chiave di licenza Dr.Web. Per farlo, premere **Sfoglia** e selezionare un file della chiave di licenza valido. Invece del file della chiave di licenza, si può indicare soltanto l'hash MD5 della chiave di licenza, che può essere visualizzato nel Pannello di controllo, nella sezione **Amministrazione** → **Gestione licenze**.
   b) **Directory di download** – impostare la directory in cui viene caricato il repository.
   c) Dalla lista **Modalità** selezionare una delle modalità di caricamento degli aggiornamenti:

- **Carica repository** – il repository viene caricato nel formato di repository di Server. I file caricati possono essere importati direttamente tramite il Pannello di controllo come gli aggiornamenti di repository di Server.
- **Sincronizza mirror degli aggiornamenti** – il repository viene caricato nel formato zona di aggiornamento di SAM. I file caricati possono essere memorizzati sul mirror di aggiornamento nella rete locale. In seguito i Server possono essere configurati per ricevere aggiornamenti direttamente da questo mirror di aggiornamento, che contiene l'ultima versione del repository, invece di ricevere gli aggiornamenti dai server di SAM.

d) Spuntare il flag **Archivia il repository** affinché il repository venga automaticamente compresso in un archivio .zip. Questa opzione permette di ottenere un file di archivio pronto per la successiva importazione del repository sul Server tramite il Pannello di controllo, dalla sezione **Amministrazione** → Contenuti del repository.

3. Se si vogliono modificare le impostazioni avanzate di connessione a SAM e di caricamento di aggiornamenti, premere **Avanzate**. Nella finestra di configurazione che si è aperta, sono disponibili le seguenti schede:

a) Nella scheda **Prodotti** si può modificare la lista dei prodotti da caricare. Nella finestra delle impostazioni che si è aperta, viene riportata la lista di tutti i prodotti di repository disponibili per il caricamento da SAM:

- Per aggiornare la lista dei prodotti disponibili attualmente in SAM, premere il pulsante **Aggiorna**.
- Spuntare i flag di fronte ai prodotti che si vogliono caricare da SAM oppure il flag nell'intestazione della tabella per selezionare tutti i prodotti nella lista.

b) Nella scheda **SAM Dr.Web**, è possibile configurare parametri dei server di aggiornamento:

- L'ordine dei server SAM nella lista determina l'ordine in cui l'utility si connette ad essi per il caricamento del repository. Per modificare l'ordine dei server SAM, utilizzare i pulsanti **In alto** e **In basso**.
- Per aggiungere un server SAM alla lista dei server utilizzati per il caricamento, inserire l'indirizzo del server SAM nel campo sopra la lista dei server e premere il pulsante **Aggiungi**.
- Per cancellare un server SAM dalla lista dei server utilizzati, selezionare dalla lista il server da cancellare e premere il pulsante **Rimuovi**.
- Nel campo **URI di base** viene indicata la directory sui server SAM che contiene gli aggiornamenti dei prodotti Dr.Web.
- Dalla lista a cascata **Protocollo** selezionare il tipo di protocollo per la ricezione degli aggiornamenti dai server di aggiornamenti. Per tutti i protocolli il caricamento degli aggiornamenti viene eseguito secondo le impostazioni della lista dei server di SAM.
- Dalla lista a cascata **Certificati validi** selezionare il tipo di certificato SSL che verrà accettato automaticamente. Questa impostazione si usa solo per i protocolli sicuri che supportano crittografia.
- **Nome utente** e **Password** – le credenziali dell'utente per l'autenticazione sul server di aggiornamento, se il server richiede l'autenticazione.

- Spuntare il flag **Utilizza CDN** per consentire l'utilizzo di Content Delivery Network per il caricamento del repository.

c) Nella scheda **Proxy** è possibile configurare le impostazioni di connessione a SAM attraverso un server proxy:

- **Indirizzo del server proxy** e **Porta** – rispettivamente l'indirizzo di rete e il numero di porta del server proxy in uso.
- **Nome utente** e **Password** – le credenziali per l'autenticazione sul server proxy, se il server proxy in uso richiede l'autenticazione.

d) Nella scheda **Scheduler** è possibile configurare un calendario di aggiornamenti periodici. Per eseguire il calendario, si usa lo scheduler di task del SO Windows. In questo caso non c'è la necessità di avviare l'utility manualmente, anzi il repository verrà caricato automaticamente tra gli intervalli di tempo impostati.

e) Nella scheda **Log** si possono configurare i parametri di registrazione del log del caricamento degli aggiornamenti.

