Dr.WEB

Enterprise Security Suite

Allegati

Dr.Web Enterprise Security Suite
Versione 13.0
Allegati
07/03/2024

Doctor Web, Sede centrale in Russia

Indirizzo: 125124, Russia, Mosca, 3a via Yamskogo polya, 2, 12A

Sito web: https://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: Introduzione

Scopo del documento

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

La documentazione dell'amministratore della rete antivirus è composta dalle seguenti parti principali:

1. **Guida all'installazione**

   Sarà utile per il responsabile aziendale che prende decisioni sull'acquisto e sull'installazione di un sistema di protezione antivirus completa.

   Nella guida all'installazione è descritto il processo di creazione di una rete antivirus e di installazione dei suoi componenti principali.

2. **Manuale dell'amministratore**

   È indirizzato *all'amministratore della rete antivirus* — dipendente dell'azienda, 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**

   Contengono informazioni tecniche che descrivono i parametri di configurazione dei componenti dell'Antivirus, nonché la sintassi e i valori delle istruzioni utilizzate per la gestione degli stessi.

Sono presenti riferimenti incrociati tra i documenti elencati sopra. Se i documenti sono stati scaricati su un computer locale, i riferimenti incrociati saranno operativi solo se i documenti sono situati in una stessa directory e hanno i nomi originali.

Inoltre, sono forniti i seguenti manuali:

1. **Guida rapida all'installazione della rete antivirus**

   Contiene brevi informazioni sull'installazione e sulla configurazione iniziale dei componenti della rete antivirus. Per informazioni dettagliate consultare la documentazione dell'amministratore.

2. **Manuali per la gestione delle postazioni**

   Contengono informazioni sulla configurazione centralizzata dei componenti del software antivirus delle postazioni, effettuata dall'amministratore della rete antivirus attraverso il Pannello di controllo della sicurezza Dr.Web.

3. **Manuali dell'utente**

   Contiene informazioni sulla configurazione della soluzione antivirus Dr.Web direttamente sulle postazioni protette.

4. **Guida alle Web API**

   Contiene informazioni tecniche sull'integrazione di Dr.Web Enterprise Security Suite con software di terzi tramite le Web API.

5. **Guida alla struttura del database del Server Dr.Web**

   Contiene una descrizione della struttura interna del database di Server Dr.Web e di esempi del suo utilizzo.

Tutti i manuali elencati sono forniti anche come parte del prodotto Dr.Web Enterprise Security Suite e possono essere aperti attraverso il Pannello di controllo della sicurezza Dr.Web.

Prima di leggere i documenti, assicurarsi che questa sia l'ultima versione dei manuali corrispondenti per la versione del prodotto in uso. I manuali vengono costantemente aggiornati, la loro ultima versione è ritrovabile sul sito ufficiale dell'azienda Doctor Web all'indirizzo https://download.drweb.com/doc/.

Segni convenzionali e abbreviazioni

Segni convenzionali

In questo manuale vengono utilizzati i seguenti simboli:

Simbolo	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.

Simbolo	Commento
`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 possono essere utilizzate le seguenti abbreviazioni senza spiegazione:

- DB, DBMS — database, database management system,
- SAM Dr.Web — Sistema di aggiornamento mondiale di Dr.Web,
- LAN — rete locale,
- SO — sistema operativo,
- SW, software — programmi per computer,
- ACL — lista di controllo degli accessi (Access Control List),
- CDN — rete di distribuzione di contenuti (Content Delivery Network),
- DFS — file system distribuito (Distributed File System),
- DNS — sistema dei nomi a dominio (Domain Name System),
- FQDN — nome di dominio completo (Fully Qualified Domain Name),
- GUI — interfaccia utente grafica (Graphical User Interface), versione del programma con la GUI — una versione che utilizza gli strumenti della GUI,
- MIB — database delle informazioni di gestione (Management Information Base),
- MTU — dimensione massima di un pacchetto dati (Maximum Transmission Unit),
- NAP — Network Access Protection,
- TTL — tempo di vita pacchetto (Time To Live),
- UDS — socket di dominio UNIX (UNIX Domain Socket).

Capitolo 2: Allegati

Allegato A. Impostazioni per l'utilizzo dei DBMS. Parametri dei driver dei DBMS

La struttura del database di Server Dr.Web è disponibile come manuale separato con lo stesso nome. Il documento può essere aperto dalla sezione **Supporto** nel Pannello di controllo della sicurezza Dr.Web.

Come database di Server Dr.Web può essere utilizzato:

- database incorporato;
- DBMS esterno.

Database incorporato

Per configurare l'utilizzo del database incorporato per la conservazione e l'elaborazione dei dati, vengono utilizzati i parametri riportati nella tabella **A-1**.

Tabella A-1. Database incorporato

Nome	Valore predefinito	Descrizione
DBFILE	database.sqlite	Percorso del file di database
CACHESIZE	2048	Dimensione della cache del database in pagine
PRECOMPILEDCACHE	1048576	Dimensione in byte della cache degli operatori SQL precompilati
MMAPSIZE	• in caso di SO UNIX — 10485760, • in caso di SO Windows — 0	Dimensione massima in byte del file di database che è ammissibile mappare allo spazio degli indirizzi del processo in una sola volta.
CHECKINTEGRITY	QUICK	Verifica dell'integrità dell'immagine database all'avvio di Server Dr.Web: • FULL — controllo completo per errori relativi alle limitazioni del tipo UNIQUE, CHECK e NOT NULL, record non ordinati, pagine saltate e indici non validi, • QUICK — variante di controllo veloce senza tracciamento di errori, limitazioni e indici non validi, • NO — il controllo non viene eseguito.

AUTOREPAIR	NO	Ripristino automatico di un'immagine database danneggiata all'avvio di Server Dr.Web: • YES — il ripristino dell'immagine del database viene avviato ogni volta che viene avviato il Server Dr.Web, • NO — il ripristino automatico è disattivato.
WAL	YES	Utilizzo della registrazione di log proattiva (Write-Ahead Logging): • YES — la registrazione del log è attivata, • NO — la registrazione del log non viene utilizzata.
WAL-MAX-PAGES	1000	Numero massimo di pagine "sporche", raggiunto il quale le pagine vengono registrate su disco.
WAL-MAX-SECONDS	30	Tempo massimo (in secondi) per il quale viene rinviata la registrazione delle pagine su disco.
SYNCHRONOUS	FULL	Modalità della scrittura su disco sincrona delle modifiche al database: • FULL — scrittura su disco completamente sincrona, • NORMAL — scrittura sincrona dei dati critici, • OFF — scrittura asincrona.

Come database incorporato è fornito SQLite3 — database supportato da Server Dr.Web a partire dalla versione 10.

DMBS esterno

Come database esterno di Server Dr.Web può essere utilizzato:

- DBMS MySQL, MariaDB. La configurazione è descritta in A4. Utilizzo del DBMS MySQL.
- DBMS Oracle. La configurazione è descritta in A2. Configurazione del driver di database per Oracle.
- DBMS PostgreSQL. La configurazione è descritta in A3. Utilizzo del DBMS PostgreSQL.

  Sono supportati i DBMS basati su PostgreSQL (PostgreSQL Pro, Jatoba ecc.).

- Microsoft SQL Server/Microsoft SQL Server Express. Per l'accesso a questi DBMS può essere utilizzato un driver ODBC (la configurazione dei parametri del driver ODBC per SO Windows è riportata in A1. Configurazione del driver ODBC).

  È supportato l'utilizzo di Microsoft SQL Server 2008 o versioni successive. È consigliato l'utilizzo di Microsoft SQL Server 2014 e versioni successive.

Il database Microsoft SQL Server Express non è consigliato per il dispiegamento di una rete antivirus con un numero elevato di postazioni (da 100 e più).

Se Microsoft SQL Server viene connesso come database esterno a un Server Dr.Web sotto SO della famiglia UNIX, il corretto funzionamento attraverso ODBC con FreeTDS non è garantito.

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 la disponibilità di aggiornamenti, consultare la seguente pagina Microsoft: https://learn.microsoft.com/en-US/troubleshoot/sql/releases/download-and-install-latest-updates.

Per ridurre il numero di blocchi nel caso di utilizzo di DBMS Microsoft SQL Server con il livello di isolamento delle transazioni predefinito (READ COMMITTED), è consigliabile attivare il parametro READ_COMMITTED_SNAPSHOT eseguendo il seguente comando SQL:

```
ALTER DATABASE <nome_database>
SET READ_COMMITTED_SNAPSHOT ON;
```

Il comando deve essere eseguito in modalità di transazioni implicite e con l'unica connessione esistente al database.

Caratteristiche comparative del database incorporato e dei DBMS esterni

Il database incorporato è progettato per la connessione al Server Dr.Web di circa 400–600 postazioni. Se lo permettono la configurazione dell'hardware del computer su cui è installato il Server Dr.Web e il carico di altri compiti eseguiti su questo computer, è possibile connettere circa 1000–1500 postazioni.

Altrimenti, è necessario utilizzare un database esterno. A seconda della configurazione e del carico sul computer che svolge le funzioni di Server Dr.Web, il database esterno può essere collocato sullo stesso computer o su un computer dedicato.

Se è utilizzato un database esterno e al Server Dr.Web sono connesse più di 10000 postazioni, sono consigliabili i seguenti requisiti minimi:

- processore con velocità 3GHz,
- da 6 core del processore,
- 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.

Quando si sceglie tra il database incorporato e quello esterno, si devono considerare alcuni parametri caratteristici di ciascuno dei database:

- Nelle grandi reti antivirus (più di 400–600 postazioni) si consiglia di utilizzare un database esterno, più resistente agli errori rispetto al database incorporato.
- Se si utilizza il database incorporato, non è richiesta un'installazione di componenti di terzi. È consigliato per l'utilizzo tipico.
- Il database incorporato non richiede le conoscenze di amministrazione di DBMS ed è una buona scelta per una rete antivirus di dimensioni piccole e medie.
- Si può utilizzare il database esterno nel caso di lavoro autonomo con il DBMS con l'accesso diretto al database. In questo caso, possono essere utilizzate le API standard di accesso ai database, per esempio OLE DB, ADO.NET o ODBC.

A1. Configurazione del driver ODBC

Per configurare l'utilizzo del DBMS esterno per la conservazione e l'elaborazione dei dati, vengono utilizzati i parametri riportati nella tabella **A-2** (i valori specifici sono riportati come esempio).

Tabella A-2. Parametri per la connessione ODBC

Nome	Valore	Descrizione
`DSN`	`drwcs`	Nome set dei dati
`USER`	`drwcs`	Nome utente
`PASS`	`fUqRbrmlvI`	Password
`TRANSACTION`	`DEFAULT`	Valori disponibili del parametro `TRANSACTION`: • `SERIALIZABLE` • `READ_UNCOMMITTED` • `READ_COMMITTED` • `REPEATABLE_READ` • `DEFAULT` Il valore predefinito `DEFAULT` significa "utilizza le impostazioni di default del server SQL". Per maggiori informazioni su livelli di isolamento di transazioni, consultare la documentazione del DBMS corrispondente.

Per escludere problemi con codifica, si devono disattivare i seguenti parametri del driver ODBC:

- **Utilizza le impostazioni regionali per l'output di valute, numeri, date e ore** — può causare errori di formattazione dei parametri numerici.

- **Esegui la conversione dei dati di tipo carattere** — può causare la visualizzazione non corretta dei caratteri nel Pannello di controllo per i parametri che provengono dal database. Imposta la dipendenza della visualizzazione dei caratteri dal parametro di lingua per i programmi che non utilizzano Unicode.

Quando viene creato un nuovo database nel DBMS Microsoft SQL, è necessario indicare un ordinamento tenendo conto della distinzione tra maiuscole e minuscole (suffisso `_CS`) e dei segni diacritici (suffisso `_AS`).

È indesiderato l'uso dei seguenti caratteri: spazio, "`{`", "`;`" e "`}`", per maggiori informazioni v. https://learn.microsoft.com/en-us/sql/odbc/reference/syntax/sqldriverconnect-function?redirectedfrom=MSDN&view=sql-server-ver15.

Il database stesso prima viene creato sul server SQL con i parametri indicati sopra.

Inoltre, è necessario configurare i parametri del driver ODBC per il computer su cui è installato il Server Dr.Web.

Le informazioni sulla configurazione del driver ODBC per i SO della famiglia UNIX sono disponibili a https://www.unixodbc.org/ sezione **Manuals**.

Configurazione del driver ODBC per il SO Windows

Per configurare i parametri del driver ODBC

1. Nel **Pannello di controllo** del SO Windows selezionare la voce **Amministrazione**, nella finestra che si è aperta fare doppio clic sull'icona **Origini dati (ODBC)**. Si apre la finestra **Amministratore origine dati ODBC**. Passare alla scheda **DSN di sistema**.
2. Premere il pulsante **Aggiungi**. Si apre la finestra di scelta del driver.
3. Selezionare nella lista la voce corrispondente al driver ODBC per questo database e premere il pulsante **Fine**. Si apre la prima delle finestre di configurazione dell'accesso al server dei database.

Se si utilizza un DBMS esterno, è necessario installare l'ultima versione del driver ODBC fornita insieme a questo DBMS. L'utilizzo del driver ODBC fornito insieme a SO Windows (SQL Server Native Client) è fortemente sconsigliato.

L'eccezione sono i database forniti da Microsoft senza il driver ODBC. Se si utilizza il DBMS MS SQL, è necessario installare e utilizzare la versione corrente del driver ODBC dal sito Microsoft.

4. Indicare i parametri di accesso all'origine dati che corrispondono a quelli indicati nelle impostazioni del Server Dr.Web. Se il server del database non si trova sullo stesso computer

del Server Dr.Web, indicare nel campo **Server** l'indirizzo IP o il nome del server del database. Premere il pulsante **Avanti**.

5. Selezionare l'opzione **autenticazione di account di SQL Server** e impostare le credenziali di utente per l'accesso al database. Premere il pulsante **Avanti**.
6. Dalla lista a cascata **Utilizza di default il database** selezionare il database utilizzato dal Server Dr.Web. In questo caso deve essere indicato obbligatoriamente il nome del database di Server Dr.Web, anziché il valore **Default**.

   Assicurarsi che siano impostati i seguenti flag: **Identificatori tra le virgolette nel formato ANSI**, **Valori null, Modelli e avvisi nel formato ANSI**. Premere il pulsante **Avanti**.

   Se durante la configurazione del driver ODBC c'è la possibilità di modificare la lingua dei messaggi di sistema del server SQL, è necessario impostare l'inglese.

7. Dopo aver finito di configurare i parametri, premere il pulsante **Fine**. Si apre la finestra con il riassunto dei parametri impostati.
8. Per controllare la correttezza delle impostazioni, premere il pulsante **Controlla origine dati**. Dopo aver visto l'avviso di controllo completato con successo, premere il pulsante **OK**.

A2. Configurazione del driver di database per Oracle

Descrizione generale

Oracle Database (o Oracle DBMS) — un DBMS relazionale a oggetti. Oracle può essere utilizzato come database esterno per Dr.Web Enterprise Security Suite.

Server Dr.Web può utilizzare DBMS Oracle come database esterno su tutte le piattaforme, ad eccezione di FreeBSD (v. p. Installazione e versioni supportate).

Per utilizzare DBMS Oracle

1. Installare una copia del database Oracle con le impostazioni di codifica `AL32UTF8`. Si può inoltre utilizzare una copia esistente del database con la codifica indicata.
2. Configurare il driver di database per l'utilizzo del database esterno corrispondente. Si può farlo nel file di configurazione oppure attraverso il Pannello di controllo: menu **Configurazione del Server Dr.Web**, scheda **Database**.

   Se si intende utilizzare come database esterno il database Oracle attraverso la connessione ODBC, nel corso dell'installazione (l'aggiornamento) di Server Dr.Web nelle impostazioni dell'installer annullare l'installazione del client incorporato per il DBMS Oracle (nella sezione **Supporto dei database** → **Driver del database Oracle**).

   Altrimenti, l'utilizzo del database Oracle attraverso ODBC non sarà possibile per conflitto di librerie.

È vietata la connessione al database Oracle con gli account degli utenti di sistema SYS e SYSTEM, nonché con i privilegi SYSDBA e SYSOPER.

Installazione e versioni supportate

Per poter utilizzare il database Oracle come database esterno, è necessario installare una copia di database Oracle e configurare per essa la codifica `AL32UTF8` (`CHARACTER SET AL32UTF8 / NATIONAL CHARACTER SET AL16UTF16`). Si può farlo nei seguenti modi:

1. Tramite l'installer del database Oracle (utilizzare la modalità avanzata di installazione e di configurazione del database).
2. Tramite il comando SQL `CREATE DATABASE`.

Per ulteriori informazioni sulla creazione e configurazione del database consultare la documentazione di database Oracle.

Se si utilizza una codifica diversa da quella indicata, i caratteri nazionali non verranno visualizzati in modo corretto.

Il client per l'accesso al database (Oracle Instant Client) fa parte del pacchetto di installazione di Dr.Web Enterprise Security Suite.

Le piattaforme supportate da DBMS Oracle sono riportate sul sito del produttore.

Le piattaforme supportate da Oracle Client sono riportate sul sito del produttore.

Dr.Web Enterprise Security Suite supporta il DBMS Oracle versione 11 e successive.

Prestare inoltre attenzione ai requisiti di sistema per il Server Dr.Web nel caso di utilizzo del database esterno Oracle (v. **Guida all'installazione**, p. Requisiti di sistema).

Parametri

Per configurare l'utilizzo del DBMS Oracle, vengono utilizzati i parametri descritti nella tabella **A-3**.

Tabella A-3. Parametri del DBMS Oracle

Parametro	Descrizione
`drworacle`	Nome driver
`User`	Nome utente del database (obbligatorio)

Parametro	Descrizione
`Password`	Password utente (obbligatorio)
`ConnectionString`	Stringa di connessione al database (obbligatorio)

La stringa di connessione al DBMS Oracle ha il seguente formato:

//<host>:<port>/<service name>

dove:

- *<host>* — indirizzo IP o nome del server Oracle;
- *<port>* — porta su cui il server è "in ascolto";
- *<service name>* — nome del database, a cui è necessario connettersi.

Per esempio:

```
//myserver111:1521/bjava21
```

dove:

- `myserver111` — nome del server Oracle.
- `1521` — porta su cui il server è "in ascolto".
- `bjava21` — nome del database, a cui è necessario connettersi.

Configurazione del driver di DBMS Oracle

Per usare il DBMS Oracle, è necessario modificare la definizione e le impostazioni del driver del database in uno dei seguenti modi:

- Nel Pannello di controllo: voce **Amministrazione** del menu principale → voce **Configurazione del Server Dr.Web** del menu di gestione → scheda **Database** → selezionare dalla lista a cascata **Database** il tipo **Oracle**, configurare le impostazioni secondo il formato riportato sopra.
- Nel file di configurazione del Server Dr.Web.

A3. Utilizzo del DBMS PostgreSQL

Descrizione generale

PostgreSQL — un DBMS relazionale a oggetti. È un'alternativa libera a un DBMS commerciale (Oracle Database, Microsoft SQL Server ecc.) In reti antivirus grandi DBMS PostgreSQL può essere utilizzato come database esterno per Dr.Web Enterprise Security Suite.

Per utilizzare PostgreSQL come database esterno

1. Installare il server PostgreSQL o Postgres Pro.
2. Configurare il Server Dr.Web per l'utilizzo del database esterno corrispondente. Si può farlo nel file di configurazione oppure attraverso il Pannello di controllo: nel menu **Configurazione del Server Dr.Web**, nella scheda **Database**.

Per la connessione al database PostgreSQL può essere utilizzata solo l'autenticazione trust, password e MD5.

Installazione e versioni supportate

1. Scaricare l'ultima versione del prodotto gratuito PostgreSQL (il server PostgreSQL e, se necessario, il relativo driver ODBC) oppure come minimo evitare di utilizzare le versioni precedenti alla **8.4** o alla 11.4.1 nel caso di Postgres Pro.
2. Creare un database PostgreSQL in uno dei seguenti modi:
   a) Attraverso l'interfaccia grafica `pgAdmin`.
   b) Tramite il comando SQL `CREATE DATABASE`.

Il database deve essere creato in codifica UTF8.

Il passaggio al database esterno è descritto in p. Cambio del tipo di database di Dr.Web Enterprise Security Suite.

Prestare inoltre attenzione ai requisiti di sistema per il Server Dr.Web nel caso di utilizzo del database esterno PostgreSQL (v. **Guida all'installazione**, p. Requisiti di sistema).

Parametri

Per configurare l'utilizzo del database PostgreSQL, vengono utilizzati i parametri descritti nella tabella **A-4**.

Tabella A-4. PostgreSQL

Nome	Valore predefinito	Descrizione
`host`	*<Socket UNIX locale>*	Host del server PostgreSQL
`port`		Porta del server PostgreSQL o l'estensione del nome di file del socket

Nome	Valore predefinito	Descrizione
dbname	drwcs	Nome del database
user	drwcs	Nome utente
password	drwcs	Password
options		Opzioni di tracciamento/debug da inviare al server
requiressl		• 1 per una richiesta di stabilire una connessione SSL • 0 per l'assenza di tale richiesta
temp_tablespaces		Namespace per le tabelle temporanee
default_transaction_isolation		Modalità di isolamento della transazione (v. documentazione di PostgreSQL)

Informazioni tecniche anche possono essere trovate sull'indirizzo https://www.postgresql.org/docs/.

Interazione del Server Dr.Web con il database PostgreSQL attraverso UDS

Se il Server Dr.Web e il database PostgreSQL sono installati sulla stessa macchina, è possibile configurare la loro interazione attraverso UDS (socket di dominio UNIX).

Per configurare l'utilizzo attraverso UDS

1. Nel file di configurazione del database PostgreSQL `postgresql.conf` trascrivere la seguente directory per UDS:

   ```
   unix_socket_directory = '/var/run/postgresql'
   ```

2. Riavviare PostgreSQL.

Configurazione del database PostgreSQL

Per migliorare le prestazioni nel caso di utilizzo del database PostgreSQL, è consigliato effettuare una configurazione basata su informazioni dai manuali database ufficiali.

Se viene utilizzato un database di grandi dimensioni e se sono disponibili le risorse di calcolo adeguate, è consigliato configurare i seguenti parametri nel file di configurazione `postgresql.conf`:

Impostazione minima:

```
shared_buffers = 256MB
```

```
temp_buffers = 64MB

work_mem = 16MB
```

Impostazione avanzata:

```
shared_buffers = 1GB

temp_buffers = 128MB

work_mem = 32MB

fsync = off

synchronous_commit = off

wal_sync_method = fdatasync

commit_delay = 1000

max_locks_per_transaction = 256

max_pred_locks_per_transaction = 256
```

Il parametro `fsync = off` migliora significativamente le prestazioni, ma può portare a una completa perdita di dati in caso di interruzione di corrente o di crash del sistema. La disattivazione del parametro `fsync` è consigliata se è disponibile un backup del database per la possibilità del completo ripristino del database.

L'impostazione del parametro `max_locks_per_transaction` può essere utile per fornire un'operazione ininterrotta nel caso di accesso massiccio alle tabelle del database, in particolare, durante l'aggiornamento del database a una versione nuova.

A4. Utilizzo del DBMS MySQL

Descrizione generale

MySQL — un sistema di gestione database relazionale libero multipiattaforma. Il DBMS MySQL può essere utilizzato come database esterno per Dr.Web Enterprise Security Suite.

Per utilizzare MySQL come database esterno

1. Installare il server MySQL.
2. Configurare il Server Dr.Web per l'utilizzo del database esterno corrispondente. Si può farlo nel file di configurazione oppure attraverso il Pannello di controllo: nel menu **Configurazione del Server Dr.Web**, nella scheda **Database**.

Installazione e versioni supportate

Dr.Web Enterprise Security Suite supporta le seguenti versioni del DBMS MySQL:

- MySQL — tutte le versioni a partire dalla 8.0.12,

> Assicurarsi che per l'utente attraverso cui viene effettuata la connessione a MySQL versione 8.X, il tipo di autenticazione corrisponda a caching_sha2_password. Questo parametro viene impostato durante l'installazione e diventa parametro di default per ciascun utente o viene configurato manualmente per ciascun utente.

- MariaDB — 10.2.2, 10.3, 10.4.

Dopo aver installato il DBMS e prima di creare un nuovo database, è necessario definire le seguenti impostazioni nel suo file di configurazione (per i dettagli consultare la documentazione del DBMS):

Per MySQL versioni 8.X:

```
[mysqld]

innodb_file_per_table = true

max_allowed_packet = 64M
```

Se la versione del DBMS MariaDB utilizzato è precedente alla 10.2.4, nel file di configurazione è inoltre necessario indicare:

```
binlog_format = mixed
```

Parametri

Per configurare l'utilizzo del DBMS MySQL, vengono utilizzati i parametri descritti nella tabella **A-5**.

Tabella A-5. Parametri del DBMS MySQL

Nome	Valore predefinito	Descrizione
HOST	localhost	• Per la connessione al database tramite TCP/IP — indirizzo del server del database. • Per l'utilizzo di UDS — percorso del file di socket UNIX. Se il percorso non è impostato, il Server Dr.Web cercherà di trovare il file nelle directory standard mysqld.

PORT	3306	• Per la connessione al database tramite TCP/IP — numero di porta per la connessione. • Per l'utilizzo di UDS — nome del file di socket UNIX.
DBNAME		Nome del database
USER		Nome dell'utente del database
PASSWORD	QUICK	Password dell'utente del database
PRECOMPILEDCACHE	1048576	Dimensione in byte della cache degli operatori sql precompilati
SSL	NO	Utilizza solamente le connessioni SSL: • YES — connettiti al database solo se viene utilizzato il protocollo SSL, • NO — il protocollo SSL non è obbligatorio per la connessione al database.

Allegato B. Autenticazione degli amministratori

Informazioni di base sull'autenticazione di amministratori sul Server Dr.Web sono riportate nel **Manuale dell'amministratore**, nel p. Autenticazione di amministratori.

B1. Autenticazione in caso di utilizzo di Active Directory

Vengono configurati solo il permesso di uso e l'ordine nella lista degli autenticatori: i tag `<enabled/>` e `<order/>` in `auth-ads.conf`.

Come funziona:

1. L'amministratore definisce il nome utente e la password in uno dei seguenti formati:
   - `username`,
   - `domain\username`,
   - `username@domain`,
   - LDAP DN dell'utente.
2. Con questo nome utente e questa password il Server Dr.Web si registra sul controller di dominio predefinito (o sul controller di dominio per il dominio specificato nel nome utente).
3. Se la registrazione non è riuscita, si passa al meccanismo di autenticazione successivo.
4. Viene determinato LDAP DN dell'utente registrato.
5. Nell'oggetto che ha il DN calcolato viene letto l'attributo `DrWebAdmin`. Se è impostato come `FALSE` — mancato successo e passaggio al meccanismo di autenticazione successivo.
6. Se in questa fase alcuni attributi non sono determinati, vengono cercati nei gruppi di cui fa parte questo utente. Per ciascun gruppo vengono controllati anche i suoi gruppi padre (la strategia di ricerca in profondità).

In caso di qualsiasi errore viene effettuato il passaggio al meccanismo di autenticazione successivo.

L'utility `drweb-<versione_pacchetto>-<build>-esuite-modify-ad-schema-<versione_SO>.exe` (è fornita separatamente dal pacchetto Server Dr.Web) crea una nuova classe di oggetti `DrWebEnterpriseUser` per Active Directory e descrive nuovi attributi per questa classe.

Gli attributi hanno i seguenti OID nello spazio Enterprise:

```
DrWeb_enterprise_OID "1.3.6.1.4.1" // iso.org.dod.internet.private.enterprise
DrWeb_DrWeb_OID DrWeb_enterprise_OID ".29690" // DrWeb
DrWeb_EnterpriseSuite_OID DrWeb_DrWeb_OID ".1" // EnterpriseSuite
```

```
DrWeb_Alerts_OID DrWeb_EnterpriseSuite_OID ".1" // Alerts
DrWeb_Vars_OID DrWeb_EnterpriseSuite_OID ".2" // Vars
DrWeb_AdminAttrs_OID DrWeb_EnterpriseSuite_OID ".3" // AdminAttrs

// 1.3.6.1.4.1.29690.1.3.1 (AKA
iso.org.dod.internet.private.enterprise.DrWeb.EnterpriseSuite.AdminAttrs.Admin)

DrWeb_Admin_OID DrWeb_AdminAttrs_OID ".1" // R/W admin
DrWeb_AdminReadOnly_OID DrWeb_AdminAttrs_OID ".2" // R/O admin
DrWeb_AdminGroupOnly_OID DrWeb_AdminAttrs_OID ".3" // Group admin
DrWeb_AdminGroup_OID DrWeb_AdminAttrs_OID ".4" // Admin's group
DrWeb_Admin_AttrName "DrWebAdmin"
DrWeb_AdminReadOnly_AttrName "DrWebAdminReadOnly"
DrWeb_AdminGroupOnly_AttrName "DrWebAdminGroupOnly"
DrWeb_AdminGroup_AttrName "DrWebAdminGroup"
```

Le proprietà degli utenti Active Directory vengono modificate manualmente sul server Active Directory (v. **Manuale dell'amministratore**, p. Autenticazione degli amministratori).

I permessi vengono assegnati agli amministratori secondo il principio generale di ereditarietà nella struttura gerarchica dei gruppi di cui fa parte un amministratore.

B2. Autenticazione in caso di utilizzo di LDAP

Le impostazioni sono riportate nel file di configurazione `auth-ldap.conf`.

I tag principali del file di configurazione sono:

- `<enabled/>` e `<order/>` — sono analoghi alla variante per Active Directory.
- `<server/>` imposta l'indirizzo del server LDAP. È possibile specificare più tag `<server/>` con gli indirizzi di server LDAP diversi, di conseguenza, verrà creata una lista di server su cui può essere eseguita l'autenticazione. Per primo deve essere indicato l'indirizzo del server principale su cui è previsto il carico massimo, dopo cui possono essere indicati gli indirizzi dei server di riserva. Alla connessione dell'amministratore, viene utilizzato il primo server LDAP disponibile. In caso di errore, verrà effettuato un tentativo di autenticazione sul server successivo e così via nell'ordine in cui gli indirizzi dei server LDAP sono specificati nel file di configurazione.
- `<user-dn/>` determina le regole di traduzione dei nomi in DN con l'impiego di maschere analoghe a maschere DOS.

  Nel tag `<user-dn/>` è ammesso l'utilizzo dei caratteri jolly:

  - `*` sostituisce una sequenza di caratteri ad eccezione di `.` `,` `=` `@` `\` e di spazi;
  - `#` sostituisce una sequenza di caratteri.
- `<user-dn-expr/>` determina le regole di traduzione dei nomi in DN con l'impiego di espressioni regolari.

  Per esempio, questa è la stessa regola in diverse varianti:

```
<user-dn user="*@example.com" dn="CN=\1,DC=example,DC=com"/>
<user-dn-expr user="(.*)@example.com" dn="CN=\1,DC=example,DC=com"/>
```

`\1` .. `\9` determina il posto per mettere nel pattern i valori *, # o espressioni tra parentesi.

Secondo questo principio: se il nome utente è scritto come `login@example.com`, in seguito alla traduzione risulta il DN: "`CN=login,DC=example,DC=com`".

- `<user-dn-extension-enabled/>` consente l'esecuzione dello script Lua `ldap_user_dn_translate.ds` (dalla directory `extensions`) per eseguire la traduzione del nome utente in DN. Questo script viene eseguito dopo i tentativi di applicare tutte le regole `user-dn`, `user-dn-expr` se non è stata trovata nessuna regola adatta. Lo script ha un singolo parametro — il nome utente inserito. Lo script restituisce una stringa che contiene DN o nulla. Se non è stata trovata nessuna regola adatta e lo script non è consentito o non ha restituito nulla, il nome utente inserito viene utilizzato così com'è.
- L'attributo dell'oggetto LDAP per il DN ottenuto come risultato di traduzione e i suoi possibili valori possono essere ridefiniti dal seguente tag (sono indicati i valori di default):

```
<!-- DrWebAdmin attribute equivalent (OID 1.3.6.1.4.1.29690.1.3.1) -->
<admin-attribute-name value="DrWebAdmin" true-value="^TRUE$" false-value="^FALSE$"/>
```

  Come valori di parametri `true-value`/`false-value` vengono impostate espressioni regolari.
- Se sono rimasti valori non definiti dell'attributo amministratore, nel caso in cui nel file di configurazione viene impostato il tag `<group-reference-attribute-name value="memberOf"/>`, il valore dell'attributo `memberOf` viene considerato come una lista di gruppi DN in cui rientra questo amministratore, e la ricerca degli attributi richiesti in questi gruppi viene eseguita allo stesso modo del caso di uso di Active Directory.

B3. Autenticazione in caso di utilizzo di LDAP/AD

File di configurazione

Le impostazioni sono riportate nel file di configurazione `auth-ldap-rfc4515.conf`.

Sono inoltre disponibili i file di configurazione con le impostazioni standard:

- `auth-ldap-rfc4515-check-group.conf` — modello di file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato con la verifica dell'appartenenza al gruppo di Active Directory.
- `auth-ldap-rfc4515-check-group-novar.conf` — modello di file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato con la verifica dell'appartenenza al gruppo di Active Directory con l'uso delle variabili.
- `auth-ldap-rfc4515-check-group.conf` — modello di file di configurazione dell'autenticazione esterna degli amministratori attraverso LDAP in base a uno schema semplificato.

I tag principali del file di configurazione auth-ldap-rfc4515.conf:

- `<server />` — definizione del server LDAP.

Attributo	Descrizione	Valore predefinito
`base-dn`	DN dell'oggetto relativamente a cui viene effettuata la ricerca.	Valore dell'attributo `rootDomainNamingContext` dell'oggetto `Root DSE`
`cacertfile`	File dei certificati radice (solo UNIX).	–
`host`	Indirizzo del server LDAP.	• Controller di dominio per il server sotto SO Windows. • `127.0.0.1` per il server sotto SO della famiglia UNIX. • È possibile specificare più tag `<server />` con gli indirizzi di server LDAP diversi. Per primo deve essere indicato l'indirizzo del server principale su cui è previsto il carico massimo. In caso di errore, verrà effettuato un tentativo di autenticazione sul server successivo e così via nell'ordine indicato.
`scope`	Area di ricerca. Valori ammissibili: • `sub-tree` — l'intera area sotto il DN di base, • `one-level` — discendenti diretti del DN di base, • `base` — DN di base.	`sub-tree`
`tls`	Stabilisci TLS per la connessione a LDAP.	`no`
`ssl`	Utilizza il protocollo LDAPS per la connessione a LDAP.	`no`

- `<set />` — impostazione delle variabili tramite la ricerca LDAP.

Attributo	Descrizione	Valore predefinito
`attribute`	Nome dell'attributo il cui valore viene assegnato alla variabile. L'assenza è inammissibile.	–
`filter`	RFC4515 filtro di ricerca LDAP.	–
`scope`	Area di ricerca. Valori ammissibili: • `sub-tree` — l'intera area sotto il DN di base, • `one-level` — discendenti diretti del DN di base, • `base` — DN di base.	`sub-tree`

Attributo	Descrizione	Valore predefinito
search	DN dell'oggetto relativamente a cui viene effettuata la ricerca.	Se è assente, viene utilizzato base-dn del tag <server />
variable	Nome della variabile. Deve iniziare con una lettera e contenere solo lettere e cifre. L'assenza è inammissibile.	–

Le variabili possono essere utilizzate nei valori dell'attributo add dei tag <mask /> ed <expr />, nel valore dell'attributo value del tag <filter /> in forma di \varname, nonché nel valore dell'attributo search del tag <set />. Il livello di ricorsione ammissibile per l'espansione delle variabili è 16.

Se la ricerca restituisce più oggetti trovati, viene utilizzato solo il primo.

- <mask /> — modelli di nome utente.

Attributo	Descrizione
add	Stringa che viene aggiunta al filtro di ricerca per operatore AND con elementi di sostituzione.
user	Maschera di nome utente con l'utilizzo dei metacaratteri di tipo DOS * e #. L'assenza è inammissibile.

Per esempio:

```
<mask user="*@#"  add="sAMAccountName=\1" />

<mask user="*\*"  add="sAMAccountName=\2" />
```

\1 e \2 — link alle maschere coincidenti nell'attributo user.

- <expr /> — modelli di nome utente con l'utilizzo delle espressioni regolari (gli attributi sono identici a <mask />).

  Per esempio:

```
<expr user="^(.*)@([^.,=@\s\\]+)$"  add="sAMAccountName=\1" />

<expr user="^(.*)\\(.*)"            add="sAMAccountName=\2" />
```

  Corrispondenza delle maschere e delle espressioni regolari:

Maschera	Espressione regolare
*	.*
#	[^.,=@\s\\]+

- <filter /> — filtro di ricerca LDAP.

Attributo	Descrizione
value	Stringa che viene aggiunta al filtro di ricerca per operatore AND con elementi di sostituzione.

Concatenazione di filtri

```
<set variable="admingrp"  filter="&amp;(objectclass=group)(cn=ESuite Admin)"
attribute="dn" />
<mask user="*\*" add="sAMAccountName=\2" />
<filter value="&amp;(objectClass=user)(memberOf=\admingrp)" />
```

Se come risultato della ricerca `admingrp` assumerà il valore `"CN=ESuite Admins,OU=some name,DC=example,DC=com"`, e l'utente ha immesso `domain\user`, il risultato è il filtro:

```
"(&(sAMAccountName=user)(&(objectClass=user)(memberOf=CN=ESuite
Admins,OU=some name,DC=example,DC=com)))"
```

Esempio di configurazione dell'autenticazione LDAP/AD

Di seguito è riportato un esempio di impostazioni tipiche per l'autenticazione tramite LDAP. Le impostazioni vengono configurate nel Pannello di controllo, sezione **Amministrazione** → **Autenticazione** → **Autenticazione LDAP/AD** (per la variante **Impostazioni semplificate**).

Parametri iniziali per gli amministratori che devono autenticarsi:

- dominio: `dc.test.local`
- gruppo in Active Directory: `DrWeb_Admins`

Impostazioni del Pannello di controllo:

Nome dell'impostazione		Valore
Tipo di server		Microsoft Active Directory
Indirizzo del server		dc.test.local
Modelli di nome utente per la conferma dell'autentificazione	Maschera dell'account	test* o *@test.local
	Nome utente	\1
Appartenenza degli utenti per la conferma dell'autentificazione	Nome	DrWeb_Admins
	Tipo	gruppo

B4. Sezioni subordinate dei permessi

Tabella B-1. Lista dei permessi di amministratori e le loro caratteristiche

Codice	Permesso	Descrizione	Sezione del Pannello di controllo
Gestione dei gruppi di postazioni			
1*	**Visualizzazione delle proprietà dei gruppi di postazioni**	Una lista dei gruppi custom che un amministratore vede nella rete antivirus. Anche tutti i gruppi di sistema vengono visualizzati nell'albero, ma in loro sono visibili soltanto le postazioni appartenenti ai gruppi dalla lista indicata. Se il permesso è concesso solo per singoli gruppi, e non per tutta la rete antivirus, la voce di menu **Amministrazione** → **Installazioni** → **Installazione via rete** non è disponibile.	Rete antivirus Rete antivirus → Generali → Proprietà
2*	**Modifica delle proprietà dei gruppi di postazioni**	Una lista dei gruppi custom di cui le proprietà l'amministratore può modificare. Deve contenere i gruppi dalla lista del permesso 1.	
3	**Visualizzazione della configurazione dei gruppi di postazioni**	Una lista dei gruppi custom di cui la configurazione può essere visualizzata dall'amministratore. Inoltre, l'amministratore può visualizzare la configurazione delle postazioni per cui i gruppi dalla lista sono primari. Deve contenere i gruppi dalla lista del permesso 1.	Rete antivirus Rete antivirus → Generali → Componenti in esecuzione Rete antivirus → Generali → Quarantena
4	**Modifica della configurazione dei gruppi di postazioni**	È simile al permesso 3, ma con la possibilità di modifica. Deve contenere i gruppi dalla lista del permesso 3.	Pagine dalla sezione **Configurazione** del menu di gestione
5	**Visualizzazione delle proprietà delle postazioni**	Una lista dei gruppi custom che sono gruppi primari per le postazioni di cui le proprietà possono essere visualizzate dall'amministratore.	Rete antivirus Rete antivirus → Generali → Proprietà

Codice	Permesso	Descrizione	Sezione del Pannello di controllo
		Deve contenere i gruppi dalla lista del permesso 1.	
6	**Modifica delle proprietà delle postazioni**	Comprese le proprietà dell'ACL, del blocco, dell'ammissione ecc. È simile al permesso 5, ma con la possibilità di modifica. Deve contenere i gruppi dalla lista del permesso 5.	
8*	**Inserimento di postazioni in gruppi ed eliminazione di postazioni dai gruppi**	Una lista dei gruppi custom. Deve contenere i gruppi dalla lista del permesso 1.	Rete antivirus
9	**Rimozione di postazioni**	Una lista dei gruppi custom che sono gruppi primari per le postazioni che l'amministratore può rimuovere. Deve contenere i gruppi dalla lista del permesso 1.	
10	**Installazione e disinstallazione di Agent su remoto**	Una lista dei gruppi custom, sulle cui postazioni l'amministratore può avviare un'installazione remota degli Agent Dr.Web con gli ID selezionati. Questi gruppi devono essere primari per le postazioni che vengono installate. Deve contenere i gruppi dalla lista del permesso 1. Se ci sono oggetti vietati, la voce non viene visualizzata nel menu. L'installazione via rete è possibile solo da /esuite/network/index.ds a condizione che il permesso 16 sia concesso.	
11	**Unione delle postazioni**	Una lista dei gruppi custom, le postazioni da cui possono essere unite. Questi gruppi devono essere primari per le postazioni. L'icona di unione di postazioni è disponibile nella barra degli strumenti. Deve contenere i gruppi dalla lista del permesso 1.	

Codice	Permesso	Descrizione	Sezione del Pannello di controllo
12*	**Visualizzazione di tabelle statistiche**	Lista dei gruppi custom per cui l'amministratore può visualizzare le statistiche. Il permesso dà la possibilità di creare un task nel calendario di Server Dr.Web per la ricezione di report periodici. Viene impostata una lista di gruppi custom che l'amministratore può indicare in questo task (i gruppi le cui postazioni verranno incluse nei report). Se è impostato il gruppo Everyone, i report includeranno tutti i gruppi dalla lista. Deve contenere i gruppi dalla lista del permesso 1.	Rete antivirus pagine dalla sezione **Statistiche** del menu di gestione
23	**Modifica delle informazioni su licenze**	Una lista dei gruppi custom per cui l'amministratore può aggiungere/sostituire/eliminare la chiave di licenza Questi gruppi devono essere primari per le postazioni. Deve contenere i gruppi dalla lista del permesso 1.	Rete antivirus → Configurazione → Chiavi di licenza
40	**Avvio e arresto dei componenti**	Avvio e arresto dei componenti installati sulla postazione.	Rete antivirus → Configurazione → Permessi
48	**Visualizzazione dei report per il supporto tecnico**	Creazione e visualizzazione dei log di sistema dei componenti di protezione installati sulla postazione.	Rete antivirus → Generali → Report per il supporto tecnico
Gestione degli amministratori			
18	**Visualizzazione del calendario del Server Dr.Web**	Visualizzazione della tabella **Log di esecuzione dei task**. Per la visualizzazione sono disponibili i task creati dall'amministratore, nonché dagli amministratori dal gruppo selezionato. Se i permessi 12 e 18 non sono concessi, è vietata la visualizzazione della pagina con il calendario del Server Dr.Web. Se è concesso il 12 e non è concesso il 18, è disponibile la visualizzazione del calendario per le statistiche.	Amministrazione → Configurazione → Scheduler del Server Dr.Web Amministrazione → Logs → Log di esecuzione dei task

Codice	Permesso	Descrizione	Sezione del Pannello di controllo
		Il task di invio di report per un amministratore specifico viene visualizzato a seconda della disponibilità del permesso 12 e della disponibilità dell'avviso **Report periodico**, anche se il permesso 18 non è concesso.	
19	**Modifica del calendario del Server Dr.Web**	Per la modifica sono disponibili i task creati dall'amministratore, nonché dagli amministratori dal gruppo selezionato.	Amministrazione → Configurazione → Scheduler del Server Dr.Web
24	**Modifica della configurazione degli avvisi**		Amministrazione → Avvisi → Configurazione degli avvisi Amministrazione → Avvisi → Avvisi non inviati Amministrazione → Avvisi → Avvisi della web console
25	**Creazione di amministratori, di gruppi di amministratori**	Inoltre viene nascosta l'icona corrispondente nella barra degli strumenti.	Amministrazione → Configurazione → Amministratori
26	**Modifica degli account amministratori**	Un amministratore dal gruppo **Newbies** vede un albero di amministratori di cui la radice è il gruppo in cui si trova, cioè vede gli amministratori dal suo gruppo e dai sottogruppi. Un amministratore dal gruppo **Administrators** vede tutti gli altri amministratori a prescindere dai loro gruppi. L'amministratore può modificare gli account degli amministratori dai gruppi indicati. In questo caso diventa disponibile la relativa icona nella barra degli strumenti.	
27	**Eliminazione degli account amministratori**	È simile al permesso 26.	
28	**Visualizzazione delle proprietà e della configurazione dei gruppi di amministratori**	Compresi gli amministratori nei gruppi e sottogruppi. L'amministratore può scegliere soltanto dal sottogruppo del suo gruppo padre.	

Codice	Permesso	Descrizione	Sezione del Pannello di controllo
29	**Modifica delle proprietà e della configurazione dei gruppi di amministratori**	Compresi gli amministratori nei gruppi e sottogruppi. L'amministratore può scegliere soltanto dal sottogruppo del suo gruppo padre. Se questo permesso non è concesso, allora anche se il permesso 26 sia concesso per questo gruppo, l'amministratore non potrà disattivare l'ereditarietà o aumentare i permessi di un amministratore nel gruppo.	
39	**Visualizzazione del gruppo di amministratori “Newbies”**	Per consentire all'amministratore di vedere il gruppo predefinito **Newbies** nell'albero degli amministratori. Se l'amministratore non ha i permessi di visualizzazione del gruppo **Newbies**, e lui stesso si trova in questo gruppo, lui vedrà solo se stesso.	
41	**Modifica degli avvisi di amministratori**	Modifica della configurazione degli avvisi agli amministratori.	
Avanzate			
7	**Creazione di postazioni**	Quando si crea una postazione, è disponibile una lista dei gruppi con il permesso 8 (il gruppo in cui le postazioni vengono messe deve avere il permesso 8). Quando si crea una postazione, uno dei gruppi custom disponibili deve diventare il suo gruppo primario.	Rete antivirus
13	**Visualizzazione della verifica**	La verifica è disponibile per un amministratore con i permessi completi e per gli oggetti con il permesso 4.	Amministrazione → Logs → Log di verifica
16	**Avvio dello Scanner di rete**	Se il permesso non è assegnato, l'installazione via rete da /esuite/network/index.ds non è disponibile.	Rete antivirus Amministrazione → Scanner di rete
17	**Approvazione di nuovi arrivi**	È disponibile la lista dei gruppi dal permesso 8.	Rete antivirus

Codice	Permesso	Descrizione	Sezione del Pannello di controllo
		Questo permesso non può essere assegnato se per l'amministratore è consentita la gestione solo di alcuni gruppi e non di tutti gli oggetti della rete antivirus. Cioè per il permesso 1 (**Visualizzazione delle proprietà dei gruppi di postazioni**) è impostato un set di gruppi.	
20	**Visualizzazione della configurazione del Server Dr.Web e di quella del repository**		Amministrazione → Configurazione → Configurazione del web server
21	**Modifica della configurazione del Server Dr.Web e di quella del repository**		Amministrazione → Repository → Stato del repository Amministrazione → Repository → Aggiornamenti differiti Amministrazione → Repository → Configurazione generale del repository Amministrazione → Repository → Configurazione dettagliata del repository Amministrazione → Repository → Contenuti del repository Amministrazione → Logs → Log di aggiornamento del repository Amministrazione → Configurazione → Procedure personalizzate Amministrazione → Server Dr.Web → Elenco delle versioni
22	**Visualizzazione delle informazioni su licenze**		Amministrazione → Amministrazione →

Codice	Permesso	Descrizione	Sezione del Pannello di controllo
			Gestione licenze
30	**Utilizzo di Web API**		-
31	**Visualizzazione delle relazioni tra i server**		Relazioni
32	**Modifica delle relazioni tra i server**		Relazioni
33	**Utilizzo delle funzioni addizionali**	Restringe l'accesso a tutte le schede della sezione **Funzioni addizionali**, ad eccezione della scheda **Utility** che è sempre disponibile.	Amministrazione → Funzioni addizionali
34	**Aggiornamento del repository**	Aggiornamento del repository del Server Dr.Web da SAM.	Il pulsante **Aggiorna il repository** nella sezione **Stato del repository**
42	**Modifica delle proprie impostazioni**	Permesso per modificare le proprie impostazioni dell'account amministratore.	Amministrazione → Configurazione → Amministratori
43	**Visualizzazione dei Server proxy Dr.Web**	Permesso di visualizzare le impostazioni dei Server proxy Dr.Web (se la visualizzazione è disattivata, anche la modifica viene automaticamente disattivata).	Rete antivirus → Proxy
44	**Modifica dei Server proxy Dr.Web**	Permesso di modificare le impostazioni dei Server proxy Dr.Web.	Rete antivirus → Proxy
45	**Visualizzazione delle proprietà e della configurazione dei criteri**	Se la visualizzazione è disattivata, anche la modifica viene automaticamente disattivata.	Rete antivirus → Criteri
46	**Modifica delle proprietà e della configurazione dei criteri**		Rete antivirus → Criteri
47	**Modifica delle regole di appartenenza**	Permesso di modificare le regole di appartenenza dei gruppi personalizzati.	Rete antivirus

* I permessi 1, 2, 8, 12 vengono definiti per una postazione secondo la lista dei gruppi di cui fa parte e non secondo il gruppo primario della postazione.

Se la postazione rientra in un gruppo e per questo gruppo sono concessi alcuni di questi permessi, allora per l'amministratore sarà disponibile il set di funzionalità che corrisponde a questi permessi a prescindere da ciò se il gruppo consentito è primario per la postazione. In questo caso il gruppo consentito ha priorità superiore: se la postazione rientra contemporaneamente in un gruppo consentito e in uno vietato, per l'amministratore saranno disponibili le funzionalità che corrispondono ai permessi del gruppo consentito.

Allegato C. Sistema di avviso

Le informazioni di base sulla configurazione degli avvisi dell'amministratore sono riportate nel **Manuale dell'amministratore**, in p. Configurazione degli avvisi.

C1. Descrizione dei parametri del sistema di avviso

Il sistema di avviso, che informa su eventi relativi al funzionamento dei componenti della rete antivirus, utilizza i seguenti tipi di invio degli avvisi:

- avvisi via email,
- avvisi attraverso la console web,
- avvisi attraverso SNMP,
- avvisi attraverso il protocollo di Agent Dr.Web,
- notifiche push,
- notifiche attraverso il protocollo Syslog.

A seconda del metodo di invio di avvisi, sono richiesti vari set di parametri nella forma opzione → valore. Per ogni metodo, vengono impostati i seguenti parametri:

Tabella C-1. Parametri generali

Parametro	Descrizione	Valore predefinito	Obbligatorio
`TO`	Insieme di destinatari dell'avviso divisi dal carattere |		sì
`ENABLED`	Attivazione o disattivazione dell'avviso	`true` o `false`	sì
`_TIME_TO_LIVE`	Numero di tentativi di invio ripetuto dell'avviso in caso di mancato invio	10 tentativi	no
`_TRY_PERIOD`	Periodo in secondi tra i tentativi di invio ripetuto dell'avviso	5 min, (invia non più spesso di una volta ogni 5 min)	no

Di seguito sono riportate le tabelle con le liste dei parametri per diversi metodi di invio di avvisi.

Tabella C-2. Avvisi via email

Parametro	Descrizione	Valore predefinito
FROM	Indirizzo email del mittente	drwcsd@${nome host}
TO	Indirizzi email dei destinatari	-
HOST	Indirizzo del server SMTP	127.0.0.1
PORT	Numero di porta del server SMTP	• 25, se il parametro SSL assume il valore no • 465, se il parametro SSL assume il valore yes
USER	Utente del server SMTP	"" se è impostato, è necessario attivare almeno un metodo di autenticazione, altrimenti la posta non verrà trasmessa.
PASS	Password dell'utente del server SMTP	""
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.	yes
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.	no
AUTH-CRAM-MD5	Utilizza l'autenticazione CRAM-MD5	no
AUTH-PLAIN	Utilizza l'autenticazione PLAIN	no
AUTH-LOGIN	Utilizza l'autenticazione LOGIN	no
AUTH-NTLM	Utilizza l'autenticazione NTLM	no
SSL-VERIFYCERT	Verifica la correttezza del certificato SSL del server	no
DEBUG	Attiva la modalità di debug, per esempio per analizzare le situazioni quando l'autenticazione non è possibile	-

Tabella C-3. Avvisi attraverso la Console web

Parametro	Descrizione	Valore predefinito
`TO`	UUID degli amministratori a cui verrà spedito questo messaggio	-
`SHOW_PERIOD`	Tempo in secondi di conservazione del messaggio, a partire dal momento della ricezione del messaggio	86400 secondi, cioè un giorno.

Tabella C-4. Avvisi attraverso SNMP

Parametro	Descrizione	Valore predefinito
`TO`	L'entità SNMP di ricezione, per esempio un indirizzo IP	-
`DOMAIN`	Dominio	• `localhost` in caso di SO Windows, • "" — in caso di SO della famiglia UNIX.
`COMMUNITY`	Community SNMP o contesto	`public`
`RETRIES`	Numero di tentativi ripetuti dell'invio dell'avviso da parte dell'API	5 tentativi
`TIMEOUT`	Tempo in secondi dopo il quale l'API riprova a spedire l'avviso	5 secondi

Tabella C-5. Avvisi attraverso il protocollo di Agent

Parametro	Descrizione	Valore predefinito
`TO`	UUID delle postazioni che ricevono l'avviso	-
`SHOW_PERIOD`	Tempo in secondi di conservazione del messaggio, a partire dal momento della ricezione del messaggio	86400 secondi, cioè un giorno.

Tabella C-6. Notifiche push

Parametro	Descrizione	Valore predefinito
`TO`	I token di dispositivi che le applicazioni ricevono al momento della registrazione su server di produttore, per esempio di Apple	-

Parametro	Descrizione	Valore predefinito
SERVER_URL	URL relay del server attraverso cui gli avvisi vengono trasmessi sul server di produttore	-

Tabella C-7. Notifiche tramite protocollo Syslog

Parametro	Descrizione	Valore predefinito
TO	Indirizzo del destinatario della notifica tramite protocollo Syslog. Il protocollo di trasmissione è TCP o UDP.	UDP, porta 514
FORMAT	Formato della notifica: RFC 5424 o CEF (Common Event Format).	RFC 5424
TIMEOUT	Periodo in secondi durante cui Server Dr.Web tenta di connettersi al destinatario della notifica tramite protocollo TCP.	5 s
FACILITY	Categoria del processo che ha generato la notifica (per esempio, kernel, sistema di posta). Assume i valori compresi tra 0 e 23.	14
HOSTNAME	Mittente. Identificatore di Server Dr.Web (nome di dominio completo, nome host, indirizzo IP).	-

C2. Parametri dei modelli di avviso

I testi dei messaggi vengono generati da un componente di Server Dr.Web, chiamato motore dei modelli, sulla base dei file dei modelli.

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 versioni successive non supportano il servizio Windows Messenger.

Il file di modello è costituito da testo e da variabili tra parentesi graffe. Quando si modificano i file di modello, si possono utilizzare le variabili riportate di seguito.

Le variabili vengono scritte in uno dei seguenti modi:

- {<*VAR*>} — per sostituire direttamente il valore della variabile <*VAR*>.
- {<*VAR*>:<*N*>} — i primi <*N*> caratteri della variabile <*VAR*>.
- {<*VAR*>:<*first*>:<*N*>} — <*N*> caratteri della variabile <*VAR*>, che seguono dopo i <*first*> primi (partendo dal carattere <*first*>+1), se il resto è meno, si aggiungono degli spazi a destra.

- {<*VAR*>:<*first*>:-<*N*>} — <*N*> caratteri della variabile <*VAR*>, che seguono dopo i <*first*> primi (partendo dal carattere <*first*>+1), se il resto è meno, si aggiungono degli spazi a sinistra.
- {<*VAR*>/<*original1*>/<*replace1*>[/<*original2*>/<*replace2*>]} — sostituzione dei caratteri indicati della variabile <*VAR*> con i valori indicati: i caratteri <*original1*> vengono sostituiti con i caratteri <*replace1*>, se disponibili, i caratteri <*original2*> vengono sostituiti con i caratteri <*replace2*> ecc.

  Il numero di coppie di sostituzione non è limitato.
- {<*VAR*>/<*original1*>/<*replace1*[{<*SUB_VAR*>}]>[/<*original2*>/<*replace2*>]} — simile alle sostituzioni con i valori impostati di cui sopra, ma con l'uso della variabile annidata <*SUB_VAR*>. Le azioni con variabili annidate sono simili a tutte le azioni con variabili padre.

  La profondità di annidamento per sostituzioni ricorsive non è limitata.
- {<*VAR*>/<*original1*>/<*replace1*>/<*original2*>/<*replace2*>/*/<*replace3*>} — simile alle sostituzioni con i valori impostati di cui sopra, ma è anche possibile utilizzare la sostituzione con il valore impostato in <*replace3*>, se non corrisponde nessuno dei valori originali elencati. Inoltre, se in <*VAR*> non si trova né <*original1*> né <*original2*>, tutti i valori saranno sostituiti con <*replace3*>.

Tabella C-8. Modo di scrittura delle variabili

Variabile	Valore	Espressione	Risultato
SYS.TIME	10:35:17:456	{SYS.TIME:5}	10:35
SYS.TIME	10:35:17:456	{SYS.TIME:3:5}	35:17
SYS.TIME	10:35:17:456	{SYS.TIME:3:-12}	°°°35:17:456
SYS.TIME	10:35:17:456	{SYS.TIME:3:12}	35:17:456°°°
SYS.TIME	10:35:17:456	{SYS.TIME/10/99/35/77}	99:77:17:456

Segni convenzionali

° — carattere di spazio.

Variabili di ambiente

Per creare i testi dei messaggi, si possono utilizzare le variabili di ambiente del processo Server Dr.Web (utente **System**).

Le variabili di ambiente sono disponibili nell'editor di messaggi del Pannello di controllo, nella lista a cascata **ENV**. Notare: le variabili devono contenere il prefisso `ENV.` (dopo il prefisso c'è un punto).

Variabili di sistema

- `SYS.BRANCH` — versione degli Agent Dr.Web e del Server Dr.Web,
- `SYS.BUILD` — data della build del Server Dr.Web,
- `SYS.DATE` — data di sistema attuale,
- `SYS.DATETIME` — data e ora di sistema attuali,
- `SYS.HOST` — nome DNS del Server Dr.Web,
- `SYS.MACHINE` — indirizzo di rete del computer su cui è installato il Server Dr.Web,
- `SYS.OS` — nome del sistema operativo sul computer su cui è installato il Server Dr.Web,
- `SYS.PLATFORM` — piattaforma del Server Dr.Web,
- `SYS.PLATFORM.SHORT` — variante breve di `SYS.PLATFORM`,
- `SYS.SERVER` — nome del prodotto (Dr.Web Server),
- `SYS.TIME` — ora di sistema attuale,
- `SYS.VERSION` — versione del Server Dr.Web.

Variabili generali per le postazioni

- `GEN.LoginTime` — ora della connessione della postazione,
- `GEN.StationAddress` — indirizzo della postazione,
- `GEN.StationDescription` — descrizione della postazione,
- `GEN.StationID` — identificatore della postazione univoco,
- `GEN.StationLDAPDN` — nome distinto (distinguished name) di una postazione con il sistema operativo Windows. Viene utilizzato per le postazioni che rientrano in un dominio ADS/LDAP,
- `GEN.StationMAC` — indirizzo MAC della postazione,
- `GEN.StationName` — nome della postazione,
- `GEN.StationPrimaryGroupID` — identificatore del gruppo primario della postazione,
- `GEN.StationPrimaryGroupName` — nome del gruppo primario della postazione,
- `GEN.StationSID` — identificatore di sicurezza della postazione.

Variabili generali per il repository

- `GEN.CurrentRevision` — identificatore attuale della versione,
- `GEN.Folder` — directory in cui si trova il prodotto,
- `GEN.NextRevision` — identificatore della versione aggiornata,
- `GEN.Product` — descrizione del prodotto.

Parametri e variabili degli avvisi per tipo

Amministratori

Amministratore sconosciuto

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se nel Pannello di controllo ha tentato di autenticarsi un amministratore con un nome utente sconosciuto.	
Ulteriore configurazione	Non richiesta.	
Variabili	`MSG.Login`	nome utente
	`MSG.Address`	indirizzo di rete del Pannello di controllo

Errore di autenticazione dell'amministratore

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se un amministratore non ha potuto autenticarsi nel Pannello di controllo. La causa dell'errore di autenticazione è riportata nel testo dell'avviso.	
Ulteriore configurazione	Non richiesta.	
Variabili	`MSG.Login`	nome utente
	`MSG.Address`	indirizzo di rete del Pannello di controllo
	`MSG.LoginErrorCode`	codice di errore numerico

Altro

Errore di rotazione del log del Server Dr.Web

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato in caso di errore di rotazione del log di funzionamento del Server Dr.Web. La causa dell'errore di rotazione del log è riportata nel testo dell'avviso.

Parametro	Valore	
Configurazione aggiuntiva	Non richiesta.	
Variabili	`MSG.Error`	testo dell'errore

Errore di registrazione del log del Server Dr.Web

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato in caso di errore di registrazione di informazioni nel log di funzionamento del Server Dr.Web. La causa dell'errore di registrazione nel log è riportata nel testo dell'avviso.	
Configurazione aggiuntiva	Non richiesta.	
Variabili	`MSG.Error`	testo dell'errore

Il Server Dr.Web adiacente non si collega da molto tempo

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato secondo un task nel calendario del Server Dr.Web. Informa che un Server Dr.Web adiacente non si collega a questo Server Dr.Web da molto tempo. La data dell'ultima connessione è riportata nel testo dell'avviso.	
Configurazione aggiuntiva	Il periodo durante cui un Server Dr.Web adiacente deve rimanere disconnesso affinché venga inviato un avviso viene impostato nel task **Il Server adiacente non si collega da molto tempo** nel calendario di Server Dr.Web che può essere configurato nella sezione **Amministrazione → Scheduler del Server Dr.Web**.	
Variabili	`MSG.LastDisconnectTime`	ora quando il Server Dr.Web era connesso per l'ultima volta
	`MSG.StationName`	nome del Server adiacente

Registrato un gran numero di blocchi Controllo applicazioni

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato nel caso di presenza di un gran numero di applicazioni bloccate sulle postazioni dal componente Controllo delle applicazioni.
Ulteriore configurazione	Per avere la possibilità di inviare avvisi circa un gran numero di applicazioni bloccate, è necessario spuntare il flag **Blocchi multipli Controllo applicazioni** nella sezione **Amministrazione →**

Parametro	Valore	
	Configurazione del Server Dr.Web → **Statistiche** e configurare i parametri corrispondenti nella stessa sezione.	
Variabili	`MSG.Total`	numero totale di blocchi
	`MSG.Profile`	i profili più diffusi in base a cui veniva effettuato il blocco

Registrato un gran numero di connessioni terminate in modo anomalo

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato nel caso di presenza di un numero elevato di connessioni terminate in modo anomalo con i client: postazioni, installer di Agent, Server Dr.Web adiacenti, Server proxy.	
Configurazione aggiuntiva	Per avere la possibilità di inviare avvisi di connessioni terminate in modo anomalo multiple, è necessario spuntare il flag **Terminazioni di connessioni anomale** nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Statistiche** e configurare i parametri corrispondenti nella stessa sezione.	
Variabili	`MSG.Total`	numero di connessioni interrotte
	`MSG.AddrsCount`	numero di indirizzi con cui sono state interrotte le connessioni

Report statistico

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato dopo la generazione di un report periodico secondo un task nel calendario di Server Dr.Web. Inoltre, nell'avviso è riportato il percorso attraverso cui è possibile scaricare il file di report.	
Configurazione aggiuntiva	Il report viene creato secondo il task **Creazione del report statistico** nel calendario di Server Dr.Web che può essere configurato nella sezione **Amministrazione** → **Scheduler del Server Dr.Web**.	
Variabili	`MSG.Attachment`	percorso del report
	`MSG.AttachmentType`	tipo MIME
	`GEN.File`	nome del file del report

Report di riepilogo di Protezione preventiva

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se è stato ricevuto dalle postazioni della rete un gran numero di report dal componente Protezione preventiva.	
Ulteriore configurazione	Per inviare un singolo avviso sul report dalla Protezione preventiva, è necessario spuntare il flag **Raggruppa i report di Protezione preventiva** nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Statistiche**. I parametri di raggruppamento dei report vengono impostati nella stessa sezione.	
Variabili	`MSG.AutoBlockedActCount`	numero di processi con un'attività sospetta, bloccati in automatico
	`MSG.AutoBlockedProc`	processo con un'attività sospetta, bloccato in automatico
	`MSG.HipsType`	tipo di oggetto protetto
	`MSG.IsShellGuard`	suddivisione per tipo di reazione della Protezione preventiva con il blocco automatico: • blocco del codice non autorizzato • controllo dell'accesso agli oggetti protetti
	`MSG.ShellGuardType`	il motivo più comune di blocco dell'esecuzione di codice non autorizzato con il blocco automatico dell'evento
	`MSG.Total`	numero totale di eventi della Protezione preventiva registrati nella rete
	`MSG.UserAllowedActCount`	numero di processi con un'attività sospetta, autorizzati dall'utente
	`MSG.UserAllowedHipsType`	tipo di oggetti che vengono più frequentemente protetti, l'accesso a cui è stato consentito dall'utente
	`MSG.UserAllowedIsShellGuard`	suddivisione per tipo di reazione della Protezione preventiva con l'accesso consentito da parte dell'utente: • blocco del codice non autorizzato

Parametro	Valore	
		• controllo dell'accesso agli oggetti protetti
	`MSG.UserAllowedProc`	processo con un'attività sospetta, autorizzato dall'utente
	`MSG.UserAllowedShellGuard`	il motivo più comune di blocco dell'esecuzione di codice non autorizzato con l'evento autorizzato dall'utente
	`MSG.UserBlockedActCount`	numero di processi con un'attività sospetta, bloccati dall'utente
	`MSG.UserBlockedHipsType`	tipo di oggetti che vengono più frequentemente protetti, l'accesso a cui è stato vietato dall'utente
	`MSG.UserBlockedIsShellGuard`	suddivisione per tipo di reazione della Protezione preventiva con l'accesso vietato da parte dell'utente: • blocco del codice non autorizzato • controllo dell'accesso agli oggetti protetti
	`MSG.UserBlockedProc`	processo con un'attività sospetta, bloccato dall'utente
	`MSG.UserBlockedShellGuard`	il motivo più comune di blocco dell'esecuzione di codice non autorizzato con l'evento bloccato dall'utente

Un'epidemia nella rete

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se è stata rilevata un'epidemia nella rete antivirus. Questo significa che nel periodo di tempo impostato sono state rilevate nella rete più minacce del numero impostato.	
Ulteriore configurazione	Per inviare avvisi di epidemie, è necessario spuntare il flag **Tieni d'occhio epidemie** nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Statistiche**. I parametri di definizione dell'epidemia vengono impostati nella stessa sezione.	
Variabili	`MSG.Infected`	numero totale di minacce rilevate

Parametro	Valore	
	`MSG.Virus`	le minacce più diffuse

Installazioni

Per i messaggi di questo gruppo sono inoltre disponibili le variabili generali per postazioni, riportate sopra.

L'installazione non è stata eseguita sulla postazione

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se un errore è occorso durante l'installazione di Agent su una postazione. La causa concreta dell'errore è riportata nel testo dell'avviso.	
Ulteriore configurazione	Non richiesta.	
Variabili	`MSG.Error`	messaggio di errore

L'installazione sulla postazione è stata completata con successo

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato in caso di un'installazione riuscita di Agent su una postazione.
Ulteriore configurazione	Non richiesta.
Variabili	Nessuna.

Licenze

Chiave di licenza non può essere aggiornata automaticamente

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato se la chiave di licenza non può essere aggiornata automaticamente in quanto la lista dei componenti concessi in licenza della chiave corrente è diversa da quella della chiave nuova. La nuova chiave è stata caricata con successo, ma non è stata distribuita su tutti gli oggetti della chiave di licenza vecchia. È necessario sostituire manualmente la chiave di licenza.
Ulteriore configurazione	Per informazioni dettagliate sull'aggiornamento automatico delle

Parametro	Valore	
	licenze consultare il **Manuale dell'amministratore**, p. Aggiornamento automatico delle licenze.	
Variabili	`MSG.ExpirationDate`	data di scadenza della licenza
	`MSG.Expired`	• 1 — la licenza è già scaduta • 0 — la licenza non è ancora scaduta
	`MSG.KeyDifference`	Il motivo per cui la sostituzione automatica della chiave non è possibile: • 1 — la lista dei componenti concessi in licenza della chiave di licenza corrente è diversa da quella della chiave di licenza nuova • 2 — la chiave di licenza nuova ha un minor numero di licenze rispetto alla chiave di licenza corrente
	`MSG.KeyId`	identificatore della chiave di licenza vecchia
	`MSG.KeyName`	nome della chiave di licenza vecchia
	`MSG.NewKeyId`	identificatore della chiave di licenza nuova
	`MSG.NewKeyName`	nome della chiave di licenza nuova

Chiave di licenza è aggiornata automaticamente

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se la chiave di licenza è stata aggiornata automaticamente. In particolare, la nuova chiave è stata caricata e distribuita con successo su tutti gli oggetti della chiave di licenza vecchia.	
Ulteriore configurazione	Per informazioni dettagliate sull'aggiornamento automatico delle licenze consultare il **Manuale dell'amministratore**, p. Aggiornamento automatico delle licenze.	
Variabili	`MSG.KeyId`	identificatore della chiave di licenza vecchia

Parametro	Valore	
	MSG.KeyName	nome della chiave di licenza vecchia
	MSG.NewKeyId	identificatore della chiave di licenza nuova
	MSG.NewKeyName	nome della chiave di licenza nuova

È stato raggiunto il limite di licenza al numero di postazioni nella rete

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se alla connessione di una postazione al Server Dr.Web viene rilevato che il numero di postazioni nel gruppo in cui rientra la postazione da connettere ha raggiunto il limite indicato nella chiave di licenza assegnata a questo gruppo. In tale caso la nuova postazione non può registrarsi sul Server Dr.Web.	
Configurazione aggiuntiva	Non richiesta.	
Variabili	MSG.ID	UUID della postazione
	MSG.StationName	nome della postazione
	Inoltre, sono disponibili le variabili generali per le postazioni riportate sopra.	

