Dr.WEB

Enterprise Security Suite

Anhänge

Dr.Web Enterprise Security Suite
Version 12.0
Anhänge
20.02.2021

Doctor Web, Zentrale in Russland

Postanschrift: 3-ja ul. Jamskogo polja 2-12A, 125124 Moskau, Russland

Website: https://www.drweb.com/

Telefon: +7 495 789 45 87

Detaillierte Kontaktinformationen der regionalen Niederlassungen von Doctor Web finden Sie auf der offiziellen Website des Unternehmens.

Doctor Web

Doctor Web ist ein russischer Anbieter hauseigener IT-Sicherheitslösungen.

Doctor Web bietet effektive Antiviren- und Antispam-Lösungen sowohl für staatliche Behörden und namhafte Großunternehmen als auch für Privatanwender.

Die Dr.Web Antiviren-Software wird seit 1992 permanent weiterentwickelt. Sie entspricht dem heute international geforderten IT-Sicherheitsstandard und weist hervorragende Ergebnisse bei der Erkennung und Beseitigung von Schadsoftware auf.

Zahlreiche Zertifikate und Auszeichnungen sowie breite internationale Präsenz zeugen von einem hohen Maß an Vertrauen in die Unternehmensprodukte.

Wir danken unseren Kunden für ihr Vertrauen in Dr.Web Antivirenlösungen!

Inhaltsverzeichnis

Kapitel 1: Einleitung

Zweck des Dokuments

Die Dokumentation für den Administrator des auf der Enterprise Security Suite basierten Antivirus-Netzwerks enthält sowohl allgemeine als auch detaillierte Informationen über das Sicherheitskonzept und die Vorgehensweise, mit der ein wirksamer und umfassender Virenschutz der IT-Infrastruktur eines Unternehmens durch die Dr.Web Enterprise Security Suite implementiert werden kann.

Die Administratordokumentation besteht aus folgenden Teilen:

1. **Installationsanleitung** (**drweb-12.0-esuite-install-manual-de.pdf**)

   Die Installationsanleitung dient als Einstieg in die weiterführende Dokumentation und gibt eine erste Entscheidungshilfe für einen eventuellen Einsatz der Software. Sie könnte daher für diejenigen Mitarbeiter des Unternehmens nützlich sein, die für den Kaufentscheid und die Implementierung von Sicherheitssystemen zuständig sind.

   In der Installationsanleitung wird beschrieben, wie Sie ein Antivirus-Netzwerk einrichten und seine Komponenten richtig installieren.

2. **Administratorhandbuch** (**drweb-12.0-esuite-admin-manual-de.pdf**)

   Das Administratorhandbuch richtet sich an die *Administratoren des Antivirus-Netzwerks* oder an die Mitarbeiter des Unternehmens, die für die Sicherheit der unternehmensweiten IT-Infrastruktur (Workstations und Server) verantwortlich sind.

   Der Administrator des Antivirus-Netzwerks muss die Systemadministratorrechte haben oder mit dem Administrator des lokalen Netzwerks zusammenarbeiten, umfangreiche Kenntnisse im Bereich IT-Sicherheit und Virenschutz besitzen sowie über Erfahrungen im Umgang mit Dr.Web Antivirenpaketen für alle im lokalen Netzwerk verwendeten Betriebssysteme verfügen.

3. **Anhänge** (**drweb-12.0-esuite-appendices-de.pdf**)

   Die Anhänge liefern technische Informationen zu den Parametern, die zur Konfiguration der Antivirenkomponenten dienen, sowie eine Beschreibung der Syntax und Werte der Befehle, die zur Steuerung dieser Komponenten verwendet werden.

Die gesamte Dokumentation besteht aus den oben genannten Teildokumenten, die untereinander mit zahlreichen Querverweisen verbunden sind. Beachten Sie bitte, dass diese Querverweise nur funktionieren, wenn alle Dokumente die ursprünglichen Dateinamen haben und sich im gleichen Verzeichnis auf dem Rechner befinden.

Zusätzlich werden folgende Handbücher bzw. Anleitungen mitgelifiert:

1. **Anleitung zur Einrichtung des Antivirus-Netzwerks**

   Die Anleitung enthält allgemeine Hinweise zur Installation und Erstkonfiguration der Komponenten des Antivirus-Netzwerks. Weiterführende Informationen zu diesem Thema finden Sie in der Administratordokumentation.

2. **Handbücher zur Verwaltung von Workstations**

   Diese Handbücher liefern hilfreiche Informationen zur zentralen Konfiguration der Antivirensoftware auf Workstations, die der Administrator des Antivirus-Netzwerks über das Dr.Web Sicherheitscenter vornehmen kann.

3. **Benutzerhandbuch**

   In diesen Handbüchern finden Sie wissenswerte Hinweise zur Konfiguration der jeweilige Antivirenlösung von Dr.Web, die direkt an der Workstations vorgenommen werden kann.

4. **Anleitung für Web API**

   Diese Anleitung enthält technische Informationen darüber, wie Sie Dr.Web Enterprise Security Suite in Drittanbieter-Software über Web API integrieren.

5. **Anleitung zur Nutzung der Dr.Web Server- Datenbank**

   Das Dokument beschreibt die innere Struktur der Dr.Web Server-Datenbank und liefert einige Beispiele der praktischen Anwendung der Datenbank.

Alle erwähnten Handbücher bzw. Anleitungen werden mit der Dr.Web Enterprise Security Suite mitgeliefert und können bei Bedarf über das Dr.Web Sicherheitscenter abgerufen werden.

Bevor Sie mit dem Lesen der Dokumente beginnen, stellen Sie sicher, dass Sie jeweils die aktuelle Ausgabe für Ihre Version des Produkts haben. Alle Handbücher werden ständig aktualisiert. Die neuesten Versionen aller Handbücher finden Sie auf der offiziellen Website von Doctor Web unter https://download.drweb.com/doc/.

Kennzeichnungen und Abkürzungen

Symbole und Hervorhebungen

In diesem Handbuch werden folgende Bezeichnungen verwendet.

Symbol/Hervorhebung	Erläuterung
	Wichtige Bemerkung oder wichtiger Hinweis.

Symbol/Hervorhebung	Erläuterung
	Wichtiger Hinweis bzw. Warnung vor potentiell gefährlichen Situationen oder möglichen Fehlern.
Antivirus-Netzwerk	Ein neuer Begriff bzw. Hervorhebung eines Begriffs im Text.
<IP-address>	Platzhalter.
Speichern	Namen von Schaltflächen, Fenstern, Menüpunkten und sonstigen Bestandteilen der Benutzeroberfläche.
STRG	Tastaturbefehle.
`C:\Windows\`	Namen von Dateien und Verzeichnissen, Ausschnitte von Programmcodes.
Anhang A	Querverweise auf andere Seiten im Handbuch oder Links auf Webseiten.

Abkürzungen

Im Handbuch können folgende Abkürzungen bzw. Akronyme ohne nähere Erläuterung auftauchen:

- ACL – Zugriffskontrolllisten (Access Control List)
- CDN – Netzwerk zur Auslieferung von Inhalten (Content Delivery Network)
- DFS – verteiltes Dateisystem (Distributed File System)
- DNS – System der Domänennamen (Domain Name System)
- FQDN – vollständig qualifizierter Domänenname (Fully Qualified Domain Name)
- GUI – grafische Benutzeroberfläche (Graphical User Interface), die GUI-Version steht für eine Version mit der grafischen Benutzeroberfläche
- MIB – Verwaltungsinformationsbasis (Management Information Base)
- MTU – maximale Übertragungseinheit (Maximum Transmission Unit)
- NAP – Network Access Protection
- TTL – Paketlebensdauer (Time To Live)
- UDS – UNIX-Domain-Socket (UNIX Domain Socket)
- DB, DBMS – Datenbank, Datenbankmanagementsystem
- Dr.Web GUS – Dr.Web Globales Update-System
- LAN – lokales Netzwerk
- OS – Betriebssystem
- SW – Software

Kapitel 2: Anhänge

Anhang A. Liste aller unterstützten Betriebssysteme

Für Dr.Web Server

UNIX-basierte Betriebssysteme

Linux, vorausgesetzt dass die Bibliothek `glibc` 2.13 oder höher installiert ist; einschließlich ALT Linux 5.0 oder höher, Astra Linux Special Edition 1.3 oder höher.

FreeBSD 10.3 oder höher.

Windows

- 32-Bit:

Windows 7

Windows 8

Windows 8.1

Windows 10

- 64-Bit:

Windows Server 2008 R2

Windows 7

Windows Server 2012

Windows Server 2012 R2

Windows 8

Windows 8.1

Windows 10

Windows Server 2016

Windows Server 2019

Für Dr.Web Agent und Antivirenpaket

UNIX-basierte Betriebssysteme

Linux für Intel x86/amd64/arm64 auf Basis der Kernel-Version 2.6.37 oder höher, mit PAM und mit der `glibc` 2.13 oder höher.

Damit die Komponente SpIDer Gate richtig funktioniert, muss der Kernel des Betriebssystems mit folgenden Optionen kompiliert werden:

- `CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG`
- `CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS`
- `CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK`

Bei 64-Bit-Versionen muss die Unterstützung für 32-Bit-Anwendungen aktiviert sein.

Die Software wurde unter den folgenden **Linux**-Distributionen (32-Bit und 64-Bit-Versionen) erfolgreich getestet:

Name der Linux-Distribution	Versionen	Erforderliche zusätzliche Bibliotheken für 64-Bit-Betriebssysteme
ALT Linux Server	9	ARM64
ALT Linux Workstation	9	ARM64
Astra Linux Special Edition (Smolensk)	1.4, 1.5, 1.6	x86_64
CentOS	6.9, 7.4	x86, x86_64, ARM64
Debian	7.11, 8.10, 9.3	x86_64
Fedora	27, 28, 29	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, 18.04	x86_64, ARM64

Unter Systemen mit der ARM64-Architektur wurden die Distributionen Ubuntu 18.04, CentOS 7.7, ALT Linux Workstation 9 und ALT Linux Server 9 auf Kompatibilität getestet.

Die Kompatibilität sonstiger konformer **Linux**-Distributionen wurde nicht überprüft. Trotzdem kann davon ausgegangen werden, dass sie höchstwahrscheinlich kompatibel sind. Falls Sie Kompatibilitätsprobleme mit Ihrer Distribution vermuten, wenden Sie sich an den technischen Support unter https://support.drweb.com.

Wenn Sie in Dr.Web Enterprise Security Suite einige Komponenten der Version 6 verwenden wollen, müssen Sie zunächst die Systemanforderungen konsultieren, die Sie in der Dokumentation zur jeweiligen Komponente finden.

Windows

- 32-Bit:

Windows XP mit SP2

Windows Server 2003 mit SP1

Windows Vista mit SP2

Windows Server 2008 mit SP2

Windows 7 mit SP1

Windows 8

Windows 8.1

Windows 10

- 64-Bit:

Windows Vista mit SP2 oder höher

Windows Server 2008 mit SP2

Windows Server 2008 R2 mit SP1

Windows 7 mit SP1

Windows Server 2012

Windows Server 2012 R2

Windows 8

Windows 8.1

Windows 10

Windows Server 2016

Windows Server 2019

Da Microsoft den Hash-Algorithmus SHA-1 nicht mehr unterstützt, stellen Sie vor der Installation des Dr.Web Agents auf Rechnern mit Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2 sicher, dass das Betriebssystem den Hash-Algorithmus SHA-256 unterstützt. Installieren Sie alle notwendigen Updates vom Microsoft Update Service. Detaillierte Informationen zu notwendigen Updates finden Sie auf der Website von Doctor Web.

Remote-Installation von Dr.Web Agents ist nicht möglich für Workstations unter Starter- und Home-Editionen von Windows.

macOS

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)

macOS 10.14 (Mojave)

macOS Server 10.14 (Mojave)

macOS 10.15 (Catalina)

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

Android 9.0

Android 10.0

Anhang B. Einstellungen des DBMS. Parameter der DBMS-spezifischen Treiber

Zur Anzeige der Struktur der Datenbank des Dr.Web Servers können Sie das SQL-Skript `init.sql` verwenden, das sich im Unterverzeichnis `etc` vom Installationsverzeichnis des Dr.Web Servers befindet.

Als Datenbank des Dr.Web Servers können folgende DBMS eingesetzt werden:

- Eingebettetes DBMS
- Externes DBMS

Eingebettetes DBMS

Beim Konfigurieren des Zugriffs auf ein eingebettetes DBMS werden zur Speicherung und Verarbeitung von Daten die in der Tabelle **B-1** aufgeführten Parameter verwendet.

Tabelle B-1: Eingebettetes DBMS

Name	Standardwert	Erläuterung
DBFILE	database.sqlite	Pfad zur Datenbankdatei
CACHESIZE	2000	Cachegröße der Datenbank in Seiten
SYNCHRONOUS	FULL	Schreibmodus beim Speichern von Änderungen auf dem Datenträger: • FULL – vollständig synchrones Schreiben auf den Datenträger • NORMAL – synchrones Schreiben kritischer Daten • OFF – asynchrones Schreiben

Als integriertes DBMS wird das vom Server ab Version 10 unterstützte eingebettete Datenbanksystem SQLite3 bereitgestellt.

Externes DBMS

Als externe Datenbank des Dr.Web Servers können folgende DBMS eingesetzt werden:

- Oracle DBMS. Einstellungen dieses DBMS werden im Anhang B2. Oracle-Datenbanktreiber konfigurieren detailliert beschrieben.
- PostgreSQL DBMS. Einstellungen dieses DBMS werden im Anhang B3. Verwendung des PostgreSQL-DBMS detailliert beschrieben.

- Microsoft SQL Server/Microsoft SQL Server Express. Für den Zugriff auf die DBMS-Daten können ODBC-Treiber verwendet werden (Konfiguration der Einstellungen des ODBC-Treibers für Windows wird im Anhang B1. ODBC-Treiber konfigurieren beschrieben).

Obwohl Microsoft SQL Server 2008 und neuere Versionen immer noch unterstützt werden, empfiehlt es sich, Microsoft SQL Server 2014 oder höher zu verwenden.

Microsoft SQL Server Express Datenbank ist generell nicht empfehlenswert für ein Antivirus-Netzwerk mit mehr als 100 Workstations.

Wenn Sie Microsoft SQL Server als externe Datenbank für einen unter einem UNIX-basierten Betriebssystem laufenden Server verwenden wollen, müssen Sie berücksichtigen, dass keine ordnungsgemäße Verbindung über FreeTDS-ODBC-Treiber garantiert werden kann.

Wenn Warnungen oder Fehler beim Betrieb des Dr.Web Servers, der auf Microsoft SQL Server über ODBC zugreift, auftreten, stellen Sie sicher, dass Sie jeweils die aktuelle Version des DBMS verwenden.

Auf der Website von Microsoft unter https://docs.microsoft.com/en-us/troubleshoot/sql/general/determine-version-edition-update-level erfahren Sie, wie Sie die Updateebene von SQL Server ermitteln und ob neue Updates für Ihre Version zur Verfügung stehen.

Um bei der Verwendung von Microsoft SQL Server mit der Standard-Transaktionsisolationsstufe (READ COMMITTED) die Zahl von Sperren zu minimieren, empfiehlt es sich, den Parameter READ_COMMITTED_SNAPSHOT zu aktivieren. Führen Sie hierzu den folgenden Befehl aus:

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

Die Voraussetzungen hierfür sind, dass der Befehl im impliziten Transaktionsmodus (implicit) ausgeführt wird und es nur eine einzige Serververbindung besteht.

Empfehlungen zur Auswahl einer optimalen Datenbank

Damit die eingebettete Datenbank ihre Aufgaben funktionsgerecht bewältigt, sollten nicht mehr als 200–300 Workstations mit dem Server verbunden sein. Wenn der Rechner, auf dem Dr.Web Server installiert ist, über ausreichend leistungsfähige Hardware verfügt und einer geringen Auslastung durch andere Prozesse ausgesetzt ist, können bis zu 1000 Workstations verbunden werden.

Anderenfalls sollte eine externe Datenbank verwendet werden.

Beim Einsatz einer externen Datenbank und wenn mehr als 10000 Workstations mit dem Server verbunden werden müssen, ist es empfehlenswert, die folgenden minimalen Anforderungen einzuhalten:

- Prozessor mit Taktfrequenz von 3 GHz
- Mindestens 4 GB Arbeitsspeicher für den Dr.Web Server und mindestens 8 GB Arbeitsspeicher für den Datenbankserver
- UNIX-basiertes Betriebssystem

Bei der Auswahl zwischen einer eingebetteten und einer externen Datenbank müssen Sie einige DBMS-spezifische Besonderheiten berücksichtigen:

- In großen Antivirus-Netzwerken (mit mehr als 200–300 Workstations) empfiehlt es sich, eine externe DB zu verwenden, da eine externe DB stabiler im Vergleich zu einer eingebetteten DB ist.
- Beim Einsatz einer eingebetteten DB sind keine weiteren Komponenten erforderlich. Diese ist für die gängigsten Anwendungsfälle empfohlen.
- Um eine eingebettete Datenbank zu bedienen, braucht der Administrator keine Kenntnisse über Datenbankverwaltung. Diese ist daher eine optimale Lösung für kleine und mittelgroße Antivirus-Netzwerke.
- Der Einsatz einer externen Datenbank ist dann sinnvoll, wenn ein direkter Zugriff auf die Datenbank erforderlich ist. Für den Zugriff auf die Datenbanken können standardisierte APIs, wie etwa OLE DB, ADO.NET oder ODBC, verwendet werden.

B1. ODBC-Treiber konfigurieren

Beim Konfigurieren des Zugriffs auf ein externes DBMS zur Speicherung und Verarbeitung von Daten werden die in der Tabelle **B-2** aufgeführten Parameter verwendet (die angegebenen Werte sind exemplarisch).

Tabelle B-2: Parameter für ODBC-Verbindung

Name	Wert	Erläuterung
`DSN`	`drwcs`	Name des Datensatzes
`USER`	`drwcs`	Benutzername
`PASS`	`fUqRbrmlvI`	Passwort
`TRANSACTION`	`DEFAULT`	Mögliche Werte des Parameters `TRANSACTION`: • `SERIALIZABLE` • `READ_UNCOMMITTED` • `READ_COMMITTED` • `REPEATABLE_READ`

Name	Wert	Erläuterung
		• `DEFAULT` Der Standardwert `DEFAULT` gibt an, dass der Standardwert des SQL-Servers verwendet werden soll. Mehr Details zu Transaktionsisolationsstufen finden Sie in der Dokumentation des jeweiligen DBMS.

Um eventuelle Probleme mit der Codierung zu vermeiden, müssen Sie die folgenden Optionen des ODBC-Treibers deaktivieren:

- **Ländereinstellungen bei der Anzeige von Währungs-, Zahlen-, Datums- und Zeitangaben verwenden**. Die Option kann Fehler beim Formatieren von Datums- und Zeitangaben verursachen.
- **Konvertierung für Zeichendaten ausführen**. Die Aktivierung dieser Option kann dazu führen, dass Zeichen für datenbankspezifische Parameter nicht richtig im Verwaltungscenter angezeigt werden. Diese Option bestimmt die Abhängigkeit der Zeichenanzeige vom Sprachparameter für nicht Unicode-fähige Programme.

Beim Erstellen einer neuen Datenbank im Microsoft SQL-DBMS müssen Sie festlegen, dass die Sortierregeln Groß- und Kleinschreibung (Unterscheidung nach Groß-/Kleinschreibung, Kürzel `_CS`) und Akzentzeichen (Unterscheidung nach Akzent, Kürzel `_AS`) berücksichtigen.

Die Datenbank selbst wird auf dem SQL-Server mit den oben genannten Parametern im Voraus erstellt.

Die Parameter des ODBC-Treibers müssen auch für den Rechner konfiguriert werden, auf dem der Dr.Web Server installiert ist.

Informationen zur Konfiguration des ODBC-Treibers unter einem UNIX-artigen Betriebssystem finden Sie unter http://www.unixodbc.org/ im Bereich **Manuals**.

ODBC-Treiber unter Windows konfigurieren

So konfigurieren Sie die Parameter des ODBC-Treibers

1. Wählen Sie in der **Systemsteuerung** von Windows den Punkt **Verwaltung**. Doppelklicken Sie im geöffneten Fenster auf das Symbol **Datenquellen (ODBC)**. Das Fenster **ODBC-Datenquellen-Administrator** öffnet sich. Wechseln Sie zur Registerkarte **System-DSN**.
2. Klicken Sie auf **Hinzufügen**. Das Fenster für die Auswahl des Treibers erscheint.

3. Wählen Sie in der Liste den Punkt aus, der dem ODBC-Treiber der gewünschten Datenbank entspricht. Klicken Sie dann auf **Fertig stellen**. Das erste Fenster für die Einstellung des Zugriffs auf den Datenbankserver öffnet sich.

   Bei der Verwendung einer externen Datenbank müssen Sie die aktuelle Version des mitgelieferten ODBC-Treibers installieren. Der mit Windows gelieferte ODBC-Treiber ist nicht empfehlenswert. Dazu zählen nicht die Datenbanken, die von Microsoft ohne ODBC-Treiber geliefert werden.

4. Geben Sie die Parameter für den Zugriff auf die Datenquelle an, die mit den in den Einstellungen des Dr.Web Servers festgelegten Parametern übereinstimmen. Wenn sich der Datenbankserver und der Dr.Web Server nicht auf dem gleichen Rechner befinden, geben Sie im Eingabefeld **Server** die IP-Adresse oder den Namen des Datenbank-Servers an. Klicken Sie auf **Weiter**.
5. Wählen Sie die Option **Mit SQL Server-Authentifizierung anhand des vom Benutzer eingegebenen Benutzernamens und Kennworts** aus und legen Sie die Anmeldedaten für den Zugriff auf die Datenbank fest. Klicken Sie auf **Weiter**.
6. Wählen Sie aus der Dropdown-Liste **Die Standarddatenbank ändern auf** die vom Dr.Web Server verwendete Datenbank. Stellen Sie sicher, dass Sie den Namen der Datenbank des Servers und nicht den Wert **Default** angegeben haben.

   Stellen Sie sicher, dass die folgenden Optionen aktiviert sind: **ANSI-Anführungszeichen verwenden** und **ANSI-Nullen, -Leerstellen und -Warnungen verwenden**. Klicken Sie dann auf **Weiter**.

   Falls bei der Einstellung des ODBC-Treibers die Sprache von Systemmeldungen des SQL-Servers geändert werden kann, wählen Sie Englisch aus.

7. Wenn Sie mit der Konfiguration fertig sind, klicken Sie auf **Fertig stellen**. Im nächsten Fenster werden alle von Ihnen konfigurierten Parameter angezeigt.
8. Um sicherzustellen, dass Ihre Eingaben richtig sind, klicken Sie auf **Datenquelle testen**. Nach erfolgreicher Prüfung erscheint eine entsprechende Meldung, klicken Sie dann auf **OK**.

B2. Oracle-Datenbanktreiber konfigurieren

Allgemeine Beschreibung

Oracle Database (bzw. Oracle DBMS) ist ein objektrelationales Datenbankmanagementsystem. Oracle kann als externe Datenbank für Dr.Web Enterprise Security Suite eingesetzt werden.

Dr.Web Server kann das Oracle DBMS als externe Datenbank auf allen Plattformen (außer FreeBSD) verwenden (s. dazu Installation und unterstützte Versionen).

So nutzen Sie das Oracle-DBMS

1. Installieren Sie eine Oracle-Instanz mit dem Zeichensatz `AL32UTF8`. Sie können aber auch die vorhandene Instanz mit dem angegebenen Zeichensatz verwenden.
2. Richten Sie den Datenbanktreiber entsprechend ein, um die gewünschte externe Datenbank einsetzen zu können. Das gelingt Ihnen mithilfe der Konfigurationsdatei oder über das Verwaltungscenter: Menü **Dr.Web Server-Konfiguration**, Registerkarte **Datenbank**.

Wenn Sie als externe Datenbank eine Oracle-Datenbank, auf die über ODBC-Verbindung zugegriffen werden soll, verwenden wollen, muss bei der Installation (Aktualisierung) des Servers in den Einstellungen des Installationsprogramms die Installation des eingebetteten Clients für das Oracle-DBMS (im Bereich **Datenbankunterstützung** → **Oracle-Datenbanktreiber**) deaktiviert werden.

Anderenfalls kann auf die Oracle-Datenbank über die ODBC-Verbindung aufgrund eventueller Probleme mit den inkompatiblen Bibliotheken nicht zugegriffen werden.

Die vordefinierten Administratoren, die Benutzer SYS und SYSTEM, bzw. Benutzer mit SYSDBA- und SYSOPER-Systemprivilegien dürfen nicht auf die Oracle-Datenbank zugreifen.

Installation und unterstützte Versionen

Um eine Oracle Datenbank als externe Datenbank verwenden zu können, müssen Sie eine Oracle-Instanz mit dem Zeichensatz `AL32UTF8` installieren (`CHARACTER SET AL32UTF8 / NATIONAL CHARACTER SET AL16UTF16`). Das kann über die folgenden Wege geschehen:

1. Mithilfe des Oracle-Installationsprogramms (verwenden Sie die erweiterte Installation und Konfiguration).
2. Über den SQL-Befehl `CREATE DATABASE`.

Detaillierte Informationen zur Erstellung und Konfiguration der Datenbank finden Sie in der Dokumentation für Oracle DBMS.

Wenn Sie einen vom oben angegebenen Zeichensatz abweichenden Zeichensatz festgelegt haben, werden nationale Sonderzeichen nicht richtig angezeigt.

Der Client für den Zugriff auf die Datenbank (Oracle Instant Client) ist im Installationspaket von Dr.Web Enterprise Security Suite enthalten.

Alle von Oracle unterstützten Plattformen finden Sie auf der Webseite des Herstellers.

Alle von Oracle Client unterstützten Plattformen finden Sie auf der Webseite des Herstellers.

Dr.Web Enterprise Security Suite unterstützt das DBMS Oracle Version 11 und höher.

Beachten Sie, dass der Einsatz einer externen Oracle-Datenbank bestimmte Anforderungen an den Dr.Web Server stellt (s. dazu im Dokument **Installationsanleitung** den Abschnitt Systemanforderungen).

Parameter

Beim Konfigurieren des Zugriffs auf das Oracle-DBMS werden die in der Tabelle **B-3** aufgeführten Parameter verwendet.

Tabelle B-3: Parameter des Oracle-DBMS

Parameter	Erläuterung
`drworacle`	Treibername
`User`	Name des Datenbankbenutzers (obligatorisch)
`Password`	Benutzerpasswort (obligatorisch)
`ConnectionString`	Verbindungszeichenfolge für die Datenbankverbindung (obligatorisch)
`Prefetch-rows`	Anzahl der Zeilen zum Vorabruf bei einer Datenbankabfrage
`Prefetch-mem`	Größe des zugeordneten Speichers für den Vorabruf der Zeilen bei einer Datenbankabfrage

Die Verbindungszeichenfolge für das Oracle DBMS hat das folgende Format:

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

wobei:

- *<host>* – die IP-Adresse bzw. der Name des Oracle-Servers.
- *<port>* – der Port, an dem der Server lauscht.
- *<service name>* – der Name der Datenbank, mit der die Verbindung hergestellt werden soll.

Beispiel:

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

wobei:

- `myserver111` – der Name des Oracle-Servers.
- `1521` – der Port, an dem der Server lauscht.
- `bjava21` – der Name der Datenbank, mit der die Verbindung hergestellt werden soll.

Oracle-Datenbanktreiber konfigurieren

Beim Einsatz des Oracle-DBMS müssen Sie die Definition und die Einstellungen des Datenbanktreibers über einen der folgenden Wege ändern:

- Wählen Sie im Verwaltungscenter den Bereich **Administration** → dann den Punkt **Dr.Web Server-Konfiguration** des Verwaltungsmenüs → wechseln Sie dann zur Registerkarte **Datenbank** → und wählen Sie in der Dropdown-Liste **Datenbank** den Typ **Oracle** aus. Legen Sie die Einstellungen wie oben beschrieben fest.
- Mithilfe der Konfigurationsdatei des Servers.

B3. Verwendung des PostgreSQL-DBMS

Allgemeine Beschreibung

PostgreSQL ist ein objektrelationales Datenbankmanagementsystem. PostgreSQL ist eine kostenlose Alternative zu anderen Datenbankmanagementsystemen wie Oracle, Microsoft SQL usw., die in größeren Antivirus-Netzwerken als externe Datenbank für Dr.Web Enterprise Security Suite eingesetzt werden kann.

So nutzen Sie PostgreSQL als externe Datenbank

1. Installieren Sie den PostgreSQL- oder Postgres Pro-Server.
2. Richten Sie den Dr.Web Server für die Verwendung der gewünschten externen Datenbank ein. Verwenden Sie dazu die Konfigurationsdatei oder das Verwaltungscenter: Wechseln Sie hierzu zu **Dr.Web Server-Konfiguration** und dann zu **Datenbank**.

Beim Einsatz des PostgreSQL-DBMS kann die Autorisierung nur über trust, password und MD5 erfolgen.

Installation und unterstützte Versionen

1. Laden Sie die neueste Version von PostgreSQL (den PostgreSQL-Server und, falls notwendig, den entsprechenden ODBC-Treiber) herunter oder nutzen Sie Version **8.4** oder höher oder (im Fall Postgres Pro) Version 11.4.1 oder höher.
2. Erstellen Sie eine PostgreSQL-Datenbank über einen der folgenden Wege:
   a) Über die grafische Oberfläche von `pgAdmin`.
   b) Über den SQL-Befehl `CREATE DATABASE`.

In der Datenbank muss UTF-8 als Zeichensatz eingestellt sein.

Umstieg auf eine externe Datenbank wird unter DBMS von Dr.Web Enterprise Security Suite wechseln detailliert beschrieben.

Beachten Sie, dass der Einsatz einer externen PostgreSQL-Datenbank bestimmte Anforderungen an den Dr.Web Server stellt (s. dazu im Dokument **Installationsanleitung** den Abschnitt Systemanforderungen).

Parameter

Beim Konfigurieren des Zugriffs auf das PostgreSQL-DBMS werden die in der Tabelle **B-4** aufgeführten Parameter verwendet.

Tabelle B-4: PostgreSQL

Name	Standardwert	Erläuterung
`host`	*<Lokaler UNIX-Socket>*	Host des PostgreSQL-Servers
`port`		Der Portnummer des PostgreSQL-Servers oder die Namenserweiterung der Datei des Sockets
`dbname`	`drwcs`	Datenbankname
`user`	`drwcs`	Benutzername
`password`	`drwcs`	Passwort
`options`		Debug- und Ablaufverfolgungsoptionen für das Senden an den Server
`requiressl`		• 1 gibt an, dass SSL-Verbindungsanforderungen gesendet werden • bei 0 werden keine SSL-Verbindungsanforderungen gesendet
`temp_tablespaces`		Der Namespace für temporäre Tabellen
`default_transaction_isolation`		Transaktionsisolationsstufe (mehr dazu finden Sie in der Dokumentation für PostgreSQL)

Technische Informationen finden Sie unter https://www.postgresql.org/docs/.

Interaktion des Dr.Web Servers mit einer PostgreSQL-Datenbank über UDS

Wenn der Dr.Web Server und die PostgreSQL-Datenbank auf einem Rechner installiert werden, ist zwischen ihnen eine Interaktion über UDS (den UNIX-Domänensocket) möglich.

So konfigurieren Sie die UDS-Verbindung

1. Geben Sie in der Konfigurationsdatei der PostgreSQL-Datenbank `postgresql.conf` das folgende Verzeichnis für den UDS an:

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

2. Starten Sie das PostgreSQL-DBMS neu.

PostgreSQL-Datenbank konfigurieren

Um Ihre PostgreSQL-Datenbank für bessere Leistung zu optimieren, sollten Sie Hinweise und Tipps zum Betrieb der Datenbank beachten, die offiziellen Handbüchern zu PostgreSQL aufgeführt sind.

Wenn es sich um recht große Datenbanken handelt und es ausreichend Rechnerleistung zur Verfügung steht, lohnt es sich, folgende Parameter in der Konfigurationsdatei `postgresql.conf` wie folgt anzupassen:

Minimale Konfiguration:

```
shared_buffers = 256MB

temp_buffers = 64MB

work_mem = 16MB
```

Erweiterte Konfiguration:

```
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
```

Deaktivierung des synchronen Schreibens durch die Einstellung `fsync = off` erhöht zwar wesentlich die Datenbankleistung, doch kann dazu führen, dass bei Stromausfällen oder Systemabstürzen möglicherweise auch alle Daten verloren gehen. Die

Deaktivierung des Parameters `fsync` ist also nur sinnvoll, wenn die Daten einfach (beispielsweise aus einer Sicherungskopie) wiederbeschafft werden können.

Die Einstellung des Parameters `max_locks_per_transaction` ist sinnvoll, um die stabile Funktion der Datenbank sicherzustellen, wenn viele gleichzeitige Anfragen an die Datenbank gestellt werden, beispielsweise bei der Aktualisierung auf eine neue Version.

B4. Verwendung des MySQL-DBMS

Allgemeine Beschreibung

MySQL ist ein freies und plattformübergreifendes relationales Datenbankmanagementsystem. MySQL kann als externe Datenbank für Dr.Web Enterprise Security Suite eingesetzt werden.

So richten Sie MySQL als externe Datenbank ein

1. Installieren Sie den MySQL-Server.
2. Richten Sie den Dr.Web Server für die Verwendung der gewünschten externen Datenbank ein. Verwenden Sie dazu die Konfigurationsdatei oder das Verwaltungscenter: Wechseln Sie hierzu zu **Dr.Web Server-Konfiguration** und dann zu **Datenbank**.

Installation und unterstützte Versionen

Dr.Web Enterprise Security Suite unterstützt folgende Versionen des MySQL-DBMS:

- MySQL 5.5.14 bis 5.7 sowie 8.0.12 und höher
- MariaDB 10.0, 10.1, 10.2

Nach der Installation des DBMS und vor dem Erstellen der neuen Datenbank müssen Sie folgende Einstellungen in der Konfigurationsdatei des DBMS festlegen (Einzelheiten entnehmen Sie der Dokumentation zu Ihrem DBMS):

Für MySQL Version 5.X:

```
[mysqld]

innodb_large_prefix = true

innodb_file_format = barracuda

innodb_file_per_table = true

max_allowed_packet = 64M
```

Für MySQL Version 8.X:

```
[mysqld]

innodb_file_per_table = true

max_allowed_packet = 64M
```

Bei MariaDB bis 10.2.4 muss die Konfigurationsdatei den folgenden Eintrag enthalten:

```
binlog_format = mixed
```

Anhang C. Authentifizierung von Administratoren

Allgemeine Informationen zur Authentifizierung von Administratoren am Dr.Web Server finden Sie im **Administratorhandbuch** unter Administrator-Authentifizierung.

C1. Authentifizierung über Active Directory

Bei der Verwendung von Active Directory können Sie nur die Authentifizierungsmethode aktivieren bzw. deaktivieren und die Reihenfolge von Authentifizierern ändern: Dazu dienen die Tags `<enabled/>` und `<order/>` in der Konfigurationsdatei `auth-ads.conf`.

Funktionsweise:

1. Der Administrator legt den Benutzernamen und das Passwort in einem der folgenden Formate fest:
   - `username`
   - `domain\username`
   - `username@domain`
   - LDAP DN des Benutzers
2. Der Server wird mit diesem Namen und Passwort auf dem Standarddomänencontroller registriert (bzw. auf dem Domänencontroller für die Domäne, die im Benutzernamen angegeben wurde).
3. Wenn die Registrierung fehlgeschlagen ist, wird der nächste Authentifizierungsmechanismus verwendet.
4. LDAP DN des registrierten Benutzers wird ermittelt.
5. Beim Objekt mit dem ermittelten DN wird das Attribut `DrWeb_Admin` gelesen. Wenn es den Wert `FALSE` hat, wird davon ausgegangen, dass die Authentifizierung fehlgeschlagen ist. In diesem Fall wird der nächste Authentifizierungsmechanismus verwendet.
6. Wenn in diesem Schritt einige Attribute nicht ermittelt wurden, werden sie in den Gruppen, denen der Benutzer angehört, gesucht. Bei jeder Gruppe werden ihre übergeordneten Gruppen durchsucht (Suche in die Tiefe).

Bei einem Fehler wird es mit dem nächsten Authentifizierungsmechanismus versucht.

Das Dienstprogramm `drweb-12.00.0-<Build>-esuite-modify-ad-schema-<Betriebssystem-Version>.exe` (gehört zum Distributionsumfang des Servers) erstellt eine neue Objektklasse `DrWebEnterpriseUser` für Active Directory und beschreibt neue Attribute für diese Klasse.

Attribute haben die folgenden OIDs in der Enterprise-Umgebung:

```
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"
```

Die Eigenschaften der Benutzer von Active Directory werden manuell auf dem Server von Active Directory bearbeitet (mehr dazu finden Sie im Dokument **Administratorhandbuch** unter Administrator-Authentifizierung).

Rechte werden den Administratoren nach dem allgemeinen Vererbungsprinzip in der Hierarchie der Gruppen, zu denen der Administrator gehört, zugewiesen.

C2. Authentifizierung über LDAP

Die Einstellungen werden in der Konfigurationsdatei `auth-ldap.conf` gespeichert.

Die wichtigsten Tags der Konfigurationsdatei:

- `<enabled/>` und `<order/>` sind identisch mit den oben beschriebenen Active Directory-Einstellungen.
- `<server/>` legt die Adresse des LDAP-Servers fest. Mehrere Tags `<server/>` mit den Adressen unterschiedlicher LDAP-Server können gleichzeitig angegeben werden. In diesem Fall wird eine Liste der Server angelegt, auf denen die Authentifizierung möglich ist. Als erste in die Liste sollte die Adresse des zuverlässigsten Servers (Hauptservers) eingetragen werden, der am stärksten belastet werden soll. Nach dieser Adresse sollten die Adressen der Backup-Server stehen. Wenn der Administrator eine Verbindung herstellt, wird der erste der verfügbaren LDAP-Server verwendet. Wenn der erste Server nicht erreichbar ist, wird versucht, den nächsten alternativen Server anzusprechen: Die LDAP-Server werden also in der in der Konfigurationsdatei angegebenen Reihenfolge ausprobiert.
- `<user-dn/>` definiert die Regeln für die Übersetzung von Namen in DN (Distinguished Name) mithilfe von DOS-artigen Masken.

  Im Tag `<user-dn/>` können einige Platzhalterzeichen verwendet werden:

  - `*` ersetzt eine Folge beliebiger Zeichen außer `.` `,` `=` `@` `\` und Leerzeichen.
  - `#` ersetzt eine Folge beliebiger Zeichen.

- <user-dn-expr/> definiert die Regeln für die Übersetzung von Namen in DN mithilfe von regulären Ausdrücken.

