Dr.WEB

Enterprise Security Suite

Allegati

Dr.Web Enterprise Security Suite
Versione 11.0.2
Allegati
31/07/2020

Doctor Web, Sede centrale in Russia

Indirizzo: 125040, 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: Dr.Web Enterprise Security Suite

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** (file **drweb-11.0-esuite-install-manual-it.pdf**)

   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** (file **drweb-11.0-esuite-admin-manual-it.pdf**)

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

   L'amministratore della rete antivirus deve avere privilegi di amministratore di sistema o collaborare con l'amministratore della rete locale, deve essere conoscente in materia di strategia della protezione antivirus e conoscere in dettaglio i pacchetti antivirus Dr.Web per tutti i sistemi operativi utilizzati nella rete.

3. **Allegati** (file **drweb-11.0-esuite-appendices-it.pdf**)

   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. **Manuale dell'amministratore per la gestione delle postazioni**

   Contiene informazioni sulla configurazione centralizzata dei componenti del software antivirus delle postazioni attraverso il Pannello di controllo della sicurezza Dr.Web da parte dell'amministratore della rete antivirus.

3. **Manuali dell'utente**

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

Tutti i manuali elencati sopra 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 aggiornati in continuazione, e la loro ultima versione è ritrovabile sul sito ufficiale dell'azienda Doctor Web sull'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:

- 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,
- 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),
- DB, DBMS – database, database management system,
- SAM Dr.Web – Sistema di aggiornamento mondiale di Dr.Web,
- LAN – rete locale,
- SO – sistema operativo,
- Software – programmi per computer.

Capitolo 2: Allegati

Allegato A. Lista completa delle versioni supportate dei sistemi operativi

Per il Server Dr.Web

SO della famiglia UNIX

ALT Linux School Server 5.0

ALT Linux School Server 5.0 x86_64

ALT Linux School 6.0

ALT Linux School 6.0 x86_64

ALT Linux 7

ALT Linux 7 x86_64

ALT Linux SPT 6.0 certificato dal Servizio Federale di Controllo Tecnico e di Esportazione della Russia

ALT Linux SPT 6.0 certificato dal Servizio Federale di Controllo Tecnico e di Esportazione della Russia x86_64

Debian/GNU Linux 7 Wheezy

Debian/GNU Linux 7 Wheezy x86_64

Debian/GNU Linux 8 Jessie

Debian/GNU Linux 8 Jessie x86_64

Debian/GNU Linux 9 Stretch

Debian/GNU Linux 9 Stretch x86_64

FreeBSD 10.3

FreeBSD 10.3 amd64

FreeBSD 10.4

FreeBSD 10.4 amd64

FreeBSD 11.0

FreeBSD 11.0 amd64

openSUSE Leap 42.1

openSUSE Leap 42.1 x86_64

RedHat Enterprise Linux 6

RedHat Enterprise Linux 6 x86_64

RedHat Enterprise Linux 7

RedHat Enterprise Linux 7 x86_64
RedHat Fedora 24
RedHat Fedora 24 x86_64
RedHat Fedora 25
RedHat Fedora 25 x86_64
RedHat Fedora 26
RedHat Fedora 26 x86_64
RedHat Fedora 27
RedHat Fedora 27 x86_64
RedHat Fedora 28
RedHat Fedora 28 x86_64
SUSE Linux Enterprise Server 10
SUSE Linux Enterprise Server 10 x86_64
SUSE Linux Enterprise Server 11
SUSE Linux Enterprise Server 11 x86_64
SUSE Linux Enterprise Server 12
SUSE Linux Enterprise Server 12 x86_64
Ubuntu 10.04
Ubuntu 10.04 x86_64
Ubuntu 12.04
Ubuntu 12.04 x86_64
Ubuntu 14.04
Ubuntu 14.04 x86_64
Ubuntu 15.04
Ubuntu 15.04 x86_64
Ubuntu 15.10
Ubuntu 15.10 x86_64
Ubuntu 16.04
Ubuntu 16.04 x86_64
Ubuntu 16.10
Ubuntu 16.10 x86_64
Ubuntu 17.04
Ubuntu 17.04 x86_64
Linux glibc2.12
Linux glibc2.12 x86_64
Linux glibc2.13

Linux glibc2.13 x86_64
Linux glibc2.14
Linux glibc2.14 x86_64
Linux glibc2.15
Linux glibc2.15 x86_64
Linux glibc2.16
Linux glibc2.16 x86_64
Linux glibc2.17
Linux glibc2.17 x86_64
Linux glibc2.18
Linux glibc2.18 x86_64
Linux glibc2.19
Linux glibc2.19 x86_64
Linux glibc2.20
Linux glibc2.20 x86_64
Linux glibc2.21
Linux glibc2.21 x86_64
Linux glibc2.22
Linux glibc2.22 x86_64
Linux glibc2.23
Linux glibc2.23 x86_64
Linux glibc2.24
Linux glibc2.24 x86_64
Linux glibc2.25
Linux glibc2.25 x86_64
Linux glibc2.26
Linux glibc2.26 x86_64
Linux glibc2.27
Linux glibc2.27 x86_64
Astra Linux 1.3 x86_64
Astra Linux 1.4 x86_64
Astra Linux 1.5 x86_64
Astra Linux 1.6 x86_64
MCBC 5.0 x86_64

SO Windows

- 32 bit:

Windows XP Professional SP3

Windows Server 2003 SP2

Windows Vista

Windows Server 2008

Windows 7

Windows 8

Windows 8.1

Windows 10

- 64 bit:

Windows Vista

Windows Server 2008

Windows Server 2008 R2

Windows 7

Windows Server 2012

Windows Server 2012 R2

Windows 8

Windows 8.1

Windows 10

Windows Server 2016

Per l'Agent Dr.Web e il pacchetto antivirus

SO della famiglia UNIX

Linux per le piattaforme Intel x86/amd64 sulla base del kernel di una versione non inferiore a 2.6.37 che utilizza PAM e la libreria glibc versione 2.13 e superiori.

Se viene utilizzata una versione del sistema operativo a 64 bit, deve essere obbligatoriamente attivato il supporto dell'esecuzione delle applicazioni a 32 bit.

L'operatività del prodotto software è stata provata sulle seguenti distribuzioni **Linux** (per le piattaforme a 32 bit e a 64 bit):

Nome della distribuzione Linux	**Versioni**	**Librerie supplementari richieste per la versione del SO a 64 bit**
Astra Linux Special Edition (Smolensk)	1.5	x86_64
CentOS	6.9, 7.4	x86, x86_64
Debian	7.11, 8.10, 9.3	x86_64
Fedora	27	x86, x86_64
Red Hat Enterprise Linux	7.4	x86_64
SUSE Linux Enterprise Server	11 SP4, 12 SP3	x86_64
Ubuntu	14.04, 16.04	x86_64

Altre distribuzioni **Linux** che corrispondono ai requisiti descritti non sono state testate per la compatibilità con Antivirus, ma possono essere compatibili. Se si verificano problemi di compatibilità con la distribuzione in uso, contattare il supporto tecnico: https://support.drweb.com.

Se a Dr.Web Enterprise Security Suite si connettono dei componenti versione 6, per le informazioni circa i requisiti di sistema consultare la documentazione del componente corrispondente.

SO Windows

- 32 bit:

Windows XP Professional SP2 e superiori

Windows Server 2003 SP2

Windows Vista

Windows Server 2008

Windows 7

Windows 8

Windows 8.1

Windows 10

- 64 bit:

Windows Vista SP2 e superiori

Windows Server 2008 SP2

Windows Server 2008 R2

Windows 7

Windows Server 2012

Windows Server 2012 R2

Windows 8

Windows 8.1

Windows 10

Windows Server 2016

Se gli Agent Dr.Web vengono installati sulle postazioni SO Windows Vista o SO Windows Server 2008, è consigliato installare l'aggiornamento SP2 per il sistema operativo corrispondente. Altrimenti, potrebbero verificarsi degli errori causati dalle particolarità dell'interazione del sistema operativo con il software antivirus.

Non è possibile installare gli Agent Dr.Web su remoto sulle postazioni SO Windows edizioni Starter e Home.

macOS

Mac OS X 10.7 (Lion)

Mac OS X 10.7 Server (Lion Server)

OS X 10.8 (Mountain Lion)

OS X Server 10.8 (Mountain Lion Server)

OS X 10.9 (Mavericks)

OS X Server 10.9 (Mavericks Server)

OS X 10.10 (Yosemite)

OS X Server 10.10 (Yosemite Server)

OS X 10.11 (El Capitan)

OS X Server 10.11(El Capitan Server)

macOS 10.12 (Sierra)

macOS Server 10.12 (Sierra)

macOS 10.13 (High Sierra)

macOS Server 10.13 (High Sierra)

SO Android

Android 4.4

Android 5.0

Android 5.1

Android 6.0

Android 7.0

Android 7.1

Android 8.0

Android 8.1.

Allegato B. Impostazioni necessarie per l'utilizzo di DBMS. Parametri dei driver di DBMS

La struttura del database di Server Dr.Web può essere ottenuta sulla base dello script `sql init.sql` locato nella sottodirectory `etc` della directory di installazione di Server Dr.Web.

Come database di Server Dr.Web può essere utilizzato:

- DBMS incorporato;
- DBMS esterno.

DBMS incorporato

Per configurare l'utilizzo del DBMS incorporato per la conservazione e l'elaborazione di dati, si utilizzano i parametri riportati nella tabella **B-1**.

Tabella B-1. DBMS incorporato

Nome	Valore predefinito	Descrizione
DBFILE	database.sqlite	Percorso del file di database
CACHESIZE	2000	Dimensione della cache del database, misurata in pagine
SYNCHRONOUS	FULL	Modalità della scrittura sincrona su disco delle modifiche nel database: • FULL — scrittura su disco completamente sincrona, • NORMAL — scrittura sincrona dei dati critici, • OFF — scrittura asincrona

Come DBMS incorporato viene fornito SQLite3 – un DBMS supportato dal Server a partire dalla versione 10.

DMBS esterno

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

- DBMS Oracle. La configurazione è descritta in Allegato B2. Configurazione del driver di database per Oracle.
- DBMS PostgreSQL. Le impostazioni necessarie per il DBMS PostgreSQL sono descritte in Allegato B3. Utilizzo di DBMS PostgreSQL.

- Microsoft SQL Server/Microsoft SQL Server Express. Per accedere ai dati del DBMS, si può utilizzare il driver ODBC (la configurazione dei parametri del driver ODBC per SO Windows è riportata in Allegato B1. Configurazione del driver ODBC).

È supportato l'utilizzo di Microsoft SQL Server 2008 e superiori. È consigliato l'utilizzo di Microsoft SQL Server 2014 e superiori.

Il database Microsoft SQL Server Express non è consigliabile se viene messa in funzione una rete antivirus con un numero grande di postazioni (da 100 e più).

Se Microsoft SQL Server viene connesso come database esterno a un Server 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://support.microsoft.com/en-us/kb/321185.

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.

Le caratteristiche comparative dei DBMS incorporati ed esterni

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

Altrimenti, si deve utilizzare un database esterno.

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

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

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

- Nelle grandi reti antivirus (più di 200-300 postazioni) si consiglia di utilizzare un database esterno, più resistente ai malfunzionamenti dei database incorporati.
- 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.

B1. Configurazione del driver ODBC

Configurando l'utilizzo del DBMS esterno per la conservazione e l'elaborazione dei dati, si utilizzano i parametri riportati nella tabella **B-2** (i valori specifici sono riportati come un esempio).

Tabella B-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 nazionali – potrebbe causare errori di modifica dei parametri numerici.

- Esegui la conversione dei dati di tipo carattere – potrebbe 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.

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 http://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 il DBMS esterno, è necessario installare l'ultima versione del driver ODBC fornita insieme a questo DBMS. L'utilizzo del driver ODBC fornito insieme al SO Windows non è consigliato. L'eccezione sono i database forniti da Microsoft senza il driver ODBC.

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 e non 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**.

B2. Configurazione del driver di database per Oracle

Descrizione generale

Oracle Database (o Oracle DBMS) è 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 è necessario:

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 il database esterno il database Oracle attraverso la connessione ODBC, nel corso dell'installazione (dell'aggiornamento) di Server 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 superiori.

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, si utilizzano i parametri descritti nella tabella **B-3**.

Tabella B-3. Parametri del DBMS Oracle

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

B3. Utilizzo del DBMS PostgreSQL

Descrizione generale

PostgreSQL è 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 il database esterno per Dr.Web Enterprise Security Suite.

Per utilizzare PostgreSQL come il database esterno, è necessario:

1. Installare il server PostgreSQL.
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 inferiori alla **8.4**.
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 DBMS 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, si utilizzano i parametri descritti nella tabella **B-4**.

Tabella B-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
`dbname`	`drwcs`	Nome del database
`user`	`drwcs`	Nome utente
`password`	`drwcs`	Password
`options`		Opzioni di tracciamento/debug da inviare al server

Nome	Valore predefinito	Descrizione
`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 si possono trovare anche sull'indirizzo http://www.postgresql.org/docs/manuals/.

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, è necessario:

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.

B4. Utilizzo del DBMS MySQL

Descrizione generale

MySQL è 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, è necessario:

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 – da 5.5.14 a 5.7 e da 8.0.12 e superiori,
- MariaDB – 10.0, 10.1, 10.2.

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 5.X:

```
[mysqld]

innodb_large_prefix = true

innodb_file_format = barracuda

innodb_file_per_table = true

max_allowed_packet = 64M
```

Per MySQL versioni 8.X:

```
[mysqld]

innodb_file_per_table = true

max_allowed_packet = 64M
```

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

```
binlog_format = mixed
```

Allegato C. 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.

C1. Autenticazione se si usa 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 con questa password il server 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` – insuccesso e passaggio al meccanismo di autenticazione successivo.
6. Se in questa fase alcuni attributi non sono determinati, essi 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-11.00.2-<build>-esuite-modify-ad-schema-<versione_SO>.exe` (viene fornita separatamente dal pacchetto Server) 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 di amministratori).

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

C2. Autenticazione se si usa 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.
- `<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 tradurre il nome utente in DN. Questo script viene eseguito dopo i tentativi di utilizzo di tutte le regole `user-dn`, `user-dn-expr` in caso se non è stata trovata nessuna regola appropriata. Lo script ha un singolo parametro – il nome utente immesso. Lo script restituisce una stringa che contiene

DN o nulla. In caso se non è stata trovata nessuna regola appropriata e lo script non è abilitato oppure non ha restituito niente, il nome utente immesso viene usato 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 ci sono valori non definiti dell'attributo amministratore, allora 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.

C3. Autenticazione se si usa 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.

Attributo	Descrizione	Valore predefinito
		• `127.0.0.1` per il server sotto SO della famiglia UNIX.
`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`
`search`	DN dell'oggetto relativamente a cui viene effettuata la ricerca.	In assenza viene utilizzato il `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

C4. Sezioni subordinate dei permessi

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

N	**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.	Rete antivirus Rete antivirus → Generali → Proprietà

N	Permesso	Descrizione	Sezione del Pannello di controllo
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 Pagine dalla sezione **Configurazione** del menu di gestione
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.	
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. Deve contenere i gruppi dalla lista del permesso 1.	Rete antivirus Rete antivirus → Generali → Proprietà
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 eliminare.	

N	Permesso	Descrizione	Sezione del Pannello di controllo
		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 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 soltanto da /esuite/network/index.ds a condizione che il permesso 16 sia consentito.	
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.	
12*	**Visualizzazione di tabelle statistiche**	Una 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 per ricevere report periodici. Viene impostata una lista dei 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.	

N	Permesso	Descrizione	Sezione del Pannello di controllo
		Deve contenere i gruppi dalla lista del permesso 1.	
Gestione degli amministratori			
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 dello stesso. 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.	
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 è vietato, allora anche se il permesso 26 sia consentito per questo gruppo, l'amministratore non potrà disattivare l'ereditarietà o aumentare i permessi di un amministratore nel gruppo.	
Avanzate			

N	Permesso	Descrizione	Sezione del Pannello di controllo
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 consentito, non è disponibile l'installazione via rete da /esuite/network/index.ds.	Rete antivirus Amministrazione → Scanner di rete
17	**Approvazione di nuovi arrivi**	È disponibile la lista dei gruppi dal permesso 8. Questo permesso non può essere concesso se per l'amministratore è consentita la gestione solo di alcuni gruppi e non di tutti gli oggetti della rete antivirus. Ossia per il permesso 1 (**Visualizzazione delle proprietà dei gruppi di postazioni**) è impostato un set di gruppi.	Rete antivirus
18	**Visualizzazione del calendario del Server**	Visualizzazione della tabella **Log di esecuzione dei task**. Se i permessi 12 e 18 non sono consentiti, è vietato visualizzare la pagina con il calendario del Server. Se è consentito 12 e non è consentito 18, si può visualizzare il calendario riguardante le statistiche. Il task di invio di resoconti per un concreto amministratore viene visualizzato a seconda della disponibilità del permesso 12 e della disponibilità della notifica **Report periodico**, anche se il permesso 18 sia vietato.	Amministrazione → Configurazione → Scheduler del Server Dr.Web Amministrazione → Logs → Log di esecuzione dei task
19	**Modifica del calendario del Server**		Amministrazione → Configurazione → Scheduler del Server Dr.Web

N	Permesso	Descrizione	Sezione del Pannello di controllo
20	**Visualizzazione della configurazione del Server e di quella del repository**		Amministrazione → Configurazione → Configurazione del web server
21	**Modifica della configurazione del Server 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 → Gestione licenze
24	**Modifica della configurazione degli avvisi**		Amministrazione → Avvisi → Configurazione degli avvisi Amministrazione → Avvisi → Avvisi non inviati Amministrazione → Avvisi → Avvisi della web console

N	Permesso	Descrizione	Sezione del Pannello di controllo
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 da SAM.	Il pulsante **Aggiorna il repository** nella sezione **Stato del repository**
39	**Visualizzazione e modifica del gruppo di amministratori "Newbies"**	Per consentire all'amministratore di vedere il gruppo predefinito **Newbies** nell'albero degli amministratori e di modificarne il nome e la descrizione.	Amministrazione → Configurazione → Amministratori
42	**Modifica delle proprie impostazioni**	Permesso per modificare le proprie impostazioni dell'account amministratore.	Amministrazione → Configurazione → Amministratori

* 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 consentiti alcuni di questi permessi, allora all'amministratore saranno disponibili le funzionalità che corrispondono a questi permessi a prescindere da ciò se il gruppo consentito è primario per la postazione o meno. In questo caso l'autorizzazione ha priorità superiore: se la postazione rientra contemporaneamente in un gruppo consentito e in uno vietato, all'amministratore saranno disponibili le funzionalità che corrispondono ai permessi del gruppo consentito.