Premere **OK** per accettare le modifiche fatte e per tornare alla finestra principale di Loader di repository Dr.Web.

4. Dopo aver configurato tutti i parametri, premere il pulsante **Carica** nella finestra principale di Loader di repository Dr.Web per avviare la connessione a SAM e il caricamento del repository.

9.4.2.2. Versione console dell'utility

La versione console dell'utility Loader di repository Dr.Web si trova nella sottodirectory bin della directory di installazione di Server Dr.Web. Questa versione dell'utility può essere eseguita soltanto da questa directory di Server. Il file eseguibile è `drwreploader`.

Opzioni valide

- `--help` – visualizza la guida sulle opzioni.
- `--show-products` – mostra l'elenco dei prodotti in SAM.
- `--path` <*argomento*> – carica il repository da SAM nella directory specificata nel parametro <*argomento*>.
- `--etc` <*argomento*> – percorso della directory `etc` di Server (si usa per cercare certificati radice e per aggiornare chiavi pubbliche).
- `--archive` – comprimi il repository in archivio.
- `--key` <*argomento*> – percorso del file della chiave di licenza (va specificata la chiave o il suo hash MD5).
- `--key-md5` <*argomento*> – hash MD5 della chiave di licenza (va specificata la chiave o il suo hash MD5).
- `--product` <*argomento*> – il prodotto che viene aggiornato. Di default, viene caricato l'intero repository.
- `--only-bases` – carica soltanto i database dei virus.

- `--update-url` <*argomento*> – la directory sui server SAM che contiene gli aggiornamenti dei prodotti Dr.Web (è consigliabile lasciare il valore predefinito).
- `--servers` <*argomento*> – gli indirizzi dei server SAM (è consigliabile lasciare il valore predefinito).
- `--prohibit-cdn` – proibisci l'utilizzo di CDN per il caricamento degli aggiornamenti (di default l'opzione è disattivata, cioè l'utilizzo di CND è consentito).
- `--prohibit-ssl` – utilizza il protocollo non sicuro HTTP invece di HTTPS (di default l'opzione è disattivata, cioè viene utilizzato HTTPS).
- `--cert-mode` [<*argomento*>] – accetta automaticamente certificati HTTPS.

  <*argomento*> può essere uno dei valori:

  - `any` – accetta tutti i certificati,
  - `valid` – accetta soltanto i certificati verificati,
  - `drweb` – accetta soltanto i certificati Dr.Web.

  Di default, viene utilizzato il valore `drweb`.
- `--proxy-host` <*argomento*> – server proxy nel formato <*server*>`[:`<*porta*>`]`.
- `--proxy-auth` <*argomento*> – informazioni per l'autenticazione sul server proxy: nome utente e password nel formato <*utente*>`[:`<*password*>`]`.
- `--strict` – interrompi il caricamento se si verifica un errore.
- `--log` <*argomento*> – crea un log di caricamento del repository nel formato dei log di Server e salvalo nella directory specificata nel parametro<*argomento*>.

Esempi di utilizzo

1. Crea un archivio da importare con tutti i prodotti:

```
drwreploader.exe --path=C:\Temp\repository.zip --archive --key "C:\Pro-
gram Files\DrWeb Server\etc\agent.key" --etc "C:\Program Files\DrWeb
Server\etc"
```

2. Crea un archivio da importare con i database dei virus:

```
drwreploader.exe --path=C:\Temp\repository.zip --archive --key "C:\Pro-
gram Files\DrWeb Server\etc\agent.key" --only-bases --etc "C:\Program
Files\DrWeb Server\etc"
```

3. Crea un archivio da importare soltanto con il Server:

```
drwreploader.exe --path=C:\Temp\repository.zip --archive --key "C:\Pro-
gram Files\DrWeb Server\etc\agent.key" --product=20-drwcs --etc "C:\Pro-
gram Files\DrWeb Server\etc"
```

9.5. Limitazione degli aggiornamenti delle postazioni

Tramite il Pannello di controllo, è possibile configurare la modalità dell'aggiornamento dei componenti di Dr.Web Enterprise Security Suite su postazioni protette per determinati intervalli di tempo.