  So sieht eine gleiche Regel in unterschiedlichen Varianten aus:

  ```
  <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 definieren, an welcher Stelle in der Vorlage die Werte *, # oder Ausdrücke in Klammern ersetzt werden sollen.

  Wenn die Zeichenkette login@example.com als Benutzername angegeben wurde, so sieht der DN nach der Übersetzung wie folgt aus: "CN=login,DC=example,DC=com".

- <user-dn-extension-enabled/> erlaubt die Ausführung des LUA-Skripts ldap-user-dn-translate.ds (aus dem Verzeichnis extensions) zur Übersetzung des Benutzernamens in DN. Dieses Skript wird erst dann ausgeführt, wenn in den Regeln user-dn, user-dn-expr keine passende Regel gefunden wird. Das Skript hat nur einen Parameter, und zwar den angegebenen Benutzernamen. Das Skript gibt die Zeile zurück, die einen DN oder nichts enthält. Wenn keine Regel gefunden wird oder das Skript deaktiviert ist bzw. nichts zurückgegeben hat, wird der angegebene Benutzername verwendet, wie er ist.

- Das Attribut eines LDAP-Objekts für den konvertierten DN und dessen mögliche Werte können durch das folgende Tag neu definiert werden (angegeben sind jeweils die Standardwerte):

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

  Als Werte der Parameter true-value/false-value müssen reguläre Ausdrücke festgelegt werden.

- Wenn einige Werte der Administrator-Attribute nicht definiert sind und das Tag <group-reference-attribute-name value="memberOf"/> in der Konfigurationsdatei festgelegt ist, gilt der Wert des Attributs memberOf als Liste von DN-Gruppen, denen der Administrator angehört. Die Suche nach erforderlichen Attributen in diesen Gruppen erfolgt ebenso wie die Suche bei der Verwendung von Active Directory.

C3. Authentifizierung über LDAP/AD

Konfigurationsdatei

Die Einstellungen werden in der Konfigurationsdatei auth-ldap-rfc4515.conf gespeichert.

Ihnen stehen auch folgende Konfigurationsdateien mit den Mustereinstellungen zur Verfügung:

- auth-ldap-rfc4515-check-group.conf. Diese Datei ist ein Muster der Konfigurationsdatei für vereinfachte externe LDAP-Autorisierung von Administratoren, bei der überprüft wird, in welchen Active Directory-Gruppen sie Mitglied sind.
- auth-ldap-rfc4515-check-group-novar.conf. Diese Datei ist ein Muster der Konfigurationsdatei für vereinfachte externe LDAP-Autorisierung von Administratoren, bei der reguläre Ausdrücke verwendet werden und überprüft wird, in welchen Active Directory-Gruppen sie Mitglied sind.

- `auth-ldap-rfc4515-simple-login.conf`. Diese Datei ist ein Muster der Konfigurationsdatei für vereinfachte externe LDAP-Autorisierung von Administratoren.

Die wichtigsten Tags der Konfigurationsdatei auth-ldap-rfc4515.conf:

- `<server />` – Definition des LDAP-Servers.

Attribut	Erläuterung	Standardwert
`base-dn`	DN des Objekts, relativ zu dem die Suche stattfindet.	Der Wert des Attributs `rootDomainNamingContext` des Objekts `Root DSE`
`cacertfile`	Stammzertifikatdatei (nur unter UNIX-artigen Betriebssystemen).	–
`host`	Adresse des LDAP-Servers.	• Domänencontroller für den Server unter Windows. • `127.0.0.1` für den Server unter UNIX-basierten Betriebssystemen. • Mehrere Tags `<server />` mit den Adressen unterschiedlicher LDAP-Server können gleichzeitig angegeben werden. Als erste in die Liste sollte die Adresse des Hauptservers eingetragen werden, der am stärksten belastet werden soll. Wenn der erste Server nicht erreichbar ist, wird versucht, den nächsten alternativen Server anzusprechen: Die Server werden also in der angegebenen Reihenfolge ausprobiert.
`scope`	Suchbereich. Zulässige Werte: • `sub-tree` – gesamter Bereich unterhalb des Basis-DN • `one-level` – direkt dem Basis-DN untergeordnete Einträge • `base` – Basis-DN	`sub-tree`
`tls`	TLS zur Verbindung mit LDAP verwenden.	`no`
`ssl`	LDAPS-Protokoll beim Herstellen der Verbindung mit LDAP verwenden.	`no`

- `<set />` – Variablen durch die LDAP-Suche festlegen.

Attribut	Erläuterung	Standardwert
attribute	Attributname, dessen Wert der Variablen zugewiesen wird. Das Attribut darf nicht weggelassen werden.	–
filter	Suchfilter in LDAP nach RFC 4515.	–
scope	Suchbereich. Zulässige Werte: • sub-tree – gesamter Bereich unterhalb des Basis-DN • one-level – direkt dem Basis-DN untergeordnete Einträge • base – Basis-DN	sub-tree
search	DN des Objekts, relativ zu dem die Suche stattfindet.	Wenn fehlt, wird der base-dn des Tags <server /> verwendet
variable	Variablenname. Der Variablenname muss mit einem Buchstaben beginnen und darf nur Buchstaben und Zahlen enthalten. Das Attribut darf nicht weggelassen werden.	–

Variablen können in den Werten des Attributs add der Tags <mask /> und <expr />, im Wert des Attributs value des Tags <filter /> als \varname und im Wert des Attributs search des Tags <set />. Die zulässige Rekursionstiefe für Variablen beträgt 16.

Wenn die Suche mehrere Ergebnisse zurückgibt, wird nur das erste Ergebnis verwendet.

- <mask /> – Benutzernamenvorlagen.

Attribut	Erläuterung
add	Zum Suchfilter hinzuzufügende Zeile, wenn die Suche mit dem UND-Operatoren und Ersetzen der Elemente erfolgt.
user	Mit DOS-kompatiblen Metazeichen * und # angegebene Benutzernamenmaske. Das Attribut kann nicht weggelassen werden.

Beispiel:

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

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

\1 und \2 sind die Links auf die übereinstimmenden Masken im Attribut user.

- <expr /> – auf regulären Ausdrücken basierende Benutzernamenvorlagen (die Attribute sind identisch mit den Attributen des Tags <mask />).

  Beispiel:

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

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

Übereinstimmung der Masken mit den regulären Ausdrücken:

Maske	Regulärer Ausdruck
*	.*
#	[^.,=@\s\\]+

- `<filter />` – LDAP-Suchfilter.

Attribut	Erläuterung
value	Zum Suchfilter hinzuzufügende Zeile, wenn die Suche mit dem UND-Operatoren und Ersetzen der Elemente erfolgt.

Konkatenation von Filtern

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

Falls `admingrp` nach der Suche den Wert `"CN=ESuite Admins,OU=some name,DC=example,DC=com"` erhält, und der Benutzer `domain\user` eingegeben hat, ist der resultierende Filter:

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

Exemplarische Konfiguration der LDAP/AD-Authentifizierung

Nachfolgend sind exemplarische Einstellungen für die LDAP-Authentifizierung aufgeführt. Diese Einstellungen werden im Verwaltungscenter unter **Administration** → **Authentifizierung** → **LDAP/AD-Authentifizierung** (für die Variante **Einfache Einstellungen**) festgelegt.

Die Ausgangsparameter der Administratoren, die sich authentifizieren müssen:

- Domäne: `dc.test.local`
- Gruppe in Active Directory: `DrWeb_Admins`

Einstellungen des Verwaltungscenters:

Name der Einstellung		Wert
Servertyp		Microsoft Active Directory
Serveradresse		dc.test.local
Benutzernamenvorlagen für die Autorisierungsbestätigung	Kontenmaske	test* oder *@test.local
	Benutzername	\1
Benutzermitgliedschaft für die Autorisierungsbestätigung	Name	DrWeb_Admins
	Typ	Gruppe

C4. Aufteilung der Rechte in Bereiche

Tabelle C-1: Rechte des Administrators und ihre Besonderheiten

Code	Recht	Erläuterung	Bereich des Verwaltungscenters
Gruppen von Workstations verwalten			
1*	**Eigenschaften von Gruppen von Workstations anzeigen**	Liste benutzerdefinierter Gruppen, die für den Administrator im Antivirus-Netzwerk sichtbar sind. Alle Systemgruppen werden ebenfalls in der Struktur des Antivirus-Netzwerks angezeigt. In diesen Gruppen werden jedoch nur die Workstations aus der angegebenen Liste benutzerdefinierter Gruppen angezeigt.	Antivirus-Netzwerk Antivirus-Netzwerk → Allgemein → Eigenschaften
2*	**Eigenschaften von Gruppen von Workstations bearbeiten**	Liste benutzerdefinierter Gruppen, deren Eigenschaften der Administrator bearbeiten kann. Die Liste muss Gruppen aus der Liste im Recht 1 enthalten.	
3	**Konfiguration von Gruppen von Workstations anzeigen**	Liste benutzerdefinierter Gruppen, deren Konfiguration für den Administrator sichtbar ist. Der Administrator kann auch die	Antivirus-Netzwerk Antivirus-Netzwerk → Allgemein → Gestartete Komponenten

Code	Recht	Erläuterung	Bereich des Verwaltungscenters
		Konfiguration der Workstations anzeigen, für welche die Gruppen aus der Liste Primärgruppen sind. Die Liste muss Gruppen aus der Liste im Recht 1 enthalten.	Antivirus-Netzwerk → Allgemein → Quarantäne
4	**Konfiguration von Gruppen von Workstations bearbeiten**	Das Recht ist mit dem Recht 3 identisch, der Administrator kann aber die Konfiguration bearbeiten. Diese Liste muss Gruppen aus der Liste im Recht 3 enthalten.	Seiten im Bereich **Konfiguration** des Verwaltungsmenüs
5	**Eigenschaften von Workstations anzeigen**	Liste benutzerdefinierter Gruppen, die primär für die Workstations sind, deren Eigenschaften für den Administrator sichtbar sind. Die Liste muss Gruppen aus der Liste im Recht 1 enthalten.	Antivirus-Netzwerk
6	**Eigenschaften von Workstations bearbeiten**	Darunter auch ACL, Sperrung, Zugriff usw. Das Recht ist mit dem Recht 5 identisch, der Administrator kann aber die Eigenschaften bearbeiten. Diese Liste muss Gruppen aus der Liste im Recht 5 enthalten.	Antivirus-Netzwerk → Allgemein → Eigenschaften
8*	**Workstations in Gruppen verschieben und aus Gruppen entfernen**	Liste benutzerdefinierter Gruppen. Die Liste muss Gruppen aus der Liste im Recht 1 enthalten.	Antivirus-Netzwerk
9	**Workstations löschen**	Liste benutzerdefinierter Gruppen, die Primärgruppen für die Workstations sind, die der Administrator löschen kann. Die Liste muss Gruppen aus der Liste im Recht 1 enthalten.	

Code	Recht	Erläuterung	Bereich des Verwaltungscenters
10	**Agents per Fernzugriff installieren bzw. deinstallieren**	Liste benutzerdefinierter Gruppen, auf deren Workstations der Administrator die Agents mit ausgewählten IDs remote installieren kann. Diese Gruppen müssen Primärgruppen für die zu installierenden Workstations sein. Die Liste muss Gruppen aus der Liste im Recht 1 enthalten. Wenn es einige verbotene Objekte gibt, wird dieser Menüpunkt nicht angezeigt. Die Netzwerkinstallation ist nur aus /esuite/network/index.ds möglich, vorausgesetzt, dass das Recht 16 gewährt ist.	
11	**Workstations zusammenführen**	Liste benutzerdefinierter Gruppen, deren Workstations zusammengeführt werden können. Diese Gruppen müssen Primärgruppen für die Workstations sein. Das Symbol, mit dem Sie Workstations zusammenführen können, befindet sich auf der Symbolleiste. Die Liste muss Gruppen aus der Liste im Recht 1 enthalten.	
12*	**Statistische Tabellen anzeigen**	Liste benutzerdefinierter Gruppen, deren Statistiken für den Administrator sichtbar sind. Das Recht berechtigt, im Zeitplan des Servers eine Aufgabe zur Anzeige von regelmäßigen Berichten zu planen. Dabei kann eine Liste benutzerdefinierter Gruppen festgelegt werden, die der Administrator in dieser Aufgabe angeben kann (Gruppen, für deren Workstations Berichte gesendet werden). Wenn die Gruppe Everyone festgelegt ist, werden Berichte über alle Gruppen aus der Liste gesendet.	Antivirus-Netzwerk Seiten im Bereich **Statistik** des Verwaltungsmenüs

Code	Recht	Erläuterung	Bereich des Verwaltungscenters
		Die Liste muss Gruppen aus der Liste im Recht 1 enthalten.	
23	**Informationen zur Lizenzierung bearbeiten**	Liste benutzerdefinierter Gruppen, für die der Administrator Lizenzschlüssel hinzufügen, ersetzen oder löschen kann. Diese Gruppen müssen Primärgruppen für die Workstations sein. Die Liste muss Gruppen aus der Liste im Recht 1 enthalten.	
Administratoren verwalten			
25	**Administratoren bzw. Gruppen von Administratoren erstellen**	Das entsprechende Symbol wird auf der Symbolleiste ausgeblendet bzw. eingeblendet.	Administration → Konfiguration → Administratoren
26	**Administratorkonten bearbeiten**	Für den Administrator der Gruppe **Newbies** ist die Baumstruktur sichtbar, deren Wurzel die Gruppe ist, in der er sich befindet: Er sieht also Administratoren seiner Gruppe und ihrer Untergruppen. Für einen Administrator der Gruppe **Administrators** sind die Administratoren aller Gruppen sichtbar. Der Administrator kann die Konten der Administratoren aus den angegebenen Gruppen bearbeiten. Das entsprechende Symbol wird auf der Symbolleiste eingeblendet.	
27	**Administratorkonten löschen**	Identisch mit dem Recht 26.	
28	**Eigenschaften und Konfiguration von Gruppen von Administratoren anzeigen**	Darunter auch Administratoren in Gruppen und Untergruppen. Der Administrator kann nur in der Untergruppe seiner übergeordneten Gruppe auswählen.	

Code	Recht	Erläuterung	Bereich des Verwaltungscenters
39	**Administrative Gruppe „Newbies“ anzeigen**	Dieses Recht ermöglicht dem Administrator, die vordefinierte Gruppe **Newbies** in der Baumstruktur der Administratoren anzuzeigen. Wenn ein Administrator kein Recht zur Anzeige der Gruppe **Newbies** hat und dieser Gruppe gehört, wird in der Baumstruktur der Administratoren nur sein Konto angezeigt.	
29	**Eigenschaften und Konfiguration von Gruppen von Administratoren bearbeiten**	Darunter auch Administratoren in Gruppen und Untergruppen. Der Administrator kann nur in der Untergruppe seiner übergeordneten Gruppe auswählen. Wenn das Recht nicht gewährt ist, ist es dem Administrator unabhängig vom Recht 26 nicht möglich, die Vererbung zu deaktivieren oder Rechte eines Administrators in der Gruppe zu erhöhen.	
Erweitert			
7	**Workstations erstellen**	Bei der Erstellung einer Workstation ist eine Liste der Gruppen mit dem Recht 8 verfügbar (die Gruppe, in welche die Workstations verschoben werden, muss das Recht 8 haben). Bei der Erstellung von Workstations muss als Primärgruppe eine von den verfügbaren Gruppen definiert werden.	Antivirus-Netzwerk
13	**Audit-Protokoll anzeigen**	Das Audit-Protokoll ist für einen Administrator mit Vollzugriff sowie für die Objekte mit dem Recht 4 verfügbar.	Administration → Protokolle → Audit-Protokoll
16	**Netzwerk-Scanner starten**	Wenn das Recht nicht erteilt ist, ist die Netzwerkinstallation aus /esuite/network/index.ds nicht möglich.	Antivirus-Netzwerk Administration → Netzwerk-Scanner

Code	Recht	Erläuterung	Bereich des Verwaltungscenters
17	**Newbies genehmigen**	Gruppen aus dem Recht 8 sind verfügbar. Dieses Recht kann nicht gewährt werden, wenn der Administrator nur einige Gruppen verwalten darf, das heißt, dass für das Recht 1 (**Eigenschaften von Gruppen von Workstations anzeigen**) bestimmte Gruppen angegeben wurden.	Antivirus-Netzwerk
18	**Server-Zeitplan anzeigen**	Anzeige der Tabelle **Aufgabenprotokoll**. Wenn das Recht 12 und 18 nicht gewährt sind, ist es nicht möglich, die Seite mit dem Zeitplan des Servers anzuzeigen. Wenn das Recht 12 gewährt und das Recht 18 nicht gewährt ist, ist es möglich, den Statistikzeitplan anzuzeigen. Die Aufgabe zum Versenden der Berichte für einen bestimmten Administrator wird je nach Verfügbarkeit des Rechts 12 und der Benachrichtigung **Statistikbericht** angezeigt, selbst wenn das Recht 18 verweigert ist.	Administration → Konfiguration → Dr.Web Server-Aufgabenplaner Administration → Protokolle → Aufgabenprotokoll
19	**Server-Zeitplan konfigurieren**		Administration → Konfiguration → Dr.Web Server-Aufgabenplaner
20	**Server- und Repository-Konfiguration anzeigen**		Administration → Konfiguration → Webserver-Konfiguration Administration → Repository → Repository-Status Administration → Repository → Verschobene Updates

Code	Recht	Erläuterung	Bereich des Verwaltungscenters
21	**Server- und Repository-Konfiguration bearbeiten**		Administration → Repository → Allgemeine Repository-Konfiguration Administration → Repository → Detaillierte Repository-Konfiguration Administration → Repository → Repository-Inhalt Administration → Protokolle → Update-Protokoll des Repository Administration → Konfiguration → Benutzerdefinierte Prozeduren Administration → Dr.Web Server → Liste der Versionen
22	**Informationen zur Lizenzierung anzeigen**		Administration → Administration → Lizenz-Manager
24	**Konfiguration von Benachrichtigungen bearbeiten**		Administration → Benachrichtigungen → Konfiguration von Benachrichtigungen Administration → Benachrichtigungen → Nicht gesendete Benachrichtigungen Administration → Benachrichtigungen → Benachrichtigungen der Web-Konsole
30	**Web API verwenden**		-

Code	Recht	Erläuterung	Bereich des Verwaltungscenters
31	**Server-Umgebung anzeigen**		Nachbarn
32	**Server-Umgebung bearbeiten**		Nachbarn
33	**Zusätzliche Funktionen verwenden**	Dadurch wird der Zugriff auf alle Unterbereiche des Bereichs **Zusätzliche Funktionen** außer **Dienstprogramme** (dieser ist immer verfügbar) eingeschränkt.	Administration → Zusätzliche Funktionen
34	**Repository aktualisieren**	Update des Server-Repository über das GUS.	Schaltfläche **Repository aktualisieren** im Bereich **Repository-Status**
42	**Eigene Einstellungen bearbeiten**	Recht zum Ändern der eigenen Einstellungen des Administratorkontos.	Administration → Konfiguration → Administratoren

* Die Rechte 1, 2, 8 und 12 für eine Workstation werden anhand der Liste der Gruppen, zu denen sie gehört, und nicht anhand ihrer Primärgruppe ermittelt.

Wenn die Workstation einer Gruppe gehört, und dieser Gruppe einige von diesen Rechten erteilt wurden, stehen dem Administrator die Funktionen zur Verfügung, die diesen Rechten entsprechen. Dabei ist es nicht relevant, ob die erlaubte Gruppe primär für die Workstation ist. Die erlaubte Gruppe hat Vorrang gegenüber einer verbotenen Gruppe: Wenn die Workstation gleichzeitig zu einer erlaubten und einer verbotenen Gruppe gehört, stehen dem Administrator die Funktionen zur Verfügung, die den Rechten der erlaubten Gruppe entsprechen.

Anhang D. Benachrichtigungssystem

Die wichtigsten Informationen rund um die Konfiguration von Administrator-Benachrichtigungen finden Sie im **Administratorhandbuch** unter Benachrichtigungen konfigurieren.

D1. Parameter des Benachrichtigungssystems

Im Benachrichtigungssystem des Antivirus-Netzwerks werden die folgenden Typen von Benachrichtigungen verwendet:

- E-Mail-Benachrichtigungen
- Benachrichtigungen über Web-Konsole
- Benachrichtigungen über SNMP
- Benachrichtigungen über das Protokoll des Agents
- Push-Benachrichtigungen

Je nach Sendemethode müssen Sie verschiedene Parameter und die dazugehörigen Werte im Format Parameter → Wert angeben. Alle möglichen Parameter werden nachfolgend aufgelistet.

Tabelle D-1: Allgemeine Parameter

Parameter	Erläuterung	Standardwert	Obligatorisch
`TO`	Empfänger von Benachrichtigungen. Um mehrere Empfänger anzugeben, verwenden Sie einen senkrechten Strich `|`.		ja
`ENABLED`	Aktivierung bzw. Deaktivierung von Benachrichtigungen.	`true` oder `false`	ja
`_TIME_TO_LIVE`	Anzahl erneuter Sendeversuche bei Sendefehler.	10 Sendeversuche	nein
`_TRY_PERIOD`	Zeitraum in Sekunden zwischen erneuten Sendeversuchen.	5 Minuten (maximal einmal pro 5 Minuten)	nein

Unten finden Sie die Parameter für einzelne Sendemethode.

Tabelle D-2: E-Mail-Benachrichtigung

Parameter	Erläuterung	Standardwert
FROM	E-Mail-Adresse, die als Absender von E-Mail-Benachrichtigungen verwendet wird.	drwcsd@${Hostname}
TO	E-Mail-Adressen, an die Benachrichtigungen gesendet werden.	-
HOST	Adresse des SMTP-Servers.	127.0.0.1
PORT	Portnummer des SMTP-Servers.	• 25, wenn der SSL-Parameter den Wert no hat. • 465, wenn der SSL-Parameter den Wert yes hat.
USER	Benutzer des SMTP-Servers.	"" Wenn ein Benutzer angegeben ist, muss mindestens eine Autorisierungsmethode aktiviert sein. Andernfalls können keine E-Mails übermittelt werden.
PASS	Passwort des SMTP-Server-Benutzers.	""
STARTTLS	Diese Option sorgt dafür, dass die Kommunikation verschlüsselt erfolgt. Um eine sichere Verbindung anzufordern, wird der Befehl STARTTLS verwendet. Der Standardport ist 25.	yes
SSL	Diese Option sorgt dafür, dass die Kommunikation verschlüsselt erfolgt. Eine separate gesicherte TLS-Verbindung wird dabei hergestellt. Der Standardport ist 465.	no
AUTH-CRAM-MD5	CRAM-MD5-Authentifizierung verwenden.	no
AUTH-PLAIN	PLAIN-Authentifizierung verwenden.	no
AUTH-LOGIN	LOGIN-Authentifizierung verwenden.	no
AUTH-NTLM	NTLM-Authentifizierung verwenden.	no

Parameter	Erläuterung	Standardwert
SSL-VERIFYCERT	SSL-Zertifikat des Servers überprüfen.	no
DEBUG	Debug-Modus zur Fehlerdiagnose aktivieren.	-

Tabelle D-3: Benachrichtigung über die Web-Konsole

Parameter	Erläuterung	Standardwert
TO	UUID der Administratoren, an die Benachrichtigungen gesendet werden sollen.	-
SHOW_PERIOD	Speicherdauer in Sekunden für Benachrichtigungen, beginnend ab dem Erhalt.	86.400 Sekunden, d. h. 24 Stunden

Tabelle D-4: Benachrichtigung über SNMP

Parameter	Erläuterung	Standardwert
TO	SNMP-Entität (z. B. IP-Adresse), an die Benachrichtigungen gesendet werden.	-
DOMAIN	Domäne.	• localhost für Windows • "" für UNIX-basierte Betriebssysteme
COMMUNITY	SNMP-Community oder Kontext.	public
RETRIES	Anzahl erneuter Sendeversuche durch API.	5 Versuche
TIMEOUT	Zeitraum, nach dem die API Benachrichtigungen erneut sendet.	5 Sekunden

Tabelle D-5: Benachrichtigung über das Agent-Protokoll

Parameter	Erläuterung	Standardwert
TO	UUID der Workstations, die die Benachrichtigungen empfangen sollen.	-

Parameter	Erläuterung	Standardwert
SHOW_PERIOD	Speicherdauer in Sekunden für Benachrichtigungen, beginnend ab dem Erhalt.	86.400 Sekunden, d. h. 24 Stunden

Tabelle D-6: Push-Benachrichtigungen

Parameter	Erläuterung	Standardwert
TO	Gerätetoken, die Apps bei der Registrierung auf dem Server des Herstellers (z. B. bei Apple) erhalten.	-
SERVER_URL	URL Relay des Servers, über den Benachrichtigungen an den Server des Herstellers weitergeleitet werden.	-

D2. Parameter für Benachrichtigungsvorlagen

Die Texte von Benachrichtigungen werden durch eine spezielle Server-Komponente, das Vorlagenverarbeitungsprogramm, anhand von Vorlagendateien generiert.

Das auf dem Windows Nachrichtendienst basierende Benachrichtigungssystem kann nur unter den Windows-Betriebssystemen betrieben werden, die den Windows-Nachrichtendienst (Net Send) unterstützen.

Der Windows-Nachrichtendienst ist ab Windows Vista nicht mehr verfügbar.

Die Vorlagendatei besteht aus einem Text und Variablen in geschweiften Klammern. Bei der Bearbeitung von Vorlagendateien können die unten aufgeführten Variablen verwendet werden.

Variablen werden wie folgt geschrieben:

- {<*VAR*>} – direkt den Wert der <*VAR*>-Variable verwenden.
- {<*VAR*>:<*N*>} – die ersten <*N*> Zeichen der <*VAR*>-Variable.
- {<*VAR*>:<*first*>:<*N*>} – <*N*> Zeichen der *VAR*>-Variable, die den <*first*> ersten Zeichen folgen (beginnend ab dem <*first*>+1. Zeichen), wenn der Rest weniger ist, werden rechts Leerzeichen hinzugefügt.
- {<*VAR*>:<*first*>:<*N*>} – <*N*> Zeichen der *VAR*>-Variable, die nach den <*first*> ersten Zeichen folgen (beginnend ab dem <*first*>+1. Zeichen), wenn der Rest weniger ist, werden links Leerzeichen hinzugefügt.
- {<*VAR*>/<*original1*>/<*replace1*>[/<*original2*>/<*replace2*>]} – ersetzt die angegebenen Zeichen der <*VAR*>-Variable durch die festgelegten Werte: Die Zeichen <*original1*> werden durch die Zeichen <*replace1*> ersetzt, und die Zeichen <*original2*> (falls vorhanden) werden durch die Zeichen <*replace2*> ersetzt usw.

Die Anzahl von Platzhalter-Paaren ist nicht begrenzt.

- {<*VAR*>/<*original1*>/<*replace1*[{<*SUB_VAR*>}]>[/<*original2*>/<*replace2*>]} – analog zu den obigen Ersetzungen, außer dass die Untervariable <*SUB_VAR*> verwendet wird. Aktionen für Untervariablen sind identisch mit allen Aktionen für die übergeordneten Variablen.

  Die Verschachtelungstiefe bei rekursiven Ersetzungen ist nicht begrenzt.
- {<*VAR*>/<*original1*>/<*replace1*>/<*original2*>/<*replace2*>/*/<*replace3*>} – analog zu den obigen Ersetzungen durch die angegebenen Werte, außer dass die Ersetzung durch den Wert in <*replace3*> möglich ist, falls keiner der aufgelisteten Ausgangswerte übereinstimmt. Falls in <*VAR*> weder <*original1*> noch <*original2*> vorkommt, werden alle Werte durch <*replace3*> ersetzt.

Tabelle D-7: Schreibweise der Variablen

Variable	Wert	Ausdruck	Ergebnis
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

Zeichenerklärung

° steht für ein Leerzeichen.

Umgebungsvariablen

Zum Verfassen von Nachrichtentexten können Sie die Umgebungsvariablen des Server-Prozesses (**System**-Benutzers) verwenden.

Die Umgebungsvariablen sind verfügbar im Nachrichteneditor des Verwaltungscenters, in der Dropdown-Liste **ENV**. Beachten Sie das Folgende: Bei der Angabe einer Variable müssen Sie das Präfix `ENV.` hinzufügen (das Präfix endet mit einem Punkt).

Systemvariablen

- `SYS.BRANCH` – Version der Agents und des Servers
- `SYS.BUILD` – Builddatum des Servers
- `SYS.DATE` – aktuelles Systemdatum
- `SYS.DATETIME` – aktuelles Systemdatum und aktuelle Systemuhrzeit

- `SYS.HOST` – DNS-Name des Servers
- `SYS.MACHINE` – Netzwerkadresse des Rechners mit dem installierten Server
- `SYS.OS` – Name des Betriebssystems auf dem Rechner mit dem installierten Server
- `SYS.PLATFORM` – Server-Plattform
- `SYS.PLATFORM.SHORT` – kurze Variante von `SYS.PLATFORM`
- `SYS.SERVER` – Produktname (Dr.Web Server)
- `SYS.TIME` – aktuelle Systemuhrzeit
- `SYS.VERSION` – Server-Version

Gemeinsame Variablen für Workstations

- `GEN.LoginTime` – Verbindungszeit der Workstation
- `GEN.StationAddress` – Adresse der Workstation
- `GEN.StationDescription` – Beschreibung der Workstation
- `GEN.StationID` – eindeutige ID der Workstation
- `GEN.StationLDAPDN` – der definierte Name (Distinguished Name) der Workstation unter Windows. Der definierte Name ist relevant, wenn die Workstation in einer ADS/LDAP-Domäne ist
- `GEN.StationMAC` – MAC-Adresse der Workstation
- `GEN.StationName` – Name der Workstation
- `GEN.StationPrimaryGroupID` – ID der Primärgruppe der Workstation
- `GEN.StationPrimaryGroupName` – Name der Primärgruppe der Workstation
- `GEN.StationSID` – Sicherheits-ID der Workstation

Gemeinsame Variablen für Repository

- `GEN.CurrentRevision` – aktuelle ID der Version
- `GEN.Folder` – Verzeichnis des Produkts
- `GEN.NextRevision` – ID der aktualisierten Version
- `GEN.Product` – Produktbeschreibung

Parameter und Variablen von Benachrichtigungen nach Typen

Administratoren

Fehler bei der Autorisierung des Administrators

Parameter	Wert	
Auslöser	Administrator konnte sich am Verwaltungscenter nicht anmelden. Die Fehlerursache wird im Text der Benachrichtigung angegeben.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.Login`	Anmeldename
	`MSG.Address`	Netzwerkadresse des Verwaltungscenters
	`MSG.LoginErrorCode`	Fehlercode

Unbekannter Administrator

Parameter	Wert	
Auslöser	Ein Administrator mit einem unbekannten Anmeldenamen versucht, sich am Verwaltungscenter anzumelden.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.Login`	Anmeldename
	`MSG.Address`	Netzwerkadresse des Verwaltungscenters

Installationen

Für Benachrichtigungen dieser Gruppe können auch die oben aufgeführten gemeinsamen Variablen für Workstations verwendet werden.

Fehler bei der Installation auf einer Workstation

Parameter	Wert
Auslöser	Diese Benachrichtigung wird gesendet, wenn der Agent auf einer

Parameter	Wert	
	Workstation nicht installiert werden konnte. Die Fehlerursache wird im Text der Benachrichtigung angegeben.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.Error`	Fehlermeldung

Installation auf einer Workstation ist erfolgreich abgeschlossen

Parameter	Wert
Auslöser	Diese Benachrichtigung wird gesendet, wenn der Agent auf einer Workstation installiert wurde.
Zusätzliche Einstellung	Nicht erforderlich.
Variablen	Keine.

Lizenzen

Anzahl von Workstations in der Gruppe erreicht bald das Lizenzlimit

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn das im zugewiesenen Schlüssel festgelegte Lizenzlimit für die Anzahl von Workstations in der Gruppe bald erreicht wird.	
Zusätzliche Einstellung	Anzahl verfügbarer Lizenzen im Schlüssel, bei der die Benachrichtigung gesendet wird: Weniger als 3 Lizenzen oder weniger als 5 Prozent von der Gesamtzahl der Lizenzen im Schlüssel.	
Variablen	`MSG.Free`	Anzahl der verbleibenden Lizenzen
	`MSG.Licensed`	Anzahl von Workstations, welche die Lizenzen dieser Gruppen verwenden
	`MSG.Total`	Gesamtzahl von Lizenzen in allen der Gruppe zugewiesenen Schlüsseln. Wichtiger Hinweis: Die

Parameter	Wert	
		Lizenzschlüssel der Gruppe können gleichzeitig mehreren lizenzierten Objekten zugewiesen sein.
	GEN.StationPrimaryGroupID	ID der Primärgruppe
	GEN.StationPrimaryGroupName	Name der Primärgruppe

Das Lizenzlimit für die Anzahl an Online-Workstations wurde erreicht

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, falls beim Herstellen der Verbindung mit dem Server festgestellt wurde, dass die im Lizenzschlüssel festgelegte Anzahl von Workstations in der Gruppe, zu der die zu verbindende Workstation gehört, erreicht wurde. Die neue Workstation kann dabei auf dem Server nicht registriert werden.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	MSG.ID	UUID der Workstation
	MSG.StationName	Name der Workstation
	Verwendet werden können auch die oben aufgeführten gemeinsamen Variablen für Workstations.	

Der Lizenzschlüssel kann nicht automatisch aktualisiert werden

Parameter	Wert	
Auslöser	Die Benachrichtigung wird gesendet, wenn der Lizenzschlüssel nicht automatisch aktualisiert werden kann, da der aktuelle und der neue Schlüssel nicht den gleichen Umfang an den lizenzierten Komponenten haben. Der neue Lizenzschlüssel wird zwar geladen, doch nicht auf alle Objekte des alten Lizenzschlüssels verteilt. Der Lizenzschlüssel muss daher manuell ersetzt werden.	
Zusätzliche Einstellung	Weiterführende Informationen zur automatischen Aktualisierung der Lizenzen finden Sie im **Administratorhandbuch** unter Automatische Lizenzaktualisierung.	
Variablen	MSG.ExpirationDate	Lizenzablaufdatum

Parameter	Wert	
	MSG.Expired	• 1 – Lizenz ist bereits abgelaufen. • 0 – Lizenz ist noch gültig.
	MSG.KeyDifference	Der Grund, warum die automatische Ersetzung des Schlüssels nicht möglich ist: • 1 - Der aktuelle und der neue Lizenzschlüssel haben nicht den gleichen Umfang an den lizenzierten Komponenten. • 2 - Der neue Lizenzschlüssel hat weniger Lizenzen als der aktuelle Lizenzschlüssel.
	MSG.KeyId	ID des alten Lizenzschlüssels
	MSG.KeyName	Name des alten Lizenzschlüssels
	MSG.NewKeyId	ID des neuen Lizenzschlüssels
	MSG.NewKeyName	Name des neuen Lizenzschlüssels

Der Lizenzschlüssel wurde automatisch aktualisiert

Parameter	Wert	
Auslöser	Die Benachrichtigung wird gesendet, nachdem der Lizenzschlüssel automatisch aktualisiert wurde. Der neue Lizenzschlüssel wird geladen und auf alle Objekte des alten Lizenzschlüssels verteilt.	
Zusätzliche Einstellung	Weiterführende Informationen zur automatischen Aktualisierung der Lizenzen finden Sie im **Administratorhandbuch** unter Automatische Lizenzaktualisierung.	
Variablen	MSG.KeyId	ID des alten Lizenzschlüssels
	MSG.KeyName	Name des alten Lizenzschlüssels
	MSG.NewKeyId	ID des neuen Lizenzschlüssels
	MSG.NewKeyName	Name des neuen Lizenzschlüssels

Der Lizenzschlüssel wurde gesperrt

Parameter	Wert	
Auslöser	Die Benachrichtigung wird gesendet, wenn beim Aktualisieren des Repository über die Server des GUS festgestellt wird, dass der Lizenzschlüssel gesperrt wurde. Der Lizenzschlüssel kann dann nicht mehr verwendet werden.	
Zusätzliche Einstellung	Wenden Sie sich an den technischen Support von Doctor Web, um den Grund für die Sperrung zu erfragen.	
Variablen	`MSG.KeyId`	ID des Lizenzschlüssels
	`MSG.KeyName`	Benutzername des Lizenzschlüssels

Die maximale Anzahl an ausgeliehenen Lizenzen wurde erreicht

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn die Anzahl angeforderter Lizenzen für Nachbar-Server die Anzahl der Lizenzen im Lizenzschlüssel überschreitet.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.ObjId`	ID des Lizenzschlüssels

Leihfrist für ausgeliehene Lizenzen ist abgelaufen

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn der Zeitraum, für den Lizenzen aus dem Lizenzschlüssel des jeweiligen Servers auf den Nachbar-Server verteilt sein können, abgelaufen ist.	
Zusätzliche Einstellung	Der Zeitraum, für den Lizenzen verteilt werden können, wird im Bereich **Administration** → **Dr.Web Server-Konfiguration** → **Lizenzen** festgelegt.	
Variablen	`MSG.ObjId`	ID des Lizenzschlüssels
	`MSG.Server`	Nachbar-Servername

Limit für die Anzahl von Lizenzen im Lizenzschlüssel

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn beim Start des Servers festgestellt wurde, dass die maximal zulässige Anzahl von Workstations in einer Gruppe, die im Lizenzschlüssel dieser Gruppe festgelegt ist, überschritten wurde.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.KeyId`	ID des Lizenzschlüssels
	`MSG.KeyName`	Benutzername des Lizenzschlüssels
	`MSG.Licensed`	Anzahl von erlaubten Lizenzen
	`MSG.LicenseLimit`	Lizenzstatus: • 1 – Alle verfügbaren Lizenzen im Lizenzschlüssel werden bald aufgebraucht. • 2 – Alle verfügbaren Lizenzen im Lizenzschlüssel sind aufgebraucht. • 3 – Der Lizenzschlüssel wurde mehr Objekten zugewiesen, als die in diesem Lizenzschlüssel erlaubte Anzahl.
	`MSG.Licensed`	Anzahl von Objekten, denen der Lizenzschlüssel zugewiesen wurde
	`MSG.Total`	Anzahl der Lizenzen im Lizenzschlüssel

Lizenzschlüsselablauf

Parameter	Wert
Auslöser	Die Benachrichtigung wird gesendet, wenn der Lizenzschlüssel bald abläuft und nicht automatisch aktualisiert werden kann.
Zusätzliche Einstellung	Nicht erforderlich.

Parameter	Wert	
Variablen	`MSG.ExpirationDate`	Lizenzablaufdatum
	`MSG.Expired`	• 1 – Lizenz ist bereits abgelaufen. • 0 – Lizenz ist noch gültig.
	`MSG.KeyId`	ID des Lizenzschlüssels
	`MSG.KeyName`	Name des Lizenzschlüssels

Newbies

Für Benachrichtigungen dieser Gruppe können auch die oben aufgeführten gemeinsamen Variablen für Workstations verwendet werden.

Workstation wartet auf Genehmigung

Parameter	Wert
Auslöser	Die Benachrichtigung wird gesendet, falls eine neue Workstation die Verbindung mit dem Server angefordert, und der Administrator diese Workstation manuell genehmigen bzw. ablehnen muss.
Zusätzliche Einstellung	Diese Situation ist möglich, wenn unter **Administration** → **Dr.Web Server-Konfiguration** → **Allgemein** in der Dropdown-Liste **Registrierungsmodus für Newbies** die Option **Zugriff manuell bestätigen** ausgewählt ist.
Variablen	Keine.

Workstation wurde automatisch abgelehnt

Parameter	Wert
Auslöser	Die Benachrichtigung wird gesendet, falls eine neue Workstation, welche die Verbindung mit dem Server angefordert hat, vom Server automatisch abgelehnt wurde.
Zusätzliche Einstellung	Diese Situation ist möglich, wenn unter **Administration** → **Dr.Web Server-Konfiguration** → **Allgemein** in der Dropdown-Liste **Registrierungsmodus für Newbies** die Option **Zugriff immer verweigern** ausgewählt ist.
Variablen	Keine.

Workstation wurde vom Administrator abgelehnt

Parameter	Wert	
Auslöser	Die Benachrichtigung wird gesendet, wenn eine neue Workstation, welche die Verbindung mit dem Server angefordert hat, vom Administrator manuell abgelehnt wurde.	
Zusätzliche Einstellung	Diese Situation ist möglich, wenn unter **Administration** → **Dr.Web Server-Konfiguration** → **Allgemein** in der Dropdown-Liste **Registrierungsmodus für Newbies** die Option **Zugriff manuell bestätigen** ausgewählt ist und der Administrator für die Workstation die Option **Antivirus-Netzwerk** → **Nicht genehmigte Workstations** → **Ausgewählte Workstations ablehnen** ausgewählt hat.	
Variablen	`MSG.AdminAddress`	Netzwerkadresse des Verwaltungscenters
	`MSG.AdminName`	Administratorname

Repository

Für Benachrichtigungen dieser Gruppe können auch die oben aufgeführten gemeinsamen Variablen für Repository verwendet werden.

Aktualisierung eines Produkts im Repository wurde gesperrt

Parameter	Wert
Auslöser	Diese Benachrichtigung wird gesendet, wenn der Administrator die Aktualisierung eines Produkts vorübergehend gesperrt hat. Eine Aktualisierung über das GUS ist dabei nicht möglich.
Zusätzliche Einstellung	Produkte des Repository können unter **Administration** → **Detaillierte Repository-Konfiguration** verwaltet werden.
Variablen	Keine.

Aktualisierung eines Produkts im Repository wurde gestartet

Parameter	Wert
Auslöser	Diese Benachrichtigung wird gesendet, falls bei der Überprüfung des Repository festgestellt wurde, dass die angeforderten Produkte aktualisiert werden müssen. Das Update über das GUS wird dabei

Parameter	Wert
	gestartet.
Zusätzliche Einstellung	Nicht erforderlich.
Variablen	Keine.

Das Repository wird bereits aktualisiert

Parameter	Wert
Auslöser	Diese Benachrichtigung wird gesendet, wenn beim Aktualisieren des Servers ein weiterer Aktualisierungsvorgang gestartet wird.
Zusätzliche Einstellung	Nicht erforderlich.
Variablen	Keine.

Fehler bei der Aktualisierung des Repository

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn ein Fehler beim Aktualisieren des Repository oder eines Produkts des Repository über das GUS aufgetreten ist. Die Fehlerursache und der Name des nicht aktualisierten Produkts werden in der Benachrichtigung angegeben.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.Error`	Fehlermeldung
	`MSG.ExtendedError`	Detaillierte Fehlerbeschreibung

Produkt im Repository ist auf dem aktuellen Stand

Parameter	Wert
Auslöser	Diese Benachrichtigung wird gesendet, falls bei der Überprüfung des Repository festgestellt wurde, dass das angeforderte Produkt im aktuellen Zustand ist. Das Update des Produkts über das GUS ist dabei nicht erforderlich.
Zusätzliche Einstellung	Nicht erforderlich.
Variablen	Keine.

Variablen der Vorlage **Produkt im Repository ist auf dem aktuellen Stand** schließen nicht die Dateien ein, die als „**bei Benachrichtigungen ignoriert**“ in der Konfigurationsdatei des Produkts markiert sind, s. dazu F1. Syntax der Konfigurationsdatei config.

Produkt im Repository wurde aktualisiert

Nachricht	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, nachdem das Repository über das GUS aktualisiert wird.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.Added`	Auflistung der hinzugefügten Dateien (ein Name pro Zeile)
	`MSG.AddedCount`	Anzahl der hinzugefügten Dateien
	`MSG.Deleted`	Auflistung der gelöschten Dateien (ein Name pro Zeile)
	`MSG.DeletedCount`	Anzahl der gelöschten Dateien
	`MSG.Replaced`	Auflistung der ersetzten Dateien (ein Name pro Zeile)
	`MSG.ReplacedCount`	Anzahl der ersetzten Dateien

Wenig Speicherplatz auf dem Datenträger

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, falls der Speicherplatz auf dem Datenträger, auf dem sich das Verzeichnis des Servers `var` mit dynamischen Daten befindet, geht zur Neige.	
Zusätzliche Einstellung	Diese Benachrichtigung wird gesendet, falls auf dem Datenträger weniger als 315 MB oder 1000 Inodes (unter UNIX) verfügbar sind, es sei denn, dass diese Werte durch Umgebungsvariable angepasst wurden.	
Variablen	Die oben aufgeführten gemeinsamen Variablen für Repository können nicht verwendet werden.	
	`MSG.FreeInodes`	Anzahl freier Inodes (relevant nur

Parameter	Wert	
		bei einigen Betriebssystemen der UNIX-Familie)
	`MSG.FreeSpace`	Freier Speicherplatz in Bytes
	`MSG.Path`	Pfad zum Verzeichnis mit geringem Speicherplatz
	`MSG.RequiredInodes`	Erforderliche Anzahl freier Inodes (relevant nur bei einigen Betriebssystemen der UNIX-Familie)
	`MSG.RequiredSpace`	Benötigter Speicherplatz

Sonstiges

Es wurde viele Sperrungen durch die Anwendungskontrolle registriert

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn auf den Workstations viele Anwendungen durch die Anwendungskontrolle gesperrt wurden.	
Zusätzliche Einstellung	Damit Benachrichtigungen über zahlreiche Anwendungssperrungen gesendet werden können, müssen das Kontrollkästchen **Zahlreiche Sperrungen durch Anwendungskontrolle** im Bereich **Administration → Dr.Web Server-Konfiguration → Statistik** aktiviert und die dazugehörigen Parameter festgelegt sein.	
Variablen	`MSG.Total`	Gesamtzahl von Sperrungen
	`MSG.Profile`	Häufigste Profile, anhand derer Anwendungen gesperrt wurden

Es wurden viele Verbindungsabbrüche registriert

Parameter	Wert
Auslöser	Diese Benachrichtigung wird gesendet, wenn sehr viele Verbindungsabbrüche mit Clients (darunter Workstations, Agent-Installationsprogrammen, Nachbar-Servern oder Proxyservern) aufgetreten sind.

Parameter	Wert	
Zusätzliche Einstellung	Damit Benachrichtigungen über zahlreiche Verbindungsabbrüche gesendet werden können, müssen das Kontrollkästchen **Verbindungsabbrüche** im Bereich **Administration → Dr.Web Server-Konfiguration → Statistik** aktiviert und die dazugehörigen Parameter festgelegt sein.	
Variablen	`MSG.Total`	Anzahl von Verbindungsabbrüchen
	`MSG.AddrsCount`	Anzahl von Adressen, deren Verbindungen abgebrochen wurden

Fehler bei der Rotation des Server-Protokolls

Parameter	Wert	
Auslöser	Fehler bei der Rotation des Server-Protokolls. Die Fehlerursache wird im Text der Benachrichtigung angegeben.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.Error`	Fehlertext

Fehler beim Schreiben ins Server-Protokoll

Parameter	Wert	
Auslöser	Fehler beim Schreiben in das Protokoll des Servers. Die Fehlerursache wird im Text der Benachrichtigung angegeben.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.Error`	Fehlertext

Massenhafte Infektion im Netzwerk

Parameter	Wert
Auslöser	Diese Benachrichtigung wird gesendet, falls Workstations des Antivirus-Netzwerks massenhaft infiziert wurden. Das bedeutet, dass innerhalb des festgelegten Zeitraums der vorgegebene Schwellenwert für die Anzahl erkannter Bedrohungen erreicht wurde.

Parameter	Wert	
Zusätzliche Einstellung	Um die Benachrichtigung versenden zu können, müssen Sie das Kontrollkästchen **Massenhafte Infektion melden** im Bereich **Administration → Dr.Web Server-Konfiguration → Statistik** aktivieren. Die dazugehörigen Parameter werden im gleichen Bereich festgelegt.	
Variablen	`MSG.Infected`	Gesamtzahl der erkannten Bedrohungen
	`MSG.Virus`	Häufigste Bedrohungen

Nachbar-Server hat lange keine Verbindung mehr mit dem Server hergestellt

Parameter	Wert	
Auslöser	Die Benachrichtigung wird entsprechend der Aufgabe im Zeitplan des Servers verschickt und enthält Informationen darüber, dass ein Nachbar-Server lange Zeit keine Verbindung mehr mit diesem Server hergestellt hat. Das Datum der letzten Verbindung wird im Text der Benachrichtigung angegeben.	
Zusätzliche Einstellung	Zeitraum, in dem der Nachbar-Server keine Verbindung mit dem Server herstellen soll, damit die Benachrichtigung gesendet wird, wird in der Aufgabe **Nachbar-Server hat lange keine Verbindung mehr mit dem Server hergestellt** im Zeitplan des Servers unter **Administration → Dr.Web Server-Aufgabenplaner** festgelegt.	
Variablen	`MSG.LastDisconnectTime`	Zeitpunkt, an dem der Server zuletzt online war
	`MSG.StationName`	Nachbar-Servername

Statistikbericht

Parameter	Wert	
Auslöser	Die Benachrichtigung wird gesendet, wenn ein regelmäßiger Bericht entsprechend der Aufgabe im Zeitplan des Servers generiert wird. In der Benachrichtigung wird auch der Pfad zum Bericht angegeben.	
Zusätzliche Einstellung	Der Bericht wird entsprechend der Aufgabe **Statistikbericht erstellen** im Zeitplan des Servers generiert. Der Zeitplan wird unter **Administration → Dr.Web Server-Aufgabenplaner** konfiguriert.	
Variablen	`MSG.Attachment`	Pfad zum Bericht

Parameter	Wert	
	MSG.AttachmentType	MIME-Typ
	GEN.File	Name der Protokolldatei

Übersichtsbericht des Präventivschutzes

Parameter	Wert	
Auslöser	Die Benachrichtigung wird gesendet, wenn die Komponente Präventivschutz eine große Anzahl von Berichten von den Workstations im Netzwerk sendet.	
Zusätzliche Einstellung	Damit eine einheitliche Benachrichtigung über den Bericht des Präventivschutzes gesendet werden kann, muss das Kontrollkästchen **Berichte des Präventivschutzes gruppieren** im Bereich **Administration → Dr.Web Server-Konfiguration → Statistik** aktiviert sein. Die Parameter zum Gruppieren der Berichte lassen sich im gleichen Bereich festlegen.	
Variablen	MSG.AutoBlockedActCount	Anzahl der automatisch gesperrten Prozesse mit verdächtiger Aktivität
	MSG.AutoBlockedProc	Automatisch gesperrter Prozess mit verdächtiger Aktivität
	MSG.HipsType	Typ des zu schützenden Objekts
	MSG.IsShellGuard	Aufteilung je nach dem Typ der Reaktion des Präventivschutzes beim automatischen Sperren: • Sperrung von nicht autorisiertem Code • Überprüfung des Zugriffs auf die geschützten Objekte
	MSG.ShellGuardType	Der häufigste Grund für das Sperren der Ausführung von nicht autorisiertem Code beim automatischen Sperren des Ereignisses
	MSG.Total	Gesamtzahl von Ereignissen des Präventivschutzes im Netzwerk
	MSG.UserAllowedActCount	Anzahl der vom Benutzer

Parameter	Wert	
		erlaubten Prozesse mit verdächtiger Aktivität
	MSG.UserAllowedHipsType	Typ der am häufigsten geschützten Objekte, auf die der Benutzer den Zugriff zugelassen hat
	MSG.UserAllowedIsShellGuard	Aufteilung je nach dem Typ der Reaktion des Präventivschutzes beim manuellen Zulassen des Zugriffs durch den Benutzer: • Sperrung von nicht autorisiertem Code • Überprüfung des Zugriffs auf die geschützten Objekte
	MSG.UserAllowedProc	Vom Benutzer zugelassener Prozess mit verdächtiger Aktivität
	MSG.UserAllowedShellGuard	Der häufigste Grund für das Sperren der Ausführung von nicht autorisiertem Code beim manuellen Zulassen des Ereignisses durch den Benutzer
	MSG.UserBlockedActCount	Anzahl der vom Benutzer gesperrten Prozesse mit verdächtiger Aktivität
	MSG.UserBlockedHipsType	Typ der am häufigsten geschützten Objekte, auf die der Benutzer den Zugriff verweigert hat
	MSG.UserBlockedIsShellGuard	Aufteilung je nach dem Typ der Reaktion des Präventivschutzes beim manuellen Verweigern des Zugriffs durch den Benutzer: • Sperrung von nicht autorisiertem Code • Überprüfung des Zugriffs auf die geschützten Objekte
	MSG.UserBlockedProc	Vom Benutzer gesperrter Prozess mit verdächtiger

Parameter	Wert	
		Aktivität
	MSG.UserBlockedShellGuard	Der häufigste Grund für das Sperren der Ausführung von nicht autorisiertem Code beim manuellen Sperren des Ereignisses durch den Benutzer

Workstations

Für Benachrichtigungen dieser Gruppe können auch die oben aufgeführten gemeinsamen Variablen für Workstations verwendet werden.

Bei einer Multiserverkonfiguration besteht es die Möglichkeit, über Ereignisse auf den Nachbar-Servern zu benachrichtigen. Sie aktivieren diese Option beim Konfigurieren der Verbindungen zwischen einzelnen Nachbar-Servern (weitere Informationen hierzu finden Sie im **Administratorhandbuch** unter Verbindungen zwischen Dr.Web Servern konfigurieren).

Sie können über folgende Ereignisse auf einem Nachbar-Server benachrichtigt werden: **Eine Sicherheitsbedrohung wurde erkannt**, **Bericht des Präventivschutzes**, **Fehler beim Scannen**, **Scanstatistik**.

Bericht des Präventivschutzes

Parameter	Wert	
Auslöser	Die Benachrichtigung wird gesendet, nachdem ein Bericht des Präventivschutzes von einer Workstation dieses oder eines Nachbar-Servers empfangen wurde.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	MSG.AdminName	Administrator, der die Ausführung der Aktion für den verdächtigen Prozess ausgelöst hat
	MSG.Denied	Aktion, die für den verdächtigen Prozess ausgeführt wurde: • verboten • erlaubt
	MSG.HipsType	Typ des zu schützenden Objekts

Parameter	Wert	
	MSG.IsShellGuard	Aufteilung je nach dem Typ der Reaktion des Präventivschutzes: • Sperrung von nicht autorisiertem Code • Überprüfung des Zugriffs auf die geschützten Objekte
	MSG.Path	Pfad zum Prozess mit verdächtiger Aktivität
	MSG.Pid	ID des Prozesses mit verdächtiger Aktivität
	MSG.ShellGuardType	Grund für das Sperren der Ausführung von nicht autorisiertem Code
	MSG.StationTime	Zeitpunkt, an dem das Ereignis auf der Workstation aufgetreten ist
	MSG.Target	Pfad zum zu schützenden Objekt, auf den zuzugreifen versucht wurde
	MSG.Total	Anzahl von Verweigerungen bei der automatischen Reaktion des Präventivschutzes
	MSG.User	Benutzer, unter dem der gesperrte Prozess mit verdächtiger Aktivität gestartet wurde
	MSG.UserAction	Auslöser der Aktion für den verdächtigen Prozess: • Benutzer • automatische Reaktion des Präventivschutzes
	GEN.ServerRecvLinkID	UUID des letzten Nachbar-Servers, der den Bericht des Präventivschutzes von den mit ihm verbundenen Workstations gesendet hat (Der Wert ist leer, falls der Bericht von den mit dem aktuellen Server verbundenen Workstations erhalten wurde)

Parameter	Wert	
	GEN.ServerRecvLinkName	Name des letzten Nachbar-Servers, der den Bericht des Präventivschutzes von den mit ihm verbundenen Workstations gesendet hat (Der Wert ist leer, falls der Bericht von den mit dem aktuellen Server verbundenen Workstations erhalten wurde)
	GEN.ServerOriginatorID	UUID des Servers, mit dem die Workstation, von welcher der Bericht des Präventivschutzes erhalten wurde, verbunden ist
	GEN.ServerOriginatorName	Name des Servers, mit dem die Workstation, von welcher der Bericht des Präventivschutzes erhalten wurde, verbunden ist

Bericht des Präventivschutzes über die Erkennung von Bedrohungen anhand bekannter Hash-Werte von Bedrohungen

Parameter	Wert	
Auslöser	Die Benachrichtigung wird gesendet, nachdem ein Bericht des Präventivschutzes über den Fund von Bedrohungen anhand der Liste der bekannten Hash-Werte von einer Workstation dieses oder eines Nachbar-Servers empfangen wurde.	
Zusätzliche Einstellung	Die Benachrichtigung über den Fund anhand der Liste der bekannten Hash-Werte kann nur gesendet werden, wenn die Nutzung von Hash-Bulletins lizenziert ist (es reicht, dass mindestens eine entsprechende Lizenz in einem der vom Server verwendeten Lizenzschlüssel vorhanden ist). Ob die Lizenz vorhanden ist, finden Sie in Informationen zum Lizenzschlüssel, die im Parameter **Erlaubte Listen von Hash-Bulletins** unter **Lizenz-Manager** verfügbar sind (falls diese Funktion nicht lizenziert ist, ist dieser Parameter nicht vorhanden).	
Variablen	MSG.AdminName	Administrator, der die Ausführung der Aktion für den verdächtigen Prozess ausgelöst hat
	MSG.Denied	Aktion, die für den verdächtigen Prozess ausgeführt wurde:

Parameter	Wert	
		• verboten • erlaubt
	MSG.Document	Bulletin, das den Hash-Wert der erkannten Bedrohung enthält
	MSG.HipsType	Typ des zu schützenden Objekts
	MSG.IsShellGuard	Aufteilung je nach dem Typ der Reaktion des Präventivschutzes: • Sperrung von nicht autorisiertem Code • Überprüfung des Zugriffs auf die geschützten Objekte
	MSG.Path	Pfad zum Prozess mit verdächtiger Aktivität
	MSG.Pid	ID des Prozesses mit verdächtiger Aktivität
	MSG.SHA1	SHA1-Hash-Wert des erkannten Objekts
	MSG.SHA256	SHA256-Hash-Wert des erkannten Objekts
	MSG.ShellGuardType	Grund für das Sperren der Ausführung von nicht autorisiertem Code
	MSG.StationTime	Zeitpunkt, an dem das Ereignis auf der Workstation aufgetreten ist
	MSG.Target	Pfad zum zu schützenden Objekt, auf den zuzugreifen versucht wurde
	MSG.Total	Anzahl von Verweigerungen bei der automatischen Reaktion des Präventivschutzes
	MSG.User	Benutzer, unter dem der gesperrte Prozess mit verdächtiger Aktivität gestartet wurde
	MSG.UserAction	Auslöser der Aktion für den verdächtigen Prozess:

Parameter	Wert	
		• Benutzer • automatische Reaktion des Präventivschutzes
	GEN.ServerRecvLinkID	UUID des letzten Nachbar-Servers, der den Bericht des Präventivschutzes von den mit ihm verbundenen Workstations gesendet hat (Der Wert ist leer, falls der Bericht von den mit dem aktuellen Server verbundenen Workstations erhalten wurde)
	GEN.ServerRecvLinkName	Name des letzten Nachbar-Servers, der den Bericht des Präventivschutzes von den mit ihm verbundenen Workstations gesendet hat (Der Wert ist leer, falls der Bericht von den mit dem aktuellen Server verbundenen Workstations erhalten wurde)
	GEN.ServerOriginatorID	UUID des Servers, mit dem die Workstation, von welcher der Bericht des Präventivschutzes erhalten wurde, verbunden ist
	GEN.ServerOriginatorName	Name des Servers, mit dem die Workstation, von welcher der Bericht des Präventivschutzes erhalten wurde, verbunden ist

Das Gerät wurde gesperrt

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn eine Workstation gemeldet hat, dass ein an die Workstation angeschlossenes Gerät durch eine Antivirenkomponente von Dr.Web gesperrt wurde.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	MSG.Capabilities	Eigenschaften des Geräts
	MSG.Class	Geräteklasse (Name der übergeordneten Gruppe)

Parameter	Wert	
	MSG.Description	Gerätebeschreibung
	MSG.FriendlyName	Anzeigename des Geräts
	MSG.InstanceId	Geräteinstanz-ID
	MSG.User	Benutzername

Die Anwendungskontrolle hat einen Prozess aus der Liste der bekannten Hash-Werte von Bedrohungen gesperrt

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn auf der Workstation eine Anwendung aus der Liste der bekannten Hash-Werte von Bedrohungen durch die Anwendungskontrolle gesperrt wurde.	
Zusätzliche Einstellung	Die Benachrichtigung über den Fund anhand der Liste der bekannten Hash-Werte kann nur gesendet werden, wenn die Nutzung von Hash-Bulletins lizenziert ist (es reicht, dass mindestens eine entsprechende Lizenz in einem der vom Server verwendeten Lizenzschlüssel vorhanden ist). Ob die Lizenz vorhanden ist, finden Sie in Informationen zum Lizenzschlüssel, die im Parameter **Erlaubte Listen von Hash-Bulletins** unter **Lizenz-Manager** verfügbar sind (falls diese Funktion nicht lizenziert ist, ist dieser Parameter nicht vorhanden).	
Variablen	MSG.AppCtlAction	Ausgeführte Aktion: • 0 – unbekannt. • 2 – gesperrt. • 3 – gesperrt (nicht gefunden in der Liste vertrauenswürdiger Anwendungen). • 5 – anhand von verbietenden Regeln gesperrt. • 7 – anhand von Richtlinieneinstellungen gesperrt.
	MSG.AppCtlType	Ereignistyp: • 0 – unbekannt. • 1 – Prozessstart. • 2 – Hostprozessstart.

Parameter	Wert	
		• 3 – Starten des Skript-Interpreters. • 4 – Laden des Moduls. • 5 – Laden des Treibers. • 6 – Starten des MSI-Installationsprogramms. • 7 – Erstellen einer neuen ausführbaren Datei auf dem Datenträger. • 8 – Ändern einer ausführbaren Datei auf dem Datenträger.
	`MSG.Document`	Bulletin, das den Hash-Wert enthält
	`MSG.Path`	Pfad zum gesperrten Prozess
	`MSG.Profile`	Name des Profils, anhand dessen die Sperrung erfolgte
	`MSG.Rule`	Name der Regel, anhand derer die Sperrung erfolgte
	`MSG.SHA256`	Hash-Wert (SHA-256) des gesperrten Prozesses
	`MSG.StationTime`	Zeit der Workstation, zu der der Prozess gesperrt wurde
	`MSG.Target`	Pfad zum gesperrten Skript, wenn es um einen Hostprozess geht
	`MSG.TargetSHA256`	Hash-Wert (SHA-256) des gesperrten Skripts, wenn es um einen Hostprozess geht
	`MSG.TestMode`	Informationen darüber, ob der Testmodus aktiviert ist
	`MSG.User`	Benutzer, unter dem das gesperrte Objekt gestartet wurde

Die Anwendungskontrolle hat einen Prozess gesperrt

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn auf der Workstation eine Anwendung durch die Anwendungskontrolle gesperrt wurde.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.AppCtlAction`	Ausgeführte Aktion: • 0 – unbekannt. • 2 – gesperrt. • 3 – gesperrt (nicht gefunden in der Liste vertrauenswürdiger Anwendungen). • 5 – anhand von verbietenden Regeln gesperrt. • 7 – anhand von Richtlinieneinstellungen gesperrt.
	`MSG.AppCtlType`	Ereignistyp: • 0 – unbekannt. • 1 – Prozessstart. • 2 – Hostprozessstart. • 3 – Starten des Skript-Interpreters. • 4 – Laden des Moduls. • 5 – Laden des Treibers. • 6 – Starten des MSI-Installationsprogramms. • 7 – Erstellen einer neuen ausführbaren Datei auf dem Datenträger. • 8 – Ändern einer ausführbaren Datei auf dem Datenträger.
	`MSG.Path`	Pfad zum gesperrten Prozess
	`MSG.Profile`	Name des Profils, anhand dessen die Sperrung erfolgte
	`MSG.Rule`	Name der Regel, anhand derer die Sperrung erfolgte

Parameter	Wert	
	MSG.SHA256	Hash-Wert (SHA-256) des gesperrten Prozesses
	MSG.StationTime	Zeit der Workstation, zu der der Prozess gesperrt wurde
	MSG.Target	Pfad zum gesperrten Skript, wenn es um einen Hostprozess geht
	MSG.TargetSHA256	Hash-Wert (SHA-256) des gesperrten Skripts, wenn es um einen Hostprozess geht
	MSG.TestMode	Informationen darüber, ob der Testmodus aktiviert ist
	MSG.User	Benutzer, unter dem das gesperrte Objekt gestartet wurde

Eine Sicherheitsbedrohung wurde erkannt

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn eine Workstation gemeldet hat, dass Bedrohungen gefunden wurden. Im Text der Benachrichtigung werden ausführliche Informationen über die erkannten Bedrohungen angegeben.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	MSG.Action	Aktion, die beim Fund ausgeführt wurde
	MSG.Component	Name der Komponente
	MSG.InfectionType	Bedrohungsart
	MSG.ObjectName	Name des infizierten Objekts
	MSG.ObjectOwner	Besitzer des infizierten Objekts
	MSG.RunBy	Benutzer, unter dessen Konto die Komponente gestartet wurde
	MSG.ServerTime	Zeitpunkt des Empfangs des Ereignisses, GMT

Parameter	Wert	
	`MSG.Virus`	Bedrohungsname
	`GEN.ServerRecvLinkID`	UUID des letzten Nachbar-Servers, der die aktuelle Nachricht über die auf den mit ihm verbundenen Workstations erkannte Bedrohung gesendet hat (Der Wert ist leer, falls die Bedrohung auf den mit dem aktuellen Server verbundenen Workstations erkannt wurde)
	`GEN.ServerRecvLinkName`	Name des letzten Nachbar-Servers, der die aktuelle Nachricht über auf den mit ihm verbundenen Workstations erkannte Bedrohung gesendet hat (Der Wert ist leer, falls die Bedrohung auf den mit dem aktuellen Server verbundenen Workstations erkannt wurde)
	`GEN.ServerOriginatorID`	UUID des Servers, mit dem die Workstation, auf der die Bedrohung erkannt wurde, verbunden ist
	`GEN.ServerOriginatorName`	Name des Servers, mit dem die Workstation, auf der die Bedrohung erkannt wurde, verbunden ist

Es wurde eine Bedrohung anhand bekannter Hash-Werte von Bedrohungen erkannt

Parameter	Wert
Auslöser	Diese Benachrichtigung wird gesendet, wenn eine Workstation gemeldet hat, dass Bedrohungen anhand der bekannten Hash-Werte von Bedrohungen erkannt wurden. Im Text der Benachrichtigung werden ausführliche Informationen über die erkannten Bedrohungen angegeben.
Zusätzliche Einstellung	Die Benachrichtigung über den Fund anhand der Liste der bekannten Hash-Werte kann nur gesendet werden, wenn die Nutzung von Hash-Bulletins lizenziert ist (es reicht, dass mindestens eine entsprechende Lizenz in einem der vom Server verwendeten Lizenzschlüssel vorhanden ist).

Parameter	Wert	
	Ob die Lizenz vorhanden ist, finden Sie in Informationen zum Lizenzschlüssel, die im Parameter **Erlaubte Listen von Hash-Bulletins** unter **Lizenz-Manager** verfügbar sind (falls diese Funktion nicht lizenziert ist, ist dieser Parameter nicht vorhanden).	
Variablen	`MSG.Action`	Aktion, die beim Fund ausgeführt wurde
	`MSG.Component`	Name der Komponente
	`MSG.Document`	Bulletin, das den Hash-Wert der erkannten Bedrohung enthält
	`MSG.InfectionType`	Bedrohungsart
	`MSG.ObjectName`	Name des infizierten Objekts
	`MSG.ObjectOwner`	Besitzer des infizierten Objekts
	`MSG.RunBy`	Benutzer, unter dessen Konto die Komponente gestartet wurde
	`MSG.SHA1`	SHA1-Hash-Wert des erkannten Objekts
	`MSG.SHA256`	SHA256-Hash-Wert des erkannten Objekts
	`MSG.ServerTime`	Zeitpunkt des Empfangs des Ereignisses, GMT
	`MSG.Virus`	Bedrohungsname
	`GEN.ServerRecvLinkID`	UUID des letzten Nachbar-Servers, der die aktuelle Nachricht über die auf den mit ihm verbundenen Workstations erkannte Bedrohung gesendet hat (Der Wert ist leer, falls die Bedrohung auf den mit dem aktuellen Server verbundenen Workstations erkannt wurde)
	`GEN.ServerRecvLinkName`	Name des letzten Nachbar-Servers, der die aktuelle Nachricht über auf den mit ihm verbundenen Workstations erkannte Bedrohung gesendet hat

Parameter	Wert	
		(Der Wert ist leer, falls die Bedrohung auf den mit dem aktuellen Server verbundenen Workstations erkannt wurde)
	`GEN.ServerOriginatorID`	UUID des Servers, mit dem die Workstation, auf der die Bedrohung erkannt wurde, verbunden ist
	`GEN.ServerOriginatorName`	Name des Servers, mit dem die Workstation, auf der die Bedrohung erkannt wurde, verbunden ist

Fehler bei der Autorisierung einer Workstation

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn eine Workstation ungültige Anmeldeinformationen bei der Herstellung der Verbindung mit dem Server mitgeteilt hat. Weitere mögliche Aktionen werden in der Benachrichtigung aufgeführt.	
Zusätzliche Einstellung	Die Richtlinie für die Genehmigung von Workstations wird in der Einstellung **Registrierungsmodus für Newbies** unter **Administration** → **Dr.Web Server-Konfiguration** → **Allgemein** festgelegt.	
Variablen	`MSG.ID`	UUID der Workstation
	`MSG.Rejected`	Werte: • `rejected` – der Workstation wurde der Zugriff verweigert. • `newbie` – es wurde versucht, die Workstation zu „Newbie“ zu machen.
	`MSG.StationName`	Name der Workstation

Fehler beim Erstellen des Workstation-Kontos

Parameter	Wert
Auslöser	Diese Benachrichtigung wird gesendet, wenn ein Konto auf dem

Parameter	Wert	
	Server nicht erstellt werden kann. Einzelheiten werden im Protokoll des Servers angegeben.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.ID`	UUID der Workstation
	`MSG.StationName`	Name der Workstation

Fehler beim Scannen

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn eine Workstation gemeldet hat, dass ein Fehler beim Scannen aufgetreten ist.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.Component`	Name der Komponente
	`MSG.Error`	Fehlermeldung
	`MSG.ObjectName`	Name des Objekts
	`MSG.ObjectOwner`	Besitzer des Objekts
	`MSG.RunBy`	Benutzer, unter dessen Konto die Komponente gestartet wurde
	`MSG.ServerTime`	Zeitpunkt des Empfangs des Ereignisses, GMT
	`GEN.ServerRecvLinkID`	UUID des letzten Nachbar-Servers, von dem die Informationen über einen Fehler beim Scannen der mit ihm verbundenen Workstations empfangen wurden (Der Wert ist leer, falls der Fehler auf den mit dem aktuellen Server verbundenen Workstations aufgetreten ist)
	`GEN.ServerRecvLinkName`	Name des letzten Nachbar-Servers, der Informationen über einen Fehler beim Scannen der mit ihm verbundenen Workstations gesendet hat (Der Wert ist leer, falls der Scanfehler auf den mit

Parameter	Wert	
		dem aktuellen Server verbundenen Workstations aufgetreten ist)
	GEN.ServerOriginatorID	UUID des Servers, mit dem die Workstation, auf welcher der Scanfehler aufgetreten ist, verbunden ist
	GEN.ServerOriginatorName	Name des Servers, mit dem die Workstation, auf welcher der Scanfehler aufgetreten ist, verbunden ist

Kritischer Fehler bei der Aktualisierung einer Workstation

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn eine Workstation gemeldet hat, dass ein Fehler beim Update der Antivirenkomponenten über den Server aufgetreten ist.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	MSG.Product	Das zu aktualisierende Produkt
	MSG.ServerTime	Zeitpunkt (in lokaler Zeit), an dem der Server die Nachricht empfangen hat

Scanfehler beim Erkennen einer Bedrohung anhand bekannter Hash-Werte von Bedrohungen

Parameter	Wert
Auslöser	Die Benachrichtigung wird gesendet, wenn ein Scanfehler beim Erkennen einer Bedrohung aus der Liste der bekannten Hash-Werte aufgetreten ist.
Zusätzliche Einstellung	Die Benachrichtigung über den Fund anhand der Liste der bekannten Hash-Werte kann nur gesendet werden, wenn die Nutzung von Hash-Bulletins lizenziert ist (es reicht, dass mindestens eine entsprechende Lizenz in einem der vom Server verwendeten Lizenzschlüssel vorhanden ist). Ob die Lizenz vorhanden ist, finden Sie in Informationen zum Lizenzschlüssel, die im Parameter **Erlaubte Listen von Hash-**

Parameter	Wert	
	Bulletins unter **Lizenz-Manager** verfügbar sind (falls diese Funktion nicht lizenziert ist, ist dieser Parameter nicht vorhanden).	
Variablen	`MSG.Component`	Name der Komponente
	`MSG.Document`	Bulletin, das den Hash-Wert der erkannten Bedrohung enthält
	`MSG.Error`	Fehlermeldung
	`MSG.ObjectName`	Name des Objekts
	`MSG.ObjectOwner`	Besitzer des Objekts
	`MSG.RunBy`	Benutzer, unter dessen Konto die Komponente gestartet wurde
	`MSG.SHA1`	SHA1-Hash-Wert des erkannten Objekts
	`MSG.SHA256`	SHA256-Hash-Wert des erkannten Objekts
	`MSG.ServerTime`	Zeitpunkt des Empfangs des Ereignisses, GMT
	`GEN.ServerRecvLinkID`	UUID des letzten Nachbar-Servers, von dem die Informationen über einen Fehler beim Scannen der mit ihm verbundenen Workstations empfangen wurden (Der Wert ist leer, falls der Fehler auf den mit dem aktuellen Server verbundenen Workstations aufgetreten ist)
	`GEN.ServerRecvLinkName`	Name des letzten Nachbar-Servers, der Informationen über einen Fehler beim Scannen der mit ihm verbundenen Workstations gesendet hat (Der Wert ist leer, falls der Scanfehler auf den mit dem aktuellen Server verbundenen Workstations aufgetreten ist)
	`GEN.ServerOriginatorID`	UUID des Servers, mit dem die Workstation, auf welcher der Scanfehler aufgetreten ist, verbunden ist

Parameter	Wert	
	GEN.ServerOriginatorName	Name des Servers, mit dem die Workstation, auf welcher der Scanfehler aufgetreten ist, verbunden ist

Scanstatistik

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn eine Workstation gemeldet hat, dass der Scanvorgang abgeschlossen ist. Im Text der Benachrichtigung werden die Ergebnisse der Untersuchung angegeben.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	MSG.Component	Name der Komponente, die den Scanvorgang ausgeführt hat
	MSG.Cured	Anzahl desinfizierter Objekte
	MSG.DeletedObjs	Anzahl gelöschter Objekte
	MSG.Errors	Anzahl von Scan-Fehlern
	MSG.Infected	Anzahl infizierter Objekte
	MSG.Locked	Anzahl gesperrter Objekte
	MSG.Modifications	Anzahl der Objekte, die mit Virusmodifikationen infiziert sind
	MSG.Moved	Anzahl der in die Quarantäne verschobenen Objekte
	MSG.Renamed	Anzahl umbenannter Objekte
	MSG.RunBy	Benutzer, unter dessen Konto die Komponente gestartet wurde
	MSG.Scanned	Anzahl gescannter Objekte
	MSG.ServerTime	Zeitpunkt des Empfangs des Ereignisses, GMT
	MSG.Speed	Verarbeitungsrate in KB/s

Parameter	Wert	
	MSG.Suspicious	Anzahl verdächtiger Objekte
	MSG.VirusActivity	
	GEN.ServerRecvLinkID	UUID des letzten Nachbar-Servers, der die Scanstatistik für die mit ihm verbundenen Workstations gesendet hat (Der Wert ist leer, falls die Scanstatistik von den mit dem aktuellen Server verbundenen Workstations erhalten wurde)
	GEN.ServerRecvLinkName	Name des letzten Nachbar-Servers, von dem die Statistik zum Scan der mit ihm verbundenen Workstations empfangen wurde (Der Wert ist leer, falls die Scanstatistik von den mit dem aktuellen Server verbundenen Workstations erhalten wurde)
	GEN.ServerOriginatorID	UUID des Servers, mit dem die Workstation, von der die Scanstatistik erhalten wurde, verbunden ist
	GEN.ServerOriginatorName	Name des Servers, mit dem die Workstation, von der die Scanstatistik erhalten wurde, verbunden ist

Unbekannte Workstation

Parameter	Wert	
Auslöser	Die Benachrichtigung wird gesendet, falls eine neue Workstation, welche die Verbindung mit dem Server angefordert hat, weder genehmigt noch abgelehnt wurde.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	MSG.ID	UUID der unbekannten Workstation
	MSG.Rejected	Werte: • rejected – der Workstation wurde der Zugriff verweigert.

Parameter	Wert	
		• `newbie` – es wurde versucht, die Workstation zu „Newbie“ zu machen.
	`MSG.StationName`	Name der Workstation

Verbindungsabbruch

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, falls die Verbindung mit einem Client (darunter einer Workstation, einem Agent-Installationsprogramm, einem Nachbar-Server oder Proxyserver) abgebrochen wurde.	
Zusätzliche Einstellung	Damit Benachrichtigungen über Verbindungsabbrüche gesendet werden können, müssen das Kontrollkästchen **Verbindungsabbrüche** im Bereich **Administration** → **Dr.Web Server-Konfiguration** → **Statistik** aktiviert und die dazugehörigen Parameter festgelegt sein.	
Variablen	`MSG.Total`	Anzahl von Verbindungsabbrüchen
	`MSG.Type`	Typ des Clients

Workstation ist bereits registriert

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn eine Workstation, deren ID mit der ID einer mit dem Server bereits verbundenen Workstation übereinstimmt, versucht, eine Verbindung mit diesem Server herzustellen.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.ID`	UUID der Workstation
	`MSG.Server`	ID des Servers, auf dem die Workstation registriert wurde
	`MSG.StationName`	Name der Workstation

Workstation hat lange keine Verbindung mehr mit dem Server hergestellt

Parameter	Wert	
Auslöser	Die Benachrichtigung wird entsprechend der Aufgabe im Zeitplan des Servers verschickt und enthält Informationen darüber, dass eine Workstation lange Zeit keine Verbindung mehr mit diesem Server hergestellt hat. Das Datum der letzten Verbindung wird im Text der Benachrichtigung angegeben.	
Zusätzliche Einstellung	Zeitraum, in dem die Workstation keine Verbindung mit dem Server herstellen soll, damit die Benachrichtigung gesendet wird, wird in der Aufgabe **Workstation hat lange keine Verbindung mehr mit dem Server hergestellt** im Zeitplan des Servers unter **Administration** → **Dr.Web Server-Aufgabenplaner** festgelegt.	
Variablen	Die oben aufgeführten gemeinsamen Variablen für Windows können nicht verwendet werden.	
	`MSG.DaysAgo`	Anzahl der Tage seit der letzten Verbindung mit dem Server
	`MSG.LastSeenFrom`	Adresse, von der aus die Workstation die Verbindung mit dem Server zuletzt hergestellt hat
	`MSG.StationDescription`	Beschreibung der Workstation
	`MSG.StationID`	UUID der Workstation
	`MSG.StationMAC`	MAC-Adresse der Workstation
	`MSG.StationName`	Name der Workstation
	`MSG.StationSID`	Sicherheits-ID der Workstation

Workstation muss neu gestartet werden

Parameter	Wert
Auslöser	Die Benachrichtigung wird gesendet, wenn die Workstation aus einem der folgenden Gründe neu gestartet werden muss: • Abschließen der Desinfizierung • Anwenden der Updates • Ändern des Status der hardwareunterstützten Virtualisierung • Abschließen der Desinfizierung und Anwenden der Updates • Abschließen der Desinfizierung und Ändern des Status der

Parameter	Wert	
	hardwareunterstützten Virtualisierung • Anwenden der Updates und Ändern des Status der hardwareunterstützten Virtualisierung • Abschließen der Desinfizierung, Anwenden der Updates und Ändern des Status der hardwareunterstützten Virtualisierung	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	`MSG.Reason`	Grund für den Neustart Alle möglichen Ursachen sind in der vordefinierten Vorlage aufgelistet

Workstation wurde automatisch genehmigt

Parameter	Wert
Auslöser	Die Benachrichtigung wird gesendet, falls eine neue Workstation, welche die Verbindung mit dem Server angefordert hat, vom Server automatisch genehmigt wurde.
Zusätzliche Einstellung	Diese Situation ist möglich, wenn unter **Administration** → **Dr.Web Server-Konfiguration** → **Allgemein** in der Dropdown-Liste **Registrierungsmodus für Newbies** die Option **Zugriff automatisch erlauben** ausgewählt ist.
Variablen	Keine.

Workstation wurde vom Administrator genehmigt

Parameter	Wert	
Auslöser	Die Benachrichtigung wird gesendet, wenn eine neue Workstation, welche die Verbindung mit dem Server angefordert hat, vom Administrator manuell genehmigt wurde.	
Zusätzliche Einstellung	Diese Situation ist möglich, wenn unter **Administration** → **Dr.Web Server-Konfiguration** → **Allgemein** in der Dropdown-Liste **Registrierungsmodus für Newbies** die Option **Zugriff manuell bestätigen** ausgewählt ist, und der Administrator für die Workstation die Option **Antivirus-Netzwerk** → **Nicht genehmigte Workstations** → **Ausgewählte Workstations genehmigen und Primärgruppe festlegen** ausgewählt hat.	
Variablen	`MSG.AdminAddress`	Netzwerkadresse des

Parameter	Wert	
		Verwaltungscenters
	MSG.AdminName	Administratorname

Zum Anwenden der Updates ist ein Neustart der Workstation erforderlich

Parameter	Wert	
Auslöser	Diese Benachrichtigung wird gesendet, wenn eine Workstation gemeldet hat, dass ein Produkt installiert oder aktualisiert wurde und ein Neustart erforderlich ist.	
Zusätzliche Einstellung	Nicht erforderlich.	
Variablen	MSG.Product	Das zu aktualisierende Produkt
	MSG.ServerTime	Zeitpunkt (in lokaler Zeit), an dem der Server die Nachricht empfangen hat

Anhang E. Spezifikation zur Schreibweise von Netzwerkadressen

In dieser Spezifikation werden die folgenden Konventionen verwendet:

- Variablen (Felder, die jeweils durch bestimmte Werte ersetzt werden müssen) werden in spitze Klammern gesetzt und kursiv geschrieben.
- Permanenter Text (bleibt nach dem Ersatz erhalten) wird in einer Festbreitenschrift geschrieben.
- Optionale Elemente werden in eckige Klammern gesetzt.
- Links von der Zeichenfolge `::=` befindet sich der zu definierende Begriff, rechts ist die Definition (wie in der Backus-Naur-Form).

E1. Allgemeines Adressformat

Die Netzwerkadresse hat das folgende Format:

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

Die Variable *<protocol>* hat standardmäßig den Wert `TCP`. Der Standardwert der Variablen *<protocol-specific-part>* variiert je nach Anwendung.

Das alte Adressformat ist zulässig:

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

IP-Adressen

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

  <ip-address> kann ein DNS-Name oder eine durch Punkte getrennte IP-Adresse sein (z. B. `127.0.0.1`).

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

  <port-number> muss eine Dezimalzahl enthalten.

Wenn Sie eine Serveradresse und die Adresse eines Agents angeben, können Sie auch die Version des verwendeten Protokolls mit angeben. Möglich sind folgende Optionen:

- *<protocol>*`://`*<interface>*`:`*<port-number>* – IPv4 und IPv6 verwenden.
- *<protocol>*`://(`*<interface>*`):`*<port-number>* – nur IPv4 verwenden.
- *<protocol>*`://[`*<interface>*`]:`*<port-number>* – nur IPv6 verwenden.

Beispiel:

1. `tcp://127.0.0.1:2193`

   steht für das `TCP`-Protokoll und den Port `2193` an der Schnittstelle `127.0.0.1`.

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

   steht für das `TCP`-Protokoll und den Port `2193` an der IPv4-Schnittstelle `example.com`.

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

   steht für das `TCP`-Protokoll und den Port `2193` an der IPv6-Schnittstelle `0000.0000.0000.0000.0000.0000.0000.0000`

4. `localhost:2193`

   Siehe oben.

5. `tcp://:9999`

   Wert für den Server: Standardschnittstelle, die von der Anwendung abhängt (normalerweise alle verfügbaren Schnittstellen), Port `9999`; Wert für den Client: Verbindung mit dem Standardhost, der von der Anwendung abhängt (normalerweise `localhost`), Port `9999`.

6. `tcp://`

   TCP-Protokoll, Standardport.

Verbindungsorientiertes Protokoll

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

Das Feld *<socket-address>* legt die lokale Socketadresse für den Server oder einen Remote-Server für den Client fest.

Datagramm-orientiertes Protokoll

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

Beispiel:

1. `udp://231.0.0.1:2193`

   bedeutet, dass die Multicast-Gruppe `231.0.0.1:2193` an der von der Anwendung abhängigen Standardschnittstelle verwendet wird.

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

   bedeutet, dass die Multicast-Gruppe `[ff18::231.0.0.1]` an der von der Anwendung anhängigen Standardschnittstelle verwendet wird.

3. `udp://`

   ist die von der Anwendung anhängige Schnittstelle und ein Endpunkt.

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

   Verwendung von Broadcast-Nachrichten am Port `9999` an der Schnittstelle `myhost1`.

UDS-Adressen

- Verbindungsorientiertes Protokoll:

  `unx://`*<file_name>*

- Datagramm-orientiertes Protokoll:

udx://<*file_name*>

Beispiel:

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

SRV-Adressen

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

E2. Adressen des Dr.Web Agents und des Installationsprogramms

Direkte Verbindung mit dem Dr.Web Server

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

Standardmäßig, je nach <*connection-protocol*>:

- tcp://127.0.0.1:2193

  wobei 127.0.0.1 für Loopback und 2193 für den Port stehen.
- tcp://[::1]:2193

  wobei [::1] für Loopback (IPv6) und 2193 für den Port stehen.

Suche nach dem Server <drwcs-name>, der das angegebene Protokoll und den Endpunkt verwendet

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

Standardmäßig, je nach <*datagram-protocol*>:

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

  Suche nach dem Server mit dem Namen drwcs für die TCP-Verbindung, welche die Multicast-Gruppe 231.0.0.1:2193 an allen Schnittstellen verwendet.

Anhang F. Repository verwalten

Das Repository sollte über die Einstellungen des Verwaltungscenters verwaltet werden. Weitere Informationen finden Sie im **Administratorhandbuch** unter Dr.Web Server-Repository verwalten.

Die Einstellungen des Repository werden in folgenden Konfigurationsdateien gespeichert:

- Allgemeine Konfigurationsdateien befinden sich im Wurzel des Repository-Verzeichnisses und legen die Parameter für die Update-Server fest.
- Konfigurationsdateien von Produkten befinden sich in der Wurzel der Verzeichnisse der im Repository verfügbaren Produkte. Sie bestimmen den Umfang von Dateien und die Einstellungen für das Update des jeweiligen Produkts.

Wenn Sie mit der Bearbeitung der Konfigurationsdateien fertig sind, starten Sie den Server neu.

Bei der Konfiguration einer Server-zu-Server-Kommunikation (mehr dazu finden Sie im Dokument **Administratorhandbuch** unter Besonderheiten eines Netzwerks mit mehreren Servern) für die Spiegelung von Produkten müssen Sie berücksichtigen, dass die Konfigurationsdateien kein Teil des jeweiligen Produkts sind und nicht vom Spiegelungssystems verarbeitet werden. Um eventuelle Fehler beim Update zu vermeiden, folgen Sie diesen Empfehlungen:

- Verwenden Sie die gleiche Konfiguration für gleichberechtigte Server.
- Deaktivieren Sie für die untergeordneten Server die Synchronisierung der Komponenten über das HTTP-Protokoll oder verwenden Sie die gleiche Konfiguration.

F1. Allgemeine Konfigurationsdateien

.servers

Die Datei `.servers` enthält eine Liste der Server, die im Repository des Dr.Web Servers zum Update der Komponenten von Dr.Web Enterprise Security Suite über das GUS verwendet werden.

Server in der Liste werden hintereinander abgerufen. Wenn die Aktualisierung erfolgreich abgeschlossen ist, wird der Abrufvorgang beendet.

Beispiel:

```
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

Die Datei `.url` enthält den Basis-URI der Updatezone, und zwar den des Verzeichnisses auf den Update-Servern, in dem sich die Updates für das jeweilige Dr.Web Produkt befinden.

Beispiel:

```
update
```

.proto

Die Datei `.proto` enthält den Namen des Protokolls, über das die Updates von den Update-Servern übertragen werden.

Folgende Werte sind möglich: `http | https | ftp | ftps | sftp | scp | smb | smbs | file`.

Die Protokolle `smb` und `smbs` sind nur für Server unter UNIX-basierten Betriebssystemen verfügbar.

Beispiel:

```
https
```

.auth

Die Datei `.auth` enthält die Parameter für die Autorisierung des Benutzers am Update-Server.

Die Parameter werden im folgenden Format angegeben:

```
<Benutzername>

<Passwort>
```

Der Benutzername ist ein obligatorischer Parameter, die Angabe des Passworts ist hingegen optional.

Beispiel:

```
admin

root
```

.delivery

Die Datei `.delivery` enthält die Parameter für die Übertragung von Updates über das GUS.

Parameter	Mögliche Werte	Erläuterung
`cdn`	`on | off`	Der Parameter legt fest, ob Content Delivery Network beim Laden des Repository verwendet werden soll: • `on` – CDN verwenden. • `off` – CDN nicht verwenden.
`cert`	`drweb | valid | any | custom`	Zulässige SSL-Zertifikate der Update-Server, die automatisch angenommen werden: • `drweb` – nur SSL-Zertifikate von Doctor Web annehmen. • `valid` – nur gültige SSL-Zertifikate annehmen. • `any` – alle Zertifikate annehmen. • `custom` – nur vom Benutzer angegebene Zertifikate annehmen.
`cert-path`		Pfad zum benutzerdefinierten Zertifikat, wenn der Wert `custom` für den Parameter `cert` festgelegt ist.
`ssh-mode`	`pwd | pubkey`	Autorisierungsmodus bei der Verwendung der Protokolle `scp` und `sftp` (*ssh2*-basiert): • `pwd` – Autorisierung mit dem Anmeldenamen und Passwort. • `pubkey` – Autorisierung mit Schlüsseln.
`ssh-pubkey`		Pfad zum öffentlichen SSH-Schlüssel des Update-Servers
`ssh-prikey`		Pfad zum privaten SSH-Schlüssel des Update-Servers

F2. Konfigurationsdateien von Produkten

.description

Die Datei `.description` legt den Produktnamen fest. Wenn diese Datei fehlt, wird als Produktname der Name des entsprechenden Produktverzeichnisses verwendet.

Beispiel:

```
Dr.Web Server
```

.sync-off

Die Datei deaktiviert das Update des Produkts. Der Inhalt der Datei kann beliebig sein.

Ausnahmedateien beim Update des Repository über das GUS

.sync-only

Die Datei `.sync-only` enthält die durch reguläre Ausdrücke festgelegten Dateien des Repository, die beim Update über das GUS synchronisiert werden sollen. Dateien des Repository, die in der Datei `.sync-only` nicht angegeben sind, werden nicht synchronisiert. Wenn die Datei `.sync-only` fehlt, erfolgt die Synchronisierung aller Dateien des Repository, außer denjenigen, die entsprechend den Parametern in der Datei `.sync-ignore` nicht synchronisiert werden sollen.

.sync-ignore

Die Datei `.sync-ignore` enthält die durch reguläre Ausdrücke festgelegten Dateien des Repository, die beim Update über das GUS nicht synchronisiert werden sollen.

Beispiel für eine Datei mit Ausnahmen

```
^windows-nt-x64/

^windows-nt/

^windows/
```

Priorität der Konfigurationsdateien

Wenn das Produkt die Dateien `.sync-only` und `.sync-ignore` enthält, werden sie folgendermaßen verwendet:

1. Zuerst wird die Datei `.sync-only` verarbeitet. Die in der Liste der Datei `.sync-only` nicht aufgezählten Dateien werden nicht verarbeitet.
2. Alle anderen Dateien werden entsprechend den Parametern in der Datei `.sync-ignore` verarbeitet.

Ausnahmedateien beim Update der Agents über den Server

.state-only

Die Datei `.state-only` enthält die durch reguläre Ausdrücke festgelegten Dateien des Repository, die beim Update der Agents über den Server synchronisiert werden sollen. Dateien, die in der Datei `.state-only` nicht angegeben sind, werden nicht synchronisiert. Wenn die Datei `.state-only` fehlt, erfolgt die Synchronisierung aller Dateien des Repository, außer denjenigen, die entsprechend den Parametern in der Datei `.state-ignore` nicht synchronisiert werden sollen.

.state-ignore

Die Datei `.state-ignore` enthält die durch reguläre Ausdrücke festgelegten Dateien, die beim Update der Agents über den Server nicht synchronisiert werden sollen.

Beispiel:

- Keine deutschen, chinesischen und spanischen Sprachressourcen für die Benutzeroberfläche erhalten (alle anderen verfügbaren Sprachressourcen werden aktualisiert).
- Keine Komponenten für 64-Bit-Versionen von Windows erhalten.

```
;^common/ru-.*\.dwl$ dies wird aktualisiert

^common/de-.*\.dwl$

^common/cn-.*\.dwl$

^common/es-.*\.dwl$

^win/de-.*

^win/cn-.*

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

Die Dateien `.state-only` und `.state-ignore` haben die gleiche Priorität wie `.sync-only` und `.sync-ignore`.

Versand von Benachrichtigungen konfigurieren

Durch die Dateien der Gruppe `notify` können Sie festlegen, wie Benachrichtigungen über erfolgreiche Aktualisierungen bestimmter Produkte versendet werden.

Diese Einstellungen betreffen nur die Benachrichtigung **Produkt wurde aktualisiert** und haben keine Auswirkung auf andere Typen von Benachrichtigungen.

Die Konfiguration des Benachrichtigungssystems wird im **Administratorhandbuch** unter Benachrichtigungen konfigurieren beschrieben.

.notify-only

Die Datei `.notify-only` enthält eine Liste der Dateien des Repository, deren Änderung gemeldet werden soll.

.notify-ignore

Die Datei `.notify-ignore` enthält eine Liste der Dateien des Repository, deren Änderung nicht gemeldet werden soll.

Priorität der Konfigurationsdateien

Wenn das Produkt die Dateien `.notify-only` und `.notify-ignore` enthält, werden sie folgendermaßen verwendet:

1. Beim Update des Produkts werden die über das GUS aktualisierten Dateien mit den Dateien in der Ausnahmeliste verglichen.
2. Zuerst werden die Dateien ausgeschlossen, die in der Datei `.notify-ignore` enthalten sind.
3. Von übrig gebliebenen Dateien werden dann die Dateien ausgeschlossen, die in der Datei `.notify-only` nicht enthalten sind.
4. Wenn noch einige Dateien übrig geblieben sind, werden Benachrichtigungen gesendet.

Falls die Dateien `.notify-only` und `.notify-ignore` fehlen, werden Benachrichtigungen immer gesendet (sofern sie auf der Seite **Konfiguration von Benachrichtigungen** im Verwaltungscenter aktiviert sind).

Beispiel:

Wenn die Datei `.notify-ignore` die Ausnahme `^.vdb.lzma$` hat, wird keine Benachrichtigung verschickt, falls nur die Virendatenbanken aktualisiert wurden. Wenn neben der Virendatenbanken auch die Engine `drweb32.dll` aktualisiert wurde, wird die Benachrichtigung gesendet.

Vorübergehende Sperrung konfigurieren

.delay-config

Die Datei `.delay-config` enthält die Einstellungen für die Sperrung von Produkten. Das Repository verteilt dabei weiterhin vorherige Revisionen, und keine Synchronisierung erfolgt (das Produkt wird für das Update gesperrt). Wenn der Administrator glaubt, dass die erhaltene Revision zur Verteilung geeignet ist, muss er im Verwaltungscenter ihre Verteilung zulassen (mehr dazu finden Sie im **Administratorhandbuch** unter Dr.Web Server-Repository verwalten).

Die Datei enthält zwei durch Semikolon getrennte Parameter, bei denen nicht auf die Groß-/Kleinschreibung geachtet wird.

Dateiformat:

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

Parameter	Mögliche Werte	Erläuterung
`Delay`	`ON|OFF`	• `ON` – Sperrung von Produkt-Updates ist aktiviert. • `OFF` – Sperrung von Produkt-Updates ist deaktiviert.
`UseFilter`	`YES|NO`	• `Yes` – Produkt-Updates nur dann sperren, wenn die aktualisierten Dateien mit den Ausnahmen in der Datei `.delay-only` übereinstimmen. • `No` – Produkt-Updates immer sperren.

Beispiel:

```
Delay ON; UseFilter NO
```

.delay-only

Die Datei `.delay-only` enthält eine Liste der Dateien, bei deren Änderung das Produkt nicht auf eine neue Revision aktualisiert werden darf. Die Dateien müssen mithilfe regulärer Ausdrücke angegeben werden.

Wenn eine Datei des Repository-Updates mit den angegebenen Mustern übereinstimmt, und die Einstellung `UseFilter` in der Datei `.sync-only` aktiviert ist, wird die Revision gesperrt.

.rev-to-keep

In der Datei `.rev-to-keep` ist die Anzahl der zu speichernden Revisionen angegeben.

Beispiel:

```
3
```

Anhang G. Format der Konfigurationsdateien

In diesem Anhang wird das Format der folgenden Dateien beschrieben:

Datei	Erläuterung
drwcsd.conf	Konfigurationsdatei des Dr.Web Servers.
webmin.conf	Konfigurationsdatei des Dr.Web Sicherheitscenters.
download.conf	Konfigurationsdatei für den Datendownload vom Server.
drwcsd-proxy.conf	Konfigurationsdatei des Dr.Web Proxyservers.
drwreploader.conf	Konfigurationsdatei des Dr.Web Repository Loaders.

Wenn auf dem Rechner mit der entsprechenden Komponente ein Dr.Web Agent mit der aktivierten Selbstschutzfunktion installiert ist, deaktivieren Sie zuerst in den Einstellungen des Agents die Komponente Dr.Web Selbstschutz, bevor Sie mit dem Bearbeiten der Konfigurationsdatei beginnen.

Nachdem alle Änderungen übernommen sind, empfiehlt es sich, die Komponente Dr.Web Selbstschutz wieder zu aktivieren.

G1. Konfigurationsdatei des Dr.Web Servers

Die Konfigurationsdatei des Dr.Web Servers `drwcsd.conf` befindet sich standardmäßig im Unterverzeichnis `etc` des Wurzelverzeichnisses des Servers. Wenn der Server über die Befehlszeile gestartet wird, kann für die Konfigurationsdatei ein anderer Speicherort und Name festgelegt werden (mehr dazu finden Sie unter H3. Dr.Web Server).

So bearbeiten Sie die Konfigurationsdatei des Dr.Web Servers

1. Beenden Sie den Dr.Web Server (mehr dazu finden Sie im **Administratorhandbuch** unter Dr.Web Server starten und beenden).
2. Deaktivieren Sie den Selbstschutz (wenn diese Komponente des Agents aktiv ist, erfolgt die Deaktivierung über das Kontextmenü des Agents).
3. Nehmen Sie alle gewünschten Änderungen an der Konfigurationsdatei des Servers vor.
4. Starten Sie den Dr.Web Server (mehr dazu finden Sie im **Administratorhandbuch** unter Dr.Web Server starten und beenden).

Format der Konfigurationsdatei des Dr.Web Servers

Die Konfigurationsdatei des Servers hat das XML-Format.

Parameter der Konfigurationsdatei des Dr.Web Servers:

- `<version value="" />`

  Aktuelle Version der Konfigurationsdatei.

- `<name value="" />`

  Name des Dr.Web Servers oder des Clusters von Dr.Web Servern, auf den die Agents, die Installationsprogramme der Agents oder des Verwaltungscenters bei der Suche zugreifen sollen. Lassen Sie den Parameter leer ('' - wird standardmäßig verwendet), um den Namen des Rechners zu verwenden, auf dem der Server installiert ist.

- `<id value="" />`

  Eindeutige ID des Servers. In früheren Versionen wurde die ID im Lizenzschlüssel des Servers gespeichert. Ab Version 10 wird sie in der Konfigurationsdatei des Servers gespeichert.

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

  Standort des Servers.

  Beschreibung der Attribute:

Attribut	Erläuterung
city	Stadt
country	Land
department	Name der Abteilung
floor	Etage
latitude	Breite
longitude	Länge
organization	Name des Unternehmens
province	Region
room	Raum
street	Straße

- `<threads count="" />`

Anzahl von Threads zur Verarbeitung von Daten der Agents. Der Minimalwert beträgt 5, der Standardwert ist 5. Dieser Parameter hat Einfluss auf die Leistung des Servers. Es wird dringend davon abgeraten, den Wert dieses Parameters zu ändern.

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

  Zugriffsmodus für neue Workstations.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`approve-to-group`	-	Gruppe, die im Modus **Zugriff automatisch erlauben** (`mode='open'`) als Standard-Primärgruppe für neue Workstations festgelegt werden soll.	Wenn kein Wert angegeben ist, wird die Gruppe **Everyone** als Primärgruppe verwendet.
`default-rate`	-	Für AV-Desk. Gruppe, die im Modus **Zugriff automatisch erlauben** (`mode='open'`) als Standard-Tarifgruppe für neue Workstations festgelegt werden soll.	Wenn kein Wert angegeben ist, wird die Tarifgruppe **Dr.Web Premium** festgelegt.
`mode`	• open – Zugriff automatisch erlauben. • closed – Zugriff immer verweigern. • approval – Zugriff manuell genehmigen.	Richtlinie für die Genehmigung neuer Workstations.	-

  Mehr dazu finden Sie im **Administratorhandbuch** unter Richtlinie für die Genehmigung von Workstations.

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

  Modus, in dem Workstation-Konten bei der Installation der Agents mithilfe eines Gruppen-Installationspakets im Verwaltungscenter erstellt werden sollen, wenn die vorhandenen Konten nicht ausreichen.

Attribut	Zulässige Werte	Standardmäßig
`enabled`	• `yes` – fehlende Konten für Workstations automatisch erstellen. • `no` – Installation ist nur für die Anzahl der vorhandenen Konten in der Gruppe möglich, für deren Workstations das Installationspaket gestartet wird.	`yes`

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

Bestimmt, wie nicht autorisierte Workstations behandelt werden. Mögliche Werte des Attributs `enabled`:

- `yes` – Nicht autorisierte Workstations (z. B. aufgrund eines Datenbankfehlers) erhalten automatisch den Newbie-Status.
- `no` (standardmäßig) – Normalmodus.

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

  Maximale Anzahl von Workstations in der Warteschlange zur Autorisierung am Server. Es wird dringend davon abgeraten, den Wert dieses Parameters zu ändern.

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

  IP-Adressen durch DNS-Namen von Rechnern in der Protokolldatei des Dr.Web Servers ersetzen. Mögliche Werte des Attributs `enabled`:

  - `yes` – DNS-Namen anzeigen.
  - `no` (standardmäßig) – IP-Adressen anzeigen.

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

  NetBIOS-Namen durch DNS-Namen von Rechnern ersetzen. Mögliche Werte des Attributs `enabled`:

  - `yes` – DNS-Namen anzeigen.
  - `no` (standardmäßig) – NetBIOS-Namen anzeigen.

- **`<dns>`**

  DNS-Einstellungen.

  `<timeout value="" />`

  Zeitlimit (in Sekunden) für die Auflösung von direkten/inversen DNS-Anfragen. Wenn kein Wert angegeben ist, gibt es kein Zeitlimit für die Auflösung.

  `<retry value="" />`

  Maximale Anzahl von DNS-Wiederholungsanfragen bei der fehlgeschlagenen Auflösung einer DNS-Anfrage.

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

  Dauer, für welche die Antworten des DNS-Servers im Cache gespeichert werden sollen.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung
`enabled`	• `yes` – Antworten im Cache speichern. • `no` – keine Antworten im Cache speichern.	Modus, mit dem die Antworten im Cache gespeichert werden sollen.
`negative-ttl`	-	Zeitraum für die Speicherung im Cache (TTL) negativer Antworten des DNS-Servers in Minuten.

Attribut	Zulässige Werte	Erläuterung
positive-ttl	-	Zeitraum für die Speicherung im Cache (TTL) positiver Antworten des DNS-Servers in Minuten.

<servers>

Liste der DNS-Server, welche die Standard-Systemliste ersetzen soll. Diese enthält ein oder mehrere untergeordnete Elemente <server address="" />, in denen der Parameter address für die IP-Adresse des Servers steht.

<domains>

Liste der DNS-Domänen, welche die Standard-Systemliste ersetzen soll. Diese enthält ein oder mehrere untergeordnete Elemente <domain name="" />, in denen der Parameter name für den Namen der Domäne steht.

- <cache>

  Cache-Einstellungen.

  Das Element <cache> enthält folgende untergeordnete Elemente:

  - <interval value="" />

    Häufigkeit, mit welcher der Cache vollständig gelöscht wird.

  - <quarantine ttl="" />

    Zeitintervall (in Sekunden), in dem Dateien aus der Quarantäne des Servers gelöscht werden. Der Standardwert ist 604800 (eine Woche).

  - <download ttl="" />

    Zeitintervall (in Sekunden), in dem individuelle Installationspakete gelöscht werden. Der Standardwert ist 604800 (eine Woche).

  - <repository ttl="" />

    Zeitintervall, in dem die Dateien im Cache des Server-Repository gelöscht werden.

  - <file ttl="" />

    Zeitintervall (in Sekunden), in dem der Dateicache gelöscht wird. Der Standardwert ist 604800 (eine Woche).

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

  Beschreibungen von Workstations auf dem Dr.Web Server mit dem Feld **Computer description** auf der Seite **System properties** auf den Workstations synchronisieren. Mögliche Werte des Attributs enabled:

  - yes – Beschreibung auf dem Server durch die Beschreibung auf der Workstation ersetzen.
  - no (Standardwert) – Beschreibung auf der Workstation ignorieren.

- <time-discrepancy value="" />

  Zulässige Differenz zwischen der Systemzeit des Dr.Web Servers und der Zeit der Dr.Web Agents in Minuten. Wenn die Differenz mehr als hier angegeben ist, wird dies in dem Status der

Workstation auf dem Dr.Web Server vermerkt. Der Standardwert beträgt 3 Minuten. Wenn kein Wert oder 0 angegeben ist, findet keine Überprüfung statt.

- `<encryption mode="" />`

  Verschlüsselungsmodus für den Datenverkehr. Zulässige Werte des Attributs `mode`:

  - `yes` – Verschlüsselung verwenden.
  - `no` – keine Verschlüsselung verwenden.
  - `possible` – Verschlüsselung ist möglich.

  Der Standardwert ist `yes`.

  Weitere Informationen hierzu finden Sie im **Administratorhandbuch** unter Verschlüsselung und Komprimierung des Datenverkehrs.

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

  Komprimierungsmodus für den Datenverkehr.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung
`level`	Ganzzahl von 1 bis 9.	Komprimierungsgrad.
`mode`	• `yes` – Komprimierung verwenden. • `no` – keine Komprimierung verwenden. • `possible` – Komprimierung ist möglich.	Komprimierungsmodus.

  Weitere Informationen hierzu finden Sie im **Administratorhandbuch** unter Verschlüsselung und Komprimierung des Datenverkehrs.

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

  Aufgabenausführung auf Workstations verfolgen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Status von Workstations überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Status der Virendatenbanken überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Mögliche Werte des Attributs `enabled`: `yes` oder `no`. Der Parameter wird ignoriert, wenn `<track-agent-status enabled="no" />`.

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

  Versionen der Module von Workstations überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Liste der auf Workstations installierten Komponenten überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Benutzersitzungen auf Workstations überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Die auf Workstations installierte Hardware und Software überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Start und Beenden von installierten Antivirenkomponenten überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Erkannte Bedrohungen überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Fehler beim Scannen von Workstations überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Scanstatistik überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Installationen von Agents überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Überwachung der von der Komponente Office Control gesperrten Geräte zulassen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled`: `yes` oder `no`.

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

  Aktivitäten der Prozesse auf Workstations überwachen, die von der Anwendungskontrolle registriert wurden (um sie in die Anwendungsliste aufzunehmen), und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled`: `yes` oder `no`.

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

  Sperrungen der Prozesse auf Workstations durch die Anwendungskontrolle überwachen, und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled`: `yes` oder `no`.

- `<quarantine enabled="" />`

  Status der Quarantänen auf Workstations überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled`: `yes` oder `no`.

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

Maximale Übertragungsrate (in KB/s) für die Übertragung von Updates zwischen dem Server und den Agents.

Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`queue-size`	• Positive ganze Zahl. • `unlimited`.	Maximale Anzahl an Update-Sitzungen, die vom Server aus gleichzeitig gestartet werden können. Wenn der festgelegte Wert erreicht ist, werden Anfragen der Agents in die Warteschlange gestellt. Die Warteschlangengröße ist unbegrenzt.	`unlimited`
`value`	• Maximale Übertragungsrate in KB/s. • `unlimited`.	Maximale Gesamtübertragungsrate für die Übertragung von Updates.	`unlimited`

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

  Maximale Übertragungsrate (in KB/s), mit welcher der Server Daten bei der Installation von Agents überträgt.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`queue-size`	• Positive ganze Zahl. • `unlimited`.	Maximale Anzahl der Installationsvorgänge von Agents, die vom Server aus gleichzeitig gestartet werden können. Wenn der festgelegte Wert erreicht ist, werden Anfragen der Agents in die Warteschlange gestellt. Die Warteschlangengröße ist unbegrenzt.	`unlimited`
`value`	• Maximale Übertragungsrate in KB/s. • `unlimited`.	Maximale Gesamtübertragungsrate, mit der Daten bei der Installation von Agents übertragen werden.	`unlimited`

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

  Informationen zum Standort von Workstations zwischen den Dr.Web Servern synchronisieren.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung
`enabled`	• `yes` – Synchronisierung zulassen. • `no` – Synchronisierung deaktivieren.	Synchronisierungsmodus.

Attribut	Zulässige Werte	Erläuterung
`startup-sync`	Positive ganze Zahl.	Anzahl von Workstations ohne geographische Koordinaten, über die Informationen bei der Herstellung der Verbindung zwischen Dr.Web Servern angefordert werden.

- `<audit enabled="" />`

  Aktionen des Administrators im Dr.Web Sicherheitscenter überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Innere Vorgänge des Dr.Web Servers überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Web-API-Vorgänge überwachen und diese Informationen in der Datenbank des Servers aufzeichnen. Zulässige Werte des Attributs `enabled` sind: `yes` oder `no`.

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

  Einstellungen für die Verbindung mit dem Dr.Web Server über HTTP-Proxyserver.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung

`auth-list`	• `none` – Keine Autorisierung verwenden.
	• `any` – beliebige unterstützte Methode.
	• `safe` – beliebige unterstützte sichere Methode.
	• Folgende Methoden (mehrere Methoden müssen durch Leerzeichen voneinander getrennt werden):
	  ▫ `basic`
	  ▫ `digest`
	  ▫ `digestie`
	  ▫ `ntlmwb`
	  ▫ `ntlm`
	  ▫ `negotiate`
		Autorisierungstyp auf dem Proxyserver. Der Standardwert ist 'any'.

`enabled`	• `yes` – Proxyserver verwenden. • `no` – keinen Proxyserver verwenden.	Modus für die Verbindung mit dem Dr.Web Server über HTTP-Proxyserver.

Attribut	Zulässige Werte	Erläuterung
host	-	Adresse des Proxyservers.
password	-	Benutzerpasswort des Proxyservers, falls der Proxyserver eine Autorisierung erfordert.
user	-	Benutzername des Proxyservers, falls der Proxyserver eine Autorisierung erfordert.

Beim Festlegen der möglichen Autorisierungsmethoden für den Proxyserver kann bei Bedarf die Markierung `only` für die Änderung des Algorithmus zur Auswahl der Autorisierungsmethoden verwendet werden. Sie muss am Ende der Liste durch ein Leerzeichen getrennt hinzugefügt werden.

Mehr Informationen dazu finden Sie unter https://curl.se/libcurl/c/CURLOPT_HTTPAUTH.html.

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

  Parameter für den Versand der Statistik zu den erkannten Bedrohungen an Doctor Web unter https://stat.drweb.com/.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
enabled	• yes – Statistik senden. • no – keine Statistik senden.	Modus für den Versand der Statistik an Doctor Web.	–
id	–	MD5-Wert des Lizenzschlüssels vom Agent.	–
interval	Positive ganze Zahl.	Sendeintervall (in Minuten).	30

- `<cluster>`

  Parameter des Clusters von Dr.Web Servern für den Datenaustausch innerhalb des Antivirus-Netzwerks, das aus mehreren Servern besteht.

  Verfügbar sind ein oder mehrere untergeordnete Elemente `<on multicast-group="" port="" interface="" />`.

  Beschreibung der Attribute:

Attribut	Erläuterung
multicast-group	IP-Adresse der Multicast-Gruppe, über die der Datenaustausch zwischen den Servern stattfindet.

Attribut	Erläuterung
port	Portnummer der Netzwerkschnittstelle, an die das Transportprotokoll gebunden wird, damit Daten an die Multicast-Gruppe gesendet werden können.
interface	IP-Adresse der Netzwerkschnittstelle, an die das Transportprotokoll, über das Informationen an die Multicast-Gruppe gesendet werden, gebunden wird.

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

  Einstellung für die Übertragung von Multicast-Updates über das Multicast-Protokoll. Mögliche Werte des Attributs `enabled`: `yes` oder `no`.

  Das Element `<multicast-updates>` enthält folgende Unterelemente und Attribute:

Unterelement	Attribut	Erläuterung	Standardmäßig
port <port value="" />	value	Portnummer der Netzwerkschnittstelle des Dr.Web Servers, an die das Multicast-Transportprotokoll gebunden wird, damit Updates übertragen werden. Dieser Port wird von allen Multicast-Gruppen verwendet. Für Multicast-Updates muss ein beliebiger freier Port angegeben werden. Er darf aber nicht mit dem Port, der für das Transportprotokoll in den Einstellungen des Servers festgelegt ist, identisch sein.	2197
ttl <ttl value="" />	value	Lebensdauer (TTL) eines übertragenen UDP-Datagramms. Dieser Wert wird von allen Multicast-Gruppen verwendet.	8
group <group address="" />	address	IP-Adresse der Multicast-Gruppe, über welche die Workstations Multicast-Updates erhalten.	233.192.86.0 für IPv4 FF0E::176 für IPv6
on <on interface="" ttl="" />	interface	IP-Adresse der Netzwerkschnittstelle des Dr.Web Servers, an die das Multicast-Transportprotokoll gebunden wird, damit Updates übertragen werden können.	–
	ttl	Lebensdauer (TTL) eines UDP-Datagramms, das über die angegebene Schnittstelle übertragen wird. Dieser Wert hat Vorrang vor dem Wert im gemeinsamen Unterelement `<ttl value="" />`.	8

Unterelement	Attribut	Erläuterung	Standardmäßig
transfer <transfer datagram-size="" assembly-timeout="" updates-interval="" chunks-interval="" resend-interval="" silence-interval="" accumulate-interval="" announce-send-times="" />	datagram-size	Größe eines UDP-Datagramms – hier wird die Größe der UDP-Datagramme (in Bytes) angegeben, die vom Multicast-Protokoll verwendet werden. Zulässig sind Werte von 512 bis 8192. Zur Vermeidung der Fragmentierung sollte der Wert geringer als der MTU-Wert (maximale Übertragungseinheit) des verwendeten Netzwerks sein.	1400
	assembly-timeout	Übertragungszeit für eine Datei (ms) – hier wird der Zeitraum angegeben, in dem eine Update-Datei übertragen werden soll. Nach Ablauf dieses Zeitraums sendet der Server die nächste Datei. Alle Dateien, die bei der Aktualisierung über Multicast nicht übertragen wurden, werden bei der standardmäßigen Aktualisierung über TCP übermittelt.	180000
	updates-interval	Dauer der Multicast-Updates (ms) – hier wird die Dauer der Aktualisierung über Multicast angegeben. Alle Dateien, die bei der Aktualisierung über Multicast nicht übertragen wurden, werden bei der standardmäßigen Aktualisierung über TCP übermittelt.	600000
	chunks-interval	Intervall zur Paketübertragung (ms) – hier wird das Zeitintervall angegeben, mit dem Pakete an eine Multicast-Gruppe gesendet werden sollen. Ein geringes Zeitintervall kann erhebliche Verluste in der Paketübertragung verursachen und das Netzwerk überlasten. Ändern Sie diesen Wert nur bei dringendem Bedarf.	14
	resend-interval	Intervall zwischen Anforderungen zur erneuten Übertragung (ms) – hier wird das Zeitintervall angegeben, mit dem die Agents Anforderungen zur erneuten Übertragung verlorener Pakete senden.	1000

Unterelement	Attribut	Erläuterung	Standardmäßig
		Dr.Web Server sammelt diese Anforderungen und sendet anschließend die verlorenen Blöcke zurück.	
	`silence-interval`	Ruheintervall im Übertragungskanal (ms) – hier wird das „Ruheintervall" angegeben: Wenn eine Datei vorzeitig übertragen wird und die Agents innerhalb dieses Ruheintervalls keine Anforderungen zur erneuten Übertragung verlorener Pakete senden, geht der Dr.Web Server davon aus, dass alle Agents die gesendete Update-Datei erhalten haben, und sendet anschließend die nächste Datei.	10000
	`accumulate-interval`	Intervall zum Sammeln von Anforderungen zur erneuten Übertragung (ms) – hier wird das Zeitintervall angegeben, in dem der Server Anforderungen der Agents zur erneuten Übertragung verlorener Pakete sammelt. Die Agents senden Anforderungen zur erneuten Übertragung verlorener Pakete. Der Server sammelt diese Anforderungen innerhalb des angegebenen Zeitraums und sendet anschließend die verlorenen Blöcke zurück.	2000
	`announce-send-times`	Anzahl von Ankündigungen zur Dateiübertragung – Anzahl der Male, die der Server eine Dateiübertragung an eine Multicast-Gruppe ankündigt, bevor die Übertragung von Updates beginnt. Bei einer Ankündigung wird an die Multicast-Gruppe ein UDP-Datagramm mit den Metadaten der Datei gesendet. Je mehr Ankündigungen Sie festlegen, desto zuverlässiger ist die Übertragung. Eine höhere Anzahl von Ankündigungen verlangsamt aber die Übertragung, sodass weniger Daten für die Dauer der Aktualisierung über Multicast übertragen werden können.	3

Das Element <**multicast-updates**> kann optional das Unterelement <**acl**> enthalten, das zur Erstellung der Zugriffssteuerungsliste verwendet wird. Mit diesem Unterelement können Sie die

TCP-Adressen von Workstations angeben, die Multicast-Updates vom angegebenen Server über Multicast erhalten können. Das Unterelement `<acl>` ist standardmäßig nicht vorhanden, was bedeutet, dass es keine Einschränkungen gibt.

`<acl>` innerhalb von `<multicast-updates>` enthält folgende Unterelemente:

- `<priority mode="" />`

  Legt die Priorität der Listen fest. Mögliche Werte des Attributs `mode`: `allow` oder `deny`. Bei der Festlegung `<priority mode="deny" />` hat die Liste `<deny>` Vorrang gegenüber der Liste `<allow>`. Adressen, die in keiner bzw. beiden Listen enthalten sind, werden nicht zugelassen. Erlaubt sind nur die Adressen, die in der Liste `<allow>` enthalten sind und nicht in der Liste `<deny>` vorhanden sind.

  - `<allow>`

  Liste der TCP-Adressen, für welche die Updates über Multicast erlaubt sind. Das Element `<allow>` enthält ein oder mehrere untergeordnete Elemente `<ip address="" />` für die Festlegung erlaubter Adressen im Format IPv4 und `<ip6 address="" />` für die Festlegung erlaubter Adressen im Format IPv6. Im Attribut `address` werden Netzwerkadressen im Format `<`*IP-Adresse*`>/[<`*Präfix*`>]` angegeben.

  - `<deny>`

  Liste der TCP-Adressen, für welche die Updates über Multicast nicht erlaubt sind. Das Element `<deny>` enthält ein oder mehrere untergeordnete Elemente `<ip address="" />` für die Festlegung verbotener Adressen im Format IPv4 und `<ip6 address="" />` für die Festlegung verbotener Adressen im Format IPv6. Im Attribut `address` werden Netzwerkadressen im Format `<`*IP-Adresse*`>/[<`*Präfix*`>]` festgelegt.

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

  Datenbankdefinition.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`connections`	Positive ganze Zahl.	Der Parameter legt die maximal zulässige Anzahl der Verbindungen mit dem Server fest. Es wird dringend davon abgeraten, den Wert dieses Parameters zu ändern.	2
`speedup`	`yes | no`	Der Parameter bestimmt, ob die Datenbank nach Vorgängen wie Initialisierung, Update und Import automatisch aufgeräumt werde soll (detaillierte Beschreibung finden Sie im **Administratorhandbuch** unter Datenbank).	`yes`

  Das Element `<database>` enthält eines der folgenden untergeordneten Elemente:

  Das Element `<database>` kann nur ein untergeordnetes Element, das eine bestimmte Datenbank definiert, enthalten.

Datenbankattribute, die im Muster der Konfigurationsdatei eventuell vorhanden sind, aber im Folgenden nicht beschrieben sind, sollten nur nach Absprache mit dem Support-Team von Doctor Web geändert werden.

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

  Einstellungen für integrierte SQLite3-Datenbank.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`dbfile`		Name der Datenbankdatei.	`database.sqlite`
`cache`	`SHARED | PRIVATE`	Cachemodus.	`SHARED`
`cachesize`	Positive ganze Zahl.	Datenbankcachegröße (in 1,5-KB-Seiten).	2048
`precompiledcache`	Positive ganze Zahl.	Größe des Cache vorkompilierter SQL-Anweisung in Kilobytes.	1024
`synchronous`	• `TRUE` oder `FULL` – synchron. • `FALSE` oder `NORMAL` – normal. • `OFF` – asynchron.	Datenspeicherung.	`FULL`
`checkintegrity`	`quick | full | no`	Integrität der Datenbank beim Start des Dr.Web Servers überprüfen.	`quick`
`autorepair`	`yes | no`	Beschädigte Datenbank beim Start des Dr.Web Servers automatisch reparieren.	`no`
`mmapsize`	Positive ganze Zahl.	Maximale Größe (in Bytes) der Datenbankdatei, die jeweils in den Prozessadressraum zugeordnet werden kann.	• Für UNIX – 10485760 • Für Windows – 0
`wal`	`yes | no`	Write-Ahead-Protokollierung (Write-Ahead Logging) verwenden.	`yes`
`wal-max-pages`		Maximale Anzahl „schmutziger" Seiten (dirty), bei der die Seiten auf	1000

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
		den Datenträger geschrieben werden sollen.	
wal-max-seconds		Maximale Dauer, um die das Schreiben der Seiten auf den Datenträger verzögert werden soll (in Sekunden).	30

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

  Einstellungen für externe PostgreSQL-Datenbank.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
dbname		Name der Datenbankdatei.	
host		Adresse des PostgreSQL-Servers oder Pfad zum UNIX-Domänen-Socket.	
port		Portnummer des PostgreSQL-Servers oder Namenserweiterung der UNIX-Socket-Datei.	
options		Befehlszeilenparameter zum Versenden der Datenbank an den Server. Einzelheiten entnehmen Sie dem Kapitel 18 unter https://www.postgresql.org/docs/9.1/libpq-connect.html	
requiressl	• 1 | 0 (über das Verwaltungscenter) • y | n • yes | no • on | off	Nur SSL-Verbindungen verwenden.	• 0 • y • yes • on
user		Name des Datenbanknutzers.	

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
password		Passwort des Datenbanknutzers.	
temp_tablespaces		Namensraum für temporäre Tabellen der Datenbank.	
default_transaction_isolation	• read uncommitted • read committed • repeatable read • serializable	Isolationsstufe für Transaktionen.	read committed

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

  Einstellungen für externe Oracle-Datenbank.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
connectionstring		Zeile, die Oracle SQL Connect URL oder das Schlüsselwort-Wertepaar von Oracle Net enthält.	
user		Anmeldename des Datenbanknutzers.	
password		Passwort des Datenbanknutzers.	
client		Pfad zum Client für den Zugriff auf die Oracle-Datenbank (Oracle Instant Client). Der Dr.Web Server wird mit dem Oracle Instant Client Version 11 geliefert. Wenn Sie eine neuere Version des Oracle-Servers verwenden bzw. der mitgelieferte Treiber für die Oracle-Datenbank Fehler aufweist, können Sie den entsprechenden Treiber von der Webseite von Oracle herunterladen und in diesem Feld den Pfad zum Treiber angeben.	
prefetch-rows	0-65535	Anzahl der Zeilen zum Vorabruf bei einer Datenbankabfrage.	0 – den Wert 1 verwenden (Standardwert der Datenbank)

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
prefetch-mem	0-65535	Größe des zugeordneten Speichers für den Vorabruf der Zeilen bei einer Datenbankabfrage.	0 – unbegrenzt

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

  Einstellungen für die ODBC-Verbindung mit einer externen Datenbank.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
dsn		Name der ODBC-Datenquelle.	drwcs
user		Anmeldename des Datenbanknutzers.	drwcs
pass		Passwort des Datenbanknutzers.	drwcs
limit	Positive ganze Zahl.	Verbindung mit dem DBMS nach der angegebenen Anzahl von Transaktionen erneut herstellen.	0 – keine erneute Herstellung
transaction	• SERIALIZABLE – serielle Ausführung. • READ_UNCOMMITTED – nicht festgeschriebene Daten lesen. • READ_UNCOMMITTED – festgeschriebene Daten lesen. • REPEATABLE_READ – wiederholbare Lesevorgänge. • DEFAULT – identisch mit "" – hängt vom DBMS ab.	Isolationsstufe für Transaktionen. Einige DBMS unterstützen nur READ_COMMITTED.	DEFAULT

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

  Einstellungen für externe MySQL/MariaDB-Datenbank.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
dbname		Datenbankname.	drwcs

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
host	Einer der beiden.	Adresse des Datenbank-Servers bei TCP/IP-Verbindung.	localhost
		Pfad zur UNIX-Socket-Datei bei Verwendung von UDS. Wenn kein Pfad angegeben ist, versucht der Server, die Datei in den Standardverzeichnissen von mysqld zu finden.	/var/run/mysqld/
port	Einer der beiden.	Portnummer für die TCP/IP-Verbindung mit der Datenbank.	3306
		UNIX-Socket-Dateiname bei Verwendung von UDS.	mysqld.sock
user		Anmeldename des Datenbanknutzers.	""
password		Passwort des Datenbanknutzers.	""
ssl	yes | beliebige Zeichenkette	Nur SSL-Verbindungen verwenden.	no
precompiledcache	Positive ganze Zahl.	Größe des Cache vorkompilierter SQL-Anweisung in Kilobytes.	1024

- **<acl>**

  Zugriffssteuerungslisten. Dadurch können Sie Einschränkungen für Netzwerkadressen festlegen, über die Agents, Netzwerk-Installer und andere Dr.Web (Nachbar-)Server auf den Server zugreifen können.

  Das Element **<acl>** enthält untergeordnete Elemente, mit denen Einschränkungen für bestimmte Verbindungstypen festgelegt werden können:

  - **<install>** – hier werden Einschränkungen für die IP-Adressen angegeben, von denen die Installationsprogramme der Dr.Web Agents auf den Server zugreifen können.
  - **<agent>** – hier werden Einschränkungen für die IP-Adressen angegeben, von denen die Dr.Web Agents auf den Server zugreifen können.
  - **<links>** – hier werden Einschränkungen für die IP-Adressen angegeben, von denen die Dr.Web Nachbar-Server auf den Server zugreifen können.
  - **<discovery>** – hier werden Einschränkungen für die IP-Adressen angegeben, von denen der *Server-Suchdienst* Broadcast-Anfragen empfangen kann.

  Alle untergeordneten Elemente haben die gleiche Struktur von Unterelementen, die folgende Einschränkungen festlegen:

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

    Priorität der Listen. Mögliche Werte des Attributs mode: allow oder deny. Bei der Festlegung **<priority mode="deny" />** hat die Liste **<deny>** Vorrang gegenüber der Liste

<allow>. Adressen, die in keiner bzw. beiden Listen enthalten sind, werden nicht zugelassen. Erlaubt sind nur die Adressen, die in der Liste <allow> enthalten sind und nicht der Liste <deny> vorhanden sind.

- <allow>

  Liste der TCP-Adressen, von denen zugegriffen werden kann. Das Element <allow> enthält ein oder mehrere untergeordnete Elemente <ip address="" /> für die Festlegung erlaubter Adressen im Format IPv4 und <ip6 address="" /> für die Festlegung erlaubter Adressen im Format IPv6. Im Attribut address werden Netzwerkadressen im Format *<IP-Adresse>*/[*<Präfix>*] angegeben.

- <deny>

  Liste der TCP-Adressen, von denen nicht zugegriffen werden darf. Das Element <deny> enthält ein oder mehrere untergeordnete Elemente <ip address="" /> für die Festlegung verbotener Adressen im Format IPv4 und <ip6 address="" /> für die Festlegung verbotener Adressen im Format IPv6. Im Attribut address werden Netzwerkadressen im Format *<IP-Adresse>*/[*<Präfix>*] festgelegt.

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

  Parameter für Skript-Profilerstellung.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
profile	• yes, • no.	Informationen über das Profilieren von Skripten des Servers protokollieren. Diese Option wird hauptsächlich vom technischen Support und Software-Entwicklern verwendet. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.	no
stack		Informationen im Aufrufstapel beim Ausführen von Skripten des Servers protokollieren. Diese Option wird hauptsächlich vom technischen Support und Software-Entwicklern verwendet. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.	
trace		Informationen über die Ablaufverfolgung beim Ausführen von Skripten des Servers protokollieren. Diese Option wird hauptsächlich vom technischen Support und Software-Entwicklern verwendet. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.	

- <lua-module-path>

  Pfade für den Lua-Interpreter.

Die Reihenfolge der Pfade wird beachtet.

Das Element <lua-module-path> enthält folgende untergeordnete Elemente:

- <cpath root="" /> – Pfad zum Verzeichnis mit binären Modulen. Mögliche Werte des Attributs root: home (standardmäßig), var, bin, lib.
- <path value="" /> – Pfad zum Verzeichnis mit Skripten. Wenn dieses nicht dem Element <jobs> oder <hooks> untergeordnet ist, gehört es den beiden. Die im Attribut value festgelegten Pfade sind relativ zu den Pfaden, die im Attribut root des Elements <cpath> angegeben sind.
- <jobs> – Pfade für Aufgaben im Zeitplan des Servers.

  Das Element <jobs> enthält ein oder mehrere untergeordnete Elemente <path value='' /> für die Festlegung des Pfades zum Verzeichnis mit Skripten.
- <hooks> – Pfade zu benutzerdefinierten Prozeduren des Servers.

  Das Element <hooks> enthält ein oder mehrere untergeordnete Elemente <path value='' /> für die Festlegung des Pfades zum Verzeichnis mit Skripten.

- <transports>

  Einstellungen der Transportprotokolle, die der Server zur Herstellung der Verbindung mit den Clients verwendet. Das Element enthält ein oder mehrere Unterelemente <transport discovery="" ip="" name="" multicast="" multicast-group="" port="" />.

  Beschreibung der Attribute:

Attribut	Erläuterung	Obligatorisch	Zulässige Werte	Standardmäßig
discovery	Bestimmt, ob der Dr.Web Server-Suchdienst verwendet werden soll.	nein, wird nur zusammen mit dem Attribut ip festgelegt.	yes, no	no
• ip • unix	Legt die zu verwendenden Protokolle und die Adresse der Schnittstelle fest.	ja	–	• 0.0.0.0 • -
name	Legt den Namen des Servers für den Dr.Web Server-Suchdienst fest.	nein	–	drwcs
multicast	Legt fest, ob der Server zur Multicast-Gruppe gehört.	nein, wird nur zusammen mit dem Attribut ip festgelegt.	yes, no	no
multicast-group	Legt die Adresse der Multicast-Gruppe fest, in die	nein, wird nur zusammen mit dem Attribut ip festgelegt.	–	• 231.0.0.1 • [ff18::231.0.0.1]

Attribut	Erläuterung	Obligatorisch	Zulässige Werte	Standardmäßig
	der Server aufgenommen ist.			
`port`	Port, der abgehört werden soll.	nein, wird nur zusammen mit dem Attribut `ip` festgelegt.	-	`2193`

- **<protocols>**

  Liste deaktivierter Protokolle. Dieses Element enthält ein oder mehrere Unterelemente **<protocol** `enabled="" name="" />`.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`enabled`	• `yes` – Protokoll ist aktiviert. • `no` – Protokoll ist deaktiviert.	Verwendung von Protokollen.	no
`name`	• `AGENT` – Protokoll für die Kommunikation zwischen dem Server und Dr.Web Agents. • `MSNAPSHV` – Protokoll für die Kommunikation zwischen dem Server und dem NAP Validator der Windows-Systemintegritätsprüfung. • `INSTALL` – Protokoll der Kommunikation zwischen dem Server und den Installationsprogrammen der Dr.Web Agents. • `CLUSTER` – Protokoll der Kommunikation zwischen den Servern innerhalb eines Clusters. • `SERVER` – Protokoll der Kommunikation zwischen dem Dr.Web Server und anderen Dr.Web Servern.	Protokollname.	-

- **<plugins>**

  Liste deaktivierter Erweiterungen. Dieses Element enthält ein oder mehrere Unterelemente **<plugin** `enabled="" name="" />`.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`enabled`	• `yes` – Erweiterung ist aktiviert. • `no` – Erweiterung ist deaktiviert.	Verwendung von Erweiterungen.	no

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
name	• WEBMIN – Browser-Erweiterung für das Dr.Web Sicherheitscenter zur Verwaltung des Servers und Antivirus-Netzwerks über das Verwaltungscenter. • FrontDoor – Erweiterung Dr.Web Server FrontDoor, die ermöglicht, das Programm zur Ferndiagnose des Servers zu verwenden.	Name der Erweiterung.	-

- `<license>`

  Lizenzierungseinstellungen.

  Das Element `<license>` enthält folgende untergeordnete Elemente:

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

    Einstellungen für die Benachrichtigung über das Limit für die Anzahl von Lizenzen im Lizenzschlüssel.

    Beschreibung der Attribute:

Attribut	Erläuterung	Standardmäßig
min-count	Maximale Anzahl der verbleibenden Lizenzen, bei der die Benachrichtigung **Limit für die Anzahl von Lizenzen im Lizenzschlüssel** gesendet werden soll.	3
min-percent	Maximaler Prozentsatz der verbleibenden Lizenzen, bei dem die Benachrichtigung **Limit für die Anzahl von Lizenzen im Lizenzschlüssel** gesendet werden soll.	5

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

    Einstellungen für den Lizenznutzungsbericht.

    Beschreibung der Attribute:

Attribut	Erläuterung	Standardmäßig
report-period	Intervall, in dem Berichte über die Nutzung von Lizenzschlüsseln auf dem Server erstellt werden sollen. Wenn der Lizenznutzungsbericht von einem untergeordneten Server erstellt wird, wird dieser Bericht sofort nach der Erstellung an den übergeordneten Server geschickt. Die erstellten Berichte werden auch bei jeder Verbindung (bzw. bei einem Neustart) des Servers und bei der Änderung der Anzahl der bereitgestellten Lizenzen auf dem übergeordneten Server geschickt.	1440

Attribut	Erläuterung	Standardmäßig
active-stations-period	Zeitraum, in dem die aktiven Workstations für die Erstellung des Lizenznutzungsberichts gezählt werden sollen. Wenn Sie 0 angeben, werden alle Workstations unabhängig von ihrem Aktivitätsstatus im Bericht berücksichtigt.	0

- <exchange>

  Einstellungen für die Verteilung von Lizenzen zwischen Dr.Web Servern.

  Das Element <exchange> enthält folgende untergeordnete Elemente:

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

  Beschreibung der Elemente:

Element	Erläuterung	Standardwert des Attributs „value“, in Min.
expiration-interval	**Laufzeit der bereitzustellenden Lizenzen** – hier wird der Zeitraum angegeben, für den Lizenzen aus dem Schlüssel des Servers verteilt werden sollen. Diese Option wird verwendet, falls der Server Lizenzen auf Nachbar-Server verteilt.	1440
prolong-preact	**Zeitraum für die Verlängerung der bereitgestellten Lizenzen** – hier wird der Zeitraum bis zum Ablauf der Lizenz angegeben, ab dem dieser Server die Verlängerung der von dem Nachbar-Server erhaltenen Lizenz initiiert. Diese Option wird verwendet, wenn der Server Lizenzen von Nachbar-Servern verteilt bekommt.	60
check-interval	**Zeitraum für die Synchronisierung der Lizenzen**– hier wird das Zeitintervall angegeben, mit dem Informationen zu den bereitgestellten Lizenzen zwischen den Servern synchronisiert werden sollen.	1440

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

  Parameter für den Versand von E-Mails über das Verwaltungscenter, die z. B. Administrator-Benachrichtigungen oder Installationspaketen enthalten.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
from	-	E-Mail-Adresse, die als Absender von E-Mail-Benachrichtigungen	drwcs@localhost

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
		verwendet werden soll.	
debug	• yes – Debug-Modus verwenden. • no – Debug-Modus nicht verwenden.	Debug-Modus zur detaillierten Protokollierung von SMTP-Sitzungen verwenden.	no

Das Element <email/> enthält folgende Unterelemente:

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

  Einstellungen des SMTP-Servers zum Versand von E-Mails.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
server	-	Adresse des SMTP-Servers, der zum Versand von E-Mails verwendet werden soll.	127.0.0.1
user	-	Benutzername des SMTP-Servers, wenn der SMTP-Server eine Autorisierung erfordert.	-
pass	-	Benutzerpasswort des SMTP-Servers, wenn der SMTP-Server eine Autorisierung erfordert.	-
port	Positive ganze Zahl.	Port des SMTP-Servers an, der zum Versand von E-Mails verwendet werden soll.	25
start_tls	• yes – diesen Typ der Authentifizierung verwenden. • no – diesen Typ der Authentifizierung nicht verwenden.	Diese Option sorgt dafür, dass die Kommunikation verschlüsselt erfolgt. Um eine sichere Verbindung anzufordern, wird der Befehl STARTTLS verwendet. Der Standardport ist 25.	yes
auth_plain		*Plaintext*-Authentifizierung am E-Mail-Server verwenden.	no
auth_login		*LOGIN*-Authentifizierung am E-Mail-Server verwenden.	no
auth_cram_md5		*CRAM-MD5*-Authentifizierung am E-Mail-Server verwenden.	no

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
auth_digest_md5		*DIGEST-MD5*-Authentifizierung am E-Mail-Server verwenden.	no
auth_ntlm		*AUTH-NTLM*-Authentifizierung am E-Mail-Server verwenden.	no
conn_timeout	Positive ganze Zahl.	Zeitlimit für die Verbindung mit dem SMTP-Server.	180

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

Parameter für die SSL-Verschlüsselung beim Versand von E-Mails.

Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
enabled	• yes – SSL verwenden. • no – SSL nicht verwenden.	SSL-Verschlüsselungsmodus.	no
verify_cert	• yes – SSL-Zertifikat überprüfen. • no – SSL-Zertifikat nicht überprüfen.	SSL-Zertifikat des E-Mail-Servers auf Richtigkeit überprüfen.	no
ca_certs	-	Pfad zum SSL-Wurzelzertifikat des Dr.Web Servers.	-

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

Einstellungen für die Überwachung von massenhaften Infektionen im Netzwerk.

Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
enabled	yes | no	Zahlreiche Ereignisse im Zusammenhang mit Infektionen von Workstations überwachen und eine Sammelbenachrichtigung an den Administrator senden.	yes
aggregation-period	Positive ganze Zahl.	Zeitraum nach dem Versand einer Benachrichtigung über eine massenhafte Infektion (in Sekunden), in dem keine Benachrichtigungen	300

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
		über einzelne Infektionen gesendet werden sollen.	
`check-period`		Zeitraum (in Sekunden), in dem die festgelegte Anzahl von Benachrichtigungen über einzelne Infektionen empfangen werden muss, damit eine Benachrichtigung über die massenhafte Infektion gesendet wird.	3600
`threshold`		Anzahl von Benachrichtigungen über Infektionen, die innerhalb des festgelegten Zeitraums empfangen werden muss, damit der Dr.Web Server eine einheitliche Benachrichtigung über massenhafte Infektion an den Administrator sendet (Benachrichtigung **Massenhafte Infektion im Netzwerk**).	100
`most-active`		Anzahl der häufigsten Bedrohungen, die in den Bericht über massenhafte Infektionen aufgenommen werden sollen.	5

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

  Einstellungen für die Überwachung von zahlreichen Ereignissen des Präventivschutzes.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`enabled`	`yes | no`	Zahlreiche Ereignisse im Zusammenhang mit dem Präventivschutz überwachen und eine Sammelbenachrichtigung an den Administrator senden.	`yes`
`aggregation-period`	Positive ganze Zahl.	Zeitraum (in Sekunden) nach dem Versand eines Übersichtsberichts im Zusammenhang mit den Ereignissen des Präventivschutzes, in dem keine Benachrichtigungen über einzelne Ereignisse gesendet werden sollen.	300

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`check-period`		Zeitraum (in Sekunden), in dem die festgelegte Anzahl von Ereignissen des Präventivschutzes registriert werden muss, damit ein Übersichtsbericht gesendet wird.	3600
`threshold`		Anzahl von Ereignissen des Präventivschutzes, die innerhalb des festgelegten Zeitraums empfangen werden müssen, damit der Dr.Web Server einen Übersichtsbericht über all diese Ereignisse an den Administrator sendet (Benachrichtigung **Übersichtsbericht des Präventivschutzes**).	100
`most-active`		Anzahl der häufigsten Prozesse mit verdächtiger Aktivität, die in den Bericht des Präventivschutzes aufgenommen werden sollen.	5

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

  Einstellungen für die Überwachung von zahlreichen Ereignissen der Anwendungskontrolle.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`enabled`	`yes | no`	Zahlreiche Ereignisse im Zusammenhang mit der Anwendungskontrolle überwachen und eine Sammelbenachrichtigung an den Administrator senden.	`yes`
`aggregation-period`	Positive ganze Zahl.	Zeitraum (in Sekunden) nach dem Versand eines Übersichtsberichts im Zusammenhang mit den von der Anwendungskontrolle gesperrten Prozessen, in dem keine Benachrichtigungen über einzelne Sperrungen gesendet werden sollen.	300
`check-period`		Zeitraum (in Sekunden), in dem die festgelegte Anzahl von Prozessen gesperrt werden muss, damit ein Übersichtsbericht gesendet wird.	3600

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`threshold`		Anzahl von Ereignissen im Zusammenhang mit den von der Anwendungskontrolle gesperrten Prozessen, die innerhalb des festgelegten Zeitraums empfangen werden muss, damit der Dr.Web Server einen Übersichtsbericht über alle diese Ereignisse an den Administrator sendet (Benachrichtigung **Es wurde viele Sperrungen durch die Anwendungskontrolle registriert**).	100
`most-active`		Anzahl der häufigsten Profile, anhand derer die Sperrungen erfolgten und die in die Benachrichtigung über zahlreiche Sperrungen aufgenommen werden sollen.	5

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

  Einstellungen für die Überwachung von zahlreichen Verbindungsabbrüchen mit Clients.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`enabled`	`yes | no`	Abgebrochene Clientverbindungen überwachen und eine entsprechende Benachrichtigung an den Administrator senden.	`yes`
`aggregation-period`	Positive ganze Zahl.	Zeitraum (in Sekunden) nach dem Versand einer Benachrichtigung über zahlreiche Verbindungsabbrüche, in dem keine Benachrichtigungen über einzelne Verbindungsabbrüche gesendet werden sollen.	300
`check-period`		Zeitraum (in Sekunden), in dem die festgelegte Anzahl von Clientverbindungen abgebrochen werden muss, damit eine entsprechende Benachrichtigung gesendet wird.	3600

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`single-alert-threshold`		Minimale Anzahl von Verbindungen mit einer Adresse, die innerhalb des Berechnungszeitraums abgebrochen werden muss, damit eine Benachrichtigung über einzelnen Verbindungsabbruch gesendet wird (Benachrichtigung **Verbindungsabbruch**).	10
`summary-alert-threshold`		Minimale Anzahl von Verbindungen, die innerhalb des Berechnungszeitraums abgebrochen werden muss, damit eine einheitliche Benachrichtigung über zahlreiche Verbindungsabbrüche gesendet wird (Benachrichtigung **Es wurden viele Verbindungsabbrüche registriert**).	1000
`min-session-duration`		Falls die Dauer einer abgebrochenen Clientverbindung weniger als die hier angegebene Dauer ist, wird ungeachtet des Berechnungszeitraums eine Benachrichtigung über einzelne Verbindungsabbrüche gesendet, sobald die festgelegte Anzahl von Verbindungen erreicht wird (Benachrichtigung **Verbindungsabbruch**). Die Voraussetzungen dafür sind allerdings, dass die Verbindung weiter nicht von einer längeren Verbindung abgebrochen wird und keine Benachrichtigung über zahlreiche Verbindungsabbrüche gesendet wird (Benachrichtigung **Es wurden viele Verbindungsabbrüche registriert**).	300

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

  Hier wird die Sprache angegeben, die standardmäßig für die Dr.Web Komponenten und den Dr.Web Server verwendet werden soll, wenn die Spracheinstellungen aus der Datenbank des Servers nicht abgerufen werden können. Die Standardsprache wird beispielsweise für das Dr.Web Sicherheitscenter und das Administrator-Benachrichtigungssystem verwendet, falls die Datenbank beschädigt ist und die Spracheinstellungen nicht verfügbar sind.

G2. Konfigurationsdatei des Dr.Web Sicherheitscenters

Die Konfigurationsdatei des Verwaltungscenters `webmin.conf` wird im XML-Format im Unterverzeichnis `etc` des Server-Wurzelverzeichnisses gespeichert.

Beschreibung der Parameter der Konfigurationsdatei des Dr.Web Sicherheitscenters:

`<version value="">`

Aktuelle Version des Dr.Web Servers.

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

  Name des Dr.Web Servers.

  Der Wert dieser Option muss im folgenden Format angegeben werden:

  <IP-Adresse oder DNS-Name des Servers>`[:`*<Port>*`]`

  Wenn keine Adresse des Servers angegeben ist, wird der vom Betriebssystem zurückgegebene Name des Rechners oder die Netzwerkadresse des Servers verwendet: DNS-Name, falls vorhanden, andernfalls IP-Adresse.

  Wenn keine Portnummer angegeben ist, wird der Port verwendet, der in der Anforderung angegeben wurde (beispielsweise wenn auf den Server über das Verwaltungscenter oder **Web API** zugegriffen wird). Bei Anforderungen über das Verwaltungscenter ist das der Port, der in der Adresszeile zur Verbindung des Verwaltungscenters mit dem Server angegeben wurde.

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

  Pfad zum Verzeichnis mit den Webseiten. Der Standardwert ist `value="webmin"`.

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

  Pfad zum Verzeichnis mit den Modulen. Der Standardwert ist `value="ds-modules"`.

- `<threads value=""/>`

  Anzahl paralleler Anfragen, die vom Webserver verarbeitet werden. Diese Option beeinflusst die Leistung des Servers. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.

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

  Anzahl von Threads zur Verarbeitung von übertragenen Daten. Dieser Parameter beeinflusst die Leistung des Servers. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.

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

  Einstellungen für die Datenverkehr-Komprimierung bei der HTTP/HTTPS-Kommunikation mit dem Webserver.

  Beschreibung der Attribute:

Attribut	Erläuterung	Standardmäßig
`value`	Komprimierungsstufe von 1 bis 9, wobei die Eins die minimale und die Neun die maximale Komprimierungsstufe ist.	9

Attribut	Erläuterung	Standardmäßig
max-size	Maximale Größe für die zu komprimierenden HTTP-Antworten. Tragen Sie 0 ein, um keine Obergrenze zu setzen.	51200 KB
min-size	Minimale Größe für die zu komprimierenden HTTP-Antworten. Tragen Sie 0 ein, um keine Untergrenze zu setzen.	32 Bytes

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

  HTTP-Sitzung aufrecht halten. Dieses Element ermöglicht, die Verbindung für Anforderungen über das Protokoll HTTP/1.X aktiv zu halten.

  Beschreibung der Attribute:

Attribut	Erläuterung	Standardmäßig
timeout	HTTP-Sitzungszeitlimit. Bei ständigen Verbindungen wird die Verbindung mit dem Server getrennt, wenn keine Anforderungen von dem Client innerhalb des hier angegebenen Zeitraums empfangen wurden.	15 Sek.
send-rate	Minimal zulässige Rate, mit der Daten gesendet werden. Wenn die Übertragungsrate ausgehender Netzwerkverbindungen diesen Wert unterschreitet, wird keine Verbindung hergestellt. Geben Sie 0 an, um diese Einschränkung aufzuheben.	1024 B/s
receive-rate	Minimal zulässige Rate, mit der Daten empfangen werden. Wenn die Übertragungsrate eingehender Netzwerkverbindungen diesen Wert unterschreitet, wird keine Verbindung hergestellt. Geben Sie 0 an, um diese Einschränkung aufzuheben.	1024 B/s

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

  Größe des Sende- bzw. Empfangspuffers.

  Beschreibung der Attribute:

Attribut	Erläuterung	Standardmäßig
send	Größe der Sendepuffer. Dieser Parameter beeinflusst die Leistung des Servers. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.	8192 Bytes
receive	Größe der Empfangspuffer. Dieser Parameter beeinflusst die Leistung des Servers. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.	2048 Bytes

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

  Maximal zulässige Größe einer HTTP-Anforderung (in KB).

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

IP-Adressen durch DNS-Namen von Rechnern in der Protokolldatei des Dr.Web Servers ersetzen. Mögliche Werte des Attributs `enabled`: `yes` oder `no`.

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

  Skriptfehler im Webbrowser anzeigen (Fehler 500). Diese Option wird vom technischen Support und Software-Entwicklern verwendet. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.

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

  Ablaufverfolgung von Skripten aktivieren. Dieser Parameter wird hauptsächlich vom technischen Support und Software-Entwicklern verwendet. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf. Mögliche Werte des Attributs `enabled`: `yes` oder `no`.

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

  Profilerstellung steuern. Beim Profilieren werden detaillierte Leistungsmessungen für die Skripte des Webservers durchgeführt. Erfasst wird die Dauer jeder Ausführung. Dieser Parameter wird hauptsächlich vom technischen Support und Software-Entwicklern verwendet. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung
`enabled`	• `yes` – Profilerstellung aktivieren. • `no` – Profilerstellung deaktivieren.	Modus der Profilerstellung.
`stack`	• `yes` – Leistungsdaten protokollieren. • `yes` – keine Leistungsdaten protokollieren.	Legt fest, ob Informationen über die Profilerstellung (Parameter der Funktion und die zurückgegebenen Werte) im Protokoll des Servers protokolliert werden sollen.

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

  Ausführen von Skripten abbrechen, wenn die Verbindung durch den Client abgebrochen wird. Dieser Parameter wird hauptsächlich vom technischen Support und Software-Entwicklern verwendet. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf. Mögliche Werte des Attributs `enabled`: `yes` oder `no`.

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

  Lokalisierte Seiten verwenden. Wenn dieser Modus aktiviert ist, wird es nach der lokalisierten Version der angegebenen Seite gesucht. Die Suche erfolgt entsprechend der Reihenfolge der Sprachen im Header-Feld `Accept-Language` des Clients. Zulässige Werte des Attributs `enabled`: `yes` oder `no`.

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

  Sprache der Dokumente, die vom Webserver zurückgegeben werden, falls der Header `Accept-Language` in der HTTP-Anforderung fehlt. Als Wert des Attributs `value` muss der ISO-Code der gewünschten Sprache angegeben werden. Der Standardwert ist `ru`.

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

  Einstellungen des SSL-Zertifikats.

  Beschreibung der Attribute:

Attribut	Erläuterung	Zulässige Werte	Standardmäßig
`certificate`	Pfad zum SSL-Zertifikat.	-	`certificate.pem`
`private-key`	Pfad der privaten SSL-Schlüsseldatei.	-	`private-key.pem`
`keep-alive`	Keep-Alive-Verbindung für SSL-gesicherte Verbindungen verwenden. Beachten Sie, dass einige alte Browser-Versionen persistente SSL-Verbindungen nicht unterstützen. Deaktivieren Sie diesen Parameter, falls Sie Probleme mit dem Verbindungsaufbau über SSL vermuten.	• `yes`, • `no`.	`yes`

- `<listen>`

  Abhörparameter.

  Das Element `<listen>` enthält folgende untergeordnete Elemente:

  - `<insecure>`

    Liste der Schnittstellen, an denen auf HTTP-Verbindungen gelauscht werden soll. Der Standardport ist 9080.

    Das Element `<insecure>` enthält ein oder mehrere Unterelemente `<endpoint address=""/>` für die Festlegung erlaubter IPv4- oder IPv6-Adressen. Im Attribut `address` werden Netzwerkadressen im Format *<Protokoll>*`://`*<IP-Adresse>* festgelegt.

  - `<secure>`

    Liste der Schnittstellen, an denen auf HTTPS-Verbindungen gelauscht werden soll. Der Standardport ist 9081.

    Das Element `<secure>` enthält ein oder mehrere Unterelemente `<endpoint address=""/>` für die Festlegung erlaubter IPv4- oder IPv6-Adressen. Im Attribut `address` werden Netzwerkadressen im Format *<Protokoll>*`://`*<IP-Adresse>* festgelegt.

- `<access>`

  Zugriffssteuerungslisten. Dadurch können Sie Einschränkungen für die Netzwerkadressen festlegen, von denen der Webserver HTTP- und HTTPS-Verbindungen empfängt.

  Das Element `<access>` enthält folgende untergeordnete Elemente, in denen Einschränkungen für bestimmte Verbindungstypen festgelegt werden:

  - `<secure priority="">`

    Liste der Schnittstellen, an denen auf HTTPS-Verbindungen gelauscht werden soll. Der Standardport ist 9081.

    Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
priority	allow	Erlaubende Regel für HTTPS bevorzugen: Adressen, die in keiner bzw. in beiden Listen enthalten sind, werden zugelassen.	deny
	deny	Verbietende Regel für HTTPS bevorzugen: Adressen, die in keiner bzw. in beiden Listen enthalten sind, werden verboten.	

Das Element <secure> enthält ein oder mehrere Unterelemente: <allow address=""/> und <deny address=""/>.

Beschreibung der Elemente:

Element	Erläuterung	Standardwert des Attributs „address“
allow	Adressen, von denen aus über HTTPS zugegriffen werden darf.	tcp://127.0.0.1
deny	Adressen, von denen aus über HTTPS nicht zugegriffen werden darf.	-

- <insecure priority="">

Liste der Schnittstellen, an denen auf HTTP-Verbindungen gelauscht werden soll. Der Standardport ist 9080.

Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
priority	allow	Erlaubende Regel für HTTP bevorzugen: Adressen, die in keiner bzw. in beiden Listen enthalten sind, werden zugelassen.	deny
	deny	Verbietende Regel für HTTP bevorzugen: Adressen, die in keiner bzw. in beiden Listen enthalten sind, werden verboten.	

Das Element <insecure> enthält ein oder mehrere Unterelemente: <allow address=""/> und <deny address=""/>.

Beschreibung der Elemente:

Element	Erläuterung	Standardwert des Attributs „address“
allow	Adressen, von denen aus über HTTP zugegriffen werden darf.	tcp://127.0.0.1

Element	Erläuterung	Standardwert des Attributs „address“
`deny`	Adressen, von denen aus über HTTP nicht zugegriffen werden darf.	-

G3. Konfigurationsdatei download.conf

Verwendung der Datei download.conf:

1. Die Verwendung dieser Konfigurationsdatei im Cluster von Dr.Web Servern führt zu einer ausgewogenen Belastung der einzelnen Server, wenn sich gleichzeitig viele neue Workstations verbinden.
2. Wenn ein nicht standardmäßiger Port auf dem Dr.Web Server verwendet wird, kann dieser Port bei der Generierung der Installationsdatei des Agents festgelegt werden.

Die Datei `download.conf` wird verwendet, wenn die Installationsdatei des Agents für eine neue Workstation des Antivirus-Netzwerks generiert wird. Die Parameter dieser Datei ermöglichen, die Adresse des Dr.Web Servers sowie den Port, die das Installationsprogramm des Agents bei der Herstellung der Verbindung mit dem Server verwendet, wie folgt festzulegen:

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

wobei:

- <*Server_Address*> – IP-Adresse oder DNS-Name des Servers.

  Beim Generieren des Installationspakets des Agents wird die Adresse des Servers zunächst der Datei `download.conf` entnommen. Wenn die Adresse des Servers in der Datei `download.conf` nicht festgelegt ist, wird der Wert des Parameters `ServerName` aus der Datei `webmin.conf` verwendet. Anderenfalls wird der vom Betriebssystem zurückgegebene Name des Rechners verwendet.

- <*port_number*> – Port, den das Installationsprogramm des Agents für die Verbindung mit dem Server verwendet.

  Wenn in den Parametern der Datei `download.conf` keine Portnummer festgelegt ist, wird standardmäßig der Port 2193 verwendet (diese Einstellung kann im Verwaltungscenter im Bereich **Administration** → **Dr.Web Server-Konfiguration** → Registerkarte **Netzwerk** → Registerkarte **Transport** geändert werden).

Standardmäßig ist der Parameter `download` in der Datei `download.conf` auskommentiert. Um die Datei `download.conf` verwenden zu können, müssen Sie diesen Parameter wirksam machen, indem Sie das Zeichen „`--`“ am Anfang der Zeile löschen, und die gewünschten Werte für die Adresse und den Port des Servers angeben.

G4. Konfigurationsdatei des Dr.Web Proxyservers

Die Konfigurationsdatei des Proxyservers `drwcsd-proxy.conf` hat das XML-Format und befindet sich in folgendem Verzeichnis:

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

Parameter der Konfigurationsdatei des Dr.Web Proxyservers:

- `<listen spec="">`

  Das Wurzelelement `<drwcsd-proxy>` enthält ein oder mehrere obligatorische Elemente `<listen>`, welche die Basiseinstellungen für den Empfang von Verbindungen des Proxyservers bestimmen.

  Das Element `<listen>` enthält nur ein obligatorisches Attribut `spec`, dessen Attribute festlegen, an welcher Schnittstelle auf eingehende Verbindungen der Clients gelauscht werden soll und ob an der festgelegten Schnittstelle der Modus `discovery` aktiviert sein soll.

  Attribute des Elements `spec`:

Attribut	Obligatorisch	Zulässige Werte	Erläuterung	Standardmäßig
`ip | unix`	ja	–	Typ des Protokolls zum Empfang eingehender Verbindungen. Als Parameter muss die Adresse angegeben werden, die der Proxyserver abhört.	`0.0.0.0 | –`
`port`	nein	–	Nummer des Ports, an dem der Proxyserver lauscht.	`2193`
`discovery`	nein	`yes, no`	Simulationsmodus des Servers. Dadurch können Clients den Proxyserver als Dr.Web Server erkennen, wenn nach ihm über Multicast gesucht wird.	`yes`
`multicast`	nein	`yes, no`	Modus zum Abhören des Netzwerks, in dem der Proxyserver Multicast-Anfragen empfängt.	`yes`

Attribut	Obligatorisch	Zulässige Werte	Erläuterung	Standardmäßig
multicast-group	nein	–	Multicast-Gruppe, in der sich der Proxyserver befindet.	231.0.0.1 [ff18::231.0.0.1]

Je nach Protokoll kann die Liste der im Attribut spec optional anzugebenden Attribute variieren.

Die Tabelle unten enthält die Liste der optionalen Eigenschaften, die im Attribut spec je nach Protokoll festgelegt (+) oder nicht festgelegt (–) werden können:

Protokoll	Verfügbare Eigenschaften			
	port	discovery	multicast	multicast-group
ip	+	+	+	+
unix	+	–	–	–

Der Modus **discovery** muss immer explizit aktiviert werden, selbst wenn der Modus **multicast** bereits aktiviert ist.

Eine detaillierte Beschreibung des Weiterleitungsalgorithmus bei der Verwendung der Liste der Dr.Web Server finden Sie im **Administratorhandbuch**.

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

Das Element <compression> als untergeordnetes Element des Elements <listen> definiert die Parameter für die Komprimierung des Datenverkehrs zwischen dem Client und dem Proxyserver.

Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
mode	yes	Komprimierung ist aktiviert.	possible
	no	Komprimierung ist deaktiviert.	
	possible	Komprimierung ist möglich.	
level	Ganzzahl von 1 bis 9	Komprimierungsrate. Nur für den Datenverkehr zwischen dem Client und dem Proxyserver.	8

- <encryption mode="">

Das Element <encryption> als untergeordnetes Element des Elements <listen> definiert die Parameter für die Verschlüsselung des Datenverkehrs zwischen dem Client und dem Proxyserver.

Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
mode	yes	Verschlüsselung ist aktiviert.	possible
	no	Verschlüsselung ist deaktiviert.	
	possible	Verschlüsselung ist möglich.	

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

Das Element bestimmt, wie eingehende Verbindungen umgeleitet werden sollen. Das Element `<forward>` ist obligatorisch. Mehrere Elemente `<forward>` mit verschiedenen Attributwerten können angegeben werden.

Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Obligatorisch
to	Die Adresse muss entsprechend der Spezifikation zur Schreibweise von Netzwerkadressen, und zwar im Format `tcp/<DNS_name>:<port>`.	Adresse des Dr.Web Servers, an den die Verbindung umgeleitet werden soll.	ja
master	• `yes` – Server wird zum bedingungslosen Kontrollserver. • `no` – Server wird unter keiner Bedingung zum Kontrollserver. • `possible` – Server wird zum Kontrollserver nur, wenn es keine bedingungslosen Kontrollserver (mit dem Wert `yes` für das Attribut `master`) gibt.	Das Attribut bestimmt, ob die Einstellungen des Proxyservers remote über das Verwaltungscenter des im Attribut `to` angegebenen Dr.Web Servers geändert werden können. Sie können beliebig viele Server zum Kontrollserver machen (Wert `master="yes"`). Es wird versucht, alle der angegebenen Kontrollserver zu kontaktieren, und zwar der Reihe nach, wie sie in den Einstellungen des Proxyservers angeführt sind, bis die erste gültige (nicht leere) Konfiguration abgerufen wird. Sie können auch keinen der Server zum Kontrollserver machen (Wert `master="no"`). In diesem Fall können die Parameter des Proxyservers (darunter auch Festlegung der Kontrollserver) nur	nein

Attribut	Zulässige Werte	Erläuterung	Obligatorisch
		lokal mithilfe der Konfigurationsdatei des Proxyservers konfiguriert werden.	

Wenn das Attribut `master` für den Server fehlt, wird standardmäßig davon ausgegangen, dass `master="possible"`.

In der vom Installationsprogramm bei der Installation des Proxyservers erstellten Konfigurationsdatei ist das Attribut `master` für keinen der Server definiert.

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

  Das Element `<compression>` als untergeordnetes Element des Elements `<forward>` definiert die Parameter für die Komprimierung des Datenverkehrs zwischen dem Server und dem Proxyserver. Seine Attribute sind identisch mit den obigen Attributen.

- `<encryption mode="">`

  Das Element `<encryption>` als untergeordnetes Element des Elements `<listen>` definiert die Parameter für die Verschlüsselung des Datenverkehrs zwischen dem Server und Proxyserver. Seine Attribute sind identisch mit den obigen Attributen.

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

Das Element `<update-bandwidth>` dient zur Einschränkung der Übertragungsrate, mit der Updates vom Server auf die Clients übertragen werden, sowie zur Einschränkung der Anzahl von Clients, die Updates gleichzeitig herunterladen können.

Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`value`	• KB/s • `unlimited`	Maximale Gesamtübertragungsrate für die Übertragung von Updates.	`unlimited`
`queue-size`	• positive ganze Zahl • `unlimited`	Maximale Anzahl an Update-Sitzungen, die vom Server aus gleichzeitig gestartet werden können. Wenn der festgelegte Wert erreicht ist, werden Anfragen der Agents in die Warteschlange gestellt. Die Warteschlangengröße ist unbegrenzt.	`unlimited`

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

  Das Element `<update-bandwidth>` kann ein oder mehrere untergeordnete Elemente `<bandwidth>` haben. Mit diesem Element kann die Übertragungsrate für einen bestimmten Zeitraum begrenzt werden.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
value	• KB/s • unlimited	Maximale Gesamtübertragungsrate, mit der Daten beim Update der Agents übertragen werden.	unlimited
time-map	–	Maske für den Zeitraum, in dem die Einschränkung gültig ist.	–

Der Wert des Parameters time-map wird entsprechend den Einschränkungen für die Datenübertragung in den Einstellungen des Servers festgelegt. Die manuelle Generierung von time-map ist zurzeit nicht möglich.

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

Das Element <install-bandwidth> dient zur Einschränkung der Übertragungsrate, mit der Installationsdateien der Agents übertragen werden, sowie zur Einschränkung der Anzahl an Clients, die diese Installationsdateien gleichzeitig herunterladen können.

Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
value	• KB/s • unlimited	Maximale Gesamtübertragungsrate, mit der Daten bei der Installation von Agents übertragen werden.	unlimited
queue-size	• positive ganze Zahl • unlimited	Maximale Anzahl der Installationsvorgänge von Agents, die vom Server aus gleichzeitig gestartet werden können. Wenn der festgelegte Wert erreicht ist, werden Anfragen der Agents in die Warteschlange gestellt. Die Warteschlangengröße ist unbegrenzt.	unlimited

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

    Das Element <install-bandwidth > kann ein oder mehrere untergeordnete Elemente <bandwidth > haben. Mit diesem Element kann die Übertragungsrate für einen bestimmten Zeitraum begrenzt werden.

    Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
value	• KB/s • unlimited	Maximale Gesamtübertragungsrate, mit der Daten bei der Installation der Agents übertragen werden.	unlimited
time-map	–	Maske für den Zeitraum, in dem die Einschränkung gültig ist.	–

Der Wert des Parameters `time-map` wird entsprechend den Einschränkungen für die Datenübertragung in den Einstellungen des Servers festgelegt. Die manuelle Generierung von `time-map` ist zurzeit nicht möglich.

- **<cache enabled="">**

  Einstellungen für den Cache des Proxyserver-Repository.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
enabled	yes | no	Gibt an, ob das Caching aktiviert ist oder nicht.	yes

  Das Element **<cache>** enthält folgende untergeordnete Elemente:

Element	Zulässige Werte	Erläuterung	Standardmäßig
<maximum-revision-queue size="">	positive ganze Zahl	Anzahl der zu speichernden Revisionen.	3
<clean-interval value="">	positive ganze Zahl	Zeitabstand (in Minuten), in dem alte Revisionen gelöscht werden.	60
<unload-interval value="">	positive ganze Zahl	Zeitabstand (in Minuten), in dem nicht mehr benutzte Dateien aus dem Speicher entladen werden.	10
<repo-check mode="">	idle | sync	Cache-Integritätsprüfung beim Start (dauert möglicherweise lange Zeit) oder im Hintergrund.	idle

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

    Einstellungen für die Synchronisierung der Repositorys des Proxyservers und des Dr.Web Servers.

Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`enabled`	`yes` | `no`	Gibt an, ob die Synchronisierung der Repositorys aktiviert ist oder nicht.	`yes`
`schedule`	–	Zeitplan für die Synchronisierung der angegebenen Produkte.	–

Der Wert des Parameters `schedule` wird analog zum Zeitplan für die Synchronisierung in den Einstellungen des Verwaltungscenters bestimmt. Die manuelle Generierung von `schedule` ist zurzeit nicht möglich.

Die Unterelemente `<product name="">` geben die zu synchronisierenden Produkte an:

- 10-drwbases – Virendatenbanken
- 10-drwgatedb – Datenbanken von SpIDer Gate
- 10-drwspamdb – Datenbanken von Anti-Spam
- 10-drwupgrade – Dr.Web Updater
- 15-drwappcntrl – vertrauenswürdige Anwendungen der Anwendungskontrolle
- 15-drwhashdb – bekannte Hashwerte von Bedrohungen
- 20-drwagent – Dr.Web Agent für Windows
- 20-drwandroid11 – Dr.Web Agent für Android
- 20-drwunix – Dr.Web Agent für UNIX
- 40-drwproxy – Dr.Web Proxyserver
- 70-drwextra – Dr.Web Unternehmensprodukte
- 70-drwutils – Dr.Web Dienstprogramme

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

  Einstellungen für das Caching von Ereignissen der Agents.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
`enabled`	`yes` | `no`	Gibt an, ob das Caching von Ereignissen aktiviert ist oder nicht. Wenn das Zwischenspeichern aktiviert ist, werden Ereignisse entsprechend dem Zeitplan an den Server gesendet. Wenn das Zwischenspeichern deaktiviert ist, werden die Ereignisse an den Server gesendet, sobald der Proxyserver sie empfangen hat.	`yes`

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
schedule	–	Zeitplan für die Übertragung der von den Agents gesendeten Ereignisse.	–

Der Wert des Parameters `schedule` wird analog zum Zeitplan für den Versand von Ereignissen in den Einstellungen des Verwaltungscenters bestimmt. Die manuelle Generierung von `schedule` ist zurzeit nicht möglich.

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

  Automatische Aktualisierung des Proxyservers.

  Falls die Synchronisierung aktiviert ist, werden bei der aktivierten automatischen Aktualisierung die Updates für den Proxyserver vom Server entsprechend dem Synchronisierungszeitplan (siehe oben) heruntergeladen und entsprechend dem Update-Zeitplan (standardmäßig zeitlich nicht begrenzt) installiert. Falls die Synchronisierung deaktiviert ist, werden die Updates entsprechend dem Update-Zeitplan (standardmäßig zeitlich nicht begrenzt) heruntergeladen und installiert.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
enabled	yes | no	Gibt an, ob die automatische Aktualisierung aktiviert ist oder nicht.	yes
schedule	–	Zeitplan, nach dem die Updates heruntergeladen und installiert werden (wenn keine Synchronisierung verwendet wird).	–

Die manuelle Generierung von `schedule` ist zurzeit nicht möglich. Die automatische Aktualisierung wird standardmäßig zeitlich nicht begrenzt.

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

  Bestimmt, wie und wie viele Speicherauszüge bei einer SEH-Ausnahme gesammelt werden sollen.

Das Konfigurieren von Speicherauszügen ist nur unter Windows möglich.

Das Betriebssystem muss die Bibliothek `dbghelp.dll` enthalten, damit Speicherauszüge erfasst werden können.

Speicherauszüge werden im folgenden Verzeichnis gespeichert: `%All Users\Application Data%\Doctor Web\drwcsd-proxy-dump\`

Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung	Standardmäßig
enabled	yes | no	Gibt an, ob das Sammeln von Speicherauszügen aktiviert ist oder nicht.	yes
maximum	positive ganze Zahl	Maximale Anzahl von Speicherauszügen. Ältere Speicherauszüge werden gelöscht.	10

- <dns>

  DNS-Einstellungen.

  <timeout value="">

  Zeitlimit (in Sekunden) für die Auflösung von direkten/inversen DNS-Anfragen. Wenn kein Wert angegeben ist, gibt es kein Zeitlimit für die Auflösung.

  <retry value="">

  Maximale Anzahl von DNS-Wiederholungsanfragen bei der fehlgeschlagenen Auflösung einer DNS-Anfrage.

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

  Dauer, für welche die Antworten des DNS-Servers im Cache gespeichert werden sollen.

  Beschreibung der Attribute:

Attribut	Zulässige Werte	Erläuterung
enabled	• yes – Antworten im Cache speichern. • no – keine Antworten im Cache speichern.	Modus, mit dem die Antworten im Cache gespeichert werden sollen.
negative-ttl	–	Zeitraum für die Speicherung im Cache (TTL) negativer Antworten des DNS-Servers in Minuten.
positive-ttl	–	Zeitraum für die Speicherung im Cache (TTL) positiver Antworten des DNS-Servers in Minuten.

<servers>

Liste der DNS-Server, welche die Standard-Systemliste ersetzen soll. Diese enthält ein oder mehrere untergeordnete Elemente <server address="">, in denen der Parameter address für die IP-Adresse des Servers steht.

<domains>

Liste der DNS-Domänen, welche die Standard-Systemliste ersetzen soll. Diese enthält ein oder mehrere untergeordnete Elemente <domain name="">, in denen der Parameter name für den Namen der Domäne steht.

G5. Konfigurationsdatei des Repository Loaders

Die Konfigurationsdatei des Repository Loaders `drwreploader.conf` hat das XML-Format und befindet sich im Verzeichnis `etc` des Server-Installationsverzeichnisses.

So nutzen Sie die Konfigurationsdatei

- Falls Sie die Konsolenversion verwenden, muss der Pfad zur Datei im Schalter `--config` angegeben sein.
- Falls Sie die grafische Version verwenden, muss sich die Datei im gleichen Verzeichnis wie das Tool selbst befinden. Wenn Sie die grafische Version ohne die Konfigurationsdatei starten, wird sie im gleichen Verzeichnis erstellt und im Nachhinein vom Tool verwendet.

Beschreibung der Parameter der Konfigurationsdatei des Repository Loaders:

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

  Beschreibung der Attribute:

Attribut	Erläuterung	Zulässige Werte
`value`	Modus, in dem die Updates geladen werden: • `repository` – erzwingt den Download des Repository im Format des Server-Repository. Die heruntergeladenen Dateien können über das Verwaltungscenter als Updates des Server-Repository importiert werden. • `mirror` – erzwingt den Download des Repository im Format der Update-Zone des GUS. Die heruntergeladenen Dateien können dann auf dem Aktualisierungsspiegel Ihres lokalen Netzwerks freigegeben werden. Sie können die Server so einstellen, dass sie die Updates direkt von diesem Aktualisierungsspiegel, der jeweils die letzte Version des Repository enthält, beziehen.	`repository | mirror`
`path`	Verzeichnis, in welches das Repository heruntergeladen werden soll.	–
`archive`	Das heruntergeladene Repository automatisch in einem ZIP-Archiv komprimieren. Dadurch kann das heruntergeladene Repository auf dem Server über das Verwaltungscenter unter **Administration** → **Repository-Inhalt** als ZIP-Datei importiert werden.	`yes | no`
`key`	Datei des Dr.Web Lizenzschlüssels. Alternativ können Sie den MD5-Hashwert des Lizenzschlüssels angeben, der im Verwaltungscenter unter **Administration** → **Lizenz-Manager** angezeigt ist.	–

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

Protokolleinstellungen für den Repository Loader.

Beschreibung der Attribute:

Attribut	Erläuterung	Zulässige Werte
path	Pfad zur Protokolldatei.	–
verbosity	Protokollierungsstufe. Voreingestellt: TRACE3.	ALL, DEBUG3, DEBUG2, DEBUG1, DEBUG, TRACE3, TRACE2, TRACE1, TRACE, INFO, NOTICE, WARNING, ERROR, CRIT. Die Werte ALL und DEBUG3 sind identisch.
rotate	Modus für die Rotation des Protokolls im Format <*N*><*f*>,<*M*><*u*>. Diese Einstellung ist identisch mit der Einstellung für die Rotation des Server-Protokolls. Der Standardwert ist 10,10m, d. h. 10 Dateien je 10 Megabytes speichern und Komprimierung verwenden.	–

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

  Allgemeine Einstellungen für den Download des Repository.

  Beschreibung der Attribute:

Attribut	Erläuterung	Zulässige Werte
url	Verzeichnis auf den Servern des GUS, das die Updates für Dr.Web Produkte beinhaltet.	–
proto	Protokoll, über das die Updates aus den Update-Servern heruntergeladen werden sollen. Die Updates werden entsprechend den Einstellungen in der Liste der GUS-Server heruntergeladen.	http | https | ftp | ftps | sftp | scp | file
cdn	Content Delivery Network beim Download des Repository zulassen.	yes | no
update-key	Pfad zum öffentlichen Schlüssel oder zum Verzeichnis mit dem öffentlichen Schlüssel, mit dem die Signaturen der über das GUS heruntergeladenen Updates überprüft werden. Öffentliche Schlüssel für die Überprüfung der Updates update-key-*.upub finden sich auf dem Dr.Web Server im Verzeichnis etc.	–
version	Version des Dr.Web Servers, für den die Updates heruntergeladen werden sollen.	–

  - <servers>

Liste der Update-Server. Alle GUS-Server werden in der Reihenfolge aufgelistet, in der sie beim Download des Repository vom Tool angesprochen werden.

Das Element enthält Unterelemente <server>, in denen Update-Server angegeben werden.

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

Anmeldedaten des Benutzers, die zur Authentifizierung (sofern erforderlich) am Update-Server verwendet werden sollen.

Beschreibung der Attribute:

Attribut	Erläuterung
user	Benutzername am Update-Server.
password	Passwort am Update-Server.

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

Einstellungen für die Proxy-Verbindung mit dem GUS.

Beschreibung der Attribute:

Attribut	Erläuterung
host	Netzwerkadresse des verwendeten Proxyservers.
port	Portnummer des verwendeten Proxyservers. Voreingestellt: 3128.
user	Benutzername am Proxyserver, falls der verwendete Proxyserver eine Autorisierung erfordert.
password	Passwort am Proxyserver, falls der verwendete Proxyserver eine Autorisierung erfordert.

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

SSL-Zertifikate, die automatisch angenommen werden sollen. Diese Einstellung ist nur für sichere Verbindungen wirksam.

Beschreibung der Attribute:

Attribut	Erläuterung	Zulässige Werte
cert-mode	Zertifikate, die automatisch angenommen werden sollen.	▫ any – alle Zertifikate annehmen. ▫ valid – nur überprüfte Zertifikate annehmen. ▫ drweb – nur Zertifikate von Dr.Web annehmen. ▫ custom – benutzerdefinierte Zertifikate annehmen.
cert-file	Pfad zur Zertifikatsdatei.	–

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

Autorisierungstyp für den Update-Server, wenn auf ihn über SCP/SFTP zugegriffen wird.

Beschreibung der Attribute:

Attribut	Erläuterung	Zulässige Werte
mode	Autorisierungstyp.	▫ pwd – passwortbasierte Autorisierung. Das Passwort wird im Tag <auth /> festgelegt. ▫ pubkey – Autorisierung mit dem öffentlichen Schlüssel. Der öffentliche Schlüssel wird über das Attribut pubkey festgelegt oder aus dem unter prikey angegebenen privaten Schlüssel abgeleitet.
pubkey	Öffentlicher SSH-Schlüssel	–
prikey	Privater SSH-Schlüssel	–

- **<products>**

  Produkte, die heruntergeladen werden sollen.

  ▫ **<product** name="" update="">

  Einstellungen eines einzelnen Produkts.

  Beschreibung der Attribute:

Attribut	Erläuterung	Zulässige Werte
name	Produktname.	• 05-drwmeta – Sicherheitsdaten des Dr.Web Servers • 10-drwbases – Virendatenbanken • 10-drwgatedb – Datenbanken von SpIDer Gate • 10-drwspamdb – Datenbanken von Anti-Spam • 10-drwupgrade – Dr.Web Updater • 20-drwagent – Dr.Web Agent für Windows • 20-drwandroid11 – Dr.Web Agent für Android • 20-drwcs – Dr.Web Server • 20-drwunix – Dr.Web Agent für UNIX • 40-drwproxy – Dr.Web Proxyserver • 80-drwnews – Nachrichten von Doctor Web
update	Download dieses Produkts aktivieren.	yes | no

- **<schedule>**

  Update-Zeitplan. Das Repository wird automatisch mit der festgelegten Häufigkeit heruntergeladen, ohne dass Sie das Tool manuell starten müssen.

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

  Planmäßige Updates.

Attribut	Erläuterung	Zulässige Werte
`period`	Häufigkeit, mit der die Updates heruntergeladen werden sollen.	• `every_n_min` – alle N Minuten • `hourly` – stündlich • `daily` – täglich • `weekly` – wöchentlich
`enabled`	Aufgabe zum Download ist aktiviert.	`yes | no`
`min`	Minute, in der die Aufgabe ausgeführt werden soll.	Ganze Zahlen von 0 bis 59
`hour`	Stunde, in der die Aufgabe ausgeführt werden soll. Der Parameter ist für die Intervalle `daily` und `weekly` relevant.	Ganze Zahlen von 0 bis 23
`day`	Wochentag, an dem die Aufgabe ausgeführt werden soll. Der Parameter ist für das Intervall `weekly` relevant.	• `mon` – Montag • `tue` – Dienstag • `wed` – Mittwoch • `thu` – Donnerstag • `fri` – Freitag • `sat` – Samstag • `sun` – Sonntag

Anhang H. Befehlszeilenparameter in Dr.Web Enterprise Security Suite

Befehlszeilenparameter haben Vorrang vor den Standardeinstellungen oder sonstigen Einstellungen (in der Konfigurationsdatei des Servers, in der Windows-Registrierung u. ä.). In einigen Fällen können die beim Start festgelegten Parameter auch diese Einstellungen außer Kraft setzen. Solche Fälle werden nachfolgend beschrieben.

Der optionale Teil von Parametern einiger Programme wird in eckige Klammern `[...]` gesetzt.

Die unten im Anhang H beschriebenen Besonderheiten gelten nicht für den Netzwerk-Installer des Agents.

Einige Befehlszeilenparameter können mit einem Bindestrich beginnen. Solche Parameter werden ebenfalls als Schalter bezeichnet.

Viele Schalter haben Synonyme. So haben die Schalter, die einen logischen Wert (ja/nein, zulassen/verbieten) implizieren, eine negative Variante. Beispielsweise hat der Schalter `-admin-rights` den Schalter mit dem gegensätzlichen Wert `-no-admin-rights`. Sie können auch mit einem expliziten Wert angegeben werden, z. B. `-admin-rights=yes` und `-admin-rights=no`.

Synonyme für den Wert `yes` sind `on`, `true`, `OK`. Synonyme für den Wert `no` sind `off`, `false`.

Wenn der Wert eines Schalters ein oder mehrere Leerzeichen bzw. Tabulatoren enthält, muss der ganze Parameter in Anführungszeichen gesetzt werden. Beispiele:

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

Schalternamen können abgekürzt werden (durch Abschneiden der letzten Buchstaben), vorausgesetzt, dass der gekürzte Name nicht mit dem ersten Teil eines anderen Schalters übereinstimmt.

Wenn es in der Befehlszeile ein Argument gibt, das mit einem Bindestrich beginnt, muss ein doppeltes Minus "--" davor gesetzt werden, z. B.:

```
[--] initdb D:\Keys\agent.key - - <Passwort>
```

Erläuterung:

- `[--]` – Separates Zeichen, das das Ende der Liste von Schaltern markiert und diese von der Liste zusätzlicher Argumente trennt.
- *<Passwort>* – Zusätzliches Argument.

Um die Ausführung der Befehle mit Administratorrechten unter Windows zu erzwingen, brauchen Sie eventuell den Parameter `elevate` anzugeben. Der Parameter muss allen anderen Schaltern und Parametern voranstehen. Zum Beispiel: `drwcsd elevate start`.

H1. Netzwerk-Installer

Format des Startbefehls:

`drwinst.exe [<Schalter>]`

Schalter

Die Befehlszeilenschalter sind wirksam für alle Installationsdateien des Agents.

Die Startschalter für den Netzwerk-Installer des Agents müssen im folgenden Format angegeben werten: `/<Schalter> <Parameter>`.

Alle Werte müssen durch Leerzeichen voneinander getrennt werden. Beispiele:

`/silent yes`

Wenn der Wert des Schalters ein oder mehrere Leerzeichen, Tabulatoren oder das Zeichen `\` enthält, muss der ganze Parameter in Anführungszeichen gesetzt werden. Beispiele:

```
/pubkey "C:\my folder\drwcsd-certificate.pem"
```

Zulässige Schalter:

- `/compression` <*Modus*> – Komprimierungsmodus für den Datenverkehr des Servers. Der Parameter <*Modus*> kann die folgenden Werte haben:
  - `yes` – Komprimierung verwenden.
  - `no` – keine Komprimierung verwenden.
  - `possible` – Komprimierung ist möglich. Entscheidend sind die serverseitigen Einstellungen.

  Wenn kein Schalter angegeben ist, wird standardmäßig der Wert `possible` verwendet.
- `/encryption` <*Modus*> – Verschlüsselungsmodus für den Datenverkehr des Servers. Der Parameter <*Modus*> kann folgende Werte haben:
  - `yes` – Verschlüsselung verwenden.
  - `no` – keine Verschlüsselung verwenden.
  - `possible` – Verschlüsselung ist möglich. Entscheidend sind die serverseitigen Einstellungen.

  Wenn kein Schalter angegeben ist, wird standardmäßig der Wert `possible` verwendet.

- `/excludeFeatures` <*Komponenten*> – Liste der Komponenten, die von der Installation ausgeschlossen werden sollen. Um mehrere Komponenten anzugeben, verwenden Sie das Zeichen „`,`“ als Trennzeichen. Verfügbare Komponenten:
  - `scanner` – Dr.Web Scanner
  - `spider-mail` – SpIDer Mail
  - `spider-g3` – SpIDer Guard
  - `outlook-plugin` – Dr.Web für Microsoft Outlook
  - `firewall` – Dr.Web Firewall
  - `spider-gate` – SpIDer Gate
  - `parental-control` – Office Control
  - `antispam-outlook` – Dr.Web Anti-Spam für die Komponente Dr.Web für Microsoft Outlook
  - `antispam-spidermail` – Dr.Web Anti-Spam für die Komponente SpIDer Mail

  Die Komponenten, die nicht direkt angegeben sind, behalten ihren Standardstatus der Installation.
- `/id` <*Workstation_ID*> – ID der Workstation, auf welcher der Agent installiert werden soll.

  Der Schalter wird zusammen mit dem Schalter `/pwd` zur automatischen Autorisierung am Server angegeben. Wenn keine Autorisierungsparameter festgelegt sind, sind die Einstellungen des Servers entscheidend.
- `/includeFeatures` <*Komponenten*> – Liste der Komponenten, die auf der Workstation installiert werden sollen. Um mehrere Komponenten anzugeben, verwenden Sie das Zeichen „`,`“ als Trennzeichen. Verfügbare Komponenten:
  - `scanner` – Dr.Web Scanner
  - `spider-mail` – SpIDer Mail
  - `spider-g3` – SpIDer Guard
  - `outlook-plugin` – Dr.Web für Microsoft Outlook
  - `firewall` – Dr.Web Firewall
  - `spider-gate` – SpIDer Gate
  - `parental-control` – Office Control
  - `antispam-outlook` – Dr.Web Anti-Spam für die Komponente Dr.Web für Microsoft Outlook
  - `antispam-spidermail` – Dr.Web Anti-Spam für die Komponente SpIDer Mail

  Die Komponenten, die nicht direkt angegeben sind, behalten ihren Standardstatus der Installation.
- `/installdir` <*Verzeichnis*> – Installationsverzeichnis.

  Wenn kein Schalter angegeben ist, wird die Software in das Verzeichnis "`Program Files\DrWeb`" auf dem Systemdatenträger installiert.
- `/installtimeout` <*Zeit*> – Zeitlimit (in Sekunden) für die Antwort der Workstation, falls die Installation vom Verwaltungscenter aus remote gestartet wird.

  Wenn kein Schalter angegeben ist, wird der Standardwert von 300 Sekunden verwendet.

- `/instMode` <*Modus*> – Startmodus für das Installationsprogramm. Der Parameter <*Modus*> kann den folgenden Wert haben:
  - `remove` – das installierte Produkt deinstallieren.

  Wenn kein Schalter angegeben ist, bestimmt das Installationsprogramm automatisch den Startmodus.
- `/lang` <*Sprachcode*> – Sprache des Installationsprogramms und des Produkts. Der Sprachcode muss der Norm ISO 639-1 entsprechen.

  Wenn kein Schalter angegeben ist, wird standardmäßig die Systemsprache verwendet.
- `/pubkey` <*Zertifikat*> – vollständiger Pfad zur Zertifikatdatei des Servers.

  Wenn kein Zertifikat angegeben ist, verwendet das Installationsprogramm das Zertifikat `*.pem`, das sich im Startverzeichnis befindet. Wenn die Zertifikatdatei in einem anderen Verzeichnis ist, müssen Sie den vollständigen Pfad zur Zertifikatdatei manuell angeben.

  Das Installationspaket, das im Verwaltungscenter generiert wurde, enthält bereits ein Zertifikat. Aus diesem Grund muss die Zertifikatdatei nicht mit angegeben werden.
- `/pwd` <*Passwort*> – Passwort des Agents für den Zugriff auf den Server.

  Der Schalter wird zusammen mit dem Schalter `/id` zur automatischen Autorisierung am Server angegeben. Wenn keine Autorisierungsparameter festgelegt sind, sind die Einstellungen des Servers entscheidend.
- `/regagent` <*Modus*> – bestimmt, ob der Agent der Liste installierter Programme hinzugefügt werden soll. Der Parameter <*Modus*> kann die folgenden Werte haben:
  - `yes` – Agent in der Liste installierter Programme registrieren.
  - `no` – Agent in der Liste installierter Programme nicht registrieren.

  Wenn kein Schalter angegeben ist, wird standardmäßig der Wert `no` verwendet.
- `/retry` <*Anzahl*> – Anzahl von Wiederholungsversuchen beim Suchen nach dem Server mittels Multicast-Anfragen. Wenn die maximale Anzahl von Suchversuchen erreicht wird, wird davon ausgegangen, dass der Server nicht gefunden werden kann.

  Wenn kein Schalter angegeben ist, werden standardmäßig 3 Suchversuche unternommen.
- `/server [`<*Protokoll*>`/]`<*Serveradresse*>`[:`<*Port*>`]` – Adresse des Servers, von dem aus der Agent installiert werden soll und mit dem der Agent anschließend die Verbindung herstellen soll.

  Wenn kein Schalter angegeben ist, wird der Server mittels Multicast gesucht.
- `/silent` <*Modus*> – bestimmt, ob das Installationsprogramm im Hintergrund gestartet werden soll. Der Parameter <*Modus*> kann die folgenden Werte haben:
  - `yes` – Installationsprogramm im Hintergrundmodus starten.
  - `no` – Installationsprogramm im Grafikmodus starten.

  Wenn kein Schalter angegeben ist, startet das Installationsprogramm im Grafikmodus (weitere Informationen finden Sie im Dokument **Installationsanleitung** unter Dr.Web Agent mithilfe des Installationsprogramms installieren).

- `/timeout` <*Zeit*> – Zeitraum (in Sekunden), in dem auf eine Antwort bei der Suche nach dem Server gewartet werden soll. Es wird auf Antwortnachrichten gewartet, bis das festgelegte Zeitlimit überschritten ist.

  Wenn kein Schalter angegeben ist, wird der Standardwert von 3 Sekunden verwendet.

H2. Dr.Web Agent für Windows

Format des Startbefehls:

`es-service.exe [`<*Schalter*>`]`

Schalter

Schalter können in einem der folgenden Formate angegeben werden (beide Formate sind gleichwertig):

`-`<*kurzer_Schalter*>`[ `<*Argument*>`]`

oder

`--`<*langer_Schalter*>`[=`<*Argument*>`]`

Kurze und lange Schalter können kombiniert werden.

Wenn das Argument ein oder mehrere Leerzeichen enthält, muss es in Klammern gesetzt werden.

Alle Schalter werden ausgeführt unabhängig von den Rechten, die der Workstation auf dem Server gewährt wurden. Das heißt: Selbst wenn das Ändern der Einstellungen des Agents auf dem Server nicht zulässig ist, können Sie diese Einstellungen über die Schalter der Befehlszeile ändern.

Zulässige Schalter:

- Hilfe anzeigen:
  - `-?`
  - `--help`
- Adresse des Servers ändern, mit dem sich der Agent verbindet:
  - `-e` <*Server*>
  - `--esserver=`<*Server*>

  Um mehrere Server auf einmal festzulegen, müssen Sie den Schalter für jede Serveradresse durch ein Leerzeichen getrennt angeben. Z. B.:

```
es-service -e 192.168.1.1:12345 -e 192.168.1.2:12345 -e 10.10.1.1:1223
```

oder

```
es-service --esserver=10.3.1.1:123 --esserver=10.3.1.2:123 --
esserver=10.10.1.1:123
```

- Öffentlichen Schlüssel hinzufügen:
  - `-p` <*Schlüssel*>
  - `--addpubkey=`<*Schlüssel*>

  Der als Argument angegebene öffentliche Schlüssel wird ins Verzeichnis des Agents (standardmäßig unter `%ProgramFiles%\DrWeb`) kopiert, in `drwcsd.pub` umbenannt (sofern der Name abweicht) und neu gelesen. Die alte Datei des öffentlichen Schlüssels, sofern diese gefunden ist, wird in `drwcsd.pub.old` umbenannt und wird nicht mehr benutzt.

  Alle vorherigen öffentlichen Schlüssel (die vom Server übertragenen und in der Registry gespeicherten Schlüssel) bleiben erhalten und werden weiterhin verwendet.
- Server-Zertifikat hinzufügen:
  - `-c` <*Zertifikat*>
  - `--addcert=`<*Zertifikat*>

  Das als Argument angegebene Server-Zertifikat wird ins Verzeichnis des Agents (standardmäßig unter `%ProgramFiles%\DrWeb`) kopiert, in `drwcsd-certificate.pem` umbenannt (sofern der Name abweicht) und neu gelesen. Die alte Zertifikatdatei, sofern diese gefunden ist, wird in `drwcsd-certificate.pem.old` umbenannt und wird nicht mehr benutzt.

  Alle vorherigen Zertifikate (die vom Server übertragenen und in der Registry gespeicherten Zertifikate) bleiben erhalten und können wieder verwendet werden.

H3. Dr.Web Server

Es gibt mehrere Befehle zum Starten des Servers. Sie werden nachfolgend einzeln beschrieben.

Die unter H3.1. Dr.Web Server verwalten bis H3.5. Sicherung kritischer Daten des Dr.Web Servers aufgeführten Befehle sind plattformübergreifend, d. h. sie können sowohl unter Windows als auch unter Betriebssystemen der UNIX-Familie verwendet werden, sofern nicht anders angegeben ist.

Wenn einer dieser Befehle nicht fehlerfrei durchgelaufen ist, prüfen Sie sorgfältig die Protokolldatei des Servers, um die Ursache des Problems zu identifizieren (mehr dazu finden Sie im Dokument **Administratorhandbuch** unter Dr.Web Server-Protokoll).

H3.1. Dr.Web Server verwalten

`drwcsd [`<*Schalter*>`]` – Einstellungen des Servers festlegen (mögliche Schalter werden nachfolgend beschrieben).

H3.2. Grundlegende Befehle

- `drwcsd restart` – den Server-Dienst vollständig neu starten (`stop` und `start` werden hintereinander ausgeführt).
- `drwcsd start` – den Server starten.
- `drwcsd stop` – den Server ordnungsgemäß beenden.
- `drwcsd stat` – Statistik in die Protokolldatei schreiben: CPU-Zeit, Speichernutzung usw. (unter UNIX-artigen Betriebssystemen entspricht dieser Schalter dem Befehl `send_signal WINCH` oder `kill SIGWINCH`).
- `drwcsd verifyakey` <*vollständiger_Name_der_Schlüsseldatei*> – Gültigkeit der Lizenzschlüsseldatei (`agent.key`) überprüfen.
- `drwcsd verifyekey` <*vollständiger_Name_der_Schlüsseldatei*> – Gültigkeit der Lizenzschlüsseldatei des Servers (`enterprise.key`) überprüfen. Beachten Sie, dass ab der Version 10 kein Server-Lizenzschlüssel mehr verwendet wird.
- `drwcsd verifyconfig` <*vollständiger_Name_der_Konfigurationsdatei*> – Syntax der Server-Konfigurationsdatei (`drwcsd.conf`) überprüfen.
- `drwcsd verifycache` – Gültigkeit des Dateicache-Inhalts überprüfen.

H3.3. Befehle zur Datenbankverwaltung

Initialisierung der Datenbank

Zum Zeitpunkt der Initialisierung muss die Datenbank nicht vorhanden sein oder leer sein.

`drwcsd [`<*Schalter*>`] initdb [`<*Lizenzschlüssel*>`|- [`<*SQL-Skript*>`|- [`<*INI-Datei*>`|- [`<*Passwort*>` [`<*LUA-Skript*>`|-]]]]]` – Datenbank initialisieren.

- <*Lizenzschlüssel*> – Pfad zum Lizenzschlüssel von Dr.Web `agent.key`. Fall kein Lizenzschlüssel angegeben ist, muss er im Nachhinein über das Verwaltungscenter hinzugefügt werden oder über die Server-zu-Server-Kommunikation von einem Nachbar-Server abgerufen werden.
- <*SQL-Skript*> – Pfad zum SQL-Skript für die Initialisierung der physischen Struktur der Datenbank.
- <*INI-Datei*> – eine im Voraus generierte Datei im Format `drweb32.ini`, mit der die Anfangskonfiguration der Komponenten der Dr.Web Software (für die Gruppe **Everyone**) festgelegt werden soll.
- <*Passwort*> – das Anfangspasswort des Server-Administrators (der Name ist **admin**). Der Standardwert ist **root**.
- <*lua-Skrip*> – Pfad zum Lua-Skript für die Initialisierung der Datenbank (zum Befüllen der Datenbank mit den Standardwerten).

Der Sonderwert (Minuszeichen) „-“ gibt an, dass das Skript nicht verwendet werden soll.

Das Minuszeichen kann ausgelassen werden, wenn ihm keine weiteren Parameter folgen.

Parameter für die Datenbankinitialisierung konfigurieren

Bei der Verwendung einer integrierten Datenbank können die Initialisierungsparameter anhand einer externen Datei festgelegt werden. Dazu dient der folgende Befehl:

`drwcsd.exe initdbex` <*response-file*>

<*response-file*> – Datei, in der die Parameter für die Datenbankinitialisierung zeilenweise und in der gleichen Reihenfolge, wie die Parameter des Befehls `initdb`, gespeichert sind.

Dateiformat:

```
<vollständiger_Name_der_Lizenzschlüsseldatei>

<vollständiger_Name_der_SQL-Skriptdatei>

<vollständiger_Name_der_INI-Datei>

<Administrator-Passwort>
```

Wenn unter Windows die RESPONSE-Datei verwendet wird, können beliebige Zeichen für das Administrator-Passwort verwendet werden.

Zeilen, die dem jeweils erforderlichen Parameter folgen, sind optional. Wenn die Zeile nur aus „-“ (einem Minuszeichen) besteht, wird der Standardwert verwendet (wie bei `initdb`).

Datenbank aktualisieren

`drwcsd [`<*Schalter*>`] updatedb` <*Skript*> – eine Aktion für die Datenbank (z. B. Aktualisierung auf eine neuere Version) durch Ausführung eines SQL-Skripts oder Lua-Skripts aus der angegebenen Datei ausführen.

Upgrade der Datenbank

`drwcsd upgradedb [`<*Verzeichnis*>`]` – den Server zwecks Aktualisierung der Datenbankstruktur beim Umstieg auf eine neuere Version aus dem angegebenen Verzeichnis (siehe das Verzeichnis `update-db`) oder mittels interner Skripte starten.

Datenbank exportieren

a) `drwcsd exportdb` <*Datei*> – Datenbank in die angegebene Datei exportieren.

Beispiel für 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"
```

Unter Betriebssystemen der **UNIX**-Familie wird die Aktion unter dem Konto `drwcs:drwcs` ausgeführt. Die Datei wird in das Verzeichnis `$DRWCS_VAR` exportiert. Unter **FreeBSD** wird die Datei im Verzeichnis gespeichert, in dem das Skript ausgeführt wurde. Wenn Sie den Pfad explizit angeben wollen, müssen Sie sicherstellen, dass das Konto <*Benutzer*>:<*Gruppe*>, das bei der Installation angelegt wurde (standardmäßig `drwcs:drwcs`), über den Schreibzugriff auf dieses Verzeichnis verfügt.

b) `drwcsd xmlexportdb` <*XML-Datei*> – Datenbank in die angegebene XML-Datei exportieren.

Wenn Sie als Dateiendung `gz` angeben, wird die Datenbankdatei als GZIP-Archiv exportiert.

Wenn Sie keine Dateiendung oder nicht `gz` angeben, wird die Datei beim Export nicht archiviert.

Beispiel für Windows:

- So exportieren Sie die Datenbank in eine nicht archivierte XML-Datei:

```
"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
```

- So exportieren Sie die Datenbank in eine archivierte XML-Datei:

```
"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
```

Beispiel für UNIX-basierte Betriebssysteme:

- So exportieren Sie die Datenbank in eine nicht archivierte XML-Datei:

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

- So exportieren Sie die Datenbank in eine archivierte XML-Datei:

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

Datenbank importieren

a) `drwcsd importdb` <*Datei*> – Datenbank von der angegebenen Datei importieren. Der alte Inhalt der Datenbank wird gelöscht.

b) `drwcsd upimportdb <Datei> [<Verzeichnis>]` – Import und Update der Datenbank, die beim Export aus dem Server vorheriger Versionen (der alte Inhalt der DB wird gelöscht) generiert wurde. Sie können den Pfad zum Verzeichnis mit den Skripten zur Aktualisierung der Datenbank beim Umstieg auf eine neuere Version (analog zum Befehl `upgradedb`) angeben.

c) `drwcsd xmlimportdb <XML-Datei>` – Datenbank von der angegebenen XML-Datei importieren.

d) `drwcsd xmlupimportdb <XML-Datei> [<Verzeichnis>]` – Import und Update der Datenbank, die beim XML-Export aus dem Server vorheriger Versionen generiert wurde. Sie können den Pfad zum Verzeichnis mit den Skripten zur Aktualisierung der Datenbank beim Umstieg auf eine neuere Version (analog zum Befehl `upgradedb`) angeben.

e) `drwcsd xmlimportdbnh <XML-Datei>` – Datenbank von der angegebenen XML-Datei importieren, ohne den Hash-Wert der Datei zu berücksichtigen. Dieser Befehl ist hilfreich, wenn die XML-Datei manuell bearbeitet wurde oder der beim Export automatisch geschriebene Hash-Wert der Datei nicht mehr gültig ist.

Vor der Ausführung der Befehle `upimportdb` und `xmlupimportdb` sollten Sie Ihre Datenbank sichern.

Unsachgemäße Anwendung dieser Befehle kann zur Löschung aller Daten in der Datenbank führen.

Die Befehle `upimportdb` und `xmlupimportdb` zum Import mit der gleichzeitigen Aktualisierung der Datenbankversion können nur im gleichen DBMS ausgeführt werden.

Exportdump der Datenbank

`drwcsd [<Schalter>] dumpimportdb <Datenbankdatei> [<SQL-Datei> [<Tabellenfilter>]]` – Informationen über die eingebettete bzw. externe Datenbank in die Protokolldatei des Servers oder in die SQL-Datei schreiben.

Bei der Ausführung des Befehls `dumpimportdb` wird die Datenbank weder exportiert noch importiert.

- *<Datenbankdatei>* ist die Exportdatei der Datenbank, zu der Informationen in das Protokoll des Servers oder in die *<SQL-Datei>* geschrieben werden sollen. Die Exportdatei kann mit dem Befehl `exportdb` generiert werden. Alternativ kann die Datei, die beim Sichern der Datenbank erstellt wurde, verwendet werden. Die mit dem Befehl `xmlexportdb` erstellte XML-Datei kann nicht verwendet werden.
- *<SQL-Datei>* ist eine Datei, in die alle SQL-Abfragen geschrieben werden, die beim Import der Datenbank aus der in der *<Datenbankdatei>* angegebenen Datei ausgeführt werden. Wenn keine SQL-Datei angegeben ist, werden die Daten in das Protokoll des Servers geschrieben (als Liste von Tabellen und deren Felder). Wenn die SQL-Datei angegeben ist, werden die Daten in die SQL-Datei geschrieben.

- <*Tabellenfilter*> ist die Liste von Datenbanktabellen, zu denen Informationen in die <*SQL-Datei*> geschrieben werden sollen. Die Tabellen müssen durch Komma voneinander getrennt angegeben werden. Die Namen müssen den Namen der Tabellen in der Datenbank entsprechen. Zum Beispiel, `admins,groups,stations`. Der Tabellenfilter ist nur beim Schreiben in die SQL-Datei wirksam. Wenn keine Tabellen angegeben sind, werden alle Tabellen ausgegeben.

Datenbank überprüfen

`drwcsd verifydb` – den Server zwecks Überprüfung der Datenbank starten. Damit Informationen zum Ergebnis der Überprüfung in die Protokolldatei geschrieben werden, fügen Sie dem Befehl den Schalter `-log` hinzu. Weitere Informationen zu diesem Schalter finden Sie unter H3.8. Beschreibung der Schalter.

Leistung der Datenbank erhöhen

`drwcsd [`<*Schalter*>`] speedupdb` – Befehle `VACUUM`, `CLUSTER`, `ANALYZE` zur Optimierung der Datenbankleistung ausführen.

Datenbank wiederherstellen

`drwcsd repairdb` – beschädigtes Abbild der eingebetteten **SQLite3**-Datenbank bzw. beschädigte Tabellen der externen **MySQL**-Datenbank reparieren.

Die **SQLite3**-Datenbank kann automatisch beim Start des Servers repariert werden, falls in den Einstellungen der **SQLite3**-Datenbank das Kontrollkästchen **Beschädigtes Abbild automatisch wiederherstellen** aktiviert ist (mehr dazu finden Sie im **Administratorhandbuch** unter Datenbank wiederherstellen).

Datenbank aufräumen

`drwcsd cleandb` – dieser Befehl löscht alle Tabellen und bereinigt somit die DB des Servers.

H3.4. Befehle zur Repository-Verwaltung

Beenden Sie den Server, bevor Sie die Befehle `syncrepository`, `restorerepo` und `saverepo` ausführen.

- `drwcsd syncrepository` – Repository mit dem Dr.Web GUS synchronisieren. Der Befehl startet den Server-Prozess. Der Server greift auf das GUS zu und aktualisiert das Repository, falls neue Updates verfügbar sind.
- `drwcsd rerepository` – Repository vom Datenträger erneut lesen.

- `drwcsd updrepository` – Repository über das Dr.Web GUS aktualisieren. Der Befehl bewirkt, dass der laufende Server auf das GUS zugreift und das Repository aktualisiert, falls neue Updates vorliegen. Falls der Server nicht ausgeführt wird, erfolgt kein Update des Repository.
- `drwcsd [<Schalter>] restorerepo <vollständiger_Archivname>` – Server-Repository aus dem mit dem Befehl `saverepo` erstellten ZIP-Archiv wiederherstellen.
- `drwcsd [<Schalter>] saverepo <vollständiger_Archivname>` – das gesamte Server-Repository im angegebenen ZIP-Archiv speichern. Das mit diesem Befehl erstellte Archiv kann später mit dem Befehl `restorerepo` auf den Server importiert werden.

Archive, welche die Befehlen `restorerepo` und `saverepo` verwenden, sind nicht kompatibel mit den Archiven, die zum Export und Import des Repository über das Verwaltungscenter verwendet werden.

H3.5. Sicherung kritischer Daten des Dr.Web Servers

Mit folgenden Befehlen erstellen Sie eine Sicherungskopie des Servers (sie umfasst die Lizenzschlüssel, den Datenbankinhalt, den privaten Schlüssel, die Konfiguration des Servers und des Verwaltungscenters):

`drwcsd -home=<Pfad> backup [<Verzeichnis> [<Anzahl>]]`

- Kritische Daten des Servers werden in das angegebene Verzeichnis <*Verzeichnis*> kopiert.
- Der Schalter `-home` legt das Installationsverzeichnis des Servers fest.
- Der Parameter <*Anzahl*> legt die Anzahl der zu speichernden Kopien einer Datei fest.

Beispiel für Windows:

```
C:\Program Files\DrWeb Server\bin>drwcsd -home="C:\Program Files\DrWeb
Server" backup C:\a
```

Alle Dateien aus der Sicherungskopie, den Datenbankinhalt ausgenommen, können sofort verwendet werden. Die Sicherungskopie der Datenbank wird im Format `.gz` gespeichert, das mit `gzip` oder anderen Packprogrammen kompatibel ist. Der Datenbankinhalt, der in der Sicherungskopie gespeichert ist, kann in die aktuelle Datenbank des Servers importiert werden. Dadurch können Sie Ihre Daten leicht wiederherstellen (mehr dazu finden Sie unter Datenbank von Dr.Web Enterprise Security Suite wiederherstellen).

Der Dr.Web Server sichert regelmäßig wichtige Daten in folgenden Verzeichnissen:

- Für **Windows**: <*Installationslaufwerk*>`:\DrWeb Backup`
- Für **Linux**: `/var/opt/drwcs/backup`
- Für **FreeBSD**: `/var/drwcs/backup`

Damit die Daten regelmäßig gesichert werden, enthält der Zeitplan des Servers eine entsprechende tägliche Aufgabe. Wenn der Zeitplan diese Aufgabe nicht enthält, sollten Sie diese manuell erstellen.

H3.6. Windows-spezifische Befehle

- `drwcsd [<Schalter>] install [<Dienstname>]` – Serverdienst im System installieren und die angegebenen Schalter zum Start des Dienstes verwenden.

  <Dienstname> – Suffix, das dem Standard-Dienstnamen hinzugefügt wird. Der vollständige Name des Dienstes ist wie folgt: `DrWebES-<Dienstname>`. Der Befehl `install` erstellt (bearbeitet) den Dienst mit dem angegebenen Namen und schreibt automatisch den Schalter `-service=<Dienstname>` in seine Argumente. Die vorhandenen Dienste werden davon nicht betroffen.

- `drwcsd uninstall [<Dienstname>]` – Serverdienst aus dem System löschen.

  <Dienstname> – Suffix, das dem Standard-Dienstnamen hinzugefügt wird. Der vollständige Name des Dienstes ist wie folgt: `DrWebES-<Dienstname>`.

- `drwcsd kill` – Beenden des Serverdiensts erzwingen (falls der Dienst nicht ordnungsgemäß beendet werden konnte). Führen Sie diesen Befehl nur bei dringendem Bedarf aus.

- `drwcsd reconfigure` – Konfigurationsdatei erneut lesen und einen Neustart ausführen (wird schneller ausgeführt, ohne dass ein neuer Prozess gestartet werden muss).

- `drwcsd silent [<Optionen>] <Befehl>` – keine Meldungen vom Server beim Start des im Parameter *<Befehl>* festgelegten Befehls ausgeben. Dieser Befehl wird in Befehlsdateien verwendet, um den Interaktivmodus des Servers zu deaktivieren.

- `drwcsd syncads` – Synchronisierung der Netzwerk-Struktur: Active Directory-Container, die Rechner enthalten, werden zu Gruppen des Antivirus-Netzwerks, in die Workstations verschoben werden.

H3.7. UNIX-spezifische Befehle

- `drwcsd config` – ist mit dem Befehl `reconfigure` bzw. `kill SIGHUP` identisch und erzwingt einen Neustart des Servers.

- `drwcsd interactive` – startet den Server, die Verwaltung wird aber nicht vom Prozess übernommen.

- `drwcsd newkey` – generiert neue Verschlüsselungsschlüssel `drwcsd.pri`, `drwcsd.pub` und das Zertifikat `drwcsd-certificate.pem`.

- `drwcsd readrepo` – bewirkt, dass das Repository vom Datenträger neu gelesen wird (analog zum Befehl `rerepository`).

- `drwcsd selfcert [<Rechnername>]` – generiert ein neues SSL-Zertifikat `(certificate.pem)` und einen privaten RSA-Schlüssel `(private-key.pem)`. Der Parameter legt den Namen des Rechners mit dem installierten Server fest, für den die Dateien generiert werden sollen. Wenn der Parameter nicht angegeben ist, wird der Name des Rechners automatisch vom System festgelegt.

- `drwcsd shell <Dateiname>` – startet eine Skriptdatei. Der Befehl startet `$SHELL` oder `/bin/sh`, indem die angegebene Datei an die Shell übergeben wird.

- `drwcsd showpath` – gibt alle im System registrierten Programmpfade aus.

- `drwcsd status` – gibt den aktuellen Status des Servers (gestartet, beendet) aus.

H3.8. Beschreibung der Schalter

Plattformübergreifende Schalter:

- `-activation-key=<`*Lizenzschlüssel*`>` – Lizenzschlüssel des Servers. Standardmäßig wird die Datei `enterprise.key` verwendet, die sich im Unterverzeichnis `etc` des Wurzelverzeichnisses befindet.

  Beachten Sie, dass ab der Version 10 kein Server-Lizenzschlüssel mehr verwendet wird. Der Schlüssel `-activation-key` wird eventuell beim Upgrade des Servers und bei der Initialisierung der Datenbank verwendet: Die ID des Servers wird dem angegebenen Lizenzschlüssel entnommen.
- `-bin-root=<`*Verzeichnis*`>` – Pfad zu ausführbaren Dateien. Standardmäßig wird das Unterverzeichnis `bin` des Wurzelverzeichnisses verwendet.
- `-conf=<`*Datei*`>` – der Name und Speicherort der Konfigurationsdatei des Servers. Standardmäßig wird die Datei `drwcsd.conf` im Unterverzeichnis `etc` des Wurzelverzeichnisses verwendet.
- `-daemon` – für Windows-Plattformen: als Dienst starten; für UNIX-Plattformen: Prozess wechselt in den Hintergrundmodus (zum Wurzelverzeichnis wechseln, vom Terminal trennen und in den Hintergrundmodus wechseln).
- `-db-verify=on` – Integrität der Datenbank beim Start des Servers überprüfen. Standardwert. Verwenden Sie den gegensätzlichen Wert nur bei dringendem Bedarf. Hierzu zählt nicht der Fall, dass ein Start unmittelbar nach der Überprüfung der Datenbank über den Befehl `drwcsd verifydb` ausgeführt werden muss (s. oben).
- `-help` – Hilfe anzeigen, ist identisch mit den oben beschriebenen Programmen.
- `-hooks` – Ausführung von benutzerdefinierten Erweiterungsskripten durch den Server zulassen. Die Skripte befinden sich im Verzeichnis:
  - Unter Windows: `var\extensions`
  - Unter FreeBSD: `/var/drwcs/extensions`
  - Unter Linux: `/var/opt/drwcs/extensions`

  des Installationsverzeichnisses des Dr.Web Servers. Die Skripte dienen zur Automatisierung sich wiederholender Aufgaben. Alle Skripte sind standardmäßig deaktiviert.
- `-home=<`*Verzeichnis*`>` – Installationsverzeichnis des Servers (Wurzelverzeichnis). Die Struktur dieses Verzeichnisses wird in der **Installationsanleitung** unter Dr.Web Server unter Windows installieren. Standardmäßig ist das aktuelle Verzeichnis beim Start.
- `-log=<`*Protokolldatei*`>` – Protokollierung des Servers in die Datei unter dem angegebenen Pfad aktivieren.

  Für Server unter UNIX-basierten Systemen kann ein Minuszeichen anstatt des Dateinamens angegeben werden. In diesem Fall wird das Protokoll in die Standardausgabe geschrieben.

  Für Windows wird standardmäßig die Datei `drwcsd.log` in dem Verzeichnis verwendet, das durch den Schalter `-var-root` definiert wird. Unter UNIX-Plattformen wird es mit dem Schalter `-syslog=user` festgelegt (s. nachfolgend).

- `-private-key=<privater_Schlüssel>` – der private Schlüssel des Servers. Standardmäßig wird `drwcsd.pri` im Unterverzeichnis `etc` des Wurzelverzeichnisses verwendet.
- `-rotate=<N><f>,<M><u>` – Modus für die Rotation des Serverprotokolls, wobei:

Parameter	Erläuterung
<*N*>	Gesamtzahl der Protokolldateien (einschließlich aktueller Datei und Archivdateien).
<*f*>	Speicherformat für Protokolldateien, mögliche Werte: • z (gzip) – Dateien komprimieren, standardmäßig. • P (plain) – Dateien nicht komprimieren.
<*M*>	Größe der Protokolldatei oder Zeitraum für die Rotation (je nach Wert <*u*>).
<*u*>	Einheit, mögliche Werte: • Für die Rotation nach Dateigröße: ▫ k – KB ▫ m – MB ▫ g – GB • Für die Rotation nach Zeit: ▫ H – Stunden ▫ D – Tage ▫ W – Wochen

Bei der Rotation nach Zeit wird die Synchronisierung unabhängig von der Startzeit des Befehls ausgeführt, d. h, für den Wert H wird die Synchronisierung am Anfang der Stunde, für D am Anfang des Tages und für W am Anfang der Woche (00:00 am Montag) mit der im Parameter <*u*> festgelegten Häufigkeit ausgeführt.

Der Referenzzeitpunkt ist der 1. Januar 1 n. Chr. UTC+0.

Der Standardwert ist `10,10m`, d.h. 10 Dateien je 10 Megabytes speichern und Komprimierung verwenden. Alternativ kann das spezielle Format `none (-rotate=none)` verwendet werden, d. h. keine Rotation verwenden, und in die gleiche Datei unbeschränkter Größe schreiben.

Wenn die Rotation verwendet wird, werden die Dateien wie folgt benannt: `file.<N>.log` oder `file.<N>.log.gz`, wobei <*N*> die laufende Nummer 1, 2 usw. ist.

Nehmen wir an, dass der Name der Protokolldatei (s. oben den Schalter `-log`) `file.log` ist, dann steht:

- `file.log` für die aktuelle Datei (in die geschrieben wird),
- `file.1.log` für die vorherige Datei,
- `file.2.log` usw. Es gilt also: Je höher die Zahl ist, desto älter ist die Version.

- `-trace` – Fehlerort detailliert protokollieren.