Allegato D. Sistema di avviso

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

D1. Descrizione degli avvisi predefiniti

Le variabili utilizzate nella modifica dei modelli di avviso sono riportate in Allegato D3.

Nome avviso	Ragione per l'invio dell'avviso	Informazioni addizionali
Amministratori		
Amministratore sconosciuto	Viene inviato se nel Pannello di controllo ha tentato di autenticarsi un amministratore con un nome utente sconosciuto.	
Errore di autenticazione dell'amministratore	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.	
Altro		
Errore di registrazione del log del Server	Viene inviato in caso di un errore durante la registrazione di informazioni nel log di funzionamento del Server. La causa dell'errore di registrazione nel log è riportata nel testo dell'avviso.	
Errore di rotazione del log del Server	Viene inviato in caso di un errore durante la rotazione del log di funzionamento del Server. La causa dell'errore di rotazione del log è riportata nel testo dell'avviso.	
Il server adiacente non si collega da molto tempo	Viene inviato secondo un task nel calendario del Server. Informa che un Server adiacente non si è	Il periodo, durante il quale un Server adiacente deve essere scollegato affinché venga mandato un avviso, viene impostato

Nome avviso	Ragione per l'invio dell'avviso	Informazioni addizionali
	collegato a questo Server da molto tempo. La data dell'ultima connessione è riportata nel testo dell'avviso.	nel task **Il server adiacente non si connette da molto tempo** nel calendario di Server che può essere configurato nella sezione **Amministrazione** → **Scheduler del Server Dr.Web**.
Report statistico	Viene inviato dopo la generazione di un report periodico secondo un task nel calendario del Server. Inoltre nell'avviso è riportato il percorso attraverso cui è possibile scaricare il file di report.	Il report viene creato secondo il task **Creazione del report statistico** nel calendario di Server che può essere configurato nella sezione **Amministrazione** → **Scheduler del Server Dr.Web**.
Report di riepilogo di Protezione preventiva	Viene inviato se è stato ricevuto dalle postazioni della rete un gran numero di report dal componente Protezione preventiva.	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.
Un'epidemia nella rete	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.	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.
Nuovi arrivi		
La postazione è in attesa di conferma	Viene inviato se una nuova postazione ha richiesto di essere connessa al Server e l'amministratore deve confermare o negare manualmente l'accesso per la postazione.	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 **Conferma l'accesso manualmente**.
La postazione è stata rifiutata automaticamente	Viene inviato se una nuova postazione ha richiesto di essere connessa al Server ed è stata declinata dal Server in maniera automatica.	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**.

Nome avviso	Ragione per l'invio dell'avviso	Informazioni addizionali
La postazione è stata rifiutata dall'amministratore	Viene inviato se una nuova postazione ha richiesto di essere connessa al Server ed è stata declinata dall'amministratore in maniera manuale.	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**.
Licenze		
È stato raggiunto il limite di licenze trasferite	Viene inviato se un Server adiacente ha richiesto più licenze da rilasciare di quante sono disponibili nella chiave di licenza.	
È stato raggiunto il limite di postazioni online	Viene inviato se con la connessione di una postazione al Server viene scoperto 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.	
È scaduto il periodo di trasferimento di licenze	Viene inviato se è scaduto il periodo di rilascio di licenze a un Server adiacente dalla chiave di licenza di questo Server.	Il periodo di rilascio di licenze ai Server adiacenti viene configurato nella sezione **Amministrazione** → **Configurazione del Server Dr.Web** → **Licenze**.
Chiave di licenza è aggiornata automaticamente	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.	Per informazioni dettagliate sull'aggiornamento automatico delle licenze consultare il **Manuale dell'amministratore**, p. Aggiornamento automatico delle licenze.
La chiave di licenza è bloccata	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 questa chiave non è possibile.	Per ricevere informazioni dettagliate sul motivo del blocco, contattare il servizio di supporto tecnico.

Nome avviso	Ragione per l'invio dell'avviso	Informazioni addizionali
Chiave di licenza non può essere aggiornata automaticamente	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.	Per informazioni dettagliate sull'aggiornamento automatico delle licenze consultare il **Manuale dell'amministratore**, p. Aggiornamento automatico delle licenze.
Scadenza della chiave di licenza	Viene inviato se la chiave di licenza è già scaduta.	
È stato superato il limite al numero di licenze	Viene inviato se all'avvio del Server 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.	
Si avvicina il limite di postazioni nel gruppo	Viene inviato se il numero di postazioni in un gruppo si sta avvicinando al limite di licenza indicato nella chiave assegnata a questo gruppo.	Numero di licenze libere rimaste nella chiave, con cui viene inviato l'avviso: meno di tre licenze o meno del 5% del totale licenze nella chiave.
Repository		
Stato aggiornato del prodotto nel repository	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.	
È stato avviato un aggiornamento del prodotto nel repository	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.	
Spazio insufficiente su disco	Viene inviato se sta per esaurirsi lo spazio sul disco su cui si trova la directory Server var.	Una mancanza di spazio su disco viene determinata se sono rimasti meno di 315 MB o meno di 1000 nodes (in caso dei SO

Nome avviso	Ragione per l'invio dell'avviso	Informazioni addizionali
		della famiglia UNIX), se questi valori non sono ridefiniti dalle variabili di ambiente.
L'aggiornamento del prodotto nel repository è stato congelato	Viene inviato se un prodotto in repository è stato congelato dall'amministratore. Il prodotto non viene aggiornato da SAM.	I prodotti dei repository, incluso il congelamento e lo scongelamento, vengono gestiti nella sezione **Amministrazione → Configurazione dettagliata del repository**.
Impossibile aggiornare il prodotto nel repository	Viene inviato se è occorso un errore durante l'aggiornamento da SAM di un prodotto di repository. Il nome del prodotto e la causa concreta dell'errore di aggiornamento vengono riportati nel testo dell'avviso.	
Il prodotto nel repository è stato aggiornato	Viene inviato in caso di un aggiornamento riuscito del repository da SAM.	
Postazioni		
Disconnessione inaspettata	Viene inviato se si è interrotta in modo anomalo una connessione con un client (postazione, installer di Agent, Server adiacente).	
Errore critico di aggiornamento della postazione	Viene inviato se da una postazione è arrivato un avviso di un errore occorso durante un aggiornamento dei componenti antivirus dal Server.	
Postazione sconosciuta	Viene inviato se una nuova postazione ha richiesto di essere connessa al Server ma non è stata ammessa alla considerazione della conferma o della negazione di registrazione.	
È stata rilevata una minaccia alla sicurezza	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.	

Nome avviso	Ragione per l'invio dell'avviso	Informazioni addizionali
È stata rilevata una minaccia alla sicurezza in base agli hash di minacce conosciuti	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.	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 (basta la licenza in almeno una delle chiavi di licenza utilizzate dal Server). La disponibilità della licenza è riportata 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).
Report di Protezione preventiva	Viene inviato quando viene ricevuto un report dal componente Protezione preventiva da una postazione di questo Server o di un Server adiacente.	
Report di Protezione preventiva sul rilevamento di minacce in base agli hash di minacce conosciuti	Viene inviato quando viene ricevuto un report dal componente Protezione preventiva da una postazione di questo Server o di un Server adiacente nel caso di rilevamento delle minacce dalla lista degli hash di minacce conosciuti.	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 (basta la licenza in almeno una delle chiavi di licenza utilizzate dal Server). La disponibilità della licenza è riportata 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).
Errore di autenticazione della postazione	Viene inviato se al tentativo di connessione al Server una postazione ha fornito credenziali non valide. Nell'avviso sono inoltre riportate le azioni successive che dipendono dai criteri di approvazione di postazioni.	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**.
Errore di scansione	Viene inviato se da una postazione è arrivato un avviso di un errore occorso durante una scansione.	
Errore di scansione al rilevamento di una minaccia in base agli	Viene inviato se è occorso un errore di scansione al rilevamento	L'avviso sul rilevamento in base alla lista degli hash conosciuti è possibile solo se è stato concesso in licenza l'uso dei

Nome avviso	Ragione per l'invio dell'avviso	Informazioni addizionali
hash di minacce conosciuti	di una minaccia dalla lista degli hash di minacce conosciuti.	bollettini degli hash di minacce conosciuti (basta la licenza in almeno una delle chiavi di licenza utilizzate dal Server). La disponibilità della licenza è riportata 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).
Impossibile creare un account di postazione	Viene inviato se non è possibile creare un nuovo account di postazione sul Server. I dettagli dell'errore vengono riportati nel file di log del Server.	
La postazione non si connette al server da molto tempo	Viene inviato secondo un task nel calendario del Server. Informa che una postazione non si collega a questo Server da molto tempo. La data dell'ultima connessione è riportata nel testo dell'avviso.	Il periodo, durante il quale una postazione deve essere scollegata affinché venga mandato un avviso, viene impostato nel task **La postazione non si connette da molto tempo** nel calendario di Server che può essere configurato nella sezione **Amministrazione** → **Scheduler del Server Dr.Web**.
La postazione è stata confermata automaticamente	Viene inviato se una nuova postazione ha richiesto di essere connessa al Server ed è stata confermata dal Server in maniera automatica.	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 **Consenti l'accesso automaticamente**.
La postazione è stata confermata dall'amministratore	Viene inviato se una nuova postazione ha richiesto di essere connessa al Server ed è stata confermata dall'amministratore in maniera manuale.	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 **Conferma l'accesso manualmente** e l'amministratore ha selezionato per la postazione la variante **Rete antivirus** → **Postazioni non confermate** → **Consenti alle postazioni selezionate di accedere e imposta gruppo primario**.
La postazione è già registrata	Viene inviato se al Server tenta di connettersi una postazione con un	

Nome avviso	Ragione per l'invio dell'avviso	Informazioni addizionali
	identificatore che coincide con l'identificatore di una postazione già connessa a questo Server.	
Statistiche di scansione	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.	
È necessario riavviare la postazione	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.	
È necessario riavviare la postazione per applicare gli aggiornamenti	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.	
Dispositivo è bloccato	Viene inviato se da una postazione è arrivato un avviso di ciò che uno dei dispositivi collegati alla postazione è stato bloccato dal componente antivirus Dr.Web.	
Installazioni		
L'installazione non è stata eseguita sulla	Viene inviato se un errore è occorso durante l'installazione di	

Nome avviso	Ragione per l'invio dell'avviso	Informazioni addizionali
postazione	Agent su una postazione. La causa concreta dell'errore è riportata nel testo dell'avviso.	
L'installazione sulla postazione è stata completata con successo	Viene inviato in caso di un'installazione riuscita di Agent su una postazione.	

D2. 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,
- Notifiche push.

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 D-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 D-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 D-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 D-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 D-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 D-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	-

D3. Parametri dei modelli del sistema di avviso

I testi dei messaggi vengono generati dal componente del Server, chiamato il motore dei modelli, sulla base del 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 superiori 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 di 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 di 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 dai caratteri <*replace1*>, se disponibili, i caratteri <*original2*> vengono sostituiti dai 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 D-7. 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 (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 e del Server,
- `SYS.BUILD` – data del build del Server,
- `SYS.DATE` – data di sistema attuale,
- `SYS.DATETIME` – data e ora di sistema attuali,
- `SYS.HOST` – nome DNS del Server,
- `SYS.MACHINE` – indirizzo di rete del computer con il Server installato,
- `SYS.OS` – nome del sistema operativo sul computer su cui è installato il Server,
- `SYS.PLATFORM` – piattaforma del Server,
- `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.

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 univoco della postazione,
- `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 protezione 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.

Variabili per tipo di messaggio

Amministratori

Messaggio	Variabili	Descrizione
Amministratore sconosciuto	`MSG.Login`	nome utente
	`MSG.Address`	indirizzo di rete del Pannello di controllo
Errore di autenticazione dell'amministratore	`MSG.Login`	nome utente
	`MSG.Address`	indirizzo di rete del Pannello di controllo
	`MSG.LoginErrorCode`	codice di errore numerico

Altro

Messaggio	Variabili	Descrizione
Errore di registrazione del log del Server	`MSG.Error`	testo dell'errore
Errore di rotazione del log del Server	`MSG.Error`	testo dell'errore
Il server adiacente non si collega da molto tempo	`MSG.LastDisconnectTime`	ora quando il Server era connesso l'ultima volta
	`MSG.StationName`	nome del Server adiacente
Report statistico	`MSG.Attachment`	percorso del report
	`MSG.AttachmentType`	tipo MIME
	`GEN.File`	nome del file del report
Report di riepilogo di Protezione preventiva	`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

Messaggio	Variabili	Descrizione
	MSG.UserAllowedIsShellGuard	suddivisione per tipo di reazione della Protezione preventiva con l'accesso consentito da parte dell'utente: • blocco del codice non autorizzato • 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	MSG.Infected	numero totale di minacce rilevate
	MSG.Virus	le minacce più diffuse

Licenze

Messaggio	Variabili	Descrizione
È stato raggiunto il limite di licenze trasferite	Viene inviato a tentativo di distribuire su un Server adiacente più licenze di quante ce ne sono nella chiave di licenza.	

Messaggio	Variabili	Descrizione
	MSG.ObjId	ID della chiave di licenza
È stato raggiunto il limite di postazioni online	Viene inviato quando una nuova postazione non può registrarsi sul Server per limitazioni di licenza.	
	MSG.ID	UUID della postazione
	MSG.StationName	nome della postazione
	Inoltre, sono disponibili le variabili generali per le postazioni riportate sopra.	
È scaduto il periodo di trasferimento di licenze	Viene inviato se è scaduto il tempo di distribuzione di licenze su un Server adiacente.	
	MSG.ObjId	ID della chiave di licenza
	MSG.Server	nome del Server adiacente
Chiave di licenza è aggiornata automaticamente	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.	
	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
La chiave di licenza è bloccata	MSG.KeyId	ID della chiave di licenza
	MSG.KeyName	Nome dell'utente della chiave di licenza
Chiave di licenza non può essere aggiornata automaticamente	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.	
	MSG.ExpirationDate	data di scadenza della licenza
	MSG.Expired	• 1 – la licenza è già scaduta • 0 – la licenza non è ancora scaduta

Messaggio	Variabili	Descrizione
	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
Scadenza della chiave di licenza	Viene inviato se è prossima la scadenza della chiave di licenza e l'aggiornamento automatico della licenza non è disponibile.	
	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
È stato superato il limite al numero di licenze	Viene inviato quando il numero di postazioni registrate si avvicina al limite di licenza, vale a dire: rimane non utilizzato meno del 5% del limite di licenza o meno di due postazioni.	
	MSG.Licensed	consentito da licenza
	MSG.Used	numero di postazioni nel database
	GEN.StationPrimaryGroupID	ID del gruppo primario
	GEN.StationPrimaryGroupName	nome del gruppo primario

Messaggio	Variabili	Descrizione
Si avvicina il limite di postazioni nel gruppo	Viene inviato ad ogni avvio del Server se il Server viene avviato con una chiave di licenza che autorizza meno postazioni di quante sono già connesse al Server.	
	MSG.Licensed	consentito da licenza
	MSG.Percent	percentuale delle licenze disponibili
	MSG.Used	numero di postazioni nel database
	GEN.StationPrimaryGroupID	ID del gruppo primario
	GEN.StationPrimaryGroupName	nome del gruppo primario

Nuovi arrivi

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

Messaggio	Variabili	Descrizione
La postazione è in attesa di conferma	non ci sono variabili	
La postazione è stata rifiutata automaticamente		
La postazione è stata rifiutata dall'amministratore	MSG.AdminAddress	indirizzo di rete del Pannello di controllo
	MSG.AdminName	nome dell'amministratore

Repository

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

Messaggio	Variabili	Descrizione
Stato aggiornato del prodotto nel repository	non ci sono variabili	
È stato avviato un aggiornamento del prodotto nel repository		

Messaggio	Variabili	Descrizione
Spazio insufficiente su disco	Viene inviato se non c'è abbastanza spazio libero sul disco con i dati dinamici. Le variabili generali per repository, riportate sopra, non sono disponibili.	
	`MSG.FreeInodes`	numero di descrittori di file inodes liberi (valido solo per alcuni sistemi 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
L'aggiornamento del prodotto nel repository è stato congelato	non ci sono variabili	
Impossibile aggiornare il prodotto nel repository	`MSG.Error`	messaggio di errore
	`MSG.ExtendedError`	descrizione dettagliata dell'errore
Il prodotto nel repository è stato aggiornato	`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

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. F1. Sintassi del file di configurazione .config.