Per configurare la modalità dell'aggiornamento delle postazioni, eseguire le seguenti azioni:

1. Selezionare la voce **Rete antivirus** del menu principale, nella finestra che si è aperta, nella lista gerarchica fare clic sul nome di una postazione o di un gruppo. Nel menu di gestione selezionare la voce **Limitazioni degli aggiornamenti**.
2. Dalla lista a cascata **Limitazione degli aggiornamenti** selezionare la modalità di limitazione:
   - **Senza limitazioni** – per non porre restrizioni alla distribuzione degli aggiornamenti alle postazioni.
   - **Proibisci ogni aggiornamento** – per proibire la distribuzione di tutti gli aggiornamenti alle postazioni negli intervalli di tempo definiti più in basso nella tabella **Calendario dell'aggiornamento delle postazioni**.
   - **Aggiorna soltanto i database** – per proibire la distribuzione soltanto degli aggiornamenti dei moduli software negli intervalli di tempo definiti più in basso nella tabella **Calendario dell'aggiornamento delle postazioni**. I database dei virus verranno aggiornati come di solito in modalità normale.
3. Spuntare il flag **Limita il volume di dati degli aggiornamenti** per limitare il traffico di rete durante la trasmissione di aggiornamenti tra il Server e gli Agent. Nel campo **Velocità di trasmissione massima (KB/s)** impostare un valore della velocità massima di trasmissione di aggiornamenti.
4. Spuntare il flag **Ricevi tutti gli aggiornamenti recenti** affinché la postazione riceva tutti gli aggiornamenti dei componenti a prescindere dalle limitazioni impostate nella sezione Configurazione dettagliata del repository.

   Se il flag è tolto, la postazione riceverà soltanto gli aggiornamenti marcati come gli aggiornamenti attuali da distribuire.
5. Nella tabella **Calendario dell'aggiornamento delle postazioni** la modalità di aggiornamento viene configurata con la seguente classificazione di colore:
   - colore verde – l'aggiornamento è consentito;
   - colore rosso – l'aggiornamento è proibito.

   La limitazione viene configurata separatamente per ogni 15 minuti di ogni giorno della settimana.

Per modificare la modalità di aggiornamento, fare clic sul relativo blocco della tabella:

- Per modificare la modalità di una riga intera (un giorno intero), fare clic sul marcatore del colore appropriato a destra della riga richiesta della tabella.
- Per modificare la modalità di una colonna intera (un intervallo di 15 minuti per tutti i giorni della settimana), fare clic sul marcatore del colore appropriato sotto la colonna richiesta della tabella.

6. Dopo aver apportato delle modifiche, premere il pulsante **Salva** per accettare le modifiche apportate.

Nella barra degli strumenti sono inoltre disponibili le seguenti opzioni per la gestione dei contenuti della sezione:

Resetta tutti i parametri ai valori iniziali – per ripristinare tutti i parametri di questa sezione ai valori che avevano prima della modifica corrente (ultimi valori salvati).

Resetta tutti i parametri ai valori default – per ripristinare tutti i parametri di questa sezione ai valori di default.

Propaga queste impostazioni verso un altro oggetto – per copiare le impostazioni da questa sezione nelle impostazioni di un altra postazione, di un gruppo o di diversi gruppi e postazioni.

Imposta l'ereditarietà delle impostazioni dal gruppo primario – per eliminare le impostazioni individuali delle postazioni e per impostare l'ereditarietà delle impostazioni di questa sezione dal gruppo primario.

Copia le impostazioni dal gruppo primario e impostale come individuali – per copiare le impostazioni di questa sezione dal gruppo primario e per assegnarle alle postazioni selezionate. In questo caso, l'ereditarietà non viene impostata e le impostazioni della postazione vengono considerate individuali.

Esporta le impostazioni da questa sezione in file – per salvare tutte le impostazioni da questa sezione in un file di formato specifico.

Importa le impostazioni in questa sezione da file – per sostituire tutte le impostazioni in questa sezione con le impostazioni salvate in un file di formato specifico.