È stato raggiunto il limite al numero di licenze trasferite

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se sono state richieste più licenze da rilasciare ai Server Dr.Web adiacenti di quante sono disponibili nella chiave di licenza.	
Configurazione aggiuntiva	Non richiesta.	
Variabili	MSG.ObjId	ID della chiave di licenza

È scaduto il periodo di trasferimento di licenze

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato se è scaduto il periodo di rilascio di licenze a un Server Dr.Web adiacente dalla chiave di licenza di questo Server Dr.Web.

Parametro	Valore	
Configurazione aggiuntiva	Il periodo di rilascio delle licenze ai Server Dr.Web adiacenti viene configurato nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Licenze**.	
Variabili	`MSG.ObjId`	ID della chiave di licenza
	`MSG.Server`	nome del Server Dr.Web adiacente

Il numero di postazioni nel gruppo sta per avvicinarsi al limite di licenza

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se il numero di postazioni in un gruppo si sta avvicinando al limite di licenza indicato nella chiave assegnata a questo gruppo.	
Configurazione aggiuntiva	Numero di licenze disponibili rimanenti nella chiave, con cui viene inviato l'avviso: meno di tre licenze o meno del 5% del totale licenze nella chiave.	
Variabili	`MSG.Free`	numero di licenze disponibili rimanenti
	`MSG.Licensed`	numero di postazioni che utilizzano le licenze di questo gruppo
	`MSG.Total`	numero totale di licenze in tutte le chiavi assegnate al gruppo. notare: le chiavi di licenza del gruppo possono anche essere assegnate ad altri oggetti di licenza.
	`GEN.StationPrimaryGroupID`	ID del gruppo primario
	`GEN.StationPrimaryGroupName`	nome del gruppo primario

La chiave di licenza è bloccata

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato se durante l'aggiornamento del repository dal Sistema di aggiornamento mondiale Dr.Web sono state ricevute informazioni su quello che la chiave di licenza era stata bloccata. L'ulteriore uso di

Parametro	Valore	
	questa chiave non è possibile.	
Ulteriore configurazione	Per ricevere informazioni dettagliate sul motivo del blocco, contattare il servizio di supporto tecnico.	
Variabili	`MSG.KeyId`	ID della chiave di licenza
	`MSG.KeyName`	nome dell'utente della chiave di licenza

Limitazione sul numero di licenze nella chiave di licenza

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se all'avvio del Server Dr.Web viene rilevato che il numero di postazioni in un determinato gruppo ha già superato il numero di licenze nella chiave di licenza assegnata a questo gruppo.	
Configurazione aggiuntiva	Non richiesta.	
Variabili	`MSG.KeyId`	ID della chiave di licenza
	`MSG.KeyName`	nome dell'utente della chiave di licenza
	`MSG.Licensed`	numero di licenze consentite
	`MSG.LicenseLimit`	stato delle licenze: • 1 — il numero di licenze disponibili nella chiave di licenza sta per esaurirsi, • 2 — il numero di licenze disponibili nella chiave di licenza si è esaurito, • 3 — la chiave di licenza è stata assegnata a più oggetti di quanti sono consentiti in questa chiave.
	`MSG.Licensed`	numero di oggetti per cui è stata assegnata la chiave
	`MSG.Total`	numero di licenze nella chiave

Scadenza della chiave di licenza

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se è prossima la scadenza della chiave di licenza e l'aggiornamento automatico della licenza non è disponibile.	
Ulteriore configurazione	Non richiesta.	
Variabili	`MSG.ExpirationDate`	data di scadenza della licenza
	`MSG.Expired`	• 1 — la licenza è già scaduta • 0 — la licenza non è ancora scaduta
	`MSG.KeyId`	identificatore della chiave di licenza
	`MSG.KeyName`	nome della chiave di licenza

Nuovi arrivi

Per i messaggi di questo gruppo sono inoltre disponibili le variabili generali per postazioni, riportate sopra.

La postazione è in attesa di conferma

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato se una nuova postazione ha richiesto di essere connessa al Server Dr.Web e l'amministratore deve confermare o negare manualmente l'accesso della postazione.
Configurazione aggiuntiva	Tale situazione può verificarsi se nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Generali** all'impostazione **Modalità di registrazione dei nuovi arrivi** è assegnato il valore **Conferma l'accesso manualmente**.
Variabili	Nessuna.

La postazione è stata rifiutata automaticamente

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato se una nuova postazione ha richiesto di essere connessa al Server Dr.Web ed è stata rifiutata automaticamente dal Server Dr.Web.

Parametro	Valore
Configurazione aggiuntiva	Tale situazione potrebbe verificarsi se nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Generali** all'impostazione **Modalità di registrazione dei nuovi arrivi** è assegnato il valore **Sempre nega l'accesso**.
Variabili	Nessuna.

La postazione è stata rifiutata dall'amministratore

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se una nuova postazione ha richiesto di essere connessa al Server Dr.Web ed è stata rifiutata manualmente dall'amministratore.	
Configurazione aggiuntiva	Tale situazione può verificarsi se nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Generali** all'impostazione **Modalità di registrazione dei nuovi arrivi** è assegnato il valore **Conferma l'accesso manualmente** e l'amministratore ha selezionato per la postazione la variante **Rete antivirus** → **Postazioni non confermate** → **Nega l'accesso delle postazioni selezionate**.	
Variabili	`MSG.AdminAddress`	indirizzo di rete del Pannello di controllo
	`MSG.AdminName`	nome dell'amministratore

Postazioni

Per i messaggi di questo gruppo sono inoltre disponibili le variabili generali per postazioni, riportate sopra.

In una rete con diversi server è possibile ricevere avvisi sugli eventi sulle postazioni dei Server Dr.Web adiacenti. Questa opzione viene attivata quando si impostano le relazioni con i Server Dr.Web adiacenti (v. **Manuale dell'amministratore**, sezione Configurazione delle relazioni tra i Server Dr.Web).

Sono disponibili i seguenti avvisi sugli eventi sul Server Dr.Web adiacente: **È stata rilevata una minaccia alla sicurezza**, **Report di protezione preventiva**, **Errore di scansione**, **Statistiche di scansione**.

Dispositivo è bloccato

Parametro	Valore
Ragione per l'invio	Viene inviato se da una postazione è arrivato un avviso di ciò che uno

Parametro	Valore	
dell'avviso	dei dispositivi collegati alla postazione è stato bloccato dal componente antivirus Dr.Web.	
Ulteriore configurazione	Non richiesta.	
Variabili	`MSG.Capabilities`	caratteristiche del dispositivo
	`MSG.Class`	classe di dispositivo (nome del gruppo padre)
	`MSG.Description`	descrizione del dispositivo
	`MSG.FriendlyName`	nome descrittivo del dispositivo
	`MSG.InstanceId`	identificatore dell'esemplare del dispositivo
	`MSG.User`	nome utente

Controllo delle applicazioni ha bloccato un processo dalla lista degli hash di minacce conosciuti

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se un'applicazione dalla lista degli hash di minacce conosciuti sulla postazione è stata bloccata dal componente Controllo delle applicazioni.	
Configurazione aggiuntiva	L'avviso sul rilevamento in base alla lista degli hash conosciuti è possibile solo se è stato concesso in licenza l'uso dei bollettini degli hash di minacce conosciuti (è sufficiente una licenza in almeno una delle chiavi di licenza utilizzate dal Server Dr.Web). La presenza della licenza è indicata nelle informazioni sulla chiave di licenza che possono essere visualizzate nella sezione **Gestione licenze**, parametro **Liste consentite dei bollettini di hash** (se le funzionalità non sono concesse in licenza, questo parametro è assente).	
Variabili	`MSG.AppCtlAction`	azione applicata: • 0 — sconosciuto, • 2 — bloccato, • 3 — bloccato (non trovato nella lista delle applicazioni affidabili), • 5 — bloccato dalle regole di divieto, • 7 — bloccato dalle impostazioni dei criteri.

Parametro	Valore	
	MSG.AppCtlType	tipo di evento: • 0 — sconosciuto, • 1 — avvio del processo, • 2 — avvio del processo host, • 3 — avvio dell'interprete di script, • 4 — caricamento del modulo, • 5 — caricamento del driver, • 6 — avvio dell'installer MSI, • 7 — creazione di un nuovo file eseguibile sul disco, • 8 — modifica del file eseguibile sul disco.
	MSG.Document	bollettino contenente l'hash
	MSG.Path	percorso del processo bloccato
	MSG.Profile	nome del profilo in base a cui è stato effettuato il blocco
	MSG.Rule	nome della regola in base a cui è stato effettuato il blocco
	MSG.SHA256	hash del processo bloccato (SHA-256)
	MSG.StationTime	ora sulla postazione quando il processo è stato bloccato
	MSG.Target	percorso dello script bloccato nel caso di processo host
	MSG.TargetSHA256	hash dello script bloccato nel caso di processo host (SHA-256)
	MSG.TestMode	se la modalità test è attivata o meno
	MSG.User	utente sotto cui veniva avviato l'oggetto bloccato

Controllo delle applicazioni ha bloccato un processo

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se un'applicazione sulla postazione è stata bloccata dal componente Controllo delle applicazioni.	
Configurazione aggiuntiva	Non richiesta.	
Variabili	`MSG.AppCtlAction`	azione applicata: • 0 — sconosciuto, • 2 — bloccato, • 3 — bloccato (non trovato nella lista delle applicazioni affidabili), • 5 — bloccato dalle regole di divieto, • 7 — bloccato dalle impostazioni dei criteri.
	`MSG.AppCtlType`	tipo di evento: • 0 — sconosciuto, • 1 — avvio del processo, • 2 — avvio del processo host, • 3 — avvio dell'interprete di script, • 4 — caricamento del modulo, • 5 — caricamento del driver, • 6 — avvio dell'installer MSI, • 7 — creazione di un nuovo file eseguibile sul disco, • 8 — modifica del file eseguibile sul disco.
	`MSG.Path`	percorso del processo bloccato
	`MSG.Profile`	nome del profilo in base a cui è stato effettuato il blocco
	`MSG.Rule`	nome della regola in base a cui è stato effettuato il blocco
	`MSG.SHA256`	hash del processo bloccato (SHA-256)
	`MSG.StationTime`	ora sulla postazione quando il processo è stato bloccato

Parametro	Valore	
	MSG.Target	percorso dello script bloccato nel caso di processo host
	MSG.TargetSHA256	hash dello script bloccato nel caso di processo host (SHA-256)
	MSG.TestMode	se la modalità test è attivata o meno
	MSG.User	utente sotto cui veniva avviato l'oggetto bloccato

È necessario riavviare la postazione

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato quando è richiesto il riavvio di una postazione per uno dei seguenti motivi: • per completare la cura, • per applicare gli aggiornamenti, • per modificare lo stato della virtualizzazione hardware, • per completare la cura e applicare gli aggiornamenti, • per completare la cura e modificare lo stato della virtualizzazione hardware, • per applicare gli aggiornamenti e modificare lo stato della virtualizzazione hardware, • per completare la cura, applicare gli aggiornamenti e modificare lo stato della virtualizzazione hardware.	
Configurazione aggiuntiva	Non richiesta.	
Variabili	MSG.Reason	ragione per il riavvio la lista delle possibili ragioni è riportata nel modello predefinito

È necessario riavviare la postazione per applicare gli aggiornamenti

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato se da una postazione è arrivato un avviso di ciò che un prodotto è stato installato o aggiornato ed è richiesto un riavvio della postazione.
Configurazione aggiuntiva	Non richiesta.

Parametro	Valore	
Variabili	MSG.Product	prodotto che viene aggiornato
	MSG.ServerTime	ora della ricezione dell'evento, GMT

È stata rilevata una minaccia alla sicurezza

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se da una postazione è arrivato un avviso di rilevamento di minacce. Nell'avviso all'amministratore sono riportate inoltre informazioni dettagliate sulle minacce rilevate.	
Configurazione aggiuntiva	Non richiesta.	
Variabili	MSG.Action	azione intrapresa a rilevamento
	MSG.Component	nome del componente
	MSG.InfectionType	tipo di minaccia
	MSG.ObjectName	nome dell'oggetto infetto
	MSG.ObjectOwner	owner dell'oggetto infetto
	MSG.RunBy	utente sotto cui il componente è in esecuzione
	MSG.ServerTime	ora della ricezione dell'evento, GMT
	MSG.Virus	nome della minaccia
	GEN.ServerRecvLinkID	UUID dell'ultimo Server Dr.Web adiacente da cui è stato ricevuto questo messaggio su una minaccia rilevata sulle postazioni connesse ad esso (valore vuoto se è stata rilevata una minaccia sulle postazioni connesse a questo Server Dr.Web)
	GEN.ServerRecvLinkName	nome dell'ultimo Server Dr.Web adiacente da cui è stato ricevuto il messaggio su una minaccia rilevata sulle postazioni connesse ad esso (valore vuoto se è stata rilevata una minaccia sulle postazioni connesse a questo Server Dr.Web)
	GEN.ServerOriginatorID	UUID del Server Dr.Web a cui è connessa la postazione su cui è

Parametro	Valore	
		stata rilevata una minaccia
	GEN.ServerOriginatorName	nome del Server Dr.Web a cui è connessa la postazione su cui è stata rilevata una minaccia

È stata rilevata una minaccia alla sicurezza in base agli hash di minacce conosciuti

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se da una postazione è arrivato un avviso di rilevamento delle minacce dalla lista degli hash di minacce conosciuti. Nell'avviso all'amministratore sono riportate inoltre informazioni dettagliate sulle minacce rilevate.	
Configurazione aggiuntiva	L'avviso sul rilevamento in base alla lista degli hash conosciuti è possibile solo se è stato concesso in licenza l'uso dei bollettini degli hash di minacce conosciuti (è sufficiente una licenza in almeno una delle chiavi di licenza utilizzate dal Server Dr.Web). La presenza della licenza è indicata nelle informazioni sulla chiave di licenza che possono essere visualizzate nella sezione **Gestione licenze**, parametro **Liste consentite dei bollettini di hash** (se le funzionalità non sono concesse in licenza, questo parametro è assente).	
Variabili	MSG.Action	azione intrapresa a rilevamento
	MSG.Component	nome del componente
	MSG.Document	bollettino contenente l'hash della minaccia rilevata
	MSG.InfectionType	tipo di minaccia
	MSG.ObjectName	nome dell'oggetto infetto
	MSG.ObjectOwner	owner dell'oggetto infetto
	MSG.RunBy	utente sotto cui il componente è in esecuzione
	MSG.SHA1	hash SHA-1 dell'oggetto rilevato
	MSG.SHA256	hash SHA-256 dell'oggetto rilevato
	MSG.ServerTime	ora della ricezione dell'evento, GMT
	MSG.Virus	nome della minaccia
	GEN.ServerRecvLinkID	UUID dell'ultimo Server Dr.Web

Parametro	Valore	
		adiacente da cui è stato ricevuto questo messaggio su una minaccia rilevata sulle postazioni connesse ad esso (valore vuoto se è stata rilevata una minaccia sulle postazioni connesse a questo Server Dr.Web)
	`GEN.ServerRecvLinkName`	nome dell'ultimo Server Dr.Web adiacente da cui è stato ricevuto il messaggio su una minaccia rilevata sulle postazioni connesse ad esso (valore vuoto se è stata rilevata una minaccia sulle postazioni connesse a questo Server Dr.Web)
	`GEN.ServerOriginatorID`	UUID del Server Dr.Web a cui è connessa la postazione su cui è stata rilevata una minaccia
	`GEN.ServerOriginatorName`	nome del Server Dr.Web a cui è connessa la postazione su cui è stata rilevata una minaccia

Errore di autenticazione della postazione

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se al tentativo di connessione al Server Dr.Web una postazione ha fornito credenziali non valide. Nell'avviso sono inoltre riportate le azioni successive che dipendono dai criteri di approvazione di postazioni.	
Configurazione aggiuntiva	I criteri di approvazione di postazioni vengono configurati nell'impostazione **Modalità di registrazione dei nuovi arrivi** nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Generali**.	
Variabili	`MSG.ID`	UUID della postazione
	`MSG.Rejected`	valori: • `rejected` — l'accesso della postazione è stato negato • `newbie` — è stato fatto un tentativo di trasferimento della postazione nello stato "nuovo arrivo"
	`MSG.StationName`	nome della postazione

Errore di scansione

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se da una postazione è arrivato un avviso di errore di scansione.	
Configurazione aggiuntiva	Non richiesta.	
Variabili	`MSG.Component`	nome del componente
	`MSG.Error`	messaggio di errore
	`MSG.ObjectName`	nome dell'oggetto
	`MSG.ObjectOwner`	owner dell'oggetto
	`MSG.RunBy`	utente sotto cui il componente è in esecuzione
	`MSG.ServerTime`	ora della ricezione dell'evento, GMT
	`GEN.ServerRecvLinkID`	UUID dell'ultimo Server Dr.Web adiacente da cui sono state ricevute informazioni su un errore di scansione delle postazioni connesse ad esso (valore vuoto se un errore di scansione si è verificato sulle postazioni connesse a questo Server Dr.Web)
	`GEN.ServerRecvLinkName`	nome dell'ultimo Server Dr.Web adiacente da cui sono state ricevute informazioni su un errore di scansione delle postazioni connesse ad esso (valore vuoto se un errore di scansione si è verificato sulle postazioni connesse a questo Server Dr.Web)
	`GEN.ServerOriginatorID`	UUID del Server Dr.Web a cui è connessa la postazione su cui si è verificato un errore di scansione
	`GEN.ServerOriginatorName`	nome del Server Dr.Web a cui è connessa la postazione su cui si è verificato un errore di scansione

Errore critico di aggiornamento della postazione

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se da una postazione è arrivato un avviso di errore nel processo di aggiornamento dei componenti antivirus dal Server Dr.Web.	
Configurazione aggiuntiva	Non richiesta.	
Variabili	`MSG.Product`	prodotto che viene aggiornato
	`MSG.ServerTime`	ora della ricezione dell'evento, GMT

Errore di scansione al rilevamento di una minaccia in base agli hash di minacce conosciuti

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se è occorso un errore di scansione al rilevamento di una minaccia dalla lista degli hash di minacce conosciuti.	
Configurazione aggiuntiva	L'avviso sul rilevamento in base alla lista degli hash conosciuti è possibile solo se è stato concesso in licenza l'uso dei bollettini degli hash di minacce conosciuti (è sufficiente una licenza in almeno una delle chiavi di licenza utilizzate dal Server Dr.Web). La presenza della licenza è indicata nelle informazioni sulla chiave di licenza che possono essere visualizzate nella sezione **Gestione licenze**, parametro **Liste consentite dei bollettini di hash** (se le funzionalità non sono concesse in licenza, questo parametro è assente).	
Variabili	`MSG.Component`	nome del componente
	`MSG.Document`	bollettino contenente l'hash della minaccia rilevata
	`MSG.Error`	messaggio di errore
	`MSG.ObjectName`	nome dell'oggetto
	`MSG.ObjectOwner`	owner dell'oggetto
	`MSG.RunBy`	utente sotto cui il componente è in esecuzione
	`MSG.SHA1`	hash SHA-1 dell'oggetto rilevato
	`MSG.SHA256`	hash SHA-256 dell'oggetto rilevato
	`MSG.ServerTime`	ora della ricezione dell'evento, GMT

Parametro	Valore	
	GEN.ServerRecvLinkID	UUID dell'ultimo Server Dr.Web adiacente da cui sono state ricevute informazioni su un errore di scansione delle postazioni connesse ad esso (valore vuoto se un errore di scansione si è verificato sulle postazioni connesse a questo Server Dr.Web)
	GEN.ServerRecvLinkName	nome dell'ultimo Server Dr.Web adiacente da cui sono state ricevute informazioni su un errore di scansione delle postazioni connesse ad esso (valore vuoto se un errore di scansione si è verificato sulle postazioni connesse a questo Server Dr.Web)
	GEN.ServerOriginatorID	UUID del Server Dr.Web a cui è connessa la postazione su cui si è verificato un errore di scansione
	GEN.ServerOriginatorName	nome del Server Dr.Web a cui è connessa la postazione su cui si è verificato un errore di scansione

Impossibile creare un account di postazione

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se non è possibile creare un nuovo account di postazione sul Server Dr.Web. I dettagli dell'errore sono riportati nel file di log del Server Dr.Web.	
Configurazione aggiuntiva	Non richiesta.	
Variabili	MSG.ID	UUID della postazione
	MSG.StationName	nome della postazione

La postazione è già registrata

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato se al Server Dr.Web tenta di connettersi una postazione con un identificatore che coincide con l'identificatore di una postazione già connessa a questo Server Dr.Web.

Parametro	Valore	
Configurazione aggiuntiva	Non richiesta.	
Variabili	`MSG.ID`	UUID della postazione
	`MSG.Server`	ID del Server Dr.Web su cui la postazione è registrata
	`MSG.StationName`	nome della postazione

La postazione non si connette al Server Dr.Web da molto tempo

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato secondo un task nel calendario del Server Dr.Web. Informa che una postazione non si collega a questo Server Dr.Web da molto tempo. La data dell'ultima connessione è riportata nel testo dell'avviso.	
Configurazione aggiuntiva	Il periodo durante cui una postazione deve rimanere disconnessa affinché venga inviato un avviso viene impostato nel task **La postazione non si connette da molto tempo** nel calendario di Server Dr.Web che può essere configurato nella sezione **Amministrazione** → **Scheduler del Server Dr.Web**.	
Variabili	Le variabili generali per postazioni, riportate sopra, non sono disponibili.	
	`MSG.DaysAgo`	numero di giorni dal momento dell'ultima connessione al Server Dr.Web
	`MSG.LastSeenFrom`	indirizzo da cui la postazione si connetteva l'ultima volta al Server Dr.Web
	`MSG.StationDescription`	descrizione della postazione
	`MSG.StationID`	UUID della postazione
	`MSG.StationMAC`	Indirizzo MAC della postazione
	`MSG.StationName`	nome della postazione
	`MSG.StationSID`	identificatore di sicurezza della postazione

La postazione è stata confermata automaticamente

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se una nuova postazione ha richiesto di essere connessa al Server Dr.Web ed è stata confermata automaticamente dal Server Dr.Web.	
Configurazione aggiuntiva	Tale situazione può verificarsi se nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Generali** all'impostazione **Modalità di registrazione dei nuovi arrivi** è assegnato il valore **Consenti l'accesso automaticamente**.	
Variabili	Nessuna.	

La postazione è stata confermata dall'amministratore

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se una nuova postazione ha richiesto di essere connessa al Server Dr.Web ed è stata confermata manualmente dall'amministratore.	
Configurazione aggiuntiva	Tale situazione può verificarsi se nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Generali** all'impostazione **Modalità di registrazione dei nuovi arrivi** è assegnato il valore **Conferma l'accesso manualmente** e l'amministratore ha selezionato per la postazione la variante **Rete antivirus** → **Postazioni non confermate** → **Consenti l'accesso alle postazioni selezionate e assegna gruppo primario**.	
Variabili	`MSG.AdminAddress`	indirizzo di rete del Pannello di controllo
	`MSG.AdminName`	nome dell'amministratore

Postazione sconosciuta

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se una nuova postazione ha richiesto di essere connessa al Server Dr.Web, ma non è stata ammessa alla considerazione della conferma o negazione della registrazione.	
Configurazione aggiuntiva	Non richiesta.	
Variabili	`MSG.ID`	UUID della postazione sconosciuta
	`MSG.Rejected`	valori:

Parametro	Valore	
		• `rejected` — l'accesso della postazione è stato negato • `newbie` — è stato fatto un tentativo di trasferimento della postazione nello stato "nuovo arrivo"
	`MSG.StationName`	nome della postazione

Report di Protezione preventiva

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato quando viene ricevuto un report dal componente Protezione preventiva da una postazione di questo Server Dr.Web o di un Server Dr.Web adiacente.	
Configurazione aggiuntiva	Non richiesta.	
Variabili	`MSG.AdminName`	amministratore che ha avviato un'azione su un processo sospetto
	`MSG.Denied`	azione eseguita su un processo sospetto: • vietato • consentito
	`MSG.HipsType`	tipo di oggetto protetto
	`MSG.IsShellGuard`	suddivisione per tipo di reazione della Protezione preventiva: • blocco del codice non autorizzato • controllo dell'accesso agli oggetti protetti
	`MSG.Path`	percorso del processo con un'attività sospetta
	`MSG.Pid`	identificatore del processo con un'attività sospetta
	`MSG.ShellGuardType`	motivo di blocco dell'esecuzione di codice non autorizzato
	`MSG.StationTime`	ora di comparsa dell'evento sulla postazione
	`MSG.Target`	percorso dell'oggetto protetto a cui

Parametro	Valore	
		è stato effettuato un tentativo di accesso
	MSG.Total	numero di divieti nel caso di reazione automatica della Protezione preventiva
	MSG.User	utente sotto cui è stato avviato il processo con un'attività sospetta
	MSG.UserAction	iniziatore dell'azione su un processo sospetto: • utente • reazione automatica della Protezione preventiva
	GEN.ServerRecvLinkID	UUID dell'ultimo Server Dr.Web adiacente da cui è stato ricevuto un report di Protezione preventiva dalle postazioni connesse ad esso (valore vuoto se è stato ricevuto un report dalle postazioni connesse a questo Server Dr.Web)
	GEN.ServerRecvLinkName	nome dell'ultimo Server Dr.Web adiacente da cui è stato ricevuto un report di Protezione preventiva dalle postazioni connesse ad esso (valore vuoto se è stato ricevuto un report dalle postazioni connesse a questo Server Dr.Web)
	GEN.ServerOriginatorID	UUID del Server Dr.Web a cui è connessa la postazione da cui è stato ricevuto un report di Protezione preventiva
	GEN.ServerOriginatorName	nome del Server Dr.Web a cui è connessa la postazione da cui è stato ricevuto un report di Protezione preventiva

Report di Protezione preventiva sul rilevamento di minacce in base agli hash di minacce conosciuti

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato quando viene ricevuto un report dal componente Protezione preventiva da una postazione di questo Server Dr.Web o di

Parametro	Valore	
	un Server Dr.Web adiacente nel caso di rilevamento delle minacce dalla lista degli hash di minacce conosciuti.	
Configurazione aggiuntiva	L'avviso sul rilevamento in base alla lista degli hash conosciuti è possibile solo se è stato concesso in licenza l'uso dei bollettini degli hash di minacce conosciuti (è sufficiente una licenza in almeno una delle chiavi di licenza utilizzate dal Server Dr.Web). La presenza della licenza è indicata nelle informazioni sulla chiave di licenza che possono essere visualizzate nella sezione **Gestione licenze**, parametro **Liste consentite dei bollettini di hash** (se le funzionalità non sono concesse in licenza, questo parametro è assente).	
Variabili	`MSG.AdminName`	amministratore che ha avviato un'azione su un processo sospetto
	`MSG.Denied`	azione eseguita su un processo sospetto: • vietato • consentito
	`MSG.Document`	bollettino contenente l'hash della minaccia rilevata
	`MSG.HipsType`	tipo di oggetto protetto
	`MSG.IsShellGuard`	suddivisione per tipo di reazione della Protezione preventiva: • blocco del codice non autorizzato • controllo dell'accesso agli oggetti protetti
	`MSG.Path`	percorso del processo con un'attività sospetta
	`MSG.Pid`	identificatore del processo con un'attività sospetta
	`MSG.SHA1`	hash SHA-1 dell'oggetto rilevato
	`MSG.SHA256`	hash SHA-256 dell'oggetto rilevato
	`MSG.ShellGuardType`	motivo di blocco dell'esecuzione di codice non autorizzato
	`MSG.StationTime`	ora di comparsa dell'evento sulla postazione
	`MSG.Target`	percorso dell'oggetto protetto a cui è stato effettuato un tentativo di

Parametro	Valore	
		accesso
	MSG.Total	numero di divieti nel caso di reazione automatica della Protezione preventiva
	MSG.User	utente sotto cui è stato avviato il processo con un'attività sospetta
	MSG.UserAction	iniziatore dell'azione su un processo sospetto: • utente • reazione automatica della Protezione preventiva
	GEN.ServerRecvLinkID	UUID dell'ultimo Server Dr.Web adiacente da cui è stato ricevuto un report di Protezione preventiva dalle postazioni connesse ad esso (valore vuoto se è stato ricevuto un report dalle postazioni connesse a questo Server Dr.Web)
	GEN.ServerRecvLinkName	nome dell'ultimo Server Dr.Web adiacente da cui è stato ricevuto un report di Protezione preventiva dalle postazioni connesse ad esso (valore vuoto se è stato ricevuto un report dalle postazioni connesse a questo Server Dr.Web)
	GEN.ServerOriginatorID	UUID del Server Dr.Web a cui è connessa la postazione da cui è stato ricevuto un report di Protezione preventiva
	GEN.ServerOriginatorName	nome del Server Dr.Web a cui è connessa la postazione da cui è stato ricevuto un report di Protezione preventiva

Statistiche di scansione

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato se da una postazione è arrivato un avviso di completamento di una scansione. Nell'avviso all'amministratore sono riportate inoltre le brevi statistiche della scansione.

Parametro	Valore	
Configurazione aggiuntiva	Non richiesta.	
Variabili	MSG.Component	nome del componente che eseguiva la scansione
	MSG.Cured	numero di oggetti guariti
	MSG.DeletedObjs	numero di oggetti eliminati
	MSG.Errors	numero di errori di scansione
	MSG.Infected	numero di oggetti infetti
	MSG.Locked	numero di oggetti bloccati
	MSG.Modifications	numero di oggetti infettati da varianti dei virus
	MSG.Moved	numero di oggetti spostati in quarantena
	MSG.Renamed	numero di oggetti rinominati
	MSG.RunBy	utente sotto cui il componente è in esecuzione
	MSG.Scanned	numero di oggetti scansionati
	MSG.ServerTime	ora della ricezione dell'evento, GMT
	MSG.Speed	velocità di processamento in Kb/s
	MSG.Suspicious	numero di oggetti sospetti
	MSG.VirusActivity	numero di virus rilevati
	GEN.ServerRecvLinkID	UUID dell'ultimo Server Dr.Web adiacente da cui sono state ricevute statistiche di scansione delle postazioni connesse ad esso (valore vuoto se sono state ricevute statistiche dalle postazioni connesse a questo Server Dr.Web)
	GEN.ServerRecvLinkName	nome dell'ultimo Server Dr.Web adiacente da cui sono state ricevute statistiche di scansione delle postazioni connesse ad esso (valore vuoto se sono state ricevute statistiche dalle postazioni connesse a questo Server Dr.Web)

Parametro	Valore	
	GEN.ServerOriginatorID	UUID del Server Dr.Web a cui è connessa la postazione da cui sono state ricevute statistiche di scansione
	GEN.ServerOriginatorName	nome del Server Dr.Web a cui è connessa la postazione da cui sono state ricevute statistiche di scansione

Terminazione di connessione anomala

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se è terminata in modo anomalo una connessione con un client: postazione, installer di Agent, Server Dr.Web adiacente, Server proxy.	
Configurazione aggiuntiva	Per avere la possibilità di inviare avvisi di connessioni terminate in modo anomalo, è necessario spuntare il flag **Terminazioni di connessioni anomale** nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Statistiche** e configurare i parametri corrispondenti nella stessa sezione.	
Variabili	MSG.Total	numero di connessioni interrotte
	MSG.Type	tipo di client

Repository

Per i messaggi di questo gruppo sono inoltre disponibili le variabili generali per repository, riportate sopra.

È stato avviato un aggiornamento del prodotto nel repository

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato se durante un controllo degli aggiornamenti di repository viene scoperto che è necessario un aggiornamento dei prodotto richiesti. Si avvia un aggiornamento da SAM.
Ulteriore configurazione	Non richiesta.
Variabili	Nessuna.

Errore di aggiornamento del repository

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se si è verificato un errore durante l'aggiornamento da SAM di un prodotto del repository. La causa di errore specifica, nonché il nome del prodotto il cui aggiornamento non è riuscito vengono riportati nel testo dell'avviso.	
Ulteriore configurazione	Non richiesta.	
Variabili	`MSG.Error`	messaggio di errore
	`MSG.ExtendedError`	descrizione dettagliata dell'errore

Il prodotto nel repository è stato aggiornato

Messaggio	Valore	
Ragione per l'invio dell'avviso	Viene inviato in caso di un aggiornamento riuscito del repository da SAM.	
Ulteriore configurazione	Non richiesta.	
Variabili	`MSG.Added`	lista dei file aggiunti (ciascun nome è in una riga separata)
	`MSG.AddedCount`	numero di file aggiunti
	`MSG.Deleted`	lista dei file eliminati (ciascun nome è in una riga separata)
	`MSG.DeletedCount`	numero di file eliminati
	`MSG.Replaced`	lista dei file sostituiti (ciascun nome è in una riga separata)
	`MSG.ReplacedCount`	numero di file sostituiti

L'aggiornamento del prodotto nel repository è stato congelato

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato se un prodotto in repository è stato congelato dall'amministratore. Il prodotto non viene aggiornato da SAM.
Ulteriore configurazione	I prodotti dei repository, incluso il congelamento e lo scongelamento, vengono gestiti nella sezione **Amministrazione** → **Configurazione dettagliata del repository**.

Parametro	Valore
Variabili	Nessuna.

L'aggiornamento del repository è già in esecuzione

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato se nel processo di aggiornamento del Server Dr.Web è stato riavviato l'aggiornamento.
Configurazione aggiuntiva	Non richiesta.
Variabili	Nessuna.

Stato aggiornato del prodotto nel repository

Parametro	Valore
Ragione per l'invio dell'avviso	Viene inviato se durante un controllo degli aggiornamenti di repository viene scoperto che il prodotto richiesto è già nello stato aggiornato. Non è necessario aggiornare questo prodotto da SAM.
Ulteriore configurazione	Non richiesta.
Variabili	Nessuna.

Le variabili del modello **Stato aggiornato del prodotto nel repository** non includono i file marcati come **ignorati in avvisi** nel file di configurazione del prodotto, v. E1. File di configurazione generali.

Spazio insufficiente su disco

Parametro	Valore	
Ragione per l'invio dell'avviso	Viene inviato se sta per esaurirsi lo spazio libero sul disco su cui si trova la directory di Server Dr.Web `var` con i dati dinamici.	
Configurazione aggiuntiva	Una mancanza di spazio su disco viene determinata se sono rimasti meno di 315 MB o meno di 1000 nodes (in caso dei SO della famiglia UNIX), se questi valori non sono ridefiniti dalle variabili di ambiente.	
Variabili	Le variabili generali per repository, riportate sopra, non sono disponibili.	
	`MSG.FreeInodes`	numero di descrittori di file inodes liberi (valido solo per alcuni sistemi

Parametro	Valore	
		della famiglia UNIX)
	MSG.FreeSpace	spazio libero in byte
	MSG.Path	percorso di directory con piccola quantità di memoria
	MSG.RequiredInodes	numero di inodes liberi, necessario per il funzionamento (valido solo per alcuni sistemi della famiglia UNIX)
	MSG.RequiredSpace	quantità di memoria libera necessaria per il funzionamento

Allegato D. Specifica dell'indirizzo di rete

In questa specifica vengono utilizzati i seguenti segni:

- variabili (campi da sostituire con valori concreti) sono racchiuse tra parentesi angolate e scritte in corsivo,
- testo costante (che si conserva dopo le sostituzioni) viene scritto in font monospaziato,
- elementi non obbligatori sono racchiusi tra parentesi quadre,
- a sinistra della stringa dei caratteri `::=` si trova il termine che viene definito, a destra la definizione (come in Backus-Naur Form).

D1. Formato generale dell'indirizzo

Indirizzo di rete ha il seguente formato:

`[`*<protocol>*`://][`*<protocol-specific-part>*`]`

Di default *<protocol>* ha il valore `TCP`. I valori predefiniti *<protocol-specific-part>* vengono determinati dall'applicazione.

È anche consentito il formato di indirizzi obsoleto:

`[`*<protocol>*`/][`*<protocol-specific-part>*`]`.

Indirizzi della famiglia IP

- *<interface>*`::=`*<ip-address>*

  <ip-address> può essere nome DNS o indirizzo IP separato da punti (per esempio, `127.0.0.1`).

- *<socket-address>*`::=`*<interface>*`:`*<port-number>*

  <port-number> deve essere un numero decimale.

Quando si imposta l'indirizzo di Server Dr.Web e l'indirizzo di Agent Dr.Web, è possibile indicare la versione del protocollo in uso. Sono ammissibili le seguenti varianti:

- *<protocol>*`://`*<interface>*`:`*<port-number>* — utilizza IPv4 e IPv6.
- *<protocol>*`://(`*<interface>*`):`*<port-number>* — utilizza solo IPv4.
- *<protocol>*`://[`*<interface>*`]:`*<port-number>* — utilizza solo IPv6.

Per esempio:

1. `tcp://127.0.0.1:2193`

   significa protocollo `TCP`, porta `2193` su interfaccia `127.0.0.1`.

2. `tcp://(examle.com):2193`

significa protocollo `TCP`, porta `2193` su interfaccia IPv4 `example.com`.

3. `tcp://[::]:2193`

   significa protocollo `TCP`, porta `2193` su interfaccia IPv6 `0000.0000.0000.0000.0000.0000.0000.0000`

4. `localhost:2193`

   la stessa cosa.

5. `tcp://:9999`

   valore per server: interfaccia predefinita che dipende da applicazione (di solito tutte le interfacce disponibili), porta `9999`; valore per client: connessione a host predefinito che dipende da applicazione (di solito `localhost`), porta `9999`.

6. `tcp://`

   protocollo TCP, porta predefinita.

Protocollo orientato alla connessione

<protocol>`://`*<socket-address>*

dove *<socket-address>* imposta l'indirizzo locale di socket per server o il server remoto per client.

Protocollo orientato al datagramma

<protocol>`://`*<endpoint-socket-address>*`[-`*<interface>*`]`

Per esempio:

1. `udp://231.0.0.1:2193`

   significa utilizzo del gruppo multicast `231.0.0.1:2193` su interfaccia che dipende da applicazione di default.

2. `udp://[ff18::231.0.0.1]:2193`

   significa utilizzo del gruppo multicast `[ff18::231.0.0.1]` su interfaccia che dipende da applicazione di default.

3. `udp://`

   endpoint ed interfaccia che dipende da applicazione.

4. `udp://255.255.255.255:9999-myhost1`

   utilizzo di messaggi broadcast su porta `9999` su interfaccia `myhost1`.

Indirizzi della famiglia UDS

- Protocollo orientato alla connessione:

  `unx://`*<file_name>*

- Protocollo orientato al datagramma:

  `udx://`*<file_name>*

Per esempio:

```
1. unx://tmp/drwcsd:stream
2. udx://tmp/drwcsd:datagram
```

Indirizzi della famiglia SRV

`srv://[`*<server name>*`][@`*<domain name/dot address>*`]`

D2. Indirizzi di Agent Dr.Web/ Installer

Connessione diretta con il Server Dr.Web

`[`*<connection-protocol>*`://[`*<remote-socket-address>*`]`

Di default, a seconda di *<connection-protocol>*:

- `tcp://127.0.0.1:2193`

  dove `127.0.0.1` — loopback, `2193` — porta;
- `tcp://[::1]:2193`

  dove `[::1]` — loopback (IPv6), `2193` — porta.

Ricerca di un Server Dr.Web <drwcs-name> che utilizza la famiglia di protocolli e l'endpoint specificati

`[`*<drwcs-name>*`]@`*<datagram-protocol>*`://[`*<endpoint-socket-address>*`[-`*<interface>*`]]`

Di default, a seconda di *<datagram-protocol>*:

- `drwcs@udp://231.0.0.1:2193-0.0.0.0`

  ricerca di un Server Dr.Web con il nome `drwcs` per la connessione TCP che utilizza il gruppo multicast `231.0.0.1:2193` su tutte le interfacce.

Allegato E. Gestione del repository

Si consiglia di gestire il repository attraverso le relative impostazioni del Pannello di controllo. Per maggiori informazioni consultare **Manuale dell'amministratore**, p Gestione del repository di Server Dr.Web.

Le impostazioni del repository vengono salvate nei seguenti file di configurazione del repository:

- I file di configurazione generali si trovano alla radice della directory di repository e impostano i parametri dei server di aggiornamenti.
- I file di configurazione dei prodotti si trovano alla radice di directory corrispondenti a prodotti specifici e definiscono la lista dei file e le impostazioni per l'aggiornamento del prodotto nella cui directory si trovano.

Dopo la modifica dei file di configurazione, è necessario riavviare il Server Dr.Web.

Quando vengono configurate le relazioni tra i server (v. **Manuale dell'amministratore**, p. Caratteristiche di una rete con diversi Server Dr.Web) per il mirror dei prodotti, si deve tenere presente che i file di configurazione non sono parte del prodotto e non vengono processati dal sistema di mirror. Per evitare malfunzionamenti del sistema di aggiornamento:

- per i Server Dr.Web paritari, mantenere identica la configurazione,
- per i Server Dr.Web subordinati, disattivare la sincronizzazione dei componenti attraverso il protocollo HTTP o mantenere identica la configurazione.

E1. File di configurazione generali

.servers

Il file `.servers` contiene una lista dei server utilizzati per aggiornare i componenti di Dr.Web Enterprise Security Suite nel repository del Server Dr.Web dai server SAM.

I server nella lista vengono interrogati uno dopo l'altro, se l'aggiornamento è stato completato con successo, la procedura di interrogazione finisce.

Per esempio:

```
esuite.geo.drweb.com
```

.url

Il file `.url` contiene l'URI di base della zona di aggiornamento — una directory sui server di aggiornamento che contiene gli aggiornamenti di un prodotto Dr.Web specifico.

Per esempio:

```
update
```

.proto

Il file `.proto` contiene il nome del protocollo attraverso cui vengono ricevuti gli aggiornamenti dai server di aggiornamento.

Può assumere uno dei seguenti valori: `http | https | ftp | ftps | sftp | scp | smb | smbs | file`.

I protocolli `smb` ed `smbs` sono disponibili solo per i Server Dr.Web sotto SO della famiglia Unix.

Per esempio:

```
https
```

.auth

Il file `.auth` contiene i parametri di autenticazione dell'utente sul server di aggiornamento.

I parametri di autenticazione vengono impostati nel seguente formato:

```
<nome utente>
<password>
```

Il nome utente è un'impostazione obbligatoria, la password è opzionale.

Per esempio:

```
admin
root
```

.version

Il file `.version` contiene la versione del server dalla cui zona devono essere scaricati gli aggiornamenti. Viene utilizzato per scopi di debug, di default corrisponde alla versione corrente del server in formato MM.mm.

.max-retry

Il file `.max-retry` contiene il numero massimo di tentativi in caso di errori di download da ciascuno dei server di aggiornamento.

.cdn-mode

Il file `.cdn-mode` contiene le impostazioni per l'utilizzo di Content Delivery Network (CDN) per il caricamento del repository.

Può assumere uno dei seguenti valori:

- `on` — per utilizzare CDN,
- `off` — per non utilizzare CDN.

.cert-mode

Il file `.cert-mode` contiene le impostazioni per i certificati SSL dei server di aggiornamento ammissibili che verranno accettati automaticamente.

Può assumere uno dei seguenti valori:

- `drweb` — accetta solo il certificato SSL della società Doctor Web,
- `valid` — accetta solo i certificati SSL validi,
- `any` — accetta qualsiasi certificato,
- `custom` — accetta il certificato indicato dall'utente.

.cert-file

Il file `.cert-file` contiene il percorso del certificato utente, se è indicata la modalità `custom` per il parametro `cert`.

.ssh-mode

Il file `.ssh-mode` contiene le impostazioni di modalità di autenticazione in caso di utilizzo dei protocolli SCP e SFTP (basati su SSH2).

Può assumere uno dei seguenti valori:

- `pwd` — autenticazione sulla base di nome utente e password,
- `pubkey` — autenticazione sulla base di chiavi di cifratura.

.ssh-pubkey

Il file `.ssh-pubkey` contiene il percorso della chiave pubblica SSH del server di aggiornamento.

.ssh-prikey

Il file `.ssh-prikey` contiene il percorso della chiave privata SSH del server di aggiornamento.

E2. File di configurazione dei prodotti

.description

Il file `.description` imposta il nome del prodotto. Se il file è assente, come nome del prodotto viene utilizzato il nome della relativa directory del prodotto.

Per esempio:

```
Dr.Web Server
```

..languages

Il file `..languages` contiene la lista dei codici delle lingue per le quali è configurato l'aggiornamento. Se il file è assente o vuoto, l'aggiornamento non è configurato per nessuna lingua e non verrà eseguito.

..platforms

Il file `..platforms` contiene i codici piattaforma completi utilizzati nel prodotto, per i quali è configurato l'aggiornamento. Se il file è assente o vuoto, l'aggiornamento non è configurato per nessuna piattaforma e non verrà eseguito.

..formats

Il file `..formats` contiene i formati di file per i quali è configurato l'aggiornamento, per esempio formati di documenti (html, pdf). Se il file è assente o vuoto, l'aggiornamento non è configurato per nessun formato e non verrà eseguito.

..items

Il file `..items` determina quali utility di amministrazione o prodotti aziendali devono essere aggiornati. Se il file è assente o vuoto, l'aggiornamento non è configurato per nessuna utility o prodotto e non verrà eseguito.

.sync-off

Il file `.sync-off` disattiva l'aggiornamento del prodotto. Il contenuto non ha importanza.

.deleted

Il file `.deleted` contrassegna il prodotto come rimosso. Tutte le revisioni da esso verranno rimosse, la sincronizzazione con SAM verrà disattivata.

I file di eccezioni per l'aggiornamento del repository di Server Dr.Web da SAM

.sync-only

Il file `.sync-only` contiene le espressioni regolari che definiscono la lista dei file di repository che verranno sincronizzati durante l'aggiornamento del repository da SAM. I file di repository non impostati in `.sync-only` non verranno sincronizzati. Se il file `.sync-only` è assente, verranno sincronizzati tutti i file di repository salvo i file esclusi secondo le impostazioni nel file `.sync-ignore`.

.sync-ignore

Il file `.sync-ignore` contiene le espressioni regolari che definiscono la lista dei file di repository che verranno esclusi dalla sincronizzazione durante l'aggiornamento del repository da SAM.

Un esempio del file con le eccezioni

```
^windows-nt-x64/

^windows-nt/

^windows/
```

Ordine dell'utilizzo dei file di configurazione

Se per un prodotto sono presenti i file `.sync-only` e `.sync-ignore`, viene utilizzato il seguente schema di azioni:

1. Prima si applica `.sync-only`. I file non elencati in `.sync-only` non vengono processati.
2. Ai file rimanenti si applica `.sync-ignore`.

I file di eccezioni per l'aggiornamento degli Agent Dr.Web dal Server Dr.Web

.state-only

Il file `.state-only` contiene le espressioni regolari che definiscono la lista dei file che verranno sincronizzati durante l'aggiornamento degli Agent Dr.Web dal Server Dr.Web. I file di repository non impostati in `.state-only` non verranno sincronizzati. Se il file `.state-only` è assente, verranno sincronizzati tutti i file di repository tranne i file di repository esclusi secondo le impostazioni nel file `.state-ignore`.

.state-ignore

Il file `.state-ignore` contiene le espressioni regolari che definiscono la lista dei file che verranno esclusi dalla sincronizzazione durante l'aggiornamento degli Agent Dr.Web dal Server Dr.Web.

Per esempio:

- non è necessario ricevere le lingue di interfaccia tedesco, cinese e spagnolo (le altre sono da ricevere),
- non c'è bisogno di ricevere i componenti progettati per gli SO Windows a 64 bit.

```
;^common/ru-.*\.dwl$ questo verrà aggiornato

^common/de-.*\.dwl$

^common/cn-.*\.dwl$

^common/es-.*\.dwl$

^win/de-.*

^win/cn-.*

^windows-nt-x64\.*
```

L'ordine di priorità di applicazione di `.state-only` e `.state-ignore` è analogo a quello di `.sync-only` e `.sync-ignore`.

Impostazioni di invio delle notifiche

I file del gruppo `notify` consentono di configurare il sistema di notifica in caso di aggiornamento riuscito dei prodotti di repository corrispondenti.

Queste impostazioni si applicano solo alla notifica **Il prodotto è aggiornato**. Le eccezioni non valgono per altri tipi di notifiche.

Le impostazioni del sistema di notifica sono descritte in **Manuale dell'amministratore**, p. Configurazione delle notifiche.

.notify-only

Il file `.notify-only` contiene la lista dei file di repository, alla modifica dei quali viene inviata una notifica.

.notify-ignore

Il file `.notify-ignore` contiene la lista dei file di repository, alla modifica dei quali non vengono inviate le notifiche.

Ordine dell'utilizzo dei file di configurazione

Se per un prodotto sono presenti i file `.notify-only` e `.notify-ignore`, viene utilizzato il seguente schema di azioni:

1. Quando si aggiorna il prodotto, i file aggiornati da SAM vengono confrontati con le liste di eccezioni.
2. Prima vengono esclusi i file presenti nella lista `.notify-ignore`.
3. Dai file rimanenti vengono esclusi i file non presenti nella lista `.notify-only`.
4. Se sono rimasti file non esclusi nei passaggi precedenti, le notifiche vengono inviate.

Se i file `.notify-only` e `.notify-ignore` sono assenti, le notifiche verranno sempre inviate (se attivate sulla pagina **Configurazione delle notifiche** nel Pannello di controllo).

Per esempio:

Se nel file `.notify-ignore` è impostata l'eccezione `^.vdb.lzma$`, in caso di aggiornamento dei soli file dei database dei virus, la notifica non verrà inviata. Se oltre ai database, è stato aggiornato il motore `drweb32.dll`, la notifica verrà inviata.

Impostazioni di congelamento

.delay-config

Il file `.delay-config` contiene le impostazioni che vietano di utilizzare una revisione nuova del prodotto. Il repository continua a distribuire la revisione precedente, la sincronizzazione non viene più eseguita (lo stato del prodotto viene "congelato"). Se l'amministratore ritiene che la revisione accettata sia adatta per la distribuzione, deve consentire la distribuzione nel Pannello di controllo (v. **Manuale dell'amministratore**, p. Gestione del repository di Server Dr.Web).

Il file contiene due parametri non sensibili alle maiuscole e separati da un punto e virgola.

Formato del file:

```
Delay [ON|OFF|APPROVAL]; UseFilter [YES|NO]
```

Parametro	Valori possibili	Descrizione
`Delay`	`ON|OFF|APPROVAL`	• `ON` — è attivato il congelamento degli aggiornamenti del prodotto. • `OFF` — è disattivato il congelamento degli aggiornamenti del prodotto. • `APPROVAL` — congelamento degli aggiornamenti del prodotto fino alla conferma da parte dell'amministratore.
`UseFilter`	`YES|NO`	• `Yes` — congela gli aggiornamenti solo se i file aggiornati corrispondono alla lista di eccezioni nel file `.delay-only`. • `No` — congela gli aggiornamenti in ogni caso.

Per esempio:

```
Delay ON; UseFilter NO
```

.delay-only

Il file `.delay-only` contiene una lista dei file, in caso di modifica dei quali è vietato utilizzare una nuova revisione del prodotto. La lista dei file viene impostata nel formato di espressioni regolari.

Se un file dall'aggiornamento di repository coincide con le maschere indicate e l'impostazione `UseFilter` nel file `.sync-only` è abilitata, la revisione verrà congelata.

.rev-to-keep

Il file `.rev-to-keep` contiene il numero di revisioni conservate del prodotto.

Per esempio:

```
3
```

.on-demand

La presenza del file significa che è attivata la sincronizzazione del prodotto su richiesta, cioè in presenza di client che chiedono questo prodotto.

.is-sync-off-in

La presenza del file significa che è disattivata la ricezione degli aggiornamenti del prodotto attraverso le relazioni tra i server.

.is-sync-off-out

La presenza del file significa che è disattivata la distribuzione degli aggiornamenti del prodotto attraverso le relazioni tra i server.

.no-platform

La presenza del file significa che le directory di livello superiore nella revisione del prodotto non sono considerate piattaforme, cioè la revisione si applica a qualsiasi piattaforma.

Allegato F. Formato dei file di configurazione

In questa sezione si descrive il formato dei seguenti file:

File	Descrizione
drwcsd.conf	File di configurazione del Server Dr.Web.
webmin.conf	File di configurazione del Pannello di controllo della sicurezza Dr.Web.
download.conf	File di configurazione per l'impostazione dei dati scaricati dal Server Dr.Web.
drwcsd-proxy.conf	File di configurazione del Server proxy Dr.Web.

File	Descrizione
drwreploader.conf	File di configurazione del Loader di repository.

Se sul computer con il componente corrispondente è installato un Agent Dr.Web con autoprotezione attivata, prima di modificare i file di configurazione, è necessario disattivare il componente di autoprotezione Dr.Web Self-protection attraverso le impostazioni di Agent Dr.Web.

Dopo che sono state salvate tutte le modifiche apportate, si consiglia di riattivare il componente Dr.Web Self-protection.

F1. File di configurazione di Server Dr.Web

Di default, il file di configurazione di Server Dr.Web `drwcsd.conf` si trova nella sottodirectory `etc` della directory radice di Server Dr.Web. Quando il Server Dr.Web viene avviato, attraverso un parametro della riga di comando è possibile impostare un percorso e un nome non standard del file di configurazione (per maggiori informazioni v. Allegato G3. Server Dr.Web).

Per modificare manualmente il file di configurazione del Server Dr.Web

1. Arrestare il Server Dr.Web (v. **Manuale dell'amministratore** p. Server Dr.Web).
2. Disattivare l'Autoprotezione (se sul computer è presente un Agent Dr.Web con l'Autoprotezione attiva — nel menu contestuale dell'Agent Dr.Web).
3. Apportare le modifiche necessarie al file di configurazione del Server Dr.Web.
4. Avviare il Server Dr.Web (v. **Manuale dell'amministratore** p. Server Dr.Web).

Il formato del file di configurazione del Server Dr.Web

Il file di configurazione del Server Dr.Web è in formato XML.

Descrizione dei parametri del file di configurazione del Server Dr.Web:

- `<version value="" />`

  La versione attuale del file di configurazione.

- `<name value="" />`

  Nome del Server Dr.Web o del cluster di Server Dr.Web utilizzato nella ricerca dagli Agent Dr.Web, installer di Agent Dr.Web o dal Pannello di controllo. Lasciare vuoto il valore del parametro ("" — si usa di default) per utilizzare il nome del computer su cui è installato il Server Dr.Web.

Come indirizzo di Server Dr.Web è consigliato utilizzare il nome di Server Dr.Web in formato FQDN, preventivamente registrato nel servizio DNS. Questo semplificherà il processo di configurazione della rete antivirus, relativo alla procedura di reinstallazione di Server Dr.Web su un altro computer. In tale caso, se verrà cambiato l'indirizzo di Server Dr.Web, sarà sufficiente modificarlo nelle impostazioni del server DNS per il nome del computer con Server Dr.Web in modo che tutti gli agent si connettano automaticamente al nuovo server.

1. Se nella rete funziona un server DNS locale, è necessario creare in esso un nome separato per Server Dr.Web, nonché per Server proxy Dr.Web (per esempio, `drwebes.company.lan`).
2. Nelle impostazioni di Agent Dr.Web, deve essere indicato il nome di Server Dr.Web in formato FQDN.
3. Oltre al nome in formato FQDN, nelle impostazioni di Agent Dr.Web è consigliato aggiungere anche l'indirizzo di Server Dr.Web e mantenere aggiornato questo indirizzo in caso di sua modifica. In questo caso, se è impossibile utilizzare il nome di server, l'agent effettuerà il tentativo di connessione in base all'indirizzo di server.

- `<id value="" />`

  Identificatore univoco del Server Dr.Web. Nelle versioni precedenti era incluso nella chiave di licenza del Server Dr.Web. A partire dalla versione 10 è conservato nel file di configurazione del Server Dr.Web.

- `<passwd-salt value="" />`

  Salt crittografico. Una stringa di dati casuali che viene aggiunta alla password dell'amministratore, dopodiché il valore combinato viene elaborato dalla funzione hash e viene conservato come un unico hash nel database per la protezione della password dalla violazione tramite la selezione di varianti possibili. Viene generato di default all'installazione o l'aggiornamento del Server Dr.Web dalle versioni precedenti.

  Oltre al salt statico, per ciascuna password viene generato anche un salt dinamico. Come codice di autenticazione HMAC al calcolo dell'impronta di una password con salt, viene utilizzato lo standard di generazione di chiavi basato su password PBKDF2. Pertanto, la combinazione della password e del salt con il successivo hashing viene eseguita molteplici volte. Il salt statico è disattivato di default, il salt dinamico viene sempre utilizzato.

  In presenza di salt, la visualizzazione e la modifica della password amministratore tramite l'utility fornita per la gestione del database Server Dr.Web (`drwidbsh3`) diventano impossibili.

  Nel caso di utilizzo di un cluster dei Server Dr.Web, è necessario impostare manualmente lo stesso valore salt su tutti i Server Dr.Web che fanno parte del cluster.

- `<location city="" country="" department="" floor="" latitude="" longitude="" organization="" province="" room="" street="" />`

  Posizione geografica del Server Dr.Web.

  Descrizione degli attributi:

Attributo	Descrizione
city	Città
country	Paese
department	Nome del reparto
floor	Piano
latitude	Latitudine
longitude	Longitudine
organization	Nome dell'ente
province	Nome della regione
room	Numero della camera
street	Nome della via

- `<threads count="" />`

  Numero di flussi di elaborazione dei dati provenienti dai client di Server Dr.Web (Agent Dr.Web e i relativi installer, Server Dr.Web adiacenti, Server proxy Dr.Web). Il valore minimo è 5. Di default è 5.

  Questo parametro influisce sulle prestazioni di Server Dr.Web. In caso di utilizzo del database incorporato, non è consigliabile modificare il valore di default. In caso di utilizzo di un database esterno, potrebbe essere necessario un valore di parametro più grande (v. sezione Carico su Server Dr.Web e parametri di configurazione raccomandati). In caso di utilizzo di una rete con un numero elevato di connessioni client a Server Dr.Web, prima di modificare il valore, si consiglia di ottenere consulenza nel servizio di supporto tecnico dell'azienda Doctor Web.

- `<newbie approve-to-group="" mode="" />`

  Modalità di accesso di nuove postazioni.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
approve-to-group	–	Il gruppo che verrà impostato di default alle nuove postazioni come il gruppo primario in modalità **Consenti l'accesso automaticamente** (`mode='open'`).	Valore vuoto che significa imposta il gruppo **Everyone** come il gruppo primario.
mode	• `open` — consenti l'accesso automaticamente,	Criteri di connessione di nuove postazioni.	–

Attributo	Valori ammissibili	Descrizione	Di default
	• `closed` — sempre nega l'accesso, • `approval` — conferma l'accesso manualmente.		

Per maggiori informazioni v. **Manuale dell'amministratore**, p. Criteri di approvazione delle postazioni.

- `<emplace-auto enabled="" />`

  Modalità di creazione di account di postazioni nel Pannello di controllo durante l'installazione degli Agent Dr.Web da un pacchetto di installazione di gruppo se gli account già creati non sono sufficienti.

Attributo	Valori ammissibili	Di default
`enabled`	• `yes` — crea automaticamente account di postazioni mancanti, • `no` — l'installazione è possibile solo per il numero di account già creati nel gruppo per le cui postazioni viene avviato il pacchetto di installazione.	`yes`

- `<unauthorized-to-newbie enabled="" />`

  I criteri applicati alle postazioni non autenticate. I valori ammissibili dell'attributo `enabled`:

  - `yes` — le postazioni non autenticate (per esempio, nel caso di danneggiamento del database) verranno trasferite automaticamente nello stato nuovi arrivi,
  - `no` (predefinito) — la modalità di funzionamento normale.

- `<maximum-authorization-queue size="" />`

  Numero massimo di postazioni nella coda per l'autenticazione sul Server Dr.Web. Non è consigliabile modificare il valore del parametro senza raccomandazione del servizio di supporto Doctor Web.

- `<reverse-resolve enabled="" />`

  Sostituisci gli indirizzi IP con i nomi DNS dei computer nel file di log del Server Dr.Web. I valori ammissibili dell'attributo `enabled`:

  - `yes` — mostra i nomi DNS,
  - `no` (predefinito) — mostra gli indirizzi IP.

- `<replace-netbios-names enabled="" host="" />`

  Sostituisci i nomi NetBIOS dei computer con i nomi DNS.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione
`enabled`	• `yes` — sostituisci,	Modalità di sostituzione dei nomi NetBIOS.

Attributo	Valori ammissibili	Descrizione
	• `no` — non sostituire. Verranno applicate le impostazioni `<agent-host-names />`.	
`host`	• `yes` — visualizza nomi DNS parzialmente qualificati (prima di un punto nel FQDN), • `no` — visualizza nomi DNS completamente qualificati (FQDN).	Formato del nome visualizzato dopo la sostituzione.

- `<agent-host-names mode="" />`

  Modalità di visualizzazione dei nomi dei computer nella rete antivirus alla connessione al Server Dr.Web. Valori ammissibili dell'attributo `mode`:

  - `netbios` — visualizza i nomi NetBIOS (viene utilizzato di default se il valore dell'attributo è vuoto o tutto il parametro è assente),
  - `fqdn` — visualizza nomi DNS completamente qualificati (FQDN),
  - `host` — visualizza nomi DNS parzialmente qualificati (prima di un punto nel FQDN).

- `<dns>`

  Le impostazioni DNS.

  - `<timeout value="" />`

    Timeout in secondi per la risoluzione delle query DNS dirette/inverse. Lasciare vuoto il valore per non limitare il tempo di attesa della fine della risoluzione.

  - `<retry value="" />`

    Il numero massimo di query DNS ripetute in caso di una risoluzione di query DNS non riuscita.

  - `<cache enabled="" negative-ttl="" positive-ttl="" />`

    Il tempo di conservazione nella cache delle risposte del server DNS.

    Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione
`enabled`	• `yes` — conserva le risposte nella cache, • `no` — non conservare le risposte nella cache.	Modalità di conservazione delle risposte nella cache.
`negative-ttl`	–	Tempo in minuti di conservazione nella cache (TTL) delle risposte negative del server DNS.
`positive-ttl`	–	Tempo in minuti di conservazione nella cache (TTL) delle risposte positive del server DNS.

- <servers>

  Una lista dei server DNS che sostituisce la lista di sistema predefinita. Contiene uno o più elementi figlio <server address="" /> in cui il parametro address definisce l'indirizzo IP del server.

- <domains>

  Una lista dei domini DNS che sostituisce la lista di sistema predefinita. Contiene uno o più elementi figlio <domain name="" /> in cui il parametro name definisce il nome del dominio.

- <cache>

  Impostazioni di memorizzazione nella cache.

  L'elemento <cache> contiene i seguenti elementi figlio:

  - <interval value="" />

    Periodicità in secondi di pulizia completa della cache.

  - <quarantine ttl="" />

    Periodicità in secondi di eliminazione dei file nella quarantena del Server Dr.Web. Di default è 604800 (una settimana).

  - <download ttl="" />

    Periodicità di eliminazione di pacchetti di installazione individuali. Di default è 604800 (una settimana).

  - <repository ttl="" />

    Periodicità in secondi di eliminazione dei file nella cache del repository del Server Dr.Web.

  - <file ttl="" />

    Periodicità in secondi di pulizia della cache dei file. Di default è 604800 (una settimana).

- <replace-station-description enabled="" />

  Sincronizza le descrizioni di postazioni sul Server Dr.Web con il campo **Computer description** sulla pagina **System properties** su postazione. I valori ammissibili dell'attributo enabled:

  - yes — sostituisci la descrizione sul Server Dr.Web con la descrizione dalla postazione,
  - no (predefinito) — ignora la descrizione sulla postazione.

- <time-discrepancy value="" />

  Differenza ammissibile in minuti tra l'ora di sistema del Server Dr.Web e quella degli Agent Dr.Web. Se la differenza supera il valore specificato, questo verrà contrassegnato nello stato della postazione sul Server Dr.Web. Di default è ammissibile una differenza di 3 minuti. Il valore vuoto o il valore 0 significa che il controllo non verrà eseguito.

- <encryption mode="" />

  Modalità di cifratura del traffico dati. I valori ammissibili dell'attributo mode:

  - yes — utilizza la cifratura,
  - no — non utilizzare la cifratura,

- `possible` — la cifratura è ammissibile.

Di default, è `yes`.

Per maggiori informazioni v. **Manuale dell'amministratore**, p. Cifratura e compressione del traffico dati.

- `<compression level="" mode="" />`

Modalità di compressione del traffico dati.

Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione
`level`	Un numero intero da 1 a 9.	Livello di compressione.
`mode`	• `yes` — utilizza la compressione, • `no` — non utilizzare la compressione, • `possible` — la compressione è ammissibile.	Modalità di compressione.

Per maggiori informazioni v. **Manuale dell'amministratore**, p. Cifratura e compressione del traffico dati.

- `<track-agent-jobs enabled="" />`

Consenti di tenere traccia dei risultati di esecuzione dei task su postazioni e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<track-agent-status enabled="" />`

Consenti di tenere traccia dei cambiamenti nello stato delle postazioni e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<track-virus-bases enabled="" />`

Consenti di tenere traccia dei cambiamenti nello stato (parti, modifiche) dei database dei virus e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`. Il parametro viene ignorato se `<track-agent-status enabled="no" />`.

- `<track-agent-modules enabled="" />`

Consenti di tenere traccia delle versioni dei moduli di postazioni e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<track-agent-components enabled="" />`

Consenti di tenere traccia della lista dei componenti installati su postazioni e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<track-agent-userlogon enabled="" />`

Consenti di tenere traccia delle sessioni utente su postazioni e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<track-agent-environment enabled="" />`

  Consenti di tenere traccia della lista degli hardware e dei software su postazioni e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<keep-run-information enabled="" />`

  Consenti di tenere traccia delle informazioni sull'avvio e l'arresto dei componenti antivirus su postazioni e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<keep-infection enabled="" />`

  Consenti di tenere traccia del rilevamento di minacce su postazioni e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<keep-scan-errors enabled="" />`

  Consenti di tenere traccia degli errori di scansione su postazioni e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<keep-scan-statistics enabled="" />`

  Consenti di tenere traccia delle statistiche di scansioni su postazioni e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<keep-installation enabled="" />`

  Consenti di tenere traccia delle informazioni sulle installazioni di Agent Dr.Web su postazione e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<keep-blocked-devices enabled="" />`

  Consenti di tenere traccia delle informazioni sui dispositivi bloccati dal componente Office control e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<keep-appcontrol-activity enabled="" />`

  Consenti di tenere traccia dell'attività dei processi su postazioni, registrata dal Controllo applicazioni (per riempire il Prontuario applicazioni), e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<keep-appcontrol-block enabled="" />`

  Consenti di tenere traccia dei blocchi dei processi su postazioni, effettuati dal Controllo applicazioni, e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<quarantine enabled="" />`

  Consenti di tenere traccia delle informazioni sullo stato della Quarantena su postazioni e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<update-bandwidth queue-size="" value="" />`

  Larghezza di banda massima in KB/s per la trasmissione di aggiornamenti tra il Server Dr.Web e gli Agent Dr.Web.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`queue-size`	• un numero intero positivo, • `unlimited`.	Numero massimo ammissibile di sessioni di distribuzione aggiornamenti avviate contemporaneamente dal Server Dr.Web. Quando viene raggiunto il limite indicato, le richieste dagli Agent Dr.Web vengono messe in una coda di attesa. La dimensione della coda di attesa non è limitata.	`unlimited`
`value`	• velocità massima in KB/s, • `unlimited`.	Valore massimo della velocità complessiva per la trasmissione di aggiornamenti.	`unlimited`

- `<install-bandwidth queue-size="" value="" />`

  Larghezza di banda massima in KB/s per la trasmissione di dati dal Server Dr.Web nel corso di installazione degli Agent Dr.Web su postazioni.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`queue-size`	• un numero intero positivo, • `unlimited`.	Numero massimo ammissibile di sessioni di installazione di Agent Dr.Web avviate contemporaneamente dal Server Dr.Web. Quando viene raggiunto il limite indicato, le richieste dagli Agent Dr.Web vengono messe in una coda di attesa. La dimensione della coda di attesa non è limitata.	`unlimited`
`value`	• velocità massima in KB/s, • `unlimited`.	Valore massimo della velocità complessiva di trasmissione di dati nel corso dell'installazione degli Agent Dr.Web.	`unlimited`

- `<geolocation enabled="" startup-sync="" />`

  Consenti la sincronizzazione della posizione geografica delle postazioni tra i Server Dr.Web.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione
`enabled`	• `yes` — consenti la sincronizzazione, • `no` — disattiva la sincronizzazione.	Modalità di sincronizzazione.

Attributo	Valori ammissibili	Descrizione
`startup-sync`	Un numero intero positivo.	Numero di postazioni senza coordinate geografiche di cui le informazioni vengono richieste quando viene stabilita una connessione tra i Server Dr.Web.

- `<audit enabled="" />`

  Consenti di tenere traccia delle operazioni dell'amministratore nel Pannello di controllo della sicurezza Dr.Web e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<audit-internals enabled="" />`

  Consenti di tenere traccia delle operazioni interne del Server Dr.Web e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<audit-xml-api enabled="" />`

  Consenti di tenere traccia delle operazioni attraverso Web API e registrare le informazioni nel database del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<proxy auth-list="" enabled="" host="" password="" user="" />`

  Parametri delle connessioni al Server Dr.Web attraverso il server proxy HTTP.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione

`auth-list`	• `none` — non utilizzare l'autenticazione,
	• `any` — qualsiasi metodo da quelli supportati,
	• `safe` — qualsiasi metodo sicuro da quelli supportati,
	• i seguenti metodi, se ci sono più metodi, indicare tutti quelli necessari separati da uno spazio:
	  ▫ `basic`
	  ▫ `digest`
	  ▫ `digestie`
	  ▫ `ntlmwb`
	  ▫ `ntlm`
	  ▫ `negotiate`
		Tipo di autenticazione sul server proxy. Di default è `any`.

`enabled`	• `yes` — utilizza server proxy, • `no` — non utilizzare server proxy.	Modalità di connessione al Server Dr.Web attraverso un server proxy HTTP.
`host`	–	Indirizzo del server proxy.
`password`	–	Password dell'utente del server proxy se sul server proxy è richiesta l'autenticazione.