Postazioni

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

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

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

Messaggio	Variabili	Descrizione
Disconnessione inaspettata	`MSG.Reason`	ragione per l'interruzione
	`MSG.Type`	tipo di client
Errore critico di aggiornamento della postazione	`MSG.Product`	prodotto che viene aggiornato
	`MSG.ServerTime`	ora locale della ricezione del messaggio da parte del Server
Postazione sconosciuta	`MSG.ID`	UUID della postazione sconosciuta
	`MSG.Rejected`	valori: • `rejected` – l'accesso è stato negato alla postazione • `newbie` – è stato fatto un tentativo di trasferimento della postazione nello stato "nuovo arrivo"
	`MSG.StationName`	nome della postazione
È stata rilevata una minaccia alla sicurezza	`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

Messaggio	Variabili	Descrizione
	MSG.ServerTime	ora della ricezione dell'evento, GMT
	MSG.Virus	nome della minaccia
	GEN.ServerRecvLinkID	UUID dell'ultimo Server 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)
	GEN.ServerRecvLinkName	nome dell'ultimo Server 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)
	GEN.ServerOriginatorID	UUID del Server a cui è connessa la postazione su cui è stata rilevata una minaccia
	GEN.ServerOriginatorName	nome del Server 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	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

Messaggio	Variabili	Descrizione
	GEN.ServerRecvLinkID	UUID dell'ultimo Server 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)
	GEN.ServerRecvLinkName	nome dell'ultimo Server 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)
	GEN.ServerOriginatorID	UUID del Server a cui è connessa la postazione su cui è stata rilevata una minaccia
	GEN.ServerOriginatorName	nome del Server a cui è connessa la postazione su cui è stata rilevata una minaccia
Report di Protezione preventiva	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

Messaggio	Variabili	Descrizione
	MSG.Target	percorso dell'oggetto protetto a cui 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 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)
	GEN.ServerRecvLinkName	nome dell'ultimo Server 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)
	GEN.ServerOriginatorID	UUID del Server a cui è connessa la postazione da cui è stato ricevuto un report di Protezione preventiva
	GEN.ServerOriginatorName	nome del Server 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	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

Messaggio	Variabili	Descrizione
	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 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 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)
	GEN.ServerRecvLinkName	nome dell'ultimo Server adiacente da cui è stato ricevuto un report di Protezione preventiva dalle postazioni connesse ad esso (valore vuoto se è

Messaggio	Variabili	Descrizione
		stato ricevuto un report dalle postazioni connesse a questo Server)
	GEN.ServerOriginatorID	UUID del Server a cui è connessa la postazione da cui è stato ricevuto un report di Protezione preventiva
	GEN.ServerOriginatorName	nome del Server a cui è connessa la postazione da cui è stato ricevuto un report di Protezione preventiva
Errore di autenticazione della postazione	MSG.ID	UUID della postazione
	MSG.Rejected	valori: • rejected – l'accesso è stato negato alla postazione • newbie – è stato fatto un tentativo di trasferimento della postazione nello stato "nuovo arrivo"
	MSG.StationName	nome della postazione
Errore di scansione	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 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)
	GEN.ServerRecvLinkName	nome dell'ultimo Server 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)

Messaggio	Variabili	Descrizione
	GEN.ServerOriginatorID	UUID del Server a cui è connessa la postazione su cui si è verificato un errore di scansione
	GEN.ServerOriginatorName	nome del Server a cui è connessa la postazione su cui si è verificato un errore di scansione
Errore di scansione al rilevamento di una minaccia in base agli hash di minacce conosciuti	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
	GEN.ServerRecvLinkID	UUID dell'ultimo Server 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)
	GEN.ServerRecvLinkName	nome dell'ultimo Server 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)
	GEN.ServerOriginatorID	UUID del Server a cui è connessa la postazione su cui si è verificato un errore di scansione
	GEN.ServerOriginatorName	nome del Server a cui è connessa la postazione su cui si è verificato un errore di scansione

Messaggio	Variabili	Descrizione
Impossibile creare un account di postazione	MSG.ID	UUID della postazione
	MSG.StationName	nome della postazione
La postazione non si connette al server da molto tempo	Le variabili generali per postazioni, riportate sopra, non sono disponibili.	
	MSG.DaysAgo	numero di giorni dal momento dell'ultima connessione al Server
	MSG.LastSeenFrom	indirizzo da cui la postazione si è connessa al Server l'ultima volta
	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 protezione della postazione
La postazione è stata confermata automaticamente	non ci sono variabili	
La postazione è stata confermata dall'amministratore	MSG.AdminAddress	indirizzo di rete del Pannello di controllo
	MSG.AdminName	nome dell'amministratore
La postazione è già registrata	Viene inviato se la postazione al momento è già registrata su questo o su un altro Server.	
	MSG.ID	UUID della postazione
	MSG.Server	ID del Server su cui la postazione è registrata
	MSG.StationName	nome della postazione
Statistiche di scansione	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

Messaggio	Variabili	Descrizione
	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	
	GEN.ServerRecvLinkID	UUID dell'ultimo Server 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)
	GEN.ServerRecvLinkName	nome dell'ultimo Server 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)
	GEN.ServerOriginatorID	UUID del Server a cui è connessa la postazione da cui sono state ricevute statistiche di scansione
	GEN.ServerOriginatorName	nome del Server a cui è connessa la postazione da cui sono state ricevute statistiche di scansione
È necessario riavviare la postazione	MSG.Reason	ragione per il riavvio la lista delle possibili ragioni è riportata nel modello predefinito

Messaggio	Variabili	Descrizione
È necessario riavviare la postazione per applicare gli aggiornamenti	MSG.Product	prodotto che viene aggiornato
	MSG.ServerTime	ora locale della ricezione del messaggio da parte del Server
Dispositivo è bloccato	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

Installazioni

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

Messaggio	Variabili	Descrizione
L'installazione non è stata eseguita sulla postazione	MSG.Error	messaggio di errore
L'installazione sulla postazione è stata completata con successo	non ci sono variabili	

Allegato E. Specifica di 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 si trova la definizione (come in Backus-Naur Form).

E1. Formato generale di 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 e l'indirizzo di Agent, 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.

Esempi:

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 `examle.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>*`]`

Esempi:

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>*

Esempi:

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

Indirizzi della famiglia SRV

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

E2. 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 del Server <drwcs-name>, che utilizza questa famiglia di protocolli ed endpoint

`[`*<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 del Server con il nome `drwcs` per connessione TCP che utilizza il gruppo multicast `231.0.0.1:2193` su tutte le interfacce.

Allegato F. 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 delle directory corrispondenti a concreti prodotti e impostano la lista dei file e le impostazioni degli aggiornamenti del prodotto nella cui directory si trovano.

Dopo una modifica dei file di configurazione, è necessario riavviare il Server.

Quando vengono configurate le relazioni tra i server (v. **Manuale dell'amministratore**, p. Caratteristiche della rete con diversi Server) 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 malfunzionamento nell'operazione del sistema di aggiornamento:

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

F1. 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

esuite.msk3.drweb.com
```

```
esuite.msk4.drweb.com

esuite.msk.drweb.com

esuite.us.drweb.com

esuite.jp.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 con SO della famiglia UNIX.

Per esempio:

```
https
```

.auth

Il file `.auth` contiene le impostazioni di autenticazione dell'utente sul server di aggiornamento.

Le impostazioni di autenticazione vengono configurate nel seguente formato:

```
<nome utente>

<password>
```

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

Per esempio:

```
admin

root
```

.delivery

Il file `.delivery` contiene le impostazioni per la trasmissione di aggiornamenti dai server SAM.

Parametro	Valori possibili	Descrizione
`cdn`	`on` | `off`	Utilizzo di Content Delivery Network per il caricamento del repository: • `on` – per utilizzare CDN, • `off` – per non utilizzare CDN.
`cert`	`drweb` | `valid` | `any` | `custom`	I certificati SSL ammissibili dei server di aggiornamento, che verranno accettati automaticamente: • `drweb` – accetta soltanto il certificato SSL della società Doctor Web, • `valid` – accetta soltanto certificati SSL validi, • `any` – accetta qualsiasi certificato, • `custom` – accetta il certificato indicato dall'utente.
`cert-path`		Il percorso del certificato dell'utente, se è selezionata la modalità `custom` per il parametro `cert`.
`ssh-mode`	`pwd` | `pubkey`	La modalità di autenticazione in caso di utilizzo dei protocolli `scp` e `sftp` (basati su *ssh2*): • `pwd` – autenticazione sulla base di nome utente e password, • `pubkey` – autenticazione sulla base di chiavi di cifratura.
`ssh-pubkey`		Percorso della chiave pubblica ssh del server di aggiornamento.
`ssh-prikey`		Percorso della chiave privata ssh del server di aggiornamento.

F2. 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
```

.sync-off

Il file disattiva l'aggiornamento del prodotto. I contenuti non importano.

I file di eccezioni per l'aggiornamento del repository del Server 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, nel formato di espressioni regolari, una 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 dal Server

.state-only

Il file `.state-only` contiene le espressioni regolari che definiscono la lista dei file che verranno sincronizzati durante l'aggiornamento degli Agent dal Server. 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 salvo 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 dal Server.

Per esempio:

- non c'è bisogno di 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 uguale a quella di `.sync-only` e `.sync-ignore`.

Impostazioni di invio di avvisi

I file del gruppo `notify` consentono di configurare il sistema di avviso per l'aggiornamento riuscito dei relativi prodotti di repository.

Queste impostazioni appartengono soltanto all'avviso **Il prodotto è aggiornato**. Le eccezioni non valgono per gli altri tipi di avvisi.

Le impostazioni del sistema di avviso sono descritte nel **Manuale dell'amministratore**, p. Configurazione degli avvisi.

.notify-only

Il file `.notify-only` contiene una lista dei file di repository, in caso di una modifica dei quali viene inviato un avviso.

.notify-ignore

Il file `.notify-ignore` contiene una lista dei file di repository, in caso di una modifica dei quali non vengono inviati avvisi.

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, gli avvisi vengono inviati.

Se i file `.notify-only` e `.notify-ignore` sono assenti, gli avvisi verranno sempre inviati (se abilitati sulla pagina **Configurazione degli avvisi** nel Pannello di controllo).

Per esempio:

Se nel file `.notify-ignore` è impostata l'eccezione `^.vdb.lzma$`, in tale caso se sono stati aggiornati soltanto i file dei database dei virus, nessun avviso verrà inviato. Se, oltre ai database, è stato aggiornato il nucleo `drweb32.dll`, un avviso verrà inviato.

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]; UseFilter [YES|NO]
```