9.6. Aggiornamento di Agent Dr.Web mobile

Se il computer, notebook o dispositivo mobile dell'utente non avrà la connessione con il Server Dr.Web per lungo tempo, per la ricezione tempestiva di aggiornamenti dai server SAM Dr.Web, si consiglia di impostare la modalità di funzionamento mobile dell'Agent Dr.Web sulla postazione.

In modalità mobile l'Agent cerca di connettersi al Server, fa tre tentativi e se non è riuscito, esegue l'aggiornamento HTTP. I tentativi di ricerca del Server si susseguono ininterrottamente a intervallo di circa un minuto.

La possibilità di attivare la modalità mobile nelle impostazioni di Agent sarà disponibile a condizione che l'utilizzo della modalità mobile sia consentito nel Pannello di controllo nella sezione **Rete antivirus** → **Permessi** → <*sistema_operativo*> → **Generali** → **Avvio in modalità mobile**.

Durante il funzionamento dell'Agent in modalità mobile la connessione dell'Agent al Server Dr.Web si interrompe. Tutte le modifiche impostate sul Server per tale postazione entreranno in vigore non appena la modalità mobile dell'Agent verrà disattivata e l'Agent si riconnetterà al Server.

In modalità mobile vengono aggiornati soltanto i database dei virus.

Le impostazioni della modalità mobile di funzionamento sul lato Agent sono descritte nel **Manuale dell'utente**.

Capitolo 10: Configurazione dei componenti addizionali

10.1. Server proxy

Uno o più Server proxy possono far parte della rete antivirus.

L'obiettivo principale del Server proxy è di assicurare la comunicazione del Server Dr.Web e degli Agent Dr.Web nel caso non sia possibile organizzare l'accesso diretto (per esempio, se il Server Dr.Web e gli Agent Dr.Web si trovano in reti diverse senza l'instradamento dei pacchetti tra di esse).

Per stabilire una connessione tra il Server e i client attraverso il Server proxy, si consiglia di disattivare la cifratura del traffico. Per farlo, basta impostare il valore **no** per il parametro **Crittografia** nella sezione Configurazione del Server Dr.Web → Generali.

Funzioni principali

Il server proxy svolge le seguenti funzioni:

1. È in ascolto e accetta connessioni secondo le impostazioni di protocollo e porta.
2. Traslazione dei protocolli (sono supportati i protocolli TCP/IP).
3. Trasmissione dei dati tra il Server Dr.Web e gli Agent Dr.Web secondo le impostazioni del Server proxy.
4. Memorizzazione nella cache degli aggiornamenti dell'Agent e del pacchetto antivirus, trasmessi dal Server. Se gli aggiornamenti vengono rilasciati dalla cache del Server proxy, questo permette di:
   - diminuire il traffico di rete,
   - diminuire il tempo di ricevimento degli aggiornamenti da parte degli Agent.

È possibile creare una gerarchia dei server proxy.

Lo schema generale della rete antivirus con utilizzo di Server proxy è riportato in immagine 10-1.