Attributo	Valori ammissibili	Descrizione
user	–	Nome dell'utente del server proxy se sul server proxy è richiesta l'autenticazione.

Nell'impostazione dell'elenco dei metodi di autenticazione disponibili per il server proxy è possibile utilizzare il tag `only` (si aggiunge alla fine dell'elenco dopo uno spazio) per modificare l'algoritmo di selezione dei metodi di autenticazione.

Per maggiori informazioni v. https://curl.se/libcurl/c/CURLOPT_HTTPAUTH.html.

- `<statistics enabled="" id="" interval="" />`

  Parametri di invio di informazioni statistiche su eventi di virus alla società Doctor Web nella sezione https://stat.drweb.com/.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
enabled	• yes — invia le statistiche, • no — non inviare le statistiche.	Modalità di invio di statistiche alla società Doctor Web.	–
id	–	MD5 della chiave di licenza di Agent Dr.Web.	–
interval	Un numero intero positivo.	Intervallo in minuti per inviare statistiche.	30

- `<cluster>`

  Parametri di cluster dei Server Dr.Web per lo scambio delle informazioni in una configurazione di rete antivirus con diversi server.

  Contiene uno o più elementi figlio `<on multicast-group="" port="" interface="" />`.

  Descrizione degli attributi:

Attributo	Descrizione
multicast-group	Indirizzo IP del gruppo multicast attraverso cui i Server Dr.Web si scambieranno informazioni.
port	Numero di porta dell'interfaccia di rete a cui è legato il protocollo di trasporto per la trasmissione delle informazioni nel gruppo multicast.
interface	Indirizzo IP dell'interfaccia di rete a cui è legato il protocollo di trasporto per la trasmissione delle informazioni nel gruppo multicast.

- `<multicast-updates enabled="" />`

  Configurazione della trasmissione degli aggiornamenti per gruppi alle postazioni attraverso il protocollo multicast. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

  L'elemento `<multicast-updates>` contiene una serie di elementi figlio e attributi:

Elemento figlio	Attributo	Descrizione	Di default

`port`
 	
`<port value="" />`
	`value`	Numero di porta dell'interfaccia di rete di Server Dr.Web a cui viene legato il protocollo di trasporto multicast per la trasmissione degli aggiornamenti. Questa porta verrà utilizzata da tutti i gruppi multicast.
		
		Per gli aggiornamenti di gruppo è necessario impostare qualsiasi porta libera che sarà diversa dalla porta assegnata nelle impostazioni al funzionamento del protocollo di trasporto del Server Dr.Web stesso.
			2197

`ttl`
 	
`<ttl value="" />`
	`value`	Durata di vita del datagramma UDP trasmesso. Il valore impostato verrà utilizzato da tutti i gruppi multicast.	8

`group`
 	
`<group address="" />`
	`address`	Indirizzo IP del gruppo multicast attraverso cui le postazioni riceveranno gli aggiornamenti per gruppi.	233.192.86.0 in caso di IPv4
			
			FF0E::176 in caso di IPv6

`on`
 	
`<on interface="" ttl="" />`
	`interface`	Indirizzo IP dell'interfaccia di rete del Server Dr.Web a cui viene legato il protocollo di trasporto multicast per la trasmissione degli aggiornamenti.	–

	`ttl`	Durata di vita di un datagramma UDP trasmesso attraverso l'interfaccia di rete impostata. Ha la precedenza sull'elemento figlio generale `<ttl value="" />`.	8

`transfer`
 	
`<transfer datagram-size="" assembly-timeout="" updates-interval="" chunks-interval="" resend-interval="" silence-interval="" accumulate-`
	`datagram-size`	Dimensione del datagramma UDP — dimensione in byte dei datagrammi UDP utilizzati dal protocollo multicast.
		
		L'intervallo ammissibile è 512–8192. Per evitare la frammentazione, si consiglia di impostare un valore inferiore all'MTU (Maximum Transmission Unit) della rete in uso.
			1400

Elemento figlio	Attributo	Descrizione	Di default
`interval="" announce-send-times="" />`	`assembly-timeout`	Tempo di trasmissione del file (ms) — durante l'intervallo specificato viene trasmesso un file di aggiornamento, dopodiché il Server Dr.Web 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.	180000
	`updates-interval`	Durata degli aggiornamenti di gruppo (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.	600000
	`chunks-interval`	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.	14
	`resend-interval`	Intervallo tra le richieste di ritrasmissione (ms) — con questo intervallo gli Agent Dr.Web inviano le richieste di ritrasmissione dei pacchetti persi. Il Server Dr.Web accumula queste query, dopodiché trasmette i blocchi persi.	1000
	`silence-interval`	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 Dr.Web, il Server Dr.Web ritiene che tutti gli Agent Dr.Web abbiano ottenuto con successo i file di aggiornamento e inizia a trasmettere il file successivo.	10000

Elemento figlio	Attributo	Descrizione	Di default
	`accumulate-interval`	Intervallo per accumulare le richieste di ritrasmissione (ms) — durante questo intervallo il Server Dr.Web accumula le richieste degli Agent Dr.Web per la ritrasmissione dei pacchetti persi. Gli Agent Dr.Web chiedono l'invio ripetuto dei pacchetti persi. Il Server Dr.Web accumula queste richieste durante il tempo specificato, dopodiché trasmette i blocchi persi.	2000
	`announce-send-times`	Numero di annunci di trasmissione del file — numero di volte in cui il Server Dr.Web annuncia la trasmissione di un file nel gruppo multicast prima di iniziare la trasmissione degli aggiornamenti. All'annuncio, nel gruppo multicast viene inviato un datagramma UDP con i metadati del file. Un aumento del numero di annunci è capace di migliorare l'affidabilità della trasmissione, ma può portare a una diminuzione della quantità di dati che potranno essere trasmessi durante il tempo assegnato per l'aggiornamento tramite il protocollo multicast.	3

L'elemento **<multicast-updates>** può anche facoltativamente contenere l'elemento figlio **<acl>** che viene utilizzato per creare liste di accesso. Ciò consente di limitare il cerchio di indirizzi TCP delle postazioni che potranno ricevere aggiornamenti di gruppo tramite il protocollo multicast da questo Server Dr.Web. Di default l'elemento figlio **<acl>** è assente, il che significa l'assenza di qualsiasi limitazione.

<acl> come parte di **<multicast-updates>** contiene i seguenti elementi figlio:

- **<priority mode="" />**

  Imposta la priorità delle liste. I valori ammissibili dell'attributo `mode`: `allow` o `deny`. Con il valore **<priority mode="deny" />** la lista **<deny>** ha una priorità più alta rispetto alla lista **<allow>**. Gli indirizzi non inclusi in nessuna delle liste o inclusi in tutte e due vengono vietati. Vengono consentiti solo gli indirizzi inclusi nella lista **<allow>** e non inclusi nella lista **<deny>**.

- **<allow>**

  Lista di indirizzi TCP per cui sono disponibili gli aggiornamenti tramite il protocollo multicast. L'elemento **<allow>** contiene uno o più elementi figlio **<ip address="" />** per impostare gli indirizzi consentiti nel formato IPv4 e **<ip6 address="" />** per impostare gli indirizzi consentiti nel formato IPv6. Nell'attributo `address` vengono impostati gli indirizzi di rete nel formato: <*indirizzo IP*>/[<*prefisso*>].

- `<deny>`

  Lista di indirizzi TCP per cui non sono disponibili gli aggiornamenti tramite il protocollo multicast. L'elemento `<deny>` contiene uno o più elementi figlio `<ip address="" />` per impostare gli indirizzi proibiti nel formato IPv4 e `<ip6 address="" />` per impostare gli indirizzi proibiti nel formato IPv6. Nell'attributo `address` vengono impostati gli indirizzi di rete nel formato: <*indirizzo IP*>/[<*prefisso*>].

- `<database connections="" speedup="" />`

  Definizione del database.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`connections`	Un numero intero positivo.	Numero massimo consentito di connessioni del database con il Server Dr.Web. In caso di utilizzo del database incorporato, non è consigliabile modificare il valore di default. In caso di utilizzo di un database esterno, potrebbe essere necessario un valore di attributo più grande (v. sezione Carico su Server Dr.Web e parametri di configurazione raccomandati). In caso di utilizzo di una rete con un numero elevato di connessioni client a Server Dr.Web, prima di modificare il valore, si consiglia di ottenere consulenza nel servizio di supporto tecnico dell'azienda Doctor Web.	2
`speedup`	`yes | no`	Esegui automaticamente la pulizia differita del database dopo un'inizializzazione, un aggiornamento e un'importazione del database (v. **Manuale dell'amministratore**, p. Database).	`yes`

  L'elemento `<database>` contiene uno dei seguenti elementi figlio:

  

  L'elemento `<database>` può contenere solo un elemento figlio che definisce un database specifico.

  Non è consigliabile modificare senza il coordinamento con il servizio di supporto tecnico Doctor Web gli attributi dei database che possono essere presenti nel modello di file di configurazione, ma non sono riportati nelle descrizioni.

  - `<sqlite dbfile="" cache="" cachesize="" readuncommitted="" precompiledcache="" synchronous="" checkintegrity="" autorepair="" mmapsize="" wal="" wal-max-pages="" wal-max-seconds="" />`

    Definisce il database incorporato SQLite3.

    Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
dbfile	–	Nome del file del database.	database.sqlite
cache	SHARED | PRIVATE	Modalità di memorizzazione nella cache.	SHARED
cachesize	Un numero intero positivo.	Dimensione della memoria cache del database (in pagine di 1,5 Kb).	2048
readuncommitted	on | off	Passaggio al livello di isolamento della transazione READ UNCOMMITTED (lettura dei dati che sono stati modificati o cancellati ma per cui non è stato eseguito il commit da un'altra transazione).	off
precompiledcache	Un numero intero positivo.	Dimensione in byte della cache degli operatori SQL precompilati.	1048576
synchronous	• TRUE o FULL — sincrona • FALSE o NORMAL — normale • OFF — asincrona	Modalità di registrazione dei dati.	FULL
checkintegrity	quick | full | no	Verifica dell'integrità dell'immagine del database ad avvio del Server Dr.Web.	quick
autorepair	yes | no	Ripristino automatico dell'integrità dell'immagine del database ad avvio del Server Dr.Web.	no
mmapsize	Un numero intero positivo.	La dimensione massima in byte del file di database che è ammissibile mappare nello spazio degli indirizzi del processo in un momento.	• in caso di SO della famiglia Unix — 10485760 • in caso di SO Windows — 0
wal	yes | no	Utilizzo della registrazione di log proattiva (Write-Ahead Logging).	yes
wal-max-pages	–	Numero massimo di pagine "sporche", raggiunto il quale le pagine vengono registrate su disco.	1000

Attributo	Valori ammissibili	Descrizione	Di default
wal-max-seconds	–	Tempo massimo (in secondi) per il quale viene rinviata la registrazione delle pagine su disco.	30

```
<pgsql dbname="drwcs" host="localhost" port="5432" options="" requiressl="" user=""
password="" temp_tablespaces="" default_transaction_isolation="" debugproto ="yes" />
```

Definisce il database esterno PostgreSQL.

Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
dbname	–	Nome del file del database.	–
host	–	Indirizzo del server PostgreSQL o percorso al socket di dominio UNIX.	–
port	–	Il numero di porta del server PostgreSQL o l'estensione del nome di file del socket Unix.	–
options	–	Parametri della riga di comando per l'invio sul server del database. Per maggiori informazioni v. capitolo 18 https://www.postgresql.org/docs/9.1/libpq-connect.html	–
requiressl	• 1 | 0 (attraverso il Pannello di controllo) • y | n • yes | no • on | off	Utilizza solamente le connessioni SSL.	• 0 • y • yes • on
user	–	Nome dell'utente del database.	–
password	–	Password dell'utente del database.	–
temp_tablespaces	–	Namespace per le tabelle temporanee del database.	–
default_transaction_isolation	• read uncommitted • read committed • repeatable read	Livello di isolamento delle transazioni.	read committed

Attributo	Valori ammissibili	Descrizione	Di default
	• serializable		
debugproto	• yes | no • on | off	Registra il log di funzionamento del DBMS di debug.	• yes • on

- `<oracle connectionstring="" user="" password="" client="" prefetch-rows="0" prefetch-mem="0" />`

  Definisce il database esterno Oracle.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
connectionstring	–	Stringa contenente Oracle SQL Connect URL o le coppie chiave-valore Oracle Net.	–
user	–	Nome dell'utente del database.	–
password	–	Password dell'utente del database.	–
client	–	Percorso del client per l'accesso al database Oracle (Oracle Instant Client). Server Dr.Web viene fornito insieme a Oracle Instant Client versione 11. Se si utilizzano server Oracle di una versione successiva o sono presenti errori nel driver del database Oracle fornito, è possibile scaricare il relativo driver dal sito Oracle e specificare il percorso di questo driver in questo campo.	–
prefetch-rows	0–65535	Numero di righe per la preselezione quando viene eseguita una query al database.	0 — utilizza il valore = 1 (il valore di default del database)
prefetch-mem	0–65535	La quantità di memoria allocata per la preselezione di righe quando viene eseguita una query al database.	0 — non è limitata

- `<odbc dsn="drwcs" user="" pass="" limit="" transaction="DEFAULT" />`

  Definisce la connessione ad un database esterno tramite ODBC.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
dsn	–	Nome dell'origine dati ODBC.	drwcs

Attributo	Valori ammissibili	Descrizione	Di default
user	–	Nome dell'utente del database.	drwcs
pass	–	Password dell'utente del database.	drwcs
limit	Un numero intero positivo.	Riconnettiti al DBMS dopo il numero indicato di transazioni.	0 — non riconnetterti
transaction	• SERIALIZABLE — ordinabilità • READ_UNCOMMITTED — lettura dei dati non impegnati • READ_COMMITTED — lettura dei dati impegnati • REPEATABLE_READ — ripetibilità di lettura • DEFAULT — equivale a "" — dipende dal DBMS.	Livello di isolamento delle transazioni. Alcuni DBMS supportano soltanto READ_COMMITTED.	DEFAULT

- `<mysql dbname="drwcs" host="localhost" port="3306" user="" password="" ssl="no" precompiledcache="" debug="no" />`

  Definisce il database esterno MySQL/MariaDB.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
dbname	–	Nome del database.	drwcs
host	Uno dei due.	Indirizzo del server del database per la connessione tramite TCP/IP.	localhost
		Percorso del file di socket UNIX per l'utilizzo di UDS. Se il percorso non è impostato, il Server Dr.Web cercherà di trovare il file nelle directory standard mysqld.	/var/run/mysqld/
port	Uno dei due.	Numero di porta per la connessione al database tramite TCP/IP.	3306
		Nome del file di socket UNIX per l'utilizzo di UDS.	mysqld.sock
user	–	Nome dell'utente del database.	""
password	–	Password dell'utente del database.	""

Attributo	Valori ammissibili	Descrizione	Di default
`ssl`	`yes` | qualsiasi altro set di caratteri	Utilizza solamente le connessioni SSL.	`no`
`precompiledcache`	Un numero intero positivo.	Dimensione in byte della cache degli operatori SQL precompilati.	1048576
`debug`	• `yes` | `no` • `on` | `off`	Registra il log di funzionamento del DBMS di debug.	• `no` • `off`

- **<acl>**

  Liste di controllo degli accessi. Consentono di impostare limitazioni agli indirizzi di rete da cui gli Agent Dr.Web, gli installer di rete e gli altri Server Dr.Web (adiacenti) possono accedere a questo Server Dr.Web.

  L'elemento **<acl>** contiene i seguenti elementi figlio in cui vengono impostate le limitazioni per i relativi tipi di connessione:

  - **<install>** — lista delle limitazioni agli indirizzi IP da cui gli installer di Agent Dr.Web possono connettersi a questo Server Dr.Web.
  - **<agent>** — lista delle limitazioni agli indirizzi IP da cui gli Agent Dr.Web possono connettersi a questo Server Dr.Web.
  - **<links>** — lista delle limitazioni agli indirizzi IP da cui i Server Dr.Web adiacenti possono connettersi a questo Server Dr.Web.
  - **<discovery>** — lista delle limitazioni agli indirizzi IP da cui le richieste broadcast vengono accettate dal Servizio di rilevamento di Server Dr.Web.

  Tutti gli elementi figlio contengono una struttura uguale di elementi nidificati che impostano le seguenti limitazioni:

  - **<priority mode="" />**

    Priorità delle liste. I valori ammissibili dell'attributo `mode`: `allow` o `deny`. Con il valore **<priority mode="deny" />**, la lista **<deny>** ha una priorità superiore alla lista **<allow>**. Gli indirizzi non inclusi in nessuna lista o inclusi in tutte e due vengono vietati. Vengono consentiti soltanto gli indirizzi inclusi nella lista **<allow>** e non inclusi nella lista **<deny>**.

  - **<allow>**

    Una lista degli indirizzi TCP da cui l'accesso è consentito. L'elemento **<allow>** contiene uno o più elementi figlio **<ip address="" />** per impostare gli indirizzi consentiti nel formato IPv4 e **<ip6 address="" />** per impostare gli indirizzi consentiti nel formato IPv6. Nell'attributo `address` vengono impostati gli indirizzi di rete nel formato: <*indirizzo IP*>/[<*prefisso*>].

  - **<deny>**

    Una lista degli indirizzi TCP da cui l'accesso è proibito. L'elemento **<deny>** contiene uno o più elementi figlio **<ip address="" />** per impostare gli indirizzi proibiti nel formato IPv4 e **<ip6 address="" />** per impostare gli indirizzi proibiti nel formato IPv6. Nell'attributo

`address` vengono impostati gli indirizzi di rete nel formato: <*indirizzo IP*>/[<*prefisso*>].

- `<scripts profile="" stack="" trace="" />`

  Configurazione dei parametri del profiling del funzionamento di script.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`profile`	• `yes`, • `no`.	Registra nel log le informazioni sul profiling del funzionamento degli script del Server Dr.Web. Questo parametro viene utilizzato dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza necessità.	`no`
`stack`		Registra nel log le informazioni dallo stack di chiamate del funzionamento degli script del Server Dr.Web. Questo parametro viene utilizzato dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza necessità.	
`trace`		Registra nel log le informazioni sul tracciamento del funzionamento degli script del Server Dr.Web. Questo parametro viene utilizzato dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza necessità.	

- `<lua-module-path>`

  Percorsi per l'interprete Lua.

  

  L'ordine di impostazione dei percorsi importa.

  L'elemento `<lua-module-path>` contiene i seguenti elementi figlio:

  - `<cpath root="" />` — percorso della directory con i moduli binari. I valori ammissibili dell'attributo `root`: `home` (predefinito), `var`, `bin`, `lib`.
  - `<path value="" />` — percorso della directory con gli script. Se non è figlio per l'elemento `<jobs>` o `<hooks>`, appartiene ad entrambi. I percorsi impostati nell'attributo `value` sono relativi ai percorsi impostati nell'attributo `root` dell'elemento `<cpath>`.
  - `<jobs>` — percorsi per i task dal calendario di Server Dr.Web.

    L'elemento `<jobs>` contiene uno o più elementi figlio `<path value="" />` per impostare i percorsi della directory con gli script.
  - `<hooks>` — percorsi per le procedure personalizzate di Server Dr.Web.

    L'elemento `<hooks>` contiene uno o più elementi figlio `<path value="" />` per impostare i percorsi della directory con gli script.

- <**transports**>

  Configurazione dei parametri dei protocolli di trasporto utilizzati dal Server Dr.Web per la comunicazione con i client. Contiene uno o più elementi figlio <**transport** discovery="" ip="" name="" multicast="" multicast-group="" port="" />.

  Descrizione degli attributi:

Attributo	Descrizione	Obbligatorio	Valori ammissibili	Di default
discovery	Determina se verrà utilizzato il servizio di rilevamento di Server Dr.Web.	no, viene impostato soltanto insieme all'attributo ip.	yes, no	no
ip | unix	Definisce la famiglia dei protocolli utilizzati (IP o socket Unix) e imposta l'indirizzo dell'interfaccia.	sì	–	0.0.0.0 | –
name	Imposta il nome di Server Dr.Web per il servizio di rilevamento di Server Dr.Web.	no	–	drwcs
multicast	Determina se il Server Dr.Web fa parte di un gruppo multicast.	no, viene impostato soltanto insieme all'attributo ip.	yes, no	no
multicast-group	Imposta l'indirizzo del gruppo multicast di cui fa parte il Server Dr.Web.	no, viene impostato soltanto insieme all'attributo ip.	–	• 231.0.0.1 • [ff18::231.0.0.1]
port	Porta di ascolto.	no, viene impostato soltanto insieme all'attributo ip.	–	2193

- <**protocols**>

  Lista dei protocolli disattivati. Contiene uno o più elementi figlio <**protocol** enabled="" name="" />.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
enabled	• yes — il protocollo è attivato, • no — il protocollo è disattivato.	Modalità di utilizzo del protocollo.	no
name	• AGENT — il protocollo di comunicazione del Server Dr.Web con gli Agent Dr.Web. • MSNAPSHV — il protocollo di comunicazione del Server Dr.Web con il componente di controllo	Nome del protocollo.	–

Attributo	Valori ammissibili	Descrizione	Di default
	dell'operatività del sistema Microsoft NAP Validator. • `INSTALL` — il protocollo di comunicazione del Server Dr.Web con gli installer di Agent Dr.Web. • `CLUSTER` — il protocollo di comunicazione tra i Server Dr.Web in un sistema cluster. • `SERVER` — il protocollo di comunicazione del Server Dr.Web con gli altri Server Dr.Web.		

- **<plugins>**

  Lista delle estensioni disattivate. Contiene uno o più elementi figlio <plugin enabled="" name="" />.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`enabled`	• `yes` — l'estensione è attivata, • `no` — l'estensione è disattivata.	Modalità di utilizzo dell'estensione.	`no`
`name`	• `WEBMIN` — l'estensione del Pannello di controllo della sicurezza Dr.Web per la gestione del Server Dr.Web e della rete antivirus attraverso il Pannello di controllo. • `FrontDoor` — l'estensione Dr.Web Server FrontDoor che consente di connettere l'utility di diagnostica remota del Server Dr.Web.	Nome dell'estensione.	–

- **<license>**

  Impostazioni di concessione delle licenze.

  L'elemento <license> contiene i seguenti elementi figlio:

  - <limit-notify min-count="" min-percent="" />

    Impostazioni dell'avviso sulla limitazione sul numero di licenze nella chiave di licenza.

    Descrizione degli attributi:

Attributo	Descrizione	Di default
`min-count`	Numero massimo di licenze rimanenti, raggiunto il quale verrà inviato l'avviso **Limitazione sul numero di licenze nella chiave di licenza**.	3
`min-percent`	Percentuale massima di licenze rimanenti, raggiunta la quale verrà inviato l'avviso **Limitazione sul numero di licenze nella chiave di licenza**.	5

  - <license-report report-period="" active-stations-period="" />

    Impostazioni per il report sull'utilizzo delle licenze.

Descrizione degli attributi:

Attributo	Descrizione	Di default
report-period	Periodicità con cui sul Server Dr.Web verranno creati i report sulle chiavi di licenza da esso utilizzate. Se un report sull'utilizzo delle licenze viene creato da un Server Dr.Web subordinato, subito dopo la creazione questo report viene inviato sul Server Dr.Web principale. I report creati vengono inoltre inviati ad ogni connessione (incluso il riavvio) del Server Dr.Web, e inoltre, quando sul Server Dr.Web principale cambia il numero di licenze rilasciate.	1440
active-stations-period	Periodo durante cui verrà conteggiato il numero di postazioni attive per la creazione del report sull'utilizzo delle licenze. Il valore 0 prescrive di prendere in considerazione nel report tutte le postazioni indipendentemente dal loro stato di attività.	0

- <exchange>

  Configurazioni della distribuzione di licenze tra i Server Dr.Web.

  L'elemento <exchange> contiene i seguenti elementi figlio:

  - <expiration-interval value="" />
  - <prolong-preact value="" />
  - <check-interval value="" />

  Descrizione degli elementi:

Elemento	Descrizione	I valori dell'attributo value di default, min.
expiration-interval	**Periodo di validità delle licenze rilasciate** — periodo di tempo per cui vengono rilasciate le licenze dalla chiave su questo Server Dr.Web. L'impostazione viene utilizzata se questo Server Dr.Web rilascia licenze ai Server Dr.Web adiacenti.	1440
prolong-preact	**Periodo per il rinnovo delle licenze ricevute** — periodo prima della scadenza della licenza a partire da cui questo Server Dr.Web richiede il rinnovo di una licenza ricevuta da un Server Dr.Web adiacente. L'impostazione viene utilizzata se questo Server Dr.Web riceve licenze dai Server Dr.Web adiacenti.	60
check-interval	**Periodo di sincronizzazione delle licenze** — periodicità di sincronizzazione delle informazioni sulle licenze rilasciate tra i Server Dr.Web.	1440

- `<auth-flood count="" only-failed="" period="" />`

  Impostazioni di autenticazione. Se il numero di tentativi specificato viene superato, l'autenticazione non sarà possibile per un determinato tempo.
  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`count`	–	Numero di tentativi di autenticazione.	`5`
`only-failed`	• `yes` — prendi in considerazione solo le autenticazioni non riuscite, • `no` — prendi in considerazione sia le autenticazioni non riuscite che quelle riuscite.	Prendi in considerazione solo le autenticazioni non riuscite.	`yes`
`period`	–	Periodo di tempo durante cui l'autenticazione non sarà possibile.	60 secondi

- `<email from="" debug="" />`

  Configurazione dei parametri di invio delle email dal Pannello di controllo, per esempio, come avvisi dell'amministratore o messaggi per l'invio dei pacchetti di installazione delle postazioni.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`from`	–	Indirizzo della casella di e-mail da cui verranno spediti messaggi elettronici.	`drwcs@localhost`
`debug`	• `yes` — utilizza la modalità debug, • `no` — non utilizzare la modalità debug.	Utilizza la modalità debug per ottenere un log dettagliato di sessione SMTP.	`no`

  L'elemento `<email>` contiene i seguenti elementi figlio:

  - `<smtp server="" user="" pass="" port="" start_tls="" auth_plain="" auth_login="" auth_cram_md5="" auth_digest_md5="" auth_ntlm="" conn_timeout="" />`

    Configurazione dei parametri del server SMTP per l'invio di email.

    Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`server`	–	Indirizzo del server SMTP che verrà utilizzato per l'invio delle email.	`127.0.0.1`

Attributo	Valori ammissibili	Descrizione	Di default
user	–	Nome dell'utente del server SMTP se il server SMTP richiede l'autenticazione.	–
pass	–	Password dell'utente del server SMTP se il server SMTP richiede l'autenticazione.	–
port	Un numero intero positivo.	Porta del server SMTP che verrà utilizzato per l'invio delle email.	25
start_tls	• yes — utilizza questo tipo di autenticazione, • no — non utilizzare questo tipo di autenticazione.	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.	yes
auth_plain		Utilizzo dell'autenticazione *plain text* sul server di posta.	no
auth_login		Utilizzo dell'autenticazione *LOGIN* sul server di posta.	no
auth_cram_md5		Utilizzo dell'autenticazione *CRAM-MD5* sul server di posta.	no
auth_digest_md5		Utilizzo dell'autenticazione *DIGEST-MD5* sul server di posta.	no
auth_ntlm		Utilizzo dell'autenticazione *AUTH-NTLM* sul server di posta.	no
conn_timeout	Un numero intero positivo.	Time-out della connessione con il server SMTP.	180

- `<ssl enabled="" verify_cert="" ca_certs="" />`

  Configurazione dei parametri della cifratura di traffico dati SSL per l'invio delle email.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
enabled	• yes — utilizza SSL, • no — non utilizzare SSL.	Modalità di utilizzo della crittografia SSL.	no
verify_cert	• yes — controlla il certificato SSL, • no — non controllare il certificato SSL.	Controlla la correttezza del certificato SSL del mail server.	no

Attributo	Valori ammissibili	Descrizione	Di default
ca_certs	–	Percorso del certificato SSL di radice del Server Dr.Web.	–

- `<track-epidemic enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

  Configurazione dei parametri di monitoraggio di epidemie di virus nella rete.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
enabled	yes | no	Consente di tenere traccia di eventi multipli di infezioni delle postazioni e avere la possibilità di inviare un avviso di riepilogo all'amministratore.	yes
aggregation-period	Un numero intero positivo.	Intervallo di tempo in secondi dopo l'invio di un avviso di epidemia, durante il quale gli avvisi di infezioni singole delle postazioni non verranno inviati.	300
check-period		Intervallo di tempo in secondi durante cui deve arrivare il numero impostato di messaggi di postazioni infette in modo che venga inviato un avviso di epidemia.	3600
threshold		Numero di messaggi di infezioni che devono arrivare nel periodo di tempo impostato affinché il Server Dr.Web invii all'amministratore un singolo avviso di epidemia racchiudente tutti i casi di infezione (l'avviso **Un'epidemia nella rete**).	100
most-active		Numero delle minacce più comuni da includere nel report su epidemie.	5

- `<track-hips-storm enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

  Configurazione dei parametri di monitoraggio degli eventi multipli del componente Protezione preventiva.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
enabled	yes | no	Consente di tenere traccia di eventi multipli di Protezione preventiva e avere la possibilità di inviare un avviso di riepilogo all'amministratore.	yes
aggregation-period	Un numero intero positivo.	Intervallo di tempo in secondi dopo l'invio di un report di riepilogo sugli eventi di Protezione	300

Attributo	Valori ammissibili	Descrizione	Di default
		preventiva, durante il quale gli avvisi di eventi singoli non verranno inviati.	
check-period		Intervallo di tempo in secondi durante cui deve verificarsi il numero impostato di eventi di Protezione preventiva in modo che venga inviato un report di riepilogo.	3600
threshold		Numero di eventi di Protezione preventiva che devono arrivare nel periodo di tempo impostato affinché il Server Dr.Web invii all'amministratore un singolo report di riepilogo su questi eventi (l'avviso **Report di riepilogo di Protezione preventiva**).	100
most-active		Numero dei processi più comuni che hanno eseguito un'azione sospetta, da includere nel report di Protezione preventiva.	5

- `<track-appctl-storm enabled="" aggregation-period="" check-period="" threshold="" most-active="" />`

  Configurazione dei parametri di monitoraggio degli eventi multipli del componente Controllo delle applicazioni.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
enabled	yes | no	Consente di tenere traccia di eventi multipli di Controllo delle applicazioni e avere la possibilità di inviare un avviso di riepilogo all'amministratore.	yes
aggregation-period	Un numero intero positivo.	Intervallo di tempo in secondi dopo l'invio di un report di riepilogo sui processi bloccati da Controllo applicazioni, durante il quale gli avvisi di blocchi singoli non verranno inviati.	300
check-period		Intervallo di tempo in secondi durante cui deve essere bloccato il numero impostato di processi in modo che venga inviato un report di riepilogo.	3600
threshold		Numero di eventi di processi bloccati da Controllo applicazioni che devono arrivare nel periodo di tempo impostato affinché il Server Dr.Web invii all'amministratore un singolo report di riepilogo su questi eventi (l'avviso **Registrato un gran numero di blocchi Controllo applicazioni**).	100

Attributo	Valori ammissibili	Descrizione	Di default
most-active		Numero dei profili più diffusi in base a cui veniva effettuato il blocco, da includere nell'avviso di blocchi multipli.	5

- `<track-disconnect enabled="" aggregation-period="" check-period="" single-alert-threshold="" summary-alert-threshold="" min-session-duration="" />`

  Configurazione dei parametri di monitoraggio delle disconnessioni client anomale multiple.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
enabled	yes | no	Consente di tenere traccia delle connessioni client terminate in modo anomalo e avere la possibilità di inviare avvisi corrispondenti all'amministratore.	yes
aggregation-period	Un numero intero positivo.	Intervallo di tempo in secondi dopo l'invio di un avviso di disconnessioni multiple, durante il quale gli avvisi di disconnessioni singole non verranno inviati.	300
check-period		Intervallo di tempo in secondi durante cui deve verificarsi il numero impostato di disconnessioni client in modo che venga inviato un avviso corrispondente.	3600
single-alert-threshold		Numero minimo di connessioni che devono essere interrotte con un indirizzo durante il periodo di conteggio in modo che venga inviato un avviso di una disconnessione anomala singola (l'avviso **Terminazione di connessione anomala**).	10
summary-alert-threshold		Numero minimo di connessioni che devono essere interrotte durante il periodo di conteggio in modo che venga inviato un avviso unico di disconnessioni anomale multiple (l'avviso **Registrato un gran numero di connessioni terminate in modo anomalo**).	1000
min-session-duration		Se la durata di una connessione client terminata è inferiore a quella specificata, quando viene raggiunto il numero di connessioni impostato, verrà inviato un avviso di disconnessioni singole (l'avviso **Terminazione di connessione anomala**), indipendentemente dal periodo di conteggio. In tale caso la connessione non deve essere interrotta ulteriormente da connessioni più lunghe, e non deve essere inviato un avviso di disconnessioni anomale multiple (l'avviso	300

Attributo	Valori ammissibili	Descrizione	Di default
		Registrato un gran numero di connessioni terminate in modo anomalo).	

- `<default-lang value="" />`

  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 Dr.Web. 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.

- `<security-through-obscurity="" />`

  Impostazione di parametri di sicurezza che consentono di rafforzare la sicurezza tramite occultamento o distorsione intenzionale di alcuni dati.

  L'elemento `<security-through-obscurity>` contiene i seguenti elementi figlio:

  - `<server-header enabled="" />`
  - `<lower-case-uri enabled="" />`
  - `<hacker-misleading enabled="" />`

  Descrizione degli attributi:

Attributo	Valori ammissibili dell'attributo enabled	Descrizione	Valore dell'attributo enabled di default
`server-header`	`yes | no`	Consente di non mostrare la riga con i dati del server (versione di Server Dr.Web, versione di sistema operativo, librerie utilizzate), il che rende più difficile il compito di ricerca di vulnerabilità conosciute. Corrisponde all'impostazione **Restituisci un'intestazione dettagliata** nella configurazione del web server.	`no`
`lower-case-uri`	`yes | no`	Se attivata, l'opzione converte l'URI in minuscolo. Corrisponde all'impostazione **Converti gli URI in minuscolo** nella configurazione del web server.	`no`
`hacker-misleading`	`yes | no`	Se attivato, in risposta alle richieste dei file del tipo `/etc/passwd`, `/etc/hosts` ecc. (che contano sulla presenza di una vulnerabilità della classe Path/Directory Traversal) restituisce i falsi valori `passwd`, `hosts` ecc. Non esiste un'impostazione corrispondente nella corrente configurazione del web server.	`yes`

F2. File di configurazione di Pannello di controllo della sicurezza Dr.Web

Il file di configurazione del Pannello di controllo `webmin.conf` è in formato XML e si trova nella sottodirectory `etc` della directory radice del Server Dr.Web.

Descrizione dei parametri del file di configurazione del Pannello di controllo della sicurezza Dr.Web:

- `<version value="">`

  Versione corrente del Server Dr.Web.

- `<server-name value=""/>`

  Nome del Server Dr.Web.

  Viene impostato nel formato:

  <Indirizzo IP o nome DNS del Server Dr.Web>`[:`*<porta>*`]`

  Se l'indirizzo del Server Dr.Web non è impostato, viene utilizzato il nome di computer restituito dal sistema operativo o l'indirizzo di rete del Server Dr.Web: il nome a dominio, 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 Dr.Web dal Pannello di controllo o attraverso **Web API**). In particolare, in caso di richiesta dal Pannello di controllo, è la porta specificata nella barra degli indirizzi per la connessione del Pannello di controllo al Server Dr.Web.

- `<document-root value=""/>`

  Percorso della directory delle pagine web. Di default è `value="webmin"`.

- `<ds-modules value=""/>`

  Percorso della directory dei moduli. Di default è `value="ds-modules"`.

- `<threads value=""/>`

  Numero di query parallele elaborate dal web server. Questo parametro influisce sulle prestazioni del server. Non è consigliabile modificarne il valore senza necessità.

- `<io-threads value=""/>`

  Numero di flussi che elaborano i dati trasmessi via rete. Questo parametro influisce sulle prestazioni del Server Dr.Web. Non è consigliabile modificarne il valore senza necessità.

- `<compression value="" max-size="" min-size=""/>`

  Impostazioni della compressione dei dati trasmessi attraverso il canale di comunicazione con il server web via HTTP/HTTPS.

  Descrizione degli attributi:

Attributo	Descrizione	Di default
value	Livello di compressione dei dati da 1 a 9, dove 1 è il livello minimo e 9 è il livello massimo di compressione.	9
max-size	Dimensione massima delle risposte HTTP che verranno compresse. Impostare il valore 0 per togliere la restrizione su dimensione massima delle risposte HTTP da comprimere.	51200 KB
min-size	Dimensione minima delle risposte HTTP che verranno compresse. Impostare il valore 0 per togliere la restrizione su dimensione minima delle risposte HTTP da comprimere.	32 byte

- `<keep-alive timeout="" send-rate="" receive-rate=""/>`

  Mantieni attiva una sessione HTTP. Consente di impostare una connessione permanente per le richieste tramite il protocollo HTTP versione 1.X.

  Descrizione degli attributi:

Attributo	Descrizione	Di default
timeout	Time-out di una sessione HTTP. In caso di connessioni permanenti, il Server Dr.Web interrompe la connessione se nel periodo indicato non arrivano richieste dal client.	15 s
send-rate	Velocità minima di invio dati. Se la velocità in uscita di trasmissione dati nella rete è più bassa di questo valore, la connessione sarà negata. Impostare il valore 0 per togliere questa restrizione.	1024 B/s
receive-rate	Velocità minima di ricezione dati. Se la velocità in ingresso di trasmissione dati nella rete è più bassa di questo valore, la connessione sarà negata. Impostare il valore 0 per togliere questa restrizione.	1024 B/s

- `<buffers-size send="" receive=""/>`

  Configurazione delle dimensioni dei buffer per inviare e ricevere dati.

  Descrizione degli attributi:

Attributo	Descrizione	Di default
send	Dimensione dei buffer utilizzati per l'invio di dati. Questo parametro influisce sulle prestazioni del Server Dr.Web. Non è consigliabile modificarne il valore senza necessità.	8192 byte
receive	Dimensione dei buffer utilizzati per la ricezione di dati. Questo parametro influisce sulle prestazioni del Server Dr.Web. Non è consigliabile modificarne il valore senza necessità.	2048 byte

- `<max-request-length value=""/>`

  Lunghezza massima ammissibile in KB di una richiesta HTTP.

- `<xheaders>`

  Parametro per aggiungere intestazioni HTTP personalizzate. Di default sono già introdotte tre intestazioni volte a proteggere dagli attacchi di rete:

  - `<xheader name="X-XSS-Protection" value="1; mode=block"/>`

    L'intestazione gestisce il comportamento del browser al rilevamento del codice incorporato nella pagina attaccata (cosiddetto "attacco XSS"). Valori possibili:

Valore	Comportamento del browser
`0`	Il filtro XSS è disattivato.
`1`	Il filtro XSS è attivato. Al rilevamento di un attacco XSS il browser rimuoverà il codice incorporato.
`1; mode=block`	Il filtro XSS è attivato. Al rilevamento di un attacco XSS il browser non caricherà la pagina compromessa. Utilizzato di default.
`1; report=<indirizzo-di-rete>`	Il filtro XSS è attivato. Al rilevamento di un attacco XSS il browser rimuoverà il codice incorporato e invierà il report all'indirizzo specificato. Supportato solo nei browser basati su Chromium.

  - `<xheader name="X-Content-Type-Options" value="nosniff"/>`

    Con il valore di default (`nosniff`) l'intestazione vieta al browser di eseguire file che implicano la sostituzione del formato MIME.

  - `<xheader name="X-Frame-Options" value="SAMEORIGIN"/>`

    L'intestazione gestisce il comportamento del browser al rilevamento di un tentativo di incorporare la pagina web in un frame di terze parti (cosiddetto "clickjacking"). Valori possibili:

Valore	Comportamento del browser
`DENY`	Vieta al browser di caricare la pagina nel frame.
`SAMEORIGIN`	Consente al browser di caricare la pagina nel frame se la pagina e il frame hanno la stessa fonte (dominio, porta e protocollo). Utilizzato di default.
`ALLOW-FROM <indirizzo-di-rete>`	Consente al browser di caricare la pagina nel frame solo a condizione che la pagina si trovi all'indirizzo specificato.

- `<reverse-resolve enabled=""/>`

  Sostituisci gli indirizzi IP con i nomi DNS dei computer nel file di log del Server Dr.Web. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<script-errors-to-browser enabled=""/>`

  Mostra errori di script nel browser (errore 500). Questo parametro viene utilizzato dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza necessità.

- `<trace-scripts enabled=""/>`

  Attiva il tracciamento del funzionamento di script. Questo parametro viene utilizzato dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza la necessità. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<profile-scripts enabled="" stack=""/>`

  Gestione del profiling. Vengono misurate le prestazioni — il tempo di esecuzione delle funzioni e degli script del web server. Questo parametro viene utilizzato dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza necessità.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione
`enabled`	• `yes` — attiva il profiling, • `no` — disattiva il profiling.	Modalità di profiling degli script.
`stack`	• `yes` — registra informazioni nel log, • `yes` — non registrare informazioni nel log.	Modalità di scrittura delle informazioni su profiling (parametri di funzione e valori restituiti) nel log del Server Dr.Web.

- `<abort-scripts enabled=""/>`

  Consenti l'interruzione dell'operazione degli script se la connessione è stata interrotta dal client. Questo parametro viene utilizzato dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza la necessità. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<search-localized-index enabled=""/>`

  Utilizza le versioni localizzate delle pagine. Se la modalità è consentita, il server cercherà la versione localizzata della pagina indicata secondo la priorità delle lingue impostate nel campo `Accept-Language` dell'intestazione del client. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<default-lang value=""/>`

  Lingua dei documenti restituiti dal web server in assenza dell'intestazione `Accept-Language` nella richiesta HTTP. I valori dell'attributo `value` sono il codice di lingua ISO. Di default è `ru`.

- `<ssl certificate="" private-key="" keep-alive="" ciphers="" />`

  Impostazioni del certificato SSL.

  Descrizione degli attributi:

Attributo	Descrizione	Valori ammissibili	Di default
`certificate`	Percorso del file del certificato SSL.	-	`certificate.pem`

Attributo	Descrizione	Valori ammissibili	Di default
`private-key`	Percorso del file della chiave privata SSL.	-	`private-key.pem`
`keep-alive`	Utilizza una connessione permanente 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.	• `yes`, • `no`.	`yes`
`ciphers`	Lista e impostazioni delle cifre utilizzate.	Per la descrizione dettagliata v. qui, sezione “CIPHER LIST FORMAT”.	`HIGH:!aNULL:!RC4:@STRENGTH`

- **<listen>**

  Configurazione dei parametri per essere in ascolto per le connessioni.

  L'elemento **<listen>** contiene i seguenti elementi figlio:

  - **<insecure>**

    Una lista delle interfacce su cui il server sarà in ascolto per accettare le connessioni non protette attraverso il protocollo HTTP. Di default, si usa la porta 9080.

    L'elemento **<insecure>** contiene uno o più elementi figlio **<endpoint address=""/>** per impostare gli indirizzi consentiti nel formato IPv4 o IPv6. Nell'attributo `address` vengono impostati gli indirizzi di rete nel formato: <*Protocollo*>**:**//<*Indirizzo IP*>.

  - **<secure>**

    Una lista delle interfacce su cui il server sarà in ascolto per accettare le connessioni sicure attraverso il protocollo HTTPS. Di default, si usa la porta 9081.

    L'elemento **<secure>** contiene uno o più elementi figlio **<endpoint address=""/>** per impostare gli indirizzi consentiti nel formato IPv4 o IPv6. Nell'attributo `address` vengono impostati gli indirizzi di rete nel formato: <*Protocollo*>**:**//<*Indirizzo IP*>.

- **<access>**

  Liste di controllo degli accessi. Consentono di impostare limitazioni agli indirizzi di rete da cui il web server accetta richieste HTTP e HTTPS.

  L'elemento **<access>** contiene i seguenti elementi figlio in cui vengono impostate le limitazioni per i relativi tipi di connessione:

  - **<secure priority="">**

    Una lista delle interfacce su cui il server sarà in ascolto per accettare le connessioni sicure attraverso il protocollo HTTPS. Di default, si usa la porta 9081.

    Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
priority	allow	Priorità del permesso per HTTPS — gli indirizzi non inclusi in nessuna delle liste (o inclusi in entrambe le liste) vengono consentiti.	deny
	deny	Priorità del divieto per HTTPS — gli indirizzi non inclusi in nessuna delle liste (o inclusi in entrambe) vengono vietati.	

L'elemento <secure> contiene uno o più dei seguenti elementi figlio: <allow address=""/> e <deny address=""/>.

Descrizione degli elementi:

Elemento	Descrizione	I valori dell'attributo address di default
allow	Gli indirizzi da cui sarà consentito l'accesso tramite il protocollo HTTPS per le connessioni sicure.	tcp://127.0.0.1
deny	Gli indirizzi da cui sarà vietato l'accesso tramite il protocollo HTTPS per le connessioni sicure.	-

- <insecure priority="">

Una lista delle interfacce su cui il server sarà in ascolto per accettare le connessioni non protette attraverso il protocollo HTTP. Di default, si usa la porta 9080.

Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
priority	allow	Priorità del permesso per HTTP — gli indirizzi non inclusi in nessuna delle liste (o inclusi in entrambe) vengono consentiti.	deny
	deny	Priorità del divieto per HTTP — gli indirizzi non inclusi in nessuna delle liste (o inclusi in entrambe) vengono vietati.	

L'elemento <insecure> contiene uno o più dei seguenti elementi figlio: <allow address=""/> e <deny address=""/>.

Descrizione degli elementi:

Elemento	Descrizione	I valori dell'attributo address di default
allow	Gli indirizzi da cui sarà consentito l'accesso tramite il protocollo HTTP per le connessioni non protette.	tcp://127.0.0.1

Elemento	Descrizione	I valori dell'attributo address di default
`deny`	Gli indirizzi da cui sarà vietato l'accesso tramite il protocollo HTTP per le connessioni non protette.	-

F3. File di configurazione download.conf

Scopo del file download.conf:

1. Se viene creato e utilizzato un sistema di cluster dei Server Dr.Web, consente di distribuire il carico tra i Server Dr.Web dei cluster quando viene connesso un gran numero di nuove postazioni.
2. In caso di utilizzo sul Server Dr.Web di una porta non standard, consente di impostare questa porta per la generazione del file di installazione di Agent Dr.Web.

Il file `download.conf` viene utilizzato per generare un file di installazione di Agent Dr.Web per una nuova postazione della rete antivirus. I parametri di questo file consentono di impostare l'indirizzo di Server Dr.Web e la porta utilizzati per la connessione dell'installer di Agent Dr.Web al Server Dr.Web nel formato:

```
download = { server = '<Server_Address>'; port = <port_number> }
```

dove:

- <*Server_Address*> — nome a dominio o indirizzo IP di Server Dr.Web.

  

  Come indirizzo di Server Dr.Web è consigliato utilizzare il nome di server in formato FQDN.

  Quando viene generato un pacchetto di installazione di Agent Dr.Web, l'indirizzo di Server Dr.Web viene inizialmente preso dal file `download.conf`. Se nel file `download.conf` non è impostato l'indirizzo di Server Dr.Web, viene utilizzato il valore del parametro `ServerName` dal file `webmin.conf`. Altrimenti, il nome di computer restituito dal sistema operativo.

- <*port_number*> — porta per la connessione dell'installer di Agent Dr.Web al Server Dr.Web.

  Se la porta non è indicata nei parametri del file `download.conf`, 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**).

Di default il parametro `download` nel file `download.conf` è commentato. Per utilizzare il file `download.conf`, decommentare questo parametro cancellando "`--`" all'inizio della riga e impostare i valori corrispondenti dell'indirizzo e della porta di Server Dr.Web.

F4. File di configurazione di Server proxy Dr.Web

Il file di configurazione del Server proxy `drwcsd-proxy.conf` è in formato XML e si trova nella seguente directory:

- SO Windows: `C:\ProgramData\Doctor Web\drwcs\etc`
- SO Linux: `/var/opt/drwcs/etc`
- in SO FreeBSD: `/var/drwcs/etc`

Descrizione dei parametri del file di configurazione del Server proxy Dr.Web:

- `<listen spec="">`

  L'elemento radice `<drwcsd-proxy>` contiene uno o più elementi obbligatori `<listen>` che determinano le principali impostazioni per la ricezione delle connessioni da parte del Server proxy.

  L'elemento `<listen>` contiene l'unico attributo obbligatorio `spec`, i cui attributi determinano su quale interfaccia il Server proxy deve essere "in ascolto" delle connessioni client in ingresso e se deve attivare su questa interfaccia la modalità `discovery`.

  Attributi dell'elemento `spec`:

Attributo	Obbligatoria	Valori ammissibili	Descrizione	Di default
`ip | unix`	sì	–	Tipo di protocollo per la ricezione delle connessioni in ingresso. Come parametro, viene indicato l'indirizzo per cui il Server proxy è in ascolto.	`0.0.0.0 | -`
`port`	no	–	Numero di porta su cui il Server proxy è in ascolto.	`2193`
`discovery`	no	`yes, no`	Modalità di simulazione del Server Dr.Web. Consente ai client di rilevare il Server proxy come Server Dr.Web nel processo di ricerca attraverso le richieste broadcast.	`yes`
`multicast`	no	`yes, no`	Modalità di "ascolto" della rete per la ricezione di richieste broadcast da parte del Server proxy.	`yes`
`multicast-group`	no	–	Gruppo multicast in cui si trova il Server proxy.	`231.0.0.1` `[ff18::231.0.0.1]`

  A secondo del protocollo, cambia la lista degli attributi non obbligatori, indicati nell'attributo `spec`.

La lista delle proprietà non obbligatorie che possono essere impostate (+) o non possono essere impostate (–) nell'attributo `spec` a seconda del protocollo:

Protocollo	Presenza delle proprietà			
	port	discovery	multicast	multicast-group
ip	+	+	+	+
unix	+	–	–	–

L'attivazione della modalità **discovery** deve essere indicata esplicitamente in qualsiasi caso, anche se sia già attivata la modalità **multicast**.

L'algoritmo di reindirizzamento se è disponibile una lista dei Server Dr.Web è riportato in **Manuale amministratore**.

- `<compression mode="" level="">`

L'elemento `<compression>` come figlio dell'elemento `<listen>` determina i parametri di compressione nei canali client — Server proxy.

Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
mode	yes	La compressione è attivata.	possible
	no	La compressione è disattivata.	
	possible	La compressione è possibile.	
level	un numero intero da 1 a 9	Livello di compressione. Solo per il canale client — Server proxy	8

- `<encryption mode="">`

L'elemento `<encryption>` come figlio dell'elemento `<listen>` determina i parametri di crittografia nei canali client — Server proxy.

Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
mode	yes	La crittografia è attivata.	possible
	no	La crittografia è disattivata.	
	possible	La crittografia è possibile.	

- `<forward to="" master="">`

Configura le impostazioni che determinano il reindirizzamento delle connessioni in entrata. L'elemento `<forward>` è obbligatorio. È possibile impostare più elementi `<forward>` con diversi valori di attributo.

Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Obbligatorio
`to`	L'indirizzo viene impostato in base alla specifica dell'indirizzo di rete: • `<protocol>://<interface>:<port-number>` — utilizza IPv4 e IPv6. • `<protocol>://(<interface>):<port-number>` — utilizza solo IPv4. • `<protocol>://[<interface>]:<port-number>` — utilizza solo IPv6.	Indirizzo di Server Dr.Web su cui verrà reindirizzata la connessione.	sì
`master`	• `yes` — Server Dr.Web sarà server di gestione incondizionato. • `no` — in nessun caso Server Dr.Web sarà server di gestione. • `possible` — Server Dr.Web sarà server di gestione solo nel caso in cui non ci sono server di gestione incondizionati (con il valore `yes` per l'attributo `master`).	L'attributo determina se è possibile la modifica remota delle impostazioni di Server proxy Dr.Web attraverso il Pannello di controllo del Server Dr.Web indicato nell'attributo `to`. È possibile nominare server di gestione qualsiasi numero di Server Dr.Web (il valore `master="yes"`), la connessione viene effettuata a tutti i Server Dr.Web di gestione sequenzialmente nell'ordine definito nelle impostazioni di Server proxy Dr.Web fino alla prima ricezione di una configurazione valida (non vuota). Inoltre, è possibile non nominare server di gestione nessuno dei Server Dr.Web (il valore `master="no"`). In questo caso, la configurazione dei parametri di Server proxy Dr.Web (compresa la nomina del Server Dr.Web di gestione) è possibile solo localmente attraverso il file di configurazione di Server proxy Dr.Web.	no

Se per il Server Dr.Web è assente l'attributo `master`, di default viene considerato che `master="possible"`.

> Nel file di configurazione creato dall'installer durante l'installazione di Server proxy Dr.Web, l'attributo `master` non è definito per nessuno dei Server Dr.Web.

- `<compression mode="" level="">`

  L'elemento `<compression>` come figlio dell'elemento `<forward>` definisce i parametri di compressione sui canali Server Dr.Web — Server proxy Dr.Web. Gli attributi sono analoghi a quelli descritti sopra.

- `<encryption mode="">`

  L'elemento `<encryption>` come figlio dell'elemento `<listen>` definisce i parametri di crittografia sui canali Server Dr.Web — Server proxy Dr.Web. Gli attributi sono analoghi a quelli descritti sopra.

- `<update-bandwidth value="" queue-size="">`

L'elemento `<update-bandwidth>` consente di impostare un limite di velocità di trasmissione degli aggiornamenti dal Server Dr.Web ai client e il numero di client che scaricano gli aggiornamenti contemporaneamente.

Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`value`	• velocità massima in KB/s, • `unlimited`	Valore massimo della velocità complessiva per la trasmissione di aggiornamenti.	`unlimited`
`queue-size`	• un numero intero positivo, • `unlimited`	Numero massimo ammissibile di sessioni di distribuzione aggiornamenti avviate contemporaneamente dal Server Dr.Web. Quando viene raggiunto il limite indicato, le richieste dagli Agent Dr.Web vengono messe in una coda di attesa. La dimensione della coda di attesa non è limitata.	`unlimited`

- `<bandwidth value="" time-map="">`

  L'elemento `<update-bandwidth>` può avere uno o più elementi figli `<bandwidth>`. Questo elemento consente di impostare una limitazione alla velocità di trasmissione dei dati per un periodo di tempo specificato.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`value`	• velocità massima in KB/s, • `unlimited`	Valore massimo della velocità complessiva di trasmissione di dati durante l'aggiornamento dell'Agent Dr.Web.	`unlimited`
`time-map`	–	Una maschera che indica il periodo di tempo durante il quale la restrizione sarà attiva.	–

Il valore dell'attributo `time-map` viene impostato automaticamente dopo l'indicazione dell'impostazione corrispondente nell'interfaccia web del Pannello di controllo (v. **Manuale dell'amministratore**, sezione Configurazione del Server proxy in remoto). Al momento non è possibile impostare `time-map` manualmente attraverso il file di configurazione in modo comodo.

- `<install-bandwidth value="" queue-size="">`

L'elemento `<install-bandwidth>` consente di impostare una limitazione di velocità di trasmissione di dati durante l'installazione degli Agent Dr.Web e il numero di client che scaricano i dati per l'installazione contemporaneamente.

Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`value`	• velocità massima in KB/s, • `unlimited`	Valore massimo della velocità complessiva di trasmissione di dati nel corso dell'installazione degli Agent Dr.Web.	`unlimited`
`queue-size`	• un numero intero positivo, • `unlimited`	Numero massimo ammissibile di sessioni di installazione di Agent Dr.Web avviate contemporaneamente dal Server Dr.Web. Quando viene raggiunto il limite indicato, le richieste dagli Agent Dr.Web vengono messe in una coda di attesa. La dimensione della coda di attesa non è limitata.	`unlimited`

  - `<bandwidth value="" time-map="">`

  L'elemento `<install-bandwidth>` può avere uno o più elementi figli `<bandwidth>`. Questo elemento consente di impostare una limitazione alla velocità di trasmissione dei dati per un periodo di tempo specificato.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`value`	• velocità massima in KB/s, • `unlimited`	Valore massimo della velocità complessiva di trasmissione di dati durante l'installazione dell'Agent Dr.Web.	`unlimited`
`time-map`	–	Una maschera che indica il periodo di tempo durante il quale la restrizione sarà attiva.	–

Il valore dell'attributo `time-map` viene impostato automaticamente dopo l'indicazione dell'impostazione corrispondente nell'interfaccia web del Pannello di controllo (v. **Manuale dell'amministratore**, sezione Configurazione del Server proxy in remoto). Al momento non è possibile impostare `time-map` manualmente attraverso il file di configurazione in modo comodo.

- `<cache enabled="">`

  Impostazioni di cache del repository del Server proxy.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
enabled	yes | no	Determina se la memorizzazione nella cache è attivata.	yes

  L'elemento `<cache>` contiene i seguenti elementi figlio:

Elemento	Valori ammissibili	Descrizione	Di default
`<maximum-revision-queue size="">`	numero intero positivo	Numero di revisioni conservate.	3
`<clean-interval value="">`	numero intero positivo	Intervallo di tempo in minuti tra le cancellazioni delle revisioni vecchie.	60
`<unload-interval value="">`	numero intero positivo	Intervallo di tempo in minuti tra gli scaricamenti da memoria dei file non utilizzati.	10
`<repo-check mode="">`	idle | sync	La verifica dell'integrità della cache all'avvio (può richiedere molto tempo) o in modalità background.	idle

  - `<synchronize enabled="" schedule="">`

    Impostazioni di sincronizzazione dei repository del Server proxy e del Server Dr.Web.

    Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
enabled	yes | no	Definisce se la sincronizzazione dei repository è attivata.	yes
schedule	–	Calendario secondo cui verrà eseguita la sincronizzazione dei prodotti impostati.	–

    

    Il valore dell'attributo `schedule` viene impostato automaticamente dopo l'indicazione dell'impostazione corrispondente nell'interfaccia web del Pannello di controllo (v. **Manuale dell'amministratore**, sezione Configurazione del Server proxy in remoto). Al momento non è possibile impostare `schedule` manualmente attraverso il file di configurazione in modo comodo.

    Come elementi figlio di `<product name="">` viene riportata una lista dei prodotti che verranno sincronizzati:

    - 05-drwmeta — dati di sicurezza di Server Dr.Web,
    - 10-drwbases — database dei virus,

- 10-drwgatedb — database di SpIDer Gate,
- 10-drwspamdb — database di Antispam,
- 10-drwupgrade — Modulo di aggiornamento Dr.Web,
- 15-drwhashdb — hash di minacce conosciuti,
- 20-drwagent — Agent Dr.Web per Windows,
- 20-drwandroid11 — database di Dr.Web per Android,
- 20-drwcs — Server Dr.Web,
- 20-drwunix — Agent Dr.Web per UNIX,
- 25-drwcsdoc — documentazione,
- 40-drwproxy — Server proxy Dr.Web,
- 70-drwextra — prodotti aziendali Dr.Web,
- 70-drwutils — utility di amministrazione Dr.Web,
- 80-drwnews — notizie di Doctor Web.

- `<events enabled="" schedule="">`

  Impostazioni di memorizzazione nella cache degli eventi ricevuti dagli Agent Dr.Web.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`enabled`	`yes | no`	Determina se la memorizzazione degli eventi nella cache è attivata. Se è attivata, gli eventi verranno inviati sul Server Dr.Web secondo il calendario. Se è disattivata, gli eventi verranno inviati sul Server Dr.Web subito dopo la ricezione da parte del Server proxy.	`yes`
`schedule`	–	Calendario secondo cui verrà eseguita la trasmissione degli eventi ricevuti dagli Agent Dr.Web.	–

  

  Il valore dell'attributo `schedule` viene impostato automaticamente dopo l'indicazione dell'impostazione corrispondente nell'interfaccia web del Pannello di controllo (v. **Manuale dell'amministratore**, sezione Configurazione del Server proxy in remoto). Al momento non è possibile impostare `schedule` manualmente attraverso il file di configurazione in modo comodo.

- `<update enabled="" schedule="">`

  Configurazione dell'aggiornamento automatico del Server proxy.

  Con l'aggiornamento automatico attivato, se la sincronizzazione è attivata, gli aggiornamenti del Server proxy verranno scaricati dal Server Dr.Web secondo il calendario della sincronizzazione (v. sopra) e installati secondo il calendario dell'aggiornamento (di default senza limitazioni al tempo). Se la sincronizzazione è disattivata, il download e l'installazione

vengono eseguiti secondo il calendario dell'aggiornamento (di default senza limitazioni al tempo).

Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`enabled`	`yes` | `no`	Definisce se l'aggiornamento automatico è attivato.	`yes`
`schedule`	–	Il calendario secondo cui verranno eseguiti il download (se la sincronizzazione non è impostata) e l'installazione degli aggiornamenti.	–

Il valore dell'attributo `schedule` viene impostato automaticamente dopo l'indicazione dell'impostazione corrispondente nell'interfaccia web del Pannello di controllo (v. **Manuale dell'amministratore**, sezione Configurazione del Server proxy in remoto). Al momento non è possibile impostare `schedule` manualmente attraverso il file di configurazione in modo comodo.

Di default l'aggiornamento automatico è consentito senza limitazioni di tempo.

- `<core-dump enabled="" maximum="">`

La modalità di raccolta e la quantità di memory dump nel caso di eccezione SEH.

La configurazione dei memory dump è disponibile soltanto in SO Windows.

Per la raccolta del memory dump, il sistema operativo deve contenere la libreria `dbghelp.dll`.

Il dump viene salvato nella directory: `%APPDATA%\Doctor Web\drwcsd-proxy\dump\`

Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`enabled`	`yes` | `no`	Definisce se la raccolta di memory dump è attivata.	`yes`
`maximum`	numero intero positivo	Numero massimo di dump. Quelli più vecchi vengono eliminati.	10

- `<dns>`

Le impostazioni DNS.

`<timeout value="">`

Timeout in secondi per la risoluzione delle query DNS dirette/inverse. Lasciare vuoto il valore per non limitare il tempo di attesa della fine della risoluzione.

`<retry value="">`

Il numero massimo di query DNS ripetute in caso di una risoluzione di query DNS non riuscita.

`<cache enabled="" negative-ttl="" positive-ttl="">`

Il tempo di conservazione nella cache delle risposte del server DNS.

Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione
`enabled`	• `yes` — conserva le risposte nella cache, • `no` — non conservare le risposte nella cache.	Modalità di conservazione delle risposte nella cache.
`negative-ttl`	–	Tempo in minuti di conservazione nella cache (TTL) delle risposte negative del server DNS.
`positive-ttl`	–	Tempo in minuti di conservazione nella cache (TTL) delle risposte positive del server DNS.

`<servers>`

Una lista dei server DNS che sostituisce la lista di sistema predefinita. Contiene uno o più elementi figlio `<server address="">` in cui il parametro `address` definisce l'indirizzo IP del server.

`<domains>`

Una lista dei domini DNS che sostituisce la lista di sistema predefinita. Contiene uno o più elementi figlio `<domain name="">` in cui il parametro `name` definisce il nome del dominio.

F5. File di configurazione di Loader di repository

Il file di configurazione del Loader di repository `drwreploader.conf` è in formato XML e si trova nella directory `etc` della directory di installazione del Server Dr.Web.

Per utilizzare il file di configurazione

- Per l'utility console, il percorso del file deve essere indicato nella opzione `--config`.
- Per l'utility grafica, il file deve essere locato nella directory in cui è locata l'utility stessa. Quando l'utility grafica viene avviata senza il file di configurazione, esso verrà creato nella directory in cui è locata l'utility e verrà utilizzato ad avvii successivi.

Descrizione dei parametri del file di configurazione del Loader di repository:

- `<mode value="" path="" archive="" key="">`

  Descrizione degli attributi:

Attributo	Descrizione	Valori ammissibili
`value`	La modalità di download degli aggiornamenti: • `repository` — il repository viene scaricato nel formato repository di Server Dr.Web. I file scaricati possono essere importati direttamente attraverso il Pannello di controllo come aggiornamento del repository di Server Dr.Web. • `mirror` — il repository viene scaricato nel formato zona di aggiornamento SAM. I file scaricati possono essere collocati su un mirror di aggiornamento nella rete locale. In seguito i Server Dr.Web possono essere configurati per ricevere gli aggiornamenti direttamente da questo mirror di aggiornamento che contiene l'ultima versione del repository, invece di ricevere gli aggiornamenti dai server SAM.	`repository | mirror`
`path`	La directory in cui viene caricato il repository.	–
`archive`	Comprimere automaticamente il repository in un archivio .zip. Questa opzione permette di ottenere un file di archivio pronto per la successiva importazione del repository sul Server Dr.Web tramite il Pannello di controllo, dalla sezione **Amministrazione → Contenuti del repository**.	`yes | no`
`key`	File della chiave di licenza Dr.Web. È inoltre possibile impostare solo l'hash MD5 della chiave di licenza che può essere visualizzato nel Pannello di controllo, nella sezione **Amministrazione → Gestione licenze**.	–

- `<log path="" verbosity="" rotate="">`

  Impostazioni del log di funzionamento di Loader di repository.

  Descrizione degli attributi:

Attributo	Descrizione	Valori ammissibili
`path`	Percorso del file di log.	–
`verbosity`	Livello di dettaglio del log. Di default è `TRACE3`.	`ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. I valori `ALL` e `DEBUG3` sono sinonimi.
`rotate`	Modalità di rotazione del log nel formato *<N><f>,<M><u>*. È simile all'impostazione di rotazione del log di Server Dr.Web. Di default `10,10m` che significa "conserva 10 file da 10 megabyte, utilizza compressione".	–

- `<update url="" proto="" cdn="" update-key="" version="">`

  Le impostazioni generali di caricamento del repository.

  Descrizione degli attributi:

Attributo	Descrizione	Valori ammissibili
`url`	La directory sui server SAM che contiene gli aggiornamenti dei prodotti Dr.Web.	–
`proto`	Il tipo di protocollo per la ricezione degli aggiornamenti dai server di aggiornamento. Per tutti i protocolli gli aggiornamenti vengono scaricati secondo le impostazioni della lista dei server SAM.	`http | https | ftp | ftps | sftp | scp | file`
`cdn`	Consenti l'utilizzo di Content Delivery Network per il caricamento del repository.	`yes | no`
`update-key`	Il percorso della chiave pubblica o della directory con la chiave pubblica per la verifica della firma degli aggiornamenti che vengono scaricati da SAM. Le chiavi pubbliche per la verifica dell'autenticità degli aggiornamenti `update-key-*.upub` sono ritrovabili sul Server Dr.Web nella directory `etc`.	–
`version`	La versione di Server Dr.Web per cui è necessario scaricare aggiornamenti.	–

  - `<servers>`

    Lista dei server di aggiornamento. L'ordine dei server SAM nella lista determina l'ordine in cui l'utility ci si connette per il caricamento del repository.

    Contiene elementi figli di `<server>` in cui vengono indicati i server di aggiornamento.

  - `<auth user="" password="">`

    Le credenziali dell'utente per l'autenticazione sul server di aggiornamento, se il server richiede l'autenticazione.

    Descrizione degli attributi:

Attributo	Descrizione
`user`	Nome utente sul server di aggiornamento.
`password`	Password sul server di aggiornamento.

  - `<proxy host="" port="" user="" password="" />`

    Parametri di connessione a SAM attraverso un server proxy.

    Descrizione degli attributi:

Attributo	Descrizione
`host`	Indirizzo di rete del server proxy in uso.

Attributo	Descrizione
port	Numero di porta del server proxy in uso. Di default è 3128.
user	Nome utente sul server proxy, se il server proxy in uso richiede l'autenticazione.
password	Password sul server proxy, se il server proxy in uso richiede l'autenticazione.

- <ssl cert-mode="" cert-file="">

  Impostazioni dei certificati SSL da accettare automaticamente. Questa impostazione si usa solo per i protocolli sicuri che supportano la crittografia.

  Descrizione degli attributi:

Attributo	Descrizione	Valori ammissibili
cert-mode	I certificati che verranno accettati automaticamente.	- any — accetta qualsiasi certificato, - valid — accetta solo i certificati verificati, - drweb — accetta solo i certificati Dr.Web, - custom — accetta i certificati personalizzati.
cert-file	Percorso del file del certificato.	–

- <ssh mode="" pubkey="" prikey="">

  Tipo di autenticazione sul server di aggiornamento nel caso di connessione via SCP/SFTP.

  Descrizione degli attributi:

Attributo	Descrizione	Valori ammissibili
mode	Tipo di autenticazione.	- pwd — autenticazione tramite la password. La password viene impostata nel tag <auth />. - pubkey — autenticazione tramite la chiave pubblica. La chiave pubblica viene impostata nell'attributo pubkey o viene estratta dalla chiave privata indicata in prikey.
pubkey	Chiave pubblica SSH	–
prikey	Chiave privata SSH	–

- <products>

  Impostazioni dei prodotti da scaricare.

  - <product name="" update="">

    Impostazioni di ciascun prodotto separatamente.

    Descrizione degli attributi:

Attributo	Descrizione	Valori ammissibili
name	Nome del prodotto.	• 05-drwmeta — dati di sicurezza di Server Dr.Web, • 10-drwbases — database dei virus,

Attributo	Descrizione	Valori ammissibili
		• `10-drwgatedb` — database di SpIDer Gate, • `10-drwspamdb` — database di Antispam, • `10-drwupgrade` — Modulo di aggiornamento Dr.Web, • `15-drwhashdb` — hash di minacce conosciuti, • `20-drwagent` — Agent Dr.Web per Windows, • `20-drwandroid11` — database di Dr.Web per Android, • `20-drwcs` — Server Dr.Web, • `20-drwunix` — Agent Dr.Web per UNIX, • `25-drwcsdoc` — documentazione, • `40-drwproxy` — Server proxy Dr.Web, • `70-drwextra` — prodotti aziendali Dr.Web, • `70-drwutils` — utility di amministrazione Dr.Web, • `80-drwnews` — notizie di Doctor Web.
`update`	Attiva il download di questo prodotto.	`yes | no`

- **<schedule>**

  Calendario degli aggiornamenti periodici. Non è necessario avviare l'utility manualmente, il caricamento del repository verrà eseguito automaticamente secondo gli intervalli di tempo impostati.

  - **<job period="" enabled="" min="" hour="" day="">**

    Impostazioni di esecuzione dei download pianificati.