Parametro	Valori possibili	Descrizione
`Delay`	`ON|OFF`	• `ON` – è attivato il congelamento degli aggiornamenti del prodotto. • `OFF` – è disattivato il congelamento degli aggiornamenti del prodotto.
`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
```

Allegato G. 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 da scaricare dal Server.
drwcsd-proxy.conf	File di configurazione del Server proxy Dr.Web.
drwreploader.conf	File di configurazione del Loader di repository.

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

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

G1. File di configurazione del 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. Quando il Server viene avviato, attraverso un parametro della riga di comando è possibile impostare un percorso e nome personalizzato del file di configurazione (per maggiori informazioni v. Allegato H4. Server Dr.Web).

Se è necessario modificare manualmente il file di configurazione di Server Dr.Web, eseguire le seguenti azioni:

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

Il formato del file di configurazione del Server Dr.Web

Il file di configurazione del Server 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 di un cluster dei Server Dr.Web utilizzato in una ricerca dagli Agent, installer di Agent 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.

- <id value=''/>

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

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

  Posizione geografica del Server.

  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 che arrivano dagli Agent. Il valore minimo è 5. Di default, è 5. Questo parametro influisce sulle prestazioni del Server. Non è consigliabile modificare il valore del parametro senza una raccomandazione del servizio di supporto.

- <newbie approve-to-group='' default-rate='' 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.
`default-rate`	-	In caso di AV-Desk. Il gruppo che verrà impostato di default alle nuove postazioni come il gruppo tariffario in modalità **Consenti l'accesso automaticamente** (`mode='open'`).	Valore vuoto che significa imposta il gruppo **Dr.Web Premium** come il gruppo tariffario.
`mode`	• open – consenti l'accesso automaticamente, • closed – sempre nega l'accesso, • approval – conferma l'accesso manualmente.	Criteri di connessione di nuove postazioni.	-

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

- `<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 dei nuovi arrivi,
  - `no` (predefinito) – la modalità di funzionamento normale.

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

  Il numero massimo di postazioni nella coda per l'autenticazione sul Server. Non è consigliabile modificare il valore del parametro senza una raccomandazione del servizio di supporto.

- `<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=''/>`

  Sostituisci i nomi NetBIOS dei computer con il nome DNS. I valori ammissibili dell'attributo `enabled`:

  - `yes` – mostra i nomi DNS.
  - `no` (predefinito) – mostra i nomi NetBIOS.

- `<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 memoria 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>`

  Le impostazioni della memorizzazione nella cache.

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

  - `<interval value=''/>`

    Periodicità in secondi di svuotamento completo della cache.

  - `<quarantine ttl=''/>`

    Periodicità in secondi di eliminazione di file nella quarantena del Server. 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 di file nella cache del repository del Server.

- `<file ttl=''/>`

  Periodicità in secondi di svuotamento della cache di 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` – sostituisce la descrizione sul Server con la descrizione dalla postazione.
  - `no` (predefinito) – ignora la descrizione sulla postazione.

- `<time-discrepancy value=''/>`

  La 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 segnalato 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 effettuato.

- `<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 d'occhio i risultati di esecuzione di task su postazioni e di registrare le informazioni nel database del Server. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

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

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

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

  Consenti di tenere d'occhio i cambi nello stato (parti, modifiche) dei database dei virus e di registrare le informazioni nel database del Server. 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 d'occhio le versioni dei moduli di postazioni e di registrare le informazioni nel database del Server. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

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

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

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

  Consenti di tenere d'occhio le sessioni degli utenti su postazioni e di registrare le informazioni nel database del Server. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

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

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

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

  Consenti di tenere d'occhio le informazioni su avvio e arresto dei componenti antivirus su postazioni e di registrare le informazioni nel database del Server. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

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

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

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

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

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

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

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

  Consenti di tenere d'occhio le informazioni su installazioni di Agent sulla postazione e di registrare le informazioni nel database del Server. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

- `<quarantine enabled=''/>`

Consenti di tenere d'occhio le informazioni circa lo stato della Quarantena su postazioni e di registrare le informazioni nel database del Server. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

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

  La larghezza di banda massima in KB/s per la trasmissione di aggiornamenti tra il Server e gli Agent.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`queue-size`	• un numero intero positivo, • `unlimited`.	Il numero massimo ammissibile di sessioni simultanee di distribuzione di aggiornamenti dal Server. Quando è stato raggiunto il limite indicato, le richieste dagli Agent 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=''/>`

  La larghezza di banda massima in KB/s per la trasmissione di dati dal Server nel corso di un'installazione degli Agent su postazioni.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`queue-size`	• un numero intero positivo, • `unlimited`.	Il numero massimo ammissibile di sessioni simultanee di installazione di Agent dal Server. Quando è stato raggiunto il limite indicato, le richieste dagli Agent 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 dati nel corso di un'installazione di Agent.	`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 d'occhio le operazioni dell'amministratore nel Pannello di controllo della sicurezza Dr.Web e di registrare le informazioni nel database del Server. I valori ammissibili dell'attributo `enabled`: `yes` o `no`.

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

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

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

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

- `<proxy auth-list='any' enabled='no' 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 attraverso il 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.haxx.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.	–
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 si scambieranno le 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.

- <**mcast-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 `<mcast-updates />` 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 le postazioni riceveranno gli aggiornamenti per gruppi.
`port`	Numero di porta dell'interfaccia di rete del Server Dr.Web a cui viene legato il protocollo di trasporto multicast per la trasmissione degli aggiornamenti. Per gli aggiornamenti per gruppi, è necessario impostare qualsiasi porta libera, in particolare, una che è diversa dalla porta assegnata nelle impostazioni al funzionamento del protocollo di trasporto del Server stesso.
`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.

L'elemento `<mcast-updates />` contiene un elemento figlio `<transfer datagram-size="" assembly-timeout="" updates-interval="" chunks-interval="" resend-interval="" silence-interval="" accumulate-interval="" />`.

Descrizione degli attributi:

Attributo	Descrizione	Di default
`datagram-size`	**Dimensione del datagramma UDP –** dimensione in byte dei datagrammi UDP utilizzati dal protocollo multicast. L'intervallo ammissibile è 512 – 8192. Per evitare frammentazione, si consiglia di impostare un valore inferiore all'MTU (Maximum Transmission Unit) della rete in uso.	4096
`assembly-timeout`	**Tempo di trasmissione del file (ms)** – nel periodo definito viene trasmesso un file di aggiornamento, dopo di che il Server inizia a trasmettere il file successivo. Tutti i file che non sono stati trasmessi in fase dell'aggiornamento tramite il protocollo multicast verranno trasmessi durante l'aggiornamento standard tramite il protocollo TCP.	180000
`updates-interval`	**Durata degli aggiornamenti per gruppi (ms)** – durata del processo di aggiornamento attraverso il protocollo multicast. Tutti i file che non sono stati trasmessi in fase dell'aggiornamento tramite il protocollo multicast verranno trasmessi durante l'aggiornamento standard tramite il protocollo TCP.	600000
`chunks-interval`	**Intervallo di trasmissione pacchetti (ms)** – intervallo di trasmissione dei pacchetti al gruppo multicast.	20

Attributo	Descrizione	Di default
	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.	
`resend-interval`	**Intervallo tra le richieste di ritrasmissione (ms)** – con questo intervallo gli Agent inviano le richieste di ritrasmissione dei pacchetti persi. Il Server Dr.Web accumula queste query, dopodiché trasmette i blocchi persi.	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, il Server Dr.Web ritiene che tutti gli Agent abbiano ottenuto con successo i file di aggiornamento e inizia a trasmettere il file successivo.	10000
`accumulate-interval`	**Intervallo per accumulare richieste di ritrasmissione (ms)** – durante questo intervallo il Server accumula le richieste degli Agent per la ritrasmissione dei pacchetti persi. Gli Agent chiedono l'invio ripetuto dei pacchetti persi. Il Server accumula queste richieste entro il tempo specificato, dopodiché trasmette i blocchi persi.	2000

- `<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. Non è consigliabile modificare il valore del parametro senza una raccomandazione del servizio di supporto.	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 soltanto un elemento figlio che definisce un concreto database.

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="database.sqlite" cache="SHARED" cachesize="2048" mmapsize="10485760" readuncommitted="off" precompiledcache="1024" synchronous="FULL" openmutex="FULL" checkintegrity="yes" autorepair="no" wal="yes" wal-max-pages="1000" wal-max-seconds="30" debug="no" />`

  Definisce il database incorporato SQLite3.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`dbfile`		Nome del file del database.	
`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
`checkintegrity`	`yes` | `no`	Verifica dell'integrità dell'immagine del database ad avvio del Server Dr.Web.	
`autorepair`	`yes` | `no`	Ripristino automatico dell'integrità dell'immagine del database ad avvio del Server Dr.Web.	`yes`
`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 UNIX – 10485760 • in caso di SO Windows – 0
`precompiledcache`	Un numero intero positivo.	Dimensione in chilobyte della cache degli operatori sql precompilati.	1024
`synchronous`	• `TRUE` o `FULL` – sincrona • `FALSE` o `NORMAL` – normale • `OFF` – asincrona	Modalità di registrazione dei dati.	`FULL`
`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		L'indirizzo del server PostgreSQL o il percorso al socket Unix.	
port		Il numero di porta del server PostgreSQL o l'estensione del nome di file del socket Unix.	
options		Parametri da riga di comando per l'invio sul server del database. Per maggiori informazioni v. capitolo 18 http://www.postgresql.org/docs/9.1/static/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 • serializable	Livello di isolamento delle transazioni.	read committed

- `<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`		Riga contenente le coppie chiave-valore Oracle SQL Connect URL o Oracle Net.	
`user`		Nome dell'utente del database.	
`password`		Password dell'utente del database.	
`client`		Il percorso del client per l'accesso al database Oracle (Oracle Instant Client). Server Dr.Web viene fornito con Oracle Instant Client versione 11. Se vengono utilizzati server Oracle delle versioni più recenti o si verificano errori nel driver del database Oracle fornito, si può scaricare il driver appropriato dal sito Oracle e specificarne il percorso 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 (l'impostazione predefinita 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="" 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`
`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

Attributo	Valori ammissibili	Descrizione	Di default
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" 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 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.	""
ssl	yes | qualsiasi altro set di caratteri	Utilizza solamente le connessioni SSL.	no
precompiledcache	Un numero intero positivo.	Dimensione in chilobyte della cache degli operatori sql precompilati.	1024

- `<acl>`

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

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.
- `<agent />` – lista delle limitazioni agli indirizzi IP da cui gli Agent Dr.Web possono connettersi a questo Server.
- `<links />` – lista delle limitazioni agli indirizzi IP da cui i Server Dr.Web adiacenti possono connettersi a questo Server.
- `<discovery />` – lista delle limitazioni agli indirizzi IP da cui le richieste broadcast vengono accettate dal *servizio di rilevamento del Server*.

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. Questo parametro viene utilizzato dal servizio di supporto tecnico e dagli sviluppatori. Non è consigliabile modificarne il valore senza necessità.	`no`

Attributo	Valori ammissibili	Descrizione	Di default
stack		Registra nel log le informazioni dallo stack di chiamate del funzionamento degli script del Server. 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. 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 rispetto ai percorsi impostati nell'attributo root dell'elemento **<cpath />**.
  - **<jobs />** – percorsi per i task dal calendario di Server.

    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.

    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 per la connessione 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 scoperta di	no, viene impostato soltanto insieme	yes, no	no

Attributo	Descrizione	Obbligatorio	Valori ammissibili	Di default
	Server.	all'attributo `ip`.		
• `ip` • `unix`	Definisce una famiglia dei protocolli utilizzati e imposta l'indirizzo di interfaccia.	sì	–	• 0.0.0.0 • -
`name`	Imposta il nome del Server per il servizio di scoperta di Server.	no	–	`drwcs`
`multicast`	Determina se il Server 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.	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 con gli Agent Dr.Web. • `MSNAPSHV` – il protocollo di comunicazione del Server con il componente di controllo dell'operatività del sistema Microsoft NAP Validator. • `INSTALL` – il protocollo di comunicazione del Server con gli installer di Agent Dr.Web. • `CLUSTER` – il protocollo di comunicazione tra i Server in un sistema cluster. • `SERVER` – il protocollo di comunicazione del Server Dr.Web con gli altri Server Dr.Web.	Nome del protocollo.	-

- **<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 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.	Nome dell'estensione.	-

- **`<license-exchange>`**

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

  L'elemento `<license-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. L'impostazione viene utilizzata se questo Server rilascia licenze ai Server adiacenti.	1440
`prolong-preact`	**Periodo per il rinnovo delle licenze ricevute** – il periodo fino alla scadenza di una licenza, a partire da cui questo Server richiede il rinnovo della licenza ricevuta da un Server adiacente. L'impostazione viene utilizzata se questo Server riceve licenze dai Server adiacenti.	60
`check-interval`	**Periodo di sincronizzazione delle licenze** – la periodicità della sincronizzazione di informazioni sulle licenze rilasciate tra i Server.	1440

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

  Configurazione dei parametri di invio delle email dal Pannello di controllo, per esempio, come gli avvisi dell'amministratore o per inviare pacchetti d'installazione di 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
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

Attributo	Valori ammissibili	Descrizione	Di default
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 certificato SSL, • no – non controllare certificato SSL.	Controlla la correttezza del certificato SSL del mail server.	no
ca_certs	-	Percorso del certificato SSL di radice del Server Dr.Web.	-

- `<track-epidemic enabled='' period='' threshold=''/>`

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

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
enabled	• yes – attiva il monitoraggio di epidemie e invia un singolo avviso di minacce, • no – disattiva il monitoraggio di epidemie e invia avvisi di minacce in modalità normale.	Modalità di avviso dell'amministratore di epidemie di virus.	no
period	Un numero intero positivo.	Periodo in secondi in cui deve arrivare il numero impostato di avvisi di infezione affinché il Server Dr.Web mandi all'amministratore un singolo avviso di epidemia racchiudente tutti i casi di infezione.	300

Attributo	Valori ammissibili	Descrizione	Di default
`threshold`		Numero di avvisi di infezione che deve arrivare nel periodo impostato affinché il Server Dr.Web mandi all'amministratore un singolo avviso di epidemia racchiudente tutti i casi di infezione.	100

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

  La lingua che viene utilizzata di default dai componenti e sistemi del Server Dr.Web, se non è stato possibile ottenere le impostazioni di lingua dal database del Server. In particolare, si usa per il Pannello di controllo della sicurezza Dr.Web e il sistema di avviso dell'amministratore, se il database è stato danneggiato e non è possibile ottenere le impostazioni di lingua.

G2. File di configurazione del 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.

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> `[:` *<porta>* `]`

  Se l'indirizzo del Server non è impostato, viene utilizzato il nome di computer restituito dal sistema operativo o l'indirizzo di rete del Server: il nome DNS, se disponibile, altrimenti l'indirizzo IP.

  Se il numero di porta non è impostato, viene utilizzata la porta impostata nella richiesta (per esempio in caso di connessione al Server dal Pannello di controllo o attraverso **Web API**). In particolare, in caso di una richiesta dal Pannello di controllo è la porta specificata nella barra degli indirizzi per la connessione del Pannello di controllo al Server.

- `<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. 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 interrompe la connessione se nel periodo indicato non arrivano query 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. 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. Non è consigliabile modificarne il valore senza necessità.	2048 byte

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

  Lunghezza massima ammissibile in KB di una richiesta HTTP.

- `<reverse-resolve enabled="no"/>`

  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="no"/>`

  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="no" stack="no"/>`

  Gestione del profiling. Vengono misurate le prestazioni – cioè il tempo di esecuzione di funzioni e 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.

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

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

  Impostazioni del certificato SSL.

  Descrizione degli attributi:

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

- `<listen>`

  Configurazione dei parametri per essere in ascolto per le connessioni.

  L'elemento `<listen />` contiene i seguenti elementi figli:

  - `<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 figli: <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 figli: <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`
`deny`	Gli indirizzi da cui sarà vietato l'accesso tramite il protocollo HTTP per le connessioni non protette.	-

G3. File di configurazione download.conf

Scopo del file download.conf:

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

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

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

dove:

- <*Server_Address*> – indirizzo IP o nome DNS del Server.

  Quando viene generato un pacchetto di installazione di Agent, inizialmente l'indirizzo di Server viene preso dal file `download.conf`. Se nel file `download.conf` non è impostato l'indirizzo di Server, viene utilizzato il valore del parametro `ServerName` dal file `webmin.conf`. Altrimenti si usa il nome di computer restituito dal sistema operativo.
- <*port_number*> – la porta per la connessione dell'installer di Agent al Server.

  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.

G4. File di configurazione del server proxy

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 della ricezione di 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 Server. Consente ai client di rilevare il Server proxy come un Server Dr.Web durante la ricerca del Server 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	Disponibilità 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 di indirizzo di rete, in particolare, nel formato `tcp/<DNS_name>:<port>`.	Indirizzo di Server Dr.Web su cui verrà reindirizzata la connessione.	sì
`master`	• `yes` – Il Server sarà un server di gestione incondizionato. • `no` – in nessun caso il Server sarà un server di gestione. • `possible` – il Server 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 in remoto delle impostazioni del Server proxy attraverso il Pannello di controllo del Server Dr.Web indicato nell'attributo `to`. È possibile nominare qualsiasi numero di server come server di gestione (il valore `master="yes"`), la connessione viene effettuata a tutti i Server di gestione consecutivamente nell'ordine definito nelle impostazioni del Server proxy fino alla prima ricezione di una configurazione valida (non vuota). È inoltre possibile non nominare un server di gestione (il valore `master="no"`) nessuno dei Server. In questo caso, l'impostazione dei parametri del Server proxy (compresa la nomina dei Server di gestione) è possibile solo localmente attraverso il file di configurazione del Server proxy.	no

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

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

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

L'elemento `<compression />` come figlio dell'elemento `<forward />` determina i parametri di compressione nei canali Server – Server proxy. Gli attributi sono simili a quelli descritti sopra.

- `<encryption mode="">`

L'elemento `<encryption />` come figlio dell'elemento `<listen />` determina i parametri di crittografia nei canali Server – Server proxy. Gli attributi sono simili a quelli descritti sopra.

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

L'elemento `<update-bandwidth />` consente di impostare una limitazione di velocità per la trasmissione di aggiornamenti dal Server ai client e il numero di client che scaricano aggiornamenti contemporaneamente.

Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
`value`	• KB/s • `unlimited`	Valore massimo della velocità complessiva per la trasmissione di aggiornamenti.	`unlimited`
`queue-size`	• numero intero positivo • `unlimited`	Il numero massimo ammissibile di sessioni simultanee di distribuzione di aggiornamenti dal Server. Quando è stato raggiunto il limite indicato, le richieste dagli Agent 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 di dati per un periodo di tempo specificato.

  Descrizione degli attributi:

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

Il valore del parametro `time-map` viene definito in modo simile al calendario delle limitazioni di traffico nelle impostazioni di Server. Al momento non è possibile generare `time-map` manualmente.

- `<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 e il numero di client che scaricano i dati contemporaneamente.

Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
value	• KB/s • unlimited	Valore massimo della velocità complessiva per la trasmissione di dati nel corso di un'installazione di Agent.	unlimited
queue-size	• numero intero positivo • unlimited	Il numero massimo ammissibile di sessioni simultanee di installazione di Agent dal Server. Quando è stato raggiunto il limite indicato, le richieste dagli Agent 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 di dati per un periodo di tempo specificato.

  Descrizione degli attributi:

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

Il valore del parametro `time-map` viene definito in modo simile al calendario delle limitazioni di traffico nelle impostazioni di Server. Al momento non è possibile generare `time-map` manualmente.

- `<cache enabled="">`

  Impostazioni della cache del repository del Server proxy.

  Descrizione degli attributi:

Attributo	Valori ammissibili	Descrizione	Di default
enabled	yes | no	Definisce 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

Elemento	Valori ammissibili	Descrizione	Di default
<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 del parametro schedule viene definito in modo simile al calendario della sincronizzazione nelle impostazioni del Pannello di controllo. Al momento non è possibile generare schedule manualmente.

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

  - 10-drwbases – database dei virus,
  - 10-drwgatedb – database di SpIDer Gate,
  - 10-drwspamdb – database di Antispam,
  - 10-drwupgrade – Modulo di aggiornamento Dr.Web,
  - 20-drwagent – Agent Dr.Web per Windows,
  - 20-drwandroid11 – Agent Dr.Web per Android,
  - 20-drwunix – Agent Dr.Web per UNIX,
  - 40-drwproxy – Server proxy Dr.Web.

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

  Impostazioni della memorizzazione nella cache degli eventi ricevuti dagli Agent.

  Descrizione degli attributi:

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

Il valore del parametro `schedule` viene definito in modo simile al calendario dell'invio degli eventi nelle impostazioni del Pannello di controllo. Al momento non è possibile generare `schedule` manualmente.

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

  Configurazione dell'aggiornamento automatico del Server proxy.

  All'aggiornamento automatico, se la sincronizzazione è attivata, gli aggiornamenti del Server proxy verranno scaricati dal Server secondo il calendario della sincronizzazione (vedi 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.	–

Al momento non è possibile generare `schedule` manualmente. Di default, l'aggiornamento automatico è consentito senza limitazioni al 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: `%All Users\Application Data%\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 memoria 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.

G5. File di configurazione del 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.

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. I file scaricati possono essere importati direttamente attraverso il Pannello di controllo come un aggiornamento del repository di Server. • `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 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 tramite il Pannello di controllo, dalla sezione **Amministrazione** → **Contenuti del repository**.	`yes | no`
`key`	File della chiave di licenza Dr.Web. E 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	La modalità di rotazione del log nel formato <*N*><*f*>,<*M*><*u*>. È simile all'impostazione di rotazione del log di Server. 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.
`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 soltanto 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

Attributo	Descrizione	Valori ammissibili
		`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, • `10-drwgatedb` – database di SpIDer Gate, • `10-drwspamdb` – database di Antispam, • `10-drwupgrade` – Modulo di aggiornamento Dr.Web, • `20-drwagent` – Agent Dr.Web per Windows, • `20-drwandroid11` – Agent Dr.Web per Android, • `20-drwcs` – Server Dr.Web, • `20-drwunix` – Agent Dr.Web per UNIX, • `40-drwproxy` – Server proxy 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.

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

Allegato H. Parametri da riga di comando per i programmi che fanno parte di Dr.Web Enterprise Security Suite

H1. Introduzione

I parametri della riga di comando hanno una priorità più alta rispetto alle impostazioni predefinite o alle altre impostazioni permanenti (definite nel file di configurazione del Server, 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 nella sezione H1 non riguardano l'installer di rete di Agent.

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.

H2. 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.

Le opzioni di avvio dell'installer di rete di Agent 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. 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 a seconda delle impostazioni sul lato Server.

  Se l'opzione non è impostata, di default si usa il valore `possible`.
- `/encryption` <*modalità*> – modalità di cifratura del traffico dati con il Server. 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 a seconda delle impostazioni sul lato Server.

  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.

  L'opzione viene impostata insieme all'opzione `/pwd` per l'autenticazione automatica sul Server. Se le impostazioni di autenticazione non sono definite, la decisione circa l'autenticazione viene presa sul lato Server.

- `/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 per aspettare una risposta dalla postazione durante un'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:
  - `remove` – rimuovi il prodotto installato.

  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.

  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 per l'accesso al Server.

  L'opzione viene impostata insieme all'opzione `/id` per l'autenticazione automatica sul Server. Se le impostazioni di autenticazione non sono definite, la decisione circa l'autenticazione viene presa sul lato Server.

- `/regagent` <*modalità*> – definisce se l'Agent verrà registrato nella lista delle applicazioni installate. Il parametro <*modalità*> può assumere i seguenti valori:
  - `yes` – registra l'Agent nella lista delle applicazioni installate.
  - `yes` – non registrare l'Agent nella lista delle applicazioni installate.

  Se l'opzione non è impostata, di default si usa il valore `no`.

- `/retry` <*numero*> – il numero di tentativi della ricerca del Server tramite l'invio di richieste multicast. Se non c'è una risposta dal Server dopo il numero di tentativi impostato, si ritiene che il Server non è stato trovato.

  Se l'opzione non è impostata, di default vengono eseguiti 3 tentativi di ricerca di Server.

- `/server [`<*protocollo*>`/]`<*indirizzo_del_server*>`[:`<*porta*>`]` – indirizzo del Server da cui verrà effettuata l'installazione di Agent e a cui Agent si connetterà dopo l'installazione.

  Se l'opzione non è impostata, di default il Server viene cercato tramite l'invio di richieste multicast.

- `/silent` <*modalità*> – definisce se l'installer verrà eseguito in modalità silenziosa. Il parametro <*modalità*> può assumere i seguenti valori:
  - `yes` – avvia l'installer in modalità silenziosa.
  - `no` – avvia l'installer in modalità grafica.

  Se l'opzione non è impostata, di default Agent viene installato in modalità grafica dell'installer (v. **Guida all'installazione**, p. Installazione di Agent Dr.Web attraverso installer).

- `/timeout` <*tempo*> – limite di tempo per aspettare ciascuna risposta nel corso della ricerca del Server. 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 del timeout.

  Se l'opzione non è impostata, di default si usa il valore di 3 secondi.

H3. 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.

Tutte le opzioni vengono eseguite a prescindere dai permessi consentiti alla postazione sul Server. Cioè anche se i permessi per la modifica delle impostazioni di Agent sono vietati sul Server, è possibile modificare queste impostazioni tramite le opzioni della riga di comando.

Opzioni ammissibili:

- Mostra la guida:
  - `-?`
  - `--help`
- Modifica l'indirizzo del Server a cui si connette l'Agent:
  - `-e <Server>`
  - `--esserver=<Server>`

  Per impostare diversi Server alla volta, è necessario ripetere l'opzione tra spazio per ciascuno indirizzo di Server, 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 (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 usato.

  Tutte le chiavi pubbliche utilizzate in precedenza (le chiavi che sono state trasferite dal Server e si conservano nel registro) rimangono e continuano a essere utilizzate.
- Aggiungi certificato Server:
  - `-c <certificato>`
  - `--addcert=<certificato>`

  Il file del certificato Server indicato come argomento viene copiato nella directory di Agent (di default è la directory `%ProgramFiles%\DrWeb`), viene rinominata 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 usato.

  Tutti i certificati utilizzati in precedenza (i certificati che sono stati trasferiti dal Server e si conservano nel registro) rimangono e continuano a essere utilizzati.
- Modifica il livello di dettaglio del log di Agent:
  - `-l <livello>`
  - `--loglevel=<livello>`

  I valori ammissibili del livello di dettaglio del log: `err`, `wrn`, `inf`, `dbg`.

H4. Server Dr.Web

Ci sono diverse varianti dei comandi di avvio di Server, per comodità vengono descritte separatamente.

I comandi riportati in H4.1. Gestione del Server Dr.Web – H4.5. Backup dei dati critici del Server Dr.Web sono multipiattaforma: è possibile utilizzarli 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, consultare il file di log di Server per cercare le possibili cause (v. **Manuale dell'amministratore**, p. Log di funzionamento di Server Dr.Web).

H4.1. Gestione del Server Dr.Web

`drwcsd [<opzioni>]` — configura le impostazioni di funzionamento del Server (le opzioni vengono descritte in maggior dettaglio sotto).

H4.2. Comandi di base

- `drwcsd reconfigure` – rileggi il file di configurazione e riavviati (si esegue più velocemente - senza avvio di un nuovo processo).
- `drwcsd restart` – esegui il riavvio completo del servizio Server (viene eseguito come coppia `stop` e quindi `start`).
- `drwcsd start` – avvia il Server.
- `drwcsd stop` – arresta normalmente il Server.
- `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 verifyakey` <*nome_completo_del_file_della_chiave*> – controllo della correttezza del file della chiave di licenza (`agent.key`).
- `drwcsd verifyekey` <*nome_completo_del_file_della_chiave*> – controllo della correttezza del file della chiave di licenza di Server (`enterprise.key`). Notare che la chiave di licenza Server non si usa più a partire dalla versione 10.
- `drwcsd verifyconfig` <*nome_completo_del_file_di_configurazione*> – controllo della sintassi del file di configurazione del Server (`drwcsd.conf`).

H4.3. Comandi di gestione del database

Inizializzazione del database

Ad inizializzazione il database deve essere assente o vuota.

`drwcsd [`<*opzioni*>`] initdb [`<*chiave_di_licenza*>`|- [`<*script_sql*>`|- [`<*file_ini*>`|- [`<*password*>` [`<*script_lua*>`|-]]]]]` – 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 adiacente.
- <*script_sql*> – percorso dello script sql per l'inizializzazione della struttura fisica del database.
- <*file_ini*> – file precedentemente creato in formato `drweb32.ini` che imposterà la configurazione iniziale dei componenti del software Dr.Web (per il gruppo **Everyone**).
- <*password*> – password iniziale dell'amministratore del Server (il nome utente è **admin**). Di default, è **root**.
- <*script_lua*> – percorso dello script lua per l'inizializzazione del database (riempimento del database con valori predefiniti).

Il valore speciale "-" (meno) significa non utilizzare questo parametro.

Il segno meno può essere omesso se sono assenti i parametri che lo seguono.

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 initdbex` <*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 `initdb`.

Formato del file:

```
<nome_di_file_completo_della_chiave_di_licenza>

<nome_di_file_completo_dello_script_sql>

<nome_completo_del_file_ini>

<password_amministratore>
```

Si il response-file viene utilizzato in SO Windows, è possibile utilizzare qualsiasi carattere nella password dell'amministratore.

Le stringhe di coda che seguono il parametro necessario in un caso particolare non sono obbligatorie. Se una stringa è un "-" (segno "meno"), viene utilizzato il valore predefinito (come in `initdb`).

Aggiornamento del database

`drwcsd [`<*opzioni*>`] updatedb` <*script*> – per eseguire una manipolazione con il database (per esempio, aggiornamento durante cambio di versione) eseguendo uno script SQL o LUA dal file specificato.

Aggiornamento della versione del database

`drwcsd upgradedb [`<*directory*>`]` – per avviare il Server per aggiornare la struttura del database durante il passaggio a una nuova versione dalla directory indicata (vedi directory `update-db`) o tramite gli script interni.

Esportazione del database

a) `drwcsd exportdb` <*file*> – esportazione del database nel file indicato.

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=all
exportdb "C:\Program Files\DrWeb Server\esbase.es"
```

In SO della famiglia **UNIX** l'azione viene eseguita sotto l'account di 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 xmlexportdb` <*file-xml*> – esportazione del database nel file xml indicato.

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=ALL -rotate=10,10m -
log=export.log xmlexportdb 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=ALL -rotate=10,10m -
log=export.log xmlexportdb database.gz
```

Esempio per il SO della famiglia UNIX:

- Per esportare il database in un file xml senza compressione:

```
/etc/init.d/drwcsd xmlexportdb /es/database.db
```

- Per esportare il database in un file xml compresso in archivio:

```
/etc/init.d/drwcsd xmlexportdb /es/database.gz
```

Importazione del database

a) `drwcsd importdb` <*file*> – importazione del database dal file indicato (il vecchio contenuto del database viene cancellato).

b) `drwcsd upimportdb` <*file*> `[`<*directory*>`]` – importazione e aggiornamento di un database ottenuto attraverso l'esportazione da un Server delle versioni precedenti (il vecchio contenuto del database viene cancellato). Inoltre, è possibile specificare il percorso di una directory con gli script per l'aggiornamento della struttura del database durante il passaggio a una nuova versione (simile al comando `upgradedb`).

c) `drwcsd xmlimportdb` <*file xml*> – importazione del database dal file xml indicato.

d) `drwcsd xmlupimportdb` <*file_xml*> `[`<*directory*>`]` – importazione e aggiornamento di un database ottenuto attraverso l'esportazione xml da un Server delle versioni precedenti. Inoltre, è possibile specificare il percorso di una directory con gli script per l'aggiornamento della struttura del database durante il passaggio a una nuova versione (simile al comando `upgradedb`).

e) `drwcsd xmlimportdbnh` <*file xml*> – importazione del database dal file xml indicato senza la considerazione dell'hash. Può essere utilizzato, per esempio, se il file xml del database veniva modificato manualmente, e l'hash del file scritto automaticamente durante l'esportazione non è più valido.

Prima di utilizzare i comandi `upimportdb` e `xmlupimportdb`, è necessario eseguire il backup del database.

Qualsiasi problema nel corso dell'esecuzione di questi comandi può comportare la rimozione di tutte le informazioni dal database.

I comandi `upimportdb` e `xmlupimportdb` possono essere utilizzati per l'importazione con l'aggiornamento della versione del database solo all'interno di un unico DBMS.

Dump dell'esportazione del database

`drwcsd [`<*opzioni*>`] dumpimportdb` <*file_di_database*> `[`<*file_SQL*>`]` `[`<*filtro_delle_tabelle*>`]]` – scrivi nel file di log di Server o nel file SQL le informazioni dettagliate sul database incorporato o esterno.

L'importazione e l'esportazione del database nel corso dell'esecuzione del comando `dumpimportdb` non viene eseguita.

- <*file_di_database*> – file di esportazione del database, di cui le informazioni verranno scritte nel log di Server o nel <*file_SQL*>. Il file di esportazione può essere ottenuto tramite il comando `exportdb`; inoltre, è possibile utilizzare un file ottenuto da un backup del database. Il file XML ottenuto tramite il comando `xmlexportdb` non viene accettato.
- <*file_SQL*> – file per la scrittura di tutte le query SQL che verranno eseguite in caso di importazione del database dal file indicato nel <*file_di_database*>. Se nessun file SQL è indicato, la scrittura viene eseguita nel log di Server (nella forma di una lista delle tabelle e dei campi). Se un file è indicato, allora soltanto nel file SQL.
- <*filtro_delle_tabelle*> – lista delle tabelle del database, informazioni su cui verranno riportate nel <*file_SQL*>. La lista delle tabelle deve essere indicata con la separazione da virgole. I

nomi devono corrispondere ai nomi delle tabelle nel database. Per esempio: `admins,groups,stations`. Il filtro delle tabelle è valido solo per l'output nel file SQL. Se la lista delle tabelle non è indicata, vengono riportate tutte le tabelle.

Verifica del database

`drwcsd verifydb` – avvia il Server per la verifica del database. Alla fine della verifica il Server restituisce informazioni sui risultati nel file di log (di default è `drwcsd.log`).

Accelerazione del database

`drwcsd [<opzioni>] speedupdb` – esegui i comandi `VACUUM`, `CLUSTER`, `ANALYZE` per accelerare l'utilizzo del database.

Ripristino del database

`drwcsd repairdb` – esegui il ripristino di un'immagine corrotta del database incorporato **SQLite3** o di tabelle corrotte del database esterno **MySQL**.

Il ripristino di **SQLite3** può anche essere effettuato automaticamente durante l'avvio del Server, 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 del database).

Pulizia del database

`drwcsd cleandb` – ripulisci il database di Server, eliminando tutte le tabelle.

H4.4. Comandi di gestione del repository

Prima di eseguire i comandi `syncrepository`, `restorerepo` e `saverepo`, è obbligatorio arrestare il Server.

- `drwcsd syncrepository` – sincronizza il repository con SAM Dr.Web. Il comando avvia il processo Server, viene stabilita una connessione con SAM e quindi il repository viene aggiornato, se sono disponibili degli aggiornamenti.
- `drwcsd rerepository` – rileggi il repository da disco.
- `drwcsd updrepository` – aggiorna il repository da SAM Dr.Web. Il comando invia un segnale al processo di Server in esecuzione di connettersi a SAM e aggiornare successivamente il repository, in caso di presenza di aggiornamenti. Se Server non è in esecuzione, l'aggiornamento del repository non viene eseguito.
- `drwcsd [<opzioni>] restorerepo <nome_completo_archivio>` – ripristina il repository di Server 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 in un archivio zip indicato. L'archivio risultante può essere importato su Server 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.

H4.5. Backup dei dati critici del Server Dr.Web

Il backup dei dati critici del Server (chiavi di licenza, contenuti del database, chiave di cifratura privata, configurazione del Server e del Pannello di controllo) viene creato tramite il seguente comando:

`drwcsd -home=<percorso> backup [<directory> [<numero>]]`

- I dati critici di Server vengono copiati nella *<directory>* indicata.
- L'opzione `-home` imposta la directory di installazione di Server.
- Il parametro *<numero>* imposta 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" backup C:\a
```

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 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 è incluso un task quotidiano. Se tale task non è disponibile nel calendario, si consiglia di crearlo.

H4.6. Comandi disponibili solo in SO Windows®

- `drwcsd [<opzioni>] install [<nome_del_servizio>]` – installa il servizio Server 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, e 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 dal sistema.

  <*nome_del_servizio*> è un suffisso che viene aggiunto al nome del servizio di default, e il nome completo del servizio è: `DrWebES-`<*nome_del_servizio*>.
- `drwcsd kill` – manda in crash il servizio Server (se non è possibile arrestarlo normalmente). Non si consiglia di utilizzare questo comando, se non assolutamente necessario.
- `drwcsd silent [`<*opzioni*>`]` <*comando*> – proibisci la visualizzazione dei messaggi Server ad avvio del comando specificato nel parametro <*comando*>. Si utilizza, in particolare, in file batch per disattivare l'interattività del funzionamento di Server.
- `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.

H4.7. Comandi disponibili solo in SO della famiglia UNIX®

- `drwcsd config` – simile al comando `reconfigure` o `kill SIGHUP` – riavvio del Server.
- `drwcsd interactive` – il comando avvia il Server ma non passa il controllo al processo.
- `drwcsd newkey` – generazione delle nuove chiavi di cifratura `drwcsd.pri` e `drwcsd.pub`, nonché del 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 fornisce il nome del computer su cui è installato il Server per cui verranno generati i file. Se il parametro non è impostato, il nome di computer viene inserito automaticamente da una 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 (in esecuzione, arrestato).

H4.8. Descrizione delle opzioni

Opzioni multipiattaforma

- `-activation-key=`<*chiave_licenza*> – chiave di licenza di Server. Di default, è il file `enterprise.key` locato nella sottodirectory `etc` della directory radice.

  Notarsi che la chiave di licenza di Server non si usa più a partire dalla versione 10. La chiave `-activation-key` può essere utilizzata quando un Server viene aggiornato da versioni

precedenti e quando un database viene inizializzato: l'identificatore di Server verrà preso dalla chiave di licenza indicata.

- `-bin-root=<directory_di_eseguibili>` – percorso dei file eseguibili. Di default, è la sottodirectory `bin` della directory radice.
- `-conf=<file_configurazione>` – nome e posizione del file di configurazione di Server. 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 in background).
- `-db-verify=on` – controlla l'integrità del database all'avvio di Server. Valore predefinito. È fortemente sconsigliato avviare il programma indicando esplicitamente il valore opposto, ad eccezione dell'avvio subito dopo un controllo di database attraverso il comando `drwcsd verifydb`, vedi sopra.
- `-help` – visualizza la guida. In modo simile ai programmi descritti sopra.
- `-hooks` – consenti al Server 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=<radice>` – directory di installazione di Server (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=<log>` – nome del file di log di Server. Invece di un nome di file, si può usare il segno "meno" (solo per un Server su piattaforme UNIX) che significa "mostra il log in output standard". Di default: per le piattaforme Windows, è `drwcsd.log` nella directory indicata dall'opzione `-var-root`, per le piattaforme UNIX viene impostato dall'opzione `-syslog=user` (v. sotto).
- `-private-key=<chiave_privata>` – chiave privata di Server. 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, 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.

Parametro	Descrizione
<*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 1° gennaio del 1° anno d.C., UTC+0.

Di default, è `10,10m`, il che significa "conserva 10 file di 10 megabyte ciascuno, utilizza compressione". Si può inoltre usare 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` – è il file attuale (in cui si registrano le informazioni),
- `file.1.log` – è 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_di_modificabili*> – percorso della directory in cui il Server ha il permesso di scrittura e che è progettata per la memorizzazione di file modificabili (per esempio, i log, nonché i file di repository). Di default, è la sottodirectory `var` della directory radice.
- `-verbosity=`<*livello_dettaglio*> – 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 (v. inoltre Allegato K. 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 in SO Windows

- `-minimized` – (solo in caso dell'avvio in modo interattivo anziché come servizio) – riduci la finestra.
- `-service=<`*nome_del_servizio*`>` – l'opzione viene utilizzata dal processo del servizio in esecuzione per l'auto-identificazione e l'impostazione dell'auto-protezione sul ramo del registro del servizio Server. *<nome_del_servizio>* è un suffisso che viene aggiunto al nome del servizio di default, e 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 in caso dell'avvio in modo interattivo anziché come servizio) – la dimensione in righe del log visibile nella finestra di Server, di default è 1000.