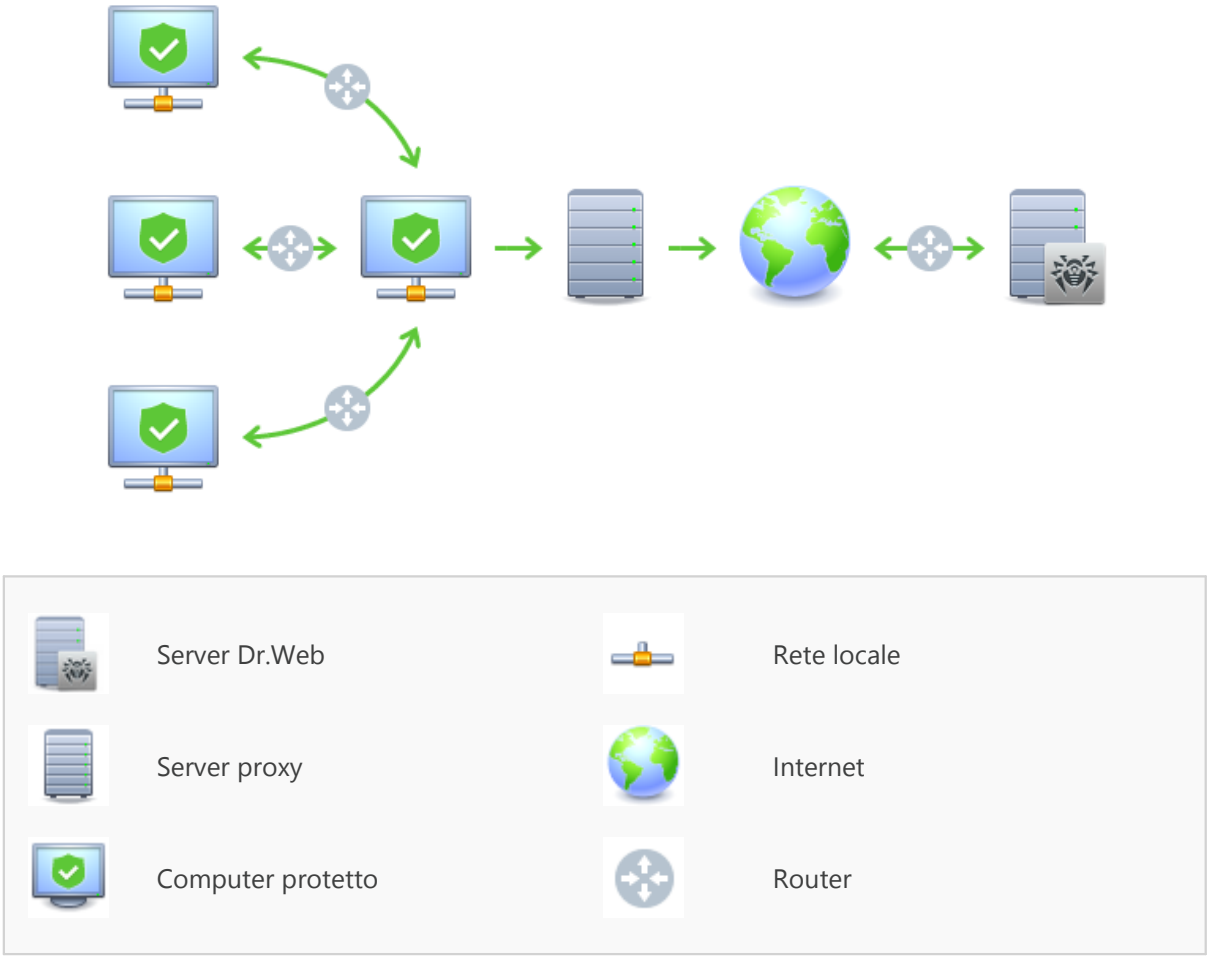


Immagine 10-1. Schema della rete antivirus con utilizzo di Server proxy

Principio di funzionamento

In caso di utilizzo del Server proxy, viene eseguita la seguente sequenza di azioni:

1. Se nell'Agent non è definito l'indirizzo del Server, l'Agent spedisce una richiesta multicast in conformità con il protocollo della rete in cui si trova.
2. Se il Server proxy è configurato per la traslazione di connessioni (il parametro `discovery="yes"`), all'Agent viene inviato un avviso di disponibilità di un Server proxy operativo.
3. L'Agent imposta i parametri del Server proxy ottenuti come i parametri del Server Dr.Web. La comunicazione successiva avviene in un modo trasparente per l'Agent.
4. Secondo i parametri del file di configurazione, il Server proxy è in ascolto sulle porte impostate per le connessioni in ingresso attraverso i protocolli indicati.
5. Per ciascuna connessione in ingresso da un Agent, il Proxy stabilisce una connessione con il Server Dr.Web.

Algoritmo di reindirizzamento se è disponibile una lista dei Server Dr.Web:

1. Server proxy carica nella memoria operativa una lista dei Server Dr.Web dal file di configurazione `drwcsd-proxy.xml` (v. documento **Allegati**, p. Allegato G4).
2. L'Agent Dr.Web si connette al Server proxy.
3. Server proxy reindirizza l'Agent Dr.Web sul primo Server Dr.Web dalla lista nella memoria operativa.
4. Server proxy ruota a lista caricata nella memoria operativa e sposta questo Server Dr.Web dal primo elemento della lista alla fine della lista.