Attributo	Descrizione	Valori ammissibili
`period`	Periodicità di esecuzione dei task di download.	• `every_n_min` — ogni N minuti, • `hourly` — ogni ora, • `daily` — ogni giorno, • `weekly` — ogni settimana.
`enabled`	Il task di download è attivato.	`yes | no`
`min`	Il minuto dell'esecuzione del task.	numeri interi da 0 a 59
`hour`	L'ora dell'esecuzione del task. È valido per i periodi `daily` e `weekly`.	numeri interi da 0 a 23
`day`	Il giorno dell'esecuzione del task. È valido per il periodo `weekly`.	• `mon` — lunedì, • `tue` — martedì, • `wed` — mercoledì, • `thu` — giovedì,

Attributo	Descrizione	Valori ammissibili
		• `fri` — venerdì, • `sat` — sabato, • `sun` — domenica.

Allegato G. Parametri della riga di comando per i programmi inclusi in Dr.Web Enterprise Security Suite

I parametri della riga di comando hanno una priorità più alta rispetto alle impostazioni predefinite o ad altre impostazioni permanenti (configurate nel file di configurazione di Server Dr.Web, nel registro di SO Windows ecc.). In alcuni casi i parametri impostati all'avvio anche ridefiniscono le impostazioni permanenti. Tali casi vengono descritti di seguito.

Nella descrizione della sintassi dei parametri di singoli programmi la parte facoltativa viene racchiusa tra parentesi quadre `[...]`.

Le caratteristiche descritte di seguito in Allegato H non riguardano l'installer di rete di Agent Dr.Web.

Una parte dei parametri della riga di comando ha la forma dell'opzione — inizia con il trattino. Tali parametri si chiamano opzioni.

Molte opzioni possono essere presentate in varie forme equivalenti. Così, le opzioni che implicano un valore logico (sì/no, consenti/blocca) hanno la variante negativa, per esempio l'opzione `-admin-rights` ha la variante coppia `-no-admin-rights` con il valore contrario. Possono essere impostate con indicazione esplicita del valore, per esempio, `-admin-rights=yes` e `-admin-rights=no`.

Sono sinonimi del valore `yes` i valori `on`, `true`, `OK`. Sono sinonimi del valore `no` i valori `off`, `false`.

Se il valore di un'opzione contiene spazi o tabulazione, tutto il parametro deve essere racchiuso tra virgolette, per esempio:

```
"-home=c:\Program Files\DrWeb Server"
```

I nomi di opzioni possono essere abbreviati (facendo cadere le ultime lettere) qualora il nome abbreviato non corrisponda alla parte iniziale di un'altra opzione.

Per l'esecuzione di comandi forzata con permessi di amministratore nei sistemi operativi della famiglia Windows può essere utilizzato il parametro `elevate`. Viene indicato prima di tutte le altre opzioni e parametri, per esempio: `drwcsd elevate start`.

G1. Installer di rete

Formato del comando di avvio:

`drwinst.exe [<opzioni>]`

Opzioni

Le opzioni della riga di comando valgono per l'esecuzione di tutti i tipi di file di installazione di Agent Dr.Web.

Le opzioni di avvio dell'installer di rete di Agent Dr.Web vengono impostate nel formato: `/<opzione> <parametro>`.

Ogni valore di parametro viene separato da spazio. Per esempio:

```
/silent yes
```

Se il valore di un'opzione contiene spazi, tabulazione o il carattere `\`, tutto il parametro deve essere racchiuso tra virgolette. Per esempio:

```
/pubkey "C:\my folder\drwcsd-certificate.pem"
```

Opzioni ammissibili:

- `/compression` <*modalità*> — modalità di compressione del traffico dati con il Server Dr.Web. Il parametro <*modalità*> può assumere i seguenti valori:
  - `yes` — utilizza la compressione.
  - `no` — non utilizzare la compressione.
  - `possible` — la compressione è possibile. La decisione finale viene presa in base alle impostazioni sul lato Server Dr.Web.

  Se l'opzione non è impostata, di default si usa il valore `possible`.
- `/encryption` <*modalità*> — modalità di cifratura del traffico dati con il Server Dr.Web. Il parametro <*modalità*> può assumere i seguenti valori:
  - `yes` — utilizza la cifratura.
  - `no` — non utilizzare la cifratura.
  - `possible` — la cifratura è possibile. La decisione finale viene presa in base alle impostazioni sul lato Server Dr.Web.

  Se l'opzione non è impostata, di default si usa il valore `possible`.
- `/excludeFeatures` <*componenti*> — una lista dei componenti da escludere dall'installazione sulla postazione. Se vengono impostati diversi componenti, utilizzare il carattere "`,`" come separatore. I componenti disponibili:
  - `scanner` — Scanner Dr.Web,
  - `spider-mail` — SpIDer Mail,
  - `spider-g3` — SpIDer Guard,
  - `outlook-plugin` — Dr.Web per Microsoft Outlook,

- `firewall` — Firewall Dr.Web,
- `spider-gate` — SpIDer Gate,
- `parental-control` — Office control,
- `antispam-outlook` — Antispam Dr.Web per il componente Dr.Web per Microsoft Outlook,
- `antispam-spidermail` — Antispam Dr.Web per il componente SpIDer Mail.

Per i componenti non direttamente indicati viene mantenuto lo status di installazione impostato per essi di default.

- `/id` <*identificatore_della_postazione*> — identificatore della postazione su cui viene installato l'Agent Dr.Web.

  L'opzione viene impostata insieme all'opzione `/pwd` per l'autenticazione automatica sul Server Dr.Web. Se i parametri di autenticazione non sono impostati, la decisione sull'autenticazione viene presa sul lato Server Dr.Web.

- `/includeFeatures` <*componenti*> — una lista dei componenti da installare sulla postazione. Se vengono impostati diversi componenti, utilizzare il carattere "`,`" come separatore. I componenti disponibili:
  - `scanner` — Scanner Dr.Web,
  - `spider-mail` — SpIDer Mail,
  - `spider-g3` — SpIDer Guard,
  - `outlook-plugin` — Dr.Web per Microsoft Outlook,
  - `firewall` — Firewall Dr.Web,
  - `spider-gate` — SpIDer Gate,
  - `parental-control` — Office control,
  - `antispam-outlook` — Antispam Dr.Web per il componente Dr.Web per Microsoft Outlook,
  - `antispam-spidermail` — Antispam Dr.Web per il componente SpIDer Mail.

  Per i componenti non direttamente indicati viene mantenuto lo status di installazione impostato per essi di default.

- `/installdir` <*directory*> — directory di installazione.

  Se l'opzione non è impostata, di default l'installazione viene eseguita nella directory "`Program Files\DrWeb`" sul disco di sistema.

- `/installtimeout` <*tempo*> — limite di tempo di attesa della risposta dalla postazione durante l'installazione remota avviata dal Pannello di controllo. Viene impostato in secondi.

  Se l'opzione non è impostata, di default si usa il valore di 300 secondi.

- `/instMode` <*modalità*> — modalità di avvio dell'installer. Il parametro <*modalità*> può assumere i seguenti valori:
  - `change` — modifica la lista dei componenti installati del prodotto;
  - `remove` — rimuovi il prodotto installato;

- `recovery` — ripristina il prodotto installato se alcuni dei suoi componenti sono stati danneggiati.

Se l'opzione non è impostata, di default l'installer definisce automaticamente la modalità di avvio.

- `/lang` <*codice_lingua*> — lingua dell'installer e del prodotto che viene installato. Viene impostata nel formato ISO-639-1 per il codice lingua.

  Se l'opzione non è impostata, di default si usa la lingua di sistema.

- `/pubkey` <*certificato*> — percorso completo del file del certificato di Server Dr.Web.

  Se il certificato non è impostato, di default durante un avvio dell'installazione locale l'installer accetta automaticamente il file del certificato `*.pem` dalla directory del suo avvio. Se il file del certificato si trova in una directory diversa dalla directory di avvio dell'installer, è necessario impostare manualmente il percorso completo del file del certificato.

  Se viene avviato un pacchetto di installazione creato nel Pannello di controllo, il certificato fa parte del pacchetto di installazione e non è richiesto indicare in aggiunta il file del certificato attraverso le opzioni della riga di comando.

- `/pwd` <*password*> — password dell'Agent Dr.Web per l'accesso al Server Dr.Web.

  L'opzione viene impostata insieme all'opzione `/id` per l'autenticazione automatica sul Server Dr.Web. Se i parametri di autenticazione non sono impostati, la decisione sull'autenticazione viene presa sul lato Server Dr.Web.

- `/regagent` <*modalità*> — determina se l'Agent Dr.Web verrà registrato nella lista dei programmi installati. Il parametro <*modalità*> può assumere i seguenti valori:
  - `yes` — registra l'Agent Dr.Web nella lista dei programmi installati.
  - `no` — non registrare l'Agent Dr.Web nella lista dei programmi installati.

  Se l'opzione non è impostata, di default si usa il valore `no`.

- `/retry` <*numero*> — numero di tentativi della ricerca del Server Dr.Web tramite l'invio di richieste multicast. Se non c'è risposta dal Server Dr.Web dopo il numero di tentativi impostato, il Server Dr.Web è ritenuto non trovato.

  Se l'opzione non è impostata, di default vengono eseguiti 3 tentativi di ricerca del Server Dr.Web.

- `/server [`<*protocollo*>`/]`<*indirizzo_del_server*>`[:`<*porta*>`]` — indirizzo del Server Dr.Web da cui verrà effettuata l'installazione di Agent Dr.Web e a cui Agent Dr.Web si connetterà dopo l'installazione.

  Se l'opzione non è impostata, di default la ricerca del Server Dr.Web viene effettuata tramite l'invio di richieste multicast.

- `/silent` <*modalità*> — determina se l'installer verrà eseguito in modalità background. Il parametro <*modalità*> può assumere i seguenti valori:
  - `yes` — avvia l'installer in modalità background.
  - `no` — avvia l'installer in modalità grafica.

  Se l'opzione non è impostata, di default Agent Dr.Web viene installato in modalità grafica dell'installer (v. **Guida all'installazione**, p. Installazione di Agent Dr.Web attraverso installer).

- `/timeout` <*tempo*> — tempo massimo di attesa di ciascuna risposta nel processo di ricerca di Server Dr.Web. Viene impostato in secondi. I messaggi di risposta continuano ad essere accettati fino a quando il tempo di attesa della risposta non supererà il valore di timeout.

  Se l'opzione non è impostata, di default si usa il valore di 3 secondi.

G2. Agent Dr.Web per Windows

Formato del comando di avvio:

`es-service.exe [`<*opzioni*>`]`

Opzioni

Ognuna delle opzioni può essere impostata in uno dei seguenti formati (i formati sono equivalenti):

`-`<*opzione_corta*>`[ `<*argomento*>`]`

o

`--`<*opzione_lunga*>`[=`<*argomento*>`]`

Le opzioni possono essere utilizzate contemporaneamente, comprese le versioni corte e lunghe.

Se un argomento contiene spazi, deve essere racchiuso tra virgolette. Le opzioni brevi possono assumere valori senza spazio di separazione, per esempio:

```
es-service -e192.168.1.1:12345
```

Tutte le opzioni vengono eseguite a prescindere dai permessi consentiti per la postazione sul Server Dr.Web. Cioè anche se i permessi di modifica delle impostazioni di Agent Dr.Web sono vietati sul Server Dr.Web, è possibile modificare queste impostazioni tramite le opzioni della riga di comando.

Opzioni ammissibili:

- Mostra la guida:
  - `-?`
  - `--help`
- Modifica l'indirizzo del Server Dr.Web a cui si connette l'Agent Dr.Web:
  - `-e` <*Server Dr.Web*>
  - `--esserver=`<*Server Dr.Web*>

Per impostare diversi Server Dr.Web alla volta, è necessario ripetere l'opzione separata da spazio per ciascun indirizzo di Server Dr.Web, per esempio:

```
es-service -e 192.168.1.1:12345 -e 192.168.1.2:12345 -e 10.10.1.1:1223
```

o

```
es-service --esserver=10.3.1.1:123 --esserver=10.3.1.2:123 --
esserver=10.10.1.1:123
```

- Aggiungi la chiave di cifratura pubblica:
  - `-p <chiave>`
  - `--addpubkey=<chiave>`

  La chiave pubblica indicata come argomento viene copiata nella directory di Agent Dr.Web (di default è la directory `%ProgramFiles%\DrWeb`), viene rinominata in `drwcsd.pub` (se il nome era diverso) e viene riletta dal servizio. Il file della chiave pubblica precedente, se trovato, viene rinominato in `drwcsd.pub.old` e in seguito non viene utilizzato.

  Tutte le chiavi pubbliche utilizzate in precedenza (le chiavi che sono state trasferite dal Server Dr.Web e si conservano nel registro) rimangono e continuano a essere utilizzate.
- Aggiungi il certificato di Server Dr.Web:
  - `-c <certificato>`
  - `--addcert=<certificato>`

  Il file del certificato di Server Dr.Web indicato come argomento viene copiato nella directory di Agent Dr.Web (di default è la directory `%ProgramFiles%\DrWeb`), viene rinominato in `drwcsd-certificate.pem` (se il nome era diverso) e viene riletto dal servizio. Il file del certificato precedente, se trovato, viene rinominato in `drwcsd-certificate.pem.old` e in seguito non viene utilizzato.

  Tutti i certificati utilizzati in precedenza (i certificati che sono stati trasferiti dal Server Dr.Web e si conservano nel registro) rimangono e continuano a essere utilizzati.
- Riconnettiti a Server come nuovo arrivo:
  - `-w <valore>`
  - `--newbie=<valore>`

  I valori ammissibili: `once, always`. Se è impostato il valore `always`, ad ogni successivo avvio del servizio i parametri di autenticazione di Agent Dr.Web verranno resettati, e di conseguenza, Agent Dr.Web ogni volta si connetterà a Server come nuovo arrivo (per maggiori informazioni v. **Manuale dell'amministratore**, p. Criteri di approvazione delle postazioni). Se è impostato il valore `once`, al successivo avvio del servizio i parametri di autenticazione di Agent Dr.Web su Server verranno resettati, dopodiché Agent Dr.Web una sola volta si connetterà a Server come nuovo arrivo.
- Modifica il livello di dettaglio del log di Agent Dr.Web:
  - `--change-loglevel=<livello>`

I valori ammissibili del livello di dettaglio del log: `err`, `wrn`, `inf`, `dbg`, `all`. Questo comando può essere eseguito solo con i permessi di amministratore. Non richiede la disattivazione dell'autoprotezione, il riavvio manuale del servizio o del sistema operativo.

G3. Server Dr.Web

Ci sono diverse varianti dei comandi di avvio di Server Dr.Web, per comodità vengono descritte separatamente.

Una serie di comandi richiede la presenza nella riga di comando delle opzioni obbligatorie `modexec` o `modexecdb` per eseguire moduli Lua e, se necessario, per passare un set di parametri ausiliari. In questo caso, il comando è costruito nel seguente modo:

`drwcsd [<opzioni>] modexec [<nome_funzione>@]<nome_modulo> [<parametri>]`

- *<nome_funzione>* — nome di una funzione specifica che deve essere eseguita nel modulo Lua.
- *<nome_modulo>* — nome del modulo eseguibile Lua.

I comandi riportati in G3.1. Gestione del Server Dr.Web — G3.5. Backup dei dati critici del Server Dr.Web sono multipiattaforma: possono essere utilizzati sia in SO Windows che in SO della famiglia UNIX, se non diversamente indicato.

Se si verificano errori durante l'esecuzione dei comandi di gestione di Server Dr.Web, consultare il file di log di Server Dr.Web per cercare le possibili cause (v. **Manuale dell'amministratore**, p. Log di Server Dr.Web).

G3.1. Gestione del Server Dr.Web

`drwcsd [<opzioni>]` — configura le impostazioni di funzionamento del Server Dr.Web (le opzioni vengono descritte in maggior dettaglio di seguito).

G3.2. Comandi di base

- `drwcsd restart` — esegui il riavvio completo del servizio Server Dr.Web (viene eseguito dalla coppia `stop` e quindi `start`).
- `drwcsd start` — avvia il Server Dr.Web.
- `drwcsd stop` — arresta normalmente il Server Dr.Web.
- `drwcsd stat` — output nel file di log delle statistiche di funzionamento: tempo di CPU, utilizzo della memoria ecc. (nei sistemi operativi della famiglia UNIX è analogo al comando `send_signal WINCH` o `kill SIGWINCH`).
- `drwcsd modexec agent@verify-key` *<nome_completo_del_file_della_chiave>* — controllo della correttezza del file della chiave di licenza (`agent.key`).
- `drwcsd modexec enterprise@verify-key` *<nome_completo_del_file_della_chiave>* — controllo della correttezza del file della chiave di licenza di Server Dr.Web

(`enterprise.key`). Notare che la chiave di licenza di Server Dr.Web non si usa più a partire dalla versione 10.

- `drwcsd verifyconfig` <*nome_completo_del_file_di_configurazione*> — controllo della sintassi del file di configurazione di Server Dr.Web (`drwcsd.conf`).
- `drwcsd verifycache` — controllo della correttezza del contenuto della cache dei file di Server Dr.Web.
- `drwcsd syncads` — sincronizza la struttura della rete: i container di Active Directory che contengono computer diventano gruppi della rete antivirus in cui vengono messe le postazioni.
- `drwcsd modexec restore@repository-server-update` — ripristina Server Dr.Web dalla revisione (esegui il rollback allo stato della revisione corrente senza salvare una copia di backup e aggiornare il database e i file di configurazione. In assenza di tale revisione nel repository il ripristino non è possibile.

Questa azione viene registrata nel log di verifica.

- `update@repository-server-update [<revision-to>]` — aggiornamento di Server Dr.Web. Se non è indicata la revisione a cui deve essere eseguito l'aggiornamento, il server verrà aggiornato alla revisione più recente.
- `revert@repository-server-update <revision-to>` — rollback di Server Dr.Web a una revisione specifica.

Le ultime due azioni vengono registrate nel log di verifica.

L'aggiornamento e il rollback di Server Dr.Web sono descritti in documentazione dell'amministratore, sezione Aggiornamento di Server Dr.Web e ripristino da copia di backup.

G3.3. Comandi di gestione del database

Inizializzazione del database

Ad inizializzazione il database deve essere assente o vuota.

`drwcsd [`<*opzioni*>`] modexecdb database-init [`<*chiave_di_licenza*>` [`<*password*>`]]` — inizializzazione del database.

- <*chiave_di_licenza*> — percorso della chiave di licenza Dr.Web `agent.key`. Se la chiave di licenza non è specificata, dovrà essere aggiunta in seguito dal Pannello di controllo o ottenuta attraverso la comunicazione tra i server da un Server Dr.Web adiacente.

- *<password>* — password iniziale dell'amministratore del Server Dr.Web (il nome utente è **admin**). Di default è **root**.

> Se è necessario omettere uno o più parametri nel comando che viene scritto, invece di ciascuno di essi va utilizzato un valore speciale `%nil`.
>
> `%nil` può essere omesso se sono assenti i parametri seguenti.

Impostazione dei parametri di inizializzazione del database

Se si utilizza il database incorporato, i parametri di inizializzazione si possono impostare via un file esterno. Per farlo, si utilizza il comando:

`drwcsd.exe modexecdb database-init@`*<response-file>*

<response-file> — file in cui sono scritti i parametri di inizializzazione del database, riga per riga, nello stesso ordine dei parametri del comando `database-init`.

Formato del file:

```
<nome_di_file_completo_della_chiave_di_licenza>

<password_amministratore>
```

> Si il response-file viene utilizzato in SO Windows, è possibile utilizzare qualsiasi carattere nella password dell'amministratore.

Se nella riga è indicato il valore `%nil`, verrà utilizzato il valore di default (come in `database-init`).

Aggiornamento della versione del database

`drwcsd modexecdb database-upgrade [pretend] [upgrade_ver_flag]` — per avviare il Server Dr.Web per aggiornare la struttura del database durante il passaggio a una nuova versione tramite gli script interni.

- `pretend=false` — valore di default. Prescrive di aggiornare il database. Se si indica il valore `true`, verrà solo eseguito il controllo di stato di aggiornamento del database invece del suo aggiornamento effettivo.
- `upgrade_ver_flag=true` — se è indicato il valore `true`, durante l'aggiornamento, viene eseguito il commit della versione del database e dei dati nel database ad ogni aggiornamento riuscito alla versione dello schema del database successiva.

Esportazione del database

a) `drwcsd modexecdb database-export` <*file*> `[ignore_tables]` — esportazione del database nel file indicato.

- <*file*> — percorso del file in cui verrà eseguita l'esportazione del database.
- `ignore_tables` — consente di indicare una stringa o una tabella di stringhe con i nomi delle postazioni da non esportare.

Esempio per SO Windows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=trace -log="C:\Program Files\DrWeb Server\var\exportdb.log"
modexecdb database-export "C:\Program Files\DrWeb Server\esbase.es"
```

Sotto SO della famiglia **UNIX** l'azione viene eseguita dall'account utente `drwcs:drwcs` nella directory `$DRWCS_VAR` (eccetto SO **FreeBSD** che di default salva il file nella directory da cui è avviato lo script; se il percorso viene indicato esplicitamente, la directory deve essere provvista dei permessi di scrittura per <*utente*>:<*gruppo*> che sono stati creati durante l'installazione, di default è `drwcs:drwcs`).

b) `drwcsd modexecdb database-export-xml` <*file_xml*> `[ignore_tables]` — esportazione del database nel file XML indicato.

- <*file_xml*> — percorso del file XML in cui verrà eseguita l'esportazione del database.
- `ignore_tables` — consente di indicare una stringa o una tabella di stringhe con i nomi delle postazioni da non esportare.

Se viene indicata l'estensione di file `gz`, il file di database verrà compresso all'esportazione in un archivio GZIP.

Se nessun'estensione viene indicata o viene indicata un'estensione diversa da `gz`, il file di esportazione non verrà compresso in archivio.

Esempio per SO Windows:

- Per esportare il database in un file XML senza compressione:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -bin-root="C:\Program Files\DrWeb Server" -var-
root="C:\Program Files\DrWeb Server\var" -verbosity=trace -rotate=10,10m -
log="C:\Program Files\DrWeb Server\var\exportxmldb.log" modexecdb
database-export-xml database.db
```

- Per esportare il database in un file XML compresso in archivio:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -bin-root="C:\Program Files\DrWeb Server" -var-
root="C:\Program Files\DrWeb Server\var" -verbosity=trace -rotate=10,10m -
log="C:\Program Files\DrWeb Server\var\exportxmldb.log" modexecdb
database-export-xml database.gz
```

Esempio per il SO della famiglia UNIX:

- Per esportare il database in un file XML senza compressione:

```
/etc/init.d/drwcsd modexecdb database-export-xml /es/database.db
```

- Per esportare il database in un file XML compresso in archivio:

```
/etc/init.d/drwcsd modexecdb database-export-xml /es/database.gz
```

Importazione del database

a) `drwcsd modexecdb database-import` <*file*> `[ignore_tables]` — importazione del database dal file indicato (il vecchio contenuto del database viene cancellato).

- <*file*> — percorso del file in cui verrà eseguita l'esportazione del database.
- `ignore_tables` — consente di indicare una stringa o una tabella di stringhe con i nomi delle postazioni da non importare.

b) `drwcsd modexecdb database-import-and-upgrade` <*file*> `[import_only_flag] [upgrade_ver_flag] [ignore_tables]` — importazione e aggiornamento di un database ottenuto attraverso l'esportazione da un Server Dr.Web delle versioni precedenti (il vecchio contenuto del database viene cancellato).

- <*file*> — percorso del file da cui verrà eseguita l'importazione del database.
- `import_only_flag` — se è indicato il valore `true`, l'aggiornamento e la verifica del database non verranno eseguiti, verrà eseguita solo l'importazione.
- `upgrade_ver_flag=true` — se è indicato il valore `true`, durante l'aggiornamento del database, viene eseguito il commit della versione del database e dei dati in esso ad ogni aggiornamento riuscito alla versione dello schema del database successiva.
- `ignore_tables` — consente di indicare una stringa o una tabella di stringhe con i nomi delle postazioni da non importare.

Prima di utilizzare il comando `database-import-and-upgrade`, è necessario eseguire il backup del database.

Qualsiasi problema nel processo dell'esecuzione di questo comando può portare alla rimozione di tutte le informazioni dal database.

L'uso del comando `database-import-and-upgrade` per l'importazione con l'aggiornamento della versione del database è solo possibile nei limiti di un singolo database.

Verifica del database

`drwcsd modexecdb database-verify [full=false [ignore-version=false]]` — avvia il Server Dr.Web per verificare il database. Per scrivere informazioni sui risultati nel file di log, il comando deve essere inserito con l'opzione `-log`. L'utilizzo di questa opzione è descritto in maggior dettaglio in p. G3.8. Descrizione delle opzioni.

- `full=false` — definisce la modalità di verifica. Con il valore di default (`false`) viene eseguita la verifica rapida, con il valore `true` la verifica completa.
- `ignore-version=false` — determina se la versione dello schema del database va ignorata durante la verifica. Di default è `false`. Se è indicato il valore `true`, la verifica continuerà anche se la versione dello schema non è corretta.

Accelerazione del database

`drwcsd [<opzioni>] modexecdb database-speedup` — esegui i comandi `VACUUM`, `CLUSTER`, `ANALYZE` per velocizzare l'utilizzo del database.

Ripristino del database

`drwcsd repairdb` — esegui il ripristino di un'immagine danneggiata del database incorporato **SQLite3** o di tabelle danneggiate del database esterno **MySQL**.

Il ripristino di **SQLite3** può anche essere effettuato automaticamente durante l'avvio del Server Dr.Web, se nelle impostazioni del database **SQLite3** nel Pannello di controllo è selezionato il flag **Ripristina immagine corrotta in automatico** (v. **Manuale dell'amministratore**, p. Ripristino dei database).

Pulizia del database

`drwcsd modexecdb database-clean` — ripulisci il database di Server Dr.Web rimuovendo tutte le tabelle.

Cambio della password amministratore

`drwcsd modexecdb set-admin-password` *<nome_utente> <nuova_password>* — imposta una nuova password per l'account amministratore specificato.

G3.4. Comandi di gestione del repository

Prima di eseguire i comandi `syncrepository`, `restorerepo` e `saverepo`, è necessario obbligatoriamente arrestare il Server Dr.Web.

- `drwcsd syncrepository` — sincronizza il repository con SAM Dr.Web. Il comando avvia il processo Server Dr.Web, viene stabilita una connessione a SAM e quindi il repository viene aggiornato, se sono disponibili aggiornamenti.
- `drwcsd rerepository` — rileggi il repository da disco.
- `drwcsd updrepository` — aggiorna il repository da SAM Dr.Web. Il comando invia a un processo Server Dr.Web in esecuzione un segnale per la connessione a SAM e il successivo

aggiornamento del repository, se sono disponibili aggiornamenti. Se Server Dr.Web non è in esecuzione, l'aggiornamento del repository non viene eseguito.

- `drwcsd [<opzioni>] restorerepo <nome_completo_archivio>` — ripristina il repository di Server Dr.Web da un archivio zip impostato che è stato creato attraverso il comando `saverepo`.
- `drwcsd [<opzioni>] saverepo <nome_completo_archivio>` — salva tutto il repository di Server Dr.Web in un archivio zip indicato. L'archivio risultante può essere importato su Server Dr.Web attraverso il comando `restorerepo`.

Gli archivi utilizzati dai comandi `restorerepo` e `saverepo` non sono compatibili con gli archivi utilizzati per l'esportazione e l'importazione del repository attraverso il Pannello di controllo.

G3.5. Backup dei dati critici del Server Dr.Web

Il backup dei dati critici del Server Dr.Web (chiavi di licenza, contenuti del database, chiave di cifratura privata, configurazione del Server Dr.Web e del Pannello di controllo) viene creato tramite il seguente comando:

`drwcsd -home=<percorso> backup [<directory> [<numero>]]`

- I dati critici di Server Dr.Web vengono copiati nella *<directory>* indicata.
- L'opzione `-home` imposta la directory di installazione di Server Dr.Web.
- Parametro *<numero>* — il numero di copie dello stesso file da salvare.

Esempio per SO Windows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd" -home="C:\Program Files\DrWeb
Server" -verbosity=all -log="C:\Program Files\DrWeb Server\var\backup.log"
backup "C:\DrWeb Backup\"
```

Tutti i file da un backup, ad eccezione del contenuto del database, sono immediatamente utilizzabili. Il backup del database viene salvato nel formato `.gz` compatibile con `gzip` e con altri programmi di archiviazione. È possibile importare il contenuto del database dal backup nel database operativo di Server Dr.Web e in questo modo ripristinare i dati (v. p. Ripristino del database di Dr.Web Enterprise Security Suite).

Nel corso del funzionamento Server Dr.Web salva regolarmente copie di backup di informazioni importanti nelle seguenti directory:

- in caso di SO **Windows**: *<disco_di_installazione>*`:\DrWeb Backup`
- in caso di SO **Linux**: `/var/opt/drwcs/backup`
- in caso di SO **FreeBSD**: `/var/drwcs/backup`

Per l'esecuzione della funzione di backup, nel calendario del Server Dr.Web è incluso un task quotidiano. Se tale task non è disponibile nel calendario, si consiglia di crearlo.

G3.6. Comandi disponibili solo in SO Windows

- `drwcsd [<opzioni>] install [<nome_del_servizio>]` — installa il servizio Server Dr.Web nel sistema e assegna le opzioni impostate per l'avvio di questo servizio.

  <nome_del_servizio> è un suffisso che viene aggiunto al nome del servizio di default, quindi il nome completo del servizio è: `DrWebES-<nome_del_servizio>`. Il comando `install` crea (modifica) un servizio con il nome impostato e scrive automaticamente nei suoi argomenti l'opzione `-service=<nome_del_servizio>`. I servizi esistenti rimangono invariati.

- `drwcsd uninstall [<nome_del_servizio>]` — rimuovi il servizio Server Dr.Web dal sistema.

  <nome_del_servizio> è un suffisso che viene aggiunto al nome del servizio di default, quindi il nome completo del servizio è: `DrWebES-<nome_del_servizio>`.

- `drwcsd kill` — manda in crash il servizio Server Dr.Web (se non è possibile arrestarlo normalmente). Si consiglia di non utilizzare questo comando se non assolutamente necessario.
- `drwcsd reconfigure` — rileggi il file di configurazione e riavviati (si esegue più velocemente — senza avvio di un nuovo processo).
- `drwcsd silent [<opzioni>] <comando>` — proibisci la visualizzazione dei messaggi da Server Dr.Web all'avvio del comando specificato nel parametro *<comando>*. Si utilizza, in particolare, nei file batch per disattivare l'interattività di funzionamento di Server Dr.Web.

G3.7. Comandi disponibili solo in SO della famiglia UNIX

- `drwcsd cacherepo` — crea o ripristina la cache di file del repository di Server Dr.Web.
- `drwcsd config` — simile al comando `reconfigure` o `kill SIGHUP` — riavvio del Server Dr.Web.
- `drwcsd interactive` — avvia il Server Dr.Web ma non passa il controllo al processo.
- `drwcsd newkey` — generazione di nuove chiavi di cifratura `drwcsd.pri` e `drwcsd.pub`, nonché di un certificato `drwcsd-certificate.pem`.
- `drwcsd readrepo` — rileggi il repository da disco. È analogo al comando `rerepository`.
- `drwcsd selfcert [<nome_computer>]` — generazione di un nuovo certificato SSL `(certificate.pem)` e di una chiave privata RSA `(private-key.pem)`. Il parametro imposta il nome del computer su cui è installato il Server Dr.Web per cui verranno generati i file. Se il parametro non è impostato, il nome di computer viene inserito automaticamente dalla funzione di sistema.
- `drwcsd shell <nome_di_file>` — avvio del file di script. Il comando avvia `$SHELL` o `/bin/sh`, passandogli il file specificato.
- `drwcsd showpath` — visualizza tutti i percorsi del programma trascritti nel sistema.
- `drwcsd status` — visualizza lo stato attuale del Server Dr.Web (in esecuzione, arrestato).

G3.8. Descrizione delle opzioni

Opzioni multipiattaforma:

- `-activation-key=<chiave_di_licenza>` — chiave di licenza di Server Dr.Web. Di default è il file `enterprise.key` situato nella sottodirectory `etc` della directory radice.

  Notare che la chiave di licenza di Server Dr.Web non si usa più a partire dalla versione 10. La chiave `-activation-key` può essere utilizzata all'aggiornamento di Server Dr.Web da versioni precedenti e all'inizializzazione del database: l'identificatore di Server Dr.Web verrà preso dalla chiave di licenza indicata.
- `-bin-root=<directory>` — percorso dei file eseguibili. Di default è la sottodirectory `bin` della directory radice.
- `-conf=<file>` — nome e posizione del file di configurazione di Server Dr.Web. Di default è il file `drwcsd.conf` nella sottodirectory `etc` della directory radice.
- `-daemon` — per le piattaforme Windows significa esecuzione come servizio; per le piattaforme UNIX significa: "processo daemon" (il processo deve passare alla directory radice, disconnettersi dal terminale e passare alla modalità background).
- `-db-verify=on` — verifica l'integrità del database all'avvio di Server Dr.Web. Valore predefinito. È fortemente sconsigliato l'avvio con l'indicazione esplicita del valore opposto, ad eccezione di un avvio immediatamente successivo a una verifica del database attraverso il comando `drwcsd modexecdb database-verify`, v. sopra.
- `-help` — visualizza la guida. Simile ai programmi descritti sopra.
- `-hooks` — consenti al Server Dr.Web di eseguire gli script di estensione personalizzati che si trovano nella cartella:
  - in caso di SO Windows: `var\extensions`
  - in caso di SO FreeBSD: `/var/drwcs/extensions`
  - in caso di SO Linux: `/var/opt/drwcs/extensions`

  della directory di installazione di Server Dr.Web. Gli script sono studiati per automatizzare il lavoro dell'amministratore, semplificando ed accelerando l'esecuzione di alcuni lavori. Di default, tutti gli script sono disabilitati.
- `-home=<directory>` — directory di installazione di Server Dr.Web (directory radice). La struttura di questa directory è descritta nella **Guida all'installazione**, p. Installazione di Server Dr.Web per SO Windows. Di default è la directory corrente all'avvio.
- `-log=<file_di_log>` — attiva la registrazione del log di Server Dr.Web nel file nel percorso specificato.

  Per il Server Dr.Web su piattaforme UNIX, invece del nome di file può essere utilizzato il segno "meno", il che significa visualizza il log in output standard. Le operazioni su piattaforme UNIX vengono eseguite dall'account utente drwcs, e se esso non dispone dei permessi di scrivere nella directory del file di log, si verificherà un errore.

Di default: per i SO Windows — `drwcsd.log` nella directory indicata dall'opzione `-var-root`, per i SO della famiglia UNIX viene impostato dall'opzione `-syslog=user` (vedi sotto).

- `-private-key=`<*chiave_privata*> — chiave di cifratura privata di Server Dr.Web. Di default è `drwcsd.pri` nella sottodirectory `etc` della directory radice.
- `-rotate=`<*N*><*f*>`,`<*M*><*u*> — modalità di rotazione del log di funzionamento di Server Dr.Web, dove:

Parametro	Descrizione
<*N*>	Numero totale di file di log (compresi il file attuale e quelli di archivio).
<*f*>	Formato di memorizzazione dei file di log, i valori possibili sono: • z (gzip) — comprimi i file, si usa di default, • p (plain) — non comprimere i file.
<*M*>	Dimensione del file di log o tempo di rotazione a seconda del valore di <*u*>;

<*u*>	Unità di misura, i valori possibili sono:
	• per impostare la rotazione per dimensione del file di log:
	  ▫ k — Kb,
	  ▫ m — Mb,
	  ▫ g — Gb.
	• per impostare la rotazione per tempo:
	  ▫ H — ore,
	  ▫ D — giorni,
	  ▫ W — settimane.

Se è impostata la rotazione per tempo, la sincronizzazione viene eseguita a prescindere dall'ora di avvio del comando: se il valore è H — la sincronizzazione viene eseguita all'inizio dell'ora, se è D — all'inizio del giorno, se è W — all'inizio della settimana (alle 00:00 lunedì) secondo il multiplo indicato nel parametro <*u*>.

Il punto di partenza è il 01 gennaio del 01 anno d.C., UTC+0.

Di default è `10z,10m`, il che significa "conserva 10 file di 10 megabyte ciascuno, utilizza compressione". È inoltre possibile utilizzare un formato specifico `none (-rotate=none)` — questo significa "non usare rotazione e registra informazioni sempre nello stesso file di dimensioni illimitate".

In modalità di rotazione viene utilizzato il seguente formato dei nomi di file: `file.`<*N*>`.log` o `file.`<*N*>`.log.gz`, dove <*N*> è un numero progressivo: 1, 2, ecc.

Per esempio, se il nome del file di log (v. l'opzione sopraccitata `-log`) è stato impostato come `file.log`. Allora:

- `file.log` — il file corrente (in cui le informazioni vengono registrate al momento),

  - `file.1.log` — il file precedente,
  - `file.2.log` e così via — maggiore è il numero, più vecchia è la versione del file di log.
- `-trace` — registra in log informazioni dettagliate sul posto del verificarsi di un errore.
- `-var-root=<directory>` — percorso della directory in cui il Server Dr.Web ha il permesso di scrittura e che è progettata per la memorizzazione dei file modificabili (per esempio, i log, nonché i file di repository). Di default è la sottodirectory `var` della directory radice.
- `-verbosity=<livello>` — livello di dettaglio del log. Di default è `WARNING`. Valori ammissibili: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. I valori `ALL` e `DEBUG3` sono sinonimi.

  Se necessario, è possibile impostare determinati livelli di dettaglio per più fonti di messaggi contemporaneamente nel seguente formato:

  `-verbosity=<fonte_messaggio1>:<livello1>,<fonte_messaggio2>:<livello2>,<fonte_messaggio3>:<livello3>` ecc. L'ereditarietà di `<livello>` si effettua secondo il principio generale, cioè viene trovata la fonte padre più vicina con il livello di dettaglio impostato. L'opzione formato `-verbosity=all:all` equivale all'opzione `-verbosity=all` (vedi inoltre Allegato J. Formato dei file di log).

  

  Questa opzione determina il grado di dettaglio di registrazione del log nel file impostato dall'opzione `-log` successiva ad essa (v. sopra). Un comando può includere diverse opzioni di questo tipo.

  Le opzioni `-verbosity` e `-log` dipendono da posizione.

  Se queste opzioni si usano contemporaneamente, l'opzione `-verbosity` deve precedere l'opzione `-log`: l'opzione `-verbosity` ridefinisce il livello di dettaglio dei log che si trovano nei percorsi che succedono nella riga di comando.

Opzioni disponibili solo nei SO Windows:

- `-minimized` — riduci la finestra (solo nel caso di avvio in modo interattivo anziché come servizio).
- `-service=<nome_del_servizio>` — l'opzione viene utilizzata dal processo del servizio in esecuzione per l'auto-identificazione e per impostare l'auto-protezione sul ramo del registro del servizio Server Dr.Web. `<nome_del_servizio>` è un suffisso che viene aggiunto al nome del servizio di default, quindi il nome completo del servizio è: `DrWebES-<nome_del_servizio>`.

  L'opzione viene utilizzata dal comando `install`, l'uso indipendente non è previsto.
- `-screen-size=<dimensione>` — (solo nel caso di avvio in modo interattivo anziché come servizio) — la dimensione in righe del log visibile nella finestra di Server Dr.Web, di default è 1000.

Opzioni disponibili solo nei SO della famiglia UNIX:

- `-etc=<percorso>` — percorso della directory `etc` (`<var>/etc`).
- `-keep` — non rimuovere il contenuto della directory temporanea dopo l'installazione del Server Dr.Web.
- `-pid=<file>` — file in cui il Server Dr.Web registra l'identificatore del suo processo.
- `-syslog=<modalità>` — registrazione di informazioni nel log di sistema. Le modalità possibili sono: `auth`, `cron`, `daemon`, `kern`, `lpr`, `mail`, `news`, `syslog`, `user`, `uucp`, `local0-local7` e in caso di alcune piattaforme — `ftp`, `authpriv` e `console`.

  Le opzioni `-syslog` e `-log` funzionano insieme. Cioè se il Server Dr.Web viene eseguito con l'opzione `-syslog` (per esempio, `service drwcsd start -syslog=user`), il Server Dr.Web si avvierà con il valore impostato per l'opzione `-syslog` e con il valore predefinito dell'opzione `-log`.

- `-user=<utente>`, `-group=<gruppo>` — sono disponibili solo per SO UNIX all'avvio con i permessi dell'utente **root**; significano "cambia l'utente o il gruppo del processo ed eseguiti con i permessi dell'utente (gruppo) indicato".

G3.9. Variabili disponibili in SO della famiglia UNIX

Per semplificare la gestione del Server Dr.Web sotto SO della famiglia UNIX, all'amministratore vengono fornite variabili che si trovano nel file di script conservato nella seguente directory:

- In caso di SO Linux: `/etc/init.d/drwcsd`.
- In caso di SO FreeBSD: `/usr/local/etc/rc.d/drwcsd` (collegamento simbolico a `/usr/local/etc/drweb.com/software/init.d/drwcsd`).

La corrispondenza tra le variabili e le opzioni della riga di comando per `drwcsd` è riportata in Tabella H-1.

Tabella H-1.

Opzione	Variabile	Parametri predefiniti
`-home`	DRWCS_HOME	• `/usr/local/drwcs` — in caso di SO FreeBSD, • `/opt/drwcs` — in caso di SO Linux.
`-var-root`	DRWCS_VAR	• `/var/drwcs` — in caso di SO FreeBSD, • `/var/opt/drwcs` — in caso di SO Linux.
`-etc`	DRWCS_ETC	`$DRWCS_VAR/etc`
`-rotate`	DRWCS_ROT	`10,10m`
`-verbosity`	DRWCS_LEV	`info`

Opzione	Variabile	Parametri predefiniti
`-log`	DRWCS_LOG	`$DRWCS_VAR/log/drwcsd.log`
`-conf`	DRWCS_CFG	`$DRWCS_ETC/drwcsd.conf`
`-pid`	DRWCS_PID	
`-user`	DRWCS_USER	
`-group`	DRWCS_GROUP	
`-hooks`	DRWCS_HOOKS	
`-trace`	DRWCS_TRACE	

Le variabili `DRWCS_HOOKS` e `DRWCS_TRACE` non hanno parametri. Se le variabili vengono impostate, le opzioni corrispondenti vengono aggiunte con l'esecuzione di script. Se le variabili non sono impostate, le opzioni non verranno aggiunte.

Le altre variabili sono riportate in Tabella H-2.

Tabella H-2.

Variabile	Parametri predefiniti	Descrizione
DRWCS_ADDOPT		Le opzioni della riga di comando aggiuntive che devono essere passate a drwcsd all'avvio.
DRWCS_CORE	`unlimited`	Dimensione massima di core file.
DRWCS_FILES	131170	Numero massimo di descrittori di file che il Server Dr.Web può aprire.
DRWCS_BIN	`$DRWCS_HOME/bin`	Directory da cui viene avviato `drwcsd`.
DRWCS_LIB	`$DRWCS_HOME/lib`	Directory con le librerie di Server Dr.Web.

I valori di parametri predefiniti entrano in vigore se tali variabili non sono definite nello script `drwcsd`.

Le variabili `DRWCS_HOME`, `DRWCS_VAR`, `DRWCS_ETC`, `DRWCS_USER`, `DRWCS_GROUP`, `DRWCS_HOOKS` sono già definite nel file dello script `drwcsd`.

Se esiste il file `/var/opt/drwcs/etc/common.conf`, questo file verrà incluso in `drwcsd`, il che può ridefinire alcune variabili, però se non vengono esportate (tramite il comando `export`), non avranno alcun impatto.

Per impostare le variabili

1. Aggiungere la definizione della variabile al file dello script `drwcsd`.
2. Esportare la variabile tramite il comando `export` (viene impostato nello stesso posto).
3. Quando viene avviato ancora un altro processo da questo script, questo processo legge i valori che sono stati definiti.

G3.10. Gestione di Server Dr.Web sotto SO della famiglia UNIX tramite il comando kill

Il Server Dr.Web sotto UNIX viene gestito dai segnali inviati al processo Server Dr.Web da parte dell'utility `kill`.

Una guida dettagliata all'utility `kill` può essere ottenuta tramite il comando `man kill`.

Segnali dell'utility e le azioni da essi eseguite:

- `SIGWINCH` — output nel file di log delle statistiche di funzionamento (tempo CPU, utilizzo di memoria ecc.),
- `SIGUSR1` — rilettura del repository da disco,
- `SIGUSR2` — rilettura dei modelli di avviso da disco,
- `SIGHUP` — riavvio del Server Dr.Web,
- `SIGTERM` — arresto del Server Dr.Web,
- `SIGQUIT` — arresto del Server Dr.Web,
- `SIGINT` — arresto del Server Dr.Web.

Le azioni analoghe per il Server Dr.Web sotto il sistema operativo Windows vengono realizzate tramite le opzioni del comando drwcsd, v. Allegato G3.3. Comandi di gestione del database.

G4. Scanner Dr.Web per Windows

Questo componente del software postazione ha i parametri della riga di comando che sono descritti nel manuale utente **Agent Dr.Web per Windows**. L'unica differenza consiste nel fatto che all'avvio di Scanner da parte di Agent Dr.Web i parametri `/go /st` vengono passati a Scanner automaticamente e obbligatoriamente.

G5. Server proxy Dr.Web

Per configurare i parametri del Server proxy, avviare con le opzioni corrispondenti il file eseguibile `drwcsd-proxy` che si trova nella sottodirectory `bin` della directory di installazione di Server proxy.

Formato del comando di avvio

`drwcsd-proxy [<opzioni>] [<comandi> [<argomenti_dei_comandi>]]`

Opzioni valide

Opzioni multipiattaforma:

- `--console=yes|no` — avvia il Server proxy in modalità interattiva. In questo caso il log di funzionamento del Server proxy viene visualizzato nella console.

  Di default: `no`.
- `--etc-root=<percorso>` — percorso della directory con i file di configurazione (`drwcsd-proxy.conf`, `drwcsd.proxy.auth` ecc.).

  Di default: `$var/etc`
- `--home=<percorso>` — percorso della directory di installazione del Server proxy.

  Di default: `$exe-dir/`
- `--log-root=<percorso>` — percorso della directory con i file di log di funzionamento del Server proxy.

  Di default: `$var/log`
- `--pool-size=<N>` — numero di thread per l'elaborazione dei dati dei client.

  Di default: il numero di core del computer su cui è installato il Server proxy (ma non meno di 2).
- `--rotate=<N><f>,<M><u>` — modalità di rotazione del log di funzionamento del Server proxy, dove:

Parametro	Descrizione
<*N*>	Numero totale di file di log (compresi il file attuale e quelli di archivio).
<*f*>	Formato di memorizzazione dei file di log, i valori possibili sono: • z (gzip) — comprimi i file, si usa di default, • p (plain) — non comprimere i file.
<*M*>	Dimensione del file di log o tempo di rotazione a seconda del valore di <*u*>;
<*u*>	Unità di misura, i valori possibili sono:

Parametro	Descrizione
	• per impostare la rotazione per dimensione del file di log: ▫ k — Kb, ▫ m — Mb, ▫ g — Gb. • per impostare la rotazione per tempo: ▫ H — ore, ▫ D — giorni, ▫ W — settimane.

Se è impostata la rotazione per tempo, la sincronizzazione viene eseguita a prescindere dall'ora di avvio del comando: se il valore è H — la sincronizzazione viene eseguita all'inizio dell'ora, se è D — all'inizio del giorno, se è W — all'inizio della settimana (alle 00:00 lunedì) secondo il multiplo indicato nel parametro <*u*>.

Il punto di partenza è il 01 gennaio del 01 anno d.C., UTC+0.

Di default `10,10m` che significa "conserva 10 file da 10 megabyte, utilizza compressione".

- `--trace=yes|no` — attiva la registrazione dettagliata delle richieste al Server proxy. È disponibile solo se la build del Server proxy supporta la registrazione dettagliata dello stack di chiamate (nel caso di un'eccezione, lo stack viene scritto nel log).

  Di default: `no`.

- `--tmp-root=`<*percorso*> — percorso della directory con i file temporanei. Si usa all'aggiornamento automatico del Server proxy.

  Di default, è `$var/tmp`.

- `--var-root=`<*percorso*> — percorso della directory di lavoro del Server proxy per la conservazione della cache e del database.

  Di default:

  ▫ SO Windows: `%ALLUSERSPROFILE%\Doctor Web\drwcs`

  ▫ SO Linux: `/var/opt/drwcs`

  ▫ SO FreeBSD: `/var/drwcs`

- `--verbosity=`<*livello_di_dettaglio*> — livello di dettaglio del log. Di default è `TRACE`. I valori ammissibili sono: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. I valori `ALL` e `DEBUG3` sono sinonimi.

  Se necessario, è possibile impostare determinati livelli di dettaglio per più fonti di messaggi contemporaneamente nel seguente formato:

  `-verbosity=`<*fonte_messaggio1*>`:`<*livello1*>`,`<*fonte_messaggio2*>`:`<*livello2*>`,`<*fonte_messaggio3*>`:`<*livello3*> ecc. L'ereditarietà di <*livello*> si effettua secondo il principio generale, cioè viene trovata la fonte padre più vicina con il livello di dettaglio

impostato. L'opzione formato `-verbosity=all:all` equivale all'opzione `-verbosity=all` (vedi inoltre Allegato J. Formato dei file di log).

Tutte le opzioni di configurazione dei parametri del funzionamento del Server proxy possono essere utilizzate contemporaneamente.

Opzioni sotto i sistemi operativi della famiglia UNIX:

- `--user` — imposta l'identificatore dell'utente. L'opzione è valida sia per il funzionamento in modalità normale che per il funzionamento in modalità daemon.
- `--group` — imposta l'identificatore del gruppo. L'opzione è valida sia per il funzionamento in modalità normale che per il funzionamento in modalità daemon.
- `--pid=`<*percorso*> — percorso della directory con l'identificatore del processo.

  Di default: `/var/opt/drwcs/run/drwcsd-proxy.pid`

Comandi ammissibili e i relativi argomenti

Se il comando non è specificato, di default si usa il comando `run`.

- `import` <*percorso*> `[`<*revisione*>`]` `[`<*prodotti*>`]` — importa i file dal repository di Server Dr.Web nella cache di Server proxy.
  - <*percorso*> — percorso della directory con il repository di Server Dr.Web. Il repository di Server Dr.Web deve prima essere scaricato sul computer su cui è installato Server proxy.
  - <*revisione*> — numero massimo di revisioni da importare. Se il valore non è indicato, verranno importate tutte le revisioni.
  - <*prodotti*> — lista dei prodotti da importare, separati dallo spazio. Di default viene utilizzata una lista vuota, cioè importa tutti i prodotti del repository, tranne Server Dr.Web. Se è specificata una lista, verranno importati solo i prodotti dalla lista.
- `help` — visualizza la guida alle opzioni per la configurazione di Server proxy.
- `run` — avvia Server proxy in modalità normale.

Comandi disponibili solo per SO Windows:

- `install` — installa il servizio.
- `start` — avvia il servizio istallato.
- `stop` — termina il servizio in esecuzione.
- `uninstall` — rimuovi il servizio.

Comandi disponibili solo per SO della famiglia UNIX:

- `daemon` — avvia Server proxy in modalità daemon (vedi inoltre Opzioni sotto i sistemi operativi della famiglia UNIX).

Script di gestione del Server proxy e variabili disponibili sotto i SO della famiglia UNIX

Per semplificare la gestione del Server proxy sotto i SO della famiglia UNIX, all'amministratore vengono fornite variabili che si trovano nel file di script `drwcsd-proxy.sh` situato nella seguente directory:

- **Linux**: `/etc/init.d/dwcp_proxy`
- **FreeBSD**: `/usr/local/etc/rc.d/dwcp_proxy`

Lo script accetta i seguenti comandi:

- `import` <*percorso*> `[`<*revisione*>`]` `[`<*prodotti*>`]` — importa i file dal repository di Server Dr.Web nella cache di Server proxy (analogo al comando di Server proxy, v. sopra).
- `interactive` — avvia Server proxy in modalità interattiva. In questo caso il log di funzionamento del Server proxy viene visualizzato nella console.
- `start` — avvia Server proxy in modalità daemon.
- `status` — controlla se il daemon è in esecuzione.
- `stop` — termina il daemon in esecuzione.

La corrispondenza tra le variabili e le opzioni della riga di comando per `drwcsd-proxy` è riportata in Tabella H-3.

Tabella H-3.

Opzione	Variabile	Parametri predefiniti
`--home=`<*percorso*>	`$DRWCS_PROXY_HOME`	`$exe-dir/`
`--var-root=`<*percorso*>	`$DRWCS_PROXY_VAR`	• SO Linux: `/var/opt/drwcs` • SO FreeBSD: `/var/drwcs`
`--etc-root=`<*percorso*>	`$DRWCS_PROXY_ETC`	`$var/etc`
`--tmp-root=`<*percorso*>	`$DRWCS_PROXY_TMP`	`$var/tmp`
`--log-root=`<*percorso*>	`$DRWCS_PROXY_LOG`	`$var/log`
–	`$DRWCS_PROXY_LIB`	`$DRWCS_PROXY_HOME/lib`
–	`$DRWCS_PROXY_BIN`	`$DRWCS_PROXY_HOME/bin`

Opzione	Variabile	Parametri predefiniti
`--verbosity=<livello_di_dettaglio>`	`$DRWCS_PROXY_VERBOSITY`	`INFO`
`--rotate=<N><f>,<M><u>`	`$DRWCS_PROXY_ROTATE`	`10,10m`
`--pid`	`$DRWCS_PROXY_PID`	`/var/opt/drwcs/run/drwcsd-proxy.pid`
-	`$NO_DRWCS_PROXY_USER`	Se è assegnato qualsiasi valore, `$DRWCS_PROXY_USER` viene ignorato.
`--user`	`$DRWCS_PROXY_USER`	–
-	`$NO_DRWCS_PROXY_GROUP`	Se è assegnato qualsiasi valore, `$DRWCS_PROXY_GROUP` viene ignorato.
`--group`	`$DRWCS_PROXY_GROUP`	–
-	`$DRWCS_PROXY_FILES`	131170, ma non inferiore al limite attuale.

G6. Installer di Server Dr.Web per SO della famiglia UNIX

Formato del comando di avvio:

`<nome_pacchetto>.run [<opzioni>] [--] [<argomenti>]`

dove:

- `[--]` — un carattere opzionale separato che indica la fine della lista delle opzioni e separa la lista delle opzioni dalla lista degli argomenti aggiuntivi.
- `[<argomenti>]` — argomenti aggiuntivi o script incorporati.

Le opzioni per avere la guida o informazioni sul pacchetto:

- `--help` — visualizza la guida sulle opzioni.
- `--info` — visualizza informazioni dettagliate sul pacchetto: nome; directory di destinazione; dimensione in forma decompressa; algoritmo di compressione; data di compressione; versione `makeself` attraverso cui la compressione è stata eseguita; comando attraverso cui la compressione è stata eseguita; script che verrà eseguito dopo la decompressione; indica se i contenuti dell'archivio verranno copiati nella directory temporanea (se no, nulla viene visualizzato); indica se la directory di destinazione è permanente o verrà rimossa dopo l'esecuzione dello script.

- `--lsm` — visualizza il contenuto del record LSM incorporato con informazioni di base sul pacchetto: nome, versione, descrizione, autore ecc. Se il record LSM non veniva compilato, verrà visualizzato il messaggio corrispondente.
- `--list` — visualizza la lista dei file nel pacchetto di installazione.
- `--check` — verifica l'integrità del pacchetto di installazione.

Le opzioni per l'avvio del pacchetto:

- `--confirm` — visualizza una richiesta prima di eseguire lo script incorporato.
- `--noexec` — non eseguire lo script incorporato.
- `--keep` — non rimuovere la directory indicata dopo aver eseguito lo script incorporato.
- `--nox11` — non eseguire l'emulazione di terminale `xterm` al termine dell'installazione.
- `--nochown` — non nominare proprietario dei file curati l'utente che avvia l'installazione.
- `--log` <*percorso*> — registra il log di installazione in un file nel percorso indicato.
- `--nolog` — non registrare il log di installazione.
- `--target` <*directory*> — estrai il pacchetto di installazione nella directory indicata.
- `--tar` <*argomento_1*> `[`<*argomento_2*> ...`]` — ottieni l'accesso ai contenuti del pacchetto di installazione tramite il comando `tar`.

Argomenti aggiuntivi:

- `--help` — visualizza la guida sulle opzioni avanzate.
- `--quiet` — avvia l'installer in background. Si usa la risposta affermativa a tutte le seguenti domande dell'installer:
  - accetta il contratto di licenza,
  - imposta la copiatura di backup nella directory predefinita,
  - continua l'installazione a condizione che il pacchetto supplementare (extra) installato in sistema verrà rimosso.
- `--clean` — installa il pacchetto con le impostazioni predefinite di Server Dr.Web senza utilizzare una copia di backup per ripristinare le impostazioni dell'installazione precedente.
- `--preseed` <*percorso*> — percorso del file di configurazione contenente le risposte predefinite alle domande dell'installer nel corso dell'installazione.

  Le variabili per impostare le risposte predefinite nel file di configurazione:
  - `DEFAULT_BACKUP_DIR=`<*percorso*> — il percorso della directory con la copia di backup che verrà utilizzata per ripristinare le impostazioni della versione precedente (non si usa se è impostata un'installazione con le impostazioni di default).
  - `QUIET_INSTALL=[0|1]` — determina l'utilizzo della modalità background dell'installer:
    - 0 — avvia l'installer in modalità background;
    - 1 — avvia l'installer in modalità normale.
  - `CLEAN_INSTALL=[0|1]` — determina l'utilizzo della copia di backup nell'installazione:

- 0 — un'installazione con le impostazioni di default senza ripristinare le impostazioni dalla copia di backup;
- 1 — un'installazione con il ripristino delle impostazioni dalla copia di backup che si trova nella directory definita dalla variabile `DEFAULT_BACKUP_DIR`. Se la variabile `DEFAULT_BACKUP_DIR` non è impostata, la copia di backup viene presa da `/var/tmp/drwcs`.

- `ADMIN_PASSWORD=<password>` — password per l'account amministratore predefinito (**admin**).
  - Se la variabile `ADMIN_PASSWORD` è impostata nel file, il suo valore è usato come password dell'amministratore, e alla fine dell'installazione viene visualizzato il messaggio:
    `Password specified in the configuration file for the default administrator (admin): <password>`
  - Se la variabile `ADMIN_PASSWORD` non è impostata nel file, la password viene generata in automatico, e alla fine dell'installazione viene visualizzato il messaggio:
    `Automatically generated password for the default administrator (admin): <password>`

Se nel caso di utilizzo dell'opzione `--preseed` nel file di configurazione non viene definito l'avvio dell'installer in modalità silenziosa tramite la variabile `QUIET_INSTALL=0`, allora i valori delle altre variabili del file di configurazione verranno ridefiniti dall'utente nel corso dell'installazione.

G7. Utility

G7.1. Utility di generazione delle chiavi e dei certificati digitali

Si mettono a disposizione le seguenti versioni dell'utility console di generazione delle chiavi e dei certificati digitali:

File eseguibile	Posizione	Descrizione
`drweb-sign-<sistema_operativo>-<numero_di_bit>`	Pannello di controllo, sezione **Amministrazione** → **Utility**	Versione indipendente dell'utility. Può essere avviata da qualsiasi directory e su qualsiasi computer con il sistema operativo corrispondente.
	Directory di Server Dr.Web `webmin/utilities`	
`drwsign`	Directory di Server Dr.Web `bin`	La versione dell'utility dipende dalla disponibilità delle librerie del server. Può essere avviata solo dalla directory della sua posizione.

Le versioni dell'utility `drweb-sign-<sistema_operativo>-<numero_di_bit>` e `drwsign` hanno le funzionalità simili. Di seguito nella sezione viene riportata la versione `drwsign`, tuttavia, tutti gli esempi sono adatti per entrambe le versioni.

Formato del comando di avvio

- `drwsign check [-public-key=<chiave_pubblica>] <file>`

  Verifica la firma del file indicato utilizzando la chiave pubblica del soggetto che ha firmato tale file.

Parametro dell'opzione	Valore predefinito
<chiave_pubblica>	`drwcsd.pub`

- `drwsign extract [-private-key=<chiave_privata>] [-cert=<certificato_Server_Dr.Web>] <chiave_pubblica>`

  Estrai la chiave pubblica dal file della chiave privata o dal file del certificato e scrivi la chiave pubblica nel file indicato.

  Le opzioni `-private-key` e `-cert` si escludono a vicenda, cioè può essere impostata solo una di esse; se vengono impostate contemporaneamente entrambe le opzioni, il comando termina con errore.

  È obbligatoria l'indicazione del parametro per le opzioni.

  Se nessuna opzione è impostata, verrà utilizzata `-private-key=drwcsd.pri` per estrarre la chiave pubblica dalla chiave privata `drwcsd.pri`.

Parametro dell'opzione	Valore predefinito
<*chiave_privata*>	`drwcsd.pri`

- `drwsign genkey [`<*chiave_privata*>` [`<*chiave_pubblica*>`]]`

  Genera una coppia chiave pubblica — chiave privata e scrivile nei file corrispondenti.

Parametro dell'opzione	Valore predefinito
<*chiave_privata*>	`drwcsd.pri`
<*chiave_pubblica*>	`drwcsd.pub`

La versione di utility per le piattaforme Windows (a differenza della versione per i SO UNIX) non protegge in nessun modo la chiave privata dalla copiatura.

- `drwsign gencert [-private-key=`<*chiave_privata*>`] [-subj=`<*campi_del_soggetto*>`] [-days=`<*validità*>`] [`<*certificato_autofirmato*>`]`

  Genera un certificato autofirmato utilizzando la chiave privata di Server Dr.Web e scrivilo nel file corrispondente.

Parametro dell'opzione	Valore predefinito
<*chiave_privata*>	`drwcsd.pri`
<*campi_del_soggetto*>	`/CN=`<*nome_host*>
<*validità*>	`3560`
<*certificato_autofirmato*>	`drwcsd-certificate.pem`

- `drwsign gencsr [-private-key=`<*chiave_privata*>`] [-subj=`<*campi_del_soggetto*>`] [`<*richiesta_di_firma_del_certificato*>`]`

  Genera una richiesta di firma del certificato in base alla chiave privata e scrivi questa richiesta nel file corrispondente.

  Può essere utilizzato per firmare il certificato di un altro server, per esempio, per firmare il certificato di Server proxy Dr.Web tramite la chiave di Server Dr.Web.

  Per firmare tale richiesta, utilizzare l'opzione `signcsr`.

Parametro dell'opzione	Valore predefinito
<*chiave_privata*>	`drwcsd.pri`
<*campi_del_soggetto*>	`/CN=`<*nome_host*>
<*richiesta_di_firma_del_certificato*>	`drwcsd-certificate-sign-request.pem`

- `drwsign genselfsign [-show] [-subj=<campi_del_soggetto>] [-days=<validità>] [<chiave_privata> [<certificato_autofirmato>]]`

  Genera un certificato autofirmato RSA e una chiave privata RSA per il web server e scrivili nei file corrispondenti.

  L'opzione `-show` restituisce il contenuto del certificato in una forma leggibile.

Parametro dell'opzione	Valore predefinito
<*campi_del_soggetto*>	`/CN=`<*nome_host*>
<*validità*>	`3560`
<*chiave_privata*>	`private-key.pem`
<*certificato_autofirmato*>	`certificate.pem`

- `drwsign hash-check [-public-key=`<*chiave_pubblica*>`]` <*file_di_hash*> <*file_di_firma*>

  Verifica la firma del numero a 256 bit indicato nel formato del protocollo client-server.

  Nel parametro <*file_di_hash*> viene impostato un file con un numero a 256 bit da firmare. Nel file <*file_di_firma*> viene impostato il risultato della firma (due numeri a 256 bit).

Parametro dell'opzione	Valore predefinito
<*chiave_pubblica*>	`drwcsd.pub`

- `drwsign hash-sign [-private-key=`<*chiave_privata*>`]` <*file_di_hash*> <*file_di_firma*>

  Firma il numero a 256 bit indicato nel formato del protocollo client-server.

  Nel parametro <*file_di_hash*> viene impostato un file con un numero a 256 bit da firmare. Nel file <*file_di_firma*> viene impostato il risultato della firma (due numeri a 256 bit).

Parametro dell'opzione	Valore predefinito
<*chiave_privata*>	`drwcsd.pri`

- `drwsign help [`<*comando*>`]`

  Restituisci la breve guida al programma o a un comando specifico nel formato della riga di comando.

- `drwsign sign [-private-key=`<*chiave_privata*>`]` <*file*>

  Firma <*file*>, utilizzando la chiave privata.

Parametro dell'opzione	Valore predefinito
<*chiave_privata*>	`drwcsd.pri`

- `drwsign signcert [-ca-key=<chiave_privata>] [-ca-cert=<certificato_Server_Dr.Web>] [-cert=<certificato_da_firmare>] [-days=<validità>] [-eku=<scopo>] [<certificato_firmato>]`

  Firma il <*certificato_da_firmare*> predisposto tramite la chiave privata e il certificato di Server Dr.Web. Il certificato firmato viene salvato in un file separato.

  Può essere utilizzato per firmare il certificato di Server proxy Dr.Web tramite la chiave di Server Dr.Web.

  Sono possibili i seguenti valori dell'opzione `-eku` (estensione Extended Key Usage):

  - `drwebServerAuth` — autenticazione di Server/Server proxy da parte di Agent Dr.Web,
  - `drwebMeshDAuth` — autenticazione di Server di scansione da parte di Agent virtuale.

Parametro dell'opzione	Valore predefinito
<*chiave_privata*>	`drwcsd.pri`
<*certificato_Server_Dr.Web*>	`drwcsd-ca-cerificate.pem`
<*certificato_da_firmare*>	`drwcsd-certificate.pem`
<*validità*>	`3560`
<*scopo*>	`drwebServerAuth`
<*certificato_firmato*>	`drwcsd-signed-certificate.pem`

- `drwsign signcsr [-ca-key=<chiave_privata>] [-ca-cert=<certificato_Server_Dr.Web>] [-csr=<richiesta_di_firma_del_certificato>] [-days=<validità>] [-eku=<scopo>] [<certificato_firmato>]`

  Firma <*richiesta_di_firma_del_certificato*>, generato dal comando `gencsr`, tramite la chiave privata e il certificato di Server Dr.Web. Il certificato firmato viene salvato in un file separato.

  Può essere utilizzato per firmare il certificato di un altro server, per esempio, per firmare il certificato di Server proxy Dr.Web tramite la chiave di Server Dr.Web.

  Sono possibili i seguenti valori dell'opzione `-eku` (estensione Extended Key Usage):

  - `drwebServerAuth` — autenticazione di Server/Server proxy da parte di Agent Dr.Web,
  - `drwebMeshDAuth` — autenticazione di Server di scansione da parte di Agent virtuale.

Parametro dell'opzione	Valore predefinito
<*chiave_privata*>	`drwcsd.pri`
<*certificato_Server_Dr.Web*>	`drwcsd-cerificate.pem`
<*richiesta_di_firma_del_certificato*>	`drwcsd-certificate-sign-request.pem`
<*validità*>	`3560`

Parametro dell'opzione	Valore predefinito
<*scopo*>	`drwebServerAuth`
<*certificato_firmato*>	`drwcsd-signed-certificate.pem`

- `drwsign tlsticketkey [`<*ticket-TLS*>`]`

  Genera ticket TLS.

  Può essere utilizzato in un cluster di Server Dr.Web per sessioni TLS comuni.

Parametro dell'opzione	Valore predefinito
<*ticket_TLS*>	`tickets-key.bin`

- `drwsign verify [-ss-cert] [-CAfile=`<*certificato_Server_Dr.Web*>`] [`<*certificato_da_verificare*>`]`

  Verifica la validità del certificato in base a un certificato di Server Dr.Web affidabile.

  L'opzione `-ss-cert` prescrive di ignorare il certificato affidabile e solo verificare la correttezza del certificato autofirmato.

Parametro dell'opzione	Valore predefinito
<*certificato_Server_Dr.Web*>	`drwcsd-certificate.pem`
<*certificato_da_verificare*>	`drwcsd-signed-certificate.pem`

- `drwsign x509dump [`<*certificato_da_stampare*>`]`

  Stampa il dump di qualsiasi certificato x509.

Parametro dell'opzione	Valore predefinito
<*certificato_da_stampare*>	`drwcsd-certificate.pem`

- `drwsign version`

  Visualizza informazioni sulla versione dell'utility.

G7.2. Utility di amministrazione del database incorporato

Per l'amministrazione del database incorporato (SQLite3) è fornita l'utility `drwidbsh3`.

L'utility si trova nelle seguenti directory:

- in caso di SO **Linux**: `/opt/drwcs/bin`
- in caso di SO **FreeBSD**: `/usr/local/drwcs/bin`
- in caso di SO **Windows**: <*directory_di_installazione_Server_Dr.Web*>`\bin`

(di default, la directory di installazione di Server Dr.Web: `C:\Program Files\DrWeb Server`).

Formato del comando di avvio:

`drwidbsh3 <nome_completo_file_database>`

Il programma funziona in modalità di testo interattivo, è in attesa di input da parte dell'utente dei comandi del programma (i comandi iniziano con il punto).

Per richiamare la guida ad altri programmi, inserire `.help`. Verrà visualizzato il testo della guida.

Per ulteriori informazioni, utilizzare manuali del linguaggio SQL.

G7.3. Utility di diagnostica remota del Server Dr.Web

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. La versione grafica dell'utility è disponibile solo in SO Windows.

L'utility è disponibile nelle seguenti versioni:

- In caso di SO Windows — versione con interfaccia grafica.
- In caso di SO della famiglia UNIX — versione console.

Si mettono a disposizione le seguenti versioni dell'utility di diagnostica remota del Server Dr.Web:

File eseguibile	Posizione	Descrizione
`drweb-cntl-<sistema_operativo>-<numero_di_bit>`	Pannello di controllo, sezione **Amministrazione** → **Utility**	Versione indipendente dell'utility. Può essere avviata da qualsiasi directory e su qualsiasi computer con il sistema operativo corrispondente.
	Directory di Server Dr.Web `webmin/utilities`	
`drwcntl`	Directory di Server Dr.Web `bin`	La versione dell'utility dipende dalla disponibilità delle librerie del server. Può essere avviata solo dalla directory della sua posizione.