Opzioni disponibili solo nei SO della famiglia UNIX

- `-etc=<`*path*`>` – percorso della directory `etc` (`<var>/etc`).
- `-pid=<`*file*`>` – file in cui il Server 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. Vuol dire che se il Server viene avviato con l'opzione `-syslog` (per esempio, `service drwcsd start -syslog=user`), il Server 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".

H4.9. Variabili disponibili in SO della famiglia UNIX®

Per semplificare la gestione del Server negli SO della famiglia UNIX l'amministratore ha a disposizione delle variabili locate in un file di script memorizzato 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` – per 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	`$DRWCS_VAR/etc`
`-rotate`	DRWCS_ROT	`10,10m`
`-verbosity`	DRWCS_LEV	`trace3`
`-log`	DRWCS_LOG	`$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		
DRWCS_CORE	`unlimited`	Dimensione massima di core file.
DRWCS_FILES	8192	Numero massimo di descrittori di file, che il Server può aprire.
DRWCS_BIN	`$DRWCS_HOME/bin`	Directory da cui viene avviato `drwcsd`.
DRWCS_LIB	`$DRWCS_HOME/lib`	Directory con le librerie del Server.

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 `${TGT_ES_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, è necessario:

1. Aggiungere la definizione della variabile nel file dello script `drwcsd`.
2. Esportare la variabile tramite il comando `export` (viene impostato sempre lì).
3. Quando viene avviato ancora un altro processo da questo script, questo processo legge i valori che sono stati definiti.

H5. Gestione del Server Dr.Web sotto SO della famiglia UNIX® tramite il comando kill

Il Server sotto UNIX viene gestito dai segnali inviati al processo Server da parte dell'utility `kill`.

Una guida dettagliata all'utility `kill` può essere ottenuta tramite il comando `man kill`.

Di seguito, viene riportata una lista dei segnali dell'utility e delle azioni da essi eseguite:

- `SIGWINCH` – includi nel file di log le statistiche di funzionamento (tempo CPU, utilizzo di memoria ecc.),
- `SIGUSR1` – rileggi il repository da disco,
- `SIGUSR2` – rileggi i modelli di avviso da disco,
- `SIGHUP` – riavvio del Server,
- `SIGTERM` – arresto del Server,
- `SIGQUIT` – arresto del Server,
- `SIGINT` – arresto del Server.

Le azioni analoghe per il Server sotto il sistema operativo Windows vengono realizzate tramite le opzioni del comando drwcsd, vedi Allegato H4.3. Comandi di gestione del database.

H6. Scanner Dr.Web per Windows®

Questo componente del software postazione ha parametri da riga di comando che vengono descritti nel manuale dell'utente **Agent Dr.Web® per Windows**. L'unica differenza è che quando lo Scanner viene avviato dall'Agent, i parametri `/go /st` vengono passati allo Scanner automaticamente ed obbligatoriamente.

H7. 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 di 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:
	• 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 1° gennaio del 1° 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 memorizzazione 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.

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.

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 deve essere scaricato anticipatamente 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 di configurazione di Server proxy.
- `run` – avvia Server proxy in modalità normale.

Solo in SO Windows

- `install` – installa il servizio.
- `uninstall` – rimuovi il servizio.
- `start` – avvia il servizio istallato.
- `stop` – termina il servizio installato.

Solo in SO della famiglia UNIX

- `daemon` – avvia Server proxy in modalità daemon (vedi inoltre Opzioni sotto i sistemi operativi della famiglia UNIX).

H8. Installer di Server Dr.Web per SO della famiglia UNIX®

Formato del comando di avvio:

<nome_pacchetto>`.run [<`*opzioni*`>] [--] [<`*argomenti*`>]`

dove:

- `[--]` – è un carattere opzionale separato che designa 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 target; 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; se i contenuti dell'archivio verranno copiati nella directory temporanea (se no, nulla viene visualizzato); se la directory target è permanente o verrà rimossa dopo l'esecuzione dello script.
- `--list` – visualizza l'elenco dei file nel pacchetto d'installazione.
- `--check` – verifica l'integrità del pacchetto d'installazione.

Le opzioni per l'avvio del pacchetto:

- `--confirm` – visualizza una richiesta prima di eseguire lo script incorporato.
- `--noexec` – non eseguire lo script incorporato.
- `--target <`*directory*`>` – estrai il pacchetto d'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.
- `--quite` – avvia l'installer in modalità silenziosa. Si usa una 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 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 dell'installazione precedente (non si usa se è impostata un'installazione con le impostazioni di default).
  - `QUIET_INSTALL=[0|1]` – definisce l'utilizzo della modalità silenziosa dell'installer:
    - 0 – avvia l'installer in modalità silenziosa;
    - 1 – avvia l'installer in modalità normale.
  - `CLEAN_INSTALL=[0|1]` – definisce 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`.

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.

H9. Utility

H9.1. 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 `webmin/utilities`	
`drwsign`	Directory di Server `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>] <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 un 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 scrivila 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 del Server 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 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>] [-cert=<certificato_da_firmare>] [-days=<validità>] [<certificato_firmato>]`

  Firma il <*certificato_da_firmare*> predisposto tramite la chiave privata e il certificato di Server. Il certificato firmato viene salvato in un file separato.

  Può essere utilizzato per firmare il certificato di Server proxy tramite la chiave di Server.

Parametro dell'opzione	Valore predefinito
<*chiave_privata*>	`drwcsd.pri`
<*certificato_Server*>	`drwcsd-ca-cerificate.pem`
<*certificato_da_firmare*>	`drwcsd-certificate.pem`
<*validità*>	`3560`
<*certificato_firmato*>	`drwcsd-signed-certificate.pem`

- `drwsign signcsr [-ca-key=<chiave_privata>] [-ca-cert=<certificato_Server>] [-csr=<richiesta_di_firma_del_certificato>] [-days=<validità>] [<certificato_firmato>]`

  Firma <*richiesta_di_firma_del_certificato*>, generato dal comando `gencsr`, tramite la chiave privata e il certificato di Server. 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 tramite la chiave di Server Dr.Web.

Parametro dell'opzione	Valore predefinito
<*chiave_privata*>	`drwcsd.pri`
<*certificato_Server*>	`drwcsd-cerificate.pem`
<*richiesta_di_firma_del_certificato*>	`drwcsd-certificate-sign-request.pem`
<*validità*>	`3560`
<*certificato_firmato*>	`drwcsd-signed-certificate.pem`

- `drwsign tlsticketkey [<ticket_TLS>]`

  Genera ticket TLS.

  Può essere utilizzato nel cluster di Server per le sessioni TLS comuni.

Parametro dell'opzione	Valore predefinito
<*ticket_TLS*>	`tickets-key.bin`

- `drwsign verify [-ss-cert] [-CAfile=<certificato_Server>] [<certificato_da_verificare>]`

  Verifica la validità del certificato in base a un certificato di Server attendibile.

L'opzione `-ss-cert` comanda di ignorare il certificato attendibile e di verificare soltanto la correttezza del certificato autofirmato.

Parametro dell'opzione	Valore predefinito
<*certificato_Server*>	`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`

H9.2. Utility di amministrazione del database incorporato

Vengono fornite le seguenti utility per l'amministrazione del database incorporato:

- `drwidbsh` – per il database IntDB,
- `drwidbsh3` – per il database SQLite3.

Le utility si trovano 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_installazione_Server*>`\bin`

  (di default, la directory di installazione di Server: `C:\Program Files\DrWeb Server`).

Formato del comando di avvio:

`drwidbsh` <*nome_completo_file_database*>

o

`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.

H9.3. 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 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 `webmin/utilities`	
`drwcntl`	Directory di Server `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, 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 è necessario che per l'amministratore che si connette attraverso l'utility sia consentito il permesso **Utilizzo delle funzioni addizionali**. Altrimenti, sarà negato l'accesso al Server attraverso l'utility di diagnostica remota.

Per connettere l'utility (sia grafica che console) con l'utilizzo di TLS, è necessario impostare il protocollo direttamente quando viene indicato l'indirizzo di Server: `ssl://<indirizzo IP o nome DNS>`.

Le impostazioni di Server 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:

- `--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, 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 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**. Questo disabilita il tag `<ssl />` nel file di configurazione `frontdoor.conf`.
Indirizzo IP o nome DNS del Server	L'utility richiederà di inserire l'indirizzo del Server in formato opportuno.
Porta	`10101`  Sul lato Server 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 si usa un'altra porta, è necessario specificare in modo esplicito questa porta al momento della connessione dell'utiilty.

- <*nome_utente*> – il nome utente dell'amministratore del Server.
- <*password*> – la password dell'amministratore per l'accesso al Server.

  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*> – utilizzo della cache di file. Per invocare una concreta 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 dell'utilizzo della cache di file.
- `calculate` <*funzione*> – il calcolo di una data sequenza. Per invocare una sequenza concreta, utilizzare i seguenti comandi:
  - `hash [`<*standard*>`] [`<*stringa*>`]` – calcola l'hash di una data stringa. Per impostare uno standard concreto, 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 concreto, 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. Per invocare una funzione concreta, utilizzare i seguenti comandi:

- `addresses [`<*espressione regolare*>`]`– mostra gli indirizzi di rete delle postazioni che soddisfano l'espressione regolare impostata. Se nessun'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 nessun'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. 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.
- `statistics` <*espressione regolare*> – mostra le statistiche per 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` – registra il dump del processo di Server.
- `cpu` <*parametro*> – mostra le statistiche dell'utilizzo della CPU del computer su cui è installato il Server. Per invocare un concreto parametro, utilizzare i seguenti comandi:

- `clear` – cancella tutti i dati statistici accumulati,
- `day` – mostra un 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 un grafico di utilizzo della CPU per il minuto passato,
- `rawd` – mostra le statistiche numeriche dell'utilizzo della CPU per il giorno,
- `rawh` – mostra le statistiche numeriche dell'utilizzo della CPU per l'ora passata,
- `rawl` – mostra le statistiche numeriche dell'utilizzo medio della CPU,
- `rawm` – mostra le statistiche numeriche dell'utilizzo della CPU per il minuto passato,
- `status` – mostra lo stato del monitoraggio delle statistiche dell'utilizzo della CPU.

- `debug` <*parametro*> – configurazione del debug. Per impostare un parametro concreto, utilizzare i comandi aggiuntivi. Per consultare l'elenco dei comandi aggiuntivi, invocare la guida tramite il comando: `? debug`.

Il comando `debug signal` è disponibile soltanto per i Server sotto SO della famiglia UNIX.

- `die` – arresta il Server e registra il dump del processo Server.

Il comando `die` è disponibile soltanto per i Server sotto SO della famiglia UNIX.

- `dwcp` <*parametro*> – imposta/mostra le impostazioni di Dr.Web Control Protocol (comprende i log di Server, Agent e di installer di Agent). I parametri ammissibili:
  - `compression` <*modalità*> – imposta una delle seguenti modalità di compressione di traffico:
    - `on` – compressione attivata,
    - `off` – compressione disattivata,
    - `possible` – la compressione è possibile.
  - `encryption` <*modalità*> – imposta una delle seguenti modalità di cifratura di 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 di dati da parte del processo Server. Per invocare un concreto parametro, 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 di dati per il giorno,
  - `rawdw` – mostra le statistiche numeriche di scrittura di dati per il giorno,
  - `rawh` – mostra le statistiche numeriche per l'ora passata,
  - `rawm` – mostra le statistiche numeriche per il minuto passato,
  - `rday` – mostra un grafico delle statistiche di lettura di dati per il giorno,
  - `rhour` – mostra un grafico delle statistiche di lettura di dati per l'ora passata,
  - `rminute` – mostra un grafico delle statistiche di lettura di dati per il minuto passato,
  - `status` – mostra lo stato del monitoraggio delle statistiche,
  - `wday` – mostra un grafico delle statistiche di scrittura di dati per il giorno,
  - `whour` – mostra un grafico delle statistiche di scrittura di dati per l'ora passata,
  - `wminute` – mostra un grafico delle statistiche di scrittura di dati per il minuto passato.
- `log` <*parametro*> – scrivi la stringa nel file di log di Server oppure imposta/visualizza il livello di dettaglio del log. A seconda dei parametri impostati, vengono eseguite le seguenti azioni:
  - `log` <*stringa*> – scrivi la stringa nel log di Server 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 di memoria. Per configurare un'impostazione concreta, utilizzare i comandi aggiuntivi. Per consultare l'elenco dei comandi aggiuntivi, invocare la guida tramite il comando: `? mallopt`.

  

  Il comando `mallopt` è disponibile soltanto per i Server 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. Per invocare un concreto parametro, utilizzare i seguenti comandi:
  - `all` – visualizza tutte le informazioni e statistiche,
  - `heap` – visualizza le informazioni su memoria dinamica,
  - `malloc` – visualizza le statistiche su allocazione di memoria,
  - `sizes` – visualizza le statistiche su dimensioni della memoria allocata,
  - `system` – visualizza le informazioni su memoria di sistema.

Il comando `memory` è disponibile soltanto per i Server 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 sotto SO Windows, SO della famiglia Linux,
- `heap` – solo per i Server sotto SO Windows, SO della famiglia Linux,
- `malloc` – solo per i Server sotto SO della famiglia Linux e SO della famiglia FreeBSD,
- `sizes` – solo per i Server 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. I comandi ammissibili:
  - `disable` – disattiva il monitoraggio,
  - `enable` – attiva il monitoraggio,
  - `show` – visualizza la modalità attuale.
- `printstat` – scrivi le statistiche del funzionamento di Server nel log.
- `reload` – riavvia l'estensione Dr.Web Server FrontDoor.
- `repository` <*parametro*> – gestione del repository. Per invocare una funzione concreta, utilizzare i seguenti comandi:
  - `all` – visualizza l'elenco di tutti i prodotti del repository e il numero totale di file dei prodotti,
  - `clear` – cancella i contenuti della cache a prescindere dal valore TTL degli oggetti locati nella cache,
  - `fill` – memorizza tutti i file del repository nella cache,
  - `keep` – conserva tutti i file del repository, che si trovano attualmente nella cache, sempre, a prescindere dal loro valore TTL,
  - `loaded` – visualizza l'elenco di tutti i prodotti del repository e il numero totale di file dei prodotti che si trovano attualmente nella cache,
  - `reload` – riavvia il repository da disco,
  - `statistics` – mostra le statistiche degli aggiornamenti del repository.
- `restart` – riavvia il Server.
- `show` <*parametro*> – mostra informazioni sul sistema su cui è installato il Server. Per impostare un parametro concreto, 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 sotto SO Windows, SO della famiglia Linux,
- `mapping` – solo per i Server sotto SO Windows, SO della famiglia Linux,
- `limits` – solo per i Server sotto SO della famiglia UNIX,

- `processors` – solo per i Server sotto SO della famiglia Linux.

- `sql` <*query*> – esegui una data query SQL.
- `stop` – arresta il Server.
- `traffic` <*parametro*> – mostra le statistiche del traffico di rete del Server. Per invocare un concreto parametro, utilizzare i seguenti comandi:
  - `all` – mostra l'intera entità di traffico dall'inizio del funzionamento di Server.
  - `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 concreta, utilizzare le seguenti opzioni:
  - `active` – mostra l'elenco degli Agent che attualmente eseguono un aggiornamento.
  - `agent [`<*modalità*>`]` – mostra/imposta la modalità di aggiornamento degli Agent dal Server. Se eseguito senza parametri aggiuntivi, mostra la modalità corrente. Per impostare una modalità, utilizzare le seguenti opzioni aggiuntive:
    - `on` – attiva gli aggiornamenti degli Agent.
    - `off` – disattiva gli aggiornamenti degli Agent.
  - `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 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 che attualmente non eseguono l'aggiornamento.
  - `track [`<*modalità*>`]` – mostra/imposta la modalità di monitoraggio di aggiornamenti di Agent. Se eseguito senza parametri aggiuntivi, mostra la modalità corrente. Per impostare una modalità, utilizzare i seguenti comandi aggiuntivi:
    - `on` – attiva il monitoraggio degli aggiornamenti di Agent.
    - `off` – disattiva il monitoraggio degli aggiornamenti di Agent. In tale caso l'opzione `update active` non visualizzerà l'elenco degli Agent che vengono aggiornati.

H9.4. 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 `webmin/utilities`	
`drwcmd`	Directory di Server `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, 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 è necessario che per l'amministratore che si connette attraverso l'utility sia consentito il permesso **Utilizzo delle funzioni addizionali**. Altrimenti, sarà negato l'accesso al Server attraverso l'utility di diagnostica remota.

Le impostazioni di Server 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 H1. Introduzione.