   Server proxy non memorizza nel suo file di configurazione la sequenza modificata dei Server. Quando Server proxy viene riavviato, la lista dei Server Dr.Web viene caricata nella memoria operativa nella sua versione originale, conservata nel file di configurazione.

5. Quando un altro Agent si connette al Server proxy, la procedura si ripete dal passo 2.
6. Se un Server Dr.Web si sconnette dalla rete antivirus (per esempio, in caso di spegnimento o negazione del servizio), l'Agent si riconnette al Server proxy e la procedura si ripete dal passo 2.

   Uno Scanner di rete, avviato su un computer di una rete esterna relativamente agli Agent, non può rilevare gli Agent installati.

   Se il flag **Sostituisci i nomi NetBIOS** è selezionato, e nella rete antivirus viene utilizzato un Server proxy, per tutte le postazioni connesse al Server attraverso il Server proxy nel Pannello di controllo come i nomi di postazioni verrà visualizzato il nome del computer su cui è installato il Server proxy.

Cifratura e compressione del traffico dati

Server proxy supporta la compressione del traffico dati. Le informazioni trasmesse vengono processate a prescindere da quello se il traffico è compresso o meno.

Server proxy non supporta la cifratura. Analizza le informazioni inviate e se il traffico dati tra il Server Dr.Web e l'Agent viene cifrato, il Server proxy passa alla modalità trasparente, cioè trasmette tutto il traffico dati tra il Server e l'Agent senza alcuna analisi dei dati.

Se è attivata la modalità della cifratura dei dati trasmessi tra l'Agent e il Server, gli aggiornamenti non vengono salvati nella cache di Server proxy.

Memorizzazione nella cache

Server proxy supporta la memorizzazione del traffico dati nella cache.

I prodotti vengono memorizzati nella cache per revisione. Ciascuna revisione si trova in una directory separata. Nella directory per ciascuna revisione successiva sono disponibili gli hard link (hard links) ai file esistenti delle revisioni precedenti e le versioni originali dei file modificati. In questo modo, i file per ciascuna versione vengono conservati sul disco rigido in una copia unica, in tutte le directory di revisioni successive vengono riportati soltanto i link ai file invariati.

I parametri che vengono impostati nel file di configurazione permettono di configurare le seguenti azioni per la memorizzazione nella cache:

- Eliminare periodicamente le revisioni obsolete. Di default, una volta all'ora.
- Conservare soltanto le revisioni recenti. Tutte le altre revisioni, in quanto precedenti, sono considerate obsolete e vengono eliminate. Di default, vengono conservate le ultime tre revisioni.
- Scaricare periodicamente dalla memoria i file *memory mapped* non utilizzati. Di default, ogni 10 minuti.

Impostazioni

Server proxy non ha l'interfaccia grafica. Le impostazioni vengono definite tramite il file di configurazione. Il formato del file di configurazione di Server proxy è riportato in documento **Allegati**, p. Allegato G4.

La gestione delle impostazioni (modifica del file di configurazione) del Server proxy può essere effettuata soltanto da un utente con i permessi dell'amministratore di tale computer.

Affinché il Server proxy funzioni in modo corretto sotto i SO della famiglia Linux, dopo il riavvio del computer occorre eseguire la configurazione di sistema della rete senza utilizzare Network Manager.

Avvio e arresto

Sotto l'SO Windows il Server proxy viene avviato e arrestato tramite gli strumenti standard attraverso l'elemento **Pannello di controllo** → **Amministrazione** → **Servizi** → nella lista dei servizi fare doppio clic su **drwcsd-proxy** e nella finestra che si è aperta selezionare l'azione necessaria.

Sotto i SO della famiglia UNIX, il Server proxy viene avviato e arrestato tramite i comandi `start` e `stop` applicati agli script creati nel corso dell'installazione del Server proxy (v. **Guida all'installazione**, p. Installazione del Server proxy).

Inoltre per avviare Server proxy negli SO Windows e negli SO della famiglia UNIX, è possibile avviare il file eseguibile `drwcsd-proxy` con i parametri corrispondenti (v. Allegato H9. Server proxy).