Le versioni dell'utility `drweb-cntl-<sistema_operativo>-<numero_di_bit>` e `drwcntl` hanno le funzionalità simili. Di seguito nella sezione viene riportata la versione `drwcntl`, tuttavia, tutti gli esempi sono adatti per entrambe le versioni.

Per connettere l'utility di diagnostica remota del Server Dr.Web, è necessario attivare l'estensione Dr.Web Server FrontDoor. 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 Dr.Web 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 Dr.Web attraverso l'utility di diagnostica remota.

Per connettere l'utility (sia grafica che console) con l'utilizzo di TLS, è necessario impostare direttamente il protocollo quando viene indicato l'indirizzo di Server Dr.Web: `ssl://`*<indirizzo IP o nome DNS>*.

Le impostazioni di Server Dr.Web per la connessione dell'utility di diagnostica remota di Server Dr.Web sono descritte nel **Manuale dell'amministratore**, p. Accesso remoto al Server Dr.Web.

Versione console dell'utility

Formato del comando di avvio:

`drwcntl [-?|-h|--help] [+`*<file_di_log>*`] [`*<server>* `[`*<nome_utente>* `[`*<password>*`]]]`

dove:

- `-? -h --help` — visualizza la guida ai comandi per l'utilizzo dell'utility.
- *<file_di_log>* — scrivi tutte le azioni dell'utility nel file di log sul percorso impostato.
- *<server>* — la stringa di indirizzo del Server Dr.Web, a cui l'utility si connette, nel formato `[(tcp|ssl)://]`*<indirizzo IP o nome DNS>*`[:`*<porta>*`]`.

  Per la possibilità di una connessione attraverso uno dei protocolli supportati, è necessario soddisfare le seguenti condizioni:

  a) Per la connessione attraverso `ssl`, nel file di configurazione `frontdoor.conf` deve essere presente il tag `<ssl />`. In questo caso la connessione sarà possibile solamente attraverso `ssl`.

  b) Per la connessione attraverso `tcp`, nel file di configurazione `frontdoor.conf` deve essere disattivato (commentato) il tag `<ssl />`. In questo caso la connessione sarà possibile solamente attraverso `tcp`.

  Se nella stringa di indirizzo di Server Dr.Web i parametri di connessione non sono impostati, vengono utilizzati i seguenti valori:

Parametro	Valore predefinito
Protocollo di connessione	`tcp` Per la connessione attraverso TCP deve essere deselezionato il flag **Utilizza TLS** nel Pannello di controllo, nella sezione **Amministrazione** → **Accesso remoto al Server Dr.Web**. Ciò disattiva il tag `<ssl />` nel file di configurazione `frontdoor.conf`.
Indirizzo IP o nome DNS del Server Dr.Web	L'utility chiederà di inserire l'indirizzo del Server Dr.Web in formato corrispondente.
Porta	`10101` Sul lato Server Dr.Web la porta consentita viene impostata nella sezione **Accesso remoto al Server Dr.Web** e viene salvata nel file di configurazione `frontdoor.conf`. Se in questa sezione viene utilizzata una porta alternativa, è necessario specificare in modo esplicito questa porta alla connessione dell'utility.

- <*nome_utente*> — il nome utente dell'amministratore del Server Dr.Web.
- <*password*> — la password dell'amministratore per l'accesso al Server Dr.Web.

  Se il nome utente e la password dell'amministratore non sono stati impostati nella stringa di connessione, l'utility richiederà di immettere le relative credenziali.

Comandi ammissibili:

- `cache` <*operazione*> — gestione della cache di file. Per invocare una specifica operazione, utilizzare i seguenti comandi:
  - `clear` — ripulisci la cache di file,
  - `list` — mostra tutti i contenuti della cache di file,
  - `matched` <*espressione regolare*> — mostra i contenuti della cache di file che soddisfano l'espressione regolare impostata,
  - `maxfilesize [`<*dimensione*>`]` — mostra/imposta la dimensione massima degli oggetti di file pre-caricati. Se eseguito senza parametri aggiuntivi, mostra la dimensione corrente. Per impostare una dimensione, specificare la dimensione richiesta in byte dopo il nome del comando.
  - `statistics` — mostra le statistiche sull'utilizzo della cache di file.
- `calculate` <*funzione*> — calcolo di una data sequenza. Per invocare una sequenza specifica, utilizzare i seguenti comandi:
  - `hash [`<*standard*>`] [`<*stringa*>`]` — calcola l'hash di una data stringa. Per impostare uno standard specifico, utilizzare i seguenti comandi:

    - `gost` — calcola l'hash di una data stringa secondo lo standard GOST,
    - `md5` — calcola l'hash MD5 di una data stringa,
    - `sha` — calcola l'hash di una data stringa secondo lo standard SHA,
    - `sha1` — calcola l'hash di una data stringa secondo lo standard SHA1,
    - `sha224` — calcola l'hash di una data stringa secondo lo standard SHA224,
    - `sha256` — calcola l'hash di una data stringa secondo lo standard SHA256,
    - `sha384` — calcola l'hash di una data stringa secondo lo standard SHA384,
    - `sha512` — calcola l'hash di una data stringa secondo lo standard SHA512.
  - `hmac [<*standard*>] [<*stringa*>]` — calcola l'HMAC di una data stringa. Per impostare uno standard specifico, utilizzare i seguenti comandi:
    - `md5` — calcola l'HMAC-MD5 per la stringa impostata,
    - `sha256` — calcola l'HMAC-SHA256 per la stringa impostata.
  - `random` — generazione di un numero casuale,
  - `uuid` — generazione di un identificatore univoco casuale.
- `clients` <*operazione*> — ricezione di informazioni e gestione dei client connessi al Server Dr.Web. Per invocare una funzione specifica, utilizzare i seguenti comandi:
  - `addresses [`<*espressione regolare*>`]` — mostra gli indirizzi di rete delle postazioni che soddisfano l'espressione regolare impostata. Se nessuna espressione regolare è impostata, mostra gli indirizzi di tutte le postazioni.
  - `caddresses [`<*espressione regolare*>`]` — mostra il numero di indirizzi IP delle postazioni che soddisfano l'espressione regolare impostata. Se nessuna espressione regolare è impostata, mostra il numero totale di postazioni.
  - `chosts [`<*espressione regolare*>`]` — mostra il numero di nomi di computer delle postazioni che soddisfano l'espressione regolare impostata. Se nessuna espressione regolare è impostata, mostra il numero totale di postazioni.
  - `cids [`<*espressione regolare*>`]` — mostra il numero di identificatori delle postazioni che soddisfano l'espressione regolare impostata. Se nessuna espressione regolare è impostata, mostra il numero totale di postazioni.
  - `cnames [`<*espressione regolare*>`]` — mostra il numero di nomi delle postazioni che soddisfano l'espressione regolare impostata. Se nessuna espressione regolare è impostata, mostra il numero totale di postazioni.
  - `disconnect [`<*espressione regolare*>`]` — interrompi la connessione corrente attiva con le postazioni di cui gli identificatori soddisfano l'espressione regolare impostata. Se nessuna espressione regolare è impostata, interrompi la connessione con tutte le postazioni connesse.
  - `enable [`<*modalità*>`]` — mostra/imposta la modalità di connessione dei client al Server Dr.Web. Se eseguito senza parametri aggiuntivi, mostra la modalità corrente. Per impostare una modalità, utilizzare i seguenti comandi aggiuntivi:
    - `on` — accetta tutte le connessioni dei client.
    - `off` — nega tutte le connessioni dei client.

- `hosts` <*espressione regolare*> — mostra i nomi di computer di postazioni che soddisfano l'espressione regolare impostata.
- `ids` <*espressione regolare*> — mostra gli identificatori di postazioni che soddisfano l'espressione regolare impostata.
- `names` <*espressione regolare*> — mostra i nomi di postazioni che soddisfano l'espressione regolare impostata.
- `online` <*espressione regolare*> — mostra la durata di connessione delle postazioni di cui l'identificatore, il nome o l'indirizzo soddisfano l'espressione regolare impostata. La durata di connessione viene calcolata dal momento dell'ultima connessione delle postazioni al Server Dr.Web.
- `statistics` <*espressione regolare*> — mostra le statistiche sul numero di client che soddisfano l'espressione regolare impostata.
- `traffic` <*espressione regolare*> — mostra i dati sul traffico dei client attualmente connessi che soddisfano l'espressione regolare impostata.

- `core` — scrivi il dump del processo Server Dr.Web.
- `cpu` <*parametro*> — mostra le statistiche di utilizzo della CPU del computer su cui è installato il Server Dr.Web. Per invocare un parametro specifico, utilizzare i seguenti comandi:
  - `clear` — cancella tutti i dati statistici accumulati,
  - `day` — mostra il grafico di utilizzo della CPU per il giorno corrente,
  - `disable` — disattiva il monitoraggio dell'utilizzo della CPU,
  - `enable` — attiva il monitoraggio dell'utilizzo della CPU,
  - `hour` — mostra il grafico di utilizzo della CPU per l'ora corrente,
  - `load` — mostra il livello medio di utilizzo della CPU,
  - `minute` — mostra il grafico di utilizzo della CPU per il minuto passato,
  - `rawd` — mostra le statistiche numeriche di utilizzo della CPU per il giorno,
  - `rawh` — mostra le statistiche numeriche di utilizzo della CPU per l'ora passata,
  - `rawl` — mostra le statistiche numeriche di utilizzo medio della CPU,
  - `rawm` — mostra le statistiche numeriche di utilizzo della CPU per il minuto passato,
  - `status` — mostra lo stato del monitoraggio delle statistiche di utilizzo della CPU.
- `debug` <*parametro*> — configurazione del debug. Per impostare un parametro specifico, utilizzare i comandi aggiuntivi. Per consultare l'elenco dei comandi aggiuntivi, invocare la guida tramite il comando: `? debug`.

  

  Il comando `debug signal` è disponibile solo per i Server Dr.Web sotto SO della famiglia UNIX.

- `die` — arresta il Server Dr.Web e scrivi il dump del processo Server Dr.Web.

Il comando `die` è disponibile solo per i Server Dr.Web sotto SO della famiglia UNIX.

- `dwcp` <*parametro*> — imposta/mostra le impostazioni di Dr.Web Control Protocol (comprende i log di Server Dr.Web, Agent Dr.Web e installer di Agent Dr.Web). I parametri ammissibili:
  - `compression` <*modalità*> — imposta una delle seguenti modalità di compressione del traffico:
    - `on` — compressione attivata,
    - `off` — compressione disattivata,
    - `possible` — la compressione è possibile.
  - `encryption` <*modalità*> — imposta una delle seguenti modalità di cifratura del traffico:
    - `on` — cifratura attivata,
    - `off` — cifratura disattivata,
    - `possible` — la cifratura è possibile.
  - `show` — visualizza le impostazioni correnti di Dr.Web Control Protocol.
- `io` <*parametro*> — mostra le statistiche di lettura/scrittura dei dati da parte del processo Server Dr.Web. Per invocare un parametro specifico, utilizzare i seguenti comandi:
  - `clear` — cancella tutti i dati statistici accumulati,
  - `disable` — disattiva il monitoraggio delle statistiche,
  - `enable` — attiva il monitoraggio delle statistiche,
  - `rawdr` — mostra le statistiche numeriche di lettura dei dati per il giorno,
  - `rawdw` — mostra le statistiche numeriche di scrittura dei dati per il giorno,
  - `rawh` — mostra le statistiche numeriche per l'ora passata,
  - `rawm` — mostra le statistiche numeriche per il minuto passato,
  - `rday` — mostra il grafico delle statistiche di lettura dei dati per il giorno,
  - `rhour` — mostra il grafico delle statistiche di lettura dei dati per l'ora passata,
  - `rminute` — mostra il grafico delle statistiche di lettura dei dati per il minuto passato,
  - `status` — mostra lo stato del monitoraggio delle statistiche,
  - `wday` — mostra il grafico delle statistiche di scrittura dei dati per il giorno,
  - `whour` — mostra il grafico delle statistiche di scrittura dei dati per l'ora passata,
  - `wminute` — mostra il grafico delle statistiche di scrittura dei dati per il minuto passato.
- `log` <*parametro*> — scrivi una stringa nel file di log di Server Dr.Web o imposta/visualizza il livello di dettaglio del log. A seconda dei parametri impostati, vengono eseguite le seguenti azioni:
  - `log` <*stringa*> — scrivi nel log di Server Dr.Web la stringa impostata con il livello di dettaglio `NOTICE`.

- `log \s [<livello>]` — imposta/visualizza il livello di dettaglio del log. Se viene eseguito con l'opzione `\s` senza indicare il livello, viene visualizzato il livello di dettaglio corrente. I valori ammissibili del livello di dettaglio: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`.

- `lua` <*script*> — esegui lo script LUA impostato.
- `mallopt` <*parametro*> — configura le impostazioni di allocazione della memoria. Per configurare un'impostazione specifica, utilizzare i comandi aggiuntivi. Per consultare l'elenco dei comandi aggiuntivi, invocare la guida tramite il comando: `? mallopt`.

  Il comando `mallopt` è disponibile solo per i Server Dr.Web sotto SO della famiglia Linux.

  Per avere dettagli circa le particolarità dei parametri di questo comando, consultare la descrizione della funzione `mallopt()` dalla libreria `glibc`. Per avere la guida a questa funzione, si può utilizzare, per esempio, il comando `man mallopt`.
- `memory` <*parametro*> — mostra le statistiche di utilizzo della memoria del computer su cui è installato il Server Dr.Web. Per invocare un parametro specifico, utilizzare i seguenti comandi:
  - `all` — visualizza tutte le informazioni e statistiche,
  - `heap` — visualizza informazioni sulla memoria dinamica,
  - `malloc` — visualizza statistiche sull'allocazione della memoria,
  - `sizes` — visualizza statistiche sulle dimensioni della memoria allocata,
  - `system` — visualizza informazioni sulla memoria di sistema.

  Il comando `memory` è disponibile solo per i Server Dr.Web sotto SO Windows, SO della famiglia Linux e SO della famiglia FreeBSD. Si applicano le seguenti limitazioni ai parametri aggiuntivi del comando `memory`:
  - `system` — solo per i Server Dr.Web sotto SO Windows, SO della famiglia Linux,
  - `heap` — solo per i Server Dr.Web sotto SO Windows, SO della famiglia Linux,
  - `malloc` — solo per i Server Dr.Web sotto SO della famiglia Linux e SO della famiglia FreeBSD,
  - `sizes` — solo per i Server Dr.Web sotto SO della famiglia Linux e SO della famiglia FreeBSD.
- `monitoring` <*modalità*> — imposta/visualizza la modalità di monitoraggio dell'utilizzo delle risorse CPU (opzione `cpu` <*parametro*>) e di input/output (opzione `io` <*parametro*>) da parte del processo Server Dr.Web. I comandi ammissibili:
  - `disable` — disattiva il monitoraggio,
  - `enable` — attiva il monitoraggio,
  - `show` — mostra la modalità attuale.
- `printstat` — scrivi le statistiche di funzionamento di Server Dr.Web nel log.
- `reload` — riavvia l'estensione Dr.Web Server FrontDoor.

- `repository` <*parametro*> — gestione del repository. Per invocare una funzione specifica, utilizzare i seguenti comandi:
  - `all` — visualizza l'elenco di tutti i prodotti del repository e il numero totale di file dei prodotti,
  - `clear` — ripulisci i contenuti della cache a prescindere dal valore TTL degli oggetti collocati nella cache,
  - `fill` — colloca tutti i file del repository nella cache,
  - `keep` — conserva sempre tutti i file del repository attualmente presenti nella cache a prescindere dal loro valore TTL,
  - `loaded` — visualizza l'elenco di tutti i prodotti del repository e il numero totale di file per i prodotti attualmente presenti nella cache,
  - `reload` — ricarica il repository da disco,
  - `statistics` — mostra le statistiche degli aggiornamenti del repository.
- `restart` — riavvia il Server Dr.Web.
- `show` <*parametro*> — mostra informazioni sul sistema su cui è installato il Server Dr.Web. Per impostare un parametro specifico, utilizzare i comandi aggiuntivi. Per consultare l'elenco dei comandi aggiuntivi, invocare la guida tramite il comando: `? show`.

  Si applicano le seguenti limitazioni ai parametri aggiuntivi del comando `show`:
  - `memory` — solo per i Server Dr.Web sotto SO Windows, SO della famiglia Linux,
  - `mapping` — solo per i Server Dr.Web sotto SO Windows, SO della famiglia Linux,
  - `limits` — solo per i Server Dr.Web sotto SO della famiglia UNIX,
  - `processors` — solo per i Server Dr.Web sotto SO della famiglia Linux.
- `sql` <*query*> — esegui una data query SQL.
- `stop` — arresta il Server Dr.Web.
- `traffic` <*parametro*> — mostra statistiche sul traffico di rete del Server Dr.Web. Per invocare un parametro specifico, utilizzare i seguenti comandi:
  - `all` — mostra l'intera quantità di traffico dall'inizio del funzionamento di Server Dr.Web.
  - `incremental` — mostra l'incremento del traffico rispetto all'ultima esecuzione del comando `traffic incremental`.
  - `last` — mostra il cambio del traffico dall'ultimo punto fisso.
  - `store` — creazione di un punto fisso per l'opzione `last`.
- `update` <*parametro*> — ottenimento di informazioni e gestione degli aggiornamenti. Per invocare una funzione specifica, utilizzare le seguenti opzioni:
  - `active` — mostra l'elenco degli Agent Dr.Web che attualmente eseguono l'aggiornamento.
  - `agent [`<*modalità*>`]` — mostra/imposta la modalità di aggiornamento degli Agent Dr.Web dal Server Dr.Web. Se eseguito senza parametri aggiuntivi, mostra la modalità corrente. Per impostare una modalità, utilizzare le seguenti opzioni aggiuntive:

        - `on` — attiva gli aggiornamenti degli Agent Dr.Web.
        - `off` — disattiva gli aggiornamenti degli Agent Dr.Web.
    - `gus` — avvia l'aggiornamento del repository da SAM a prescindere dallo stato del processo di aggiornamento da SAM.
    - `http [<modalità>]` — mostra/imposta la modalità di aggiornamento del repository del Server Dr.Web da SAM. Se eseguito senza parametri aggiuntivi, mostra la modalità corrente. Per impostare una modalità, utilizzare le seguenti opzioni aggiuntive:
        - `on` — attiva gli aggiornamenti del repository da SAM.
        - `off` — disattiva gli aggiornamenti del repository da SAM.
    - `inactive` — mostra l'elenco degli Agent Dr.Web che attualmente non eseguono l'aggiornamento.
    - `track [<modalità>]` — mostra/imposta la modalità di monitoraggio degli aggiornamenti degli Agent Dr.Web. Se eseguito senza parametri aggiuntivi, mostra la modalità corrente. Per impostare una modalità, utilizzare i seguenti comandi aggiuntivi:
        - `on` — attiva il monitoraggio degli aggiornamenti degli Agent Dr.Web.
        - `off` — disattiva il monitoraggio degli aggiornamenti degli Agent Dr.Web. In tale caso l'opzione `update active` non visualizzerà l'elenco degli Agent Dr.Web che vengono aggiornati.
- `version` — visualizza informazioni sulla versione dell'utility.

G7.4. Utility di diagnostica remota di Server Dr.Web per l'uso degli script

L'utility di diagnostica remota del Server Dr.Web consente di connettersi al Server Dr.Web su remoto per effettuare la gestione di base e visualizzare le statistiche di funzionamento. A differenza di drwcntl, l'utility `drwcmd` può essere utilizzata per l'uso degli script.

Si mettono a disposizione le seguenti versioni dell'utility console di diagnostica remota di Server Dr.Web per l'uso degli script:

File eseguibile	Posizione	Descrizione
`drweb-cmd-<sistema_operativo>-<numero_di_bit>`	Pannello di controllo, sezione **Amministrazione** → **Utility**	Versione indipendente dell'utility. Può essere avviata da qualsiasi directory e su qualsiasi computer con il sistema operativo corrispondente.
	Directory di Server Dr.Web `webmin/utilities`	
`drwcmd`	Directory di Server Dr.Web `bin`	La versione dell'utility dipende dalla disponibilità delle librerie del server. Può essere avviata solo dalla directory della sua posizione.

Le versioni dell'utility `drweb-cmd-<sistema_operativo>-<numero_di_bit>` e `drwcmd` hanno le funzionalità simili. Di seguito nella sezione viene riportata la versione `drwcmd`, tuttavia, tutti gli esempi sono adatti per entrambe le versioni.

Per connettere l'utility di diagnostica remota del Server Dr.Web, è necessario attivare l'estensione Dr.Web Server FrontDoor. 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 Dr.Web 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 Dr.Web attraverso l'utility di diagnostica remota.

Le impostazioni di Server Dr.Web per la connessione dell'utility di diagnostica remota di Server Dr.Web sono descritte nel **Manuale dell'amministratore**, p. Accesso remoto al Server Dr.Web.

Formato del comando di avvio:

`drwcmd [<opzioni>] [<file>]`

Opzioni valide

Il principio di uso delle opzioni dall'utility `drwcmd` è soggetto alle regole generali descritte nella sezione Allegato G. Parametri della riga di comando per i programmi inclusi in Dr.Web Enterprise Security Suite.

- `--?` — visualizza la guida sulle opzioni.
- `--help` — visualizza la guida sulle opzioni.
- `--commands=<comandi>` — esegui i comandi impostati (sono analoghi ai comandi dell'utility drwcntl). È possibile impostare più comandi separati dal carattere `;`.
- `--debug=yes|no` — registra il log di funzionamento dell'utility in modalità debug (flusso di output standard `stderr`). Di default è `no`.
- `--files=yes|no` — consenti l'esecuzione di comandi (sono analoghi ai comandi dell'utility drwcntl) dai file impostati. Di default è `yes`.

  I comandi in file devono essere impostati un comando per riga. Le righe vuote vengono ignorate. Come inizio di un commento può essere utilizzato il carattere `#`.
- `--keep=yes|no` — mantieni la connessione con il Server Dr.Web dopo l'esecuzione dell'ultimo comando fino al completamento del processo dell'utility. Di default è `no`.
- `--output=<file>` — file per l'output delle risposte del Server Dr.Web. Di default, se nessun file è specificato, viene utilizzato il flusso di output standard `stdout`.

Se il nome del file inizia con il carattere (+), il risultato dell'esecuzione dei comandi verrà aggiunto alla fine del file, altrimenti il file verrà sovrascritto.

- `--password=<password>` — password per l'autenticazione sul Server Dr.Web. Può essere definita nel file specificato nell'opzione `--resource`.
- `--read=yes|no` — consenti la lettura dei parametri di connessione al Server Dr.Web dal file di risorse. Di default è `yes`.
- `--resource=<file>` — file di risorse con i parametri di connessione al Server Dr.Web: l'indirizzo del Server Dr.Web e i dati di registrazione di amministratore per l'autenticazione sul Server Dr.Web. Di default viene utilizzato il file `.drwcmdrc` situato nella seguente directory:
  - In caso di SO della famiglia UNIX: `$HOME`
  - In caso di SO Windows: `%LOCALAPPDATA%`

  Ogni riga nel file deve essere composta da 3 parole separate da spazi: <*Server_Dr.Web*> <*utente*> <*password*>.

  Se è necessario utilizzare lo spazio nel mezzo di una parola, viene impostato come `%S`. Se è necessario utilizzare il simbolo di percentuale, viene impostato come `%P`.

  Per esempio:

```
ssl://127.0.0.1 user1 password1

ssl://127.0.0.1 user2 password2

ssl://127.0.0.1 user pass%Sword
```

  

  Nel caso di utilizzo dell'opzione `--resource` è anche necessario indicare l'opzione `--server`. La connessione viene effettuata al Server Dr.Web indicato nell'opzione `--server` in base ai dati di registrazione dal file di risorse, corrispondenti all'indirizzo di questo Server Dr.Web.

- `--server=<Server_Dr.Web>` — indirizzo del Server Dr.Web. Di default è `ssl://127.0.0.1`. Può essere definito nel file specificato nell'opzione `--resource`.
- `--user=<utente>` — nome utente per l'autenticazione sul Server Dr.Web. Può essere definito nel file specificato nell'opzione `--resource`.
- `--verbose=yes|no` — restituisci una risposta dettagliata del Server Dr.Web (flusso di output standard `stdout`). Di default è `no`.
- `--version` — visualizzare informazioni sulla versione dell'utility.

Procedura per la connessione al Server Dr.Web:

1. Per la determinazione dei dati di connessione al Server Dr.Web i valori di priorità sono quelli specificati nelle opzioni `--server`, `--user` e `--password`.
2. Se l'opzione `--server` non è impostata, viene utilizzato il suo valore di default — `ssl://127.0.0.1`.

3. Se l'opzione `--user` non è impostata, nel file `.drwcmdrc` (può essere ridefinito nell'opzione `--resource`) viene effettuata la ricerca del Server Dr.Web richiesto e viene utilizzato il primo nome utente in ordine alfabetico.
4. Se l'opzione `--password` non è impostata, nel file `.drwcmdrc` (può essere ridefinito nell'opzione `--resource`) viene effettuata una ricerca per Server Dr.Web e nome utente.

   Il nome utente e la password verranno letti dal file `.drwcmdrc` (può essere ridefinito nell'opzione `--resource`), se tale operazione non è vietata dall'opzione `--read`.

5. Se il nome utente e la password non sono impostati dalle opzioni o attraverso il file di risorse, l'utility chiederà di immettere le credenziali tramite la console.

Caratteristiche dell'esecuzione dei comandi:

- Se è impostato un valore vuoto come file con comandi (`-`), vengono letti i comandi immessi tramite la console.
- Se sono impostati allo stesso tempo comandi nell'opzione `--commands` e una lista di file, prima vengono eseguiti i comandi impostati nell'opzione `--commands`.
- Se non sono impostati né i file né i comandi nell'opzione `--commands`, vengono letti i comandi immessi tramite la console.

Per esempio:

Per eseguire i comandi dall'opzione `--command` e quindi i comandi dalla console, immettere come segue:

```
drwcmd --commands=<comandi> -- -
```

Codici di completamento

- 0 — esecuzione riuscita.
- 1 — è stata richiesta la guida sulle opzioni: `--help` o `--?`.
- 2 — errore di analisi della riga di comando: non sono impostati parametri di autenticazione, ecc.
- 3 — errore di creazione del file per l'output della risposta del Server Dr.Web.
- 4 — errore di autenticazione sul Server Dr.Web: nome e/o password dell'amministratore non validi.
- 5 — caduta inaspettata della connessione con il Server Dr.Web.
- 127 — errore fatale non definito.

G7.5. Loader di repository Dr.Web

La descrizione della versione grafica dell'utility Loader di repository è riportata in **Manuale amministratore**, la sezione Utility grafica.

Si mettono a disposizione le seguenti versioni dell'utility console Loader di repository Dr.Web:

File eseguibile	Posizione	Descrizione
`drweb-reploader-<sistema_operativo>-<numero_di_bit>`	Pannello di controllo, sezione **Amministrazione** → **Utility**	Versione indipendente dell'utility. Può essere avviata da qualsiasi directory e su qualsiasi computer con il sistema operativo corrispondente.
	Directory di Server Dr.Web `webmin/utilities`	
`drwreploader`	Directory di Server Dr.Web `bin`	La versione dell'utility dipende dalla disponibilità delle librerie del server. Può essere avviata solo dalla directory della sua posizione.

Le versioni dell'utility `drweb-reploader-<sistema_operativo>-<numero_di_bit>` e `drwreploader` hanno le funzionalità simili. Di seguito nella sezione viene riportata la versione `drwreploader`, tuttavia, tutti gli esempi sono adatti per entrambe le versioni.

Per semplificare l'impostazione delle opzioni per l'esecuzione dell'utility console, è possibile utilizzare il file di configurazione del Loader di repository. Nel file di configurazione predefinito i valori delle opzioni corrispondono ai valori di default riportati di seguito, ad eccezione dell'opzione `--ssh-auth`: per essa nel file di configurazione il valore viene sostituito con `pubkey`.

Opzioni valide

- `--archive` — comprimi il repository in archivio. Di default: `no`.
- `--auth` <*argomento*> — credenziali per l'autenticazione sul server di aggiornamento in formato <*utente*>`[:`<*password*>`]`.
- `--cert-file` <*percorso*> — percorso dell'archivio dei certificati radice per l'autenticazione SSL.
- `--cert-mode [`<*argomento*>`]` — tipo di certificati SSL da accettare automaticamente. Questa impostazione si usa solo per i protocolli sicuri che supportano la crittografia.

  <*argomento*> può essere uno dei valori:

  - `any` — accetta qualsiasi certificato,
  - `valid` — accetta solo i certificati verificati,
  - `drweb` — accetta solo i certificati Dr.Web,

  - `custom` — accetta i certificati personalizzati.

  Di default, viene utilizzato il valore `drweb`.
- `--config` <*percorso*> — percorso del file di configurazione del Loader di repository.
- `--cwd` <*percorso*> — percorso della directory di lavoro corrente.
- `--ipc` — attiva la trasmissione dei dati sul processo di operazione dell'utility nel flusso di output standard. Di default: `no`.
- `--help` — visualizza la guida sulle opzioni.
- `--license-key` <*percorso*> — percorso del file della chiave di licenza (deve essere specificata la chiave o il suo MD5).
- `--log` <*percorso*> — percorso del file di log della procedura di caricamento del repository.
- `--mode` <*modalità*> — modalità di download degli aggiornamenti:
  - `repo` — il repository viene scaricato nel formato repository di Server Dr.Web. I file scaricati possono essere importati direttamente attraverso il Pannello di controllo come aggiornamento del repository di Server Dr.Web. Viene usato di default.
  - `mirror` — il repository viene scaricato nel formato zona di aggiornamento SAM. I file scaricati possono essere collocati su un mirror di aggiornamento nella rete locale. In seguito i Server Dr.Web possono essere configurati per ricevere gli aggiornamenti direttamente da questo mirror di aggiornamento che contiene l'ultima versione del repository, invece di ricevere gli aggiornamenti dai server SAM.
- `--only-bases` — scarica solo i database dei virus. Di default: `no`.
- `--path` <*argomento*> — scarica il repository da SAM nella directory specificata nel parametro <*argomento*>. Alla compressione del repository in archivio tramite l'opzione `--archive`, è possibile indicare il percorso sia fino al nome della directory che fino al nome del file di archivio. Se il nome di archivio non è specificato, verrà attribuito un nome di default — `repository.zip`.
- `--product` <*argomento*> — il prodotto che viene aggiornato. Di default, viene scaricato l'intero repository.
- `--prohibit-cdn` — proibisci l'utilizzo della CDN per il caricamento degli aggiornamenti. Di default: `no`, cioè l'utilizzo della CDN è consentito.
- `--proto` <*protocollo*> — protocollo di download degli aggiornamenti: `file | ftp | ftps | http | https | scp | sftp | smb | smbs`. Di default: `https`.
- `--proxy-auth` <*argomento*> — informazioni per l'autenticazione sul server proxy: nome utente e password nel formato <*utente*>`[:`<*password*>`]`.
- `--proxy-host` <*argomento*> — indirizzo del server proxy nel formato <*server*>`[:`<*porta*>`]`. La porta di default: `3128`.
- `--rotate` <*N*><*f*>`,`<*M*><*u*> — modalità di rotazione del log di funzionamento di Loader di repository. È simile all'impostazione di rotazione del log di Server Dr.Web.

  Di default `10,10m` che significa "conserva 10 file da 10 megabyte, utilizza compressione".
- `--servers` <*argomento*> — gli indirizzi dei server SAM. È consigliabile lasciare il valore predefinito: `esuite.geo.drweb.com`.

- `--show-products` — mostra l'elenco dei prodotti in SAM. Di default: `no`.
- `--ssh-auth` <*tipo*> — tipo di autenticazione sul server di aggiornamento nel caso di connessione via SCP/SFTP. Come parametro <*tipo*> è ammissibile uno dei seguenti valori:
  - `pwd` — autenticazione tramite la password. La password viene impostata nell'opzione `--auth`.
  - `pubkey` — autenticazione tramite la chiave pubblica. In questo caso è necessario impostare la chiave privata attraverso `--ssh-prikey` per estrarre la relativa chiave pubblica.
- `--ssh-prikey` <*percorso*> — percorso della chiave privata SSH.
- `--ssh-pubkey` <*percorso*> — percorso della chiave pubblica SSH.
- `--strict` — interrompi il caricamento se si verifica un errore. Di default: `no`.
- `--update-key` <*percorso*> — percorso della chiave pubblica o della directory con la chiave pubblica per la verifica della firma degli aggiornamenti che vengono scaricati da SAM. Le chiavi pubbliche per la verifica dell'autenticità degli aggiornamenti `update-key-*.upub` sono ritrovabili sul Server Dr.Web nella directory `etc`.
- `--update-url` <*argomento*> — directory sui server SAM che contiene gli aggiornamenti dei prodotti Dr.Web. È consigliabile lasciare il valore predefinito — `/update`.
- `--V` — visualizza informazioni sulla versione dell'utility.
- `--verbosity` <*livello_di_dettaglio*> — livello di dettaglio del log. Di default, è `TRACE3`. I valori ammissibili sono: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. I valori `ALL` e `DEBUG3` sono sinonimi.
- `--version` <*versione*> — versione del Server Dr.Web per cui è necessario scaricare aggiornamenti nel formato <*versione_principale*>`.`<*versione_secondaria*>. Per esempio, nel caso di Server Dr.Web versione 13, il parametro <*versione*> assume il valore `13.00`. La lista dei prodotti per cui sono disponibili aggiornamenti può variare a seconda della versione di Server Dr.Web. La lista dei prodotti disponibili può essere consultata, per esempio, controllando la descrizione del parametro `<products>` per il file di configurazione di Loader di repository nel manuale per la versione in questione.

Caratteristiche dell'utilizzo delle opzioni

All'avvio dell'utility Loader di repository prestare attenzione alle seguenti regole:

Le opzioni devono essere obbligatoriamente configurate	A condizione
`--license-key`	Sempre
`--update-key`	
`--path`	
`--cert-file`	Se le seguenti opzioni assumono uno dei valori: • `--cert-mode valid | drweb | custom`, • `--proto https | ftps | smbs`.
`--ssh-prikey`	Se le seguenti opzioni assumono uno dei valori: • `--proto sftp | scp`, • `--ssh-auth pubkey`.

Esempi di utilizzo

1. Crea un archivio da importare con tutti i prodotti:

```
drwreploader.exe --path C:\Temp --archive --license-key C:\agent.key --
update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program
Files\DrWeb Server\etc"
```

2. Crea un archivio da importare con i database dei virus:

```
drwreploader.exe --path C:\Temp --archive --license-key "C:\agent.key" --
update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program
Files\DrWeb Server\etc" -only-bases
```

3. Crea un archivio da importare solo con il Server Dr.Web:

```
drwreploader.exe --path C:\Temp --archive --license-key "C:\agent.key" --
update-key "C:\Program Files\DrWeb Server\etc" --cert-file "C:\Program
Files\DrWeb Server\etc" --product=20-drwcs
```

G7.6. Utility per l'installazione remota di Agent Dr.Web per UNIX

L'utility per l'installazione remota di Agent Dr.Web per UNIX consente di installare Agent Dr.Web in remoto su postazioni protette della rete antivirus che sono gestiti dai sistemi operativi della famiglia UNIX. Se necessario, tramite questa utility può anche essere installato Dr.Web per file server UNIX.

L'utility funziona in modalità riga di comando ed è disponibile nelle seguenti versioni:

File eseguibile	Posizione	Descrizione
`drweb-unix-install-<sistema_operativo>-<numero_di_bit>`	Pannello di controllo, sezione **Amministrazione** → **Utility**	Versione indipendente dell'utility. Può essere avviata da qualsiasi directory e su qualsiasi computer con il sistema operativo corrispondente. Viene aggiornata con l'aggiornamento del repository o Server Dr.Web.
	Directory di Server Dr.Web `webmin/utilities`	
`drwunixinstall`	Directory di Server Dr.Web `bin`	La versione dell'utility dipende dalla disponibilità delle librerie del server. Può essere avviata solo dalla directory della sua posizione. Viene aggiornata solo con l'aggiornamento del Server Dr.Web.

Le versioni dell'utility `drweb-unix-install-<sistema_operativo>-<numero_di_bit>` e `drwunixinstall` hanno funzionalità identiche. Di seguito nella sezione viene riportata la versione `drwunixinstall`, però il formato e le opzioni ammissibili sono adatti per entrambe le versioni.

Formato del comando di avvio:

`drwunixinstall [<opzioni>] <indirizzo_IP_postazione_1>[:<porta_SSH>[^<nome_utente>[^<password>]]] <indirizzo_IP_postazione_2>[:<porta_SSH>[^<nome_utente>[^<password>]]] ...`

Opzioni valide

Il principio di uso delle opzioni da parte dell'utility `drwunixinstall` è soggetto alle regole generali descritte nella sezione Allegato G. Parametri della riga di comando per i programmi inclusi in Dr.Web Enterprise Security Suite.

- `--help` — visualizza la guida sulle opzioni.
- `--ak <parametri_autenticazione>` — imposta i parametri di autenticazione alternativa su postazioni remote con l'uso delle chiavi di cifratura nel seguente formato:

  `<nome_utente>^<percorso_chiave_privata_Server_Dr.Web>^<percorso_chiave_pubblica_Server_Dr.Web>[^<password_chiave_privata>]`

Se formando il comando, impostare contemporaneamente i parametri di autenticazione standard attraverso la coppia `<nome_utente>^<password>` e di autenticazione alternativa

attraverso le chiavi di cifratura, i parametri con le chiavi verranno utilizzati per primi all'avvio dell'utility.

- `--ap` <*nome_utente*>^<*password*> — utilizza la modalità di autenticazione su postazioni remote con l'inserimento password molteplice (keyboard-interactive).
- `--certificate` <*percorso*> — imposta il percorso del file del certificato Server Dr.Web. Di default è `webmin/install/unix/workstation/drwcsd-certificate.pem`.
- `--cpus` <*numero*> — imposta il numero di core del processore utilizzati per l'installazione remota. Di default è `4`.
- `--ctimeout` <*tempo*> — imposta il tempo massimo di attesa del completamento del processo di trasmissione dei pacchetti di installazione sulle postazioni remote. Viene impostata in secondi, di default è `600`.
- `--debug` — registra il log di funzionamento dell'utility in modalità debug. Di default è `no`.
- `--esuite` <*indirizzo_server*> — inserisci l'indirizzo del Server Dr.Web da cui verrà eseguita l'installazione remota e a cui si connetterà l'Agent Dr.Web al termine dell'installazione. Formato: `[udp://]`<*indirizzo_IP o nome_DNS*>`[:`<*porta*>`]`
- `--etimeout` <*tempo*> — imposta il tempo massimo di attesa del completamento dell'installazione dei pacchetti sulle postazioni remote. Viene impostata in secondi, di default è `900`.
- `--from` <*percorso*> — imposta il percorso della directory con i pacchetti di installazione sul Server Dr.Web. Di default è `webmin/install/unix`.
- `--long` — registra il log di funzionamento dell'utility con l'indicazione di timestamp. Di default è `no`.
- `--pwd` <*password*> — password per l'autenticazione sulle postazioni remote per l'utilizzo del comando `su` e/o `sudo`.
- `--remote-temp` <*percorso*> — imposta il percorso della directory sulle postazioni remote per la conservazione temporanea del pacchetto e del certificato di Server Dr.Web. Di default viene utilizzata la directory definita nel sistema.
- `--server` — installa il prodotto Dr.Web per file server UNIX invece di Agent Dr.Web. Di default è `no`.
- `--simultaneously` <*numero*> — imposta il numero massimo di postazioni su cui Agent Dr.Web verrà installato contemporaneamente.
- `--sshdebug` — registra il log di funzionamento dell'utility in modalità debug con l'indicazione dei dettagli di tutte le operazioni che utilizzano il protocollo SSH. Di default è `no`.
- `--sshwaitdebug` — registra il log di funzionamento dell'utility in modalità debug con l'indicazione dei dettagli di tutte le operazioni che utilizzano il protocollo SSH, nonché delle operazioni di timer. Di default è `no`.
- `--stimeout` <*tempo*> — imposta il tempo massimo di attesa dell'inserimento della password per l'utilizzo del comando `su` e/o `sudo` sulle postazioni remote. Viene impostata in secondi, di default è `10`.

- `--su` — utilizza il comando `su` durante l'installazione per elevare i permessi al livello di superutente sulle postazioni remote. Di default è `no`.
- `--sudo` — utilizza il comando `sudo` durante l'installazione per elevare i permessi al livello di superutente sulle postazioni remote. Di default è `no`.
- `--temp` <*percorso*> — imposta il percorso della directory sul Server Dr.Web per la conservazione temporanea del certificato. Di default viene utilizzata la directory definita nel sistema.
- `--timeout` <*tempo*> — imposta il tempo massimo di attesa del stabilimento della connessione e dell'autenticazione sulle postazioni remote. Viene impostata in secondi, di default è `30`.
- `--verbosity` <*livello*> — imposta il livello di dettaglio del log di funzionamento dell'utility. Di default è `info`. I valori ammissibili sono: `all`, `debug3`, `debug2`, `debug1`, `debug`, `trace3`, `trace2`, `trace1`, `trace`, `info`, `notice`, `warning`, `error`, `crit`. I valori `all` e `debug3` sono sinonimi.
- `--version` — visualizzare informazioni sulla versione dell'utility.

G7.7. Utility per l'installazione remota di Agent Dr.Web per Windows

L'utility per l'installazione remota di Agent Dr.Web per Windows consente di installare Agent Dr.Web in remoto su postazioni protette della rete antivirus che sono gestiti dal sistema operativo Windows.

L'utility funziona in modalità riga di comando ed è disponibile nelle seguenti versioni:

File eseguibile	Posizione	Descrizione
`drweb-windows-install-`<*sistema_operativo*>`-`<*numero_di_bit*>	Pannello di controllo, sezione **Amministrazione** → **Utility**	Versione indipendente dell'utility. Può essere avviata da qualsiasi directory e su qualsiasi computer con il sistema operativo corrispondente. Viene aggiornata con l'aggiornamento del repository o Server Dr.Web.
	Directory di Server Dr.Web `webmin/utilities`	
`drwwindowsinstall`	Directory di Server Dr.Web `bin`	La versione dell'utility dipende dalla disponibilità delle librerie del server. Può essere avviata solo dalla directory della sua posizione. Viene aggiornata solo con l'aggiornamento del Server Dr.Web.

Le versioni dell'utility `drweb-windows-install-`<*sistema_operativo*>`-`<*numero_di_bit*> e `drwwindowsinstall` hanno funzionalità identiche. Di seguito nella sezione viene riportata la versione `drwwindowsinstall`, però il formato e le opzioni ammissibili sono adatti per entrambe le versioni.

Formato del comando di avvio:

`drwwindowsinstall <opzioni>`

Opzioni valide

Il principio di uso delle opzioni da parte dell'utility `drwwindowsinstall` è soggetto alle regole generali descritte nella sezione Allegato G. Parametri della riga di comando per i programmi inclusi in Dr.Web Enterprise Security Suite.

- `--help` — visualizza la guida sulle opzioni.
- `--console=yes|no` — visualizzata il log di funzionamento dell'utility nella console. Di default è `no`.
- `--disable-v1=yes|no` — disattiva il protocollo SMB versione 1 (SMBv1) per il tempo del funzionamento dell'utility. Di default è `no`.
- `--distribution <nome_file>` — imposta manualmente il nome del file dell'installer di Agent Dr.Web che verrà avviato sulle postazioni remote. Di default è `drwinst.exe`.
- `--install-address <indirizzo_IP_postazione>` — inserisci l'indirizzo della postazione remota su cui verrà installato l'Agent Dr.Web. All'indicazione contemporanea di più postazioni, gli indirizzi devono essere separati da virgola (`,`) o punto e virgola (`;`) senza spazi.
- `--install-certificate <percorso>` — imposta il percorso del file del certificato Server Dr.Web.
- `--install-clients <numero>` — imposta il numero massimo di postazioni su cui l'Agent Dr.Web verrà installato contemporaneamente. Di default è `8`.
- `--install-compression <modalità>` — imposta la modalità di compressione traffico per la comunicazione del Server Dr.Web con le postazioni remote: `on` — compressione attivata, `off` — compressione disattivata, `possible` — compressione possibile. Quest'ultimo valore significa che la modalità dipende dalle impostazioni specificate sul Server Dr.Web. Di default è `possible`.
- `--install-encryption <modalità>` — imposta la modalità di cifratura traffico per la comunicazione del Server Dr.Web con le postazioni remote: `on` — cifratura attivata, `off` — cifratura disattivata, `possible` — cifratura possibile. Quest'ultimo valore significa che la modalità dipende dalle impostazioni specificate sul Server Dr.Web. Di default è `possible`.
- `--install-language <codice_lingua>` — imposta la lingua dell'interfaccia Agent Dr.Web come codice di due lettere secondo lo standard ISO 639-1. Se l'opzione non è impostata, o Agent Dr.Web non è disponibile nella lingua impostata, viene utilizzata la lingua di sistema sulla postazione remota.
- `--install-path <percorso>` — imposta il percorso della directory di installazione di Agent Dr.Web sulle postazioni remote. Di default è `%ProgramFiles%\DrWeb`.
- `--install-register=yes|no` — registra l'Agent Dr.Web nella lista dei programmi installati al termine dell'installazione. Di default è `no`.

- `--install-server` <*indirizzo_server*> — inserisci l'indirizzo del Server Dr.Web da cui verrà eseguita l'installazione remota e a cui si connetterà l'Agent al termine dell'installazione. Formato: `[udp://]`<*indirizzo_IP_o_nome_DNS*>`[:`<*porta*>`]`.
- `--install-timeout` <*tempo*> — imposta il tempo massimo di attesa del completamento dell'installazione dell'Agent Dr.Web sulle postazioni remote. Viene impostata in secondi, di default è `300`.
- `--install-user` <*nome_utente*>`@`<*dominio*>`:`<*password*> o <*dominio*>`\`<*nome_utente*>`:`<*password*> — imposta il nome utente e la password per l'autenticazione sulle postazioni remote.
- `--log` <*percorso*> — imposta il percorso del file del log di funzionamento dell'utility. Di default è `drwsmb.log` nella sottodirectory `var` della directory di installazione del Server Dr.Web.
- `--machine` <*nome*> — imposta il nome che verrà assegnato alla postazione remota nella rete antivirus Dr.Web Enterprise Security Suite al termine dell'installazione dell'Agent Dr.Web e della sua connessione al Server Dr.Web. Di default viene utilizzato il nome computer registrato nel sistema operativo.
- `--rotate=`<*N*><*f*>`,`<*M*><*u*> — imposta la modalità di rotazione del log di funzionamento dell'utility. Il formato è identico a quello della opzione analoga che viene utilizzata per gestire la rotazione del log di Server Dr.Web. Di default è `10,10m`.
- `--service-id` <*nome_nel_registro*> — imposta il nome che verrà assegnato alla sezione del servizio di installazione remota di Agent Dr.Web nel registro di Windows. Di default è `DrWebRsvcRunner`.
- `--service-name` <*nome_visualizzato*> — imposta il nome del servizio di installazione remota di Agent Dr.Web, visualizzato nello snap-in Services. Di default è `Dr.Web Remote Runner Service`.
- `--target-root` <*nome_directory*> — imposta il nome della directory nella risorsa di amministrazione condivisa sulla postazione remota da cui verrà avviato l'installer di Agent Dr.Web, copiato dal Server Dr.Web. Di default è `TEMP`.
- `--target-volume` <*nome_risorsa*> — imposta il nome della risorsa di amministrazione condivisa in cui verranno collocati i file di installazione di Agent Dr.Web. Di default è `ADMIN$`.
- `--threads` <*numero*> — impostare il numero di thread di input/output nel pool. Di default è `2`.
- `--verbosity` <*livello*> — imposta il livello di dettaglio del log di funzionamento dell'utility. Di default è `trace`. I valori ammissibili sono: `all, debug3, debug2, debug1, debug, trace3, trace2, trace1, trace, info, notice, warning, error, crit`. I valori `all` e `debug3` sono sinonimi.
- `--version` — visualizzare informazioni sulla versione dell'utility.

Allegato H. Variabili di ambiente esportate da Server Dr.Web

Per semplificare la configurazione dei processi avviati da parte del Server Dr.Web secondo il calendario, sono richieste informazioni sulla posizione delle directory di Server Dr.Web. A questo scopo il Server Dr.Web esporta nell'ambiente dei processi da avviare le seguenti variabili:

- `DRWCSD_HOME` — percorso della directory radice (directory di installazione). È il valore dell'opzione `-home`, se è stata impostata per l'avvio del Server Dr.Web, altrimenti è la directory corrente all'avvio.
- `DRWCSD_BIN` — percorso della directory dei file eseguibili. È il valore dell'opzione `-bin-root`, se è stata impostata per l'avvio del Server Dr.Web, altrimenti è la sottodirectory `bin` della directory radice.
- `DRWCSD_VAR` — percorso della directory in cui il Server Dr.Web ha il permesso di scrittura e che è progettata per la memorizzazione dei file modificabili (per esempio, i log, nonché i file di repository). È il valore dell'opzione `-var-root`, se è stata impostata per l'avvio del Server Dr.Web, altrimenti è la sottodirectory `var` della directory radice.

Allegato I. Utilizzo delle espressioni regolari in Dr.Web Enterprise Security Suite

Alcuni parametri di Dr.Web Enterprise Security Suite possono essere impostati nel formato delle espressioni regolari dei seguenti tipi:

- Le espressioni regolari del linguaggio Lua.

  Vengono utilizzate per configurare l'appartenenza automatica delle postazioni della rete antivirus ai gruppi custom.

  La descrizione dettagliata della sintassi delle espressioni regolari del linguaggio Lua è disponibile sul sito http://www.lua.org/manual/5.1/manual.html#5.4.1.
- Le espressioni regolari della libreria software PCRE.

  La descrizione dettagliata della sintassi della libreria PCRE è disponibile sul sito http://www.pcre.org/.

  In questo allegato è riportata solo una breve descrizione dei punti principali di utilizzo delle espressioni regolari della libreria PCRE.

I1. Opzioni delle espressioni regolari PCRE

Le espressioni regolari vengono utilizzate sia nel file di configurazione di Server Dr.Web che nel Pannello di controllo per indicare gli oggetti da escludere dalla scansione nelle impostazioni di Scanner Dr.Web.

Le espressioni regolari si scrivono nella seguente forma:

```
qr{EXP}options
```

dove `EXP` è l'espressione stessa, `options` è una sequenza di opzioni (stringa di lettere), `qr{}` è metacaratteri letterali. In generale, la struttura si presenta così, come esempio:

`qr{pagefile\.sys}i` — file di swap di SO Windows NT

Di seguito vengono descritte le opzioni e le espressioni regolari stesse. Per una descrizione più dettagliata consultare http://www.pcre.org/pcre.txt.

- Opzione `'a'` che corrisponde a `PCRE_ANCHORED`

  Con questa impostazione, il pattern ha forzatamente un "ancoraggio", cioè si limita a confrontare solo la prima posizione da cercare nella stringa in base a cui si esegue la ricerca ("stringa di oggetto"). Ciò può anche essere raggiunto tramite strutture appropriate del pattern stesso.
- Opzione `'i'` che corrisponde a `PCRE_CASELESS`

  Con questa impostazione le lettere del pattern vengono confrontate sia con le maiuscole che con le minuscole. Questa possibilità può essere modificata nel pattern tramite l'opzione `(?i)`.

- Opzione `'x'` che corrisponde a `PCRE_EXTENDED`

  Con questa impostazione vengono ignorati gli spazi tra caratteri nel pattern, ad eccezione dei casi in cui essi sono preceduti da caratteri di controllo oppure si trovano dentro una classe di caratteri. Lo spazio non include il carattere `VT` (codice 11). Inoltre, vengono ignorati i caratteri che si trovano al di fuori di una classe di caratteri tra il carattere `#`, non preceduto da un carattere di controllo, e il segno di nuova riga, inclusivo. Questa opzione può essere modificata nel pattern tramite l'opzione `(?x)`. Questa impostazione consente di includere commenti all'interno di pattern composti. Tenere presente che questo è applicabile solo ai caratteri di dati. I caratteri di spazio non possono stare nel pattern all'interno delle sequenze di caratteri speciali, per esempio, all'interno della sequenza `(?(` la quale introduce un subpattern condizionale.

- Opzione `'m'` che corrisponde a `PCRE_MULTILINE`

  Di default, PCRE considera che la stringa di oggetto sia composta da una singola riga di caratteri (anche se in realtà essa contiene caratteri di nuova riga). Il metacarattere "*inizio riga*" `"^"` viene confrontato solo all'inizio della stringa, mentre il metacarattere "*fine riga*" `"$"` viene confrontato solo alla fine della stringa oppure prima della nuova riga finale (se non è impostata l'opzione `PCRE_DOLLAR_ENDONLY`).

  Se è impostata l'opzione `PCRE_MULTILINE`, i metacaratteri "*inizio riga*" e "*fine riga*" si attaccano a qualsiasi carattere di nuova riga che viene direttamente prima o dopo di essi nella stringa di oggetto e anche all'inizio e alla fine della stringa. Questa opzione può essere modificata nel pattern tramite l'opzione `(?m)`. Se il testo non contiene i caratteri `"\n"` o se il pattern non contiene `^` o `$`, l'opzione `PCRE_MULTILINE` non ha senso.

- Opzione `'u'` che corrisponde a `PCRE_UNGREEDY`

  Questa opzione annulla "l'avidità" dei quantificatori e così essi diventano "non avidi" di default, ma ripristinano "l'avidità" se sono seguiti da `"?"`. Questa possibilità può anche essere configurata tramite l'opzione `(?U)` nel pattern.

- Opzione `'d'` che corrisponde a `PCRE_DOTALL`

  Con questa impostazione il metacarattere di punto nel pattern viene confrontato con tutti i caratteri, compreso il carattere di nuova riga. Senza di esso i caratteri di nuova riga vengono esclusi. Questa opzione può essere modificata nel pattern tramite la nuova opzione `(?s)`. Una classe negativa, per esempio `[^a]`, viene sempre confrontata con il carattere di nuova riga, a prescindere dalle impostazioni di questa opzione.

- Opzione `'e'` che corrisponde a `PCRE_DOLLAR_ENDONLY`

  Con questa impostazione il segno di dollaro nel pattern viene confrontato solo alla fine della stringa di oggetto. Senza questa opzione il segno di dollaro viene confrontato anche nella posizione direttamente prima del carattere di nuova riga alla fine della stringa (ma non davanti a qualsiasi altro carattere di nuova riga). L'opzione `PCRE_DOLLAR_ENDONLY` viene ignorata se è impostata l'opzione `PCRE_MULTILINE`.

I2. Caratteristiche delle espressioni regolari PCRE

Espressione regolare — un modello che viene confrontato con un testo da sinistra a destra. La maggior parte dei caratteri nel modello significa se stessa e viene applicata ai caratteri corrispondenti nel testo.

Il vantaggio principale delle espressioni regolari sta nella possibilità di includere nel modello varianti e ripetizioni. Vengono codificate attraverso metacaratteri che non significano sé stessi ma, invece, vengono interpretati in un modo particolare.

Esistono due set di metacaratteri diversi: quelli che si utilizzano fra parentesi quadre e quelli che si utilizzano fuori parentesi quadre. Li vediamo in dettagli. Fuori parentesi quadre si utilizzano i seguenti metacaratteri:

Carattere	Valore
\	carattere di controllo standard (escape) che permette diverse varianti di applicazione
^	dichiara l'inizio di linea (o di testo in modalità con diverse linee)
$	dichiara la fine di linea (o di testo in modalità con diverse linee)
.	corrisponde a qualsiasi carattere, ad eccezione del segno da capo (di default)
[	inizio di descrizione di classe dei caratteri
]	fine di descrizione di classe dei caratteri
|	inizio di un ramo alternativo
(	inizio di un subpattern
)	fine di subpattern
?	estende il valore (inoltre quantificatore 0 o 1 inoltre quantificatore di minimizzazione
*	0 o più
+	1 o più anche "quantificatore possessivo"
{	inizio di quantificatore minimale/massimale

La parte di modello tra parentesi quadre si chiama "classe di caratteri". In classe di caratteri, i metacaratteri sono:

Carattere	Valore
\	carattere di controllo standard (escape)
^	nega la classe, ma solamente se all'inizio della classe
-	definisce un intervallo di caratteri
[	classe dei caratteri POSIX (solo se seguito da sintassi POSIX)
]	chiude la classe dei caratteri

Allegato J. Formato dei file di log

I file di log del Server Dr.Web (v. **Manuale dell'amministratore**, p. Log di Server Dr.Web) e dell'Agent Dr.Web sono in formato di testo, dove ogni riga rappresenta un avviso separato.

Il formato della riga di avviso è il seguente:

<anno><mese><giorno>.<ora><minuto><secondo>.<centesimi_del_secondo> *<tipo_avviso>* `[`*<id_processo>*`]` *<nome_flusso>* `[`*<fonte_avviso>*`]` *<avviso>*

dove:

- *<anno><mese><giorno>.<ora><minuto><secondo>.<centesimi_del_secondo>* — data precisa di scrittura dell'avviso nel file di log.
- *<tipo_avviso>* — livello di registrazione delle informazioni nel log:
  - **ftl** (fatal error — errore fatale) — avvisi di errori critici di funzionamento;
  - **err** (error — errore) — avvisi di errori di funzionamento;
  - **wrn** (warning — avviso) — avvertimenti di errori;
  - **ntc** (notice — commento) — avvisi informativi importanti;
  - **inf** (info — informazione) — avvisi informativi;
  - **tr0..3** (trace0..3 — tracciamento) — tracciamento di eventi con i vari livelli di dettaglio (**Tracciamento3** — livello di dettaglio massimo);
  - **db0..3** (debug0..3 — debug) — avvisi di debug con i vari livelli di dettaglio (**Debug3** — livello di dettaglio massimo).

  Gli avvisi con il livello di logging **tr0..3** (tracciamento) e **db0..3** (debugging) vengono registrati solamente per gli sviluppatori del software Dr.Web Enterprise Security Suite.

- `[`*<id_processo>*`]` — l'identificatore numerico univoco del processo, nel quadro del quale si eseguiva il flusso che ha scritto l'avviso nel file di log. In alcuni SO `[`*<id_processo>*`]` può essere rappresentato come `[`*<id_processo>* *<id_flusso>*`]`.
- *<nome_flusso>* — indicazione in caratteri del flusso, nel quadro del quale l'avviso è stato scritto nel file di log.
- `[`*<fonte_avviso>*`]` — indicazione del sistema che ha avviato la scrittura dell'avviso nel file di log. La fonte non è sempre presente.
- *<avviso>* — descrizione di testo delle azioni secondo il livello di log. Può comprendere sia una descrizione formale dell'avviso, che i valori di alcune variabili, importanti per tale caso concreto.

Per esempio:

1. `20081023.171700.74 inf [001316] mth:12 [Sch] Job "Purge unsent IS events" said OK`

   dove:

- `20081023` — <*anno*><*mese*><*giorno*>,
- `171700` — <*ora*><*minuto*><*secondo*>,
- `74` — <*centesimi_del_secondo*>,
- `inf` — <*tipo_di_avviso*> — avviso informativo,
- `[001316]` — [<*id_processo*>],
- `mth:12` — <*nome_flusso*>,
- `[Sch]` — [<*fonte_avviso*>] — scheduler,
- `Job "Purge unsent IS events" said OK` — avviso di corretta esecuzione del task **Pulizia degli eventi non inviati**.

2. `20081028.135755.61 inf [001556] srv:0 tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193`

   dove:

   - `20081028` — <*anno*><*mese*><*giorno*>,
   - `135755` — <*ora*><*minuto*><*secondo*>,
   - `61` — <*centesimi_del_secondo*>,
   - `inf` — <*tipo_di_avviso*> — avviso informativo,
   - `[001556]` — [<*id_processo*>],
   - `srv:0` — <*nome_flusso*>,
   - `tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193` — avviso di stabilimento di una nuova connessione via il socket indicato.

Allegato K. Integrazione di Web API e di Dr.Web Enterprise Security Suite

La descrizione di **Web API** viene riportata nel manuale **Web API per Dr.Web Enterprise Security Suite**.

Uso

Con l'integrazione di **Web API** e di Dr.Web Enterprise Security Suite vengono fornite le funzioni per gestire account e per automatizzare l'amministrazione degli utenti del servizio. Si può utilizzarla, per esempio, quando si creano pagine dinamiche per ottenere una richiesta dell'utente e per concedergli un file d'installazione.

Autenticazione

Per la comunicazione con il Server Dr.Web, viene utilizzato il protocollo HTTP(S). **Web API** accetta richieste REST e restituisce XML. Per l'accesso a Web API, si usa l'autenticazione Basic HTTP (secondo lo standard RFC 2617). Se lo standard RFC 2617 non viene osservato, il server HTTP(S) non richiede le credenziali del client (nome utente e password dell'amministratore di Dr.Web Enterprise Security Suite).

Allegato L. Licenze

Questa sezione elenca le librerie di programma di terze parti che vengono utilizzate dal software Dr.Web Enterprise Security Suite, le informazioni sulle loro licenze e gli indirizzi dei rispettivi progetti di sviluppo.

Libreria di terze parti	Licenza	URL del progetto
asio	https://www.boost.org/LICENSE_1_0.txt*	https://think-async.com/Asio/
Base58	https://github.com/leafo/lua-base58/blob/master/LICENSE	https://github.com/leafo/lua-base58
boost	https://www.boost.org/LICENSE_1_0.txt*	https://www.boost.org/
brotli	MIT License**	https://github.com/google/brotli
bsdiff	Custom	http://www.daemonology.net/bsdiff/
c-ares	https://c-ares.org/license.html*	https://c-ares.org/
cairo	Mozilla Public License** GNU Lesser General Public License**	https://www.cairographics.org/
CodeMirror	MIT License**	https://codemirror.net/
curl	https://curl.se/docs/copyright.html*	https://curl.se/libcurl/
fontconfig	Custom	https://www.freedesktop.org/wiki/Software/fontconfig/
freetype	GNU General Public License** FreeType Project License (BSD like)	https://freetype.org/
GCC runtime libraries	GNU General Public License** with exception*	https://gcc.gnu.org/
HTMLayout	Custom	https://terrainformatica.com/a-homepage-section/htmlayout/
ICU	https://www.unicode.org/copyright.html#License*	https://icu.unicode.org/home
jemalloc	https://github.com/jemalloc/jemalloc/blob/dev/COPYING*	https://github.com/jemalloc/jemalloc
jQuery	MIT License**	https://jquery.com/

Libreria di terze parti	Licenza	URL del progetto
	GNU General Public License**	
JSON	https://github.com/nlohmann/json/blob/develop/LICENSE.MIT	https://github.com/nlohmann/json
JSON4Lua	MIT License**	https://github.com/craigmj/json4lua
Leaflet	BSD License https://github.com/Leaflet/Leaflet/blob/main/LICENSE*	https://leafletjs.com
libipeg turbo	https://github.com/libjpeg-turbo/libjpeg-turbo/blob/main/LICENSE.md	https://libjpeg-turbo.org/
libpng	http://libpng.org/pub/png/src/libpng-LICENSE.txt*	http://libpng.org/pub/png/libpng.html
libradius	Juniper Networks, Inc.*	https://www.freebsd.org
libssh2	3-Clause BSD License https://github.com/libssh2/libssh2/blob/master/COPYING*	https://libssh2.org/
libxml2	MIT License**	https://gitlab.gnome.org/GNOME/libxml2/-/wikis/home
Linenoise NG	BSD License*	https://github.com/arangodb/linenoise-ng
lua	MIT License**	https://www.lua.org/
lua-xmlreader	MIT License**	https://asbradbury.org/projects/lua-xmlreader/
lzma	Public Domain	https://www.7-zip.org/sdk.html
ncurses	MIT License**	https://invisible-island.net/ncurses/announce.html
Net-snmp	http://www.net-snmp.org/about/license.html*	http://www.net-snmp.org/
nghttp2	MIT License**	https://nghttp2.org/
Noto Sans CJK	https://scripts.sil.org/cms/scripts/render_download.php?format=file&media_id=OFL_plaintext&filename=OFL.txt*	https://fonts.google.com/noto/use

Libreria di terze parti	Licenza	URL del progetto
OpenLDAP	https://www.openldap.org/software/release/license.html*	https://www.openldap.org
OpenSSL	https://www.openssl.org/source/license.html*	https://www.openssl.org/
Oracle Instant Client	https://www.oracle.com/downloads/licenses/instant-client-lic.html*	https://www.oracle.com
ParaType Free Font	https://www.paratype.ru/eula*	https://www.paratype.ru
pcre	http://www.pcre.org/licence.txt*	http://www.pcre.org/
pixman	MIT License**	http://pixman.org/
Prototype JavaScript framework	MIT License**	http://prototypejs.org/assets/2009/8/31/prototype.js
quirc	https://github.com/dlbeer/quirc/blob/master/LICENSE	https://github.com/dlbeer/quirc/
QR Code generator	https://github.com/nayuki/QR-Code-generator	https://www.nayuki.io/page/qr-code-generator-library
script.aculo.us scriptaculous.js	https://madrobby.github.io/scriptaculous/license/*	http://script.aculo.us/
slt	MIT License**	https://code.google.com/archive/p/slt
SQLite	Public Domain https://www.sqlite.org/copyright.html	https://www.sqlite.org/index.html
wtl	Common Public License** Microsoft Public License**	https://sourceforge.net/projects/wtl/
zlib	https://www.zlib.net/zlib_license.html*	https://www.zlib.net/

* — i testi delle licenze sono riportati di seguito.

** — i testi delle licenze di base sono ritrovabili sui seguenti indirizzi:

Licenza	Indirizzo
Common Public License	https://opensource.org/license/cpl1-0-txt/
GNU General Public License	https://www.gnu.org/licenses/gpl-3.0.html

Licenza	Indirizzo
GNU Lesser General Public License	https://www.gnu.org/licenses/lgpl-3.0.html
Microsoft Public License	https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff649456(v=pandp.10)
MIT License	https://opensource.org/license/mit/
Mozilla Public License	https://www.mozilla.org/en-US/MPL/2.0/
3-Clause BSD License	https://opensource.org/license/bsd-3-clause/

L1. Base58

```
The MIT License (MIT)


Copyright (c) 2015 leaf


Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:


The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.


THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
```

```
SOFTWARE.
```

L2. Boost

```
Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a
copy of the software and accompanying documentation covered by this license (the
"Software") to use, reproduce, display, distribute, execute, and transmit the Software,
and to prepare derivative works of the Software, and to permit third-parties to whom
the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above
license grant, this restriction and the following disclaimer, must be included in all
copies of the Software, in whole or in part, and all derivative works of the Software,
unless such copies or derivative works are solely in the form of machine-executable
object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS
OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY,
WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
```

L3. C-ares

```
Copyright (c) 2007 - 2018, Daniel Stenberg with many contributors, see AUTHORS file.

Copyright 1998 by the Massachusetts Institute of Technology.

Permission to use, copy, modify, and distribute this software and its documentation for
any purpose and without fee is hereby granted, provided that the above copyright notice
appear in all copies and that both that copyright notice and this permission notice
appear in supporting documentation, and that the name of M.I.T. not be used in
advertising or publicity pertaining to distribution of the software without specific,
written prior permission. M.I.T. makes no representations about the suitability of this
software for any purpose. It is provided "as is" without express or implied warranty.
```

L4. Curl

```
Copyright (c) 1996 - 2013, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or
without fee is hereby granted, provided that the above copyright notice and this
permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE
```

```
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN
CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in
advertising or otherwise to promote the sale, use or other dealings in this Software
without prior written authorization of the copyright holder.
```

L5. GCC runtime libraries—exception

```
GCC is Copyright (C) 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996,
1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008 Free Software
Foundation, Inc.

GCC is free software; you can redistribute it and/or modify it under the terms of the
GNU General Public License as published by the Free Software Foundation; either version
3, or (at your option) any later version.

GCC is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY;
without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR
PURPOSE.  See the GNU General Public License for more details.

Files that have exception clauses are licensed under the terms of the GNU General
Public License; either version 3, or (at your option) any later version.

The following runtime libraries are licensed under the terms of the GNU General Public
License (v3 or later) with version 3.1 of the GCC Runtime Library Exception (included
in this file):

 - libgcc (libgcc/, gcc/libgcc2.[ch], gcc/unwind*, gcc/gthr*, gcc/coretypes.h,
gcc/crtstuff.c, gcc/defaults.h, gcc/dwarf2.h, gcc/emults.c, gcc/gbl-ctors.h, gcc/gcov-
io.h, gcc/libgcov.c,  gcc/tsystem.h, gcc/typeclass.h).

 - libdecnumber

 - libgomp

 - libssp

 - libstdc++-v3

 - libobjc

 - libmudflap

 - libgfortran

 - The libgnat-4.4 Ada support library and libgnatvsn library.

 - Various config files in gcc/config/ used in runtime libraries.

GCC RUNTIME LIBRARY EXCEPTION

Version 3.1, 31 March 2009

Copyright (C) 2009 Free Software Foundation, Inc. <http://fsf.org/>
```

```
Everyone is permitted to copy and distribute verbatim copies of this license document,
but changing it is not allowed.

This GCC Runtime Library Exception ("Exception") is an additional permission under
section 7 of the GNU General Public License, version 3 ("GPLv3"). It applies to a given
file (the "Runtime Library") that bears a notice placed by the copyright holder of the
file stating that the file is governed by GPLv3 along with this Exception.

When you use GCC to compile a program, GCC may combine portions of certain GCC header
files and runtime libraries with the compiled program. The purpose of this Exception is
to allow compilation of non-GPL (including proprietary) programs to use, in this way,
the header files and runtime libraries covered by this Exception.

0. Definitions.

A file is an "Independent Module" if it either requires the Runtime Library for
execution after a Compilation Process, or makes use of an interface provided by the
Runtime Library, but is not otherwise based on the Runtime Library.

"GCC" means a version of the GNU Compiler Collection, with or without modifications,
governed by version 3 (or a specified later version) of the GNU General Public License
(GPL) with the option of using any subsequent versions published by the FSF.

"GPL-compatible Software" is software whose conditions of propagation, modification and
use would permit combination with GCC in accord with the license of GCC.

"Target Code" refers to output from any compiler for a real or virtual target processor
architecture, in executable form or suitable for input to an assembler, loader, linker
and/or execution phase. Notwithstanding that, Target Code does not include data in any
format that is used as a compiler intermediate representation, or used for producing a
compiler intermediate representation.

The "Compilation Process" transforms code entirely represented in non-intermediate
languages designed for human-written code, and/or in Java Virtual Machine byte code,
into Target Code. Thus, for example, use of source code generators and preprocessors
need not be considered part of the Compilation Process, since the Compilation Process
can be understood as starting with the output of the generators or preprocessors.

A Compilation Process is "Eligible" if it is done using GCC, alone or with other GPL-
compatible software, or if it is done without using any work based on GCC. For example,
using non-GPL-compatible Software to optimize any GCC intermediate representations
would not qualify as an Eligible Compilation Process.

1. Grant of Additional Permission.

You have permission to propagate a work of Target Code formed by combining the Runtime
Library with Independent Modules, even if such propagation would otherwise violate the
terms of GPLv3, provided that all Target Code was generated by Eligible Compilation
Processes. You may then convey such a combination under terms of your choice,
consistent with the licensing of the Independent Modules.

2. No Weakening of GCC Copyleft.

The availability of this Exception does not imply any general presumption that third-
party software is unaffected by the copyleft requirements of the license of GCC.
```

L6. ICU

```
Copyright © 1991-2018 Unicode, Inc. All rights reserved.
```

```
Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the
Unicode data files and any associated documentation (the "Data Files") or Unicode
software and any associated documentation (the "Software") to deal in the Data Files or
Software without restriction, including without limitation the rights to use, copy,
modify, merge, publish, distribute, and/or sell copies of the Data Files or Software,
and to permit persons to whom the Data Files or Software are furnished to do so,
provided that either (a) this copyright and permission notice appear with all copies of
the Data Files or Software, or (b) this copyright and permission notice appear in
associated Documentation.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR
A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE
COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY
SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER
TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE
DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in
advertising or otherwise to promote the sale, use or other dealings in these Data Files
or Software without prior written authorization of the copyright holder.
```

L7. Jemalloc

```
Unless otherwise specified, files in the jemalloc source distribution are subject to
the following license:

--------------------------------------------------------------------------------

Copyright (C) 2002-2018 Jason Evans <jasone@canonware.com>.

All rights reserved.

Copyright (C) 2007-2012 Mozilla Foundation.  All rights reserved.

Copyright (C) 2009-2018 Facebook, Inc.  All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice(s), this list
of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice(s), this
list of conditions and the following disclaimer in the documentation and/or other
materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER(S) ``AS IS'' AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE COPYRIGHT HOLDER(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

```
--------------------------------------------------------------------------------
```

L8. JSON

```
MIT License


Copyright (c) 2013-2022 Niels Lohmann


Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:


The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.


THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
```

L9. Leaflet

```
Copyright (c) 2010-2018, Vladimir Agafonkin
Copyright (c) 2010-2011, CloudMade
All rights reserved.
```

```
Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

   1. Redistributions of source code must retain the above copyright notice, this list
of conditions and the following disclaimer.

   2. Redistributions in binary form must reproduce the above copyright notice, this
list of conditions and the following disclaimer in the documentation and/or other
materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

L10. libjpeg turbo

```
libjpeg-turbo note:  This file has been modified by The libjpeg-turbo
Project

to include only information relevant to libjpeg-turbo, to wordsmith certain

sections, and to remove impolitic language that existed in the libjpeg v8

README.  It is included only for reference.  Please see README.md for

information specific to libjpeg-turbo.



The Independent JPEG Group's JPEG software

==========================================



This distribution contains a release of the Independent JPEG Group's free
JPEG

software.  You are welcome to redistribute this software and to use it for
any

purpose, subject to the conditions under LEGAL ISSUES, below.



This software is the work of Tom Lane, Guido Vollbeding, Philip Gladstone,
```

```
Bill Allombert, Jim Boucher, Lee Crocker, Bob Friesenhahn, Ben Jackson,
Julian Minguillon, Luis Ortiz, George Phillips, Davide Rossi, Ge' Weijers,
and other members of the Independent JPEG Group.

IJG is not affiliated with the ISO/IEC JTC1/SC29/WG1 standards committee
(also known as JPEG, together with ITU-T SG16).



DOCUMENTATION ROADMAP
=====================

This file contains the following sections:

OVERVIEW            General description of JPEG and the IJG software.
LEGAL ISSUES        Copyright, lack of warranty, terms of distribution.
REFERENCES          Where to learn more about JPEG.
ARCHIVE LOCATIONS   Where to find newer versions of this software.
FILE FORMAT WARS    Software *not* to get.
TO DO               Plans for future IJG releases.

Other documentation files in the distribution are:

User documentation:
  usage.txt         Usage instructions for cjpeg, djpeg, jpegtran,
                    rdjpgcom, and wrjpgcom.
  *.1               Unix-style man pages for programs (same info as
usage.txt).
  wizard.txt        Advanced usage instructions for JPEG wizards only.
  change.log        Version-to-version change highlights.
```

```
Programmer and internal documentation:

  libjpeg.txt       How to use the JPEG library in your own programs.

  example.txt       Sample code for calling the JPEG library.

  structure.txt     Overview of the JPEG library's internal structure.

  coderules.txt     Coding style rules --- please read if you contribute
code.


Please read at least usage.txt.  Some information can also be found in the
JPEG

FAQ (Frequently Asked Questions) article.  See ARCHIVE LOCATIONS below to
find

out where to obtain the FAQ article.


If you want to understand how the JPEG code works, we suggest reading one or

more of the REFERENCES, then looking at the documentation files (in roughly

the order listed) before diving into the code.



OVERVIEW

========


This package contains C software to implement JPEG image encoding, decoding,

and transcoding.  JPEG (pronounced "jay-peg") is a standardized compression

method for full-color and grayscale images.  JPEG's strong suit is
compressing

photographic images or other types of images that have smooth color and

brightness transitions between neighboring pixels.  Images with sharp lines
or

other abrupt features may not compress well with JPEG, and a higher JPEG

quality may have to be used to avoid visible compression artifacts with such

images.
```

```
JPEG is lossy, meaning that the output pixels are not necessarily identical
to

the input pixels.  However, on photographic content and other "smooth"
images,

very good compression ratios can be obtained with no visible compression

artifacts, and extremely high compression ratios are possible if you are

willing to sacrifice image quality (by reducing the "quality" setting in the

compressor.)


This software implements JPEG baseline, extended-sequential, and progressive

compression processes.  Provision is made for supporting all variants of
these

processes, although some uncommon parameter settings aren't implemented yet.

We have made no provision for supporting the hierarchical or lossless

processes defined in the standard.


We provide a set of library routines for reading and writing JPEG image
files,

plus two sample applications "cjpeg" and "djpeg", which use the library to

perform conversion between JPEG and some other popular image file formats.

The library is intended to be reused in other applications.


In order to support file conversion and viewing software, we have included

considerable functionality beyond the bare JPEG coding/decoding capability;

for example, the color quantization modules are not strictly part of JPEG

decoding, but they are essential for output to colormapped file formats or

colormapped displays.  These extra functions can be compiled out of the

library if not required for a particular application.
```

```
We have also included "jpegtran", a utility for lossless transcoding between
different JPEG processes, and "rdjpgcom" and "wrjpgcom", two simple
applications for inserting and extracting textual comments in JFIF files.

The emphasis in designing this software has been on achieving portability
and
flexibility, while also making it fast enough to be useful.  In particular,
the software is not intended to be read as a tutorial on JPEG.  (See the
REFERENCES section for introductory material.)  Rather, it is intended to
be reliable, portable, industrial-strength code.  We do not claim to have
achieved that goal in every aspect of the software, but we strive for it.

We welcome the use of this software as a component of commercial products.
No royalty is required, but we do ask for an acknowledgement in product
documentation, as described under LEGAL ISSUES.



LEGAL ISSUES
============

In plain English:

1. We don't promise that this software works.  (But if you find any bugs,
   please let us know!)
2. You can use this software for whatever you want.  You don't have to pay
us.
3. You may not pretend that you wrote this software.  If you use it in a
   program, you must acknowledge somewhere in your documentation that
   you've used the IJG code.
```

```
In legalese:

The authors make NO WARRANTY or representation, either express or implied,
with respect to this software, its quality, accuracy, merchantability, or
fitness for a particular purpose.  This software is provided "AS IS", and
you,
its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2020, Thomas G. Lane, Guido Vollbeding.
All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this
software (or portions thereof) for any purpose, without fee, subject to
these
conditions:
(1) If any part of the source code for this software is distributed, then
this
README file must be included, with this copyright and no-warranty notice
unaltered; and any additions, deletions, or changes to the original files
must be clearly indicated in accompanying documentation.
(2) If only executable code is distributed, then the accompanying
documentation must state that "this software is based in part on the work of
the Independent JPEG Group".
(3) Permission for use of this software is granted only if the user accepts
full responsibility for any undesirable consequences; the authors accept
NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG
code,
```

```
not just to the unmodified library.  If you use our work, you ought to
acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company
name
in advertising or publicity relating to this software or products derived
from
it.  This software may be referred to only as "the Independent JPEG Group's
software".

We specifically permit and encourage the use of this software as the basis
of
commercial products, provided that all warranty or liability claims are
assumed by the product vendor.



REFERENCES
==========

We recommend reading one or more of these references before trying to
understand the innards of the JPEG software.

The best short technical introduction to the JPEG compression algorithm is
        Wallace, Gregory K.  "The JPEG Still Picture Compression Standard",
        Communications of the ACM, April 1991 (vol. 34 no. 4), pp. 30-44.
(Adjacent articles in that issue discuss MPEG motion picture compression,
applications of JPEG, and related topics.)  If you don't have the CACM issue
handy, a PDF file containing a revised version of Wallace's article is
available at http://www.ijg.org/files/Wallace.JPEG.pdf.  The file (actually
a preprint for an article that appeared in IEEE Trans. Consumer Electronics)
```

omits the sample images that appeared in CACM, but it includes corrections and some added material. Note: the Wallace article is copyright ACM and IEEE, and it may not be used for commercial purposes.

A somewhat less technical, more leisurely introduction to JPEG can be found in "The Data Compression Book" by Mark Nelson and Jean-loup Gailly, published by M&T Books (New York), 2nd ed. 1996, ISBN 1-55851-434-1. This book provides good explanations and example C code for a multitude of compression methods including JPEG. It is an excellent source if you are comfortable reading C code but don't know much about data compression in general. The book's JPEG sample code is far from industrial-strength, but when you are ready to look at a full implementation, you've got one here...

The best currently available description of JPEG is the textbook "JPEG Still Image Data Compression Standard" by William B. Pennebaker and Joan L. Mitchell, published by Van Nostrand Reinhold, 1993, ISBN 0-442-01272-1. Price US$59.95, 638 pp. The book includes the complete text of the ISO JPEG standards (DIS 10918-1 and draft DIS 10918-2).

The original JPEG standard is divided into two parts, Part 1 being the actual specification, while Part 2 covers compliance testing methods. Part 1 is titled "Digital Compression and Coding of Continuous-tone Still Images, Part 1: Requirements and guidelines" and has document numbers ISO/IEC IS 10918-1, ITU-T T.81. Part 2 is titled "Digital Compression and Coding of Continuous-tone Still Images, Part 2: Compliance testing" and has document numbers ISO/IEC IS 10918-2, ITU-T T.83.

```
The JPEG standard does not specify all details of an interchangeable file
format.  For the omitted details, we follow the "JFIF" conventions, revision
1.02.  JFIF version 1 has been adopted as ISO/IEC 10918-5 (05/2013) and
Recommendation ITU-T T.871 (05/2011): Information technology - Digital
compression and coding of continuous-tone still images: JPEG File
Interchange
Format (JFIF).  It is available as a free download in PDF file format from
https://www.iso.org/standard/54989.html and http://www.itu.int/rec/T-REC-
T.871.
A PDF file of the older JFIF 1.02 specification is available at
http://www.w3.org/Graphics/JPEG/jfif3.pdf.


The TIFF 6.0 file format specification can be obtained from
http://mirrors.ctan.org/graphics/tiff/TIFF6.ps.gz.  The JPEG incorporation
scheme found in the TIFF 6.0 spec of 3-June-92 has a number of serious
problems.  IJG does not recommend use of the TIFF 6.0 design (TIFF
Compression
tag 6).  Instead, we recommend the JPEG design proposed by TIFF Technical
Note
#2 (Compression tag 7).  Copies of this Note can be obtained from
http://www.ijg.org/files/.  It is expected that the next revision
of the TIFF spec will replace the 6.0 JPEG design with the Note's design.
Although IJG's own code does not support TIFF/JPEG, the free libtiff library
uses our library to implement TIFF/JPEG per the Note.



ARCHIVE LOCATIONS
=================
```

```
The "official" archive site for this software is www.ijg.org.
The most recent released version can always be found there in
directory "files".

The JPEG FAQ (Frequently Asked Questions) article is a source of some
general information about JPEG.  It is available at
http://www.faqs.org/faqs/jpeg-faq.



FILE FORMAT COMPATIBILITY
=========================

This software implements ITU T.81 | ISO/IEC 10918 with some extensions from
ITU T.871 | ISO/IEC 10918-5 (JPEG File Interchange Format-- see REFERENCES).
Informally, the term "JPEG image" or "JPEG file" most often refers to JFIF
or
a subset thereof, but there are other formats containing the name "JPEG"
that
are incompatible with the DCT-based JPEG standard or with JFIF (for
instance,
JPEG 2000 and JPEG XR).  This software therefore does not support these
formats.  Indeed, one of the original reasons for developing this free
software
was to help force convergence on a common, interoperable format standard for
JPEG files.

JFIF is a minimal or "low end" representation.  TIFF/JPEG (TIFF revision 6.0
as
modified by TIFF Technical Note #2) can be used for "high end" applications
that need to record a lot of additional data about an image.
```

```
TO DO

=====


Please send bug reports, offers of help, etc. to jpeg-info@jpegclub.org.
```

```
Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:



1. The origin of this software must not be misrepresented; you must not
claim that you wrote the original software. If you use this software in a
product, an acknowledgment in the product documentation would be appreciated
but is not required.



2. Altered source versions must be plainly marked as such, and must not be
misrepresented as being the original software.



3. This notice may not be removed or altered from any source distribution.
```

L11. Libpng

```
If you modify libpng you may insert additional notices immediately following this
sentence.

This code is released under the libpng license.

libpng versions 1.0.7, July 1, 2000 through 1.6.32, August 24, 2017 are Copyright (c)
2000-2002, 2004, 2006-2017 Glenn Randers-Pehrson, are derived from libpng-1.0.6, and
are distributed according to the same disclaimer and license as libpng-1.0.6 with the
following individuals added to the list of Contributing Authors:

   Simon-Pierre Cadieux

   Eric S. Raymond

   Mans Rullgard

   Cosmin Truta

   Gilles Vollant

   James Yu

   Mandar Sahastrabuddhe

   Google Inc.

   Vadim Barkov

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against
infringement.  There is no warranty that our efforts or the library will fulfill any of
your particular purposes or needs.  This library is provided with all faults, and the
```

```
entire risk of satisfactory quality, performance, accuracy, and effort is with the
user.

Some files in the "contrib" directory and some configure-generated files that are
distributed with libpng have other copyright owners and are released under other open
source licenses.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c)
1998-2000 Glenn Randers-Pehrson, are derived from libpng-0.96, and are distributed
according to the same disclaimer and license as libpng-0.96, with the following
individuals added to the list of Contributing Authors:

   Tom Lane

   Glenn Randers-Pehrson

   Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996-1997
Andreas Dilger, are derived from libpng-0.88, and are distributed according to the same
disclaimer and license as libpng-0.88, with the following individuals added to the list
of Contributing Authors:

   John Bowler

   Kevin Bracey

   Sam Bushell

   Magnus Holmgren

   Greg Roelofs

   Tom Tanner

Some files in the "scripts" directory have other copyright owners but are released
under this license.

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995-1996
Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as
the following set of individuals:

   Andreas Dilger

   Dave Martindale

   Guy Eric Schalnat

   Paul Schmidt

   Tim Wegner

The PNG Reference Library is supplied "AS IS".  The Contributing Authors and Group 42,
Inc. disclaim all warranties, expressed or implied, including, without limitation, the
warranties of merchantability and of fitness for any purpose.  The Contributing Authors
and Group 42, Inc. assume no liability for direct, indirect, incidental, special,
exemplary, or consequential damages, which may result from the use of the PNG Reference
Library, even if advised of the possibility of such damage.
```

```
Permission is hereby granted to use, copy, modify, and distribute this source code, or
portions hereof, for any purpose, without fee, subject to the following restrictions:

  1. The origin of this source code must not be misrepresented.

  2. Altered versions must be plainly marked as such and must not be misrepresented as
being the original source.

  3. This Copyright notice may not be removed or altered from any source or altered
source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and
encourage the use of this source code as a component to supporting the PNG file format
in commercial products.  If you use this source code in a product, acknowledgment is
not required but would be appreciated.



Glenn Randers-Pehrson

glennrp at users.sourceforge.net

April 1, 2017
```

L12. Libradius

```
 Copyright 1998 Juniper Networks, Inc.

 All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

 1. Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

 2. Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

$FreeBSD: src/lib/libradius/radlib_private.h,v 1.6.30.3 2012/04/21 18:30:48 melifaro
Exp $
```

L13. Libssh2

L14. Linenoise NG

linenoise

```
  * Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

  * Neither the name of Redis nor the names of its contributors may be used to endorse
or promote products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

wcwidth

```
Markus Kuhn -- 2007-05-26 (Unicode 5.0)

Permission to use, copy, modify, and distribute this software for any purpose and
without fee is hereby granted. The author disclaims all warranties with regard to this
software.
```

ConvertUTF

```
Copyright 2001-2004 Unicode, Inc.

 Disclaimer

 This source code is provided as is by Unicode, Inc. No claims are made as to fitness
for any particular purpose. No warranties of any kind are expressed or implied. The
recipient agrees to determine applicability of information provided. If this file has
been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any
claim will be exchange of defective media within 90 days of receipt.

 Limitations on Rights to Redistribute This Code

 Unicode, Inc. hereby grants the right to freely use the information supplied in this
file in the creation of products supporting the Unicode Standard, and to make copies of
this file in any form for internal or external distribution as long as this notice
remains attached.
```

L15. Net-snmp

```
Various copyrights apply to this package, listed in various separate parts below.
Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

 Copyright 1989, 1991, 1992 by Carnegie Mellon University
```

```
      Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

      All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for
any purpose and without fee is hereby granted, provided that the above copyright notice
appears in all copies and that both that copyright notice and this permission notice
appear in supporting documentation, and that the name of CMU and The Regents of the
University of California not be used in advertising or publicity pertaining to
distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD
TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN
NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY
SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER
TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS
SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its
contributors may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:
```

```
Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or
product names may not be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ''AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED
AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be
used to endorse or promote products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:
```

```
* Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its contributors may be used
to endorse or promote products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

L16. Noto Sans CJK

```
Copyright (c) <dates>, <Copyright Holder> (<URL|email>), with Reserved Font Name
<Reserved Font Name>.

Copyright (c) <dates>, <additional Copyright Holder> (<URL|email>), with Reserved Font
Name <additional Reserved Font Name>.

Copyright (c) <dates>, <additional Copyright Holder> (<URL|email>).

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at:

http://scripts.sil.org/OFL

-----------------------------------------------------------

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

-----------------------------------------------------------

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of
collaborative font projects, to support the font creation efforts of academic and
linguistic communities, and to provide a free and open framework in which fonts may be
shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed
freely as long as they are not sold by themselves. The fonts, including any derivative
works, can be bundled, embedded, redistributed and/or sold with any software provided
that any reserved names are not used by derivative works. The fonts and derivatives,
however, cannot be released under any other type of license. The requirement for fonts
to remain under this license does not apply to any document created using the fonts or
their derivatives.
```

DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION

This license becomes null and void if any of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

L17. OpenLDAP

```
The OpenLDAP Public License

  Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with
or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and
notices, this list of conditions, and the following disclaimer in the documentation
and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is
distinguished by a version number. You may use this Software under terms of this
license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND
ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN
NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S)
OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED
AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN IF ADVISED OF THE  POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or
otherwise to promote the sale, use or other dealing in this Software without specific,
written prior permission.  Title to copyright in this Software shall at all times
remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA.  All Rights
Reserved.  Permission to copy and distribute verbatim copies of this document is
granted.
```

L18. OpenSSL

```
Copyright (c) 1998-2018 The OpenSSL Project.  All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.
```

```
3. All advertising materials mentioning features or use of this software must display
the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL
Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or
promote products derived from this software without prior written permission. For
written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL"
appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL
Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL
PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

====================================================================

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
 This product includes software written by Tim Hudson (tjh@cryptsoft.com).

 Original SSLeay License

 -----------------------

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following
conditions are aheared to.  The following conditions apply to all code found in this
distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code.  The
SSL documentation included with this distribution is covered by the same copyright
terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not
to be removed.

If this package is used in a product, Eric Young should be given attribution as the
author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation
(online or textual) provided with the package.
```

```
Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of
conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

3. All advertising materials mentioning features or use of this software must display
the following acknowledgement:

   "This product includes cryptographic software written by Eric Young
(eay@cryptsoft.com)"

   The word 'cryptographic' can be left out if the rouines from the library being used
are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps
directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED
AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative
of this code cannot be changed.  i.e. this code cannot simply be copied and put under
another distribution licence [including the GNU Public Licence.]
```

L19. Oracle Instant Client

```
Export Controls on the Programs

Selecting the "Accept License Agreement" button is a confirmation of your agreement
that you comply, now and during the trial term, with each of the following statements:

-You are not a citizen, national, or resident of, and are not under control of, the
government of Cuba, Iran, Sudan, Libya, North Korea, Syria, nor any country to which
the United States has prohibited export.

-You will not download or otherwise export or re-export the Programs, directly or
indirectly, to the above mentioned countries nor to citizens, nationals or residents of
those countries.

-You are not listed on the United States Department of Treasury lists of Specially
Designated Nationals, Specially Designated Terrorists, and Specially Designated
Narcotic Traffickers, nor are you listed on the United States Department of Commerce
Table of Denial Orders.
```

You will not download or otherwise export or re-export the Programs, directly or indirectly, to persons on the above mentioned lists.

You will not use the Programs for, and will not allow the Programs to be used for, any purposes prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction.

EXPORT RESTRICTIONS

You agree that U.S. export control laws and other applicable export and import laws govern your use of the programs, including technical data; additional information can be found on Oracle®'s Global Trade Compliance web site (http://www.oracle.com/products/export).

You agree that neither the programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Oracle Employees: Under no circumstances are Oracle Employees authorized to download software for the purpose of distributing it to customers. Oracle products are available to employees for internal use or demonstration purposes only. In keeping with Oracle's trade compliance obligations under U.S. and applicable multilateral law, failure to comply with this policy could result in disciplinary action up to and including termination.

Note: You are bound by the Oracle Technology Network ("OTN") License Agreement terms. The OTN License Agreement terms also apply to all updates you receive under your Technology Track subscription.

The OTN License Agreement terms below supercede any shrinkwrap license on the OTN Technology Track software CDs and previous OTN License terms (including the Oracle Program License as modified by the OTN Program Use Certificate).

Oracle Technology Network Development and Distribution License Agreement for Instant Client

"We," "us," and "our" refers to Oracle America, Inc. "You" and "your" refers to the individual or entity that wishes to use the Programs from Oracle under this Agreement. "Programs" refers to the Software Products referenced below that you wish to download and use and Program documentation. "License" refers to your right to use the Programs and Program documentation under the terms of this Agreement. The substantive and procedural laws of California govern this Agreement. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, San Mateo, or Santa Clara counties in California in any dispute arising out of or relating to this Agreement.

We are willing to license the Programs to you only upon the condition that you accept all of the terms contained in this Agreement. Read the terms carefully and select the "Accept" button at the bottom of the page to confirm your acceptance. If you are not willing to be bound by these terms, select the "Do Not Accept" button and the registration process will not continue.

Software Product

- Instant Client

License Rights

License.

We grant you a non-exclusive right and license to use the Programs solely for your business purposes and development and testing purposes, subject to the terms of this Agreement. You may allow third parties to use the Programs, subject to the terms of this Agreement, provided such third party use is for your business operations only.

Distribution License

We grant you a non-exclusive right and license to distribute the Programs, provided that you do not charge your end users for use of the Programs. Your distribution of such Programs shall at a minimum include the following terms in an executed license agreement between you and the end user that: (1) restrict the use of the Programs to the business operations of the end user; (2) prohibit (a) the end user from assigning, giving, or transferring the Programs or an interest in them to another individual or entity (and if your end user grants a security interest in the Programs, the secured party has no right to use or transfer the Programs); (b) make the Programs available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted for the specific program license or materials from the services you have acquired); and (c) title to the Programs from passing to the end user or any other party; (3) prohibit the reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs and prohibit duplication of the Programs except for a sufficient number of copies of each Program for the end user's licensed use and one copy of each Program media; (4) disclaim, to the extent permitted by applicable law, our liability for any damages, whether direct, indirect, incidental, or consequential, arising from the use of the Programs; (5) require the end user at the termination of the Agreement, to discontinue use and destroy or return to you all copies of the Programs and documentation; (6) prohibit publication of any results of benchmark tests run on the Programs; (7) require the end user to comply fully with all relevant export laws and regulations of the United States and other applicable export and import laws to assure that neither the Programs, nor any direct product thereof, are exported, directly or indirectly, in violation of applicable laws; (8) do not require us to perform any obligations or incur any liability not previously agreed to between you and us; (9) permit you to audit your end user's use of the Programs or to assign your right to audit the end user's use of the Programs to us; (10) designate us as a third party beneficiary of the end user license agreement; (11) include terms consistent with those contained in the sections of this Agreement entitled "Disclaimer of Warranties and Exclusive Remedies," "No Technical Support," "End of Agreement," "Relationship Between the Parties," and "Open Source"; and (11) exclude the application of the Uniform Computer Information Transactions Act.

You may allow your end users to permit third parties to use the Programs on such end user's behalf for the purposes set forth in the end user license agreement, subject to the terms of such agreement. You shall be financially responsible for all claims and damages to us caused by your failure to include the required contractual terms set forth above in each end user license agreement between you and an end user. We are a third party beneficiary of any end user license agreement between you and the end user, but do not assume any of your obligations thereunder, and you agree that you will not enter into any end user license agreement that excludes us as a third party beneficiary and will inform your end users of our rights.

If you want to use the Programs for any purpose other than as expressly permitted under this Agreement you must contact us to obtain the appropriate license. We may audit your use of the Programs. Program documentation is either shipped with the Programs, or documentation may be accessed online at
http://www.oracle.com/technetwork/indexes/documentation/index.html.

You agree to: (a) defend and indemnify us against all claims and damages caused by your distribution of the Programs in breach of this Agreement and/or failure to include the required contractual provisions in your end user agreement as stated above; (b) keep executed end user agreements and records of end user information including name, address, date of distribution and identity of Programs distributed; (c) allow us to inspect your end user agreements and records upon request; and, (d) enforce the terms of your end user agreements so as to effect a timely cure of any end user breach, and to notify us of any breach of the terms.

Ownership and Restrictions

We retain all ownership and intellectual property rights in the Programs. You may make a sufficient number of copies of the Programs for the licensed use and one copy of the Programs for backup purposes.

You may not:

-use the Programs for any purpose other than as provided above;

-charge your end users for use of the Programs;

-remove or modify any Program markings or any notice of our proprietary rights;

-assign this agreement or give the Programs, Program access or an interest in the Programs to any individual or entity except as provided under this agreement;

-cause or permit reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs;

-disclose results of any Program benchmark tests without our prior consent.

Export

You agree that U.S. export control laws and other applicable export and import laws govern your use of the Programs, including technical data; additional information can be found on Oracle's Global Trade Compliance web site located at http://www.oracle.com/products/export/index.html. You agree that neither the Programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Disclaimer of Warranty and Exclusive Remedies

THE PROGRAMS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. WE FURTHER DISCLAIM ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

IN NO EVENT SHALL WE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

No Technical Support

Our technical support organization will not provide technical support, phone support, or updates to you or end users for the Programs licensed under this agreement.

Restricted Rights

If you distribute a license to the United States government, the Programs, including documentation, shall be considered commercial computer software and you will place a legend, in addition to applicable copyright notices, on the documentation, and on the media label, substantially similar to the following:

NOTICE OF RESTRICTED RIGHTS

"Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the

applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065."

End of Agreement

You may terminate this Agreement by destroying all copies of the Programs. We have the right to terminate your right to use the Programs if you fail to comply with any of the terms of this Agreement, in which case you shall destroy all copies of the Programs.

Relationship Between the Parties

The relationship between you and us is that of licensee/licensor. Neither party will represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other party, nor to represent the other party as agent, employee, franchisee, or in any other capacity. Nothing in this Agreement shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

Open Source

"Open Source" software - software available without charge for use, modification and distribution - is often licensed under terms that require the user to make the user's modifications to the Open Source software or any software that the user 'combines' with the Open Source software freely available in source code form. If you use Open Source software in conjunction with the Programs, you must ensure that your use does not: (i) create, or purport to create, obligations of us with respect to the Oracle Programs; or (ii) grant, or purport to grant, to any third party any rights to or immunities under our intellectual property or proprietary rights in the Oracle Programs. For example, you may not develop a software program using an Oracle Program and an Open Source program where such use results in a program file(s) that contains code from both the Oracle Program and the Open Source program (including without limitation libraries) if the Open Source program is licensed under a license that requires any "modifications" be made freely available. You also may not combine the Oracle Program with programs licensed under the GNU General Public License ("GPL") in any manner that could cause, or could be interpreted or asserted to cause, the Oracle Program or any modifications thereto to become subject to the terms of the GPL.

Entire Agreement

You agree that this Agreement is the complete agreement for the Programs and licenses, and this Agreement supersedes all prior or contemporaneous Agreements or representations. If any term of this Agreement is found to be invalid or unenforceable, the remaining provisions will remain effective.

Last updated: 01/24/08

L20. ParaType Free Font

LICENSING AGREEMENT

for the fonts with Original Name: PT Sans, PT Serif, PT Mono

Version 1.3 - January 20, 2012

GRANT OF LICENSE

```
ParaType Ltd grants you the right to use, copy, modify the fonts and distribute
modified and unmodified copies of the fonts by any means, including placing on Web
servers for free downloading, embedding in documents and Web pages, bundling with
commercial and non commercial products, if it does not conflict with the conditions
listed below:

- You may bundle the fonts with commercial software, but you may not sell the fonts by
themselves. They are free.

- You may distribute the fonts in modified or unmodified versions only together with
this Licensing Agreement and with above copyright notice. You have no right to modify
the text of Licensing Agreement. It can be placed in a separate text file or inserted
into the font file, but it must be easily viewed by users.

- You may not distribute modified version of the font under the Original name or a
combination of Original name with any other words without explicit written permission
from ParaType.

TERMINATION & TERRITORY

This license has no limits on time and territory, but it becomes null and void if any
of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT.
IN NO EVENT SHALL PARATYPE BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER
IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY
TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

ParaType Ltd
```

L21. PCRE

```
PCRE2 is a library of functions to support regular expressions whose syntax and
semantics are as close as possible to those of the Perl 5 language.

Release 10 of PCRE2 is distributed under the terms of the "BSD" licence, as specified
below, with one exemption for certain binary redistributions. The documentation for
PCRE2, supplied in the "doc" directory, is distributed under the same terms as the
software itself. The data in the testdata directory is not copyrighted and is in the
public domain.

The basic library functions are written in C and are freestanding. Also included in the
distribution is a just-in-time compiler that can be used to optimize pattern matching.
This is an optional feature that can be omitted when the library is built.

THE BASIC LIBRARY FUNCTIONS

---------------------------

Written by:       Philip Hazel

Email local part: ph10
```

```
Email domain:     cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England.

Copyright (c) 1997-2018 University of Cambridge

All rights reserved.

PCRE2 JUST-IN-TIME COMPILATION SUPPORT

-------------------------------------

Written by:       Zoltan Herczeg

Email local part: hzmester

Email domain:     freemail.hu

Copyright(c) 2010-2018 Zoltan Herczeg

All rights reserved.

STACK-LESS JUST-IN-TIME COMPILER

--------------------------------

Written by:       Zoltan Herczeg

Email local part: hzmester

Email domain:     freemail.hu

Copyright(c) 2009-2018 Zoltan Herczeg

All rights reserved.

THE "BSD" LICENCE

-----------------

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions are met:

 * Redistributions of source code must retain the above copyright notices, this list of
conditions and the following disclaimer.

 * Redistributions in binary form must reproduce the above copyright notices, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

  * Neither the name of the University of Cambridge nor the names of any contributors
may be used to endorse or promote products derived from this      software without
specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
```

```
THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

EXEMPTION FOR BINARY LIBRARY-LIKE PACKAGES

------------------------------------------

The second condition in the BSD licence (covering binary redistributions) does not
apply all the way down a chain of software. If binary package A includes PCRE2, it must
respect the condition, but if package B is software that includes package A, the
condition is not imposed on package B unless it uses PCRE2 independently.
```

L22. QR Code Generator

```
Copyright © 2022 Project Nayuki. (MIT License)

https://www.nayuki.io/page/qr-code-generator-library



Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to
deal in the Software without restriction, including without limitation the
rights to use, copy, modify, merge, publish, distribute, sublicense, and/or
sell copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:



The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.



The Software is provided "as is", without warranty of any kind, express or
implied, including but not limited to the warranties of merchantability,
fitness for a particular purpose and noninfringement. In no event shall the
authors or copyright holders be liable for any claim, damages or other
liability, whether in an action of contract, tort or otherwise, arising
from, out of or in connection with the Software or the use or other dealings
in the Software.
```

L23. quirc

```
quirc -- QR-code recognition library

Copyright (C) 2010-2012 Daniel Beer <dlbeer@gmail.com>
```

```
ISC License

==========

Permission to use, copy, modify, and/or distribute this software for
any purpose with or without fee is hereby granted, provided that the
above copyright notice and this permission notice appear in all
copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL
WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE
AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL
DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR
PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER
TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

L24. Script.aculo.us

```
Copyright © 2005-2008 Thomas Fuchs (http://script.aculo.us, http://mir.aculo.us)

Permission is hereby granted, free of charge, to any person obtaining a copy of this
software and associated documentation files (the “Software”), to deal in the Software
without restriction, including without limitation the rights to use, copy, modify,
merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to the following
conditions:

The above copyright notice and this permission notice shall be included in all copies
or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF
CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR
THE USE OR OTHER DEALINGS IN THE SOFTWARE.
```

L25. Zlib

```
zlib.h -- interface of the 'zlib' general purpose compression library

  version 1.2.11, January 15th, 2017

  Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler

  This software is provided 'as-is', without any express or implied warranty.  In no
event will the authors be held liable for any damages arising from the use of this
software.

  Permission is granted to anyone to use this software for any purpose, including
commercial applications, and to alter it and redistribute it freely, subject to the
following restrictions:

  1. The origin of this software must not be misrepresented; you must not claim that
you wrote the original software. If you use this software in a product, an
acknowledgment in the product documentation would be appreciated but is not required.

  2. Altered source versions must be plainly marked as such, and must not be
misrepresented as being the original software.

  3. This notice may not be removed or altered from any source distribution.

  Jean-loup Gailly        Mark Adler

  jloup@gzip.org          madler@alumni.caltech.edu
```

Allegato M. Procedure personalizzate

In questa sezione vengono descritte le seguenti categorie di procedure personalizzate:

Procedura	Descrizione
Amministratori	gestione dell'autenticazione degli amministratori
Gruppo	gestione dei gruppi
Accesso	gestione dell'accesso
Altro	varie
Nuovi arrivi	gestione delle nuove postazioni
Relazioni	gestione delle relazioni con i Server Dr.Web adiacenti
Server	gestione del Server Dr.Web
Connessioni	gestione delle connessioni con i client
Postazioni	gestione delle postazioni

Procedura	Descrizione
Ldap	traduzione dei nomi utente

M1. Amministratori

Amministratore è autenticato

Viene invocata in caso di autenticazione riuscita dell'amministratore nel Pannello di controllo della sicurezza.

Database	Parametri	Valore restituito
è disponibile	• `login` — nome utente dell'amministratore, • `address` — indirizzo di rete da cui si è autenticato l'amministratore, • `subsys` — sottosistema del Server Dr.Web (v. file `adm-subsys.ds`), • `id` — ID dell'amministratore, • `authorizer` — nome del modulo di autenticazione (database, LDAP, AD), • `language` — codice lingua dell'account amministratore, • `date_format` — formato data dell'account amministratore	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when Administrator authorize successfully

Database:
  available

Parameters:
  login              Administrator`s login name
  address            Administrator`s network address
  subsys             Server subsystem (see adm-subsys.ds)
  id                 Administrator`s ID
  authorizer         Authorizer name (database, LDAP, AD)
  language           Administrator`s language code
  date_format        Administrator`s date format

Returned value:
  ignored

]]
```

```
local args = ... -- args.login, args.address, args.subsys, args.error, args.id,
args.authorizer,
                 -- args.language, args.date_format
```

Amministratore è autenticato tramite Microsoft Active Directory Service

Viene invocata in caso di autenticazione riuscita dell'amministratore tramite Microsoft Active Directory Service (MSAD).

Database	Parametri	Valore restituito
è disponibile	• `login` — nome utente dell'amministratore, • `address` — indirizzo di rete da cui si è autenticato l'amministratore, • `is_secure` — l'amministratore utilizza una connessione sicura HTTPS (`true` | `false`), • `name` — nome LDAP dell'amministratore, • `DN` — LDAP DN dell'amministratore, • `SID` — identificatore di protezione Windows (SID) dell'amministratore, • `GUID` — identificatore univoco globale (GUID) dell'amministratore, • `primary_group` — nome del gruppo primario dell'amministratore, • `primary_group_DN` — LDAP DN del gruppo primario dell'amministratore, • `primary_group_SID` — identificatore di protezione (SID) del gruppo primario dell'amministratore, • `primary_group_GUID` — identificatore univoco globale (GUID) del gruppo primario dell'amministratore, • `groups` — tabella contenente i nomi del gruppo dell'amministratore (inclusi nell'attributo MSAD), • `groups_DN` — tabella contenente i nomi DN del gruppo dell'amministratore (nello stesso ordine dei gruppi), • `groups_SID` — tabella contenente gli identificatori di protezione (SID) del gruppo dell'amministratore (nello stesso ordine dei gruppi), • `groups_GUID` — tabella contenente gli identificatori univoci globali (GUID) del gruppo dell'amministratore (nello stesso ordine dei gruppi)	• `nil` — non fare nulla, • `string` — empty non fare nulla, • `not-empty` — imposta come gruppo dell'amministratore il gruppo con l'ID che corrisponde a questa stringa

Testo della procedura personalizzata:

```
--[[
Called:
```

```
  when the external administrator was authorized successfully using Microsoft Active
Directory Service

Database:
  available

Parameters:
  login              Administrator's login name
  address            Administrator's network address
  is_secure          Is true if administrator uses HTTPS connection
  name               Administrator's LDAP name
  DN                 Administrator's LDAP distinguished name
  SID                Administrator's Windows security identifier
  GUID               Administrator's GUID
  primary_group      Administrator's primary group name
  primary_group_DN   Administrator's primary group LDAP distinguished name
  primary_group_SID  Administrator's primary group SID
  primary_group_GUID Administrator's primary group GUID
  groups             Table containg Administrator's group names (memberOf MSAD
attribute)
  groups_DN          Table containg Administrator's group distinguished names (in the
same order as groups)
  groups_SID         Table containg Administrator's group SIDs (in the same order as
groups)
  groups_GUID        Table containg Administrator's group GUIDs (in the same order as
groups)

Returned value:
             nil        do nothing
  string     empty      do nothing
             not-empty  set administrator group to this string (group ID)

]]

local args = ... -- args.is_secure, args.login, args.address,
                 -- args.name, args.DN, args.SID, args.GUID,
                 -- args.primary_group, args.primary_group_DN, args.primary_group_SID,
args.primary_group_GUID,
                 -- args.groups, args.groups_DN, args.groups_SID, args.groups_GUID
```

Amministratore non è autenticato

Viene invocata in caso di errore di autenticazione dell'amministratore nel Pannello di controllo della sicurezza.

Database	Parametri	Valore restituito
è disponibile	• `login` — nome utente dell'amministratore, • `address` — indirizzo di rete dell'amministratore, • `subsys` — sottosistema del Server Dr.Web (v. file adm-subsys.ds), • `error` — codice di errore (v. file auth-error.ds)	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when Administrator authorization failed

Database:
  available

Parameters:
  login              Administrator`s login name
  address            Administrator`s network address
  subsys             Server subsystem (see adm-subsys.ds)
  error              Error code (see auth-error.ds)

Returned value:
  ignored

]]

local args = ... -- args.login, args.address, args.subsys, args.error
```

M2. Gruppo

Il gruppo è stato creato

Viene invocata dopo la creazione del nuovo gruppo.

Database	Parametri	Valore restituito
è disponibile se la procedura non è stata lanciata dalla funzione `drwcs.new_group()`	• `login` — nome utente dell'amministratore, • `id` — ID del gruppo, • `name` — nome del gruppo, • `pid` — ID del gruppo padre	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when new group created

Database:
  available

Parameters:
  login      administrator`s login name
  id         group ID
  name       group name
  pid        parent group ID

Returned value:
  ignored
```

```
]]

local args = ... -- args.login, args.id, args.name, args.pid
```

Il gruppo è stato rimosso

Viene invocata dopo la rimozione del gruppo.

Database	Parametri	Valore restituito
è disponibile	• `login` — nome utente dell'amministratore, • `id` — ID del gruppo, • `name` — nome del gruppo	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when group deleted

Database:
  available

Parameters:
  login      administrator`s login name
  id         group ID
  name       group name

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name
```

Le proprietà del gruppo sono state modificate

Viene invocata dopo la modifica delle proprietà del gruppo.

Database	Parametri	Valore restituito
è disponibile	• `login` — nome utente dell'amministratore, • `id` — ID del gruppo, • `name` — nome del gruppo, • `descr` — descrizione del gruppo, • `pid` — ID del gruppo padre	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when group properties changed

Database:
  available

Parameters:
  login      administrator`s login name
  id         group ID
  name       group name
  descr      group description
  pid        parent group ID

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name, args.descr, args.pid
```

M3. Accesso

Accesso proibito

Viene invocata se l'accesso viene negato secondo le impostazioni ACL o il risultato dell'esecuzione della procedura `access_check`.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID provvisorio del client (per nuovi arrivi/Server Dr.Web), • `address` — indirizzo di rete del client, • `station` — nome NetBIOS del client. Non viene impostato per i Server Dr.Web e non viene sostituito con il nome DNS, • `type` — “station”, “installer”, “newbie”, “server”, “proxy”, • `description` — descrizione della postazione	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when access denied according ACLs settings or result
  of 'access_check' procedure

Database:
  available

Parameters:
  id             station (temporary for newbie/server) ID
```

```
  address        station network address
  station        station name (undefined for servers)
                 this is NetBIOS station name (not replaced by DNS one)
  type           one of 'station' | 'installer' | 'newbie' | 'server' | 'proxy'
  description    station description

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.type, args.description

-- no return => `nil' value
```

Controllo dell'accesso

Viene invocata prima di controllare l'accesso sulla base delle relative ACL (Access Control List, liste di controllo degli accessi).

Database	Parametri	Valore restituito

è disponibile	• `id` — ID provvisorio del client (per nuovi arrivi/Server Dr.Web),
	• `address` — indirizzo di rete del client,
	• `station` — nome NetBIOS del client. Non viene impostato per i Server Dr.Web e non viene sostituito con il nome DNS,
	• `type` — “station”, “installer”, “newbie”, “server”, “proxy”
		• `nil` — controlla indirizzi attraverso le ACL impostate,
		• `boolean` — non controllare indirizzi attraverso le ACL, per tutti:
		  ▫ `true` — consenti l'accesso,
		  ▫ `false` — nega l'accesso

Testo della procedura personalizzata

```
--[[
Called:
  before check access against appropriate ACL

Database:
  available

Parameters:
  id              station ID (temporary for newbie/server)
  address         station network address
  station         station name (undefined for servers)
                  this is NetBIOS station name (not replaced by DNS one)
  type            one of 'station | installer | newbie | server | proxy'

Returned value:
              nil         check address against configured ACLs
  boolean     true        allow access, do not check agains ACLs
              false       reject access, do not check agains ACLs

Procedure from next set will be called if returned nothing.
]]

local args = ... -- args.id, args.address, args.station, args.type

-- no return => `nil' value
```

M4. Altro

Aggiornamento automatico della chiave di licenza

Viene invocata quando scade la chiave di licenza.

Database	Parametri	Valore restituito

è disponibile	• `event` — tipo di evento:
	  ▫ `expire` — la chiave di licenza sta per scadere, l'aggiornamento automatico non è disponibile
	  ▫ `diff` — è stata caricata una nuova chiave di licenza, ma la lista dei componenti concessi in licenza della chiave corrente è diversa da quella della chiave nuova. La chiave di licenza deve essere sostituita manualmente
	  ▫ `renew` — la chiave di licenza è stata aggiornata automaticamente
	• `old_key` — il contenuto della vecchia chiave di licenza
	• `new_key` — il contenuto della nuova chiave di licenza. È disponibile se il tipo di evento è `diff` o `renew`
		viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when license key expire or have been renewed

Database:
  available

Parameters:
  event       event type: "expire" - license key expires or have done it
                          "diff"   - received new key, but components differs from
current one
                          "renew"  - current key have been renewed, old one was deleted

  old_key     content of old license key
  new_key     content of renew license key, available at event type "diff" or "renew"

Returned value:
  ignored

]]

local args = ... -- args.event, args.old_key, args.new_key
```

Rilevata un'epidemia

Viene invocata al rilevamento di un'epidemia di virus nella rete.

Database	Parametri	Valore restituito
è disponibile	• `virus` — la minaccia più diffusa, • `total` — numero totale di minacce rilevate	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when virus epidemic has been detected by the server

Database:
  available

Parameters:
  total             total count of viruses
  virus             most frequently detected virus name

Returned value:
  ignored

]]

local args = ... -- args.total, args.virus
```

Report di Controllo delle applicazioni

Viene invocata quando viene ricevuto un report di Controllo delle applicazioni dalla postazione.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo di rete della postazione, • `station` — nome della postazione, • `time` — ora del verificarsi dell'evento (ora della postazione), • `sid` — SID della postazione, • `user` — utente che ha avviato il processo con un'attività sospetta, • `type` — tipo di evento, • `action` — azione applicata, • `policy_type` — tipo di criterio scattato, • `policy_mask` — maschera di criterio scattato,	viene ignorato

Database	Parametri	Valore restituito
	• `test_mode` — l'evento si è verificato in modalità test, • `profile_id` — UUID del profilo in base a cui è stato effettuato il blocco, • `profile_name` — nome del profilo in base a cui è stato effettuato il blocco, • `rule_id` — UUID della regola in base a cui è stato effettuato il blocco (se disponibile), • `rule_name` — nome della regola in base a cui è stato effettuato il blocco (se disponibile), • `process_path` — percorso del processo bloccato, • `process_file_sha256` — SHA-256 del file del processo, • `process_file_version` — versione del file del processo, • `process_file_description` — descrizione del file del processo, • `process_file_origname` — nome originale del file del processo, • `process_file_prodname` — nome del prodotto del file del processo, • `process_file_prodver` — versione del prodotto del file del processo, • `process_file_company` — nome dell'azienda del file del processo, • `process_cert_thumbprint` — impronta del certificato (SHA-1) con cui è firmato il processo (se disponibile), • `process_cert_serial` — numero di serie del certificato con cui è firmato il processo (se disponibile), • `process_cert_issuer` — emittente del certificato con cui è firmato il processo (se disponibile), • `process_cert_subject` — soggetto del certificato con cui è firmato il processo (se disponibile), • `process_cert_timestamp` — data di rilascio del certificato con cui è firmato il processo (se disponibile), • `process_cert_not_before` — data di entrata in vigore del certificato con cui è firmato il processo (se disponibile), • `process_cert_not_after` — data di scadenza del certificato con cui è firmato il processo (se disponibile), • `process_hashdb` — bollettino contenente l'hash del file del processo,	

Database	Parametri	Valore restituito
	• `object_path` — percorso dello script bloccato o un valore vuoto, • `object_file_sha256` — SHA-256 del file dello script (se disponibile), • `object_file_version` — versione del file dello script (se disponibile), • `object_file_description` — descrizione del file dello script (se disponibile), • `object_file_origname` — nome originale del file dello script (se disponibile), • `object_file_prodname` — nome del prodotto del file dello script (se disponibile), • `object_file_prodver` — versione del prodotto del file dello script (se disponibile), • `object_file_company` — nome dell'azienda del file dello script (se disponibile), • `object_cert_thumbprint` — impronta del certificato (SHA-1) con cui è firmato lo script (se disponibile), • `object_cert_serial` — numero di serie del certificato con cui è firmato lo script (se disponibile), • `object_cert_issuer` — emittente del certificato con cui è firmato lo script (se disponibile), • `object_cert_subject` — soggetto del certificato con cui è firmato lo script (se disponibile), • `object_cert_timestamp` — data di rilascio del certificato con cui è firmato lo script (se disponibile), • `object_cert_not_before` — data di entrata in vigore del certificato con cui è firmato lo script (se disponibile), • `object_cert_not_after` — data di scadenza del certificato con cui è firmato lo script (se disponibile), • `object_hashdb` — bollettino contenente l'hash del file dello script	

Testo della procedura personalizzata:

```
--[[
Called:
  when application control event received from Agent

Database:
  available

Parameters:
  id                station ID
  address           station address
```

```
  station             station name
  time                station time
  sid                 SID of user initiated activity
  user                name of user initiated activity
  type                event type
  action              applied action
  policy_type         matched policy type
  policy_mask         matched policy mask
  test_mode           event occured in test mode
  profile_id          profile UUID used for activity blocking
  profile_name        profile name used for activity blocking
  rule_id             rule UUID used for activity blocking (if exist)
  rule_name           rule name used for activity blocking (if exist)

  process_path                path to affected process file
  process_file_sha256         process file SHA-256
  process_file_version        process file version
  process_file_description    process file description
  process_file_origname       process file original name
  process_file_prodname       process file product name
  process_file_prodver        process file product version
  process_file_company        process file company name
  process_cert_thumbprint     process file signing certificate thumbprint (SHA-1) (if
exist)
  process_cert_serial         process file signing certificate serial number (if exist)
  process_cert_issuer         process file signing certificate issuer (if exist)
  process_cert_subject        process file signing certificate subject (if exist)
  process_cert_timestamp      process file signing certificate sign issuance timestamp
(if exist)
  process_cert_not_before     process file signing certificate NotBefore timestamp (if
exist)
  process_cert_not_after      process file signing certificate NotAfter timestamp (if
exist)
  process_hashdb              hash database containing process file

  object_path                 path to affected object file (script, etc) or empty
  object_file_sha256          object file SHA-256 (if exist)
  object_file_version         object file version (if exist)
  object_file_description     object file description (if exist)
  object_file_origname        object file original name (if exist)
  object_file_prodname        object file product name (if exist)
  object_file_prodver         object file product version (if exist)
  object_file_company         object file company name (if exist)
  object_cert_thumbprint      object file signing certificate thumbprint (SHA-1) (if
exist)
  object_cert_serial          object file signing certificate serial number (if exist)
  object_cert_issuer          object file signing certificate issuer (if exist)
  object_cert_subject         object file signing certificate subject (if exist)
  object_cert_timestamp       object file signing certificate sign issuance timestamp (if
exist)
  object_cert_not_before      object file signing certificate NotBefore timestamp (if
exist)
  object_cert_not_after       object file signing certificate NotAfter timestamp (if
exist)
  object_hashdb               hash database containing object file

Returned value:
  ignored

]]
```

```
local args = ...
```

Report di Controllo delle applicazioni dal Server adiacente

Viene invocata quando viene ricevuto un report di Controllo delle applicazioni per la postazione dal Server Dr.Web adiacente.

Database	Parametri	Valore restituito
è disponibile	• `neighborid` — ID del Server Dr.Web adiacente da cui è stato ricevuto l'evento, • `neighborname` — nome del Server Dr.Web adiacente, • `originatorid` — ID del Server Dr.Web che è la fonte dell'evento, • `originatorname` — nome del Server Dr.Web che è la fonte dell'evento, • `stationid` — ID della postazione, • `stationname` — nome della postazione, • `eventid` — ID dell'evento, • `event_time` — ora di comparsa dell'evento sulla postazione, • `sid` — SID della postazione, • `user` — utente che ha avviato il processo con un'attività sospetta, • `type` — tipo di evento, • `action` — azione applicata, • `policy_type` — tipo di criterio scattato, • `policy_mask` — maschera di criterio scattato, • `test_mode` — l'evento si è verificato in modalità test, • `profile_id` — UUID del profilo in base a cui è stato effettuato il blocco, • `profile_name` — nome del profilo in base a cui è stato effettuato il blocco, • `rule_id` — UUID della regola in base a cui è stato effettuato il blocco (se disponibile), • `rule_name` — nome della regola in base a cui è stato effettuato il blocco (se disponibile), • `process_path` — percorso del processo bloccato, • `process_file_sha256` — SHA-256 del file del processo, • `process_file_version` — versione del file del processo,	viene ignorato

Database	Parametri	Valore restituito
	• process_file_description — descrizione del file del processo, • process_file_origname — nome originale del file del processo, • process_file_prodname — nome del prodotto del file del processo, • process_file_prodver — versione del prodotto del file del processo, • process_file_company — nome dell'azienda del file del processo, • process_cert_thumbprint — impronta del certificato (SHA-1) con cui è firmato il processo (se disponibile), • process_cert_serial — numero di serie del certificato con cui è firmato il processo (se disponibile), • process_cert_issuer — emittente del certificato con cui è firmato il processo (se disponibile), • process_cert_subject — soggetto del certificato con cui è firmato il processo (se disponibile), • process_cert_timestamp — data di rilascio del certificato con cui è firmato il processo (se disponibile), • process_cert_not_before — data di entrata in vigore del certificato con cui è firmato il processo (se disponibile), • process_cert_not_after — data di scadenza del certificato con cui è firmato il processo (se disponibile), • process_hashdb — bollettino contenente l'hash del file del processo, • object_path — percorso dello script bloccato o un valore vuoto, • object_file_sha256 — SHA-256 del file dello script (se disponibile), • object_file_version — versione del file dello script (se disponibile), • object_file_description — descrizione del file dello script (se disponibile), • object_file_origname — nome originale del file dello script (se disponibile), • object_file_prodname — nome del prodotto del file dello script (se disponibile), • object_file_prodver — versione del prodotto del file dello script (se disponibile),	

Database	Parametri	Valore restituito
	• `object_file_company` — nome dell'azienda del file dello script (se disponibile), • `object_cert_thumbprint`— impronta del certificato (SHA-1) con cui è firmato lo script (se disponibile), • `object_cert_serial` — numero di serie del certificato con cui è firmato lo script (se disponibile), • `object_cert_issuer` — emittente del certificato con cui è firmato lo script (se disponibile), • `object_cert_subject` — soggetto del certificato con cui è firmato lo script (se disponibile), • `object_cert_timestamp` — data di rilascio del certificato con cui è firmato lo script (se disponibile), • `object_cert_not_before` — data di entrata in vigore del certificato con cui è firmato lo script (se disponibile), • `object_cert_not_after` — data di scadenza del certificato con cui è firmato lo script (se disponibile), • `object_hashdb` — bollettino contenente l'hash del file dello script	

Testo della procedura personalizzata:

```
--[[
Called:
  when application control event received from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  event_time          station time
  recv_time           server originator time
  sid                 SID of user initiated activity
  user                name of user initiated activity
  type                event type
  action              applied action
  policy_type         matched policy type
  policy_mask         matched policy mask
  test_mode           event occured in test mode
  profile_id          profile UUID used for activity blocking
  profile_name        profile name used for activity blocking
  rule_id             rule UUID used for activity blocking (if exist)
  rule_name           rule name used for activity blocking (if exist)
```

```
  process_path               path to affected process file
  process_file_sha256        process file SHA-256
  process_file_version       process file version
  process_file_description   process file description
  process_file_origname      process file original name
  process_file_prodname      process file product name
  process_file_prodver       process file product version
  process_file_company       process file company name
  process_cert_thumbprint    process file signing certificate thumbprint (SHA-1) (if
exist)
  process_cert_serial        process file signing certificate serial number (if exist)
  process_cert_issuer        process file signing certificate issuer (if exist)
  process_cert_subject       process file signing certificate subject (if exist)
  process_cert_timestamp     process file signing certificate sign issuance timestamp
(if exist)
  process_cert_not_before    process file signing certificate NotBefore timestamp (if
exist)
  process_cert_not_after     process file signing certificate NotAfter timestamp (if
exist)
  process_hashdb             hash database containing process file

  object_path                path to affected object file (script, etc) or empty
  object_file_sha256         object file SHA-256 (if exist)
  object_file_version        object file version (if exist)
  object_file_description    object file description (if exist)
  object_file_origname       object file original name (if exist)
  object_file_prodname       object file product name (if exist)
  object_file_prodver        object file product version (if exist)
  object_file_company        object file company name (if exist)
  object_cert_thumbprint     object file signing certificate thumbprint (SHA-1) (if
exist)
  object_cert_serial         object file signing certificate serial number (if exist)
  object_cert_issuer         object file signing certificate issuer (if exist)
  object_cert_subject        object file signing certificate subject (if exist)
  object_cert_timestamp      object file signing certificate sign issuance timestamp (if
exist)
  object_cert_not_before     object file signing certificate NotBefore timestamp (if
exist)
  object_cert_not_after      object file signing certificate NotAfter timestamp (if
exist)
  object_hashdb              hash database containing object file

Returned value:
  ignored

]]

local args = ...
```

Il Server proxy Dr.Web è stato creato

Viene invocata quando è stata completata la creazione di Server proxy Dr.Web.

Database	Parametri	Valore restituito
è disponibile	• `login` — nome utente dell'amministratore, • `id` — ID del Server proxy Dr.Web,	viene ignorato

Database	Parametri	Valore restituito

	• `name` — nome del Server proxy Dr.Web,
	• `state` — stato di completamento dell'operazione:
	  ▫ `0` — creato con successo,
	  ▫ `1` — errore durante l'esecuzione dell'operazione (errore di database),
	  ▫ `2` — il timeout dell'operazione è scaduto (il database è sovraccaricato),
	  ▫ `4` — Server proxy Dr.Web esiste già	

Testo della procedura personalizzata:

```
--[[
Called:
  when proxy create completed

Database:
  available

Parameters:
  login         administrator`s login name
  id            proxy ID
  name          proxy name
  state         operation completion state:
                  0  created successfully
                  1  operation failed (database error)
                  2  operation timed out (database overloaded)
                  4  already exists

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name, args.state
```

Il Server proxy Dr.Web è stato rimosso

Viene invocata quando viene rimosso il Server proxy Dr.Web.

Database	Parametri	Valore restituito
è disponibile	• `login` — nome utente dell'amministratore, • `id` — ID del Server proxy Dr.Web, • `name` — nome del Server proxy Dr.Web,	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when proxy deleted

Database:
  available

Parameters:
  login     administrator`s login name
  id        proxy id
  name      proxy name

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name
```

M5. Nuovi arrivi

Registrato il nuovo arrivo

Dopo che al nuovo arrivato è stato consentito l'accesso, ma prima che le relative informazioni vengano registrate nel database.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID provvisorio/permanente della postazione, • `address` — indirizzo di rete della postazione, • `station` — nome della postazione, • `existing` — conferma per la postazione esistente	viene ignorato

Testo della procedura personalizzata:

```
--[[
Database:
  available

Called:
  when newbie access granted but before information stored in database

Parameters:
  id              station temporary/permanent ID
  address         station network address
  station         station name
  existing        approved using existing station

Returned value:
  ignored

]]
```

```
local args = ... -- args.id, args.address, args.station
```

Nuovo arrivo si connette al Server Dr.Web

Viene invocata se il nuovo arrivato si connette al Server Dr.Web.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID provvisorio della postazione, • `address` — indirizzo di rete della postazione, • `station` — nome della postazione, • `description` — descrizione della postazione (solo per i client SO Windows), • `ldapdn` — LDAP DN della postazione (solo per i client SO Windows), • `sid` — SID della postazione, • `mac` — indirizzo MAC della postazione,	• `nil` — utilizza le impostazioni predefinite come nel funzionamento standard del Server Dr.Web, • `boolean` — azione del Server Dr.Web: ▫ `true` — richiedi la conferma manuale (simile a `Newbie approval`), ▫ `false` — nega l'accesso (simile a `Newbie closed`), • `string` — gruppo primario in caso di conferma: ▫ `empty` — conferma, imposta il gruppo `Everyone` come gruppo primario (simile a `Newbie open`), ▫ `not-empty` — conferma l'accesso e assegna come primario il gruppo con l'ID che corrisponde a questa stringa. Attenzione! L'esistenza di questo ID verrà controllata, e se non esiste, il gruppo

Database	Parametri	Valore restituito
		`Everyone` verrà assegnato come primario, • `vector` — conferma di default, contiene i seguenti comandi e argomenti facoltativi: ▫ `pgroup` — imposta il gruppo primario, quindi deve seguire l'ID del gruppo, ▫ `rate` — imposta il gruppo di tariffa, quindi deve seguire l'ID del gruppo di tariffa, ▫ `id` — imposta l'ID della postazione, quindi deve seguire l'ID della postazione, ▫ approve — richiedi la conferma manuale invece della conferma automatica, ▫ `into` — conferma nella postazione esistente, quindi deve seguire l'ID della postazione esistente

Testo della procedura personalizzata:

```
--[[
Called:
  when newbie connected

Database:
  available

Parameters:
  id             station temporary ID
  address        station network address
  station        station name
  description    station description (Windows client only)
```

```
  ldapdn          station LDAP DN (Windows client only)
  sid             station computer SID
  mac             station computer MAC

Returned value:
              nil         default, standard server operation according settings
  boolean     true        request approval (like 'Newbie approval' does)
              false       reject access (like 'Newbie closed' does)
  string      empty       accept, set primary group to 'Everyone'
                            (like 'Newbie open' does)
              not-empty   accept, set primary group to this string (ID) (substring after
space treated as rate group id)
                          Attention! Existence of This ID will be checked and
                          if it does not exist it will be replaced by `Everyone'
  vector                  accept by default, must contain commands and optional arguments:
                          "pgroup"  - set primary group, must be followed by group id
                          "rate"    - set rate group, must be followed by rate group id
                          "id"      - set station id, must be followed by station id
                          "approve" - request approval instead of accepting
                          "into"    - accept into existing station, must be followed by
existing station id


Procedure from next set will be called if returned nothing.
]]

local args = ... -- args.id, args.address, args.station

-- place my station (named ADMINISTRATOR) into `Everyone' group ignoring newbie policy
and newbie's preference
if string.upper( args.station ) == 'ADMINISTRATOR' then
  return ''
end

-- set new UUID for any station with this id and request for manual approve, useful for
cloned stations
if args.id == '01234567-89ab-cdef-0123-456789abcdef' then
  return { "id", dwcore.get_uuid(), "approve" }
end

-- no return => `nil' value => according server settings
```

Accettato il nuovo arrivo

Viene invocata se il nuovo arrivato ha ottenuto l'accesso, si è autenticato con successo e la postazione è stata creata nel database.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID provvisorio della postazione, • `address` — indirizzo di rete della postazione, • `station` — nome della postazione, • `compsid` — SID della postazione, • `compmac` — indirizzo MAC della postazione,	viene ignorato

Database	Parametri	Valore restituito
	• `description` — descrizione della postazione	

Testo della procedura personalizzata:

```
--[[
Called:
  when newbie access granted, authorization is successfull
  and station created in database

Database:
  available

Parameters:
  id              station temporary ID
  address         station network address
  station         station name
  compsid         station UID (SID on Windows)
  compmac         station MAC address
  description     station description

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.compsid, args.compmac,
args.description
```

M6. Relazioni

Arresto del componente su postazione di Server Dr.Web adiacente

Viene invocata alla ricezione dell'evento `component completed` dal Server Dr.Web adiacente.

Database	Parametri	Valore restituito
è disponibile	• `neighborid` — ID del Server Dr.Web adiacente da cui è stato ricevuto l'evento, • `neighborname` — nome del Server Dr.Web adiacente, • `originatorid` — ID del Server Dr.Web che è la fonte dell'evento, • `originatorname` — nome del Server Dr.Web che è la fonte dell'evento, • `stationid` — ID della postazione, • `stationname` — nome della postazione, • `eventid` — ID dell'evento,	viene ignorato

Database	Parametri	Valore restituito
	• `component` — numero del componente, • `pid` — ID del processo, • `infections` — sono state rilevate minacce, • `errors` — sono stati rilevati errori di accesso, • `exitcode` — codice di uscita del componente, • `time` — ora di fine (ora della postazione)	

Testo della procedura personalizzata:

```
--[[
Called:
  when "component completed" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           component number
  pid                 process ID
  infections          infections found
  errors              access errors detected
  exitcode            component exit code
  time                end time (station time)

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname, args.time
                 -- args.component, args.pid, args.infections
                 -- args.errors, args.exitcode
```

Avvio del componente su postazione di Server Dr.Web adiacente

Viene invocata alla ricezione dell'evento `component started` dal Server Dr.Web adiacente.

Database	Parametri	Valore restituito
è disponibile	• `neighborid` — ID del Server Dr.Web adiacente da cui è stato ricevuto l'evento, • `neighborname` — nome del Server Dr.Web adiacente, • `originatorid` — ID del Server Dr.Web che è la fonte dell'evento, • `originatorname` — nome del Server Dr.Web che è la fonte dell'evento, • `stationid` — ID della postazione, • `stationname` — nome della postazione, • `eventid` — ID dell'evento, • `component` — numero del componente, • `pid` — ID del processo, • `engine` — versione del motore di ricerca, • `records` — numero di record dei virus, • `user` — nome utente e gruppo del proprietario del processo, • `time` — ora di inizio (ora della postazione)	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when "component started" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           component number
  pid                 process ID
  engine              virus-finding engine version
  records             virus records number
  user                user name and group (process owner)
  time                start time (station time)

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
```

```
                -- args.originatorid, args.originatorname,
                -- args.eventid, args.stationid,
                -- args.stationname,
                -- args.component, args.pid, args.engine
                -- args.records, args.user, args.time
```

Sono cambiate le coordinate di Server Dr.Web adiacente o di una postazione di Server Dr.Web adiacente

Viene invocata alla ricezione dell'evento `geolocation` dal Server Dr.Web adiacente.

Database	Parametri	Valore restituito
è disponibile	• `neighborid` — ID del Server Dr.Web adiacente da cui è stato ricevuto l'evento, • `neighborname` — nome del Server Dr.Web adiacente, • `originatorid` — ID del Server Dr.Web che è la fonte dell'evento, • `originatorname` — nome del Server Dr.Web che è la fonte dell'evento, • `stationid` — ID della postazione, • `stationname` — nome della postazione, • `latitude` — latitudine in formato DD.DDDDDD, • `longitude` — longitudine in formato DD.DDDDDD	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when "geolocation" event received from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  latitude            latitude in DD.DDDDDD format
  longitude           longitude in DD.DDDDDD format

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
```

```
                -- args.eventid, args.stationid,
                -- args.stationname,
                -- args.latidue,args.longitude
                -- ...
```

Sono cambiati hardware e software su postazione di server adiacente

Viene invocata alla ricezione dell'evento `environment changed` dal Server Dr.Web adiacente.

Database	Parametri	Valore restituito
è disponibile	• `neighborid` — ID del Server Dr.Web adiacente da cui è stato ricevuto l'evento, • `neighborname` — nome del Server Dr.Web adiacente, • `originatorid` — ID del Server Dr.Web che è la fonte dell'evento, • `originatorname` — nome del Server Dr.Web che è la fonte dell'evento, • `stationid` — ID della postazione, • `stationname` — nome della postazione, • `eventid` — ID dell'evento, • `group_name` — nome del gruppo primario della postazione, • `category` — categoria di oggetto dell'ambiente	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when "environment changed" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  group_name          station primary group name
  category            environment category

Returned value:
  ignored

]]
```

```
local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,args.stationname,
                 -- args.group_name, args.category
```

Rilevata una minaccia alla sicurezza su una postazione di Server Dr.Web adiacente

Viene invocata alla ricezione dell'evento `virus detected` dal Server Dr.Web adiacente.

Database	Parametri	Valore restituito

è disponibile	• `neighborid` — ID del Server Dr.Web adiacente da cui è stato ricevuto l'evento,
	• `neighborname` — nome del Server Dr.Web adiacente,
	• `originatorid` — ID del Server Dr.Web che è la fonte dell'evento,
	• `originatorname` — nome del Server Dr.Web che è la fonte dell'evento,
	• `stationid` — ID della postazione,
	• `stationname` — nome della postazione,
	• `eventid` — ID dell'evento,
	• `component` — numero del componente,
	• `pid` — ID del processo,
	• `time` — ora del verificarsi dell'evento (ora della postazione),
	• `user` — nome utente e gruppo del proprietario del processo,
	• `object` — percorso dell'oggetto nel file system,
	• `owner` — nome utente e gruppo del proprietario dell'oggetto,
	• `action` — codice dell'operazione,
	• `objecttype` — tipo di oggetto:
	  ▫ `-1` sconosciuto
	  ▫ `0` file
	  ▫ `1` settore di avvio
	  ▫ `2` blocco di memoria o processo
	  ▫ `3` attività dei virus
	• `infectiontype` — tipo di minaccia (v. Dr.Web API),
	• `sha1` — hash SHA-1 dell'oggetto rilevato,
	• `sha256` — hash SHA-256 dell'oggetto rilevato,
		viene ignorato

Database	Parametri	Valore restituito
	• `hashdb` — bollettino contenente l'hash	

Testo della procedura personalizzata:

```
--[[
Called:
  when "" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           component number
  pid                 process ID
  time                event time (station time)
  user                user name and group (process owner)
  object              filesystem object path
  owner               object owner (user name and group)
  action              action code (see Dr.Web API; only errors bit set)
  objecttype          object type
                        -1    unknown
                         0    file
                         1    boot sector
                         2    memory block / process
                         3    virus like activity
  infectiontype       infection type (see Dr.Web API)
  sha1                object SHA-1 hash
  sha256              object SHA-256 hash
  hashdb              hash database containing object

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.component, args.pid, args.time, args.user,
                 -- args.object, args.owner,
                 -- args.action, args.objecttype, args.infectiontype,
                 -- args.sha1, args.sha256, args.hashdb
```

Report di Protezione preventiva dal Server adiacente

Viene invocata quando viene ricevuto un report di Protezione preventiva per la postazione dal Server Dr.Web adiacente.

Database	Parametri	Valore restituito
è disponibile	• `neighborid` — ID del Server Dr.Web adiacente da cui è stato ricevuto l'evento, • `neighborname` — nome del Server Dr.Web adiacente, • `originatorid` — ID del Server Dr.Web che è la fonte dell'evento, • `originatorname` — nome del Server Dr.Web che è la fonte dell'evento, • `stationid` — ID della postazione, • `stationname` — nome della postazione, • `eventid` — ID dell'evento, • `pid` — ID del processo, • `path` — percorso del file eseguibile del processo con un'attività sospetta, • `target_path` — percorso dell'oggetto protetto a cui è stato effettuato un tentativo di accesso, • `hips_type` — tipo di oggetto protetto (valore numerico), • `shell_guard_type` — motivo di blocco del codice non autorizzato (valore numerico), • `denied` — vietato accesso (`true` | `false`), • `is_user_action` — azione chiesta all'utente (`true` | `false`), • `event_count` — numero di eventi automaticamente vietati (solo se per `is_user_action` il valore è `false`), • `event_user` — utente che ha avviato il processo con un'attività sospetta, • `action_user` — utente che ha impostato una reazione a un'attività sospetta del processo (solo se per `is_user_action` il valore è `true`), • `event_time` — ora di comparsa dell'evento sulla postazione, • `recv_time` — ora di ricezione del report da parte del Server Dr.Web adiacente, • `sha1` — hash SHA-1 dell'oggetto rilevato, • `sha256` — hash SHA-256 dell'oggetto rilevato, • `hashdb` — bollettino contenente l'hash	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when HIPS event received from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  pid                 numeric,process id
  path                process file path
  target_path         affected resource path
  hips_type           numeric, HIPS type
  shell_guard_type    numeric, Shell Guard event type
  denied              boolean, access was denied
  is_user_action      boolean, user was asked
  event_count         event number (for accumulation period - if is_user_action is false)
  event_user          user which initiated the suspicious activity
  action_user         user which allowed or denied the activity (non-empty only if
is_user_action is true)
  event_time          station time
  recv_time           server originator time
  sha1                process file SHA-1 hash
  sha256              process file SHA-256 hash
  hashdb              hash database containing process file

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname, args.originatorid,
args.originatorname,
                 -- args.stationid, args.stationname, args.eventid
                 -- args.pid, args.path, args.target_path, args.hips_type,
args.shell_guard_type,
                 -- args.denied, args.is_user_action, args.event_count, args.event_user,
args.action_user
                 -- args.event_time, args.recv_time, args.sha1, args.sha256, args.hashdb
```

Errore di autenticazione sul Server Dr.Web adiacente

Viene invocata dopo che la connessione al Server Dr.Web adiacente è stata rifiutata a causa di errore di autenticazione.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID del Server Dr.Web, • `address` — indirizzo del Server Dr.Web, • `name` — nome del Server Dr.Web,	viene ignorato

Database	Parametri	Valore restituito
	• `reason` — causa di fallimento	

Testo della procedura personalizzata:

```
--[[
Called:
  just after server connection rejected due (authorization) error

Database:
  available

Parameters:
  id          server ID
  address     server address
  name        server name
  reason      failure reason

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.name, args.reason
```

Errore di scansione su postazione di Server Dr.Web adiacente

Viene invocata alla ricezione dell'evento `scan error` dal Server Dr.Web adiacente.