- `-var-root=<Verzeichnis>` – Pfad des Verzeichnisses, in das der Server schreiben darf und in dem die geänderten Dateien (z. B. Protokollen sowie Repository-Dateien) gespeichert werden sollen. Standardmäßig ist es das Unterverzeichnis `var` im Wurzelverzeichnis.
- `-verbosity=<Stufe>` – Protokollierungsstufe. Der Standardwert ist `WARNING`. Mögliche Werte: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Die Werte `ALL` und `DEBUG3` sind identisch.

  Sie können bei Bedarf einen Ausführlichkeitsgrad für mehrere Nachrichtenquellen gleichzeitig im folgenden Format festlegen:

  `-verbosity=<Nachrichtenquelle1>:<Ausführlichkeitsgrad1>,<Nachrichtenquelle2>:<Ausführlichkeitsgrad2>,<Nachrichtenquelle3>:<Ausführlichkeitsgrad3>` usw. Der `<Ausführlichkeitsgrad>` wird dabei nach allgemeinem Prinzip geerbt: Es wird also nach der nächsten übergeordneten Nachrichtenquelle gesucht, die den angegebenen Ausführlichkeitsgrad hat. Der Schalter `-verbosity=all:all` ist identisch mit dem Schalter `-verbosity=all` (siehe auch Anhang K. Formate von Protokolldateien).

  Dieser Schalter definiert die Ausführlichkeit des Protokolls, das in die Datei, die in dem ihm folgenden Schalter `-log` (s. oben) angegeben ist, geschrieben werden soll. Der Befehl kann mehrere Schalter dieses Typs enthalten.

  Die Schalter `-verbosity` und `-log` sind positionsabhängig.

  Wenn diese Schalter gleichzeitig verwendet werden, muss der Schalter `-verbosity` vor dem Schalter `-log` stehen: Der Schalter `-verbosity` ändert die Ausführlichkeit der Protokolle, die sich in den Verzeichnissen befinden, die nachfolgend in der Befehlszeile angegeben sind.

Windows-spezifische Schalter:

- `-minimized` – das Fenster minimieren (nur im Interaktivmodus).
- `-service=<Dienstname>` – diesen Schalter verwendet der gestartete Dienstprozess für die Selbstidentifikation und den Schutz des entsprechenden Registrierungsschlüssel des Server-Dienstes. `<Dienstname>` – Suffix, das dem Standard-Dienstnamen hinzugefügt wird. Der vollständige Name des Dienstes ist wie folgt: `DrWebES-<Dienstname>`.

  Der Schalter wird vom Befehl `install` verwendet, eine selbständige Verwendung ist nicht vorgesehen.
- `-screen-size=<Größe>` – (nur im Interaktivmodus) – die Größe (in Zeilen) des Protokolls, das im Fenster des Servers angezeigt wird. Der Standardwert ist 1000.

UNIX-spezifische Schalter:

- `-etc=<Pfad>` – Pfad des Verzeichnisses `etc` (`<var>/etc`).
- `-keep` – den Inhalt des temporären Verzeichnisses nach der Installation des Servers behalten.
- `-pid=<Datei>` – Datei, in die der Server die Prozess-ID schreibt.

- `-syslog=<Modus>` – Schreiben in das Systemprotokoll. Mögliche Modi: `auth, cron, daemon, kern, lpr, mail, news, syslog, user, uucp, local0 – local7`. Für einige Plattformen sind auch `ftp, authpriv` und `console` möglich.

  > Die Schalter `-syslog` und `-log` können nur gemeinsam ausgeführt werden. Wenn der Server mit dem Schalter `-syslog` gestartet wird (zum Beispiel, `service drwcsd start -syslog=user`), wird der Server mit dem festgelegten Wert für den Schalter `-syslog` und mit dem Standardwert für den Schalter `-log` gestartet.

- `-user=<Benutzer>`, `-group=<Gruppe>` – sind nur unter UNIX und beim Start durch den Benutzer **root** verfügbar. Diese Schalter erzwingen Änderung des Benutzers bzw. der Gruppe des Prozesses und benötigen die Rechte des angegebenen Benutzers (der Gruppe).

H3.9. UNIX-spezifische Variablen

Um die Verwaltung des Servers unter UNIX-basierten Betriebssystemen zu erleichtern, kann der Administrator die Variablen verwenden, die sich in der Datei des Skripts /etc/init.d/drwcsd befinden. Diese Datei befindet sich im folgenden Verzeichnis:

- Für Linux: `/etc/init.d/drwcsd`.
- Für FreeBSD: `/usr/local/etc/rc.d/drwcsd` (symbolische Verknüpfung auf `/usr/local/etc/drweb.com/software/init.d/drwcsd`).

Tabelle H-1 veranschaulicht die Übereinstimmung zwischen den Variablen und Befehlszeilenschaltern für `drwcsd`.

Tabelle H-1.

Schalter	Variable	Standardparameter
`-home`	DRWCS_HOME	• `/usr/local/drwcs` – für FreeBSD • `/opt/drwcs` – für Linux
`-var-root`	DRWCS_VAR	• `/var/drwcs` – für FreeBSD • `/var/opt/drwcs` – für Linux
`-etc`	DRWCS_ETC	`$DRWCS_VAR/etc`
`-rotate`	DRWCS_ROT	`10,10m`
`-verbosity`	DRWCS_LEV	`info`
`-log`	DRWCS_LOG	`$DRWCS_VAR/log/drwcsd.log`
`-conf`	DRWCS_CFG	`$DRWCS_ETC/drwcsd.conf`
`-pid`	DRWCS_PID	

Schalter	Variable	Standardparameter
-user	DRWCS_USER	
-group	DRWCS_GROUP	
-hooks	DRWCS_HOOKS	
-trace	DRWCS_TRACE	

Die Variablen DRWCS_HOOKS und DRWCS_TRACE haben keine Parameter. Wenn die Variablen angegeben sind, werden die entsprechenden Schalter bei der Ausführung des Skripts hinzugefügt. Wenn keine Variablen angegeben sind, werden keine Schalter hinzugefügt.

Andere Variablen sind in der Tabelle H-2 aufgeführt.

Tabelle H-2.

Variable	Standardparameter	Erläuterung
DRWCS_ADDOPT		Zusätzliche Schalter, die beim Start an drwcsd übergeben werden müssen.
DRWCS_CORE	unlimited	Maximale Größe der CORE-Datei.
DRWCS_FILES	131170	Die maximale Anzahl von Dateihandles, die der Server öffnen kann.
DRWCS_BIN	$DRWCS_HOME/bin	Verzeichnis, aus dem drwcsd gestartet werden soll.
DRWCS_LIB	$DRWCS_HOME/lib	Verzeichnis mit den Bibliotheken des Servers.

Die Werte der Standardparameter werden wirksam, wenn diese Variablen im Skript /etc/init.d/drwcsd nicht angegeben sind.

Die Variablen DRWCS_HOME, DRWCS_VAR, DRWCS_ETC, DRWCS_USER, DRWCS_GROUP, DRWCS_HOOKS sind bereits definiert in der Datei des Skripts drwcsd.

Wenn die Datei /var/opt/drwcs/etc/common.conf vorhanden ist, wird diese Datei zu drwcsd hinzugefügt. Dadurch können einige Variablen neu definiert werden. Wenn aber diese nicht exportiert werden (über den Befehl export), werden sie nicht wirksam.

So legen Sie die Variablen fest

1. Fügen Sie die Variablendefinition in der Datei des Skripts `drwcsd` hinzu.
2. Exportieren Sie die Variable mit dem Befehl `export` (wird ebenso dort angegeben).
3. Wenn ein weiterer Prozess aus diesem Skript gestartet wird, liest dieser Prozess die festgelegten Werte aus.

H3.10. Dr.Web Server unter UNIX-basierten Betriebssystemen über den Befehl kill verwalten

Der Server unter UNIX wird mittels Signalen verwaltet, die an den Prozess des Servers durch das Dienstprogramm `kill` gesendet werden.

Hilfe zum Dienstprogramm `kill` können Sie mit dem Befehl `man kill` abrufen.

Signale des Dienstprogramms und deren Aktionen:

- `SIGWINCH` – Statistiken in die Protokolldatei schreiben (CPU-Zeit, Speichernutzung usw.).
- `SIGUSR1` – Repository vom Datenträger neu lesen.
- `SIGUSR2` – Benachrichtigungsvorlagen vom Datenträger neu lesen.
- `SIGHUP` – Server neu starten.
- `SIGTERM` – Server beenden.
- `SIGQUIT` – Server beenden.
- `SIGINT` – Server beenden.

Diese Aktionen für den Server unter Windows werden mit den Schaltern des Befehls drwcsd ausgeführt. Mehr dazu finden Sie im Anhang H3.3. Befehle zur Datenbankverwaltung.

H4. Dr.Web Scanner für Windows

Diese Komponente der Software der Workstation verwendet die Befehlszeilenparameter, die im Benutzerhandbuch **Dr.Web Agent für Windows** beschrieben sind. Der einzige Unterschied besteht darin, dass die Parameter `/go /st` automatisch und obligatorisch an den Scanner gesendet werden, wenn der Scanner vom Agent gestartet wird.

H5. Dr.Web Proxyserver

Um die Einstellungen des Proxyservers zu konfigurieren, starten Sie die ausführbare Datei `drwcsd-proxy` mit entsprechenden Schaltern. Die Datei befindet sich im Unterverzeichnis `bin` des Installationsverzeichnisses des Proxyservers.

Format des Startbefehls

`drwcsd-proxy [<Schalter>] [<Befehle> [<Argumente>]]`

Zulässige Schalter

Plattformübergreifende Schalter:

- `--console=yes|no` – Proxyserver im Interaktivmodus starten. Das Protokoll des Proxyservers wird dabei in der Konsole ausgegeben.

  Standardmäßig: `no`.
- `--etc-root=<Pfad>` – Pfad zum Verzeichnis mit den Konfigurationsdateien (`drwcsd-proxy.conf`, `drwcsd.proxy.auth` usw.).

  Standardmäßig: `$var/etc`
- `--home=<Pfad>` – Pfad zum Installationsverzeichnis des Proxyservers.

  Standardmäßig: `$exe-dir/`
- `--log-root=<Pfad>` – Pfad zum Verzeichnis mit den Protokolldateien des Proxyservers.

  Standardmäßig: `$var/log`
- `--pool-size=<N>` – Anzahl von Threads für die Verarbeitung von Client-Verbindungen.

  Standardmäßig: Anzahl der Prozessorkerne des Rechners, auf dem der Proxyserver eingerichtet ist (mindestens 2).
- `--rotate=<N><f>,<M><u>` – Modus für die Rotation des Proxyserver-Protokolls, wobei:

Parameter	Erläuterung
<*N*>	Gesamtzahl der Protokolldateien (einschließlich aktueller Datei und Archivdateien).
<*f*>	Speicherformat für Protokolldateien, mögliche Werte: • z (gzip) – Dateien komprimieren, standardmäßig. • P (plain) – Dateien nicht komprimieren.
<*M*>	Größe der Protokolldatei oder Zeitraum für die Rotation (je nach Wert <*u*>).

<*u*>	Einheit, mögliche Werte:
	• Für die Rotation nach Dateigröße:
	  ▫ k – KB
	  ▫ m – MB
	  ▫ g – GB
	• Für die Rotation nach Zeit:
	  ▫ H – Stunden

Parameter	Erläuterung
	▫ D – Tage ▫ W – Wochen

Bei der Rotation nach Zeit wird die Synchronisierung unabhängig von der Startzeit des Befehls ausgeführt, d. h, für den Wert H wird die Synchronisierung am Anfang der Stunde, für D am Anfang des Tages und für W am Anfang der Woche (00:00 am Montag) mit der im Parameter <*u*> festgelegten Häufigkeit ausgeführt.

Der Referenzzeitpunkt ist der 1. Januar 1 n. Chr. UTC+0.

Der Standardwert ist `10,10m`, d. h. 10 Dateien je 10 Megabytes speichern und Komprimierung verwenden.

- `--trace=yes|no` – detaillierte Protokollierung der Zugriffe auf den Proxyserver aktivieren. Dieser Schalter ist nur verfügbar, wenn der Build des Proxyservers detaillierte Protokollierung des Aufrufstapels unterstützt (wenn eine Ausnahme auftritt, wird der Aufrufstapel ins Protokoll geschrieben).

  Standardmäßig: `no`.

- `--tmp-root=`<*Pfad*> – Pfad zum Verzeichnis mit temporären Dateien. Der Schalter wird verwendet, wenn der Proxyserver automatisch aktualisiert wird.

  Standardmäßig: `$var/tmp`.

- `--var-root=`<*Pfad*> – Pfad zum Arbeitsverzeichnis des Proxyservers, in dem der Cache und die Datenbank gespeichert werden.

  Standardmäßig:

  ▫ Unter Windows: `%ALLUSERSPROFILE%\Doctor Web\drwcs`

  ▫ Unter Linux: `/var/opt/drwcs`

  ▫ Unter FreeBSD: `/var/drwcs`

- `--verbosity=`<*Ausführlichkeitsgrad*> – Protokollierungsstufe. Der Standardwert ist `TRACE`. Mögliche Werte: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Die Werte `ALL` und `DEBUG3` sind identisch.

  Sie können bei Bedarf einen Ausführlichkeitsgrad für mehrere Nachrichtenquellen gleichzeitig im folgenden Format festlegen:

  `-verbosity=`<*Nachrichtenquelle1*>`:`<*Ausführlichkeitsgrad1*>`,`<*Nachrichtenquelle2*>`:`<*Ausführlichkeitsgrad2*>`,`<*Nachrichtenquelle3*>`:`<*Ausführlichkeitsgrad3*> usw. Der <*Ausführlichkeitsgrad*> wird dabei nach allgemeinem Prinzip geerbt: Es wird also nach der nächsten übergeordneten Nachrichtenquelle gesucht, die den angegebenen Ausführlichkeitsgrad hat. Der Schalter `-verbosity=all:all` ist identisch mit dem Schalter `-verbosity=all` (siehe auch Anhang K. Formate von Protokolldateien).

Alle Schalter für die Festlegung der Parameter des Proxyservers können gleichzeitig angegeben werden.

UNIX-spezifische Schalter:

- `--user` – Benutzer-ID festlegen. Der Schalter ist relevant sowohl für den normalen Modus als auch für den Daemon-Modus.
- `--group` – Gruppen-ID festlegen. Der Schalter ist relevant sowohl für den normalen Modus als auch für den Daemon-Modus.
- `--pid=`<*Pfad*> – Pfad zum Verzeichnis mit der Prozess-ID.

  Standardmäßig: `/var/opt/drwcs/run/drwcsd-proxy.pid`

Zulässige Befehle und dazugehörige Argumente

Wenn kein Befehl angegeben ist, wird standardmäßig der Befehl `run` verwendet.

- `import` <*Pfad*> `[`<*Revision*>`]` `[`<*Produkte*>`]` – Dateien aus dem Repository des Dr.Web Servers in den Cache des Proxyservers importieren.
  - <*Pfad*> – Pfad zum Verzeichnis mit dem Repository des Dr.Web Servers. Das Server-Repository muss vorab auf den Rechner mit dem installierten Proxyserver heruntergeladen werden.
  - <*Revision*> – maximale Anzahl der zu importierenden Revisionen. Wenn kein Wert angegeben ist, werden alle Revisionen importiert.
  - <*Produkte*> – Liste der Produkte (durch Leerzeichen getrennt), die importiert werden sollen. Die Liste ist standardmäßig leer, was bedeutet, dass alle Produkte des Repository außer dem Dr.Web Server importiert werden. Wenn die Liste nicht leer ist, werden nur die in der Liste angegebenen Produkte importiert.
- `help` – Hilfe zu Schaltern für die Konfiguration des Proxyservers anzeigen.
- `run` – Proxyserver im normalen Modus starten.

Windows-spezifische Befehle:

- `install` – Service installieren.
- `start` – installierten Service starten.
- `stop` – installierten Service beenden.
- `uninstall` – Service deinstallieren.

UNIX-spezifische Befehle:

- `daemon` – Proxyserver als Daemon starten (siehe auch UNIX-spezifische Schalter).

Skript zur Steuerung des Proxyservers und UNIX-spezifische Variablen

Um die Verwaltung des Proxyservers unter UNIX-basierten Betriebssystemen zu erleichtern, kann der Administrator die Variablen verwenden, die sich in der Skriptdatei `drwcsd-proxy.sh` befinden. Diese Datei liegt im folgenden Verzeichnis:

- **Linux**: `/etc/init.d/dwcp_proxy`
- **FreeBSD**: `/usr/local/etc/rc.d/dwcp_proxy`

Das Skript kann folgende Befehle ausführen:

- `import` <*Pfad*> `[`<*Revision*>`]` `[`<*Produkte*>`]` – Dateien aus dem Repository des Dr.Web Servers in den Cache des Proxyservers importieren (identisch mit dem obigen Befehl für den Proxyserver).
- `interactive` – Proxyserver im Interaktivmodus starten. Das Protokoll des Proxyservers wird dabei in der Konsole ausgegeben.
- `start` – Proxyserver als Dämon starten.
- `status` – prüfen, ob der Dämon gestartet ist.
- `stop` – laufenden Dämon beenden.

Tabelle H-3 veranschaulicht die Übereinstimmung zwischen den Variablen und Befehlszeilenschaltern für `drwcsd-proxy`.

Tabelle H-3.

Schalter	Variable	Standardparameter
`--home=`<*Pfad*>	`$DRWCS_PROXY_HOME`	`$exe-dir/`
`--var-root=`<*Pfad*>	`$DRWCS_PROXY_VAR`	• Unter Linux: `/var/opt/drwcs` • Unter FreeBSD: `/var/drwcs`
`--etc-root=`<*Pfad*>	`$DRWCS_PROXY_ETC`	`$var/etc`
`--tmp-root=`<*Pfad*>	`$DRWCS_PROXY_TMP`	`$var/tmp`
`--log-root=`<*Pfad*>	`$DRWCS_PROXY_LOG`	`$var/log`
–	`$DRWCS_PROXY_LIB`	`$DRWCS_PROXY_HOME/lib`
–	`$DRWCS_PROXY_BIN`	`$DRWCS_PROXY_HOME/bin`
`--verbosity=`<*Ausführlichkeitsgrad*>	`$DRWCS_PROXY_VERBOSITY`	`INFO`

Schalter	Variable	Standardparameter
`--rotate=<N><f>,<M><u>`	`$DRWCS_PROXY_ROTATE`	`10,10m`
`--pid`	`$DRWCS_PROXY_PID`	`/var/opt/drwcs/run/drwcsd-proxy.pid`
-	`$NO_DRWCS_PROXY_USER`	Wenn ein Wert festgelegt ist, wird `$DRWCS_PROXY_USER` ignoriert.
`--user`	`$DRWCS_PROXY_USER`	-
-	`$NO_DRWCS_PROXY_GROUP`	Wenn ein Wert festgelegt ist, wird `$DRWCS_PROXY_GROUP` ignoriert.
`--group`	`$DRWCS_PROXY_GROUP`	-
-	`$DRWCS_PROXY_FILES`	131170 aber nicht kleiner als das aktuelle Limit.

H6. Installationsprogramm des Dr.Web Servers für Betriebssysteme der UNIX-Familie

Format des Startbefehls:

<Paketname>`.run [`*<Schalter>*`] [--] [`*<Argumente>*`]`

wobei:

- `[--]` – ein separates optionales Zeichen, welches das Ende der Liste von Schaltern markiert und diese von der Liste zusätzlicher Argumente trennt.
- `[`*<Argumente>*`]` – zusätzliche Argumente oder eingebettete Skripte.

Befehle zur Anzeige der Hilfe oder Informationen zu einem Paket:

- `--help` – Hilfe zu Schaltern anzeigen.
- `--info` – Detaillierte Informationen zum Paket anzeigen: darunter Name; Zielverzeichnis; Größe nach dem Extrahieren; Komprimierungsalgorithmus; Archivierungsdatum; Version von `makeself`, mit dem das Paket archiviert wurde; Befehl, der zum Archivieren ausgeführt wurden; Skript, das nach dem Extrahieren gestartet werden soll; Informationen darüber, ob der Inhalt des Archivs kopiert werden soll (wenn nicht, werden keine Informationen ausgegeben) und ob das Zielverzeichnis nach der Ausführung des Skripts gelöscht werden soll.
- `--list` – Liste der Dateien im Installationspaket anzeigen.
- `--check` – Integrität des Installationspakets überprüfen.

Befehle zum Starten des Pakets:

- `--confirm` – Aufforderung zur Bestätigung vor dem Start des eingebetteten Skripts ausgeben.
- `--noexec` – eingebettetes Skript nicht ausführen.
- `--target` <*Verzeichnis*> – Installationspaket in das angegebene Verzeichnis extrahieren.
- `--tar` <*Argument_1*> `[`<*Argument_2*> ...`]` – Zugriff auf den Inhalt des Installationspakets mit dem Befehl `tar` erlangen.

Zusätzliche Argumente:

- `--help` – Hilfe zu den zusätzlichen Argumenten anzeigen.
- `--quiet` – Installationsprogramm im Hintergrund starten. Alle darauffolgenden Fragen werden bejaht:
  - Lizenzvereinbarung annehmen.
  - Sicherungskopie im Standardverzeichnis erstellen.
  - Installation fortsetzen, vorausgesetzt dass die zusätzliche Distribution (extra) gelöscht wird.
- `--clean` – Paket mit den Standardeinstellungen des Servers installieren, ohne eine Sicherungskopie zum Wiederherstellen der Einstellungen der früheren Installation zu verwenden.
- `--preseed` <*Pfad*> – Pfad zur Konfigurationsdatei, welche die vordefinierten Antworten auf die Fragen des Installationsprogramms enthält.

  Variablen zur Festlegung der vordefinierten Antworten in der Konfigurationsdatei:
  - `DEFAULT_BACKUP_DIR=`<*Pfad*> – Pfad des Verzeichnisses mit der Sicherungskopie, die zur Wiederherstellung der Einstellungen der früheren Version verwendet werden soll (wird nicht verwendet, falls die Standardinstallation ausgeführt wird).
  - `QUIET_INSTALL=[0|1]` – legt fest, ob das Installationsprogramm im Hintergrund ausgeführt werden soll:
    - 0 – Installationsprogramm im Hintergrundmodus starten.
    - 1 – Installationsprogramm im Normalmodus starten.
  - `CLEAN_INSTALL=[0|1]` – legt fest, ob die Sicherungskopie bei der Installation verwendet werden soll:
    - 0 – Installation mit den Standardeinstellungen ohne Wiederherstellung der Einstellungen aus der Sicherungskopie.
    - 1 – Installation mit der Wiederherstellung der Einstellungen aus der Sicherungskopie. Die jeweilige Sicherungskopie befindet sich im Verzeichnis, das in der Variable `DEFAULT_BACKUP_DIR` festgelegt ist. Wenn die Variable `DEFAULT_BACKUP_DIR` nicht angegeben ist, wird die Sicherungskopie aus dem Verzeichnis `/var/tmp/drwcs` verwendet.
  - `ADMIN_PASSWORD=`<*Passwort*> – Passwort für das Standard-Administratorkonto (**admin**).
    - Falls die Variable `ADMIN_PASSWORD` in der Datei angegeben ist, wird der aktuelle Wert der Variablen als Administratorpasswort verwendet. Nach Abschluss des Installationsvorgangs

wird dabei die folgende Meldung ausgegeben:
`Password specified in the configuration file for the default administrator (admin): <Passwort>`

- Falls die Variable `ADMIN_PASSWORD` in der Datei nicht angegeben ist, wird das Passwort automatisch generiert. Nach Abschluss des Installationsvorgangs wird dabei die folgende Meldung ausgegeben:
  `Automatically generated password for the default administrator (admin): <Passwort>`

Beachten Sie bei der Verwendung des Schalters `--preseed` das Folgende: Wenn Sie mithilfe der Variable `QUIET_INSTALL=0` in der Konfigurationsdatei nicht festgelegt haben, dass die Installation im Hintergrundmodus erfolgen soll, werden während der Installation alle anderen Variablen in der Konfigurationsdatei vom Benutzer neu definiert.

H7. Dienstprogramme

H7.1. Dienstprogramm zum Generieren von digitalen Schlüsseln und Zertifikaten

Folgende Konsolenversionen des Dienstprogramms zum Generieren digitaler Schlüssel und Zertifikate sind verfügbar:

Ausführbare Datei	Speicherort	Erläuterung
`drweb-sign-<OS>-<Bitanzahl>`	Verwaltungscenter **Administration → Dienstprogramme**	Autonome Version des Dienstprogramms. Diese Version kann von einem beliebigen Verzeichnis aus auf einem beliebigen Rechner, auf dem ein entsprechendes Betriebssystem installiert ist, gestartet werden.
	Server-Verzeichnis `webmin/utilities`	
`drwsign`	Server-Verzeichnis `bin`	Die jeweilige Version des Dienstprogramms hängt von den vorhandenen Serverbibliotheken ab. Sie kann nur aus dem Verzeichnis, in dem sie liegt, gestartet werden.

Die Versionen des Dienstprogramms `drweb-sign-<OS>-<Bitanzahl>` und `drwsign` haben die gleichen Funktionalitäten. Nachfolgend wird die Version `drwsign` erläutert, obwohl die aufgeführten Beispiele für die beiden Versionen gültig sind.

Format des Startbefehls

- `drwsign check [-public-key=<öffentlicher_Schlüssel>] <Datei>`

  Dieser Befehl überprüft die Signatur der angegebenen Datei mithilfe des öffentlichen Schlüssels des Subjekts, das die Datei signiert hat.

Schalterparameter	Standardwert
<öffentlicher_Schlüssel>	`drwcsd.pub`

- `drwsign extract [-private-key=<privater_Schlüssel>] [-cert=<Serverzertifikat>] <öffentlicher_Schlüssel>`

  Dieser Befehl extrahiert aus der Datei des privaten Schlüssels oder der Zertifikatdatei den öffentlichen Schlüssel und schreibt den öffentlichen Schlüssel in die angegebene Datei.

  Die Schlüssel `-private-key` und `-cert` schließen sich gegenseitig aus, da nur einer von ihnen angegeben werden kann. Wenn die beiden Schlüssel gleichzeitig angegeben wurden, gibt der Befehl einen Fehler aus.

Die Schalterparameter müssen unbedingt angegeben sein.

Wenn keiner der Schalter angegeben ist, wird `-private-key=drwcsd.pri` zum Extrahieren des öffentlichen Schlüssels aus dem privaten Schlüssel `drwcsd.pri` verwendet.

Schalterparameter	Standardwert
<*privater_Schlüssel*>	`drwcsd.pri`

- `drwsign genkey [`<*privater_Schlüssel*>` [`<*öffentlicher_Schlüssel*>`]]`

  Dieser Befehl generiert ein Schlüsselpaar (öffentlich/privat) und schreibt die beiden Schlüssel in die entsprechenden Dateien.

Schalterparameter	Standardwert
<*privater_Schlüssel*>	`drwcsd.pri`
<*öffentlicher_Schlüssel*>	`drwcsd.pub`

  Das Dienstprogramm für Windows (im Unterschied zur UNIX-Version) kann den privaten Schlüssel nicht vor unbefugtem Kopieren schützen.

- `drwsign gencert [-private-key=`<*privater_Schlüssel*>`] [-subj=`<*Subjektfelder*>`] [-days=`<*Gültigkeitsdauer*>`] [`<*selbstsigniertes_Zertifikat*>`]`

  Dieser Befehl generiert ein selbstsigniertes Zertifikat mithilfe des privaten Schlüssels des Servers und schreibt es in die entsprechende Datei.

Schalterparameter	Standardwert
<*privater_Schlüssel*>	`drwcsd.pri`
<*Subjektfelder*>	`/CN=`<*Hostname*>
<*Gültigkeitsdauer*>	`3560`
<*selbstsigniertes_Zertifikat*>	`drwcsd-certificate.pem`

- `drwsign gencsr [-private-key=`<*privater_Schlüssel*>`] [-subj=`<*Subjektfelder*>`] [`<*Anforderung_zum_Signieren_des_Zertifikats*>`]`

  Dieser Befehl generiert eine Anforderung zum Signieren des Zertifikats mithilfe des privaten Schlüssels und schreibt sie in die entsprechende Datei.

  Dieser Befehl kann zum Signieren des Zertifikats eines anderen Servers verwendet werden, beispielsweise zum Signieren des Zertifikats des Dr.Web Proxyservers mithilfe des Schlüssels des Dr.Web Servers.

  Mit dem Schalter `signcsr` lassen Sie Ihre Anforderung signieren.

Schalterparameter	Standardwert
<*privater_Schlüssel*>	`drwcsd.pri`
<*Subjektfelder*>	`/CN=`<*Hostname*>
<*Anforderung_zum_Signieren_des_Zertifikats*>	`drwcsd-certificate-sign-request.pem`

- `drwsign genselfsign [-show] [-subj=`<*Subjektfelder*>`] [-days=`<*Gültigkeitsdauer*>`] [`<*privater_Schlüssel*>` [`<*selbstsigniertes_Zertifikat*>`]]`

  Dieser Befehl generiert ein selbstsigniertes RSA-Zertifikat und einen privaten RSA-Schlüssel für den Webserver und schreibt sie in die entsprechenden Dateien.

  Mit dem Schalter `-show` geben Sie den Zertifikatinhalt in einer lesbaren Form aus.

Schalterparameter	Standardwert
<*Subjektfelder*>	`/CN=`<*Hostname*>
<*Gültigkeitsdauer*>	`3560`
<*privater_Schlüssel*>	`private-key.pem`
<*selbstsigniertes_Zertifikat*>	`certificate.pem`

- `drwsign hash-check [-public-key=`<*öffentlicher_Schlüssel*>`]` <*Hash-Datei*> <*Signaturdatei*>

  Dieser Befehl überprüft die Signatur der angegebenen 256-Bit-Zahl im Format des Client-Server-Protokolls.

  Im Parameter <*Hash-Datei*> muss die Datei mit einer 256-Bit-Zahl angegeben werden, die signiert werden soll. Die Datei <*Signaturdatei*> ist das Ergebnis des Signierens (zwei 256-Bit-Zahlen).

Schalterparameter	Standardwert
<*öffentlicher_Schlüssel*>	`drwcsd.pub`

- `drwsign hash-sign [-private-key=`<*privater_Schlüssel*>`]` <*Hash-Datei*> <*Signaturdatei*>

  Dieser Befehl signiert die angegebene 256-Bit-Zahl im Format des Client-Server-Protokolls.

  Im Parameter <*Hash-Datei*> muss die Datei mit einer 256-Bit-Zahl angegeben werden, die signiert werden soll. Die Datei <*Signaturdatei*> ist das Ergebnis des Signierens (zwei 256-Bit-Zahlen).

Schalterparameter	Standardwert
<*privater_Schlüssel*>	`drwcsd.pri`

- `drwsign help [<Befehl>]`

  Dieser Befehl liefert in der Befehlszeile kurze Hilfe zum Programm oder einem Befehl.

- `drwsign sign [-private-key=<privater_Schlüssel>] <Datei>`

  Dieser Befehl signiert die in *<Datei>* angegebene Datei mithilfe des privaten Schlüssels.

Schalterparameter	Standardwert
<privater_Schlüssel>	`drwcsd.pri`

- `drwsign signcert [-ca-key=<privater_Schlüssel>] [-ca-cert=<Serverzertifikat>] [-cert=<zu_signierendes_Zertifikat>] [-days=<Gültigkeitsdauer>] [<signiertes_Zertifikat>]`

  Dieser Befehl signiert das vorhandene *<zu_signierendes_Zertifikat>* mithilfe des privaten Schlüssels und des Serverzertifikats. Das signierte Zertifikat wird in einer separaten Datei gespeichert.

  Der Befehl kann zum Signieren des Zertifikats des Dr.Web Proxyservers mithilfe des Schlüssels des Dr.Web Servers verwendet werden.

Schalterparameter	Standardwert
<privater_Schlüssel>	`drwcsd.pri`
<Serverzertifikat>	`drwcsd-ca-cerificate.pem`
<zu_signierendes_Zertifikat>	`drwcsd-certificate.pem`
<Gültigkeitsdauer>	`3560`
<signiertes_Zertifikat>	`drwcsd-signed-certificate.pem`

- `drwsign signcsr [-ca-key=<privater_Schlüssel>] [-ca-cert=<Serverzertifikat>] [-csr=<Anforderung_zum_Signieren_des_Zertifikats>] [-days=<Gültigkeitsdauer>] [<signiertes_Zertifikat>]`

  Dieser Befehl signiert mithilfe des privaten Schlüssels und des Serverzertifikats eine *<Anforderung_zum_Signieren_des_Zertifikats>*, die über den Befehl `gencsr` erzeugt wurde. Das signierte Zertifikat wird in einer separaten Datei gespeichert.

  Dieser Befehl kann zum Signieren des Zertifikats eines anderen Servers verwendet werden, beispielsweise zum Signieren des Zertifikats des Dr.Web Proxyservers mithilfe des Schlüssels des Dr.Web Servers.

Schalterparameter	Standardwert
<privater_Schlüssel>	`drwcsd.pri`
<Serverzertifikat>	`drwcsd-cerificate.pem`

Schalterparameter	Standardwert
<Anforderung_zum_Signieren_des_Zertifikats>	`drwcsd-certificate-sign-request.pem`
<Gültigkeitsdauer>	`3560`
<signiertes_Zertifikat>	`drwcsd-signed-certificate.pem`

- `drwsign tlsticketkey [`*<TLS-Sitzungsticket>*`]`

  Dieser Befehl generiert TLS-Sitzungstickets.

  Der Befehl kann für gemeinsame TLS-Sitzungen in einem Server-Cluster verwendet werden.

Schalterparameter	Standardwert
<TLS-Sitzungsticket>	`tickets-key.bin`

- `drwsign verify [-ss-cert] [-CAfile=`*<Serverzertifikat>*`] [`*<zu_prüfendes_Zertifikat>*`]`

  Dieser Befehl validiert ein Zertifikat gegen ein vertrauenswürdiges Zertifikat des Servers.

  Der Schalter `-ss-cert` bewirkt, dass das vertrauenswürdige Zertifikat ignoriert wird und nur das selbstsigniertes Zertifikat validiert wird.

Schalterparameter	Standardwert
<Serverzertifikat>	`drwcsd-certificate.pem`
<zu_prüfendes_Zertifikat>	`drwcsd-signed-certificate.pem`

- `drwsign x509dump [`*<zu_druckendes_Zertifikat>*`]`

  Der Befehl druckt den Dump eines beliebigen x509-Zertifikats.

Schalterparameter	Standardwert
<zu_druckendes_Zertifikat>	`drwcsd-certificate.pem`

H7.2. Dienstprogramm zur Verwaltung der eingebetteten Datenbank

Zur Verwaltung der eingebetteten Datenbank können Sie folgende Tools verwenden:

- `drwidbsh` für die IntDB-Datenbank
- `drwidbsh3` für die SQLite3-Datenbank

Diese Dienstprogramme befinden sich in den folgenden Verzeichnissen:

- Für **Linux**: `/opt/drwcs/bin`

- Für **FreeBSD**: `/usr/local/drwcs/bin`
- Für **Windows**: <*Server-Installationsverzeichnis*>`\bin`

  (standardmäßig das Installationsverzeichnis des Servers: `C:\Program Files\DrWeb Server`).

Format des Startbefehls:

`drwidbsh` <*vollständiger_Name_der_Datenbankdatei*>

oder

`drwidbsh3` <*vollständiger_Name_der_Datenbankdatei*>

Das Programm läuft im Textmodus, wartet auf die Eingabe von Programmbefehlen durch den Benutzer (Befehle beginnen mit einem Punkt).

Um die Hilfe zu anderen Befehlen aufzurufen, geben Sie `.help` ein. Der Hilfetext wird angezeigt.

Weitere Informationen finden Sie in einem SQL-Handbuch.

H7.3. Dienstprogramm zur Ferndiagnose des Dr.Web Servers

Das Dienstprogramm zur Ferndiagnose des Dr.Web Servers ermöglicht es Ihnen, den Dr.Web Server remote zu verwalten und seine Statistik anzusehen. Die grafische Version des Dienstprogramms ist nur für Windows verfügbar.

Folgende Versionen des Dienstprogramms stehen zur Verfügung:

- Für Windows ist eine grafische Version verfügbar.
- Für UNIX-basierte Betriebssysteme steht sie als Konsolenversion zur Verfügung.

Folgende Versionen des Dienstprogramms zur Ferndiagnose des Dr.Web Servers stehen zur Verfügung:

Ausführbare Datei	Speicherort	Erläuterung
`drweb-cntl-`<*OS*>`-`<*Bitanzahl*>	Verwaltungscenter **Administration** → **Dienstprogramme**	Autonome Version des Dienstprogramms. Diese Version kann von einem beliebigen Verzeichnis aus auf einem beliebigen Rechner, auf dem ein entsprechendes Betriebssystem installiert ist, gestartet werden.
	Server-Verzeichnis `webmin/utilities`	
`drwcntl`	Server-Verzeichnis `bin`	Die jeweilige Version des Dienstprogramms hängt von den vorhandenen Serverbibliotheken ab. Sie kann nur aus dem Verzeichnis, in dem sie liegt, gestartet werden.

Die Versionen des Dienstprogramms `drweb-cntl-<OS>-<Bitanzahl>` und `drwcntl` haben die gleichen Funktionalitäten. Nachfolgend wird die Version `drwcntl` erläutert, obwohl die aufgeführten Beispiele für die beiden Versionen gültig sind.

Um das Dienstprogramm zur Ferndiagnose des Servers verwenden zu können, aktivieren Sie die Erweiterung Dr.Web Server FrontDoor. Aktivieren Sie dafür im Bereich **Dr.Web Server-Konfiguration** auf der Registerkarte **Module** das Kontrollkästchen **Erweiterung Dr.Web Server FrontDoor**.

Um das Dienstprogramm zur Ferndiagnose des Servers verwenden zu können, muss der Administrator über das Recht **Zusätzliche Funktionen verwenden** verfügen. Anderenfalls ist der Zugriff auf den Server über das Dienstprogramm zur Ferndiagnose nicht möglich.

Damit das Dienstprogramm zur Ferndiagnose des Servers (sowohl die grafische Version als auch Konsolen-Version) TLS-Verbindungen unterstützt, müssen Sie bei der Angabe der Server-Adresse das Protokoll explizit angeben: `ssl://<IP-Adresse oder DNS-Name>`.

Die Einstellungen des Servers für die Verbindung mit dem Dienstprogramm zur Ferndiagnose des Dr.Web Servers werden im **Administratorhandbuch** unter Fernzugriff auf Dr.Web Server beschrieben.

Konsolenversion des Dienstprogramms

Format des Startbefehls:

`drwcntl [-?|-h|--help] [+<Protokolldatei>] [<Server> [<Anmeldename> [<Passwort>]]]`

wobei:

- `-? -h --help` – Hilfe zu Befehlen anzeigen.
- *<Protokolldatei>* – alle Aktionen des Dienstprogramms im Protokoll, das sich unter dem angegebenen Pfad befindet, aufzeichnen.
- *<Server>* – Adresse des Servers, mit dem sich das Dienstprogramm verbindet. Das Eingabeformat ist `[(tcp|ssl)://]`*<IP-Adresse oder DNS-Name>*`[:<Port>]`.

  Zum Herstellen der Verbindung über eines der unterstützten Protokolle müssen folgende Bedingungen erfüllt sein:

  a) Zum Herstellen der Verbindung über `ssl` muss die Konfigurationsdatei `frontdoor.conf` das Tag `<ssl />` enthalten. In diesem Fall können die Verbindungen nur über `ssl` hergestellt werden.

b) Zum Herstellen der Verbindung über `tcp` ist es erforderlich, dass das Tag `<ssl />` in die Konfigurationsdatei `frontdoor.conf` auskommentiert ist. In diesem Fall können die Verbindungen nur über `tcp` hergestellt werden.

Wenn die Adresszeile des Servers leer ist, werden folgende Werte verwendet:

Parameter	Standardwert
Verbindungsprotokoll	`tcp` ⚠ Damit die TCP-Verbindung möglich ist, muss das Kontrollkästchen **TLS verwenden** im Verwaltungscenter unter **Administration** → **Fernzugriff auf Dr.Web Server** deaktiviert sein. Dies setzt das Tag `<ssl />` in der Konfigurationsdatei `frontdoor.conf` außer Kraft.
IP-Adresse oder DNS-Name des Servers	Sie werden aufgefordert, die Adresse des Servers in einem entsprechenden Format einzugeben.
Port	`10101` ⚠ Um den Port auf dem Server freizugeben, wechseln Sie zum Bereich **Fernzugriff auf Dr.Web Server**. Die Einstellung wird in der Konfigurationsdatei `frontdoor.conf` gespeichert. Wenn ein anderer Port in diesem Abschnitt verwendet wird, muss dieser Port beim Herstellen der Verbindung mit dem Dienstprogramm explizit angegeben werden.

- <*Anmeldename*> – Anmeldename des Administrators vom Server.
- <*Passwort*> – Passwort des Administrators für den Zugriff auf den Server.

  Wenn der Anmeldename und das Passwort des Administrators nicht in der Zeile angegeben sind, werden Sie aufgefordert, diese Daten einzugeben.

Zulässige Befehle:

- `cache` <*Vorgang*> – Verwaltung des Dateicache. Folgende Befehle sind möglich:
  - `clear` – Dateicache löschen.
  - `list` – den ganzen Inhalt des Dateicache anzeigen.
  - `matched` <*regulärer_Ausdruck*> – den Inhalt des Dateicache anzeigen, der dem angegebenen regulären Ausdruck entspricht.
  - `maxfilesize [`<*Größe*>`]` – maximale Größe von vorab geladenen Dateiobjekten anzeigen/festlegen. Wenn der Befehl ohne zusätzliche Parameter ausgeführt wird, wird die aktuelle Größe angezeigt. Um die Größe festzulegen, geben Sie die gewünschte Größe in Bytes nach dem Namen des Befehls an.
  - `statistics` – Statistik zur Nutzung des Dateicache anzeigen.

- `calculate` <*Funktion*> – Ermittlung der festgelegten Reihenfolge. Verwenden Sie zum Aufruf einer bestimmten Reihenfolge folgende Befehle:
  - `hash [`<*Norm*>`] [`<*Zeile*>`]` – Berechnung des Hashwerts der angegebenen Zeile. Um eine bestimmte Norm anzuwenden, führen Sie folgende Befehle aus:
    - `gost` – Hashwert der angegebenen Zeile gemäß GOST-Norm berechnen.
    - `md5` – MD5-Hashwert der angegebenen Zeile berechnen.
    - `sha` – Hashwert der angegebenen Zeile gemäß SHA berechnen.
    - `sha1` – Hashwert der angegebenen Zeile gemäß SHA1 berechnen.
    - `sha224` – Hashwert der angegebenen Zeile gemäß SHA224 berechnen.
    - `sha256` – Hashwert der angegebenen Zeile gemäß SHA256 berechnen.
    - `sha384` – Hashwert der angegebenen Zeile gemäß SHA384 berechnen.
    - `SHA512` – Hashwert der angegebenen Zeile gemäß SHA512 berechnen.
  - `hmac [`<*Norm*>`] [`<*Zeile*>`]` – Berechnung des HMAC-Werts der angegebenen Zeile. Um eine bestimmte Norm anzuwenden, führen Sie folgende Befehle aus:
    - `md5` – Berechnung des HMAC-MD5-Werts der angegebenen Zeile.
    - `sha256` – Berechnung des HMAC-SHA256-Werts der angegebenen Zeile.
  - `random` – eine beliebige Zahl generieren.
  - `uuid` – eine beliebige ID generieren.
- `clients` <*Vorgang*> – Anzeige der Informationen und Steuerung der Clients, die mit dem Server verbunden sind. Verwenden Sie zum Aufruf einer bestimmten Funktion folgende Befehle:
  - `addresses [`<*regulärer_Ausdruck*>`]` – Anzeige der Netzwerkadressen der Workstations, die dem angegebenen Ausdruck entsprechen. Wenn kein regulärer Ausdruck angegeben ist, werden die Adressen aller Workstations angezeigt.
  - `caddresses [`<*regulärer_Ausdruck*>`]` – Anzeige der Anzahl der IP-Adressen der Workstations, die dem angegebenen Ausdruck entsprechen. Wenn kein regulärer Ausdruck angegeben ist, wird die Anzahl aller Workstations angezeigt.
  - `chosts [`<*regulärer_Ausdruck*>`]` – Anzeige der Anzahl der Rechnernamen der Workstations, die dem angegebenen Ausdruck entsprechen. Wenn kein regulärer Ausdruck angegeben ist, wird die Anzahl aller Workstations angezeigt.
  - `cids [`<*regulärer_Ausdruck*>`]` – Anzeige der Anzahl der IDs der Workstations, die dem angegebenen Ausdruck entsprechen. Wenn kein regulärer Ausdruck angegeben ist, wird die Anzahl aller Workstations angezeigt.
  - `cnames [`<*regulärer_Ausdruck*>`]` – Anzeige der Anzahl der Namen der Workstations, die dem angegebenen Ausdruck entsprechen. Wenn kein regulärer Ausdruck angegeben ist, wird die Anzahl aller Workstations angezeigt.
  - `disconnect [`<*regulärer_Ausdrück*>`]` – aktive Verbindung mit den Workstations trennen, deren IDs dem angegebenen regulären Ausdruck entsprechen. Wenn kein regulärer Ausdruck angegeben ist, wird die Verbindung mit allen Workstations getrennt.

- `enable [<Modus>]` – Modus, in dem sich Clients mit dem Server verbinden, anzeigen/festlegen. Wenn keine zusätzlichen Parameter angegeben sind, wird der aktuelle Modus angezeigt. Um den gewünschten Modus festzulegen, verwenden Sie folgende Befehle:
  - `on` – alle Client-Verbindungen annehmen.
  - `off` – allen Clients die Verbindung verweigern.
- `hosts` *[<regulärer_Ausdruck>]* – Anzeige der Rechnernamen der Workstations, die dem angegebenen Ausdruck entsprechen.
- `ids` *[<regulärer_Ausdruck>]* – Anzeige der IDs der Workstations, die dem angegebenen Ausdruck entsprechen.
- `names` *[<regulärer_Ausdruck>]* – Anzeige der Namen der Workstations, die dem angegebenen Ausdruck entsprechen.
- `online` <*regulärer_Ausdruck*> – Dauer der Verbindung der Workstations anzeigen, deren IDs, Namen oder Adressen dem angegebenen regulären Ausdruck entsprechen. Die Verbindungsdauer entspricht der Zeit, die seit der letzten Verbindung mit dem Server vergangen ist.
- `statistics` *[<regulärer_Ausdruck>]* – Anzeige der Statistik zur Anzahl der Clients, die dem angegebenen Ausdruck entsprechen.
- `traffic` *[<regulärer_Ausdruck>]* – Anzeige der Informationen zum Datenverkehr der aktuell verbundenen Clients, die dem angegebenen regulären Ausdruck entsprechen.

- `core` – Speicherauszug des Server-Prozesses aufzeichnen.
- `benchmark` <*Parameter*> – Anzeige der Statistik zur CPU-Auslastung des Rechners, auf dem der Server installiert ist. Um einen bestimmten Parameter anzuzeigen, führen Sie einen der folgenden Befehle aus:
  - `clear` – alle gesammelten Statistiken löschen.
  - `day` – Diagramm der CPU-Auslastung für den aktuellen Tag anzeigen.
  - `disable` – Überwachung der CPU-Auslastung deaktivieren.
  - `enable` – Überwachung der CPU-Auslastung aktivieren.
  - `hour` – Diagramm der CPU-Auslastung für die aktuelle Stunde anzeigen.
  - `load` – durchschnittliche CPU-Auslastung anzeigen.
  - `minute` – Diagramm der CPU-Auslastung für die letzte Minute anzeigen.
  - `rawd` – zahlenmäßige Erfassung der CPU-Auslastung für den aktuellen Tag anzeigen.
  - `rawh` – zahlenmäßige Erfassung der CPU-Auslastung für die letzte Stunde anzeigen.
  - `rawl` – zahlenmäßige Erfassung der durchschnittlichen CPU-Auslastung anzeigen.
  - `rawm` – zahlenmäßige Erfassung der CPU-Auslastung für die letzte Minute anzeigen.
  - `status` – Status der Überwachung der CPU-Auslastung anzeigen.
- `debug` <*Parameter*> – Einstellungen des Debug-Modus. Um einen bestimmten Parameter festzulegen, führen Sie zusätzliche Befehle aus. Um die Hilfe zu den zusätzlichen Befehlen aufzurufen, führen Sie den Befehl `? debug` aus.

Der Befehl `debug signal` ist nur für Server unter UNIX-basierten Betriebssystemen möglich.

- `die` – Server beenden und den Speicherauszug des Server-Prozesses aufzeichnen.

Der Befehl `die` ist nur für Server unter UNIX-basierten Betriebssystemen möglich.

- `dwcp` <*Parameter*> – Einstellungen von Dr.Web Control Protocol (darunter Protokolle des Servers, der Agents und Installationsprogramme von Agents) anzeigen. Folgende Parameter sind verfügbar:
  - `compression` <*Modus*> – einen der folgenden Komprimierungsmodi festlegen:
    - `on` – Komprimierung ist aktiviert.
    - `off` – Komprimierung ist deaktiviert.
    - `possible` – Komprimierung ist möglich.
  - `encryption` <*Modus*> – einen der folgenden Verschlüsselungsmodi festlegen:
    - `on` – Verschlüsselung ist aktiviert.
    - `off` – Verschlüsselung ist deaktiviert.
    - `possible` – Verschlüsselung ist möglich.
  - `show` – die aktuellen Einstellungen von Dr.Web Control Protocol anzeigen.
- `io` <*Parameter*> – Statistik zum Lesen/Schreiben von Daten durch den Prozess des Servers anzeigen. Um einen bestimmten Parameter anzuzeigen, führen Sie einen der folgenden Befehle aus:
  - `clear` – alle gesammelten Statistiken löschen.
  - `disable` – Überwachung der Statistik deaktivieren.
  - `enable` – Überwachung der Statistik aktivieren.
  - `rawdr` – zahlenmäßige Erfassung zum Lesen von Daten für den aktuellen Tag anzeigen.
  - `rawdw` – zahlenmäßige Erfassung zum Schreiben von Daten für den aktuellen Tag anzeigen.
  - `rawh` – zahlenmäßige Erfassung für die letzte Stunde anzeigen.
  - `rawm` – zahlenmäßige Erfassung für die letzte Minute anzeigen.
  - `rday` – Statistik zum Lesen von Daten für den aktuellen Tag im Diagramm anzeigen.
  - `rhour` – Statistik zum Lesen von Daten für die letzte Stunde im Diagramm anzeigen.
  - `rminute` – Statistik zum Lesen von Daten für die letzte Minute im Diagramm anzeigen.
  - `status` – Status der Statistik-Überwachung anzeigen.
  - `wday` – Statistik zum Schreiben von Daten für den aktuellen Tag im Diagramm anzeigen.
  - `whour` – Statistik zum Schreiben von Daten für die letzte Stunde im Diagramm anzeigen.
  - `wminute` – Statistik zum Schreiben von Daten für die letzte Minute im Diagramm anzeigen.

- `log` <*Parameter*> – Zeile in die Protokolldatei des Servers schreiben oder Protokollierungsstufe festlegen/anzeigen. Je nach festgelegten Parametern werden folgende Aktionen ausgeführt:
  - `log` <*Zeile*> – die angegebene Zeile in das Protokoll des Servers mit der Protokollierungsstufe `NOTICE` schreiben.
  - `log \s [`<*Stufe*>`]` – Protokollierungsstufe festlegen/anzeigen. Wenn der Befehl `\s` ohne Angabe einer Protokollierungsstufe ausgeführt wird, wird die aktuelle Protokollierungsstufe angezeigt. Zulässige Protokollierungsstufen: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`.
- `lua` <*Skript*> – das angegebene LUA-Skript ausführen.
- `mallopt` <*Parameter*> – Einstellungen für die Speicherreservierung festlegen. Um eine bestimmte Einstellung festzulegen, führen Sie zusätzliche Befehle aus. Um die Hilfe zu den zusätzlichen Befehlen aufzurufen, führen Sie den Befehl `? mallopt` aus.