10.2. NAP Validator

Informazioni generali

Microsoft® Network Access Protection (NAP) è una piattaforma di criteri, incorporata nei sistemi operativi Windows, che provvede a una maggiore sicurezza della rete. La sicurezza è dovuta al fatto che vengono soddisfatti i requisiti di operatività dei sistemi della rete.

Utilizzando la tecnologia NAP, si possono creare criteri di operatività personalizzati per valutare lo stato di un computer. Le valutazioni ottenute vengono analizzate nei seguenti casi:

- prima di consentire l'accesso o l'interazione,
- per aggiornare in automatico computer che corrispondono ai requisiti per provvedere alla loro compatibilità continua,
- per portare alla conformità computer che non corrispondono ai requisiti per farli corrispondere ai requisiti stabiliti.

Una descrizione dettagliata della tecnologia NAP è disponibile sul sito di Microsoft.

Utilizzo di NAP in Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite permette di utilizzare la tecnologia NAP per controllare l'operatività del software antivirus di postazioni protette. Il componente utilizzato per questo fine è Dr.Web NAP Validator.

Per controllare l'operatività, vengono utilizzati i seguenti strumenti:

- Server NAP di controllo di operatività installato e configurato.
- Dr.Web NAP Validator è uno strumento per valutare l'operatività del software antivirus del sistema protetto (System Health Validator – SHV) sulla base dei criteri personalizzati Dr.Web. Viene installato sul computer insieme al server NAP.
- Agent di operatività del sistema (System Health Agent - SHA). Viene installato automaticamente insieme al software Agent Dr.Web su postazione.
- Server Dr.Web funge da un server di correzioni che provvede all'operatività del software antivirus di postazioni.

Immagine 10-2. Schema della rete antivirus con utilizzo di NAP

La procedura di controllo viene eseguita nel seguente modo:

1. Attivazione del processo di controllo viene eseguita alla configurazione delle impostazioni corrispondenti di Agent.
2. SHA su postazione si connette al componente Dr.Web NAP Validator installato sul server NAP.
3. Dr.Web NAP Validator controlla i criteri di operatività (v. sotto). Il controllo dei criteri è un processo in cui NAP Validator valuta gli strumenti antivirus dal punto di vista della conformità alle regole stabilite da esso e determina la categoria dello stato attuale del sistema:
   - le postazioni, che hanno superato il controllo della conformità agli elementi dei criteri, vengono considerate operative e vengono ammesse all'operazione a piena funzionalità nella rete.
   - le postazioni, che non soddisfano almeno uno degli elementi dei criteri, vengono considerate non operative. Tali postazioni possono accedere soltanto al Server Dr.Web e vengono

isolate dal resto della rete. L'operatività della postazione viene ripristinata tramite il Server, dopodiché la procedura di controllo per la postazione viene rifatta.

Requisiti di operatività:

1. Stato operativo dell'agent (è avviato e funziona).
2. Database dei virus aggiornati (i database coincidono con i database sul server).

Configurazione di NAP Validator

Dopo l'installazione di Dr.Web NAP Validator (v. **Guida all'installazione**, p. Installazione di NAP Validator), è necessario eseguire le seguenti azioni sul computer su cui è installato il server NAP:

1. Aprire il componente di configurazione del server NAP (comando `nps.msc`).
2. Nella sezione **Policies** selezionare la sottovoce **Health Policies**.
3. Nella finestra che si è aperta, selezionare le proprietà di elementi:
   - **NAP DHCP Compliant**. Nella finestra delle impostazioni, spuntare il flag **Dr.Web System Health Validator** che comanda l'utilizzo dei criteri del componente Dr.Web NAP Validator. Dalla lista a cascata selezionare la voce **Client passed all SHV checks** affinché venga riconosciuta operativa una postazione se corrisponde a tutti gli elementi del criterio impostato.
   - **NAP DHCP Noncompliant**. Nella finestra delle impostazioni, spuntare il flag **Dr.Web System Health Validator** che comanda l'utilizzo dei criteri del componente Dr.Web NAP Validator. Dalla lista a cascata selezionare la voce **Client fail one or more SHV checks** affinché venga riconosciuta non operativa una postazione se non corrisponde almeno ad uno degli elementi del criterio impostato.

Indice analitico

Indice analitico

Indice analitico

T