Database	Parametri	Valore restituito
è disponibile	• `neighborid` — ID del Server Dr.Web adiacente da cui è stato ricevuto l'evento, • `neighborname` — nome del Server Dr.Web adiacente, • `originatorid` — ID del Server Dr.Web che è la fonte dell'evento, • `originatorname` — nome del Server Dr.Web che è la fonte dell'evento, • `stationid` — ID della postazione, • `stationname` — nome della postazione, • `eventid` — ID dell'evento, • `component` — numero del componente, • `pid` — ID del processo, • `time` — ora del verificarsi dell'evento (ora della postazione), • `user` — nome utente e gruppo del proprietario del processo,	viene ignorato

Database	Parametri	Valore restituito
	• `object` — percorso dell'oggetto nel file system, • `owner` — nome utente e gruppo del proprietario dell'oggetto, • `action` — codice dell'operazione, • `sha1` — hash SHA-1 dell'oggetto rilevato, • `sha256` — hash SHA-256 dell'oggetto rilevato, • `hashdb` — bollettino contenente l'hash	

Testo della procedura personalizzata:

```
--[[
Called:
  when "" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           component number
  pid                 process ID
  time                event time (station time)
  user                user name and group (process owner)
  object              filesystem object path
  owner               object owner (user name and group)
  action              action code (error bit(s) set)
  sha1                object SHA-1 hash
  sha256              object SHA-256 hash
  hashdb              hash database containing object

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.component, args.pid, args.time, args.user,
                 -- args.object, args.owner, args.action,
                 -- args.sha1, args.sha256, args.hashdb
```

Il Server Dr.Web adiacente è connesso

Viene invocata alla connessione al Server Dr.Web adiacente.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID del Server Dr.Web, • `address` — indirizzo del Server Dr.Web, • `name` — nome del Server Dr.Web	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when server connected

Database:
  available

Parameters:
  id          server ID
  address     server address
  name        server name

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.name
```

Stato della postazione di Server Dr.Web adiacente

Viene invocata quando il Server Dr.Web adiacente comunica lo stato della postazione che include lo stato dei componenti, dei database dei virus e alcuni criteri locali (invio di eventi, ricezione di aggiornamenti e task).

Database	Parametri	Valore restituito
è disponibile	• `neighborid` — ID del Server Dr.Web adiacente da cui è stato ricevuto l'evento, • `neighborname` — nome del Server Dr.Web adiacente, • `originatorid` — ID del Server Dr.Web che è la fonte dell'evento, • `originatorname` — nome del Server Dr.Web che è la fonte dell'evento, • `stationid` — ID della postazione, • `stationname` — nome della postazione, • `eventid` — ID dell'evento, • `count` — numero di diversi codici di stato,	viene ignorato

Database	Parametri	Valore restituito
	• `state_0` — valore dello stato, • `number_0` — numero di postazioni in `state_0`	

Testo della procedura personalizzata:

```
--[[
Called:
  when "" event recived from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  count               number of different status code
  state_0             state value
  number_0            number of the stations in 'state_0'

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.count,
                 -- args.state_0, args.number_0
                 -- args.state_1, args.number_1
                 -- ...
```

È stata rimossa una postazione di Server Dr.Web adiacente

Viene invocata quando viene rimossa una postazione sul Server Dr.Web adiacente.

Database	Parametri	Valore restituito
è disponibile	• `neighborid` — ID del Server Dr.Web adiacente da cui è stato ricevuto l'evento, • `neighborname` — nome del Server Dr.Web adiacente, • `originatorid` — ID del Server Dr.Web che è la fonte dell'evento,	viene ignorato

Database	Parametri	Valore restituito
	• `originatorname` — nome del Server Dr.Web che è la fonte dell'evento, • `stationid` — ID della postazione, • `stationname` — nome della postazione	

Testo della procedura personalizzata:

```
--[[
Called:
  when station was deleted on neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname
                 -- ...
```

Statistiche di scansione su postazione di Server Dr.Web adiacente

Viene invocata alla ricezione dell'evento `scan statistics` dal Server Dr.Web adiacente.

Database	Parametri	Valore restituito
è disponibile	• `neighborid` — ID del Server Dr.Web adiacente da cui è stato ricevuto l'evento, • `neighborname` — nome del Server Dr.Web adiacente, • `originatorid` — ID del Server Dr.Web che è la fonte dell'evento, • `originatorname` — nome del Server Dr.Web che è la fonte dell'evento, • `stationid` — ID della postazione, • `stationname` — nome della postazione,	viene ignorato

Database	Parametri	Valore restituito
	• `eventid` — ID dell'evento, • `component` — numero del componente, • `pid` — ID del processo, • `user` — nome utente e gruppo del proprietario del processo, • `time` — ora del verificarsi dell'evento (ora della postazione), • `size` — dimensione totale di tutti gli oggetti scansionati, • `elapsedtime` — tempo impiegato, • `scanned` — numero di oggetti scansionati, • `infected` — numero di oggetti infettati da un virus conosciuto, • `modifications` — numero di oggetti infettati da una variante di virus, • `suspicious` — numero di oggetti sospetti, • `cured` — numero di file curati, • `deleted` — numero di file eliminati, • `renamed` — numero di file rinominati, • `moved` — numero di file trasferiti in quarantena, • `locked` — numero di file bloccati (solo SpIDer Guard), • `errors` — numero di file non scansionati a causa di errore di accesso	

Testo della procedura personalizzata:

```
--[[
Called:
  when "scan statistics" event received from neighbor server

Database:
  available

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  component           number of component
  pid                 process ID
  user                user name and group (process owner)
  time                event time (station time)
  size                summary size of all scanned objects
  elapsedtime         elapsed time
```

```
  scanned            number of scanned objects
  infected           number of objects infected by known virus
  modifications      number of objects infected by virus modification
  suspicious         number of suspicious objects
  cured              number of cured files
  deleted            number of deleted files
  renamed            number of renamed files
  moved              number of quarantined files
  locked             number of locked files (SpIDer Guard only)
  errors             number of not scanned files (due access error)

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.component, args.pid, args.time, args.user,
                 -- args.scanned, args.infected, args.modifications,
                 -- args.suspicious, args.cured, args.deleted, args.renamed,
                 -- args.moved, args.locked, args.errors, args.size, args.elapsedtime
```

Installazione di Agent dal Server Dr.Web adiacente

Viene invocata alla ricezione dell'evento `installation` dal Server Dr.Web adiacente.

Database	Parametri	Valore restituito

è disponibile	• `neighborid` — ID del Server Dr.Web adiacente da cui è stato ricevuto l'evento,
	• `neighborname` — nome del Server Dr.Web adiacente,
	• `originatorid` — ID del Server Dr.Web che è la fonte dell'evento,
	• `originatorname` — nome del Server Dr.Web che è la fonte dell'evento,
	• `stationid` — ID della postazione,
	• `stationname` — nome della postazione,
	• `eventid` — ID dell'evento,
	• `event` — tipo di evento:
	  ▫ `0` — l'installazione è iniziata,
	  ▫ `1` — l'installazione è stata completata con successo,
	  ▫ `2` — rifiuto,
	  ▫ `3` — il tempo è scaduto,
	  ▫ `4` — fallito,
	  ▫ `5` — non completato
		viene ignorato

Database	Parametri	Valore restituito
	• `message` — messaggio di errore (o vuoto se non è occorso nessun errore), • `address` — indirizzo della postazione, • `begtime` — ora di inizio (ora della postazione), • `endtime` — ora di fine	

Testo della procedura personalizzata:

```
--[[
Called:
  when "installation" event recived from neighbor server

Parameters:
  neighborid          neighbor server ID which the event received from
  neighborname        neighbor server name
  originatorid        ID of the event server originator
  originatorname      name of the event server originator
  stationid           station ID
  stationname         station name
  eventid             event ID
  event               event type:
                        0   installation begin
                        1   successully completed
                        2   rejected
                        3   timed out
                        4   failed
                        5   incomplete
  message             error message (or empty if there is no error)
  address             station address
  begtime             begin time
  endtime             end time

Returned value:
  ignored

]]

local args = ... -- args.neighborid, args.neighborname,
                 -- args.originatorid, args.originatorname,
                 -- args.eventid, args.stationid,
                 -- args.stationname,
                 -- args.event, args.message, args.address
                 -- args.begtime, args.endtime
```

M7. Server

Caricato il file binario di Server Dr.Web

Viene invocata dopo il caricamento del file binario del Server Dr.Web per l'esecuzione di alcune funzioni di manutenzione (il Server Dr.Web non servirà i client).

Database	Parametri	Valore restituito
non è disponibile	no	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when server binary file loaded for execute some service function
  (the server will not serve clients)

Database:
  NOT available

Parameters:
  none

Returned value:
  ignored

]]
```

La verifica del database è stata completata

Viene invocata dopo il completamento della verifica del database.

Database	Parametri	Valore restituito
non è disponibile	• `state` — stato di completamento: ▫ `true` — con successo, ▫ `false` — fallito	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when database verification completed

Database:
  NOT available
```

```
Parameters:
  state     true   success
                   failed

Returned value:
  ignored

]]

local args = ... -- args.state
```

Limite di licenza raggiunto (connessione non stabilita)

Viene invocata quando non è possibile connettersi al client a causa di limitazione di licenza. Dopo la disconnessione viene invocato `bad_connection.ds`.

Database	Parametri	Valore restituito
è disponibile	• `reason` — causa di errore di connessione: ▫ `connection` — non ci sono licenze disponibili, ▫ `database` — errore di creazione della nuova postazione nel database in quanto non ci sono più licenze disponibili	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when new client connection cannot be established due license limitation

Database:
  available

Parameters:
  reason     "connection"   no free license
             "database"     cannot create new station in database due
                            no free license

Returned value:
  ignored

]]

local args = ... -- args.reason
```

Completamento di alcune funzioni del Server Dr.Web

Viene invocata dopo che il Server Dr.Web ha finito di eseguire alcune funzioni di manutenzione (il Server Dr.Web non servirà i client).

Database	Parametri	Valore restituito
non è disponibile	no	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when server completed execute some service function
  (the server did not serve clients)

Database:
  NOT available

Parameters:
  none

Returned value:
  ignored

]]
```

Il driver del database è stato caricato

Viene invocata dopo che è stato completato il processo di caricamento del driver del database.

Database	Parametri	Valore restituito

non è disponibile	• `state` — stato di completamento:
	  ▫ `true` — caricamento riuscito,
	  ▫ `false` — errore di caricamento,
	• `driver` — nome del driver del database,
	• `library` — percorso completo della libreria del driver del database,
	• `message` — testo del messaggio di errore se lo stato è `false`
		viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when database driver load process completed

Database:
  NOT available

Parameters:
  state     true     successful load
            false    load failed
  driver             database driver name
  library            full path to database driver library
  message            error message text when state is 'false'

Returned value:
  ignored

]]

local args = ... -- args.state, args.driver, args.library, args.message
```

Eseguito un task sul Server Dr.Web

Viene invocata dopo che il task è stato eseguito sul Server Dr.Web.

Database	Parametri	Valore restituito

è disponibile	• `id` — ID del Server Dr.Web,
	• `done` — stato di completamento:
	  ▫ `true` — eseguito con successo,
	  ▫ `false` — esecuzione fallita,
	• `time` — tempo di completamento del task,
	• `name` — nome del task,
	• `error` — messaggio dal log di esecuzione
		viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when job executed on the server

Database:
  available

Parameters:
  id                server ID
  done      true    executed successfully
            false   execution failed
```

```
  time              job completion time
  name              job name
  error             error or other message

Returned value:
  ignored

]]

local args = ... -- args.id, args.done, args.name, args.time, args.error
```

Modulo di protocollo scaricato dalla memoria

Viene invocata se il modulo di protocollo viene scaricato dalla memoria.

Database	Parametri	Valore restituito
non è disponibile	• `name` — nome interno del modulo di protocollo, • `path` — percorso del file del modulo di protocollo	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when protocol module unloaded

Database:
  NOT available

Parameters:
  name                    protocol name
  path                    path to protocol module file

Returned value:
  ignored

]]

local args = ... -- args.path
```

Caricato il modulo di protocollo

Viene invocata dopo il caricamento del modulo di protocollo.

Database	Parametri	Valore restituito
non definito	• `path` — percorso del file del modulo di protocollo,	viene ignorato

Database	Parametri	Valore restituito

	• `name` — nome interno del modulo di protocollo,
	• `desc` — descrizione del modulo di protocollo,
	• `state` — stato:
	  ▫ `loaded` — il modulo di protocollo è stato caricato con successo,
	  ▫ `disabled` — l'utilizzo del modulo di protocollo è disattivato nel file `drwcsd.conf`,
	• `error` — testo del messaggio di errore se lo stato è `invalid`	

Testo della procedura personalizzata:

```
--[[
Called:
  when protocol module loaded

Parameters:
  path                    path to protocol module file
  name                    internal protocol name
  desc                    protocol module description string
  state      "loaded"     protocol module loaded successfully
             "disabled"   protocol module is disabled in drwcsd.conf
             "invalid"    invalid protocol module format
  error                   error message if state is "invalid"

Returned value:
  ignored

]]

local args = ... -- args.state, args.path, args.name
```

Estensione scaricata dalla memoria

Viene invocata se il modulo di estensione viene scaricato dalla memoria.

Database	Parametri	Valore restituito
non è disponibile	• `name` — nome dell'estensione, • `path` — percorso del file dell'estensione	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when plugin module unloaded

Database:
  NOT available

Parameters:
  name                    plugin name
  path                    path to plugin file

Returned value:
  ignored

]]

local args = ... -- args.name, yargs.path
```

Caricata l'estensione

Viene invocata dopo il caricamento del modulo di estensione.

Database	Parametri	Valore restituito

non è disponibile	• `path` — percorso del file dell'estensione,
	• `name` — nome interno dell'estensione,
	• `desc` — descrizione dell'estensione,
	• `state` — stato:
	  ▫ `loaded` — l'estensione è stata caricata con successo,
	  ▫ `disabled` — l'utilizzo dell'estensione è disattivato nel file `drwcsd.conf`,
	  ▫ `invalid` — formato di estensione non valido,
	• `error` — testo del messaggio di errore se lo stato è `invalid`
		viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when plugin module loaded
```

```
Database:
  NOT available

Parameters:
  path                    path to plugin file
  name                    internal plugin name
  desc                    plugin description string
  state      "loaded"     plugin loaded successfully
             "disabled"   plugin is disabled in drwcsd.conf
             "invalid"    invalid plugin format
  error                   error message if state is "invalid"

Returned value:
  ignored

]]


local args = ... -- args.state, args.path, args.name, args.error
```

Copiatura di backup

Viene invocata dopo il completamento del backup di file, ma prima della rimozione dei file di backup precedenti.

Database	Parametri	Valore restituito
è disponibile	• `state` — stato di completamento: ▫ `true` — con successo, ▫ `false` — fallito	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when backup completed but before deleting previous backup files

Database:
  available

Parameters:
  state  true  successful
         false failed

Returned value:
  ignored

]]

local args = ... -- args.state
```

Il Server Dr.Web sta completando il servizio

Viene invocata quando il Server Dr.Web completa il servizio dei client.

Database	Parametri	Valore restituito
non è disponibile	no	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when server completed serve clients

Database:
  NOT available

Parameters:
  none

Returned value:
  ignored

]]
```

Il Server Dr.Web è in esecuzione e pronto

Viene invocata se il Server Dr.Web è stato avviato ed è pronto a servire i client.

Database	Parametri	Valore restituito
non è disponibile	no	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when server started and going to serve clients

Database:
  NOT available

Parameters:
  none

Returned value:
  ignored

]]
```

M8. Connessioni

Limite di licenza raggiunto (connessione rifiutata)

Viene invocata se la connessione è stata rifiutata in base alle limitazioni del contratto di licenza.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo di rete della postazione, • `station` — nome NetBIOS della postazione. Non viene sostituito con il nome DNS, • `type` — tipo `station`	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when connection denied according license limitation

Database:
  available

Parameters:
  id              station ID
  address         station network address
  station         station name
                  this is NetBIOS station name (not replaced by DNS one)
  type            one of 'station'

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.type

-- no return => `nil' value
```

Errore di connessione

Viene invocata se non è possibile stabilire la connessione al nuovo client.
Possibili cause: sono esaurite le licenze (prima viene invocato `license_error.ds`), nessuna connessione al database, errore di database, superato il numero di postazioni in attesa di autenticazione, server o database sovraccaricato.

Database	Parametri	Valore restituito
è disponibile se la causa è `no license`, ed è potenzialmente disponibile se la causa è `overload` (non è consigliato utilizzare il database in questo tempo)	• `address` — indirizzo del client, • `reason` — causa di errore di connessione: ▫ `no database` — non stabilita la connessione al database, ▫ `overload` — il database è sovraccaricato, ▫ `no license` — non ci sono più licenze disponibili per accettare la connessione	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when new client connection cannot be established

Database:
  available if reason is "no license" and potentialy available if
  reason is "overload" (but it is not recommended to use DB that time)

Parameters:
  address                  client address
  reason   "no database"   no established database connection
           "overload"      database is overloaded
           "no license"    no free license to accept connection

Returned value:
  ignored

]]

local args = ... -- args.address, args.reason
```

Ricevuto PONG da client

Viene invocata se viene ricevuto un PONG dal client.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID del client, • `address` — indirizzo di rete del client, • `station` — nome del client (per Agent, Server, Installer), • `time` — tempo di ritorno (round-trip) del pacchetto	viene ignorato

Testo della procedura personalizzata:

```
--[[
```

```
Called:
  when 'PONG' received from client

Database:
  available

Parameters:
  id          client ID
  address     network address
  station     station name (for Agent, Server, Installer)
  time        packet round-trip time in milliseconds

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station,
                 -- args.time
```

Il client si è disconnesso

Viene invocata dopo la disconnessione del client.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID del client, • `address` — indirizzo di rete del client, • `type` — tipo del client: `unknown`, `station`, `console`, `server`, `installer`, `newbie` • `station` — nome della postazione (solo per Agent), • `bytesin` — ricevuti byte non compressi, • `bytesout` — inviati byte non compressi, • `totalbytesin` — ricevuti byte compressi, • `totalbytesout` — inviati byte compressi, • `reason` — causa di disconnessione	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when client disconnected

Database:
  available

Parameters:
  id              client ID
  address         network address
  type            client type: "unknown", "station", "proxy",
                               "server", "installer", "newbie"
  station         station name (only for Agent)
  bytesin         bytes received
  bytesout        bytes sent
  totalbytesin    compressed bytes received
  totalbytesout   compressed bytes sent
  reason          disconnect reason

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.type, args.station
                 -- args.bytesin, args.bytesout
                 -- args.totalbytesin, args.totalbytesout
                 -- args.reason
```

M9. Postazioni

L'Agent è stato disinstallato

Viene invocata dopo che la rimozione di Agent è stata completata.

Database	Parametri	Valore restituito

è disponibile	• `login` — nome utente dell'amministratore,
	• `state` — stato di completamento:
	  ▫ `true` — con successo,
	  ▫ `false` — fallito,
	• `id` — ID della postazione,
	• `address` — indirizzo della postazione,
	• `station` — nome della postazione,
	• `message` — vuoto se lo stato è `true`, altrimenti contiene un messaggio di errore
		viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when deinstallation of Agent completed

Database:
  available

Parameters:
  login           login name of administrator
  state           true    success
                  false   failed
  id                      station ID
  address                 station address
  station                 station name
  message                 empty if state is 'true' or contains error message

Returned value:
  ignored

]]

local args = ... -- args.login, args.state, args.id
                 -- args.address, args.station, args.message
```

Arresto del componente su postazione

Viene invocata alla ricezione dell'evento `component completed` dall'Agent.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo della postazione, • `station` — nome della postazione, • `component` — numero del componente, • `pid` — ID del processo, • `infections` — sono state rilevate minacce, • `errors` — sono stati rilevati errori di accesso, • `exitcode` — codice di uscita del componente,	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when "component completed" event received from Agent

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  component   component number
  pid         process ID
  infections  infections found
  errors      access errors detected
  exitcode    component exit code

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.exitcode, args.infections, args.errors
```

Il task è stato eseguito

Viene invocata alla ricezione dell'evento `job executed` dall'Agent.

Database	Parametri	Valore restituito

è disponibile	• `id` — ID della postazione,
	• `address` — indirizzo della postazione,
	• `station` — nome della postazione,
	• `done` — stato di esecuzione:
	  ▫ `true` — eseguito con successo,
	  ▫ `false` — esecuzione fallita,
	• `time` — tempo di completamento del task,
	• `name` — nome del task,
	• `error` — messaggio di errore o di stato
		viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when "job executed" event received from Agent

Database:
  available

Parameters:
  id                station ID
  address           station address
  station           station name
  done      true    executed successfully
            false   execution failed
  time              job completion time
  name              job name
  job               job ID (empty for Agent prior version 11 (protocol 3.1+))
  error             error or other message

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.done,
                 -- args.name, args.job, args.time, args.error
```

Avvio del componente su postazione

Viene invocata alla ricezione dell'evento `component started` dall'Agent.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo della postazione, • `station` — nome della postazione, • `component` — numero del componente, • `pid` — ID del processo, • `engine` — versione del motore di ricerca, • `records` — numero di record dei virus, • `user` — nome utente e gruppo del proprietario del processo, • `time` — ora di inizio (ora della postazione)	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when "component started" event received from Agent

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  component   component number
  pid         process ID
  engine      virus-finding engine version
  records     virus records number
  user        user name and group (process owner)
  time        start time (station time)

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.records, args.user, args.time, args.engine
```

È cambiata la posizione geografica di una postazione

Viene invocata quando è cambiata la posizione geografica di una postazione.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo della postazione, • `station` — nome della postazione, • `latitude` — latitudine della postazione in formato DD.DDDDDD, • `longitude` — longitudine della postazione in formato DD.DDDDDD	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when agent geolocation changed

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  latitude    station latitude in DD.DDDDDD format
  longitude   station longitude in DD.DDDDDD format

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.name, args.latitude, args.longitude
```

È necessario riavviare la postazione

Viene invocata dopo che il Server Dr.Web ha ricevuto il messaggio `reboot required` dalla postazione.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo di rete della postazione, • `station` — nome NetBIOS della postazione. Non viene sostituito con il nome DNS,	viene ignorato

Database	Parametri	Valore restituito
	• `product` — ID del prodotto, • `description` — descrizione del prodotto, • `from_revision` — numero della revisione corrente, • `to_revision` — numero della revisione nuova, • `from_revision_date` — data della revisione corrente, • `to_revision_date` — data della revisione nuova	

Testo della procedura personalizzata:

```
--[[
Called:
  after server received 'reboot required' station message.

Database:
  available

Parameters:
  id                  station ID
  address             station network address
  station             station name (this is NetBIOS station name not replaced by DNS
one)
  product             product ID
  description         product description
  from_revision       current revision number
  to_revision         new revision number
  from_revision_date  current revision date
  to_revision_date    new revision date

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.product, args.description,
args.from_revision, args.to_revision, args.from_revision_date, args.to_revision_date
```

È stata rilevata una minaccia alla sicurezza della postazione

Viene invocata alla ricezione dell'evento `virus detected` dall'Agent.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione,	viene ignorato

Database	Parametri	Valore restituito

	• `address` — indirizzo della postazione,
	• `station` — nome della postazione,
	• `component` — numero del componente,
	• `pid` — ID del processo,
	• `time` — ora del verificarsi dell'evento (ora della postazione),
	• `user` — nome utente e gruppo del proprietario del processo,
	• `object` — percorso dell'oggetto nel file system,
	• `owner` — nome utente e gruppo del proprietario dell'oggetto,
	• `virus` — nome del virus,
	• `action` — codice dell'operazione,
	• `objecttype` — tipo di oggetto:
	  ▫ `-1` sconosciuto,
	  ▫ `0` file,
	  ▫ `1` —settore di avvio,
	  ▫ `2` —blocco di memoria o processo,
	  ▫ `3` —attività dei virus
	• `infectiontype` — tipo di minaccia (v. Dr.Web API),
	• `compsid` — SID della postazione,
	• `compmac` — indirizzo MAC della postazione,
	• `description` — descrizione della postazione,
	• `compdn` — LDAP DN della postazione (solo per i client SO Windows),
	• `sha1` — hash SHA-1 dell'oggetto rilevato,	

Database	Parametri	Valore restituito
	• `sha256` — hash SHA-256 dell'oggetto rilevato, • `hashdb` — bollettino contenente l'hash	

Testo della procedura personalizzata:

```
--[[
Called:
  when "virus detected" event received from Agent

Database:
  available

Parameters:
  id                station ID
  address           station address
  station           station name
  component         component number
  pid               process ID
  time              event time (station time)
  user              user name and group (process owner)
  object            filesystem object path
  owner             object owner (user name and group)
  virus             virus name
  action            action code (see Dr.Web API; only errors bit set)
  objecttype        object type
                      -1    unknown
                       0    file
                       1    boot sector
                       2    memory block / process
                       3    virus like activity
  infectiontype     infection type (see Dr.Web API)
  compsid           computer sid
  compmac           computer MAC
  description       computer description
  compdn            computer LDAP DN
  sha1              object SHA-1 hash
  sha256            object SHA-256 hash
  hashdb            hash database containing object

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.time, args.user, args.object, args.owner,
                 -- args.virus, args.action, args.objecttype, args.infectiontype
                 -- args.compsid, args.compmac, args.description, args.compdn
                 -- args.sha1, args.sha256, args.hashdb
```

Report di Protezione preventiva

Viene invocata quando viene ricevuto un report di Protezione preventiva dalla postazione.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo della postazione, • `station` — nome della postazione, • `time` — ora di comparsa dell'evento sulla postazione, • `pid` — ID del processo, • `path` — percorso del file eseguibile del processo con un'attività sospetta, • `target_path` — percorso dell'oggetto protetto a cui è stato effettuato un tentativo di accesso, • `hips_type` — tipo di oggetto protetto (valore numerico), • `shell_guard_type` — motivo di blocco del codice non autorizzato (valore numerico), • `denied` — vietato accesso (true | false), • `is_user_action` — azione chiesta all'utente (`true` | `false`), • `event_count` — numero di eventi automaticamente vietati (solo se per `is_user_action` il valore è `false`), • `event_user` — utente che ha avviato il processo con un'attività sospetta, • `action_user` — utente che ha impostato una reazione a un'attività sospetta del processo (solo se per `is_user_action` il valore è `true`), • `sha1` — hash SHA-1 dell'oggetto rilevato,	viene ignorato

Database	Parametri	Valore restituito
	• `sha256` — hash SHA-256 dell'oggetto rilevato, • `hashdb` — bollettino contenente l'hash	

Testo della procedura personalizzata:

```
--[[
Called:
  when HIPS event received from Agent

Database:
  available

Parameters:
  id                  station ID
  address             station address
  station             station name
  time                station time
  pid                 numeric,process id
  path                process file path
  target_path         affected resource path
  hips_type           numeric, HIPS type
  shell_guard_type    numeric, Shell Guard event type
  denied              boolean, access was denied
  is_user_action      boolean, user was asked
  event_count         event number (for accumulation period - if is_user_action is false)
  event_user          user which initiated the suspicious activity
  action_user         user which allowed or denied the activity (non-empty only if
is_user_action is true)
  sha1                process file SHA-1 hash
  sha256              process file SHA-256 hash
  hashdb              hash database containing process file

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.time,
                 -- args.pid, args.path, args.target_path, args.hips_type,
args.shell_guard_type,
                 -- args.denied, args.is_user_action, args.event_count, args.event_user,
args.action_user
                 -- args.sha1, args.sha256, args.hashdb
```

Errore di autenticazione della postazione

Viene invocata dopo che la connessione all'Agent è stata rifiutata a causa di errore di autenticazione.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo della postazione, • `station` — nome della postazione, • `reason` — causa di fallimento, • `type` — uno dei `station`, `installer`, `proxy`, • `compsid` — SID della postazione, • `compmac` — indirizzo MAC della postazione, • `description` — descrizione della postazione	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  just after Agent connection rejected due authorization error

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  reason      failure reason
  type        one of 'station' | 'installer' | 'proxy'
  compsid     station UID (SID on Windows)
  compmac     station MAC address
  description station description

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.reason, args.type,
args.compsid, args.compmac, args.description
```

Errore di data/ora sulla postazione

Viene invocata al rilevamento sulla postazione di un'ora/una data non valida.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo della postazione, • `station` — nome della postazione, • `now` — ora sul Server Dr.Web (in millisecondi), • `time` — ora sulla postazione (in millisecondi), • `valid_delta` — differenza di ora ammissibile (in millisecondi),	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when invalid station time/date detected

Database:
  available

Parameters:
  id              station ID
  address         station address
  station         station name
  now             server time (in milliseconds)
  time            station time (in milliseconds)
  valid_delta     valid time delta (in milliseconds)

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station
                 -- args.now, args.date, args.valid_delta
```

Errore di aggiornamento della postazione

Viene invocata dopo che il Server Dr.Web ha ricevuto il messaggio `update failed` dalla postazione.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo di rete della postazione,	viene ignorato

Database	Parametri	Valore restituito
	• `station` — nome NetBIOS della postazione. Non viene sostituito con il nome DNS, • `product` — ID del prodotto, • `description` — descrizione del prodotto, • `from_revision` — numero della revisione corrente, • `to_revision` — numero della revisione nuova, • `from_revision_date` — data della revisione corrente, • `to_revision_date` — data della revisione nuova	

Testo della procedura personalizzata:

```
--[[
Called:
  after server received 'update failed' station message.

Database:
  available

Parameters:
  id                  station ID
  address             station network address
  station             station name (this is NetBIOS station name not replaced by DNS
one)
  product             product ID
  description         product description
  from_revision       current revision number
  to_revision         new revision number
  from_revision_date  current revision date
  to_revision_date    new revision date

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.product, args.description,
args.from_revision, args.to_revision, args.from_revision_date, args.to_revision_date
```

Errore di scansione su postazione

Viene invocata alla ricezione dell'evento `scan error` dall'Agent.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo della postazione, • `station` — nome della postazione, • `component` — numero del componente, • `pid` — ID del processo, • `time` — ora del verificarsi dell'evento (ora della postazione), • `user` — nome utente e gruppo del proprietario del processo, • `object` — percorso dell'oggetto nel file system, • `owner` — nome utente e gruppo del proprietario dell'oggetto, • `action` — codice dell'operazione, • `compsid` — SID della postazione, • `compmac` — indirizzo MAC della postazione, • `description` — descrizione della postazione, • `ldapdn` — LDAP DN della postazione (solo per i client SO Windows), • `sha1` — hash SHA-1 dell'oggetto rilevato, • `sha256` — hash SHA-256 dell'oggetto rilevato, • `hashdb` — bollettino contenente l'hash	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when "scan error" event received from Agent

Database:
  available
```

```
Parameters:
  id                station ID
  address           station address
  station           station name
  component         component number
  pid               process ID
  time              event time (station time)
  user              user name and group (process owner)
  object            filesystem object path
  owner             object owner (user name and group)
  action            action code (error bit(s) set)
  compsid           computer SID
  compmac           computer MAC
  description       computer description
  ldapdn            computer LDAP DN
  sha1              object SHA-1 hash
  sha256            object SHA-256 hash
  hashdb            hash database containing object

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.time, args.user, args.object, args.owner,
                 -- args.action, args.compsid, args.compmac, args.description,
args.ldapdn
                 -- args.sha1, args.sha256, args.hashdb
```

La lista dei componenti è stata ricevuta

Viene invocata quando l'Agent comunica la lista dei componenti installati.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo della postazione, • `station` — nome della postazione, • `count` — numero di componenti segnalati, • `component_0` — nome componente, • `time_0` — ora di installazione, • `from_0` — fonte di installazione (indirizzo del Server Dr.Web, MSI ecc.), • `path_0` — percorso di installazione	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when Agent reported installed components

Database:
  available

Parameters:
  id                  station ID
  address             station address
  station             station name
  count               number of components reported
  component_0         component name
  time_0              installation time
  from_0              installation source (server address, MSI, etc)
  path_0              installation path

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.count
                 -- args.component_0, args.time_0, args.from_0, args.path_0
                 -- args.component_1, args.time_1, args.from_1, args.path_1
                 -- ...
```

Ricevute le informazioni sui database dei virus

Viene invocata quando l'Agent invia informazioni sui database dei virus.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo della postazione, • `station` — nome della postazione, • `count` — numero di database dei virus, • `name_0` — nome del file del database dei virus, • `md5_0` — MD5 del file del database dei virus, • `version_0` — versione del database dei virus, • `issued_0` — data e ora di rilascio del database dei virus,	viene ignorato

Database	Parametri	Valore restituito
	• `records_0` — numero di record nel database dei virus, • `type_0` — tipo di database dei virus	

Testo della procedura personalizzata:

```
--[[
Called:
  when Agent sent virus bases information

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  count       number of found virus bases
  name_0      virus base file name
  md5_0       virus base file MD5
  version_0   virus base version
  issued_0    virus base issue date and time
  records_0   number of records
  type_0      virus base type

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.count,
                 -- args.name_0, args.md5_0, args.version_0,
                 -- args.issued_0, args.records_0, args.type_0,
                 -- args.name_1, args.md5_1, args.version_1,
                 -- args.issued_1, args.records_1, args.type_1,
                 -- ...
```

Stato della postazione

Viene invocata quando l'Agent comunica lo stato dei componenti, dei database dei virus e di alcuni criteri locali (invio di eventi, ricezione di aggiornamenti e task).

Database	Parametri	Valore restituito
è disponibile	• `events` — messaggio di eventi: ▫ `true` — l'Agent invia informazioni su eventi,	viene ignorato

Database	Parametri	Valore restituito
	▫ `false` — l'Agent non invia informazioni su eventi, • `jobs` — accettazione di task (secondo il calendario e scansioni remote): ▫ `true` — l'Agent accetta task, ▫ `false` — l'Agent non accetta task, • `updates` — ricezione di aggiornamenti: ▫ `true` — l'Agent riceve aggiornamenti, ▫ `false` — l'Agent non riceve aggiornamenti	

Testo della procedura personalizzata:

```
--[[
Called:
  when Agent report its local policy

Database:
  available

Parameters:
  events    true     Agent send events
            false    Agent do not send events
  jobs      true     Agent accept jobs (schedule & remote scan)
            false    Agent do not accept jobs
  updates   true     Agent accept updates
            false    Agent do not accept updates


Returned value:
  ignored

]]

local args = ... -- args.events, args.jobs, args.updates
```

La postazione viene autenticata

Viene invocata se la postazione cerca di autenticarsi (l'ID e la password sono già stati verificati, sono validi e conosciuti).

Database	Parametri	Valore restituito

è disponibile	• `id` — ID della postazione,
	• `connected` — controllo della presenza di postazioni con questo ID già connesse al Server Dr.Web:
	  ▫ `true` — un'altra postazione con questo ID è già connessa al Server Dr.Web,
	  ▫ `false` — non vi sono altre postazioni con questo ID connesse,
	• `current_address` — indirizzo di rete della postazione con questo ID già connessa (non è vuoto solo se `connected` assume il valore `true`),
	• `current_name` — nome della postazione con questo ID già connessa,
	• `last_address` — indirizzo di rete della postazione con questo ID all'ultima connessione,
	• `last_time` — ora dell'ultima comparsa della postazione con questo ID,
	• `last_server` — Server Dr.Web della postazione con questo ID alla sua ultima connessione,
	• `new_name` — nome della postazione che si connette,
	• `new_address` — indirizzo di rete della postazione che si connette
		• `string` — risultato della richiesta di connessione della postazione
		• `nil` — comportamento predefinito del Server Dr.Web
		• `deny` — nega l'autenticazione della postazione
		• `force` — consenti l'autenticazione anche se un'altra postazione con questo ID è già connessa (scollega la postazione connessa)
		• `newbie` — resetta la postazione in nuovi arrivi

Testo della procedura personalizzata:

```
--[[
Called:
  when station tries to authorize (id and password already checked, valid and known)

Database:
  available

Parameters:
```

```
  id                      station ID
  connected       true    station with same ID already connected to server
                  false   no any station with same ID connected
  current_address         already connected station network address (not empty only if
'connected' is true)
  current_name            last connected station name
  last_address            last disconnected station network address
  last_time               last disconnected station seen time
  last_server             last connected station server
  new_name                now connecting station name
  new_address             now connecting station network address

Returned value:
          nil             default server behavior
  string  'deny'          deny authorization for station
          'force'         allow authorization even if other station with same ID already
connected (by disconnecting it)
          'newbie'        reset station to newbie

Procedure from next set will be called if returned nothing.
]]

local args = ... -- args.id, args.connected, args.current_address, args.current_name,
args.last_address,
                 -- args.last_time, args.last_server, args.new_name, args.new_address

-- no return => `nil' value
```

La postazione è connessa

Viene invocata se l'Agent si è connesso con successo.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo della postazione, • `station` — nome della postazione, • `os` — SO della postazione, • `platform` — piattaforma della postazione, • `compsid` — SID della postazione, • `compmac` — indirizzo MAC della postazione, • `description` — descrizione della postazione	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when Agent connected successfully

Database:
  available

Parameters:
  id          station ID
  address     station address
  station     station name
  os          station os
  platform    station platform
  compsid     station UID (Security ID on Windows)
  compmac     station MAC address
  description station description

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.name, args.os, args.platform,
args.compsid, args.compmac, args.description
```

La postazione è stata creata

Viene invocata quando è stata completata la creazione di una postazione.

Database	Parametri	Valore restituito

è disponibile	• `login` — nome utente dell'amministratore,
	• `id` — ID della postazione,
	• `name` — nome della postazione,
	• `state` — stato di completamento dell'operazione:
	  ▫ `0` — creata con successo,
	  ▫ `1` — errore durante l'esecuzione dell'operazione (errore di database),
	  ▫ `2` — il timeout dell'operazione è scaduto (il database è sovraccaricato),
	  ▫ `3` — non ci sono licenze disponibili,
	  ▫ `4` — la postazione esiste già
		viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when station create completed

Database:
  available

Parameters:
  login         administrator`s login name
  id            station ID
  name          station name
  state         operation completion state:
                  0  created successfully
                  1  operation failed (database error)
                  2  operation timed out (database overloaded)
                  3  no free license
                  4  already exists

Returned value:
  ignored

]]

local args = ... -- args.login, args.id, args.name, args.state
```

La postazione è stata rimossa

Viene invocata alla rimozione della postazione.

Database	Parametri	Valore restituito
è disponibile	• `login` — nome utente dell'amministratore, • `id` — ID della postazione	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when station deleted

Database:
  available

Parameters:
  login     administrator`s login name
  id        station id

Returned value:
  ignored

]]
```

```
local args = ... -- args.login, args.id
```

Statistiche di scansione su postazione

Viene invocata alla ricezione dell'evento `scan statistics` dall'Agent.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo della postazione, • `station` — nome della postazione, • `component` — numero del componente, • `pid` — ID del processo, • `user` — nome utente e gruppo del proprietario del processo, • `time` — ora del verificarsi dell'evento (ora della postazione), • `size` — dimensione totale di tutti gli oggetti scansionati, • `elapsedtime` — tempo impiegato, • `scanned` — numero di oggetti scansionati, • `infected` — numero di oggetti infettati da un virus conosciuto, • `modifications` — numero di oggetti infettati da una variante di virus, • `suspicious` — numero di oggetti sospetti, • `cured` — numero di file curati, • `deleted` — numero di file eliminati, • `renamed` — numero di file rinominati, • `moved` — numero di file trasferiti in quarantena, • `locked` — numero di file bloccati (solo SpIDer Guard),	viene ignorato

Database	Parametri	Valore restituito
	• `errors` — numero di file non scansionati a causa di errore di accesso	

Testo della procedura personalizzata:

```
--[[
Called:
  when "scan statistics" event received from Agent

Database:
  available

Parameters:
  id                  station ID
  address             station address
  station             station name
  component           number of component
  pid                 process ID
  user                user name and group (process owner)
  time                event time (station time)
  size                summary size of all scanned objects
  elapsedtime         elapsed time
  scanned             number of scanned objects
  infected            number of objects infected by known virus
  modifications       number of objects infected by virus modification
  suspicious          number of suspicious objects
  cured               number of cured files
  deleted             number of deleted files
  renamed             number of renamed files
  moved               number of quarantined files
  locked              number of locked files (SpIDer Guard only)
  errors              number of not scanned files (due access error)

Returned value:
  ignored

]]

local args = ... -- args.id, args.address, args.station, args.component,
                 -- args.pid, args.time, args.user, args.scanned,
                 -- args.infected, args.modifications, args.suspicious,
                 -- args.cured, args.deleted, args.renamed, args.moved,
                 -- args.locked, args.errors, args.size, args.elapsedtime
```

Installazione di Agent

Viene invocata dopo che è stato ricevuto l'evento `installation`.

Database	Parametri	Valore restituito

è disponibile	• `id` — ID dell'installazione (attenzione: non è l'ID della postazione),
	• `address` — indirizzo della postazione,
	• `station` — nome della postazione,
	• `event` — tipo di evento:
	  ▫ `0` — inizio dell'installazione,
	  ▫ `1` — completato con successo,
	  ▫ `2` — rifiuto,
	  ▫ `3` — il tempo è scaduto,
	  ▫ `4` — fallito,
	  ▫ `5` — non completato
	• `message` — messaggio di errore (o vuoto se non è occorso nessun errore),
	• `sessionid` — ID della sessione di installazione
		viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when "installation" event occured

Database:
  available

Parameters:
  id                installation ID (not station!)
  address           station address
  station           station name
  event             event type:
                      0   installation begin
                      1   successully completed
                      2   rejected
                      3   timed out
                      4   failed
                      5   incomplete
  message           error message (or empty if there is no error)
  sessionid         installation session ID

Returned value:
  ignored

]]
```

```
local args = ... -- args.id, args.address, args.station
                 -- args.event, args.message, args.sessionid
```

Dispositivo è bloccato

Viene invocata al blocco del dispositivo sulla postazione.

Database	Parametri	Valore restituito
è disponibile	• `id` — ID della postazione, • `address` — indirizzo della postazione, • `name` — nome della postazione, • `user` — nome utente, • `instance_id` — identificatore dell'esemplare del dispositivo, • `friendly_name` — nome descrittivo del dispositivo, • `description` — descrizione del dispositivo, • `guid` — GUID del dispositivo, • `class` — classe di dispositivo (nome del gruppo padre)	viene ignorato

Testo della procedura personalizzata:

```
--[[
Called:
  when device on station blocked

Database:
  available

Parameters:
  id               station ID
  address          station address
  station          station name
  user             user name
  instance_id      device instance id
  friendly_name    device friendly name
  description      device description
  guid             device guid
  class            device group class guid
  blocktime        time when station was blocked
  blockrcvtime     time when server received alert

Returned value:
  ignored

]]

local args = ... -- args.id args.address args.station args.user args.instance_id
                 -- args.friendly_name args.description args.guid args.class
                 -- args.station_time args.args.recv_time
```

M10. LDAP

Traduzione dei nomi utenti in LDAP DN

Viene invocata se i nomi utente vengono tradotti in LDAP DN.

Database	Parametri	Valore restituito
è disponibile	• `user` — nome utente	• `nil` — utente sconosciuto • `string` — informazioni sull'utente: ▫ `empty` — utente sconosciuto ▫ `non-empty` — DN dell'utente

Testo della procedura personalizzata

```
--[[

Called:
  when AuthLDAP module translates user name to DN
```

```
Database:
  available

Parameters:
  user           username

Returned value:
             nil         unknown user
  string     empty       unknown user
             non-empty   DN of user

Procedure from next set will be called if returned nothing.
]]

local args = ... -- args.user

-- example code:
-- if args.user == 'super-admin' then return 'CN=super,DC=example,DC=com' end

-- no return => `nil' value
```

Capitolo 3: Domande ricorrenti

Trasferimento di Server Dr.Web su un altro computer (in caso di SO Windows)

Quando il Server Dr.Web viene trasferito su un altro computer, prestare attenzione alle impostazioni dei protocolli di trasporto e, se necessario, apportare le opportune modifiche nella sezione **Amministrazione** → **Configurazione del Server Dr.Web**, nella scheda **Trasporto**.

La procedura per l'avvio e l'arresto di Server Dr.Web è descritta in **Manuale dell'amministratore**, p. Avvio e arresto di Server Dr.Web.

Per trasferire il Server Dr.Web (se viene installata una versione di Server Dr.Web analoga) sotto il SO Windows

1. Arrestare il servizio Server Dr.Web.
2. Avviare dalla riga di comando il file `drwcsd.exe` con l'opzione `modexecdb database-export` per esportare i contenuti del database in file. La completa riga di comando di esportazione nella versione per SO Windows si vede approssimativamente così:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -verbosity=trace -log="C:
   \Program Files\DrWeb Server\var\exportdb.log" modexecdb database-export
   <nome_file_completo>
   ```

3. Salvare i contenuti della directory `C:\Program Files\DrWeb Server\etc`.
4. Eliminare il Server Dr.Web.
5. Installare un Server Dr.Web nuovo (vuoto, con un nuovo database) sul computer desiderato. Arrestare il servizio Server Dr.Web tramite gli strumenti di gestione dei servizi di SO Windows o tramite il Pannello di controllo.
6. Copiare i contenuti della directory precedentemente salvata `etc` in `C:\Program Files\DrWeb Server\etc`.
7. Avviare dalla riga di comando il file `drwcsd.exe` con l'opzione `modexecdb database-import` per importare i contenuti del database da file. La completa riga di comando di importazione nella versione per SO Windows si vede approssimativamente così:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -verbosity=trace -log="C:
   \Program Files\DrWeb Server\var\importdb.log" modexecdb database-import
   <nome_file_completo>
   ```

8. Avviare il servizio Server Dr.Web.

Se viene utilizzato il database interno, si può omettere l'esportazione e l'importazione del database, ma salvare semplicemente il file di database interno `database.sqlite` e sostituire il nuovo file di database sul Server Dr.Web installato con il file precedente conservato dal Server Dr.Web precedente.

Per trasferire il Server Dr.Web (se viene installata un'altra versione di Server Dr.Web) sotto il SO Windows

1. Arrestare il servizio Server Dr.Web.
2. Salvare il database tramite gli strumenti del server SQL (se viene utilizzato il database incorporato, salvare semplicemente il file `database.sqlite`).
3. Salvare i contenuti della directory `C:\Program Files\DrWeb Server\etc`.
4. Eliminare il Server Dr.Web.
5. Installare un Server Dr.Web nuovo (vuoto, con un nuovo database) sul computer desiderato. Arrestare il servizio Server Dr.Web tramite gli strumenti di gestione dei servizi di SO Windows o tramite il Pannello di controllo.
6. Copiare i contenuti della directory precedentemente salvata `etc` in `C:\Program Files\DrWeb Server\etc`.
7. Ripristinare il database sul nuovo Server Dr.Web, indicare il percorso del database nel file di configurazione `drwcsd.conf`.
8. Avviare dalla riga di comando il file `drwcsd.exe` con l'opzione `modexecdb database-upgrade` per aggiornare il database. La completa riga di comando di aggiornamento database nella versione per SO Windows si vede approssimativamente così:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -verbosity=all -log="C:
\Program Files\DrWeb Server\var\upgradedb.log" modexecdb database-upgrade
```

9. Avviare il servizio Server Dr.Web.

In caso di cambio di nome o indirizzo IP a trasferimento di Server Dr.Web:

Affinché possano passare gli Agent Dr.Web per i quali l'indirizzo nel nuovo Server Dr.Web viene impostato tramite il Pannello di controllo e non nella configurazione dell'Agent Dr.Web stesso su postazione, lasciare attivati entrambi i Server Dr.Web fino al momento del completamento della procedura.

Come indirizzo di Server Dr.Web è consigliato utilizzare il nome di server in formato FQDN.

1. Trasferire il Server Dr.Web secondo la procedura corrispondente descritta sopra.

2. Per tutti gli Agent Dr.Web che erano connessi al vecchio Server Dr.Web, impostare l'indirizzo del nuovo Server Dr.Web secondo la procedura corrispondente da sezione Connessione dell'Agent Dr.Web ad un altro Server Dr.Web.

   Per gli Agent Dr.Web per i quali l'indirizzo del nuovo Server Dr.Web veniva impostato tramite il Pannello di controllo e non nella configurazione dell'Agent Dr.Web stesso su postazione, su entrambi i Server Dr.Web nelle impostazioni di Agent Dr.Web deve essere indicato l'indirizzo del nuovo Server Dr.Web.
3. Attendere che tutti gli Agent Dr.Web passino al nuovo Server Dr.Web. Quindi si può rimuovere il vecchio Server Dr.Web.

Trasferimento di Server Dr.Web su un altro computer (in caso di SO Linux)

Quando il Server Dr.Web viene trasferito su un altro computer, prestare attenzione alle impostazioni dei protocolli di trasporto e, se necessario, apportare le opportune modifiche nella sezione **Amministrazione** → **Configurazione del Server Dr.Web**, nella scheda **Trasporto**.

La procedura per l'avvio e l'arresto di Server Dr.Web è descritta in **Manuale dell'amministratore**, p. Avvio e arresto di Server Dr.Web.

Per trasferire il Server Dr.Web (se viene installata una versione di Server Dr.Web analoga) sotto il SO Linux

1. Installare un nuovo Server Dr.Web (vuoto, con nuovo database) sul computer richiesto secondo le istruzioni descritte in **Guida all'installazione**, p. Installazione di Server Dr.Web per SO della famiglia UNIX.

   Se si intende trasferire il vecchio Server Dr.Web mantenendo l'indirizzo IP, assegnare al nuovo Server Dr.Web un indirizzo IP temporaneo in modo che le postazioni possano interagire con il vecchio Server Dr.Web durante il trasferimento.

2. Aggiungere in **Gestione licenze** per il nuovo Server Dr.Web la chiave della propria licenza attiva `Agent.key` e distribuirla al gruppo **Everyone**.
3. Nell'interfaccia web del nuovo Server Dr.Web andare alla sezione **Stato del repository** e assicurarsi che il repository venga aggiornato correttamente.
4. Andare alla sezione **Amministrazione** → **Server Dr.Web** e assicurarsi che in questa sezione sia visualizzata una data che corrisponda alla data della revisione corrente di Server Dr.Web nella sezione **Stato del repository**. Se la data non corrisponde ed è presente un messaggio su disponibilità di aggiornamenti, premere il pulsante **Visualizza lista delle versioni** e aggiornare il Server Dr.Web alla versione attuale.
5. Arrestare il nuovo Server Dr.Web attraverso l'interfaccia web o attraverso la console tramite il comando:

   ```
   # /etc/init.d/drwcsd stop
   ```

6. Sul nuovo Server Dr.Web sostituire il file `/var/opt/drwcs/etc/drwcsd.conf` con il file analogo dal vecchio Server Dr.Web.

   In caso di passaggio a un altro sistema operativo, è necessario controllare il contenuto del file `drwcsd.conf` per la presenza di percorsi win. Se tali percorsi sono presenti, è necessario correggerli manualmente prima del trasferimento.

Notare che i percorsi per FreeBSD sono diversi:

- `/var/opt/drwcs/ -> /var/drwcs/`
- `/opt/drwcs/ -> /usr/local/drwcs/`

7. Dalla directory `/opt/drwcs/webmin/install/windows` sul nuovo Server Dr.Web rimuovere il file del certificato `drwcsd-certificate.pem`.

```
# rm /opt/drwcs/webmin/install/windows/drwcsd-certificate.pem
```

8. Dalla directory `/var/opt/drwcs/etc/` sul nuovo Server Dr.Web rimuovere il file della chiave privata `drwcsd.pri` e la seconda copia del certificato `drwcsd-certificate.pem`.
9. Dalla directory `/var/opt/drwcs/` sul nuovo Server Dr.Web rimuovere il file del database.
10. Se sul vecchio Server Dr.Web è installato SO Windows, copiare la chiave privata `drwcsd.pri` e il certificato `drwcsd-certificate.pem` dalla directory `%programfiles%\DrWeb Server\etc` sul vecchio Server Dr.Web nella directory `/var/opt/drwcs/etc/` sul nuovo Server Dr.Web. Se sul vecchio Server Dr.Web è installato SO della famiglia Linux, copiare questi file dalla directory `var/opt/drwcs/etc/` sul vecchio Server nella directory analoga su quello nuovo.
11. Arrestare il vecchio Server Dr.Web attraverso l'interfaccia web (**Start** → **Tutti i programmi** → **Dr.Web Server** → **Gestione server**) o (se su di esso è installato SO della famiglia Linux) attraverso la console:

```
# /etc/init.d/drwcsd stop
```

12. Controllare il database sul vecchio Server Dr.Web tramite il comando:
    - in caso di Server Dr.Web fino alla versione 13:

```
# /etc/init.d/drwcsd verifydb
```

    - in caso di Server Dr.Web della versione 13:

```
# /etc/init.d/drwcsd modexecdb database-verify
```

    Se dopo l'esecuzione di questo comando nel file `drwscd.log` comparirà un messaggio di errore, contattare il supporto tecnico.
13. Salvare il database tramite gli strumenti del server SQL (se viene utilizzato il database incorporato, salvare semplicemente il file `database.sqlite`). Copiare il file del database dalla directory `%programfiles%\DrWeb Server\var` del vecchio Server Dr.Web (dalla directory `/var/opt/drwcs/`, se era installato SO della famiglia Linux) nella directory `/var/opt/drwcs/` del nuovo Server Dr.Web.
14. Avviare il vecchio Server Dr.Web, in modo che continui a fornire servizio agli agent, o attraverso l'interfaccia web o attraverso la console tramite il comando:

```
# /etc/init.d/drwcsd start
```

15. Sul nuovo Server Dr.Web nominare l'utente `drwcs` proprietario della directory `/var/opt/drwcs/database.sqlite`, nonché proprietario dei file `/var/opt/drwcs/etc/drwcsd.pri` e `/var/opt/drwcs/etc/drwcsd-certificate.pem`:

```
# chown -R drwcs /var/opt/drwcs/database.sqlite

# chown drwcs /var/opt/drwcs/etc/drwcsd.pri

# chown drwcs /var/opt/drwcs/etc/drwcsd-certificate.pem
```

16. Copiare il certificato `drwcsd-certificate.pem` nella directory `/opt/drwcs/webmin/install/windows`

```
# cp /var/opt/drwcs/etc/drwcsd?
certificate.pem /opt/drwcs/webmin/install/windows
```

17. Avviare il nuovo Server Dr.Web:

```
# /etc/init.d/drwcsd start
```

18. Entrare nell'interfaccia web del nuovo Server Dr.Web con gli stessi login e password che sono sul vecchio Server Dr.Web. Assicurarsi che tutti gli Agent Dr.Web siano visualizzati correttamente nella lista della rete antivirus.
19. Andare alla sezione **Amministrazione** → **Stato del repository** e assicurarsi che il repository sul nuovo Server Dr.Web venga aggiornato senza errori. Se nella tabella con la lista dei prodotti nella colonna "Stato del repository" sono presenti messaggi di errore, contattare il supporto tecnico. Alla richiesta allegare il file `drwscd.log`. Non si dovrebbero intraprendere ulteriori azioni dall'istruzione fino a quando non si riceverà un feedback nella richiesta.
20. Andare alla sezione **Amministrazione** → **Scheduler di Server Dr.Web** e selezionare il task **Backup sensitive data** (Backup dei dati critici del Server Dr.Web). Premere l'icona  ; nella finestra di modifica del task selezionare la scheda **Azione**. Assicurarsi che nel campo **Percorso** non sia indicato il percorso della directory sul vecchio Server Dr.Web. Ripulire questo campo e lasciare questo campo vuoto (in questo caso per la conservazione delle copie di backup verrà utilizzata la directory di default — `/var/opt/drwcs/backup`) o indicare il percorso della directory sul nuovo Server Dr.Web.
21. Sul nuovo server andare alla sezione **Rete antivirus** → **Everyone** → **Parametri di connessione** e indicare l'indirizzo del nuovo Server nel campo **Server Dr.Web**.

Se è necessario mantenere per il nuovo Server Dr.Web il vecchio indirizzo IP (v. p.1), arrestare il vecchio Server Dr.Web e assegnare al nuovo Server Dr.Web il suo indirizzo IP. Riavviare il nuovo Server Dr.Web affinché le impostazioni di rete modificate abbiano effetto.

Per connettere le postazioni al nuovo Server Dr.Web

1. Entrare nell'interfaccia web del vecchio Server Dr.Web e selezionare la postazione o il gruppo di postazioni da riconnettere.
2. Andare alla sezione **Parametri di connessione** e indicare l'indirizzo del nuovo Server Dr.Web per gli oggetti selezionati. Controllare che tutte le postazioni siano disconnesse dal vecchio Server e siano connesse a quello nuovo.

Connessione dell'Agent Dr.Web ad un altro Server Dr.Web

L'Agent Dr.Web può essere connesso a un altro Server Dr.Web in due modi:

1. Tramite il Pannello di controllo.

   È possibile configurare la postazione senza accedere direttamente ad essa se la postazione è ancora connessa al Server Dr.Web vecchio. È necessario l'accesso ai Pannelli di controllo sia del vecchio che del nuovo Server Dr.Web.

2. Direttamente sulla postazione.

   Per eseguire le azioni direttamente sulla postazione, sono richiesti i permessi di amministratore su questa postazione e i permessi di modifica delle impostazioni di Agent Dr.Web stabilite sul Server Dr.Web. Se questi permessi non sono disponibili, la riconnessione a un altro Server Dr.Web in modo locale su postazione è possibile solo dopo la rimozione dell'Agent Dr.Web installato e l'installazione di un nuovo Agent Dr.Web con le impostazioni del nuovo Server Dr.Web. Se non sono disponibili i permessi di rimozione di Agent Dr.Web in modo locale, utilizzare l'utility Dr.Web Remover per rimuovere l'Agent Dr.Web sulla postazione, o rimuovere l'Agent Dr.Web tramite il Pannello di controllo.

Connessione dell'Agent Dr.Web ad un altro Server Dr.Web

La connessione dell'Agent Dr.Web a un altro Server Dr.Web può essere necessaria nel caso in cui gli agent sono connessi a un Server Dr.Web il cui indirizzo è cambiato, o se il Server Dr.Web è stato reinstallato senza l'utilizzo del certificato del server precedente.

L'Agent Dr.Web può essere connesso a un altro Server Dr.Web in due modi:

1. Tramite il Pannello di controllo.

   È possibile configurare la postazione senza accedere direttamente ad essa se la postazione è ancora connessa al Server Dr.Web vecchio. È necessario l'accesso ai Pannelli di controllo sia del vecchio che del nuovo Server Dr.Web.

2. Direttamente sulla postazione.

   Per eseguire azioni direttamente sulla postazione, sono richiesti i permessi di amministratore di tale postazione, e nel caso di loro modifica tramite l'interfaccia agent, i permessi di modifica delle impostazioni Agent Dr.Web, che vengono stabiliti sul Server Dr.Web. Se questi permessi non sono disponibili, la riconnessione a un altro Server Dr.Web è

possibile solo dopo la disinstallazione tramite Pannello di controllo dell'agent installato e l'installazione di un nuovo Agent Dr.Web con le impostazioni del nuovo Server Dr.Web.

È possibile modificare una serie di impostazioni di connessione dalla riga di comando dall'account amministratore della postazione:

- SO Windows:
  `"%ProgramFiles%\DrWeb\es-service.exe" --esserver=<indirizzo_server> --addcert=<percorso_del_certificato>`
- SO UNIX:
  `drweb-ctl esdisconnect && drweb-ctl esconnect <indirizzo_server> --Certificate <percorso_del_certificato>`

  `<indirizzo_server>` - se l'indirizzo del server è cambiato.

  `<percorso_del_certificato>` - se il server è stato reinstallato senza l'utilizzo del certificato del server precedente.

Il certificato del server è disponibile in Pannello di controllo, sezione **Amministrazione > Chiavi di crittografia**.

Per trasferire Agent Dr.Web a un altro Server Dr.Web attraverso il Pannello di controllo

1. Sul Server Dr.Web nuovo consentire alle postazioni con credenziali non valide di richiedere nuovi parametri di autenticazione come nuovi arrivi. A tale scopo nel Pannello di controllo selezionare la voce **Amministrazione** del menu principale → la voce **Configurazione del Server Dr.Web** del menu di gestione → scheda **Generali**:
   a) Spuntare il flag **Trasferisci le postazioni non autenticate in nuovi arrivi** se è deselezionato.
   b) Se nella lista a cascata **Modalità di registrazione dei nuovi arrivi** è selezionata l'opzione **Sempre nega l'accesso**, cambiarla a **Conferma l'accesso manualmente** o a **Consenti l'accesso automaticamente**.
   c) Per rendere effettive le modifiche apportate, premere il pulsante **Salva** e riavviare il Server Dr.Web.

Se i criteri di sicurezza aziendali non permettono di modificare le impostazioni dal passo 1, i parametri di autenticazione di postazione corrispondenti all'account precedentemente creato nel Pannello di controllo devono essere impostati direttamente sulla postazione.

2. Sul vecchio Server Dr.Web a cui è connesso l'Agent Dr.Web impostare i parametri del nuovo Server Dr.Web. A tale scopo nel Pannello di controllo selezionare nel menu principale la voce **Rete antivirus** → nella lista gerarchica della rete selezionare la postazione richiesta (o un gruppo per riconnettere tutte le postazioni di questo gruppo) → nel menu di gestione selezionare la voce **Parametri di connessione**:
   a) Se il certificato del Server Dr.Web nuovo non coincide con il certificato del Server Dr.Web vecchio, nel campo **Certificato** indicare il percorso del certificato del Server Dr.Web nuovo.

b) Nel campo **Server** indicare l'indirizzo del Server Dr.Web nuovo.

> Come indirizzo di Server Dr.Web è consigliato utilizzare il nome di server in formato FQDN.

c) Premere il pulsante **Salva**.

Per trasferire Agent Dr.Web a un altro Server Dr.Web direttamente sulla postazione stessa

1. Nelle impostazioni di Agent Dr.Web configurare i parametri del nuovo Server Dr.Web. A tale scopo, attraverso il menu contestuale dell'icona di Agent Dr.Web aprire il **Centro sicurezza** → fare clic sul lucchetto, se non è ancora aperto, per accedere alle impostazioni avanzate → pulsante per accedere alle impostazioni → voce **Server** → pulsante **Modifica impostazioni**:
   a) Se il certificato del Server Dr.Web nuovo non coincide con il certificato del Server Dr.Web vecchio, tramite il pulsante **Lista dei certificati** indicare il percorso del certificato del Server Dr.Web nuovo.
   b) Tramite il pulsante **Aggiungi** impostare i parametri corrispondenti del Server Dr.Web nuovo.
2. Trasferire la postazione in nuovi arrivi (resettare i parametri di autenticazione sul Server Dr.Web). A tale scopo nella sezione dei parametri di connessione dal passaggio 1 premere come segue: pulsante **Parametri di connessione della postazione** → pulsante **Resetta parametri e connettiti come nuovo arrivo** → pulsante **Resetta parametri**.

> Se sono conosciuti in anticipo l'ID e la password per la connessione al Server Dr.Web nuovo, è possibile indicarle nei campi **ID della postazione** e **Password**. In tale caso non è necessario trasferire la postazione in nuovi arrivi.

Carico su Server Dr.Web e parametri di configurazione raccomandati

In caso di utilizzo di un database esterno in reti antivirus di grandi dimensioni, per assicurare l'operatività di Server Dr.Web, può essere necessario modificare i valori dei seguenti parametri:

- **Amministrazione** → **Configurazione del Server Dr.Web** → **Database** → **Numero di connessioni** (parametro `database connections=""` nel file di configurazione di Server Dr.Web) — numero massimo ammissibile di connessioni di Server Dr.Web al database.
- **Amministrazione** → **Configurazione del Server Dr.Web** → **Generali** → **Numero di richieste parallele dai client** (parametro `threads count=""` nel file di configurazione di Server Dr.Web) — numero di flussi per l'elaborazione dei dati provenienti dai client: Agent Dr.Web, installer di Agent, Server Dr.Web adiacenti, Server proxy Dr.Web.

Questi parametri influiscono sulle prestazioni di Server Dr.Web. Evitare di modificarne i valori se non necessario. Per determinare la necessità di modificarli, consultare la tabella delle interrelazioni tra le dimensioni della rete antivirus, le capacità hardware di Server Dr.Web e i valori ottimali dei parametri:

Numero di connessioni dei client a Server Dr.Web	Numero di core del processore di Server Dr.Web	Numero di connessioni al database (database connections)	Numero di richieste parallele dai client (threads count)
fino a 500	2	2 (valore di default)	5 (valore di default)
500–1500	3–5	3–5	6–10
oltre 1500	5–8	5–8	10–14

Il valore del parametro **Numero di richieste parallele dai client** (`threads count`) non deve essere più del doppio del numero di core del processore sul computer che svolge le funzioni di Server Dr.Web.

In caso di utilizzo del database incorporato, non è consigliabile modificare i valori di default.

In caso di utilizzo di una rete con un numero elevato di connessioni, prima di modificare i valori dei parametri riportati sopra, si consiglia di ottenere consulenza nel servizio di supporto tecnico dell'azienda Doctor Web.

Cambio del tipo di database di Dr.Web Enterprise Security Suite

In caso di SO Windows

La procedura per l'avvio e l'arresto di Server Dr.Web è descritta in **Manuale dell'amministratore**, p. Avvio e arresto di Server Dr.Web.

1. Arrestare il servizio Server Dr.Web.
2. Avviare dalla riga di comando il file `drwcsd.exe` con l'opzione `modexecdb database-export` per esportare i contenuti del database in file. La completa riga di comando di esportazione nella versione per SO Windows si vede approssimativamente così:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
   Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
   verbosity=trace -log="C:\Program Files\DrWeb Server\var\exportdb.log"
   modexecdb database-export D:\esbase.es
   ```

   In questo esempio si sottintende che il Server Dr.Web sia installato nella directory `C:\Program Files\DrWeb Server` e che il database viene esportato in un file con il nome `esbase.es` alla radice dell'unità `D`.

   Se nel percorso del file ci sono degli spazi e/o caratteri nazionali (o il nome del file contiene degli spazi e/o caratteri nazionali), il percorso deve essere messo tra virgolette:

   ```
   "D:\<nome completo>\esbase.es"
   ```

3. Avviare il servizio Server Dr.Web, connettere ad esso il Pannello di controllo e riconfigurare il Server Dr.Web per l'utilizzo di un altro database. Rifiutare la proposta di riavvio del Server Dr.Web.
4. Arrestare il servizio Server Dr.Web.
5. Spostare il file di database in una directory temporanea fino a quando non si è sicuri che il cambio del tipo di database sia andato a buon fine.
6. Avviare dalla riga di comando il file `drwcsd.exe` con l'opzione `modexecdb database-init` per inizializzare il nuovo database. La riga di inizializzazione del database per la versione di Server Dr.Web per SO Windows si vede approssimativamente così:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
   Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
   verbosity=all -log="C:\Program Files\DrWeb Server\var\initdb.log"
   modexecdb database-init
   ```

   Si sottintende che il Server Dr.Web è installato nella directory `"C:\Program Files\DrWeb Server"`.