  Der Befehl `mallopt` ist nur für Server unter Linux relevant.

  Um die Hilfe zu den Parametern dieses Befehls aufzurufen, lesen Sie die Beschreibung der Funktion `mallopt()` der Bibliothek `glibc`. Um die Hilfe zu dieser Funktion aufzurufen, führen Sie den Befehl `man mallopt` aus.
- `memory` <*Parameter*> – Anzeige der Statistik zur Speichernutzung auf dem Rechner, auf dem der Server installiert ist. Um einen bestimmten Parameter anzuzeigen, führen Sie einen der folgenden Befehle aus:
  - `all` – alle Informationen und Statistiken anzeigen.
  - `heap` – Informationen zum dynamischen Speicher anzeigen.
  - `malloc` – Informationen zur Speicherzuordnung anzeigen.
  - `sizes` – Statistik zur Größe des zugewiesenen Speichers anzeigen.
  - `system` – Informationen zum Systemspeicher anzeigen.

  Der Befehl `memory` kann nur unter Windows, Linux- und FreeBSD-artigen Betriebssystemen ausgeführt werden. Zusätzliche Parameter des Befehls `memory` können nicht unter allen Betriebssystemen angegeben werden.

  - `system` ist nur unter Windows und Linux-artigen Betriebssystemen verfügbar.
  - `heap` ist nur unter Windows und Linux-artigen Betriebssystemen verfügbar.
  - `malloc` ist nur unter Linux- und FreeBSD-artigen Betriebssystemen verfügbar.
  - `sizes` ist nur unter Linux- und FreeBSD-artigen Betriebssystemen verfügbar.
- `monitoring` <*Modus*> – Modus für die Überwachung der CPU-Auslastung (Schalter `cpu` <*Parameter*>) und die Eingabe/Ausgabe (Schalter `io` <*Parameter*>) durch den Prozess des Servers festlegen/anzeigen. Folgende Befehle sind möglich:
  - `disable` – Überwachung deaktivieren.
  - `enable` – Überwachung aktivieren.

  - `show` – den aktuellen Modus anzeigen.
- `printstat` – Statistik zur Leistung des Servers protokollieren.
- `reload` – Dr.Web Server FrontDoor-Erweiterung neu starten.
- `repository` <*Parameter*> – Repository verwalten. Verwenden Sie zum Aufruf einer bestimmten Funktion folgende Befehle:
  - `all` – Liste aller Repository-Produkte und die Anzahl aller Dateien nach Produkt sortiert anzeigen.
  - `clear` – Cache unabhängig vom TTL-Wert der im Cache befindlichen Objekte löschen.
  - `fill` – alle Dateien des Repository im Cache speichern.
  - `keep` – alle Dateien des Repository, die zum aktuellen Zeitpunkt im Cache sind, immer und unabhängig vom TTL-Wert behalten.
  - `loaded` – Liste aller Repository-Produkte und die Anzahl aller Dateien jedes Produkts, die zum aktuellen Zeitpunkt im Cache sind, anzeigen.
  - `reload` – Repository vom Datenträger erneut laden.
  - `statistics` – Update-Statistik des Repository anzeigen.
- `restart` – Server neu starten.
- `show` <*Parameter*> – Anzeige der Informationen zum System des Rechners, auf dem der Server installiert ist. Um einen bestimmten Parameter festzulegen, führen Sie zusätzliche Befehle aus. Um die Hilfe zu den zusätzlichen Befehlen aufzurufen, führen Sie den Befehl `? show` aus.

  Zusätzliche Parameter des Befehls `show` haben folgende Einschränkungen:
  - `memory` ist nur für Server unter Windows und Linux-artigen Betriebssystemen verfügbar.
  - `mapping` ist nur für Server unter Windows und Linux-artigen Betriebssystemen verfügbar.
  - `limits` ist nur für Server unter UNIX-basierten Betriebssystemen verfügbar.
  - `processors` ist nur für Server unter Linux-artigen Betriebssystemen verfügbar.
- `sql` <*Abfrage*> – die angegebene SQL-Abfrage ausführen.
- `stop` – Server beenden.
- `traffic` <*Parameter*> – Statistik zum Netzwerkdatenverkehr des Servers anzeigen. Um einen bestimmten Parameter abzurufen, führen Sie einen der folgenden Befehle aus:
  - `all` – den gesamten Datenverbrauch seit dem Start des Servers anzeigen.
  - `incremental` – graduelle Erhöhung des Datenverkehrs relativ zur letzten Ausführung des Befehls `traffic incremental` anzeigen.
  - `last` – Unterschied im Datenvolumen seit dem letzten festen Zeitpunkt anzeigen.
  - `store` – festen Zeitpunkt für den Schalter `last` festlegen.
- `update` <*Parameter*> – Informationen abrufen und Updates verwalten. Verwenden Sie zum Aufruf einer bestimmten Funktion folgende Befehle:

- `active` – Anzeige der Liste der Agents, die zum jeweils aktuellen Zeitpunkt aktualisiert werden.
- `agent [<Modus>]` – Modus, in dem die Agents über den Server aktualisiert werden, anzeigen/festlegen. Wenn keine zusätzlichen Parameter angegeben sind, wird der aktuelle Modus angezeigt. Um den gewünschten Modus festzulegen, verwenden Sie folgende Befehle:
  - `on` – Aktualisierung der Agents aktivieren.
  - `off` – Aktualisierung der Agents deaktivieren.
- `gus` – Aktualisierung des Repository über das GUS erzwingen, unabhängig vom Status des Update-Vorgangs über das GUS.
- `http [<Modus>]` – Modus, in dem der Server über das GUS aktualisiert wird, anzeigen/festlegen. Wenn keine zusätzlichen Parameter angegeben sind, wird der aktuelle Modus angezeigt. Um den gewünschten Modus festzulegen, verwenden Sie folgende Befehle:
  - `on` – Aktualisierung des Repository über das GUS aktivieren.
  - `off` – Aktualisierung des Repository über das GUS deaktivieren.
- `inactive` – Anzeige der Liste der Agents, die zum jeweils aktuellen Zeitpunkt nicht aktualisiert werden.
- `track [<Modus>]` – Modus für die Überwachung der Updates von Agents anzeigen/festlegen. Wenn keine zusätzlichen Parameter angegeben sind, wird der aktuelle Modus angezeigt. Um den gewünschten Modus festzulegen, verwenden Sie folgende Befehle:
  - `on` – Überwachung der Updates der Agents aktivieren.
  - `off` – Überwachung der Updates der Agents deaktivieren. Der Schalter `update active` zeigt dann keine Liste der Agents an, die zum jeweils aktuellen Zeitpunkt aktualisiert werden.

H7.4. Skriptbasiertes Dienstprogramm zur Ferndiagnose des Dr.Web Servers

Das Dienstprogramm zur Ferndiagnose des Dr.Web Servers ermöglicht Ihnen, den Dr.Web Server remote zu verwalten und seine Statistik anzusehen. Im Unterschied zu drwcntl kann `drwcmd` mit Skripten umgehen.

Folgende Konsolenversionen des skriptbasierten Dienstprogramms zur Ferndiagnose des Dr.Web Servers stehen zur Verfügung:

Ausführbare Datei	Speicherort	Erläuterung
`drweb-cmd-<OS>-<Bitanzahl>`	Verwaltungscenter **Administration → Dienstprogramme**	Autonome Version des Dienstprogramms. Diese Version kann von einem beliebigen Verzeichnis aus auf einem beliebigen Rechner, auf dem ein entsprechendes Betriebssystem installiert ist, gestartet werden.
	Server-Verzeichnis `webmin/utilities`	

Ausführbare Datei	Speicherort	Erläuterung
`drwcmd`	Server-Verzeichnis `bin`	Die jeweilige Version des Dienstprogramms hängt von den vorhandenen Serverbibliotheken ab. Sie kann nur aus dem Verzeichnis, in dem sie liegt, gestartet werden.

Die Versionen des Dienstprogramms `drweb-cmd-<OS>-<Bitanzahl>` und `drwcmd` haben die gleichen Funktionalitäten. Nachfolgend wird die Version `drwcmd` erläutert, obwohl die aufgeführten Beispiele für die beiden Versionen gültig sind.

Um das Dienstprogramm zur Ferndiagnose des Servers verwenden zu können, aktivieren Sie die Erweiterung Dr.Web Server FrontDoor. Aktivieren Sie dafür im Bereich **Dr.Web Server-Konfiguration** auf der Registerkarte **Module** das Kontrollkästchen **Erweiterung Dr.Web Server FrontDoor**.

Um das Dienstprogramm zur Ferndiagnose des Servers verwenden zu können, muss der Administrator über das Recht **Zusätzliche Funktionen verwenden** verfügen. Anderenfalls ist der Zugriff auf den Server über das Dienstprogramm zur Ferndiagnose nicht möglich.

Die Einstellungen des Servers für die Verbindung mit dem Dienstprogramm zur Ferndiagnose des Dr.Web Servers werden im **Administratorhandbuch** unter Fernzugriff auf Dr.Web Server beschrieben.

Format des Startbefehls:

`drwcmd [<Schalter>] [<Dateien>]`

Zulässige Schalter

Das Tool `drwcmd` verwendet die Schalter entsprechend den Regeln, die unter Anhang H. Befehlszeilenparameter in Dr.Web Enterprise Security Suite beschrieben werden.

- `--?` – Hilfe zu Schaltern anzeigen.
- `--help` – Hilfe zu Schaltern anzeigen.
- `--commands=<Befehle>` – die angegebenen Befehle ausführen (identisch mit den Befehlen des Tools drwcntl). Mehrere Befehle können mit dem Zeichen `;` voneinander getrennt angegeben werden.
- `--debug=yes|no` – Tool im Debug-Modus protokollieren (Standardausgabe `stderr`). Standardmäßig wird `no` verwendet.

- `--files=yes|no` – Ausführung von Befehlen (identisch mit den Befehlen des Tools drwcntl) aus den angegebenen Dateien erlauben. Standardmäßig wird `yes` verwendet.

  Jeder Befehl muss in einer eigenen Zeile stehen. Leere Zeilen werden nicht berücksichtigt. Kommentare können mit dem Rautezeichen `#` eingeleitet werden.

- `--keep=yes|no` – Verbindung mit dem Server nach der Ausführung des letzten Befehls aufrechthalten, bis der Prozess des Tools abgeschlossen ist. Standardmäßig wird `no` verwendet.
- `--output=<`*Datei*`>` – Datei für die Ausgabe der Serverantworten. Wenn keine Datei angegeben ist, wird die Standardausgabe `stdout` verwendet.

  Falls der Dateiname mit einem Pluszeichen (+) beginnt, wird das Ergebnis der Befehlsausführung am Ende der Datei eingefügt, andernfalls wird die Datei umgeschrieben.

- `--password=<`*Passwort*`>` – Passwort zur Autorisierung am Server. Es kann in der im Schalter `--resource` angegebenen Datei definiert werden.
- `--read=yes|no` – Lesen der Serververbindungsparameter in der Ressourcendatei zulassen. Standardmäßig wird `yes` verwendet.
- `--resource=<`*Datei*`>` – Ressourcendatei mit den Serververbindungsparametern: Serveradresse und Administrator-Anmeldedaten für die Autorisierung am Server. Standardmäßig wird die Datei `.drwcmdrc` verwendet, die sich im folgenden Verzeichnis befindet:
  - Für UNIX-basierte Betriebssysteme: `$HOME`
  - Für Windows: `%LOCALAPPDATA%`

  Jede Zeile muss aus 3 folgenden durch Leerzeichen voneinander getrennten Wörtern bestehen: *<Server> <Benutzer> <Passwort>*.

  Falls Sie in einem dieser Wörter ein Leerzeichen angeben wollen, müssen Sie es mit der Zeichenfolge `%S` ersetzen. Falls Sie in einem dieser Wörter ein Prozentzeichen angeben wollen, müssen Sie es mit der Zeichenfolge `%P` ersetzen.

  Beispiel:

  ```
  ssl://127.0.0.1 user1 password1

  ssl://127.0.0.1 user2 password2

  ssl://127.0.0.1 user pass%Sword
  ```

  Der Schalter `--resource` erfordert den Schalter `--server`. Die Verbindung wird mit dem im Schalter `--server` angegebenen Server anhand der Anmeldeinformationen in der Ressourcendatei hergestellt, die der Adresse dieses Servers entsprechen.

- `--server=<`*Server*`>` – Serveradresse. Standardmäßig wird `ssl://127.0.0.1` verwendet. Sie kann in der im Schalter `--resource` angegebenen Datei definiert werden.
- `--user=<`*Benutzer*`>` – Benutzername zur Autorisierung am Server. Er kann in der im Schalter `--resource` angegebenen Datei definiert werden.
- `--verbose=yes|no` – ausführliche Serverantwort ausgeben (Standardausgabe `stdout`). Standardmäßig wird `no` verwendet.

Die Verbindung mit dem Server erfolgt wie folgt:

1. Die in den Schaltern `--server`, `--user` und `--password` angegebenen Werte haben Vorrang beim Abrufen der Serververbindungsparameter.
2. Falls der Schalter `--server` nicht angegeben ist, wird der Standardwert `ssl://127.0.0.1` verwendet.
3. Falls der Schalter `--user` nicht festgelegt ist, wird in der Datei `.drwcmdrc` (kann im Schalter `--resource` neu definiert werden) nach dem benötigten Server gesucht, und der alphabetisch an erster Stelle stehende Benutzername wird verwendet.
4. Falls der Schalter `--password` nicht festgelegt ist, wird in der Datei `.drwcmdrc` (kann im Schalter `--resource` neu definiert werden) nach dem benötigten Server und Benutzernamen gesucht.

   Der Benutzername und das Passwort werden aus der Datei `.drwcmdrc` ausgelesen (kann im Schalter `--resource` neu definiert werden), falls der Schalter `--read` dies nicht verhindert.

5. Wenn der Benutzername und das Passwort nicht in den Schaltern oder in der Ressourcendatei festgelegt sind, werden sie aufgefordert, die Anmeldedaten über die Konsole einzugeben.

Besonderheiten der Befehlsausführung:

- Wenn ein leerer Wert (–) für die Dateien mit Befehlen angegeben ist, liest das Tool die über die Konsole eingegebenen Befehle aus.
- Wenn Befehle im Schalter `--commands` und die Dateiliste gleichzeitig angegeben sind, werden zunächst die im Schalter `--commands` angegebenen Befehle ausgeführt.
- Wenn keine Dateien und keine Befehle im Schalter `--commands` angegeben sind, liest das Tool die über die Konsole eingegebenen Befehle aus.

Beispiel:

Um die im Schalter `--command` angegebenen Befehle auszuführen und anschließend die Ausführung der Befehle aus der Konsole zu bewirken, geben Sie Folgendes ein:

```
drwcmd --commands=<Befehle> -- -
```

Exit-Codes

- 0 – fehlerfreie Ausführung.
- 1 – Hilfe zu Befehlen wurde aufgerufen: `--help` oder `--?`.
- 2 – Fehler beim Analysieren der Befehlszeile: Es wurden keine Autorisierungsparameter angegeben o. Ä.
- 3 – Fehler beim Erstellen der Datei zum Ausgeben der Serverantwort.

- 4 – Fehler beim Autorisieren am Server: Der Anmeldename und/oder das Administratorpasswort sind/ist falsch.
- 5 – unerwartete Trennung der Serververbindung.
- 127 – unbekannter schwerwiegender Fehler.

H7.5. Dr.Web Repository Loader

Die grafische Version des Repository Loaders wird detailliert im **Administratorhandbuch** unter Grafische Version des Dienstprogramms beschrieben.

Folgende Konsolenversionen des Dienstprogramms des Dr.Web Repository Loaders sind verfügbar:

Ausführbare Datei	Speicherort	Erläuterung
`drweb-reploader-<OS>-<Bitanzahl>`	Verwaltungscenter **Administration** → **Dienstprogramme**	Autonome Version des Dienstprogramms. Diese Version kann von einem beliebigen Verzeichnis aus auf einem beliebigen Rechner, auf dem ein entsprechendes Betriebssystem installiert ist, gestartet werden.
	Server-Verzeichnis `webmin/utilities`	
`drwreploader`	Server-Verzeichnis `bin`	Die jeweilige Version des Dienstprogramms hängt von den vorhandenen Serverbibliotheken ab. Sie kann nur aus dem Verzeichnis, in dem sie liegt, gestartet werden.

Die Versionen des Dienstprogramms `drweb-reploader-<OS>-<Bitanzahl>` und `drwreploader` haben die gleichen Funktionalitäten. Nachfolgend wird die Version `drwreploader` erläutert, obwohl die aufgeführten Beispiele für die beiden Versionen gültig sind.

Um die Eingabe von Schaltern zum Start der Konsolenversion zu erleichtern, verwenden Sie die Konfigurationsdatei des Repository Loaders. Die Schalter in der Standardkonfigurationsdatei haben die unten aufgeführten Standardwerte. Die einzige Ausnahme ist der Schalter `--ssh-auth`: In der Konfigurationsdatei hat er den Wert `pubkey`.

Zulässige Schalter

- `--archive` – Repository in eine Archivdatei packen. Voreingestellt: `no`.
- `--auth` *<Argument>* – Anmeldedaten für die Autorisierung am Update-Server im Format *<Benutzer>*`[:`*<Passwort>*`]`.
- `--cert-file` *<Pfad>* – Pfad zum Speicher der Stammzertifikate für die SSL-Autorisierung.

- `--cert-mode [`<*Argument*>`]` – Typ von SSL-Zertifikaten, die automatisch angenommen werden sollen. Diese Einstellung ist nur für verschlüsselte Verbindungen verfügbar.

  <*Argument*> kann einen der folgenden Werte haben:

  - `any` – alle Zertifikate annehmen.
  - `valid` – nur überprüfte Zertifikate annehmen.
  - `drweb` – nur Zertifikate von Dr.Web annehmen.
  - `custom` – benutzerdefinierte Zertifikate annehmen.

  Standardmäßig wird der Wert `drweb` verwendet.
- `--config` <*Pfad*> – Pfad zur Konfigurationsdatei des Dr.Web Repository Loaders.
- `--cwd` <*Pfad*> – Pfad zum aktuellen Arbeitsverzeichnis.
- `--ipc` – Informationen zur Leistung des Tools in die Standardausgabe schreiben. Voreingestellt: `no`.
- `--help` – Hilfe zu Schaltern anzeigen.
- `--license-key` <*Pfad*> – Pfad zur Lizenzschlüsseldatei (ein Schlüssel oder sein MD5-Hash muss angegeben werden).
- `--log` <*Pfad*> – Pfad zur Datei, in welcher der Downloadvorgang des Repository protokolliert wird.
- `--mode` <*Modus*> – Modus, in dem die Updates geladen werden:
  - `repo` – erzwingt den Download des Repository im Format des Server-Repository. Die heruntergeladenen Dateien können über das Verwaltungscenter als Updates des Server-Repository importiert werden. Die Option wird standardmäßig verwendet.
  - `mirror` – erzwingt den Download des Repository im Format der Update-Zone des GUS. Die heruntergeladenen Dateien können dann auf dem Aktualisierungsspiegel Ihres lokalen Netzwerks freigegeben werden. Sie können die Server so einstellen, dass sie die Updates direkt von diesem Aktualisierungsspiegel, der jeweils die letzte Version des Repository enthält, beziehen.
- `--only-bases` – nur Virendatenbanken herunterladen. Voreingestellt: `no`.
- `--path` <*Argument*> – bewirkt den Download des Repository vom GUS in das im Parameter <*Argument*> angegebene Verzeichnis. Wenn das Repository mit dem Schalter `--archive` in eine Archivdatei verpackt wird, können Sie den Pfad zum Verzeichnis oder direkt zur Archivdatei angeben. Wenn kein Name für die Archivdatei angegeben ist, wird der Standardname `repository.zip` verwendet.
- `--product` <*Argument*> – zu aktualisierendes Produkt. Standardmäßig wird das gesamte Repository herunterladen.
- `--prohibit-cdn` – CDN beim Herunterladen der Updates verbieten. Standardmäßig wird der Wert `no` verwendet, der bedeutet, dass CDN erlaubt ist.
- `--proto` <*Protokoll*> – Protokoll zum Download der Updates: `file | ftp | ftps | http | https | scp | sftp | smb | smbs`. Voreingestellt: `https`.
- `--proxy-auth` <*Argument*> – Informationen für die Authentifizierung am Proxyserver: der Anmeldename des Benutzers und das Passwort im Format <*Benutzer*>`[:`<*Passwort*>`]`.

- `--proxy-host` <*Argument*> – Adresse des Proxyservers im Format <*Server*>`[:`<*Port*>`]`. Der Standardport ist `3128`.
- `--rotate` <*N*><*f*>`,`<*M*><*u*> – Modus für die Rotation des Protokolls des Repository Loaders. Diese Einstellung ist identisch mit der Einstellung für die Rotation des Server-Protokolls.

  Der Standardwert ist `10,10m`, d. h. 10 Dateien je 10 Megabytes speichern und Komprimierung verwenden.
- `--servers` <*Argument*> – Adressen der GUS-Server. Sie sollten den Standardwert `esuite.geo.drweb.com` belassen.
- `--show-products` – Liste der im GUS verfügbaren Produkte ausgeben. Voreingestellt: `no`.
- `--ssh-auth` <*Typ*> – Autorisierungstyp für den Update-Server, wenn auf ihn über SCP/SFTP zugegriffen wird. Die Option <*Typ*> kann einen der folgenden Werte haben:
  - `pwd` – passwortbasierte Autorisierung. Das Passwort wird im Schalter `--auth` festgelegt.
  - `pubkey` – Autorisierung mit dem öffentlichen Schlüssel. Voraussetzung hierfür ist jedoch, dass der private Schlüssel, aus dem der entsprechende öffentliche Schlüssel abgeleitet wird, im Schalter `--ssh-prikey` angegeben ist.
- `--ssh-prikey` <*Pfad*> – Pfad zum privaten SSH-Schlüssel.
- `--ssh-pubkey` <*Pfad*> – Pfad zum öffentlichen SSH-Schlüssel.
- `--strict` – Download bei einem Fehler abbrechen. Voreingestellt: `no`.
- `--update-key` <*Pfad*> – Pfad zum öffentlichen Schlüssel oder zum Verzeichnis mit dem öffentlichen Schlüssel, mit dem die Signaturen der über das GUS heruntergeladenen Updates überprüft werden. Öffentliche Schlüssel für die Überprüfung der Updates `update-key-*.upub` finden sich auf dem Dr.Web Server im Verzeichnis `etc`.
- `--update-url` <*Argument*> – Verzeichnis auf den GUS-Servern, das die Updates für die Dr.Web Produkte beinhaltet. Sie sollten den folgenden Standardwert belassen: `/update`.
- `--verbosity` <*Ausführlichkeitsgrad*> – Protokollierungsstufe. Der Standardwert ist `TRACE3`. Mögliche Werte: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Die Werte `ALL` und `DEBUG3` sind identisch.
- `--version` <*Version*> – Version des Servers (im Format <*Hauptversionsnummer*>`.`<*Nebenversionsnummer*>), für den die Updates heruntergeladen werden sollen. Zum Beispiel: Bei der Server-Version 11 muss der Parameter <*Version*> den Wert `11.00` haben.

Besonderheiten der Verwendung der Schalter

Beachten Sie folgende Regeln, bevor Sie den Repository Loader starten:

Schalter müssen angegeben werden	Bedingung
`--license-key`	Immer
`--update-key`	
`--path`	
`--cert-file`	Wenn folgende Schalter einen der folgenden Werte haben: • `--cert-mode valid | drweb | custom` • `--proto https | ftps | smbs`
`--ssh-prikey`	Wenn folgende Schalter einen der folgenden Werte haben: • `--proto sftp | scp` • `--ssh-auth pubkey`

Anwendungsbeispiele

1. Erstellen einer importierbaren Archivdatei mit allen Produkten:

```
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. Erstellen einer importierbaren Archivdatei mit den Virendatenbanken:

```
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. Erstellen einer importierbaren Archivdatei mit nur dem 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
```

Anhang I. Vom Dr.Web Server exportierte Umgebungsvariablen

Um die Konfiguration der Prozesse, die durch den Dr.Web Server nach Zeitplan gestartet werden, zu erleichtern, sind Informationen zum Speicherort der Verzeichnisse des Servers erforderlich. Der Server exportiert daher die folgenden Variablen in die Umgebung der gestarteten Prozesse:

- `DRWCSD_HOME` – Pfad des Wurzelverzeichnisses (des Installationsverzeichnisses). Der Wert des Schalters ist `-home`, wenn er beim Start des Servers festgelegt wird. Anderenfalls wird das aktuelle Verzeichnis beim Start verwendet.
- `DRWCSD_BIN` – Pfad des Verzeichnisses für ausführbare Dateien. Der Wert des Schalters ist `-bin-root`, wenn er beim Start des Servers festgelegt wird. Andernfalls wird das Unterverzeichnis `bin` des Wurzelverzeichnisses verwendet.
- `DRWCSD_VAR` – Pfad des Verzeichnisses, in das der Server schreiben darf und das zur Speicherung ausführbarer Dateien (z. B. Protokolle sowie Repository-Dateien) verwendet wird. Der Wert des Schalters ist `-var-root`, wenn er beim Start des Servers festgelegt wird. Andernfalls wird das Unterverzeichnis `var` des Wurzelverzeichnisses verwendet.

Anhang J. Anwendung regulärer Ausdrücke in Dr.Web Enterprise Security Suite

Einige Parameter von Dr.Web Enterprise Security Suite können als reguläre Ausdrücke folgender Typen angegeben werden:

- Reguläre Ausdrücke der Lua-Skriptsprache.

  Diese Ausdrücke werden bei der Festlegung der Regeln für die automatische Aufnahme von Workstations in benutzerdefinierte Gruppen verwendet.

  Eine detaillierte Beschreibung regulärer Ausdrücke der Lua-Sprache finden Sie unter http://www.lua.org/manual/5.1/manual.html#5.4.1.

- Reguläre Ausdrücke der PCRE-Bibliothek.

  Eine ausführliche Beschreibung der PCRE-Bibliothek finden Sie unter http://www.pcre.org/.

  Dieser Anhang enthält nur einige Beispiele, welche die praxisnahe Anwendung von regulären PCRE-Ausdrücken demonstrieren.

J1. Optionen für reguläre PCRE-Ausdrücke

Reguläre Ausdrücke werden sowohl in der Konfigurationsdatei des Servers als auch im Verwaltungscenter verwendet, wenn die vom Scan auszuschließenden Objekte in den Einstellungen des Scanners festgelegt werden müssen.

Reguläre Ausdrücke haben das folgende Format:

```
qr{EXP}options
```

wobei `EXP` für den Ausdruck steht, `options` für die Reihenfolge der Optionen (Buchstabenkette) steht und `qr{}` für literale Metazeichen steht. Die Konstruktion sieht generell wie folgt aus:

`qr{pagefile\.sys}i` – Auslagerungsdatei unter Windows NT

Nachfolgend werden reguläre Ausdrücke und ihre Optionen beschrieben. Weitere detaillierte Informationen dazu finden Sie unter http://www.pcre.org/pcre.txt.

- Die Option `'a'` ist gleichwertig mit `PCRE_ANCHORED`

  Diese Option erzwingt die Verankerung des Musters. Wenn diese Option gesetzt ist, wird die Suche auf den Anfang der Zeichenkette (Betreffzeile) eingeschränkt. Dies kann auch durch entsprechende Konstrukte im Muster erreicht werden.

- Die Option `'i'` ist gleichwertig mit `PCRE_CASELESS`

  Wenn diese Option gesetzt ist, wird Groß- und Kleinschreibung nicht berücksichtigt. Diese Option kann im Muster durch die Option `(?i)` geändert werden.

- Die Option `'x'` ist gleichwertig mit `PCRE_EXTENDED`

  Wenn diese Option gesetzt ist, werden Leerzeichen, Tabulatoren und Zeilenumbrüche nicht beachtet, außer wenn sie Steuerzeichen folgen oder sich innerhalb einer Zeichenklasse befinden.

Das Leerzeichen beinhaltet kein Zeichen `VT` (Code 11). Darüber hinaus werden die Zeichen ignoriert, die sich außerhalb der Zeichenklasse zwischen dem Zeichen `#` ohne voranstehendes Steuerzeichen und dem Zeilenumbruch befinden. Dies kann im Muster durch die Option `(?x)` geändert werden. Durch diese Einstellung kann ein Kommentar in ein komplexes Muster eingefügt werden. Beachten Sie, dass dies nur für Datenzeichen möglich ist. Leerzeichen sind nicht zulässig innerhalb einer speziellen Zeichenfolge des Musters, beispielsweise innerhalb der Zeichenfolge `(?(`, die einen bedingten Untermuster einführt.

- Die Option `'m'` ist identisch mit `PCRE_MULTILINE`

  Standardmäßig betrachtet PCRE die Betreffzeile als eine Zeile (selbst wenn sie Zeilenumbrüche enthält). Das Metazeichen für den *Zeilenanfang* `"^"` wird nur am Anfang der Zeichenkette verglichen. Das Metazeichen für das *Zeilenende* `"$"` wird nur am Ende der Zeichenkette bzw. vor dem letzten Zeilenumbruch verglichen (sofern die Option `PCRE_DOLLAR_ENDONLY` nicht gesetzt ist).

  Wenn die Option `PCRE_MULTILINE` gesetzt ist, gilt jeder *Zeilenanfang* und jedes *Zeilenende* als Start und Ende für das Muster. Diese Option kann im Muster durch die Option `(?m)` geändert werden. Auf Zeichenketten, die keine `\n`, `^` oder `$` enthalten, hat die Option `PCRE_MULTILINE` keinen Einfluss.

- Die Option `'u'` ist identisch mit `PCRE_UNGREEDY`

  Die Option kehrt die „Gier“ aller Quantoren um, sodass sie standardmäßig nicht gierig werden. Wenn ihnen aber `"?"` folgt, werden sie wieder gierig. Dies kann auch im Muster durch die Option `(?U)` eingestellt werden.

- Die Option `'d'` ist identisch mit `PCRE_DOTALL`

  Wenn diese Option gesetzt ist, ersetzt der Punkt sämtliche Zeichen einschließlich Zeilenumbrüchen. Diese Option kann im Muster geändert werden, wenn die neue Option `(?s)` gesetzt wird. Eine negative Zeichenklasse wie `[^a]` stimmt unabhängig von dieser Option immer mit dem Zeilenumbruch überein.

- Die Option `'e'` ist identisch mit `PCRE_DOLLAR_ENDONLY`

  Diese Option zwingt das Dollarzeichen dazu, eine Übereinstimmung mit dem Ende der Betreffzeile zu haben. Wenn diese Option nicht vorhanden ist, hat das Dollarzeichen direkt vor dem letzten Zeilenumbruch eine Übereinstimmung (aber nicht vor einem anderen Zeilenumbruch). Die Option `PCRE_DOLLAR_ENDONLY` wird ignoriert, wenn die Option `PCRE_MULTILINE` gesetzt ist.

J2. Besonderheiten der Perl-kompatiblen regulären Ausdrücke (PCRE)

Reguläre Ausdrücke sind Muster, die von links nach rechts mit dem Text abgeglichen werden. In einem Muster repräsentieren die meisten Zeichen sich selbst und passen auf die entsprechenden Zeichen im Text.

Der Hauptvorteil regulärer Ausdrücke ist, dass ein Muster mehrere Varianten und Wiederholungen enthalten kann. Sie werden mittels Metazeichen kodiert. Metazeichen sind die Zeichen, die nicht für sich selbst stehen, sondern eine besondere Bedeutung haben.

Es gibt zwei Arten von Metazeichen: Die einen werden in eckigen Klammern gesetzt, und die anderen werden ohne eckige Klammern verwendet. Nachfolgend werden sie detailliert beschrieben. Ohne eckige Klammern werden die folgenden Metazeichen verwendet:

Zeichen	Wert
\	ein gewöhnliches Steuerzeichen (escape), das mehrere Anwendungsvarianten hat
^	Start einer Zeile (oder Beginn des Textes im Mehrzeilenmodus)
$	Zeilenende (oder Ende des Textes im Mehrzeilenmodus)
.	beliebiges Zeichen außer Zeilentrenner (standardmäßig)
[	Anfang der Zeichenklasse
]	Ende der Zeichenklasse
|	Alternative
(	Anfang des Untermusters
)	Ende des Untermusters
?	erweitert die Bedeutung von (tritt auch als Quantor auf: 0 oder 1 tritt auch als Minimizer auf
*	keinmal oder beliebig oft
+	mindestens einmal tritt auch als possessiver Quantor auf
{	Anfang eines minimalen/maximalen Quantors

Der Teil des Musters, der von eckigen Klammern umschlossen ist, wird als Zeichenklasse bezeichnet. Metazeichen in der Zeichenklasse sind:

Zeichen	Wert
\	ein gewöhnliches Steuerzeichen (escape)
^	findet ein Zeichen oder eine Zeichenfolge am Anfang, am Anfang eines Zeichenbereichs steht es für eine Negation
-	definiert einen Zeichenbereich

Zeichen	Wert
[	POSIX-Zeichenklasse (nur wenn die POSIX-Syntax ihr folgt)
]	Ende der Zeichenklasse

Anhang K. Formate von Protokolldateien

Protokolldateien des Servers (mehr dazu finden Sie im Dokument **Administratorhandbuch** unter Dr.Web Server-Protokoll) und des Agents haben das Textformat. Jede Zeile steht für eine einzelne Nachricht.

Die Nachrichtenzeile hat das folgende Format:

<Jahr><Monat><Tag>.<Stunde><Minute><Sekunde>.<Hundertstel_der_Sekunde>
<Nachrichtentyp> [*<Prozess-ID>*] *<Threadname>* [*<Nachrichtenquelle>*] *<Nachricht>*

wobei:

- *<Jahr><Monat><Tag>.<Stunde><Minute><Sekunde>.<Hundertstel_der_Sekunde>* das genaue Datum ist, an dem die Nachricht in die Protokolldatei geschrieben wurde.
- *<Nachrichtentyp>* die Protokollierungsstufe ist:
  - **ftl** (fatal error ist ein schwerwiegender Fehler) – Nachrichten über kritische Fehler;
  - **err** (error – Fehler) – Nachrichten über Fehler.
  - **wrn** (warning – Warnungen) – Warnungen über Fehler.
  - **ntc** (notice – Bemerkungen) – wichtige Informationen.
  - **inf** (info – Information) – Informationen.
  - **tr0..3** (trace0..3 – Ablaufverfolgung) – Ablaufverfolgung von Aktionen mit unterschiedlichen Detailstufen (**Tracing3** ist die maximale Detailstufe).
  - **db0..3** (debug0..3 – Debugging) – Debug-Nachrichten mit unterschiedlichen Detailstufen (**Debugging3** ist die maximale Detailstufe).

  Nachrichten mit der Protokollierungsstufe **tr0..3** (Tracing) und **db0..3** (Debugging) sind nur für die Entwickler von Dr.Web Enterprise Security Suite bestimmt.

- [*<Prozess-ID>*] ist eine eindeutige nummerische ID des Prozesses, innerhalb von dem der Thread, der die Nachricht in die Protokolldatei geschrieben hat, ausgeführt wird. Unter einigen Betriebssystemen kann [*<Prozess-ID>*] als [*<Prozess-ID>* *<Thread-ID>*] dargestellt werden.
- *<Threadname>* ist die Symbolbezeichnung des Threads, innerhalb von dem die Nachricht in die Protokolldatei geschrieben wurde.
- [*<Nachrichtenquelle>*] ist die Bezeichnung des Systems, welches das Schreiben der Nachricht in die Protokolldatei initiiert hat. Die Quelle ist nicht immer verfügbar.
- *<Nachricht>* ist die Textbeschreibung von Aktionen gemäß der Protokollierungsstufe. Das Feld kann sowohl eine formale Beschreibung der Nachricht als auch die Werte einiger jeweils relevanter Variablen beinhalten.

Beispiel:

```
1. 20081023.171700.74 inf [001316] mth:12 [Sch] Job "Purge unsent IS
   events" said OK
```

wobei:

- `20081023` – <*Jahr*><*Monat*><*Tag*>.
- `171700` – <*Stunde*><*Minute*><*Sekunde*>.
- `74` – <*Hundertstel_der_Sekunde*>.
- `inf` – <*Nachrichtentyp*> – Informationen.
- `[001316]` – [<*Prozess-ID*>].
- `mth:12` – <*Threadname*>.
- `[Sch]` – [<*Nachrichtenquelle*>] - Planer.
- `Job "Purge unsent IS events" said OK` – <*Nachricht*> über die ordnungsgemäße Ausführung der Aufgabe **Nicht gesendete Ereignisse löschen**.

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`

   wobei:

   - `20081028` – <*Jahr*><*Monat*><*Tag*>.
   - `135755` – <*Stunde*><*Minute*><*Sekunde*>.
   - `61` – <*Hundertstel_der_Sekunde*>.
   - `inf` – <*Nachrichtentyp*> – Informationen.
   - `[001556]` – [<*Prozess-ID*>].
   - `srv:0` – <*Threadname*>.
   - `tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193` – <*Nachricht*> über die Herstellung einer neuen Verbindung über den angegebenen Socket.

Anhang L. Integration von Web API und Dr.Web Enterprise Security Suite

Detaillierte Informationen über **Web API** finden Sie im Handbuch **Web API für Dr.Web Enterprise Security Suite**.

Verwendung

Die in Dr.Web Enterprise Security Suite integrierte **Web API** ermöglicht Ihnen, Konten und Benutzer des Service automatisiert zu verwalten. So können Sie die API bei der Erstellung von dynamischen Seiten verwenden, durch die Sie Anforderungen von Benutzern entgegennehmen und Ihnen Installationsdateien versenden.

Authentifizierung

Zur Kommunikation mit dem Dr.Web Server wird das Protokoll HTTP(S) verwendet. **Web API** nimmt REST-Anfragen entgegen und schickt eine Antwort in Form einer XML-Datei zurück. Für den Zugriff auf Web API wird die Basic HTTP-Authentifizierung verwendet (nach RFC 2617). Wird die Norm RFC 2617 nicht eingehalten, werden die Client-Angaben (der Anmeldename und das Passwort des Administrators von Dr.Web Enterprise Security Suite) vom HTTP(S) Server nicht angefordert.

Anhang M. Lizenzen

In diesem Abschnitt finden Sie eine Liste der Drittanbieter-Programmbibliotheken, die Dr.Web Enterprise Security Suite zurzeit verwendet, Informationen zu ihrer Lizenzierung und Links auf ihre offiziellen Webseiten.

Drittanbieter-Bibliothek	Lizenz	URL des Projekts
asio	https://www.boost.org/LICENSE_1_0.txt*	https://think-async.com/Asio/
boost	https://www.boost.org/LICENSE_1_0.txt*	https://www.boost.org/
brotli	MIT License**	https://github.com/google/brotli
bsdiff	Custom	http://www.daemonology.net/bsdiff/
c-ares	https://c-ares.haxx.se/license.html*	https://c-ares.haxx.se/
cairo	Mozilla Public License** GNU Lesser General Public License**	https://www.cairographics.org/
CodeMirror	MIT License**	https://codemirror.net/
curl	https://curl.se/docs/copyright.html*	https://curl.se/libcurl/
ICU	http://www.unicode.org/copyright.html#License*	http://site.icu-project.org/home
fontconfig	Custom	https://www.freedesktop.org/wiki/Software/fontconfig/
freetype	GNU General Public License** FreeType Project License (BSD like)	https://www.freetype.org/
GCC runtime libraries	GNU General Public License** with exception*	http://gcc.gnu.org/
HTMLayout	Custom	https://terrainformatica.com/a-homepage-section/htmlayout/
jemalloc	https://github.com/jemalloc/jemalloc/blob/dev/COPYING*	https://github.com/jemalloc/jemalloc
jQuery	MIT License** GNU General Public License**	https://jquery.com/

Drittanbieter-Bibliothek	Lizenz	URL des Projekts
JSON4Lua	MIT License**	https://github.com/craigmj/json4lua
Leaflet	BSD License https://github.com/Leaflet/Leaflet/blob/master/LICENSE*	https://leafletjs.com/
libpng	http://libpng.org/pub/png/src/libpng-LICENSE.txt*	http://libpng.org/pub/png/libpng.html
libradius	Juniper Networks, Inc.*	https://www.freebsd.org/
libssh2	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/
lzma	GNU Lesser General Public License** Common Public License**	https://www.7-zip.org/sdk.html
ncurses	MIT License**	https://invisible-island.net/ncurses/announce.html
Net-snmp	http://www.net-snmp.org/about/license.html*	http://www.net-snmp.org/
nghttp2	MIT License**	https://nghttp2.org/
Noto Sans CJK	https://scripts.sil.org/cms/scripts/render_download.php?format=file&media_id=OFL_plaintext&filename=OFL.txt*	https://www.google.com/get/noto/help/cjk/
OpenLDAP	https://www.openldap.org/software/release/license.html*	https://www.openldap.org/
OpenSSL	https://www.openssl.org/source/license.html*	https://www.openssl.org/

Drittanbieter-Bibliothek	Lizenz	URL des Projekts
Oracle Instant Client	https://www.oracle.com/downloads/licenses/instant-client-lic.html*	https://www.oracle.com/index.html
ParaType Free Font	https://www.paratype.ru/public/pt_openlicense_eng.asp*	https://www.paratype.ru/
pcre	http://www.pcre.org/licence.txt*	http://www.pcre.org/
pixman	MIT License**	http://pixman.org/
Prototype JavaScript framework	MIT License**	http://prototypejs.org/assets/2009/8/31/prototype.js
script.aculo.us scriptaculous.js	http://madrobby.github.io/scriptaculous/license/*	http://script.aculo.us/
slt	MIT License**	https://code.google.com/archive/p/slt
SQLite	Public Domain https://www.sqlite.org/copyright.html	https://www.sqlite.org/index.html
wtl	Common Public License** Microsoft Public License**	https://sourceforge.net/projects/wtl/
zlib	http://www.zlib.net/zlib_license.html*	http://www.zlib.net/

* – Der Lizenztext wird nachfolgend aufgeführt.

** – Die Texte der Basis-Lizenzen sind im Internet unter folgenden Links abrufbar:

Lizenz	Adresse
Common Public License	https://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
Microsoft 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

Lizenz	Adresse
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

```
Copyright © 1991-2018 Unicode, Inc. All rights reserved.

Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data
files and any associated documentation (the "Data Files") or Unicode software and any associated
documentation (the "Software") to deal in the Data Files or Software without restriction,
including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or
sell copies of the Data Files or Software, and to permit persons to whom the Data Files or
Software are furnished to do so, provided that either (a) this copyright and permission notice
appear with all copies of the Data Files or Software, or (b) this copyright and permission
notice appear in associated Documentation.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT
HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR
CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS,
WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in
advertising or otherwise to promote the sale, use or other dealings in these Data Files or
Software without prior written authorization of the copyright holder.
```

M5. GCC runtime libraries—exception

```
GCC is Copyright (C) 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997,
1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008 Free Software Foundation, Inc.

GCC is free software; you can redistribute it and/or modify it under the terms of the GNU
General Public License as published by the Free Software Foundation; either version 3, or (at
your option) any later version.

GCC is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even
the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
General Public License for more details.

Files that have exception clauses are licensed under the terms of the GNU General Public
License; either version 3, or (at your option) any later version.

The following runtime libraries are licensed under the terms of the GNU General Public License
(v3 or later) with version 3.1 of the GCC Runtime Library Exception (included in this file):

 - libgcc (libgcc/, gcc/libgcc2.[ch], gcc/unwind*, gcc/gthr*, gcc/coretypes.h, gcc/crtstuff.c,
gcc/defaults.h, gcc/dwarf2.h, gcc/emults.c, gcc/gbl-ctors.h, gcc/gcov-io.h, gcc/libgcov.c,
gcc/tsystem.h, gcc/typeclass.h).

 - libdecnumber
```

```
 - libgomp

 - libssp

 - libstdc++-v3

 - libobjc

 - libmudflap

 - libgfortran

 - The libgnat-4.4 Ada support library and libgnatvsn library.

 - Various config files in gcc/config/ used in runtime libraries.

GCC RUNTIME LIBRARY EXCEPTION

Version 3.1, 31 March 2009

Copyright (C) 2009 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but
changing it is not allowed.

This GCC Runtime Library Exception ("Exception") is an additional permission under section 7 of
the GNU General Public License, version 3 ("GPLv3"). It applies to a given file (the "Runtime
Library") that bears a notice placed by the copyright holder of the file stating that the file
is governed by GPLv3 along with this Exception.

When you use GCC to compile a program, GCC may combine portions of certain GCC header files and
runtime libraries with the compiled program. The purpose of this Exception is to allow
compilation of non-GPL (including proprietary) programs to use, in this way, the header files
and runtime libraries covered by this Exception.

0. Definitions.

A file is an "Independent Module" if it either requires the Runtime Library for execution after
a Compilation Process, or makes use of an interface provided by the Runtime Library, but is not
otherwise based on the Runtime Library.

"GCC" means a version of the GNU Compiler Collection, with or without modifications, governed by
version 3 (or a specified later version) of the GNU General Public License (GPL) with the option
of using any subsequent versions published by the FSF.

"GPL-compatible Software" is software whose conditions of propagation, modification and use
would permit combination with GCC in accord with the license of GCC.

"Target Code" refers to output from any compiler for a real or virtual target processor
architecture, in executable form or suitable for input to an assembler, loader, linker and/or
execution phase. Notwithstanding that, Target Code does not include data in any format that is
used as a compiler intermediate representation, or used for producing a compiler intermediate
representation.

The "Compilation Process" transforms code entirely represented in non-intermediate languages
designed for human-written code, and/or in Java Virtual Machine byte code, into Target Code.
Thus, for example, use of source code generators and preprocessors need not be considered part
of the Compilation Process, since the Compilation Process can be understood as starting with the
output of the generators or preprocessors.

A Compilation Process is "Eligible" if it is done using GCC, alone or with other GPL-compatible
software, or if it is done without using any work based on GCC. For example, using non-GPL-
compatible Software to optimize any GCC intermediate representations would not qualify as an
Eligible Compilation Process.
```

```
1. Grant of Additional Permission.

You have permission to propagate a work of Target Code formed by combining the Runtime Library
with Independent Modules, even if such propagation would otherwise violate the terms of GPLv3,
provided that all Target Code was generated by Eligible Compilation Processes. You may then
convey such a combination under terms of your choice, consistent with the licensing of the
Independent Modules.

2. No Weakening of GCC Copyleft.

The availability of this Exception does not imply any general presumption that third-party
software is unaffected by the copyleft requirements of the license of GCC.
```

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

```
Copyright (c) 2010-2018, Vladimir Agafonkin

Copyright (c) 2010-2011, CloudMade

All rights reserved.
```

```
Redistribution and use in source and binary forms, with or without modification, are permitted
provided that the following conditions are met:

   1. Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.

   2. Redistributions in binary form must reproduce the above copyright notice, this list of
conditions and the following disclaimer in the documentation and/or other materials provided
with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.
```

M8. Libpng

```
If you modify libpng you may insert additional notices immediately following this sentence.

This code is released under the libpng license.

libpng versions 1.0.7, July 1, 2000 through 1.6.32, August 24, 2017 are Copyright (c) 2000-2002,
2004, 2006-2017 Glenn Randers-Pehrson, are derived from libpng-1.0.6, and are distributed
according to the same disclaimer and license as libpng-1.0.6 with the following individuals
added to the list of Contributing Authors:

   Simon-Pierre Cadieux

   Eric S. Raymond

   Mans Rullgard

   Cosmin Truta

   Gilles Vollant

   James Yu

   Mandar Sahastrabuddhe

   Google Inc.

   Vadim Barkov

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against
infringement.  There is no warranty that our efforts or the library will fulfill any of your
particular purposes or needs.  This library is provided with all faults, and the entire risk of
satisfactory quality, performance, accuracy, and effort is with the user.

Some files in the "contrib" directory and some configure-generated files that are distributed
with libpng have other copyright owners and are released under other open source licenses.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c) 1998-2000
Glenn Randers-Pehrson, are derived from libpng-0.96, and are distributed according to the same
```

disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors:

   Tom Lane

   Glenn Randers-Pehrson

   Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996-1997 Andreas Dilger, are derived from libpng-0.88, and are distributed according to the same disclaimer and license as libpng-0.88, with the following individuals added to the list of Contributing Authors:

   John Bowler

   Kevin Bracey

   Sam Bushell

   Magnus Holmgren

   Greg Roelofs

   Tom Tanner

Some files in the "scripts" directory have other copyright owners but are released under this license.

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995-1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the following set of individuals:

   Andreas Dilger

   Dave Martindale

   Guy Eric Schalnat

   Paul Schmidt

   Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

  1. The origin of this source code must not be misrepresented.

  2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.

  3. This Copyright notice may not be removed or altered from any source or altered source distribution.

```
The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the
use of this source code as a component to supporting the PNG file format in commercial products.
 If you use this source code in a product, acknowledgment is not required but would be
appreciated.



Glenn Randers-Pehrson

glennrp at users.sourceforge.net

April 1, 2017
```

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

```
Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>

Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>

Copyright (c) 2006-2007 The Written Word, Inc.