- `--?` – 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 una connessione con il Server 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. 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. Può essere definita nel file specificato nell'opzione `--resource`.
- `--read=yes|no` – consenti la lettura dei parametri di connessione al Server da un file di risorse. Di default è `yes`.
- `--resource=<file>` – file di risorse con i parametri di connessione al Server: l'indirizzo del Server e le credenziali di amministratore per l'autenticazione sul Server. Di default viene utilizzato il file `.drwcmdrc` locato 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*> <*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
```

- `--server=<Server>` – indirizzo del Server. 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. Può essere definito nel file specificato nell'opzione `--resource`.
- `--verbose=yes|no` – restituisci una risposta dettagliata del Server (flusso di output standard `stdout`). Di default è `no`.

Procedura per la connessione al Server:

1. Per la determinazione dei dati di connessione al Server 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 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 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.
- 4 – errore di autenticazione sul Server: nome e/o password dell'amministratore non validi.
- 5 – caduta inaspettata della connessione con il Server.
- 127 – errore fatale non definito.

H9.5. 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 `webmin/utilities`	
`drwreploader`	Directory di Server `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 soltanto 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. I file scaricati possono essere importati direttamente attraverso il Pannello di controllo come un aggiornamento del repository di Server. 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 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 caricato l'intero repository.
- `--prohibit-cdn` – proibisci l'utilizzo di CDN per il caricamento degli aggiornamenti. Di default: `no`, cioè l'utilizzo di 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.

  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 il 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*> – la directory sui server SAM che contiene gli aggiornamenti dei prodotti Dr.Web. È consigliabile lasciare il valore predefinito – `/update`.
- `--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*> – la versione del Server per cui è necessario scaricare gli aggiornamenti nel formato <*versione_principale*>`.`<*versione_secondaria*>. Per esempio, nel caso di Server versione 11, il parametro <*versione*> assume il valore `11.00`.

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 soltanto con il Server:

```
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
```

Allegato I. Variabili di ambiente esportate dal Server Dr.Web

Per semplificare la configurazione dei processi avviati da Server Dr.Web secondo il calendario, sono richieste informazioni sulla posizione delle directory di Server. A questo scopo il Server 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, 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, altrimenti, è la sottodirectory `bin` della directory radice.
- `DRWCSD_VAR` – percorso della directory in cui il Server può registrare informazioni e in cui si conservano i file modificabili (per esempio, log e file di repository). È il valore dell'opzione `-var-root`, se è stata impostata per l'avvio del Server, altrimenti è la sottodirectory `var` della directory radice.

Allegato J. Utilizzo di 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.

J1. Opzioni delle espressioni regolari PCRE

Le espressioni regolari vengono utilizzate sia nel file di configurazione di Server che nel Pannello di controllo per indicare oggetti da escludere dalla scansione nelle impostazioni di Scanner.

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`.

J2. 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 sé 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 K. Formato dei file di log

I file di log del Server (v. **Manuale dell'amministratore**, p. Log di funzionamento di Server Dr.Web) e dell'Agent hanno un formato di testo, in essi ogni riga è 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 di avviso nel file di log.
- *<tipo_avviso>* – livello di registrazione di informazioni in 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 – debugging) – avvisi di debugging con i vari livelli di dettaglio (**Debugging3** – 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>*`]` – è 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 presentato 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 di azioni secondo il livello di log. Può comprendere sia una descrizione formale di avviso, che 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 L. 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 M. 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*	http://think-async.com/
boost	https://www.boost.org/LICENSE_1_0.txt*	http://www.boost.org/
brotli	MIT License**	https://github.com/google/brotli
bsdiff	Custom	http://www.daemonology.net/bsdiff/
c-ares	https://c-ares.haxx.se/license.html*	http://c-ares.haxx.se/
cairo	Mozilla Public License** GNU Lesser General Public License**	http://cairographics.org/
CodeMirror	MIT License**	http://codemirror.net/
curl	http://curl.haxx.se/docs/copyright.html*	http://curl.haxx.se/libcurl/
ICU	http://www.unicode.org/copyright.html#License*	http://site.icu-project.org/home
fontconfig	Custom	http://www.freedesktop.org/wiki/Software/fontconfig
freetype	GNU General Public License** FreeType Project License (BSD like)	http://www.freetype.org/
GCC runtime libraries	GNU General Public License** with exception*	http://gcc.gnu.org/
HTMLayout	Custom	http://www.terrainformatica.com/htmlayout/
jemalloc	https://github.com/jemalloc/jemalloc/blob/dev/COPYING*	https://github.com/jemalloc/jemalloc
jQuery	MIT License** GNU General Public License**	http://jquery.com/
Leaflet	BSD License	http://leafletjs.com

Libreria di terze parti	Licenza	URL del progetto
	https://github.com/Leaflet/Leaflet/blob/master/LICENSE*	
libpng	http://libpng.org/pub/png/src/libpng-LICENSE.txt*	http://libpng.org/pub/png/libpng.html
libradius	© Juniper Networks, Inc.*	http://www.freebsd.org
libssh2	https://www.libssh2.org/license.html*	https://www.libssh2.org/
libxml2	MIT License**	http://www.xmlsoft.org/
Linenoise NG	BSD License*	https://github.com/arangodb/linenoise-ng
lua	MIT License**	http://www.lua.org/
lua-xmlreader	MIT License**	http://asbradbury.org/projects/lua-xmlreader/
lua4json	MIT License**	http://json.luaforge.net/
lzma	GNU Lesser General Public License** Common Public License**	http://www.7-zip.org/sdk.html
ncurses	MIT License**	https://www.gnu.org/software/ncurses/ncurses.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	http://scripts.sil.org/cms/scripts/render_download.php?format=file&media_id=OFL_plaintext&filename=OFL.txt*	https://www.google.com/get/noto/help/cjk/
OpenLDAP	http://www.openldap.org/software/release/license.html*	http://www.openldap.org
OpenSSL	http://www.openssl.org/source/license.html*	http://www.openssl.org/
Oracle Instant Client	http://www.oracle.com/technetwork/licenses/instant-client-lic-152016.html*	http://www.oracle.com
ParaType Free Font	http://www.paratype.ru/public/pt_openlicense_eng.asp*	http://www.paratype.ru
pcre	http://www.pcre.org/licence.txt*	http://www.pcre.org/

Libreria di terze parti	Licenza	URL del progetto
pixman	MIT License**	http://pixman.org/
Prototype JavaScript framework	MIT License**	http://prototypejs.org/assets/2009/8/31/prototype.js
script.aculo.us scriptaculous.js	http://madrobby.github.io/scriptaculous/license/*	http://script.aculo.us/
slt	MIT License**	http://code.google.com/p/slt/
SQLite	Public Domain http://www.sqlite.org/copyright.html	http://www.sqlite.org/
wtl	Common Public License** Mozilla Public License**	http://sourceforge.net/projects/wtl/
zlib	http://www.zlib.net/zlib_license.html*	http://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	http://opensource.org/licenses/cpl1.0.php
GNU General Public License	https://www.gnu.org/licenses/gpl-3.0.html
GNU Lesser General Public License	https://www.gnu.org/licenses/lgpl-3.0.html
Mozilla Public License	https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649456(v=pandp.10)
MIT License	https://opensource.org/licenses/mit-license.php
Mozilla Public License	https://www.mozilla.org/en-US/MPL/2.0/

M1. 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.
```

M2. 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.
```

M3. 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.
```

M4. ICU

M5. GCC runtime libraries—exception

```
 - 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.
```

M6. 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.

--------------------------------------------------------------------------------
```

M7. Leaflet

M8. Libpng

```
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
```

M9. 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 $
```

M10. Libssh2

M11. 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.
```

M12. 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:
```

```
* 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 Cambridge Broadband Ltd. 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 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks
of Sun Microsystems, Inc. in the U.S. and other countries.

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 Sun Microsystems, 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 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.
```

```
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.
```

M13. 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.

M14. 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.
```

M15. 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.]
```

M16. 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

M17. 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
```

M18. 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.
```

M19. 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.
```

M20. 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
```

Capitolo 3: Domande ricorrenti

Trasferimento del Server Dr.Web su un altro computer (in caso del SO Windows®)

Quando il Server 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 del Server viene descritta in **Manuale dell'amministratore**, p. Avvio e arresto del Server Dr.Web.

Per trasferire il Server Dr.Web (se viene installata una versione di Server Dr.Web uguale) sotto il SO Windows:

1. Arrestare il servizio Server Dr.Web.
2. Avviare dalla riga di comando il file `drwcsd.exe` con l'opzione `exportdb` per esportare i contenuti del database in un file. La completa riga di comando di esportazione in caso di versione per SO Windows si presenta approssimativamente così:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" exportdb <nome_completo_file>
   ```

3. Salvare i contenuti della directory `C:\Program Files\DrWeb Server\etc`, e inoltre la chiave `drwcsd.pub` da `C:\Program Files\DrWeb Server\webmin\install`.
4. Eliminare il Server.
5. Installare un Server 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`, e inoltre la chiave `drwcsd.pub` e il certificato `drwcsd-certificate.pem` in `C:\Program Files\DrWeb Server\webmin\install`.
7. Avviare dalla riga di comando il file `drwcsd.exe` con l'opzione `importdb` per importare i contenuti del database da file. La completa riga di comando di importazione in caso di versione per SO Windows si presenta approssimativamente così:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" importdb <nome_completo_file>
   ```

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 installato con il file precedente, conservato dal Server 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`, e inoltre la chiave `drwcsd.pub` da `C:\Program Files\DrWeb Server\webmin\install`.
4. Eliminare il Server.
5. Installare un Server 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`, e inoltre la chiave `drwcsd.pub` e il certificato `drwcsd-certificate.pem` in `C:\Program Files\DrWeb Server\webmin\install`.
7. Ripristinare il database sul nuovo Server, indicare il percorso del database nel file di configurazione `drwcsd.conf`.
8. Avviare dalla riga di comando il file `drwcsd.exe` con l'opzione `upgradedb` per aggiornare il database. La completa riga di comando di aggiornamento database in caso di versione per SO Windows si presenta approssimativamente così:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" upgradedb "C:\Program Files\DrWeb Server\update-db"
```

9. Avviare il servizio Server Dr.Web.

In caso di cambio di nome o indirizzo IP a trasferimento di Server Dr.Web:

Affinché possano migrare gli Agent per i quali l'indirizzo nel nuovo Server viene impostato tramite il Pannello di controllo e non nella configurazione dell'Agent stesso su postazione, lasciare attivati entrambi i Server fino al momento del completamento della procedura.

1. Trasferire il Server secondo la procedura corrispondente descritta sopra.
2. Per tutti gli Agent che erano connessi al vecchio Server, impostare l'indirizzo del nuovo Server secondo la procedura corrispondente descritta nella sezione Connessione di Agent Dr.Web ad un altro Server Dr.Web.

Per gli Agent per i quali l'indirizzo nel nuovo Server veniva impostato tramite il Pannello di controllo e non nella configurazione dell'Agent stesso su postazione, su entrambi i Server nelle impostazioni di Agent deve essere indicato l'indirizzo del nuovo Server.

3. Aspettare che tutti gli Agent passino al nuovo Server. Quindi si può rimuovere il vecchio Server.

Connessione dell'Agent Dr.Web ad un altro Server Dr.Web

È possibile connettere l'Agent ad un altro Server 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 vecchio. È necessario l'accesso ai Pannelli di controllo dei Server vecchio e nuovo.

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 dell'Agent stabilite sul Server. Se questi permessi non sono disponibili, la connessione ad un altro Server in modo locale su postazione è possibile soltanto dopo la rimozione dell'Agent installato e dopo l'installazione di un Agent nuovo con le impostazioni del nuovo Server. Se non ci sono i permessi di rimozione dell'Agent in modo locale, utilizzare l'utility Dr.Web Remover per rimuovere l'Agent sulla postazione o rimuovere l'Agent tramite il Pannello di controllo.

Per connettere Agent Dr.Web ad un altro Server Dr.Web attraverso il Pannello di controllo:

1. Sul nuovo Server consentire alle postazioni con credenziali non valide di richiedere nuove impostazioni 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** od a **Consenti l'accesso automaticamente**.
   c) Per rendere effettive le modifiche apportate, premere il pulsante **Salva** e riavviare il Server.

   Se i criteri di sicurezza aziendali non permettono di modificare le impostazioni dal passo 1, le impostazioni di autenticazione di postazione corrispondenti all'account creato in precedenza nel Pannello di controllo devono essere stabilite direttamente sulla postazione.

2. Sul Server vecchio a cui è connesso l'Agent, impostare i parametri del Server nuovo. 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 nuovo non coincide con il certificato del Server vecchio, nel campo **Certificato** indicare il percorso del certificato del Server nuovo.

b) Nel campo **Server** indicare l'indirizzo del nuovo Server.

c) Premere il pulsante **Salva**.

Per connette l'Agent Dr.Web ad un altro Server Dr.Web direttamente sulla postazione:

1. Nelle impostazioni di Agent impostare i parametri del Server nuovo. A tale scopo nel menu contestuale dell'icona Agent selezionare: **Impostazioni** → scheda **Principali** → voce **Server** → sezione **Parametri di connessione** → pulsante **Modifica impostazioni**:
   a) Se il certificato del Server nuovo non coincide con il certificato del Server vecchio, utilizzando il pulsante **Lista dei certificati** indicare il percorso del certificato del Server nuovo.
   b) Utilizzando il pulsante **Aggiungi** impostare i parametri corrispondenti del Server nuovo.
2. Trasferire la postazione in nuovi arrivi (resettare i parametri di autenticazione sul Server). 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 nuovo Server, è possibile indicarle nei campi **ID della postazione** e **Password**. In tale caso non è necessario trasferire la postazione in nuovi arrivi.

Cambio del tipo di DBMS di Dr.Web Enterprise Security Suite

In caso di SO Windows

La procedura per l'avvio e l'arresto del Server viene descritta in **Manuale dell'amministratore**, p. Avvio e arresto del Server Dr.Web.

1. Arrestare il servizio Server Dr.Web.
2. Avviare dalla riga di comando il file `drwcsd.exe` con l'opzione `exportdb` per esportare i contenuti del database in un file. La completa riga di comando di esportazione in caso di versione per 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 exportdb D:\esbase.es
   ```

   Questo esempio presuppone che il Server Dr.Web sia installato nella directory `C:\Program Files\DrWeb Server` e che il database venga 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, connetterci il Pannello di controllo e riconfigurare il Server per l'utilizzo di un altro DBMS. Rifiutare la proposta di riavvio del Server.
4. Arrestare il servizio Server Dr.Web.
5. Eliminare il file del database.
6. Avviare dalla riga di comando il file `drwcsd.exe` con l'opzione `initdb` per inizializzare il nuovo database. La riga di inizializzazione del database per la versione di Server 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 initdb D:\Keys\agent.key - - <password>
   ```

   Questo esempio presuppone che il Server sia installato nella directory `"C:\Program Files\DrWeb Server"` e la chiave di agent `agent.key` sia locata in `D:\Keys`.

   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>\agent.key"
   ```

7. Avviare dalla riga di comando il file `drwcsd.exe` con l'opzione `importdb` per importare i contenuti del database da file. La completa riga di comando di importazione in caso di versione per 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 importdb 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 con l'opzione `exportdb` per esportare i contenuti del database in un file. La riga di comando dalla directory di installazione del Server si presenta approssimativamente così:
   - in caso di SO **Linux**:

```
/etc/init.d/drwcsd exportdb /var/opt/drwcs/esbase.es
```

   - in caso di SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd exportdb /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 per l'utilizzo di un altro DBMS: nel menu **Amministrazione** → voce **Configurazione del Server Dr.Web** → scheda **Database**.

Si può riconfigurare il Server per l'utilizzo di un altro DBMS anche modificando direttamente il file di configurazione del Server `drwcsd.conf`. Per farlo, si deve commentare/cancellare il record del database corrente e trascrivere il database nuovo (per maggiori informazioni v. Allegato G1. File di configurazione del Server Dr.Web).

Rifiutare la proposta di riavviare il Server.

4. Arrestare il Server Dr.Web (v. passaggio **1**).
5. Eliminare il file del database.
6. Avviare il file `drwcsd` con l'opzione `initdb` per inizializzare il database nuovo. La riga di inizializzazione si presenta approssimativamente così:
   - in caso di SO **Linux**:

```
/etc/init.d/drwcsd initdb
```

   - in caso di SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd initdb
```

7. Avviare il file `drwcsd` con l'opzione `importdb` per importare i contenuti del database da file. La riga di comando di importazione si presenta approssimativamente così:
   - in caso di SO **Linux**:

```
/etc/init.d/drwcsd importdb /var/opt/drwcs/esbase.es
```

   - in caso di SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd importdb /var/drwcs/esbase.es
```

8. Avviare il Server Dr.Web (v. passaggio **3**).

Se durante l'avvio dello script del Server è necessario impostare parametri (per esempio, indicare la directory di installazione del Server, modificare il livello di dettagli di 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 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 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 con altri programmi di archiviazione. È possibile importare il contenuto del database dal backup nel database operativo di Server tramite il comando `importdb` 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** (soltanto per la modalità **Esporta l'intero database**). Tuttavia, in tale caso la copia di backup viene salvata nel formato xml, e per l'importazione è necessario utilizzare il comando `xmlimportdb`.

Ripristino del database per varie versioni di Server Dr.Web

È possibile ripristinare un database solo da un backup creato tramite un Server con la stessa versione principale della versione del Server su cui avviene il ripristino.

Per esempio:

- un database da un backup creato tramite il Server versione 10 può essere ripristinato solo tramite il Server versione 10.
- un database da un backup creato tramite il Server versione 5 o 6 non può essere ripristinato tramite il Server versione 10.

Se durante l'aggiornamento del Server alla versione 11.0.2 dalle versioni più vecchie il database viene danneggiato per qualche motivo, eseguire le seguenti azioni:

1. Rimuovere il Server versione 11.0.2. In tale caso, verranno salvati automaticamente i backup dei file utilizzati dal Server.

2. Installare il Server della versione precedente all'aggiornamento, attraverso cui è stato creato il backup.

   In questo caso, secondo la procedura standard di aggiornamento, si devono utilizzare tutti i file salvati del Server ad eccezione del file del database.