7. Avviare dalla riga di comando il file `drwcsd.exe` con l'opzione `modexecdb database-import` per importare i contenuti del database da file. La completa riga di comando di importazione nella versione per SO Windows si vede approssimativamente così:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=trace -log="C:\Program Files\DrWeb Server\var\importdb.log"
modexecdb database-import D:\esbase.es
```

8. Avviare il servizio Server Dr.Web.

In caso di SO della famiglia UNIX

1. Arrestare il servizio Server Dr.Web tramite lo script:
   - in caso di SO **Linux**:

   ```
   /etc/init.d/drwcsd stop
   ```

   - in caso di SO **FreeBSD**:

   ```
   /usr/local/etc/rc.d/drwcsd stop
   ```

   o tramite il Pannello di controllo.
2. Avviare il Server Dr.Web con l'opzione `modexecdb database-export` per esportare i contenuti del database in file. La riga di comando dalla directory di installazione del Server Dr.Web si vede approssimativamente così:
   - in caso di SO **Linux**:

   ```
   /etc/init.d/drwcsd modexecdb database-export /var/opt/drwcs/esbase.es
   ```

   - in caso di SO **FreeBSD**:

   ```
   /usr/local/etc/rc.d/drwcsd modexecdb database-export /var/drwcs/esbase.es
   ```

   In questo esempio si sottintende che il database viene esportato nel file `esbase.es` locato nella directory di utente.
3. Avviare il servizio Server Dr.Web tramite lo script:
   - in caso di SO **Linux**:

   ```
   /etc/init.d/drwcsd start
   ```

   - in caso di SO **FreeBSD**:

   ```
   /usr/local/etc/rc.d/drwcsd start
   ```

   connettere ad esso il Pannello di controllo e riconfigurare il Server Dr.Web per l'utilizzo di un altro database: nel menu **Amministrazione** → voce **Configurazione del Server Dr.Web** → scheda **Database**.

   

   È inoltre possibile riconfigurare il Server Dr.Web per l'utilizzo di un altro database modificando direttamente il file di configurazione di Server Dr.Web `drwcsd.conf`. Per

farlo, è necessario commentare/cancellare il record del database corrente e trascrivere il database nuovo (per maggiori informazioni v. F1. File di configurazione di Server Dr.Web).

Rifiutare la proposta di riavvio del Server Dr.Web.

4. Arrestare il Server Dr.Web (v. passaggio **1**).
5. Spostare il file di database in una directory temporanea fino a quando non si è sicuri che il cambio del tipo di database sia andato a buon fine.
6. Avviare il file `drwcsd` con l'opzione `modexecdb database-init` per inizializzare il nuovo database. La riga di inizializzazione si vede approssimativamente così:
   - in caso di SO **Linux**:

```
/etc/init.d/drwcsd modexecdb database-init
```

   - in caso di SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd modexecdb database-init
```

7. Avviare il file `drwcsd` con l'opzione `modexecdb database-import` per importare i contenuti del database da file. La riga di comando di importazione si vede approssimativamente così:
   - in caso di SO **Linux**:

```
/etc/init.d/drwcsd modexecdb database-import /var/opt/drwcs/esbase.es
```

   - in caso di SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd modexecdb database-import /var/drwcs/esbase.es
```

8. Avviare il Server Dr.Web (v. passaggio **3**).

Se all'avvio dello script del Server Dr.Web è necessario impostare parametri (per esempio, indicare la directory di installazione del Server Dr.Web, modificare il livello di dettaglio del log ecc.), i valori corrispondenti vengono modificati nello script di avvio:

- in caso di SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd
```

- in caso di SO **Linux**:

```
/etc/init.d/drwcsd
```

Ripristino del database di Dr.Web Enterprise Security Suite

Nel corso del funzionamento Server Dr.Web salva regolarmente copie di backup delle informazioni importanti: chiavi di licenza, contenuti del database, chiave di cifratura privata, configurazione del Server Dr.Web e del Pannello di controllo.

I backup vengono salvati nelle seguenti directory:

- in caso di SO **Windows**: <*disco_di_installazione*>`:\DrWeb Backup`
- in caso di SO **Linux**: `/var/opt/drwcs/backup`
- in caso di SO **FreeBSD**: `/var/drwcs/backup`

Per l'esecuzione della funzione di backup, nel calendario del Server Dr.Web è incluso un task quotidiano. Se tale task non è disponibile nel calendario, si consiglia di crearlo.

Tutti i file da un backup, ad eccezione del contenuto del database, sono immediatamente utilizzabili. Il backup del database viene salvato nel formato `.gz` compatibile con `gzip` e altri programmi di archiviazione. È possibile importare il contenuto del database dal backup nel database operativo di Server Dr.Web tramite il comando `modexecdb database-import` e in questo modo ripristinare i dati.

Per ripristinare il database, è inoltre possibile utilizzare una copia di backup creata manualmente dall'amministratore attraverso il Pannello di controllo nella sezione **Amministrazione** → **Gestione del database** → **Esportazione** (solo per la modalità **Esporta l'intero database**).

È possibile ripristinare il database solo da un backup creato tramite un Server Dr.Web con la stessa versione principale della versione del Server Dr.Web su cui avviene il ripristino.

Per esempio:

- un database da un backup creato tramite il Server Dr.Web versione 13 può essere ripristinato solo tramite il Server Dr.Web versione 13.
- un database da un backup creato tramite il Server Dr.Web versione 10 non può essere ripristinato tramite il Server Dr.Web versione 13.

Se durante l'aggiornamento del Server Dr.Web alla versione 13 dalle versioni precedenti, per qualche motivo è stato danneggiato il database, eseguire le seguenti azioni:

1. Rimuovere il Server Dr.Web versione 13. In tale caso verranno salvati automaticamente i backup dei file utilizzati dal Server Dr.Web.
2. Installare il Server Dr.Web della versione precedente all'aggiornamento attraverso cui è stato creato il backup.

   In questo caso, secondo la procedura di aggiornamento standard, devono essere utilizzati tutti i file salvati del Server Dr.Web ad eccezione del file del database.

Durante l'installazione del Server Dr.Web creare un nuovo database.

3. Ripristinare il database dal backup secondo le regole generali (v. sotto).
4. Nelle impostazioni di Server Dr.Web disattivare i protocolli di Agent Dr.Web, Server Dr.Web e Installer 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 **Configurazione del Server Dr.Web**, passare alla scheda **Moduli** e deselezionare i flag corrispondenti.
5. Aggiornare il Server Dr.Web alla versione 13 secondo le regole generali (v. in **Manuale dell'amministratore** p. Capitolo 11: Aggiornamento dei componenti di Dr.Web Enterprise Security Suite durante il funzionamento).
6. Attivare i protocolli di Agent Dr.Web, Server Dr.Web e Installer di rete disattivati al passaggio 4.

Ripristino del database sotto SO Windows

La procedura per l'avvio e l'arresto di Server Dr.Web è descritta in **Manuale dell'amministratore**, p. Avvio e arresto di Server Dr.Web.

Per ripristinare il database da un backup

1. Arrestare il servizio Server Dr.Web, se è in esecuzione.
2. Importare dal relativo file di backup i contenuti del database. La riga di importazione si presenta approssimativamente così:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=trace -log="C:\Program Files\DrWeb Server\var\importdb.log"
modexecdb database-import "<percorso_file_di_backup>\database.gz"
```

   Anche questo comando deve essere digitato in una sola riga. Nell'esempio si sottintende che il Server Dr.Web è installato nella directory `C:\Program Files\DrWeb Server`.
3. Avviare il servizio Server Dr.Web.

Per ripristinare il database da un backup se cambia la versione di Server Dr.Web (all'interno di una versione principale) o se la versione attuale del database è danneggiata

1. Arrestare il servizio Server Dr.Web, se è in esecuzione.
2. Inizializzare il nuovo database.
   - Se viene utilizzato il database incorporato:
     a) Spostare il file di database `database.sqlite` in una directory temporanea fino a quando non si è sicuri che il ripristino del database sia andato a buon fine.
     b) La riga di inizializzazione del database nella versione di Server Dr.Web sotto SO Windows si presenta approssimativamente così:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log="C:\Program Files\DrWeb Server\var\initdb.log"
modexecdb database-init
```

Questo comando deve essere digitato in una sola riga (v. inoltre il formato del comando `drwcsd` con l'opzione `modexecdb database-init` in Allegato G3.3. Comandi di gestione del database). Nell'esempio si sottintende che il Server Dr.Web è installato nella directory `C:\Program Files\DrWeb Server`.

c) Dopo l'esecuzione di questo comando, nella cartella `var` della directory di installazione di Server Dr.Web deve comparire il nuovo file di database `database.sqlite`.

- Se viene utilizzato un database esterno:

a) esportare il file di database in una directory temporanea fino a quando non si è sicuri che il ripristino del database sia andato a buon fine.

b) ripulire il database tramite il comando `modexecdb database-clean` (v. Allegato G3.3. Comandi di gestione del database).

3. Importare dal relativo file di backup i contenuti del database. La riga di importazione si presenta approssimativamente così:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=trace -log="C:\Program Files\DrWeb Server\var\importdb.log"
modexecdb database-import "<percorso_file_di_backup>\database.gz"
```

Anche questo comando deve essere digitato in una sola riga. Nell'esempio si sottintende che il Server Dr.Web è installato nella directory `C:\Program Files\DrWeb Server`.

4. Avviare il servizio Server Dr.Web.

Ripristino del database sotto SO della famiglia UNIX

1. Arrestare il Server Dr.Web (se è in esecuzione):

- in caso di SO **Linux**:

```
/etc/init.d/drwcsd stop
```

- in caso di SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd stop
```

2. Spostare il file di database in una directory temporanea fino a quando non si è sicuri che il ripristino del database sia andato a buon fine. Il file di database `database.sqlite` si trova nella seguente directory della directory di installazione di Server Dr.Web:

- in caso di SO **Linux**: `/var/opt/drwcs/`
- in caso di SO **FreeBSD**: `/var/drwcs/`

Se si utilizza un database esterno, esso viene ripulito tramite il comando `modexecdb database-clean` (v. Allegato G3.3. Comandi di gestione del database).

3. Inizializzare il database del Server Dr.Web. Per farlo, si utilizza il seguente comando:
   - in caso di SO **Linux**:

```
/etc/init.d/drwcsd modexecdb database-init
```

   - in caso di SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd modexecdb database-init
```

4. Dopo l'esecuzione di questo comando, nella cartella `var` della directory di installazione di Server Dr.Web deve comparire il nuovo file di database `database.sqlite`.
5. Importare dal relativo file di backup i contenuti del database. La riga di importazione si presenta approssimativamente così:
   - in caso di SO **Linux**:

```
/etc/init.d/drwcsd modexecdb database-import
"<percorso_del_file_di_backup>/database.gz"
```

   - in caso di SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd modexecdb database-import
"<percorso_del_file_di_backup>/database.gz"
```

6. Avviare il Server Dr.Web.
   - in caso di SO **Linux**:

```
/etc/init.d/drwcsd start
```

   - in caso di SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd start
```

Se all'avvio dello script del Server Dr.Web è necessario impostare parametri (per esempio, indicare la directory di installazione di Server Dr.Web ecc.), i valori corrispondenti vengono modificati nello script di avvio:

- in caso di SO FreeBSD: `/usr/local/etc/rc.d/drwcsd`;
- in caso di SO Linux: `/etc/init.d/drwcsd`.

Se è necessario modificare il livello di dettaglio del log di Server Dr.Web, per questo scopo utilizzare il file `local.conf`:

- in caso di SO Linux: `/var/opt/drwcs/etc/local.conf`;
- in caso di SO FreeBSD: `/var/drwcs/etc/local.conf`.

Se qualche Agent Dr.Web è stato installato dopo la creazione dell'ultimo backup, non potrà connettersi al Server Dr.Web dopo il ripristino del database da questo backup. È possibile trasferire tali postazioni in remoto in modalità nuovi arrivi. Nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** nella scheda **Generali** spuntare il flag **Trasferisci le postazioni non autenticate in nuovi arrivi**. Dalla lista a cascata **Modalità di registrazione dei nuovi arrivi** selezionare la variante **Consenti l'accesso automaticamente**. Premere **Salva** e riavviare il Server Dr.Web.

Dopo che tutte le postazioni si connetteranno al nuovo Server Dr.Web, sostituire queste impostazioni di Server Dr.Web con le impostazioni adottate in conformità ai criteri aziendali.

Dopo il ripristino del database, si consiglia di connettersi al Server Dr.Web attraverso il Pannello di controllo, aprire la sezione **Amministrazione** → **Scheduler del Server Dr.Web** e controllare la disponibilità del task **Backup dei dati critici del Server**. Se tale task non è disponibile nel calendario, si consiglia di crearlo.

Aggiornamento degli Agent sui server LAN

In caso di aggiornamento di Agent Dr.Web installati su server LAN, possono essere indesiderati i riavvi delle postazioni o gli arresti dei software di rete in esecuzione su tali postazioni.

Al fine di evitare tempi di inattività operativa di postazioni che svolgono funzionalità LAN critiche, è suggerita la seguente modalità di aggiornamento degli Agent Dr.Web e del software antivirus:

1. Nel calendario del Server Dr.Web cambiare i task standard di aggiornamento di tutti i componenti con l'aggiornamento dei soli database dei virus.
2. Creare un nuovo task dell'aggiornamento di tutti i componenti in un momento conveniente quando tale processo non avrà impatto critico sull'operazione dei server LAN.

   Come creare e modificare task nel calendario del Server Dr.Web viene descritto in **Manuale dell'amministratore** p. Configurazione del calendario del Server Dr.Web.

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.

Utilizzo di DFS per l'installazione di Agent tramite Active Directory

Per l'installazione dell'Agent Dr.Web tramite Active Directory, è possibile utilizzare il servizio file system distribuito (DFS).

Questo approccio potrebbe essere utile, per esempio, se nella rete LAN ci sono diversi controller di dominio.

Per installare Agent Dr.Web in una rete con diversi controller di dominio

1. Su ogni controller di dominio creare una directory con il nome uguale.
2. Tramite DFS, unire le directory create in una directory radice di destinazione.
3. Effettuare l'installazione amministrativa del pacchetto `*.msi` nella directory di destinazione creata (vedi **Guida all'installazione**, p. Installazione di Agent Dr.Web con utilizzo di Active Directory).
4. Utilizzare la directory di destinazione per l'assegnazione del pacchetto nell'editor degli oggetti di criteri di gruppo.

   Per questo utilizzare il nome di rete tipo: \\<*domain*>\<*folder*>

   dove: <*domain*> — nome a dominio, <*folder*> — nome della directory di destinazione.

Ripristino della rete antivirus dopo un errore di Server Dr.Web

Nel caso di un errore fatale di Server Dr.Web è consigliabile utilizzare le procedure riportate per ripristinare l'operatività della rete antivirus senza la reinstallazione di Agent Dr.Web sulle postazioni.

Si sottintende che il nuovo Server Dr.Web verrà installato su un computer con lo stesso indirizzo IP e nome DNS.

Ripristino se è disponibile un backup di Server Dr.Web

Nel corso del funzionamento Server Dr.Web salva regolarmente copie di backup delle informazioni importanti: chiavi di licenza, contenuti del database, chiave di cifratura privata, configurazione del Server Dr.Web e del Pannello di controllo.

I backup vengono salvati nelle seguenti directory:

- in caso di SO **Windows**: <*disco_di_installazione*>`:\DrWeb Backup`
- in caso di SO **Linux**: `/var/opt/drwcs/backup`
- in caso di SO **FreeBSD**: `/var/drwcs/backup`

Per l'esecuzione della funzione di backup, nel calendario del Server Dr.Web è incluso un task quotidiano. Se tale task non è disponibile nel calendario, si consiglia di crearlo.

Tutti i file da un backup, ad eccezione del contenuto del database, sono immediatamente utilizzabili. Il backup del database viene salvato nel formato `.gz` compatibile con `gzip` e altri programmi di archiviazione. È possibile importare il contenuto del database dal backup nel database operativo di Server Dr.Web tramite il comando `modexecdb database-import-and-upgrade` e in questo modo ripristinare i dati.

Per ripristinare il database, è inoltre possibile utilizzare una copia di backup creata manualmente dall'amministratore attraverso il Pannello di controllo nella sezione **Amministrazione** → **Gestione del database** → **Esportazione** (solo per la modalità **Esporta l'intero database**).

Si consiglia inoltre di memorizzare su un altro PC i backup creati e altri file importanti. In questo modo si può evitare la perdita dei dati se viene danneggiato il computer su cui è installato Server Dr.Web e si possono ripristinare completamente i dati e l'operatività di Server Dr.Web. In caso di smarrimento delle chiavi di licenza, è possibile richiederle nuovamente, come indicato in **Manuale dell'amministratore,** p. Concessione delle licenze.

Per ripristinare Server Dr.Web dopo un errore di operazione, se si è conservata una copia di backup dei dati di Server Dr.Web

1. Selezionare il computer su cui verrà installato il nuovo Server Dr.Web. Isolare questo computer da Agent Dr.Web attivi: scollegarlo dalla rete in cui sono installati Agent Dr.Web, o modificare temporaneamente il suo indirizzo IP, o utilizzare qualsiasi altro metodo più conveniente.
2. Installare il nuovo Server Dr.Web.
3. Nella sezione **Amministrazione** → **Gestione licenze** aggiungere la chiave di licenza dall'installazione di Server Dr.Web precedente e distribuirla ai gruppi corrispondenti, in particolare al gruppo **Everyone**. Il passaggio è obbligatorio se durante l'installazione di Server Dr.Web la chiave di licenza non è stata impostata.
4. Aggiornare da SAM il repository del Server Dr.Web installato:
   a) Aprire la sezione del Pannello di controllo **Amministrazione** → **Stato del repository**.
   b) 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.
5. Se sono disponibili nuove versioni del software Server Dr.Web, aggiornarlo all'ultima versione:
   a) Aprire la sezione del Pannello di controllo **Amministrazione** → **Server Dr.Web**.
   b) Per passare all'elenco delle versioni di Server Dr.Web, premere la versione corrente di Server Dr.Web o il pulsante **Elenco delle versioni**. Si aprirà la sezione **Aggiornamenti del Server Dr.Web** con un elenco di aggiornamenti e backup di Server Dr.Web disponibili.
   c) Per passare alla nuova versione di Server Dr.Web, spuntare il flag di fronte all'ultima versione nell'elenco **Tutte le versioni** e premere il pulsante **Applica**.
   d) Attendere che il processo di aggiornamento di Server Dr.Web sia completato.
6. Arrestare Server Dr.Web.
7. Sostituire i dati critici di Server Dr.Web con i dati ottenuti dal backup:

Sistema operativo	File di configurazione
Windows	`etc` nella directory di installazione di Server Dr.Web
Linux	`/var/opt/drwcs/etc`
FreeBSD	`/var/drwcs/etc`

8. Configurare il database.
   a) Database esterno:

      Non sono richieste ulteriori azioni per la connessione del database a Server Dr.Web (a condizione che è conservato il file di configurazione di Server Dr.Web).

Se la versione Server Dr.Web installata dagli ultimi aggiornamenti è una versione successiva rispetto a quella del Server Dr.Web perso, aggiornare il database esterno attraverso il comando `modexecdb database-upgrade`:

- in caso di SO Windows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -verbosity=all -log="C:
\Program Files\DrWeb Server\var\upgradedb.log" modexecdb database-
upgrade
```

- in caso di SO Linux:

```
/etc/init.d/drwcsd modexecdb database-upgrade
```

- in caso di SO FreeBSD:

```
/usr/local/etc/rc.d/drwcsd modexecdb database-upgrade
```

b) Copia di backup di un database esterno o incorporato:

Se si utilizza un database esterno, ripulirlo preliminarmente tramite il comando `modexecdb database-clean` (vedi Allegato G3.3. Comandi di gestione del database).

Importare il database dal file di backup corrispondente aggiornando il formato del database alla versione del Server Dr.Web installato utilizzando il comando `modexecdb database-import-and-upgrade`:

- in caso di SO Windows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=trace -log="C:\Program Files\DrWeb
Server\var\importupgradedb.log" modexecdb database-import-and-upgrade
"<percorso_file_di_backup>\database.gz"
```

- in caso di SO Linux:

```
/etc/init.d/drwcsd modexecdb database-import-and-upgrade
"<percorso_del_file_di_backup>/database.gz"
```

- in caso di SO FreeBSD:

```
/usr/local/etc/rc.d/drwcsd modexecdb database-import-and-upgrade
"<percorso_del_file_di_backup>/database.gz"
```

A tutti i file di Server Dr.Web sostituiti è necessario assegnare gli stessi permessi di sistema di quelli selezionati nell'installazione di Server Dr.Web precedente (persa).

In caso di SO della famiglia UNIX: `rw` per `drwcs:drwcs`.

9. Avviare il Server Dr.Web.
10. Accertarsi che siano integri e aggiornati i dati ottenuti dalla copia di backup del database: impostazioni di Agent Dr.Web, stato dell'albero della rete antivirus ecc.

11. Ripristinare la disponibilità di Server Dr.Web per Agent Dr.Web a seconda del metodo di isolamento di Server Dr.Web selezionato al passaggio 1.

> Se qualche Agent Dr.Web è stato installato dopo la creazione dell'ultimo backup, non potrà connettersi al Server Dr.Web dopo il ripristino del database da questo backup. È possibile trasferire tali postazioni in remoto in modalità nuovi arrivi. Nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** nella scheda **Generali** spuntare il flag **Trasferisci le postazioni non autenticate in nuovi arrivi**. Dalla lista a cascata **Modalità di registrazione dei nuovi arrivi** selezionare la variante **Consenti l'accesso automaticamente**. Premere **Salva** e riavviare il Server Dr.Web.
>
> Dopo che tutte le postazioni si connetteranno al nuovo Server Dr.Web, sostituire queste impostazioni di Server Dr.Web con le impostazioni adottate in conformità ai criteri aziendali.

Ripristino se non è disponibile alcun backup di Server Dr.Web

Per ripristinare Server dopo un errore di operazione, se nessuna copia di backup si è conservata

1. Selezionare il computer su cui verrà installato il nuovo Server Dr.Web. La connessione al server può essere ripristinata sia allo stesso computer (con lo stesso indirizzo) che a un altro (modificando nelle impostazioni degli Agent Dr.Web l'indirizzo per la connessione a Server Dr.Web).
   Affinché si possa eseguire la configurazione iniziale di Server Dr.Web e della rete antivirus prima della connessione degli Agent Dr.Web, isolare questo computer dagli Agent Dr.Web attivi: durante l'installazione modificare temporaneamente la porta per una porta diversa da quella di default 2193 (in seguito potrà essere modificata di nuovo per quella di default). Dopo la configurazione iniziale controllare la connessione a Server Dr.Web sulla base dell'esempio di uno o due Agent Dr.Web.
   Il Server può essere ripristinato sia sullo stesso computer (con lo stesso indirizzo) che su un altro modificando nelle impostazioni degli Agent Dr.Web l'indirizzo per la connessione al server.
2. Installare il nuovo Server Dr.Web.
3. Nella sezione **Amministrazione** → **Gestione licenze** aggiungere la chiave di licenza dall'installazione di Server Dr.Web precedente e distribuirla ai gruppi corrispondenti, in particolare al gruppo **Everyone**. Il passaggio è obbligatorio se durante l'installazione di Server Dr.Web la chiave di licenza non è stata impostata.
4. Aggiornare da SAM il repository del Server Dr.Web installato:
   a) Aprire la sezione del Pannello di controllo **Amministrazione** → **Stato del repository**.
   b) 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.
5. Se sono disponibili nuove versioni del software Server Dr.Web, aggiornarlo all'ultima versione:

a) Aprire la sezione del Pannello di controllo **Amministrazione** → **Server Dr.Web**.

b) Per passare all'elenco delle versioni di Server Dr.Web, premere la versione corrente di Server Dr.Web o il pulsante **Elenco delle versioni**. Si aprirà la sezione **Aggiornamenti del Server Dr.Web** con un elenco di aggiornamenti e backup di Server Dr.Web disponibili.

c) Per passare alla nuova versione di Server Dr.Web, spuntare il flag di fronte all'ultima versione nell'elenco **Tutte le versioni** e premere il pulsante **Salva**.

d) Attendere che il processo di aggiornamento di Server Dr.Web sia completato.

6. Modificare le impostazioni di connessione delle postazioni nella configurazione di Server Dr.Web:

   a) Aprire la sezione **Amministrazione** → **Configurazione del Server Dr.Web**.

   b) Nella scheda **Generali** spuntare il flag **Trasferisci le postazioni non autenticate in nuovi arrivi**.

   c) Nella scheda **Generali** nella lista a cascata **Modalità di registrazione dei nuovi arrivi** selezionare la variante **Consenti l'accesso automaticamente**.

   d) Premere **Salva** e riavviare Server Dr.Web.

7. Nella sezione **Rete antivirus** del Pannello di controllo creare gruppi custom nell'albero della rete antivirus per analogia con la versione precedente. Se necessario, creare regole automatiche di appartenenza delle postazioni ai gruppi custom creati.

8. Se necessario, configurare le impostazioni di Agent Dr.Web e le impostazioni di Server Dr.Web (ad eccezione delle impostazioni temporanee dal passaggio 6) per analogia con la versione precedente.

9. Se necessario, modificare le impostazioni del repository nella sezione **Amministrazione** → **Configurazione dettagliata del repository**.

10. Ripristinare la disponibilità di Server Dr.Web per Agent Dr.Web a seconda del metodo di isolamento di Server Dr.Web selezionato al passaggio 1.

11. Sostituire il certificato su tutte le postazioni della rete che dovranno connettersi al nuovo Server Dr.Web. Il certificato può essere scaricato nella sezione **Amministrazione** → **Chiavi di crittografia**.

    - Se l'auto-protezione è attivata, copiare sulla postazione il certificato creato durante l'installazione del nuovo Server Dr.Web ed eseguire il seguente comando:

      ```
      %ProgramFiles%\DrWeb\es-service.exe -p <chiave>
      ```

      o

      ```
      %ProgramFiles%\DrWeb\es-service.exe --addcert=<chiave>
      ```

      Come *<chiave>* indicare il percorso del certificato del server copiato.

      Come risultato, il certificato verrà copiato nella directory di installazione di Agent Dr.Web. Di default è la directory `%ProgramFiles%\DrWeb` (per maggiori informazioni v. Allegato G2. Agent Dr.Web per Windows).

- Se l'auto-protezione sulla postazione è disattivata, è possibile prendere il certificato creato durante l'installazione del nuovo Server Dr.Web e collocarlo nella directory indicata sopra.

12. Se si ripristinava la connessione a Server Dr.Web a un altro computer, modificare l'indirizzo per la connessione al server nelle impostazioni degli Agent Dr.Web.

Come indirizzo di Server Dr.Web è consigliato utilizzare il nome di server in formato FQDN.

13. Dopo che tutte le postazioni si connetteranno al nuovo Server Dr.Web, sostituire le impostazioni di Server Dr.Web configurate al passaggio 6 con le impostazioni adottate in conformità ai criteri aziendali.

Ripristino di un nodo del cluster di Server Dr.Web

Se uno dei Server Dr.Web di un cluster non funziona per qualche motivo, gli Agent Dr.Web che hanno perso la connessione con esso si collegheranno a un altro nodo del cluster. Nel caso di un errore fatale di Server Dr.Web, è necessario ripristinarlo (installare Server Dr.Web e aggiungerlo nuovamente al cluster).

Installazione di Server Dr.Web per la successiva aggiunta al cluster

Per poter utilizzare un database unico, tutti i Server Dr.Web devono essere della stessa versione.

È possibile utilizzare una copia di backup del Server Dr.Web guasto, se disponibile, per semplificare la procedura di ripristino del nodo del cluster. La copia di backup contiene le impostazioni di repository, i file di configurazione, le chiavi di cifratura, i certificati, il backup del database interno.

Durante l'installazione di Server Dr.Web per la sostituzione di un nodo di cluster guasto, attenersi alle prescrizioni riportate di seguito.

Installazione di Server su SO della famiglia UNIX

Seguire le istruzioni da **Guida all'installazione**, sezione Installazione di Server Dr.Web per SO della famiglia UNIX. È possibile installare un nuovo Server Dr.Web o utilizzare una copia di backup del Server Dr.Web guasto che faceva parte del cluster.

Di default le copie di backup sono conservate nelle seguenti directory:

- per Server Dr.Web per SO Linux — `/var/opt/drwcs/backup`,
- per Server Dr.Web per SO FreeBSD — `/var/drwcs/backup`.

Un Server Dr.Web installato da una copia di backup utilizzerà il database comune utilizzato dai nodi del cluster.

Nel caso di installazione senza impiego di una copia di backup, Server Dr.Web utilizzerà il database incorporato. Dopo il completamento del processo di installazione, sarà necessario cambiare il Server Dr.Web al database comune utilizzato dal cluster.

Istallazione di Server Dr.Web su SO Windows

È possibile installare un nuovo Server Dr.Web o utilizzare una copia di backup del Server Dr.Web guasto che faceva parte del cluster. Di default le copie di backup sono conservate nella directory <*disco_di_installazione*>`:\DrWeb Backup`.

Seguire le istruzioni da **Guida all'installazione**, sezione Installazione di Server Dr.Web per SO Windows, prestando attenzione ai seguenti momenti:

- L'installazione con la connessione all'database esterno non è consigliata in quanto durante la connessione di Server Dr.Web al cluster è possibile la perdita dei dati memorizzati nel database.
- Nel caso di installazione da una copia di backup, indicare i seguenti parametri di configurazione:
  - **Driver del database**: selezionare l'opzione **SQLite (database incorporato)**. Non è consigliato lasciare il database esterno in quanto questo potrebbe provocare la perdita di dati durante la connessione di Server Dr.Web al cluster. Il database esterno utilizzato nel cluster deve essere connesso dopo il completamento dell'installazione di Server Dr.Web.
  - **Configurazione della rete**: indicare i valori aggiornati dei campi **Interfaccia** e **Porta**. Se il flag **Attiva il servizio di rilevamento di Server Dr.Web** non è impostato, impostarlo in modo che Server Dr.Web possa scambiarsi informazioni con gli altri nodi del cluster tramite gruppo multicast. Di seguito sono indicati i parametri del gruppo multicast utilizzato dai Server Dr.Web in un cluster.

  Per gli altri parametri i valori possono essere impostati secondo la sezione **Installazione di Server Dr.Web per SO Windows**.
- Nel caso di installazione di un nuovo Server Dr.Web, indicare i seguenti parametri di configurazione:
  - **Configurazione del Server Dr.Web**: indicare i percorsi del file di configurazione `drwcsd.conf` e della chiave di cifratura privata, che venivano utilizzati dal Server Dr.Web guasto, se disponibili. In caso contrario, lasciare i campi vuoti per creare nuove chiavi di cifratura, certificato e file di configurazione con le impostazioni di default. I valori di questi parametri dovranno essere modificati dopo l'installazione di Server Dr.Web.
  - **Driver del database**: selezionare l'opzione **SQLite (database incorporato)**. Il database esterno utilizzato nel cluster deve essere connesso dopo il completamento dell'installazione di Server Dr.Web.
  - **Configurazione della rete**: indicare i valori aggiornati dei campi **Interfaccia** e **Porta**. Spuntare il flag **Attiva il servizio di rilevamento di Server Dr.Web** in modo che Server Dr.Web possa scambiarsi informazioni con gli altri nodi del cluster tramite gruppo

multicast. Di seguito sono indicati i parametri del gruppo multicast utilizzato dai Server Dr.Web in un cluster.

Per gli altri parametri i valori possono essere impostati secondo la sezione **Installazione di Server Dr.Web per SO Windows**.

Inserimento di Server Dr.Web nel cluster

Per connettere il Server Dr.Web installato al cluster, seguire le prescrizioni riportate in **Manuale amministratore**, sezione Cluster dei Server Dr.Web.

Gestione del livello di registrazione del log di Server Dr.Web sotto SO Windows

Il livello di dettaglio del log di Server Dr.Web sotto SO Windows può essere modificato in uno dei seguenti modi:

- Tramite la sezione **Configurazione del Server Dr.Web → Log** nel Pannello di controllo.

  Questo metodo è preferibile. Nella sezione **Log** è possibile impostare qualsiasi livello di dettaglio possibile del log di Server Dr.Web, e inoltre definire alcune altre impostazioni.

  Informazioni dettagliate sono riportate in **Manuale amministratore**, sezione Configurazione del Server Dr.Web → Log.

- Tramite il comando console:

  ```
  drwcsd [<opzioni>] install
  ```

  È possibile impostare qualsiasi livello di dettaglio possibile del log di Server Dr.Web tramite l'opzione `--verbosity`.

  Informazioni dettagliate sulle opzioni della riga di comando per la gestione del Server Dr.Web sono ritrovabili nella sezione G3.8. Descrizione delle opzioni.

  Un esempio del comando per impostare il livello di registrazione del log **Tracciamento**:

  ```
  drwcsd --daemon "--home=C:\Program Files\DrWeb Server" "--bin-root=C:
  \Program Files\DrWeb Server" "--var-root=C:\Program Files\DrWeb Server\var"
  --verbosity=trace --log="C:\Program Files\DrWeb Server\var\install.log" --
  rotate=10,50m install
  ```

  Le altre opzioni sono obbligatorie, in particolare, se sono stati ridefiniti i percorsi standard di installazione del Server Dr.Web e delle sue directory di lavoro.

  Dopo aver modificato il livello di registrazione del log, è necessario riavviare il Server Dr.Web:

  ```
  drwcsd restart
  ```

- Tramite comandi locati nel menu principale di SO Windows **Start**.

In tale caso sono disponibili solo due possibili livelli di dettaglio del log: **Dettagliato** o **Standard**:

a) **Programmi** → **Dr.Web Server** → **Log dettagliato**
o
Programmi → **Dr.Web Server** → **Log standard**

b) **Programmi** → **Dr.Web Server** → **Riavvia**

Rilevamento automatico della posizione di una postazione con SO Android

Dr.Web Enterprise Security Suite permette di fornire automaticamente all'amministratore informazioni sulla posizione geografica dei dispositivi mobili protetti con SO Android.

Per determinare la posizione di un dispositivo mobile

1. Configurare la trasmissione sul Server Dr.Web dei dati circa la posizione del dispositivo mobile protetto:
   a) Nel Pannello di controllo della sicurezza Dr.Web, nella sezione **Rete antivirus**, nell'albero della rete selezionare la postazione Android richiesta o il gruppo di postazioni Android richiesto.
   b) Selezionare la voce del menu di gestione **Dr.Web per Android**.
   c) Nella scheda **Generali** spuntare il flag **Localizza**. Dalla lista a discesa **Periodicità di trasmissione delle coordinate** selezionare un valore in base a cui verranno aggiornati i dati sulla posizione del dispositivo.
   d) Salvare le modifiche apportate.
2. Il rilevamento automatico della posizione viene effettuato in uno dei seguenti modi:
   - Se sul dispositivo mobile dell'utente sono attivati i provider di localizzazione (GPS, reti mobili) e il segnale è stabile, il rilevamento della posizione viene effettuato tramite gli strumenti del dispositivo mobile stesso.
   - Se sul dispositivo mobile dell'utente sono disattivati i provider di localizzazione (GPS, reti mobili) o è assente il segnale GPS, Dr.Web Enterprise Security Suite fornisce la possibilità di utilizzare la tecnologia Yandex.Locator per determinare la posizione del dispositivo mobile in base alle coordinate di torri di telefonia mobile (GSM, 3D, LTE) e in base a WiFi ID.
     Per configurare la tecnologia Yandex.Locator, è necessario attivare e configurare **Estensione Yandex.Locator**:
     a) Ottenere la chiave API sul sito web dell'azienda Yandex all'indirizzo: https://yandex.ru/dev/locator/keys/.
     b) Nel Pannello di controllo della sicurezza Dr.Web, nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Moduli** spuntare il flag **Estensione Yandex.Locator**.
     c) Nel campo **Chiave API** inserire la chiave ottenuta nel passaggio a).

d) Salvare le modifiche apportate e riavviare il Server Dr.Web.

L'utilizzo di WiFi ID è possibile solo per dispositivi mobili con SO Android 5.1 e versioni precedenti.

3. Per visualizzare la posizione di una postazione nel Pannello di controllo della sicurezza Dr.Web:
   a) Nella sezione **Rete antivirus**, nell'albero della rete selezionare una postazione per cui nel passaggio 1 sono state definite le impostazioni corrispondenti.
   b) Nelle proprietà della postazione, nella sezione **Posizione** verranno riempite automaticamente le coordinate geografiche ricevute dal dispositivo mobile.
   c) Premere **Mostra sulla mappa** per visualizzare la posizione geografica del dispositivo mobile su OpenStreetMap in base alle coordinate ricevute.

Criteri di analisi funzionale

I criteri di analisi funzionale consentono di costruire la massima protezione, pertanto, dovrebbero essere impostati quando si configura l'analisi funzionale.

Nella sezione **Criteri di analisi funzionale** sono indicate le categorie che possono essere utilizzate per la protezione del profilo. La scelta della categoria dipende dal livello di sicurezza richiesto e dalle caratteristiche del sistema. Il valore di tutti i parametri di default è **Disattivato**.

Categorie di criteri di analisi funzionale

Avvio di applicazioni

Attiva il controllo di processi avviati per la lista delle applicazioni affidabili.

- *Proibisci l'avvio di applicazioni firmate con certificati conosciuti in Doctor Web come certificati per adware.*
  Blocca l'avvio di applicazioni che possono distribuire pubblicità.
- *Proibisci l'avvio di applicazioni firmate con certificati conosciuti in Doctor Web come grigi.*
  Blocca l'avvio di applicazioni firmate con certificati "grigi". Tali certificati vengono spesso utilizzati per firmare applicazioni non sicure.
- *Proibisci l'avvio di applicazioni firmate con certificati conosciuti in Doctor Web come certificati per hacktool.*
  Blocca l'avvio di applicazioni firmate con certificati utilizzati per l'hacking di programmi. L'uso di questo criterio è consigliato.
- *Proibisci l'avvio di applicazioni firmate con certificati falsi/danneggiati.*
  Blocca l'avvio di applicazioni malevole che sono firmate con certificati non validi (danneggiati o attaccati a un file binario per impedire l'identificazione della minaccia — per esempio, certificati di software legittimi). Può anche aiutare ai tentativi di modificare un file legittimo o infettarlo con un virus. L'uso di questo criterio è consigliato.
- *Proibisci l'avvio di applicazioni firmate con certificati conosciuti in Doctor Web come certificati per programmi malevoli.*
  Blocca l'avvio di applicazioni firmate con certificati compromessi. L'uso di questo criterio è consigliato.
- *Proibisci l'avvio di applicazioni firmate con certificati revocati.*
  Blocca l'avvio di applicazioni firmate con certificati rubati o compromessi. L'uso di questo criterio è consigliato in quanto consente di impedire preventivamente l'avvio di applicazioni potenzialmente malevole.
- *Proibisci l'avvio di applicazioni firmate con certificati autofirmati.*
  Blocca software senza licenza che potrebbero risultare malevoli. I programmi malevoli possono aggiungere ai propri file binari una firma falsa con un nome noto (per esempio, Microsoft) e/o aggiungere al sistema un certificato radice in modo che tale file venga mostrato e riconosciuto dal sistema operativo come recante una firma legittima.

- *Proibisci l'avvio di applicazioni non firmate*.
  Blocca l'avvio di applicazioni potenzialmente malevole e inaffidabili la cui origine è sconosciuta.
- *Proibisci l'avvio di utility da Sysinternals*.
  Protegge dalla compromissione del sistema tramite le utility Sysinternals.

> Se nella scheda **Permessi** è selezionato il flag **Consenti l'avvio di applicazioni di sistema e applicazioni da Microsoft**, le utility Sysinternals verranno avviate anche se l'avvio è vietato.

- *Proibisci l'avvio di applicazioni da flussi alternativi NTFS (ADS)*.
  Le applicazioni da flussi alternativi NTFS (ADS) sono spesso malevole, pertanto, l'uso di questo criterio è obbligatorio.
- *Proibisci l'avvio di applicazioni dalla rete e risorse condivise*.
  L'avvio di applicazioni dalla rete e da risorse condivise è scenario atipico e rappresenta un rischio per la sicurezza del sistema. Questo criterio è consigliato per l'uso.
- *Proibisci l'avvio di applicazioni da supporti rimovibili*.
  L'avvio di applicazioni da supporti rimovibili è scenario atipico e rappresenta un rischio per la sicurezza del sistema. Questo criterio è consigliato per l'uso.
- *Proibisci l'avvio di applicazioni da directory temporanee*.
  Blocca l'avvio di applicazioni da directory temporanee.
- *Proibisci l'avvio di applicazioni Windows/Microsoft Store (solo per Windows 8 e superiori)*.
  Blocca l'avvio di applicazioni caricate da Windows/Microsoft Store.
- *Proibisci l'avvio di applicazioni con estensione doppia/atipica*.
  Blocca l'avvio di file sospetti con estensione non standard (per esempio, `*.jpg.exe`).
- *Proibisci l'avvio di shell bash e applicazioni WSL (solo per Windows 10 e superiori)*.
  Blocca l'avvio di shell di comandi Bash e applicazioni WSL.

Eccezioni ai blocchi sopra:

- *Consenti l'avvio di applicazioni di sistema e applicazioni da Microsoft*.
- *Consenti l'avvio di applicazioni conosciute/ritenute affidabili da Doctor Web*.
  Se è attivata, è consentito il funzionamento di applicazioni firmate con un certificato affidabile.

> Se questa opzione è attivata, è consentito il funzionamento di applicazioni firmate con un certificato affidabile. Questa funzionalità consente di non creare un numero eccessivo di regole basandosi su dati già verificati da Dr.Web. L'affidabilità in questo caso si basa sulla crittografia, un database esteso e in costante crescita.

Caricamento ed esecuzione di moduli

Attiva il controllo di moduli caricati. I criteri possono funzionare in due modalità:

- *Controlla il caricamento e l'esecuzione di tutti i moduli*. Opzione globale che attiva il controllo di moduli per le applicazioni affidabili. Questa modalità consuma molte

risorse, pertanto, si consiglia di utilizzarla solo quando è necessario un controllo aumentato.

- *Controlla il caricamento e l'esecuzione di moduli in applicazioni host*.
  Questa modalità consuma meno risorse. Controlla il funzionamento di moduli solo in processi utilizzati per la compromissione del sistema o per l'infiltrazione di software malevoli sotto le sembianze di un file di sistema o affidabile. Se non è necessario un controllo aumentato, utilizzare questa modalità. In questa modalità è possibile:

- *Proibisci il caricamento e l'esecuzione di moduli firmati con certificati conosciuti in Doctor Web come certificati per adware*.
  Blocca l'avvio di moduli che possono diffondere pubblicità.
- *Proibisci il caricamento e l'esecuzione di moduli firmati con certificati conosciuti in Doctor Web come grigi*.
  Blocca l'avvio di moduli firmati con certificati "grigi". Tali certificati vengono spesso utilizzati per firmare applicazioni non sicure.
- *Proibisci il caricamento e l'esecuzione di moduli firmati con certificati conosciuti in Doctor Web come certificati per hacktool*.
  Blocca l'avvio di moduli firmati con certificati utilizzati per l'hacking di programmi. L'uso di questo criterio è consigliato.
- *Proibisci il caricamento e l'esecuzione di moduli firmati con certificati falsi/danneggiati*.
  Blocca l'avvio di moduli malevoli che sono firmati con certificati non validi (danneggiati o attaccati a un file binario per impedire l'identificazione della minaccia — per esempio, certificati di software legittimi). Può anche aiutare ai tentativi di modificare un file legittimo o infettarlo con un virus. L'uso di questo criterio è consigliato.
- *Proibisci il caricamento e l'esecuzione di moduli firmati con certificati conosciuti in Doctor Web come certificati per programmi malevoli*.
  Blocca l'avvio di moduli firmati con certificati compromessi. L'uso di questo criterio è consigliato.
- *Proibisci il caricamento e l'esecuzione di moduli firmati con certificati revocati*.
  Blocca l'avvio di moduli firmati con certificati rubati o compromessi. L'uso di questo criterio è consigliato in quanto consente di impedire preventivamente l'avvio di applicazioni potenzialmente malevole.
- *Proibisci il caricamento e l'esecuzione di moduli firmati con certificati autofirmati*.
  Blocca software senza licenza che potrebbero risultare malevoli. I programmi malevoli possono aggiungere ai propri file binari una firma falsa con un nome noto (per esempio, Microsoft) e/o aggiungere al sistema un certificato radice in modo che tale file venga mostrato e riconosciuto dal sistema operativo come recante una firma legittima.
- *Proibisci il caricamento e l'esecuzione di moduli non firmati*.
  Blocca l'avvio di moduli potenzialmente malevoli e inaffidabili la cui origine è sconosciuta.
- *Proibisci il caricamento e l'esecuzione di moduli da flussi alternativi NTFS (ADS)*.
  I moduli da flussi alternativi NTFS (ADS) sono spesso malevoli, pertanto, l'uso di questo criterio è obbligatorio.

- *Proibisci il caricamento e l'esecuzione di moduli dalla rete e risorse condivise*.
  L'avvio di moduli dalla rete e da risorse condivise è scenario atipico e rappresenta un rischio per la sicurezza del sistema. Questo criterio è consigliato per l'uso.
- *Proibisci il caricamento e l'esecuzione di moduli da supporti rimovibili*.
  L'avvio di moduli da supporti rimovibili è scenario atipico e rappresenta un rischio per la sicurezza del sistema. Questo criterio è consigliato per l'uso.
- *Proibisci il caricamento e l'esecuzione di moduli da directory temporanee*.
  Blocca l'avvio di moduli da directory temporanee.
- *Proibisci il caricamento e l'esecuzione di moduli con estensione doppia/atipica*.
  Blocca l'avvio di moduli sospetti con estensione non standard (per esempio, *.jpg.exe).

Eccezioni ai blocchi sopra:

- *Consenti il caricamento e l'esecuzione di moduli di sistema e di moduli da Microsoft*.
- *Consenti il caricamento e l'esecuzione di moduli conosciuti/ritenuti affidabili da Doctor Web*.
  Se è attivata, è consentito il funzionamento di moduli firmati con un certificato affidabile.

Avvio di interpreti di script

Attiva il controllo di script avviati per la lista delle applicazioni affidabili.

- *Proibisci l'avvio di script CMD/BAT*.
  Blocca l'avvio di file con estensioni `cmd` e `bat`.
- *Proibisci l'avvio di script HTA*.
  Blocca l'avvio di script HTA. Tali script possono elaborare script malevoli e scaricare sul computer file eseguibili che possono arrecare danno al sistema.
- *Proibisci l'avvio di VBScript/JavaScript*.
  Blocca l'avvio di applicazioni scritte nei linguaggi di scripting VBScript e JavaScript. Tali applicazioni possono elaborare script malevoli e scaricare sul computer file eseguibili che possono arrecare danno al sistema.
- *Proibisci l'avvio di script PowerShell*.
  Blocca l'avvio di script scritti nel linguaggio di scripting PowerShell. Tali script possono elaborare script malevoli e scaricare sul computer file eseguibili che possono arrecare danno al sistema.
- *Proibisci l'avvio di script REG*.
  Blocca l'avvio di script di registro (file con estensione `reg`). Tali file possono essere utilizzati per l'aggiunta o la modifica di valori nel registro.
- *Proibisci l'avvio di script da flussi alternativi NTFS (ADS)*.
  Le applicazioni da flussi alternativi NTFS (ADS) sono spesso malevole, pertanto, l'uso di questo criterio è obbligatorio.
- *Proibisci l'avvio di script dalla rete e risorse condivise*.
  L'avvio di script dalla rete e da risorse condivise è scenario atipico e rappresenta un rischio per la sicurezza del sistema. Questo criterio è consigliato per l'uso.

- *Proibisci l'avvio di script da supporti rimovibili*.
  L'avvio di script da supporti rimovibili è scenario atipico e rappresenta un rischio per la sicurezza del sistema. Questo criterio è consigliato per l'uso.
- *Proibisci l'avvio di script da directory temporanee*.
  Blocca l'avvio di script da directory temporanee.

Eccezioni ai blocchi sopra:

- *Consenti l'avvio di script di sistema e di script da Microsoft*.
- *Consenti l'avvio di script conosciuti/ritenuti affidabili da Doctor Web*.
  Se è attivata, è consentito l'avvio di script firmati con un certificato affidabile.

Caricamento dei driver

Attiva il controllo di driver caricati per la lista delle applicazioni affidabili.

- *Proibisci il caricamento di driver firmati con certificati conosciuti in Doctor Web come certificati per adware*.
  Blocca l'avvio di driver che possono diffondere pubblicità.
- *Proibisci il caricamento di driver firmati con certificati conosciuti in Doctor Web come grigi*.
  Blocca l'avvio di driver firmati con certificati "grigi". Tali certificati vengono spesso utilizzati per firmare applicazioni non sicure.
- *Proibisci il caricamento di driver firmati con certificati conosciuti in Doctor Web come certificati per hacktool*.
  Blocca l'avvio di driver firmati con certificati utilizzati per l'hacking di programmi. L'uso di questo criterio è consigliato.
- *Proibisci il caricamento di driver firmati con certificati falsi/danneggiati*.
  Blocca l'avvio di driver malevoli che sono firmati con certificati non validi (danneggiati o attaccati a un file binario per impedire l'identificazione della minaccia — per esempio, certificati di software legittimi). Può anche aiutare ai tentativi di modificare un file legittimo o infettarlo con un virus. L'uso di questo criterio è consigliato.
- *Proibisci il caricamento di driver firmati con certificati conosciuti in Doctor Web come certificati per programmi malevoli*.
  Blocca l'avvio di driver firmati con certificati compromessi. L'uso di questo criterio è consigliato.
- *Proibisci il caricamento di driver firmati con certificati revocati*.
  Blocca l'avvio di driver firmati con certificati rubati o compromessi. L'uso di questo criterio è consigliato in quanto consente di impedire preventivamente l'avvio di applicazioni potenzialmente malevole.
- *Proibisci il caricamento di driver firmati con certificati autofirmati*.
  Blocca software senza licenza che potrebbero risultare malevoli. I programmi malevoli possono aggiungere ai propri file binari una firma falsa con un nome noto (per esempio, Microsoft) e/o aggiungere al sistema un certificato radice in modo che tale file venga mostrato e riconosciuto dal sistema operativo come recante una firma legittima.

- *Proibisci il caricamento di driver non firmati.*
  Blocca l'avvio di driver potenzialmente malevoli e inaffidabili la cui origine è sconosciuta.
- *Proibisci il caricamento di driver da flussi alternativi NTFS (ADS).*
  Le applicazioni da flussi alternativi NTFS (ADS) sono spesso malevole, pertanto, l'uso di questo criterio è obbligatorio.
- *Proibisci il caricamento di driver dalla rete e risorse condivise.*
  Il caricamento di driver dalla rete e da risorse condivise è scenario atipico e rappresenta un rischio per la sicurezza del sistema. Questo criterio è consigliato per l'uso.
- *Proibisci il caricamento di driver da supporti rimovibili.*
  Il caricamento di driver da supporti rimovibili è scenario atipico e rappresenta un rischio per la sicurezza del sistema. Questo criterio è consigliato per l'uso.
- *Proibisci il caricamento di driver da directory temporanee.*
  Blocca il caricamento di driver da directory temporanee.
- *Proibisci il caricamento di versioni di driver vulnerabili dei software popolari.*
  Blocca il caricamento di versioni non sicure dei driver di software popolari. I driver di software legittimi, come per esempio, VirtualBox, Asus ecc. possono essere utilizzati per l'intrusione nel sistema tramite RDP. Se questa opzione è attivata, le versioni non sicure di questi driver verranno bloccate al caricamento.

Il divieto di caricare versioni vulnerabili dei driver di software popolari non può essere sovrapposto da eccezioni.

- Proibisci il caricamento di driver con estensione doppia / atipica.
  Blocca l'avvio di driver sospetti con estensione non standard (per esempio, *.jpg.exe).

Eccezioni ai blocchi sopra:

- *Consenti il caricamento di driver di sistema e di driver da Microsoft.*
- *Consenti il caricamento di driver conosciuti/ritenuti affidabili da Doctor Web.*
  Se è attivata, è consentito il caricamento di driver firmati con un certificato affidabile.

Installazione di pacchetti MSI

Attiva il controllo di pacchetti MSI avviati per la lista delle applicazioni affidabili.

- *Proibisci l'installazione di pacchetti firmati con certificati conosciuti in Doctor Web come certificati per adware.*
  Blocca l'avvio di pacchetti che possono diffondere pubblicità.
- *Proibisci l'installazione di pacchetti firmati con certificati conosciuti in Doctor Web come grigi.*
  Blocca l'avvio di pacchetti firmati con certificati "grigi". Tali certificati vengono spesso utilizzati per firmare applicazioni non sicure.
- *Proibisci l'installazione di pacchetti firmati con certificati conosciuti in Doctor Web come certificati per hacktool.*

Blocca l'avvio di pacchetti firmati con certificati utilizzati per l'hacking di programmi. L'uso di questo criterio è consigliato.

- *Proibisci l'installazione di pacchetti firmati con certificati falsi/danneggiati*.
  Blocca l'avvio di pacchetti malevoli che sono firmati con certificati non validi (danneggiati o attaccati a un file binario per impedire l'identificazione della minaccia — per esempio, certificati di software legittimi). Può anche aiutare ai tentativi di modificare un file legittimo o infettarlo con un virus. L'uso di questo criterio è consigliato.
- *Proibisci l'installazione di pacchetti firmati con certificati conosciuti in Doctor Web come certificati per programmi malevoli*.
  Blocca l'avvio di pacchetti firmati con certificati compromessi. L'uso di questo criterio è consigliato.
- *Proibisci l'installazione di pacchetti firmati con certificati revocati*.
  Blocca l'avvio di pacchetti firmati con certificati rubati o compromessi. L'uso di questo criterio è consigliato in quanto consente di impedire preventivamente l'avvio di applicazioni potenzialmente malevole.
- *Proibisci l'installazione di pacchetti firmati con certificati autofirmati*.
  Blocca software senza licenza che potrebbero risultare malevoli. I programmi malevoli possono aggiungere ai propri file binari una firma falsa con un nome noto (per esempio, Microsoft) e/o aggiungere al sistema un certificato radice in modo che tale file venga mostrato e riconosciuto dal sistema operativo come recante una firma legittima.
- *Proibisci l'installazione di pacchetti non firmati*.
  Blocca l'avvio di pacchetti potenzialmente malevoli e inaffidabili la cui origine è sconosciuta.
- *Proibisci l'installazione di pacchetti da flussi alternativi NTFS (ADS)*.
  Le applicazioni da flussi alternativi NTFS (ADS) sono spesso malevole, pertanto, l'uso di questo criterio è obbligatorio.
- *Proibisci l'installazione di pacchetti dalla rete e risorse condivise*.
  L'installazione di pacchetti dalla rete e da risorse condivise è scenario atipico e rappresenta un rischio per la sicurezza del sistema. Questo criterio è consigliato per l'uso.
- *Proibisci l'installazione di pacchetti da supporti rimovibili*.
  L'installazione di pacchetti da supporti rimovibili è scenario atipico e rappresenta un rischio per la sicurezza del sistema. Questo criterio è consigliato per l'uso.
- *Proibisci l'installazione di pacchetti da directory temporanee*.
  Blocca l'installazione di pacchetti da directory temporanee.

Eccezioni ai blocchi sopra:

- *Consenti l'installazione di pacchetti di sistema e di pacchetti da Microsoft*.
- *Consenti l'installazione di pacchetti conosciuti/ritenuti affidabili da Doctor Web*.
  Se è attivata, è consentita l'installazione di pacchetti firmati con un certificato affidabile.

Integrità di file eseguibili

Attiva il controllo dell'integrità di file eseguibili. I criteri **Integrità di file eseguibili** sono utilizzati solo su sistemi che funzionano in modalità ambiente affidabile. In tali sistemi tutti i processi vengono controllati dall'amministratore (per esempio, sportelli automatici e altri sistemi). Nel caso di utilizzo dei criteri **Integrità di file eseguibili** in altri sistemi il comportamento è imprevedibile fino al guasto alla postazione.

- *Proibisci la creazione di nuovi file eseguibili.*
  Blocca i tentativi di creazione di nuovi file eseguibili sul disco.
- *Proibisci la modifica di file eseguibili.*
  Blocca i tentativi di modifica dei file eseguibili esistenti sul disco.

Eccezioni ai blocchi sopra:

- *Consenti la creazione e la modifica di file eseguibili alle applicazioni di sistema firmate e alle applicazioni da Microsoft.*
- *Consenti la creazione e la modifica di file eseguibili alle applicazioni firmate che sono conosciute/ritenute affidabili da Doctor Web.*
  Se è attivata, è consentita l'installazione di pacchetti firmati con un certificato affidabile.

I criteri **Integrità di file eseguibili** non possono essere sovrapposti da regole di permesso/di divieto.

Esempi di utilizzo delle query al database di Server Dr.Web

Di seguito sono riportati esempi di query SQL al database PostgreSQL. Le query ad altri database possono contenere alcune differenze dovute alle particolarità del database stesso e del suo utilizzo.

Le funzionalità del linguaggio SQL non consentono di tenere in considerazione nelle query la gerarchia di gruppi e postazioni.

Per fare una query direttamente al database

1. Aprire il Pannello di controllo del Server Dr.Web.
2. Passare alla sezione **Amministrazione** → **Console SQL**.
3. Inserire la query SQL richiesta. Di seguito sono riportati esempi di query.
4. Premere il pulsante **Esegui**.

Esempi di query SQL

1. Trova le postazioni su cui è installata la versione server di SO Windows e su cui i database dei virus sono più vecchi del 2019.07.04-00:00:00 UTC (12.0).

```
SELECT
  stations.name Station,
  groups_list.name OS,
  station_products.crev Bases
FROM
  stations
  INNER JOIN groups_list ON groups_list.platform =(
    CAST(stations.lastos AS INTEGER) & ~15728640
  )
  AND (
    (
      CAST(stations.lastos AS INTEGER) & 2130706560
    ) = 33554560
  )
  INNER JOIN station_products ON station_products.id = stations.id
  AND station_products.product = '10-drwbases'
  AND station_products.crev < 12020190704000000;
```

2. Trova le postazioni che hanno nella sezione **Rete antivirus** → **Statistiche** → **Stato** record con la gravità **Alta** o **Massima**.

```
SELECT
  stations.name Station
FROM
  stations
WHERE
  id IN (
    SELECT
      DISTINCT id
    FROM
      station_status
    WHERE
      severity >= 1342177280
  );
```

3. Ottieni la corrispondenza tra stati e il numero delle postazioni che hanno questi stati.

```
SELECT
  code Code,
  COUNT(code) Num
FROM
  (
    SELECT
      DISTINCT id,
      code
    FROM
      station_status
  ) AS t
GROUP BY
  Code
ORDER BY
  Code;
```

4. Ottieni le 10 minacce più popolari che sono state rilevate dal 2019.06.01 al 2019.07.01 sulle postazioni appartenenti al gruppo con l'identificatore '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5' o a qualsiasi gruppo nidificato.

```
SELECT
  cat_virus.str Threat,
  COUNT(cat_virus.str) Num
```

```
FROM
  station_infection
  INNER JOIN cat_virus ON cat_virus.id = station_infection.virus
WHERE
  station_infection.infectiontime BETWEEN 20190601000000000
  AND 20190701000000000
  AND station_infection.id IN (
    SELECT
      sid
    FROM
      station_groups
    WHERE
      gid = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      OR gid IN (
        SELECT
          child
        FROM
          group_children
        WHERE
          id = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      )
  )
GROUP BY
  cat_virus.str
ORDER BY
  Num DESC
LIMIT
  10;
```

5. Ottieni le 10 postazioni più frequentemente infettate.

```
SELECT
  Station,
  Grp,
  Num
FROM
  (
    SELECT
      stations.id,
      groups_list.id,
      stations.name Station,
      groups_list.name Grp,
      COUNT(stations.id) Num
    FROM
      station_infection
      INNER JOIN stations ON station_infection.id = stations.id
      INNER JOIN groups_list ON groups_list.id = stations.gid
    GROUP BY
      stations.id,
      groups_list.id,
      stations.name,
      groups_list.name
    ORDER BY
      Num DESC
    LIMIT
      10
  ) AS t;
```

6. Rimuovi l'appartenenza di tutte le postazioni dai gruppi personalizzati che non sono primari per queste postazioni.

```
DELETE FROM
  station_groups;
INSERT INTO station_groups(sid, gid)
SELECT
  stations.id,
  groups_list.id
FROM
  stations
  INNER JOIN groups_list ON stations.gid = groups_list.id
  AND groups_list.type NOT IN(1, 4);
```

7. Trova gli oggetti della rete antivirus su cui il dominio specificato è presente nella white list del componente SpIDer Gate, nelle impostazioni individuali.

```
SELECT
  stations.name Station
FROM
  station_cfg
  INNER JOIN stations ON stations.id = station_cfg.id
WHERE
  station_cfg.component = 38
  AND station_cfg.name = 'WhiteVirUrlList'
  AND station_cfg.value = 'domain.tld';
SELECT
  groups_list.name Grp
FROM
  group_cfg
  INNER JOIN groups_list ON groups_list.id = group_cfg.id
WHERE
  group_cfg.component = 38
  AND group_cfg.name = 'WhiteVirUrlList'
  AND group_cfg.value = 'domain.tld';
SELECT
  policy_list.name Policy
FROM
  policy_cfg
  INNER JOIN policy_list ON policy_list.id = policy_cfg.id
WHERE
  policy_cfg.component = 38
  AND policy_cfg.name = 'WhiteVirUrlList'
  AND policy_cfg.value = 'domain.tld';
```

8. Ottieni dalla verifica gli eventi di accesso non riuscito degli amministratori al Pannello di controllo con i rispettivi codici di errore di autenticazione.

```
SELECT
  admin_activity.login Login,
  admin_activity.address Address,
  activity_data.value ErrorCode,
  admin_activity.createtime EventTimestamp
FROM
  admin_activity
  INNER JOIN activity_data ON admin_activity.record = activity_data.record
WHERE
  admin_activity.oper = 10100
  AND admin_activity.status != 1
  AND activity_data.item = 'Error';
```

9. Trova le postazioni con SO Windows su cui non sono installate le correzioni di sicurezza necessarie.

```
SELECT
  stations.name Station
FROM
  stations
WHERE
  id NOT IN (
    SELECT
      station_env_kb.id
    FROM
      station_env_kb
      INNER JOIN stations ON stations.id = station_env_kb.id
    WHERE
      (
        CAST(stations.lastos AS INTEGER) & 2130706432
      )= 33554432
      AND station_env_kb.name IN (
        SELECT
          id
        FROM
          env_strings
        WHERE
          str IN(
            'KB4012212', 'KB4012213', 'KB4012214',
            'KB4012215', 'KB4012216', 'KB4012217',
            'KB4012598'
          )
      )
  );
```

Capitolo 4: Risoluzione dei problemi

Diagnostica dei problemi di installazione remota

Il principio di installazione:

1. Il Server Dr.Web si connette alla risorsa `ADMIN$` su una macchina remota (`\\<macchina_remota>\ADMIN$\Temp`) e copia l'installer di rete `drwinst.exe` situato nella directory `webmin\install\windows` della directory di installazione di Server Dr.Web e il certificato SSL `drwcsd-certificate.pem` situato nella directory `etc` della directory di installazione di Server Dr.Web nella directory `\\<macchina_remota>\ADMIN$\Temp`.
2. Il Server Dr.Web esegue il file `drwinst.exe` sulla macchina remota con le opzioni della riga di comando corrispondenti alle impostazioni nel Pannello di controllo.

Per un'installazione di successo è necessario che sul Server Dr.Web da cui avviene l'installazione:

1. Sia disponibile la risorsa `ADMIN$\Temp` sulla macchina remota.

   Si può controllare la disponibilità nel seguente modo:

   Immettere nella barra degli indirizzi dell'applicazione `Windows Explorer`:

   `\\<macchina_remota>\ADMIN$\Temp`

   Deve comparire un invito di immissione del nome utente e della password di accesso a questa risorsa. Immettere le credenziali che erano indicate sulla pagina di installazione.

   La risorsa `ADMIN$\Temp` può essere non disponibile per le seguenti ragioni:

   a) l'account non ha permessi di amministratore;

   b) la macchina è disconnessa o il firewall blocca l'accesso alla porta 445;

   c) limitazioni di accesso remoto alla risorsa `ADMIN$\Temp` su SO Windows Vista e versioni successive se non fanno parte del dominio;

   d) nessun owner della directory o permessi dell'utente o del gruppo sulla directory insufficienti.
2. Si abbia accesso al file `drwinst.exe` e alla chiave di cifratura pubblica `*.pub`.

Nel Pannello di controllo vengono visualizzate le informazioni estese (fase e codice di errore) le quali aiutano ad individuare la causa dell'errore.

Lista degli errori di installazione in remoto di Agent Dr.Web

Fase	Errore	Causa
Connessione tramite SMB alla postazione <*host*>	Indirizzo errato della postazione <*host*>	L'indirizzo IP della postazione indicato per l'installazione di Agent Dr.Web non è un indirizzo IPv4/IPv6 corretto o non è possibile convertire il nome DNS in un indirizzo: tale nome DNS non esiste o il name server non è configurato correttamente.

	Errore di connessione tramite SMB alla postazione <*host*>	Impossibile connettersi alla postazione tramite SMB. Le possibili ragioni:
		• il servizio del server è disabilitato sulla postazione;
		• non è disponibile la porta TCP 445 sulla macchina remota, le possibili ragioni:
		  ▫ la macchina è disconnessa;
		  ▫ il firewall blocca la porta indicata;
		  ▫ sulla macchina remota è installato un sistema operativo diverso da Windows;
		• non è configurato il modello di condivisione e di protezione per gli account locali;
		• non è disponibile il server di autenticazione (controller di dominio);
		• utente sconosciuto o password non valida.

	Permessi insufficienti per aprire la risorsa condivisa <*share*> sulla postazione <*host*>	Non esiste la risorsa `ADMIN$` sulla macchina remota o mancano i permessi sufficienti per aprirla.
Invio dei file sulla postazione <*host*>	Non è stato trovato il percorso <*path*> nella risorsa condivisa <*share*> sulla postazione <*host*>	Nessuna directory `ADMIN$/TEMP`.
	Impossibile creare la directory temporanea <*path*> nella risorsa condivisa <*share*> sulla postazione <*host*>	Impossibile creare una directory temporanea in `ADMIN$/TEMP`, per esempio mancano i permessi di scrittura.
	Impossibile rimuovere la directory temporanea <*path*> nella risorsa condivisa <*share*> sulla postazione <*host*>	Impossibile rimuovere la directory in `ADMIN$/TEMP` dopo il completamento della procedura. Per esempio, se l'amministratore non ha aspettato il completamento del servizio, o qualcuno ha aperto un file in questa directory.

Fase	Errore	Causa
	Impossibile aprire il file per la lettura <*path*> sul Server Dr.Web Impossibile leggere il file <*path*> sul Server Dr.Web	Nessun file dell'installer sul Server Dr.Web stesso, o sono stati impostati permessi errati sul file dell'installer.
	Impossibile aprire il file per la scrittura <*path*> nella risorsa condivisa <*share*> sulla postazione <*host*> Impossibile scrivere il file <*path*> nella risorsa condivisa <*share*> sulla postazione <*host*>	Permessi insufficienti per la lettura/scrittura dei file corrispondenti o nelle directory corrispondenti.
Creazione del servizio sulla postazione <*host*>	Errore di connessione al servizio server (srvsvc RPC) sulla postazione <*host*>	Non è disponibile la gestione dei servizi in remoto.
	Errore di connessione a SCM sulla postazione <*host*> Impossibile creare il servizio sulla postazione <*host*> Impossibile avviare il servizio sulla postazione <*host*> Impossibile arrestare il servizio sulla postazione <*host*> Impossibile rimuovere il servizio sulla postazione <*host*>	Permessi insufficienti per la gestione dei servizi.
Utilizzo del servizio sulla postazione <*host*>	Impossibile ottenere lo status del servizio sulla postazione <*host*>	Probabilmente, è un errore con SCM.
	L'installazione è stata interrotta secondo il timeout sulla postazione <*host*>	L'installer non ha fatto in tempo a installare Agent Dr.Web entro il periodo di tempo impostato. Le possibili ragioni: canale lento tra la postazione e il Server Dr.Web, non c'era abbastanza tempo per scaricare i dati necessari.
	Impossibile ottenere il percorso locale della risorsa condivisa <*share*> sulla postazione <*host*>	Impossibile determinare sulla postazione il percorso della risorsa `ADMIN$`.
	Servizio completato con un errore sulla postazione <*host*>. Status di	Errori dell'installer di Agent Dr.Web.

Fase	Errore	Causa
	completamento: <*state*>. Codice di errore: <*rc*>.	

Risoluzione di un errore del servizio BFE ad installazione di Agent Dr.Web per Windows

Per il funzionamento di alcuni componenti di Antivirus Dr.Web per Windows è necessario che sia in esecuzione il servizio modulo di filtraggio di base (BFE). Se questo servizio è mancante o danneggiato, l'installazione di Agent Dr.Web per Windows sarà impossibile. Un servizio BFE danneggiato o mancante può indicare la presenza di minacce per la sicurezza della postazione.

Se un tentativo di installazione di Agent Dr.Web per Windows è terminato con un errore del servizio BFE, eseguire le seguenti operazioni:

1. Scansionare il sistema della postazione tramite l'utility di cura CureNet! dall'azienda Doctor Web.

   Le versione demo dell'utility (diagnostica senza funzionalità di cura) può essere richiesta qui: https://download.drweb.com/curenet/.

   Qui è possibile prendere visione delle condizioni d'uso e del costo della versione completa dell'utility: https://estore.drweb.com/utilities/.
2. Avviare o riavviare manualmente il servizio BFE. Se il servizio BFE non è stato avviato o il servizio è assente nella lista, contattare il servizio di supporto tecnico Microsoft.
3. Avviare l'installer di Agent Dr.Web per Windows ed eseguire l'installazione secondo la procedura normale, riportata nella **Guida all'installazione**.

   Se il problema non è stato risolto, rivolgersi al servizio di supporto tecnico Doctor Web.

Supporto tecnico

Se si riscontrano problemi con l'installazione o il funzionamento dei prodotti della società, prima di contattare per l'assistenza il servizio di supporto tecnico, provare a trovare una soluzione nei seguenti modi:

1. Leggere le ultime versioni delle descrizioni e dei manuali sull'indirizzo https://download.drweb.com/doc/.
2. Leggere la sezione delle domande ricorrenti sull'indirizzo https://support.drweb.com/show_faq/.
3. Visitare i forum della società Doctor Web sull'indirizzo https://forum.drweb.com/.

Se provati questi modi, non si è riusciti a risolvere il problema, è possibile utilizzare uno dei seguenti modi per contattare il servizio di supporto tecnico della società Doctor Web:

1. Compilare il modulo web nella relativa sezione della pagina https://support.drweb.com/.
2. Chiamare il numero +7 (495) 789-45-86 o 8-800-333-7932 (numero gratuito per utenti in Russia).

Le informazioni sulle rappresentanze regionali e sedi della società Doctor Web sono ritrovabili sul sito ufficiale sull'indirizzo https://company.drweb.com/contacts/offices/.

Indice analitico