   Durante l'installazione del Server, creare un nuovo database.
3. Ripristinare il database dal backup secondo le regole generali (v. sotto).
4. Nelle impostazioni del Server disattivare i protocolli di Agent, Server 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 alla versione 11.0.2 secondo le regole generali (v. in **Manuale dell'amministratore** p. Aggiornamento di Dr.Web Enterprise Security Suite e dei singoli componenti).
6. Attivare i protocolli di Agent, Server e Installer di rete disattivati al passaggio 4.

In caso di SO Windows

La procedura per l'avvio e l'arresto del Server viene descritta in **Manuale dell'amministratore**, p. Avvio e arresto del 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=all importdb "<percorso_del_file_di_backup>\database.gz"
   ```

   Anche questo comando deve essere digitato in una sola riga. Nell'esempio si sottintende che il Server 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 corrotta:

1. Arrestare il servizio Server Dr.Web, se è in esecuzione.
2. Eliminare i contenuti del database attuale. Per farlo:
   2.1. Se viene utilizzato il database incorporato:
      a) Eliminare il file del database `database.sqlite`.

b) Inizializzare il nuovo database. La riga di inizializzazione del database nella versione del Server 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 initdb D:\Keys\agent.key - - <password>
```

Questo comando deve essere digitato in una riga sola (v. inoltre il formato del comando `drwcsd` con l'opzione `initdb` in Allegato H4.3). Nell'esempio si sottintende che Server è installato nella directory `C:\Program Files\DrWeb Server` e la chiave di licenza `agent.key` si trova nella directory `D:\Keys`.

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`.

2.2. Se si utilizza un database esterno: ripulire il database tramite il comando `cleandb` (v. Allegato H4.3).

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=all importdb "<percorso_del_file_di_backup>\database.gz"
```

Anche questo comando deve essere digitato in una sola riga. Nell'esempio si sottintende che il Server è installato nella directory `C:\Program Files\DrWeb Server`.

4. Avviare il servizio Server Dr.Web.

In caso di 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. Eliminare il file di database `database.sqlite` dalla 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, viene ripulito tramite il comando `cleandb` (v. Allegato H4.3).

3. Inizializzare il database del Server. Per farlo, si utilizza il seguente comando:
   - in caso di SO **Linux**:

```
/etc/init.d/drwcsd initdb
```

   - in caso di SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd initdb
```

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 importdb "<percorso_del_file_di_backup>/database.gz"
```

   - in caso di SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd importdb "<percorso_del_file_di_backup>/database.gz"
```

   - in caso delle **altre** versioni supportate:

```
bin/drwcsd -var-root=./var -verbosity=all -log=logfile.log importdb
"<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 durante l'avvio dello script di Server è necessario impostare parametri (per esempio, indicare la directory di installazione di Server 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 richiesto modificare il livello di dettagli del log di Server, 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 è stato installato dopo la creazione dell'ultimo backup, non potrà connettersi a Server 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.

Dopo che tutte le postazioni si connetteranno al nuovo Server, sostituire queste impostazioni di Server con le impostazioni adottate in conformità con i criteri aziendali.

Dopo il ripristino del database, si consiglia di connettersi al Server 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

Durante l'aggiornamento degli Agent installati sui 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 delle postazioni che svolgono funzionalità LAN critiche, è suggerita la seguente modalità di aggiornamento degli Agent e del software antivirus:

1. Nel calendario del Server cambiare i task standard di aggiornamento di tutti i componenti ai task di 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 viene descritto nel **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.

Ripristino della password dell'amministratore di Dr.Web Enterprise Security Suite

Se è stata persa la password amministratore per l'accesso al Server Dr.Web, è possibile visualizzarla o modificarla utilizzando l'accesso diretto al database del Server:

a) In caso di utilizzo del database interno, per la visualizzazione e per la modifica della password amministratore viene utilizzata l'utility `drwidbsh` che fa parte del pacchetto Server (v. p. H9.2. Utility di amministrazione del database incorporato).

b) Per il database esterno, usare il client sql appropriato.

> I parametri degli account amministratori vengono conservati nella tabella `admins`.

Esempi di utilizzo dell'utility drwidbsh

1. Avviare l'utility `drwidbsh3` indicando il percorso del file di database:
   - In caso del database interno sotto SO Linux:

```
/opt/drwcs/bin/drwidbsh3 /var/opt/drwcs/database.sqlite
```

   - In caso del database interno sotto SO Windows:

```
"C:\Program Files\DrWeb Server\bin\drwidbsh3" "C:\Program Files\DrWeb Server\var\database.sqlite"
```

> Se viene utilizzato il database incorporato del vecchio formato IntDB, per esempio, se il Server viene aggiornato dalla versione 6, il nome del database predefinito è `dbinternal.dbs`, l'utility di gestione del database è `drwidbsh`.

2. Per visualizzare tutti i dati memorizzati nella tabella `admins`, eseguire il comando:

```
select * from admins;
```

3. Per visualizzare i nomi utenti e le password di tutti gli account amministratori, eseguire il comando:

```
select login,password from admins;
```

4. La schermata sottostante mostra il risultato per la variante quando esiste solo un account con il nome utente `admin` e la password `root`:

```
sqlite> select login,password from admins;
admin|root
sqlite>
```

5. Per modificare la password, usare il comando `update`. Il seguente è un esempio del comando che cambia la password dell'account `admin` a `qwerty`:

```
update admins set password='qwerty' where login='admin';
```

6. Per uscire dall'utility, eseguire il comando:

```
.exit
```

Il funzionamento dell'utility `drwidbsh` è descritto nell'allegato H9.2. Utility di amministrazione del database incorporato.

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.

Quando il software viene installato 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 sulle postazioni.

Resta inteso 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 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 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 con altri programmi di archiviazione. È possibile importare il contenuto del database dal backup nel database operativo di Server tramite il comando `upimportdb` 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** (soltanto per la modalità **Esporta l'intero database**). Tuttavia, in tale caso la copia di backup viene salvata nel formato xml, e per l'importazione è necessario utilizzare il comando `xmlupimportdb`.

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 è indicato nel **Manuale dell'amministratore,** p. Concessione delle licenze.

Se dopo un errore di Server si è conservata una copia di backup dei dati di Server, eseguire la seguente procedura:

1. Selezionare il computer su cui verrà installato un nuovo Server Dr.Web. Isolare questo computer da Agent attivi: scollegarlo dalla rete in cui sono installati Agent 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 precedente e distribuirla ai gruppi corrispondenti, in particolare al gruppo **Everyone**. Il passaggio è obbligatorio se durante l'installazione di Server la chiave di licenza non è stata impostata.
4. Aggiornare da SAM il repository del Server 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, 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, premere la versione corrente di Server o il pulsante **Elenco delle versioni**. Si aprirà la sezione **Aggiornamenti di Server Dr.Web** con un elenco degli aggiornamenti e dei backup di Server disponibili.
   c) Per passare alla nuova versione di Server, selezionare la casella di controllo di fronte all'ultima versione nell'elenco **Tutte le versioni** e premere il pulsante **Salva**.
   d) Attendere che il processo di aggiornamento di Server sia completato.
6. Arrestare il Server.
7. Per ottenere la chiave di cifratura pubblica da un backup della chiave privata, utilizzare l'utility `drwsign` che si trova nella sottodirectory `\bin` della directory di installazione di Server:

   `drwsign extract [-private-key=<chiave_privata>] <chiave_pubblica>`

   Come <*chiave_privata*> e <*chiave_pubblica*> indicare i rispettivi percorsi in cui si trova la chiave privata e inoltre in cui va collocata la chiave pubblica che viene creata.
8. Sostituire i dati critici di Server con i dati ottenuti dal backup:

Sistema operativo	Chiave di cifratura pubblica	File di configurazione
Windows	`webmin\install` nella directory di installazione di Server	`etc` nella directory di installazione di Server
Linux	`/opt/drwcs/webmin/install`	`/var/opt/drwcs/etc`
FreeBSD	`/usr/local/drwcs/webmin/install`	`/var/drwcs/etc`

9. Configurare il database.

   a) Database esterno:

   Non sono richieste ulteriori azioni per la connessione del database a Server (a condizione che è conservato il file di configurazione di Server).

   Se la versione di Server installata dagli ultimi aggiornamenti è più nuova della versione del Server perso, aggiornare il database esterno attraverso il comando `upgradedb`:

   - in caso di SO Windows:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" upgradedb
   ```

   - in caso di SO Linux:

   ```
   /etc/init.d/drwcsd upgradedb
   ```

   - in caso di SO FreeBSD:

   ```
   /usr/local/etc/rc.d/drwcsd upgradedb
   ```

   b) Copia di backup di un database esterno o incorporato:

   Se si utilizza un database esterno, ripulirlo preliminarmente tramite il comando `cleandb` (v. Allegato H4.3).

   Importare il database dal file di backup corrispondente, aggiornando il formato del database alla versione del Server installato, utilizzando il comando `upimportdb`:

   - 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=all upimportdb "<percorso_del_file_di_backup>\database.gz"
   ```

   - in caso di SO Linux:

   ```
   /etc/init.d/drwcsd upimportdb "<percorso_del_file_di_backup>/database.gz"
   ```

   - in caso di SO FreeBSD:

   ```
   /usr/local/etc/rc.d/drwcsd upimportdb
   "<percorso_del_file_di_backup>/database.gz"
   ```

   

   A tutti i file di Server sostituiti è necessario assegnare gli stessi permessi di sistema di quelli selezionati nell'installazione di Server precedente (persa).

   In caso di SO della famiglia UNIX: `rw` per `drwcs:drwcs`.

10. Avviare il Server.
11. Accertarsi che siano integri e aggiornati i dati ottenuti dalla copia di backup del database: impostazioni di Agent, stato dell'albero della rete antivirus ecc.

12. Ripristinare la disponibilità di Server per Agent a seconda del metodo di isolamento di Server selezionato al passaggio 1.

> Se qualche Agent è stato installato dopo la creazione dell'ultimo backup, non potrà connettersi a Server 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.
>
> Dopo che tutte le postazioni si connetteranno al nuovo Server, sostituire queste impostazioni di Server con le impostazioni adottate in conformità con i criteri aziendali.

Ripristino se non è disponibile alcun backup di Server Dr.Web

Se dopo un errore di Server non sono conservate alcune copie di backup, eseguire la seguente procedura:

1. Selezionare il computer su cui verrà installato un nuovo Server Dr.Web. Isolare questo computer da Agent attivi: scollegarlo dalla rete in cui sono installati Agent o modificare temporaneamente l'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 precedente e distribuirla ai gruppi corrispondenti, in particolare al gruppo **Everyone**. Il passaggio è obbligatorio se durante l'installazione di Server la chiave di licenza non è stata impostata.
4. Aggiornare da SAM il repository del Server 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, 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, premere la versione corrente di Server o il pulsante **Elenco delle versioni**. Si aprirà la sezione **Aggiornamenti di Server Dr.Web** con un elenco degli aggiornamenti e dei backup di Server disponibili.
   c) Per passare alla nuova versione di Server, selezionare la casella di controllo di fronte all'ultima versione nell'elenco **Tutte le versioni** e premere il pulsante **Salva**.
   d) Attendere che il processo di aggiornamento di Server sia completato.
6. Modificare le impostazioni di connessione delle postazioni nella configurazione di Server:
   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.

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 e le impostazioni di Server (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 per Agent a seconda del metodo di isolamento di Server selezionato al passaggio 1.
11. Sostituire la chiave di cifratura pubblica su tutte le postazioni della rete che dovranno connettersi al nuovo Server.
    - Se l'auto-protezione è attivata, copiare sulla postazione la chiave pubblica creata durante l'installazione del nuovo Server ed eseguire il seguente comando:

      `es-service.exe -p <chiave>`

      o

      `es-service.exe --addpubkey=<chiave>`

      Come *<chiave>* indicare il percorso della chiave di cifratura pubblica copiata.

      Come risultato, la chiave pubblica verrà copiata nella directory di installazione di Agent. Di default è la directory `%ProgramFiles%\DrWeb` (per maggiori informazioni v. Allegato H3. Agent Dr.Web per Windows®).
    - Se l'auto-protezione è disattivata sulla postazione, è possibile prendere la chiave pubblica creata durante l'installazione del nuovo Server e collocarla nella directory indicata sopra.
12. Dopo che tutte le postazioni si connetteranno al nuovo Server, sostituire le impostazioni di Server configurate al passaggio 5 con le impostazioni adottate in conformità con i criteri aziendali.

Gestione del livello di registrazione del log di Server Dr.Web sotto SO Windows®

È possibile modificare il livello di dettaglio del log di Server sotto SO Windows in uno dei seguenti modi:

1. 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, e inoltre definire alcune altre impostazioni.

Informazioni dettagliate sono riportate in **Manuale amministratore**, sezione Configurazione del Server Dr.Web → Log.

2. Tramite il comando console:

```
drwcsd [<opzioni>] install
```

È possibile impostare qualsiasi livello di dettaglio possibile del log di Server tramite l'opzione `--verbosity`.

Informazioni dettagliate sulle opzioni della riga di comando per la gestione del Server sono ritrovabili nella sezione H4.8. Descrizione delle opzioni.

Un esempio del comando per impostare il livello di registrazione del log **Dettagliato**:

```
drwcsd --daemon "--home=C:\Program Files\DrWeb Server" "--bin-root=C:
\Program Files\DrWeb Server" "--var-root=C:\Program Files\DrWeb
Server\var" --verbosity=ALL --rotate=10,50m install
```

Le altre opzioni sono obbligatorie, in particolare, se sono stati ridefiniti i percorsi standard di installazione del Server e delle sue directory di lavoro.

Dopo aver modificato il livello di registrazione del log, è necessario riavviare il Server:

```
drwcsd restart
```

3. 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 → Gestione del server → Log dettagliato**
o
Programmi → Gestione del server → Log standard

b) **Programmi → Gestione del 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:

- Nel caso in cui sul dispositivo mobile dell'utente sono attivati i fornitori di localizzazione (GPS, reti mobili) e in presenza di un segnale stabile, il rilevamento della posizione viene effettuato tramite i mezzi del dispositivo mobile stesso.
- Nel caso in cui sul dispositivo mobile dell'utente sono disattivati i fornitori 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 delle 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 sull'indirizzo: https://tech.yandex.ru/maps/keys/get/.

  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 i 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.

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 e il certificato SSL `drwcsd-certificate.pem` situato nella directory `etc` della directory di installazione di Server nella directory `\\<macchina_remota>\ADMIN$\Temp`.
2. Il Server 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 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 per l'utente a immettere il login e la 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) restrizioni di accesso su remoto alla risorsa `ADMIN$\Temp` su SO Windows Vista o superiori se non fanno parte di dominio;

   d) nessun owner della directory o permessi dell'utente o del gruppo sulla directory insufficienti.
2. Ci sia l'accesso ai file `drwinst.exe` e `drwcsd.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 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);
		• nome utente sconosciuto o password errata;
		• disattivato il protocollo SMBv1.

	Per installare Agent in remoto, è necessario attivare il protocollo SMBv1 che di default è disattivato in alcune versioni di Windows. Le informazioni su come rilevare, attivare e disattivare i protocolli SMB delle versioni 1, 2 e 3 in Windows e Windows Server sono riportate sul sito Microsoft.	
	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	Impossibile creare una directory temporanea in `ADMIN$/TEMP`, per esempio mancano i

Fase	Errore	Causa
	condivisa <*share*> sulla postazione <*host*>	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.
	Impossibile aprire il file per la lettura <*path*> sul Server Impossibile leggere il file <*path*> sul Server	Nessun file dell'installer sul Server 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 dal timeout sulla postazione <*host*>	L'installer non ha fatto in tempo a installare Agent per il periodo di tempo impostato. Le possibili ragioni: un canale lento tra la

Fase	Errore	Causa
		postazione e il Server, 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 completamento: <*state*>. Codice di errore: <*rc*>.	Errori dell'installer di Agent.

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 necessaria la presenza di un servizio del modulo di filtraggio di base (BFE) avviato. Se questo servizio è assente o danneggiato, l'installazione di Agent Dr.Web per Windows non sarà possibile.

Se un tentativo di installazione di Agent Dr.Web per Windows è terminato con un errore del servizio BFE, eseguire le seguenti operazioni:

1. Il danneggiamento o l'assenza del servizio BFE può indicare la presenza di minacce alla sicurezza della postazione. 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. Ripristinare il servizio BFE sulla postazione. Per farlo, è possibile impiegare l'utility per la risoluzione dei problemi del firewall dall'azienda Microsoft (per i sistemi operativi Windows 7 e superiori).

   L'utility può essere scaricata qui: https://support.microsoft.com/en-us/help/17613/automatically-diagnose-and-fix-problems-with-windows-firewall.
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 verificano dei problemi con l'installazione o il funzionamento dei prodotti della società, prima di chiedere aiuto al reparto di supporto tecnico, provare a trovare una soluzione nei seguenti modi:

- leggere le ultime versioni delle descrizioni e dei manuali sull'indirizzo https://download.drweb.com/doc/;
- leggere la sezione delle domande ricorrenti sull'indirizzo https://support.drweb.com/show_faq/;
- 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:

- compilare il modulo web nella relativa sezione della pagina https://support.drweb.com/;
- chiamare il numero di telefono a Mosca: +7 (495) 789-45-86 o il numero verde per tutta la Russia: 8-800-333-7932.

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