Copyright (c) 2007 Eli Fant <elifantu@mail.ru>

Copyright (c) 2009-2014 Daniel Stenberg

Copyright (C) 2008, 2009 Simon Josefsson

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 copyright holder nor the names of any other 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.
```

M11. Linenoise NG

linenoise

```
Copyright (c) 2010, Salvatore Sanfilippo <antirez at gmail dot com>

Copyright (c) 2010, Pieter Noordhuis <pcnoordhuis at gmail dot com>

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 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:
```

```
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
```

Kapitel 3: Häufig gestellte Fragen

Dr.Web Server auf einen anderen Rechner umziehen (unter Windows)

Beim Server-Umzug müssen Sie die Einstellungen von Transportprotokollen berücksichtigen. Ändern Sie bei Bedarf die entsprechenden Einstellungen im Bereich **Administration** → **Dr.Web Server-Konfiguration**, in der Registerkarte **Transport**.

Detaillierte Anweisungen zum Start und Beenden des Servers finden Sie im **Administratorhandbuch** unter Dr.Web Server starten und beenden.

So verschieben den Dr.Web Server unter Windows (für gleiche Versionen des Dr.Web Servers)

1. Beenden Sie den Dienst des Dr.Web Servers.
2. Führen Sie die Datei `drwcsd.exe` mit dem Schalter `exportdb` über die Befehlszeile aus, um den Inhalt der Datenbank in eine Datei zu exportieren. Beim Export unter Windows sollte der vollständige Exportbefehl ungefähr wie folgt aussehen:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log exportdb <vollständiger_Dateiname>
   ```

3. Speichern Sie den Inhalt des Verzeichnisses `C:\Program Files\DrWeb Server\etc` und den Schlüssel `drwcsd.pub` aus `C:\Program Files\DrWeb Server\webmin\install`.
4. Deinstallieren Sie den Server.
5. Installieren Sie den neuen Server (mit einer neuen Datenbank) auf dem gewünschten Rechner. Beenden Sie den Dienst des Dr.Web Servers über die Windows-Diensteverwaltung oder über das Verwaltungscenter.
6. Kopieren Sie den Inhalt des bereits gespeicherten Verzeichnisses `etc` in `C:\Program Files\DrWeb Server\etc` und den Schlüssel `drwcsd.pub` sowie das Zertifikat `drwcsd-certificate.pem` in `C:\Program Files\DrWeb Server\webmin\install`.
7. Führen Sie die Datei `drwcsd.exe` mit dem Schalter `importdb` über die Befehlszeile aus, um den Inhalt der Datenbank aus der Datei zu importieren. Unter Windows sollte der vollständige Importbefehl ungefähr wie folgt aussehen:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -log=drwcsd.log importdb <vollständiger_Dateiname>
   ```

8. Starten Sie den Dienst des Dr.Web Servers.

Wenn eine eingebettete Datenbank verwendet wird, ist es nicht erforderlich, Datenbanken zu exportieren und zu importieren. Sie können einfach die Datei der eingebetteten Datenbank `database.sqlite` abspeichern und die neue Datenbankdatei auf dem installierten Server durch die alte Datei aus dem vorherigen Server ersetzen.

So verschieben Sie den Dr.Web Server unter Windows (für unterschiedliche Versionen des Dr.Web Servers)

1. Beenden Sie den Dienst des Dr.Web Servers.
2. Speichern Sie die Datenbank mithilfe des SQL Server-Tools (wenn eine eingebettete Datenbank verwendet wird, speichern Sie einfach die Datei `database.sqlite`).
3. Speichern Sie den Inhalt des Verzeichnisses `C:\Program Files\DrWeb Server\etc` und den Schlüssel `drwcsd.pub` aus `C:\Program Files\DrWeb Server\webmin\install`.
4. Deinstallieren Sie den Server.
5. Installieren Sie den neuen Server (mit einer neuen Datenbank) auf dem gewünschten Rechner. Beenden Sie den Dienst des Dr.Web Servers über die Windows-Diensteverwaltung oder über das Verwaltungscenter.
6. Kopieren Sie den Inhalt des bereits gespeicherten Verzeichnisses `etc` in `C:\Program Files\DrWeb Server\etc` und den Schlüssel `drwcsd.pub` sowie das Zertifikat `drwcsd-certificate.pem` in `C:\Program Files\DrWeb Server\webmin\install`.
7. Stellen Sie die Datenbank auf dem neuen Server wiederher. Geben Sie in der Konfigurationsdatei `drwcsd.conf` den Pfad zur Datenbank an.
8. Führen Sie die Datei `drwcsd.exe` mit dem Schalter `upgradedb` über die Befehlszeile aus, um das Datenbank-Upgrade auszuführen. Der Befehl unter Windows sollte ungefähr wie folgt aussehen:

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

9. Starten Sie den Dienst des Dr.Web Servers.

Änderung des Namens oder der IP-Adresse beim Umzug des Dr.Web Servers

Um die Agents, für welche die Adresse des Servers nicht in den Einstellungen des Agents auf der Workstation, sondern über das Verwaltungscenter festgelegt wird, verschieben zu können, lassen Sie die beiden Server eingeschaltet, bis der Vorgang abgeschlossen ist.

1. Verschieben Sie den Server wie oben beschrieben.
2. Für alle Agents, die vom alten Server bedient wurden, geben Sie die Adresse des neuen Servers gemäß der Vorgehensweise unter Dr.Web Agent mit einem anderen Dr.Web Server verbinden an.

Bei den Agents, für welche die Adresse des neuen Servers nicht in den Einstellungen des Agents auf der Workstations, sondern über das Verwaltungscenter festgelegt wurde, muss die Adresse des neuen Servers in den Einstellungen des Agents auf beiden Servern angegeben werden.

3. Warten Sie, bis alle Agents mit dem neuen Server verbunden sind. Erst danach können Sie den alten Server deinstallieren.

Dr.Web Agent mit einem anderen Dr.Web Server verbinden

Sie können den Agent mit einem anderen Server über einen der folgenden Wege verbinden:

1. Über das Verwaltungscenter

   Ohne direkten Zugriff auf die Workstation können Sie den Agent nur dann remote konfigurieren, wenn diese Workstation mit dem alten Server verbunden ist. Sie müssen auch über den Zugriff auf das Verwaltungscenter sowohl des alten als auch des neuen Servers verfügen.

2. Direkt auf der Workstation

   Um Änderungen direkt auf der Workstation vornehmen zu können, brauchen Sie Administratorrechte und Rechte zum Ändern der Einstellungen des Agents, die auf dem Server festgelegt werden. Falls Sie diese Rechte nicht besitzen, können Sie die Verbindung mit dem anderen Server lokal erst dann erneut herstellen, wenn Sie den installierten Agent deinstallieren und danach einen neuen Agent mit den Einstellungen des neuen Servers installieren. Wenn Sie kein Recht zur lokalen Deinstallation des Agents haben, verwenden Sie das Dienstprogramm Dr.Web Remover, um den Agent von der Workstation zu deinstallieren. Alternativ können Sie den Agent über das Verwaltungscenter deinstallieren.

So verbinden Sie den Dr.Web Agent mit einem anderen Server über das Verwaltungscenter

1. Erlauben Sie auf dem neuen Server den Workstations mit falschen Autorisierungsparametern, als Newbie neue Autorisierungsparameter anzufordern. Wechseln Sie hierzu im Verwaltungscenter zur Registerkarte unter **Administration** → **Dr.Web Server-Konfiguration** → **Allgemein**:
   a) Aktivieren Sie das Kontrollkästchen **Nicht autorisierte Workstations zu Newbies machen**, falls es deaktiviert ist.
   b) Wenn in der Dropdown-Liste **Registrierungsmodus für Newbies** die Option **Zugriff immer verweigern** gewählt ist, setzen Sie diese auf **Zugriff manuell bestätigen** oder **Zugriff automatisch erlauben**.
   c) Um die vorgenommenen Änderungen zu übernehmen, klicken Sie auf die Schaltfläche **Speichern** und starten Sie den Server neu.

   Wenn Ihre Unternehmensrichtlinie Änderung der im Schritt 1 aufgeführten Einstellung verbietet, müssen Sie die Autorisierungsparameter der Workstation, die dem im Verwaltungscenter erstellten Konto entsprechen, direkt an der Workstation festlegen.

2. Auf dem alten Server, mit dem der Agent verbunden ist, müssen Sie die Parameter des neuen Servers festlegen. Wählen Sie dafür im Hauptmenü des Verwaltungscenters den Punkt **Antivirus-Netzwerk** → wählen Sie in der hierarchischen Liste des Antivirus-Netzwerks die gewünschte Workstation (oder die Gruppe, um alle Workstations dieser Gruppe auf einmal neu zu verbinden) → wählen Sie dann im Verwaltungsmenü den Punkt **Verbindungsparameter**:
   a) Wenn das Zertifikat des neuen Servers nicht mit dem Zertifikat des alten Servers übereinstimmt, geben Sie im Feld **Zertifikat** den Pfad zum Zertifikat des neuen Servers an.
   b) Geben Sie im Feld **Server** die Adresse des neuen Servers an.

c) Klicken Sie auf die Schaltfläche **Speichern**.

So verbinden Sie den Dr.Web Agent mit einem anderen Server direkt auf der Workstation

1. In den Einstellungen des Agents müssen Sie die Parameter des neuen Servers festlegen. Wählen Sie dafür im Kontextmenü des Agent-Symbols: **Einstellungen** → Rubrik **Allgemein** → Punkt **Server** → Bereich **Verbindungsparameter** → Schaltfläche **Einstellungen ändern**:
   a) Wenn das Zertifikat des neuen Servers nicht mit dem Zertifikat des alten Servers übereinstimmt, geben Sie mit der Schaltfläche **Zertifikatliste** den Pfad zum Zertifikat des neuen Servers an.
   b) Geben Sie mit der Schaltfläche **Hinzufügen** die entsprechenden Parameter des neuen Servers an.
2. Fügen Sie die Workstation zu Newbies hinzu (setzen Sie die Parameter für die Autorisierung auf dem Server zurück). Klicken Sie dafür im Verbindungsparameter-Bereich aus dem Schritt 1 der Reihe nach folgende Schaltflächen an: Schaltfläche **Workstation-Verbindungsparameter** → Schaltfläche **Parameter zurücksetzen und als Newbie verbinden** → Schaltfläche **Parameter zurücksetzen**.

Wenn Ihnen die ID und das Passwort zum Verbinden mit dem neuen Server bekannt sind, können Sie diese in den Feldern **ID der Workstation** und **Passwort** angeben. In diesem Fall müssen Sie die Workstation nicht zu Newbies hinzufügen.

DBMS von Dr.Web Enterprise Security Suite wechseln

Für Windows

Detaillierte Anweisungen zum Start und Beenden des Servers finden Sie im **Administratorhandbuch** unter Dr.Web Server starten und beenden.

1. Beenden Sie den Dienst des Dr.Web Servers.
2. Führen Sie die Datei `drwcsd.exe` mit dem Schalter `exportdb` über die Befehlszeile aus, um den Inhalt der Datenbank in eine Datei zu exportieren. Beim Export unter Windows sollte der vollständige Exportbefehl ungefähr wie folgt aussehen:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
   Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
   verbosity=all -log=drwcsd.log exportdb D:\esbase.es
   ```

   In diesem Beispiel wird davon ausgegangen, dass der Dr.Web Server in dem Verzeichnis `C:\Program Files\DrWeb Server` installiert ist und die Datenbank in eine gewisse Datei `esbase.es` im Wurzelverzeichnis des Laufwerks `D` exportiert wird.

   Wenn der Pfad zur Datei (bzw. der Dateiname) Leerzeichen und/oder nationale Sonderzeichen enthält, muss der Pfad in Anführungszeichen gesetzt werden:

   ```
   "D:\<langer Name>\esbase.es"
   ```

3. Starten Sie den Dr.Web Server, stellen Sie eine Verbindung zwischen dem Verwaltungscenter und Server her und konfigurieren Sie den Server für das andere DBMS. Ignorieren Sie dabei die Aufforderung zum Neustart des Servers.
4. Beenden Sie den Dienst des Dr.Web Servers.
5. Löschen Sie die Datenbankdatei.
6. Starten Sie über die Befehlszeile die Datei `drwcsd.exe` mit dem Schalter `initdb`, um die neue Datenbank zu initialisieren. Der Initialisierungsbefehl für den Server unter Windows sollte ungefähr wie folgt aussehen:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
   Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
   verbosity=all -log=drwcsd.log -- initdb D:\Keys\agent.key - - <Passwort>
   ```

   In diesem Beispiel wird davon ausgegangen, dass der Server im Verzeichnis `"C:\Program Files\DrWeb Server"` installiert ist, und der Schlüssel des Agents `agent.key` in `D:\Keys` liegt.

   Wenn der Pfad zur Datei (bzw. der Dateiname) Leerzeichen und/oder nationale Sonderzeichen enthält, muss der Pfad in Anführungszeichen gesetzt werden:

   ```
   "D:\<langer Name>\agent.key"
   ```

7. Führen Sie die Datei `drwcsd.exe` mit dem Schalter `importdb` über die Befehlszeile aus, um den Inhalt der Datenbank aus der Datei zu importieren. Unter Windows sollte der vollständige Importbefehl ungefähr wie folgt aussehen:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log importdb D:\esbase.es"
```

8. Starten Sie den Dienst des Dr.Web Servers.

Für Betriebssysteme der UNIX-Familie

1. Beenden Sie den Dienst des Dr.Web Servers mit dem folgenden Skript:
   - Für **Linux**:

```
/etc/init.d/drwcsd stop
```

   - Für **FreeBSD**:

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

   oder über das Verwaltungscenter.
2. Starten Sie den Server mit dem Schalter `exportdb`, um den Inhalt der Datenbank in eine Datei zu exportieren. Die Befehlszeile aus dem Installationsverzeichnis des Servers sollte ungefähr wie folgt aussehen:
   - Für **Linux**:

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

   - Für **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log exportdb /var/drwcs/esbase.es
```

   In diesem Beispiel wird davon ausgegangen, dass die Datenbank in die Datei `esbase.es` exportiert wird, die sich im Benutzerverzeichnis befindet.
3. Starten Sie den Dienst des Dr.Web Servers mit dem folgenden Skript:
   - Für **Linux**:

```
/etc/init.d/drwcsd start
```

   - Für **FreeBSD**:

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

   Stellen Sie eine Verbindung zwischen dem Verwaltungscenter und Server her und konfigurieren Sie den Server für das andere DBMS. Wählen Sie dafür im Menü **Administration** → den Punkt **Dr.Web Server-Konfiguration** → und dann die Registerkarte **Datenbank**.

Sie können den Server für ein anderes DBMS konfigurieren, indem Sie die Konfigurationsdatei des Servers `drwcsd.conf` bearbeiten. Dafür müssen Sie den Eintrag über die aktuelle Datenbank auskommentieren/löschen und die neue Datenbank angeben (mehr dazu finden Sie im Anhang G1. Konfigurationsdatei des Dr.Web Servers).

Ignorieren Sie dabei die Aufforderung zum Neustart des Servers.

4. Beenden Sie den Dr.Web Server (s. den Schritt **1**).
5. Löschen Sie die Datenbankdatei.
6. Starten Sie die Datei `drwcsd` mit dem Schalter `initdb`, um die neue Datenbank zu initialisieren. Der Initialisierungsbefehl sollte ungefähr wie folgt aussehen:
   - Für **Linux**:

```
/etc/init.d/drwcsd -log=drwcsd.log initdb
```

   - Für **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log initdb
```

7. Starten Sie die Datei `drwcsd` mit dem Schalter `importdb`, um den Inhalt der Datenbank aus der Datei zu importieren. Der Importbefehl sollte ungefähr wie folgt aussehen:
   - Für **Linux**:

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

   - Für **FreeBSD**:

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

8. Starten Sie den Dr.Web Server (s. den Schritt **3**).

Wenn Sie das Skript des Servers anpassen (z. B. das Installationsverzeichnis des Servers angeben, die Ausführlichkeit der Protokollierung ändern usw.) wollen, ändern Sie die entsprechenden Werte im Start-Skript:

- Für **FreeBSD**:

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

- Für **Linux**:

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

Datenbank von Dr.Web Enterprise Security Suite wiederherstellen

Der Dr.Web Server sichert regelmäßig wichtige Daten, darunter auch die Lizenzschlüssel, den Datenbankinhalt, den privaten Schlüssel, die Konfiguration des Servers und des Verwaltungscenters.

Sicherungskopien werden in folgenden Verzeichnissen abgespeichert:

- Für **Windows**: <*Installationslaufwerk*>`:\DrWeb Backup`
- Für **Linux**: `/var/opt/drwcs/backup`
- Für **FreeBSD**: `/var/drwcs/backup`

Damit die Daten regelmäßig gesichert werden, enthält der Zeitplan des Servers eine entsprechende tägliche Aufgabe. Wenn der Zeitplan diese Aufgabe nicht enthält, sollten Sie diese manuell erstellen.

Alle Dateien aus der Sicherungskopie, den Datenbankinhalt ausgenommen, können sofort verwendet werden. Die Sicherungskopie der Datenbank wird im Format `.gz` gespeichert, das mit `gzip` oder anderen Packprogrammen kompatibel ist. Der Datenbankinhalt, der in der Sicherungskopie gespeichert ist, kann in die aktuelle Datenbank des Servers über den Befehl `importdb` importiert werden. Somit können Sie die Daten wiederherstellen.

Die Sicherungskopie, die vom Administrator manuell über das Verwaltungscenter **Administration** → **Datenbankverwaltung** → **Export** (nur im Modus **Gesamte Datenbank exportieren**) erstellt wurde, kann ebenfalls zur Wiederherstellung der Datenbank verwendet werden. Da solche Sicherungskopie als XML-Datei gespeichert wird, müssen Sie für den Import den Befehl `xmlimportdb` ausführen.

Datenbank für verschiedene Versionen des Dr.Web Servers wiederherstellen

Die Datenbank kann nur aus der Sicherungskopie wiederhergestellt werden, die mithilfe des Servers derselben Hauptversion wie die der Server, auf dem die Wiederherstellung ausgeführt wird, erstellt wurde.

Beispiel:

- Sie können die Datenbank aus der Sicherungskopie, die mithilfe des Servers der Version 10 erstellt wurde, nur bei der Verwendung des Servers der Version 10 wiederherstellen.
- Bei der Verwendung des Servers der Version 10 können Sie keine Datenbank aus der Sicherungskopie, die mithilfe des Servers der Version 5 oder 6 erstellt wurde, wiederherstellen.

Wenn die Datenbank bei der Aktualisierung des Servers von einer früheren Version auf die Version 12.0 beschädigt wurde, gehen Sie so vor:

1. Deinstallieren Sie den Server der Version 12.0. Die Sicherungskopien der vom Server verwendeten Dateien werden automatisch gespeichert.
2. Installieren Sie den Server derjenigen Version, die vor der Aktualisierung installiert war und mit deren Hilfe die Sicherungskopie erstellt wurde.

   Gemäß der standardmäßigen Upgrade-Vorgehensweise müssen Sie dabei alle gespeicherten Dateien des Servers, Datenbankdatei ausgenommen, verwenden.

   Erstellen Sie eine neue Datenbank während der Installation des Servers.
3. Stellen Sie die Datenbank aus der Sicherungskopie gemäß der allgemeinen Vorgehensweise wiederher (s. unten).
4. Deaktivieren Sie in den Einstellungen des Servers die Protokolle des Agents, Servers und Netzwerk-Installers. Wählen Sie dafür im Hauptmenü des Verwaltungscenters den Punkt **Administration**. Wählen Sie im geöffneten Fenster den Punkt **Dr.Web Server-Konfiguration**, wechseln Sie dann zur Registerkarte **Module** und deaktivieren Sie die entsprechenden Kontrollkästchen.
5. Aktualisieren Sie den Server auf die Version 12.0 gemäß der allgemeinen Vorgehensweise (mehr dazu finden Sie im **Administratorhandbuch** unter Dr.Web Enterprise Security Suite und ihre einzelnen Komponenten aktualisieren).
6. Aktivieren Sie wieder die Protokolle des Agents, Servers und Netzwerk-Installers, die Sie im Schritt 4 deaktiviert haben.

Für Windows

Detaillierte Anweisungen zum Start und Beenden des Servers finden Sie im **Administratorhandbuch** unter Dr.Web Server starten und beenden.

So stellen Sie die Datenbank aus einer Sicherungskopie wiederher

1. Beenden Sie den Dient des Dr.Web Servers, falls er gerade ausgeführt wird.
2. Importieren Sie aus der entsprechenden Sicherungsdatei den Inhalt der Datenbank. Der Importbefehl sollte ungefähr wie folgt aussehen:

   ```
   "C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all -log=drwcsd.log importdb "<Pfad_zur_Sicherungsdatei>\database.gz"
   ```

   Dieser Befehl muss in einer Zeile stehen. Bei diesem exemplarischen Befehl wird davon ausgegangen, dass der Server im Verzeichnis `C:\Program Files\DrWeb Server` installiert ist.
3. Starten Sie den Dienst des Dr.Web Servers.

So stellen Sie die Datenbank aus einer Sicherungskopie beim Wechsel der Server-Version (innerhalb einer Hauptversion) oder bei der Beschädigung der aktuellen Datenbank-Version wiederher

1. Beenden Sie den Dient des Dr.Web Servers, falls er gerade ausgeführt wird.
2. Löschen Sie den Inhalt der aktuellen Datenbank. Gehen Sie so vor:
   2.1. Wenn Sie eine eingebettete Datenbank verwenden:
      a) Löschen Sie die Datenbankdatei `database.sqlite`.
      b) Initialisieren Sie die neue Datenbank. Der Initialisierungsbefehl für den Server unter Windows sollte ungefähr wie folgt aussehen:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log -- initdb D:\Keys\agent.key - - <Passwort>
```

      Dieser Befehl muss in einer Zeile stehen (siehe auch das Format des Befehls `drwcsd` mit dem Schalter `initdb` im H3.3. Befehle zur Datenbankverwaltung). Im Beispiel wird davon ausgegangen, dass der Server im Verzeichnis `C:\Program Files\DrWeb Server` installiert ist, und der Lizenzschlüssel `agent.key` im Verzeichnis `D:\Keys` liegt.
      c) Sobald dieser Befehl ausgeführt wird, wird im Unterverzeichnis `var` des Installationsverzeichnisses vom Dr.Web Server die Datei der neuen Datenbank `database.sqlite` angelegt.
   2.2. Wenn Sie eine externe Datenbank verwenden, bereinigen Sie die Datenbank mit dem Befehl `cleandb` (s. den H3.3. Befehle zur Datenbankverwaltung).
3. Importieren Sie aus der entsprechenden Sicherungsdatei den Inhalt der Datenbank. Der Importbefehl sollte ungefähr wie folgt aussehen:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all -log=drwcsd.log importdb "<Pfad_zur_Sicherungsdatei>\database.gz"
```

   Dieser Befehl muss in einer Zeile stehen. Bei diesem exemplarischen Befehl wird davon ausgegangen, dass der Server im Verzeichnis `C:\Program Files\DrWeb Server` installiert ist.
4. Starten Sie den Dienst des Dr.Web Servers.

Für Betriebssysteme der UNIX-Familie

1. Beenden Sie den Dr.Web Server (falls ausgeführt):
   - Für **Linux**:

```
/etc/init.d/drwcsd stop
```

   - Für **FreeBSD**:

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

2. Löschen Sie die Datenbankdatei `database.sqlite` aus dem folgenden Installationsverzeichnis des Dr.Web Servers:
   - Für **Linux**: `/var/opt/drwcs/`
   - Für **FreeBSD**: `/var/drwcs/`

   Wenn Sie eine externe Datenbank verwenden, können Sie die Datenbank mit dem Befehl `cleandb` aufräumen (s. den H3.3. Befehle zur Datenbankverwaltung).

3. Initialisieren Sie die Datenbank des Servers. Dazu dient der folgende Befehl:
   - Für **Linux**:

```
/etc/init.d/drwcsd -log=drwcsd.log initdb
```

   - Für **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log initdb
```

4. Sobald dieser Befehl ausgeführt wird, wird im Ordner `var` des Installationsverzeichnisses vom Dr.Web Server die Datei der neuen Datenbank `database.sqlite` angelegt.
5. Importieren Sie aus der entsprechenden Sicherungsdatei den Inhalt der Datenbank. Der Importbefehl sollte ungefähr wie folgt aussehen:
   - Für **Linux**:

```
/etc/init.d/drwcsd -log=drwcsd.log importdb
"<Pfad_zur_Sicherungsdatei>/database.gz"
```

   - Für **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log importdb
"<Pfad_zur_Sicherungsdatei>/database.gz"
```

6. Starten Sie den Dr.Web Server.
   - Für **Linux**:

```
/etc/init.d/drwcsd start
```

   - Für **FreeBSD**:

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

   Wenn Sie das Skript des Servers anpassen (z. B. das Installationsverzeichnis des Servers angeben usw.) wollen, ändern Sie die entsprechenden Werte im Start-Skript:
   - Für FreeBSD: `/usr/local/etc/rc.d/drwcsd`

- Für Linux: `/etc/init.d/drwcsd`

Wenn Sie die Ausführlichkeit des Serverprotokolls ändern wollen, verwenden Sie die Datei `local.conf`:

- Für Linux: `/var/opt/drwcs/etc/local.conf`
- Für FreeBSD: `/var/drwcs/etc/local.conf`

Falls einige Agents nach der Erstellung der letzten Sicherungskopie installiert wurden, können sie sich nach der Wiederherstellung der Datenbank mit dem Server nicht mehr verbinden. Sie können aber solche Workstations zu Newbies machen. Aktivieren Sie hierzu im Abschnitt **Administration** → **Dr.Web Server-Konfiguration** auf der Registerkarte **Allgemein** das Kontrollkästchen bei **Nicht autorisierte Workstations zu Newbies machen**. Wählen Sie in der Dropdown-Liste **Registrierungsmodus für Newbies** die Option **Zugriff automatisch erlauben** aus. Klicken Sie auf **Speichern** und starten Sie den Server neu.

Nachdem alle Workstations mit dem neuen Server verbunden sind, passen Sie die aktuellen Einstellungen des Servers entsprechend der Sicherheitsrichtlinie Ihres Unternehmens an.

Wir empfehlen Ihnen, nach der Wiederherstellung der Datenbank eine Verbindung mit Server über das Verwaltungscenter herzustellen. Wählen Sie hierzu **Administration** → **Dr.Web Server-Aufgabenplaner** aus und überprüfen Sie, ob der Zeitplan die Aufgabe **Kritische Daten des Servers sichern** enthält. Wenn solche Aufgabe fehlt, sollten Sie diese Aufgabe manuell erstellen.

Agents auf LAN-Servern aktualisieren

Bei der Aktualisierung der Agents, die auf LAN-Servern installiert sind, kann der Neustart der Workstations oder das Beenden der Netzwerksoftware, die auf diesen Workstations betrieben wird, unerwünscht sein.

Um unnötige Ausfallzeiten von Workstations, die wichtige LAN-Funktionen ausführen, zu vermeiden, können Sie zur Aktualisierung der Agents und Antivirensoftware folgende Vorgehensweise verwenden:

1. Ersetzen Sie im Zeitplan des Servers die standardmäßigen Aufgaben zur Aktualisierung aller Komponenten durch die Aufgaben zur Aktualisierung der Virendatenbanken.
2. Erstellen Sie eine neue Aufgabe zur Aktualisierung aller Komponenten zum passenden Zeitpunkt, in dem die Aktualisierung die Leistung und Stabilität der LAN-Server nicht beeinträchtigen kann.

   Die Vorgehensweise beim Erstellen und Bearbeiten von Aufgaben im Zeitplan des Servers finden Sie im **Administratorhandbuch** unter Zeitplan des Dr.Web Servers konfigurieren.

Solche Komponenten wie SpIDer Gate, SpIDer Mail und die Dr.Web Firewall sollten nicht auf den Servern installiert werden, die wichtige Netzwerkfunktionen (z. B. Funktion eines Domänencontrollers oder Lizenz-Verteilungsservers usw.) erfüllen. Dadurch verhindern Sie eventuelle Konflikte zwischen Netzwerkdiensten und internen Komponenten des Dr.Web Antivirenprogramms.

Administrator-Passwort von Dr.Web Enterprise Security Suite wiederherstellen

Wenn Sie Ihr Administrator-Passwort für den Zugriff auf den Dr.Web Server verloren oder vergessen haben, können Sie es anzeigen lassen bzw. ändern, indem Sie auf die Server-Datenbank direkt zugreifen:

a) Bei der Verwendung einer eingebetteten Datenbank können Sie das Administrator-Passwort auslesen und ändern, indem Sie das Tool `drwidbsh` benutzen, das in der Distribution des Servers enthalten ist (siehe den Abschnitt H7.2. Dienstprogramm zur Verwaltung der eingebetteten Datenbank).

b) Bei der Verwendung einer externen Datenbank benutzen Sie den jeweiligen SQL-Client.

> Die Parameter von Administratorkonten sind in der Tabelle `admins` gespeichert.

Exemplarische Verwendung von drwidbsh:

1. Starten Sie das Tool `drwidbsh3` und geben Sie den Pfad zur Datenbankdatei an:
   - Für eine eingebettete DB unter Linux:

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

   - Für eine eingebettete DB unter Windows:

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

> Wenn Sie eine eingebettete DB im älteren Format IntDB verwenden, z. B. beim Upgrade des Servers von der Version 6, hat die Datenbank den Standardnamen `dbinternal.dbs`. Der Name des Tools zur Datenbankverwaltung ist `drwidbsh`.

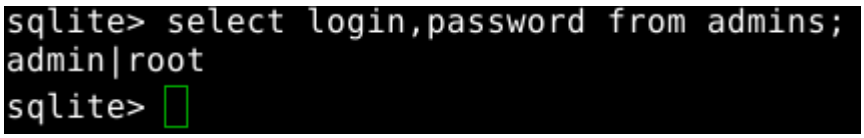
2. Um alle Daten, die in der Tabelle `admins` gespeichert sind, anzuzeigen, führen Sie den folgenden Befehl aus:

```
select * from admins;
```

3. Um die Namen und Passwörter aller Administratorkonten anzeigen zu lassen, führen Sie den folgenden Befehl aus:

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

4. Das Ergebnis für den Fall, dass es nur ein Konto mit dem Namen `admin` und dem Passwort `root` gibt, sehen Sie im folgenden Bildschirmabbild:



5. Um das Passwort zu ändern, verwenden Sie den Befehl `update`. Im folgenden Beispielbefehl wird das Passwort des Kontos `admin` durch `qwerty` ersetzt:

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

6. Um das Tool zu beenden, führen Sie den folgenden Befehl aus:

```
.exit
```

Detaillierte Beschreibung des Tools `drwidbsh` finden Sie im Anhang H7.2. Dienstprogramm zur Verwaltung der eingebetteten Datenbank.

DFS bei der Installation des Agents über Active Directory verwenden

Bei der Installation eines Dr.Web Agents über Active Directory können Sie das verteilte Dateisystem (DFS) verwenden.

Dieses Verfahren empfiehlt sich vor allem, wenn im lokalen Netzwerk mehrere Domänencontroller vorhanden sind.

So installieren Sie den Dr.Web Agent in einem Netzwerk mit mehreren Domänencontrollern

1. Erstellen Sie auf jedem der Domänencontroller ein Verzeichnis mit dem gleichen Namen.
2. Führen Sie mithilfe von DFS die erstellten Verzeichnisse in ein Zielverzeichnis zusammen.
3. Führen Sie eine administrative Installation des Pakets `*.msi` im erstellten Zielverzeichnis durch (mehr dazu finden Sie in der **Installationsanleitung** unter Dr.Web Agent über Active Directory installieren).
4. Verwenden Sie das erstellte Zielverzeichnis beim Zuweisen des Pakets im Gruppenrichtlinienobjekt-Editor.

   Verwenden Sie hierfür das folgende Format: `\\<domain>\<folder>`

   wobei <*domain*> der Domänenname und <*folder*> der Zielverzeichnisname ist.

Funktionsfähigkeit des Antivirus-Netzwerks nach einem Absturz des Dr.Web Servers wiederherstellen

Falls Ihr Dr.Web Server aufgrund eines Fehlers ausfällt, sollten Sie der nachfolgend beschriebenen Vorgehensweise folgen, um die Funktionsfähigkeit des Antivirus-Netzwerks wiederherzustellen, ohne die Agents auf den Workstations neu installieren zu müssen.

Es wird davon ausgegangen, dass der neue Dr.Web Server auf einem Rechner mit der gleichen IP-Adresse und dem gleichen DNS-Namen installiert wird.

Wiederherstellung aus einer Sicherungskopie des Dr.Web Servers

Der Dr.Web Server sichert regelmäßig wichtige Daten, darunter auch die Lizenzschlüssel, den Datenbankinhalt, den privaten Schlüssel, die Konfiguration des Servers und des Verwaltungscenters.

Sicherungskopien werden in folgenden Verzeichnissen abgespeichert:

- Für **Windows**: <*Installationslaufwerk*>`:\DrWeb Backup`
- Für **Linux**: `/var/opt/drwcs/backup`
- Für **FreeBSD**: `/var/drwcs/backup`

Damit die Daten regelmäßig gesichert werden, enthält der Zeitplan des Servers eine entsprechende tägliche Aufgabe. Wenn der Zeitplan diese Aufgabe nicht enthält, sollten Sie diese manuell erstellen.

Alle Dateien aus der Sicherungskopie, den Datenbankinhalt ausgenommen, können sofort verwendet werden. Die Sicherungskopie der Datenbank wird im Format `.gz` gespeichert, das mit `gzip` oder anderen Packprogrammen kompatibel ist. Der Datenbankinhalt, der in der Sicherungskopie gespeichert ist, kann in die aktuelle Datenbank des Servers über den Befehl `upimportdb` importiert werden. Somit können Sie die Daten wiederherstellen.

Die Sicherungskopie, die vom Administrator manuell über das Verwaltungscenter **Administration** → **Datenbankverwaltung** → **Export** (nur im Modus **Gesamte Datenbank exportieren**) erstellt wurde, kann ebenfalls zur Wiederherstellung der Datenbank verwendet werden. Da solche Sicherungskopie als XML-Datei gespeichert wird, müssen Sie für den Import den Befehl `xmlupimportdb` ausführen.

Es empfiehlt sich, die erstellten Sicherungskopien und andere wichtige Dateien auf einem anderen Rechner zu speichern. Dadurch vermeiden Sie Datenverluste, falls der Rechner, auf dem Dr.Web Server installiert ist, beschädigt wird. Bei Bedarf können Sie die Daten schnell zurückkopieren und alle Funktionen des Servers wiederherstellen. Bei Verlust der Lizenzschlüssel können Sie diese jederzeit erneut anfordern. Detaillierte Informationen zur Vorgehensweise finden Sie im **Administratorhandbuch** unter Lizenzierung.

So stellen Sie den Server nach einem Absturz mithilfe einer Sicherungskopie wiederher

1. Wählen Sie den Rechner aus, auf dem der neue Dr.Web Server installiert werden soll. Isolieren Sie den Rechner von aktiven Agents: Trennen Sie den Rechner vom Netzwerk, in dem die Agents aktiv sind, oder vergeben Sie dem Rechner vorübergehend eine andere IP-Adresse. Auf Wunsch können Sie den Rechner über einen alternativen Weg im Netzwerk nicht mehr erreichbar machen.
2. Installieren Sie den neuen Dr.Web Server.
3. Fügen Sie im Bereich **Lizenz-Manager** den Lizenzschlüssel der vorherigen Installation des Servers hinzu und verteilen Sie ihn auf die entsprechenden Gruppen, insbesondere auf die Gruppe **Everyone**. Diese Einstellung muss vorgenommen werden, falls bei der Installation des Servers kein Lizenzschlüssel festgelegt wurde.
4. Aktualisieren Sie das Repository des installierten Dr.Web Servers über das GUS:
   a) Wechseln Sie im Veraltungscenter zu **Administration** → **Repository-Status**.
   b) Klicken Sie auf **Auf Updates überprüfen**, um zu überprüfen, ob neue Updates für alle Produkte auf dem GUS verfügbar sind, und eventuelle die Updates vom GUS herunterzuladen.
5. Falls neue Versionen der Server-Software verfügbar sind, aktualisieren Sie den Server auf die neueste Version:
   a) Wechseln Sie im Veraltungscenter zu **Administration** → **Dr.Web Server**.
   b) Um die Auflistung aller Versionen des Servers anzuzeigen, klicken Sie auf die aktuelle Version des Servers oder klicken Sie die Schaltfläche **Liste der Versionen** an. Der Bereich **Dr.Web Server-Updates** mit der Liste verfügbarer Updates und Sicherungskopien des Servers öffnet sich.
   c) Um die Software des Servers auf die neueste Version zu aktualisieren, aktivieren Sie in der Liste **Alle Versionen** die Option neben der letzten Version des Servers und klicken Sie auf **Speichern**.
   d) Warten Sie, bis der Aktualisierungsvorgang abgeschlossen ist.
6. Beenden Sie den Server.
7. Um den öffentlichen Schlüssel aus der Sicherungskopie des privaten Schlüssels abzurufen, verwenden Sie das Tool `drwsign`, das sich im Unterverzeichnis `\bin` des Server-Installationsverzeichnisses befindet:

   `drwsign extract [-private-key=`<*privater_Schlüssel*>`]` <*öffentlicher_Schlüssel*>

   Geben Sie als <*privaten_Schlüssel*> und <*öffentlichen_Schlüssel*> den Pfad, unter dem der private Schlüssel liegt, und den Pfad ein, unter dem der erstellte öffentliche Schlüssel abgelegt werden soll.
8. Ersetzen Sie die kritischen Daten des Servers durch die Daten aus der Sicherungskopie:

Betriebssystem	Öffentlicher Schlüssel	Konfigurationsdateien
Windows	`webmin\install` im Installationsverzeichnis des Servers	`etc` im Installationsverzeichnis des

Betriebssystem	Öffentlicher Schlüssel	Konfigurationsdateien
		Servers
Linux	`/opt/drwcs/webmin/install`	`/var/opt/drwcs/etc`
FreeBSD	`/usr/local/drwcs/webmin/install`	`/var/drwcs/etc`

9. Konfigurieren Sie die Datenbank.

   a) Externe Datenbank:

   Keine weiteren Eingriffe sind erforderlich, sofern die Konfigurationsdatei des Servers gespeichert wurde.

   Falls die Version des Servers aus den neuesten Updates höher als die Version des ausgefallenen Servers ist, aktualisieren Sie die externe Datenbank mit dem Befehl `upgradedb`:

   - Für Windows:

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

   - Für Linux:

```
/etc/init.d/drwcsd -log=drwcsd.log upgradedb
```

   - Für FreeBSD:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log upgradedb
```

   b) Sicherungskopie einer externen oder eingebetteten Datenbank:

   Wenn Sie eine externe Datenbank verwenden, müssen Sie zunächst die Datenbank mit dem Befehl `cleandb` (s. den Anhang H3.3. Befehle zur Datenbankverwaltung) aufräumen.

   Importieren Sie die Datenbank aus der entsprechenden Sicherungsdatei und aktualisieren Sie die Datenbank auf die Version des installierten Servers, indem Sie den Befehl `upimportdb` ausführen:

   - Für 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 -log=drwcsd.log upimportdb
"<Pfad_zur_Sicherungsdatei>\database.gz"
```

   - Für Linux:

```
/etc/init.d/drwcsd -log=drwcsd.log upimportdb
"<Pfad_zur_Sicherungsdatei>/database.gz"
```

   - Für FreeBSD:

```
/usr/local/etc/rc.d/drwcsd -log=drwcsd.log upimportdb
"<Pfad_zur_Sicherungsdatei>/database.gz"
```

Allen ersetzten Dateien des Servers müssen die gleichen Berechtigungen vergeben werden, die bei der vorherigen Installation des Servers festgelegt wurden.

Für UNIX-basierte Betriebssysteme: `rw` für `drwcs:drwcs`.

10. Starten Sie den Server.
11. Vergewissern Sie sich, dass die Daten aus der Sicherungskopie der Datenbank (Einstellungen der Agents, Struktur des Antivirus-Netzwerks u. a.) sicher und aktuell sind.
12. Machen Sie den Server wieder erreichbar für die Agents (siehe den Schritt 1).

Falls einige Agents nach der Erstellung der letzten Sicherungskopie installiert wurden, können sie sich nach der Wiederherstellung der Datenbank mit dem Server nicht mehr verbinden. Sie können aber solche Workstations zu Newbies machen. Aktivieren Sie hierzu im Abschnitt **Administration** → **Dr.Web Server-Konfiguration** auf der Registerkarte **Allgemein** das Kontrollkästchen bei **Nicht autorisierte Workstations zu Newbies machen**. Wählen Sie in der Dropdown-Liste **Registrierungsmodus für Newbies** die Option **Zugriff automatisch erlauben** aus. Klicken Sie auf **Speichern** und starten Sie den Server neu.

Nachdem alle Workstations mit dem neuen Server verbunden sind, passen Sie die aktuellen Einstellungen des Servers entsprechend der Sicherheitsrichtlinie Ihres Unternehmens an.

Wiederherstellung ohne Sicherungskopie des Dr.Web Servers

So stellen Sie den Server nach einem Absturz ohne Sicherungskopie wiederher

1. Wählen Sie den Rechner aus, auf dem der neue Dr.Web Server installiert werden soll. Isolieren Sie den Rechner von den aktiven Agents: Trennen Sie den Rechner vom Netzwerk, in dem die Agents aktiv sind, oder vergeben Sie dem Rechner vorübergehend eine andere IP-Adresse. Auf Wunsch können Sie den Rechner über einen alternativen Weg im Netzwerk nicht mehr erreichbar machen.
2. Installieren Sie den neuen Dr.Web Server.
3. Fügen Sie im Bereich **Lizenz-Manager** den Lizenzschlüssel der vorherigen Installation des Servers hinzu und verteilen Sie ihn auf die entsprechenden Gruppen, insbesondere auf die Gruppe **Everyone**. Diese Einstellung muss vorgenommen werden, falls bei der Installation des Servers kein Lizenzschlüssel festgelegt wurde.
4. Aktualisieren Sie das Repository des installierten Dr.Web Servers über das GUS:
   a) Wechseln Sie im Veraltungscenter zu **Administration** → **Repository-Status**.

b) Klicken Sie auf **Auf Updates überprüfen**, um zu überprüfen, ob neue Updates für alle Produkte auf dem GUS verfügbar sind, und eventuelle die Updates vom GUS herunterzuladen.

5. Falls neue Versionen der Server-Software verfügbar sind, aktualisieren Sie den Server auf die neueste Version:
   a) Wechseln Sie im Veraltungscenter zu **Administration** → **Dr.Web Server**.
   b) Um die Auflistung aller Versionen des Servers anzuzeigen, klicken Sie auf die aktuelle Version des Servers oder klicken Sie die Schaltfläche **Liste der Versionen** an. Der Bereich **Dr.Web Server-Updates** mit der Liste verfügbarer Updates und Sicherungskopien des Servers öffnet sich.
   c) Um die Software des Servers auf die neueste Version zu aktualisieren, aktivieren Sie in der Liste **Alle Versionen** die Option neben der letzten Version des Servers und klicken Sie auf **Speichern**.
   d) Warten Sie, bis der Aktualisierungsvorgang abgeschlossen ist.
6. Ändern Sie die Verbindungseinstellungen der Workstations in der Konfiguration des Servers:
   a) Wechseln Sie zu **Administration** → **Dr.Web Server-Konfiguration**.
   b) Aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **Nicht autorisierte Workstations zu Newbies machen**.
   c) Wählen Sie auf der Registerkarte **Allgemein** in der Dropdown-Liste **Registrierungsmodus für Newbies** die Option **Zugriff automatisch erlauben** aus.
   d) Klicken Sie auf **Speichern** und starten Sie den Server neu.
7. Erstellen Sie im Abschnitt **Antivirus-Netzwerk** des Verwaltungscenters die benutzerdefinierten Gruppen, die in der hierarchischen Struktur der früheren Version vorhanden waren. Definieren Sie bei bedarf die Mitgliedschaftsregeln für die Workstations in der erstellten benutzerdefinierten Gruppen.
8. Konfigurieren Sie bei Bedarf die Agents und den Server (außer Einstellungen im Schritt 6) entsprechend den Einstellungen in der früheren Version.
9. Passen Sie bei Bedarf die Einstellungen des Repository unter **Administration** → **Detaillierte Repository-Konfiguration** an.
10. Machen Sie den Server wieder erreichbar für die Agents (siehe den Schritt 1).
11. Ersetzen Sie den öffentlichen Schlüssel auf allen Workstations des Netzwerks, die sich mit dem neuen Server verbinden sollen.
    - Falls der Selbstschutz auf der Workstation aktiviert ist, kopieren Sie den öffentlichen Schlüssel, der bei der Installation des neuen Servers erstellt wurde, auf die Workstation und führen Sie den folgenden Befehl aus:

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

      oder

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

      Geben Sie als <*Schlüssel*> den Pfad zur kopierten öffentlichen Schlüssel an.

Der öffentliche Schlüssel wird ins Installationsverzeichnis des Agents (standardmäßig ins Verzeichnis `%ProgramFiles%\DrWeb` kopiert (mehr dazu finden Sie im Anhang H2. Dr.Web Agent für Windows).

- Falls der Selbstschutz auf der Workstation deaktiviert ist, können Sie den öffentlichen Schlüssel verwenden, der bei der Installation des neuen Servers erstellt wurde. Kopieren Sie hierzu diesen Schlüssel in das oben angegebene Verzeichnis.

12. Nachdem alle Workstations mit dem neuen Server verbunden sind, passen Sie die Einstellungen des Servers, die Sie im Schritt 5 konfiguriert haben, entsprechend der Sicherheitsrichtlinie Ihres Unternehmens an.

Protokollierungsstufe für den Dr.Web Server unter Windows konfigurieren

Sie können die Protokollierungsstufe für den Dr.Web Server unter Windows auf eine der folgenden Weisen ändern:

- Über den Bereich **Dr.Web Server-Konfiguration** → **Protokoll** im Verwaltungscenter.

  Diese Vorgehensweise sollte bevorzugt werden. Im Abschnitt **Protokoll** können Sie eine beliebige Protokollierungsstufe und andere Einstellungen des Servers festlegen.

  Weitere Informationen hierzu finden Sie im **Administratorhandbuch** unter Dr.Web Server konfigurieren → Protokoll.

- Mit dem folgende Konsolenbefehl:

  ```
  drwcsd [<Schalter>] install
  ```

  Sie können eine beliebige Protokollierungsstufe mit dem Schalter `--verbosity` festlegen.

  Befehlszeilenoptionen zur Serververwaltung werden unter H3.8. Beschreibung der Schalter erläutert.

  Mit diesem exemplarischen Befehl setzen Sie die Protokollierungsstufe auf **Detailliert**:

  ```
  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 --log=drwcsd.log --rotate=10,50m install
  ```

  Alle anderen Schalter sind optional und werden verwendet, wenn die Standardpfade für die Installation des Servers und für die Arbeitsverzeichnisse des Servers geändert wurden.

  Nachdem Sie die Protokollierungsstufe geändert haben, starten Sie den Server mit dem folgenden Befehl neu:

  ```
  drwcsd restart
  ```

- Über die Befehle im **Startmenü** von Windows.

  Zur Auswahl stehen nur folgende Protokollierungsstufen: **Detaillierte Protokollierung** und **Standardprotokoll**:

a) **Programme → Dr.Web Server → Serververwaltung → Detaillierte Protokollierung**
oder
Programme → Dr.Web Server → Serververwaltung → Standardprotokoll

b) **Programme → Dr.Web Server → Serververwaltung → Neu starten**

Automatische Positionsbestimmung für Workstations unter Android

Dr.Web Enterprise Security Suite ermöglicht, den Administrator des Antivirus-Netzwerks über den Standort der geschützten mobilen Android-Geräte zu informieren.

So ermitteln Sie den Standort des mobilen Geräts

1. Konfigurieren Sie auf dem Dr.Web Server die Übermittlung der Ortungsdaten des gewünschten mobilen Geräts:
   a) Wechseln Sie im Verwaltungscenter zum Bereich **Antivirus-Netzwerk** und wählen Sie in der Baumstruktur des Antivirus-Netzwerks die benötigte Workstation oder Gruppe von Workstations unter Android aus.
   b) Wählen Sie im Verwaltungsmenü den Punkt **Dr.Web für Android**.
   c) Aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **Standort verfolgen**. Legen Sie über die Dropdown-Liste **Sendeintervall für Koordinaten** fest, wie häufig die Standortinformationen aktualisiert werden sollen.
   d) Speichern Sie die vorgenommenen Änderungen.
2. Die automatische Positionsbestimmung erfolgt wie folgt:
   - Falls die Standortermittlung (GPS, Mobilfunknetze) auf dem mobilen Gerät aktiviert ist und es ausreichend starkes und stabiles Signal besteht, wird die Position des mobilen Geräts clientseitig mit Android-Bordmitteln bestimmt.
   - Falls die Standortermittlung (GPS, Mobilfunknetze) auf dem mobilen Gerät deaktiviert ist oder es nicht ausreichend starkes und stabiles Signal besteht, bietet Dr.Web Enterprise Security Suite die Möglichkeit, den Lokalisierungsdienst Yandex.Locator zur Ermittlung der Position des mobilen Geräts zu verwenden. Der Standort des Geräts wird hierbei über die festen Koordinaten der Mobilfunksendemasten (GSM, 3D, LTE) und über WiFi ID bestimmt.
     Um den Lokalisierungsdienst Yandex.Locator zu konfigurieren, müssen Sie zunächst das **Yandex.Locator Plug-in** aktivieren und entsprechend konfigurieren:
     a) Holen Sie sich einen API-Schlüssel auf der Webseite von Yandex unter https://yandex.ru/dev/locator/keys/get/.
     b) Aktivieren Sie im Dr.Web Sicherheitscenter unter **Administration → Dr.Web Server-Konfiguration → Module** das Kontrollkästchen **Yandex.Locator Plug-in**.
     c) Tragen Sie ins Feld **API-Schlüssel** den Schlüssel ein, den Sie im Schritt a) erhalten haben.
     d) Speichern Sie die vorgenommenen Änderungen und starten Sie den Dr.Web Server neu.

WiFi ID ist nur für mobile Geräte unter Android 5.1 und früher verfügbar.

3. Gehen Sie so vor, um den Standort der Workstation im Dr.Web Sicherheitscenter anzuzeigen:
   a) Wechseln Sie zum Bereich **Antivirus-Netzwerk** und wählen Sie in der Baumstruktur die Workstation aus, für die Sie die entsprechenden Einstellungen im Schritt 1 festgelegt haben.
   b) In den Eingeschärften der Workstation unter **Standort** werden automatisch die Koordinaten angezeigt, die das mobile Gerät sendet.
   c) Klicken Sie auf **Auf Karte anzeigen**, um die aktuelle Position des mobilen Geräts auf der Landkarte von OpenStreetMap anzeigen zu lassen.

Beispiele für Dr.Web Server-Datenbankabfragen

Nachfolgend finden Sie einige exemplarische SQL-Befehle, mit denen Sie Daten aus einer PostgreSQL-Datenbank abfragen können. SQL-Abfragen für andere Datenbanken können je nach konkretem Datenbanksystem abweichen.

Für bessere Lesbarkeit und Verständlichkeit wurden alle aufgeführten Abfragen absichtlich in nicht optimierter Form aufgeführt.

Aufgrund von Besonderheiten der SQL-Sprache werden bei den Abfragen die Hierarchie von Gruppen und Workstations nicht berücksichtigt.

So greifen Sie direkt auf die Datenbank zu

1. Öffnen Sie das Verwaltungscenter Ihres Servers.
2. Wechseln Sie zum Bereich **Administration** → **SQL-Konsole**.
3. Geben Sie die benötigte SQL-Abfrage ein. Unten finden Sie einige exemplarische Abfragen.
4. Klicken Sie auf die Schaltfläche **Ausführen**.

Beispiele für SQL-Abfragen

1. Workstations finden, auf denen eine Server-Version von Windows installiert ist und die Virendatenbanken älter als vom 2019.07.04-00:00:00 UTC (12.0) sind.

```
SELECT
  stations.name Station,
  groups_list.name OS,
  station_products.crev Bases
FROM
  stations
  INNER JOIN groups_list ON groups_list.platform =(
    CAST(stations.lastos AS INTEGER) & ~15728640
  )
  AND (
    (
      CAST(stations.lastos AS INTEGER) & 2130706560
    ) = 33554560
  )
  INNER JOIN station_products ON station_products.id = stations.id
  AND station_products.product = '10-drwbases'
  AND station_products.crev < 12020190704000000;
```

2. Workstations finden, bei denen es unter **Antivirus-Netzwerk** → **Statistik** → **Status** Einträge mit dem Schweregrad **Hoch** oder **Maximal** gibt.

```
SELECT
  stations.name Station
FROM
  stations
WHERE
  id IN (
    SELECT
      DISTINCT id
```

```
    FROM
      station_status
    WHERE
      severity >= 1342177280
  );
```

3. Anzahl von Workstations pro Status ermitteln.

```
SELECT
  code Code,
  COUNT(code) Num
FROM
  (
    SELECT
      DISTINCT id,
      code
    FROM
      station_status
  ) AS t
GROUP BY
  Code
ORDER BY
  Code;
```

4. 10 häufigste Bedrohungen auswählen, die im Zeitraum von 2019.06.01 bis 2019.07.01 auf den Workstations der Gruppe mit der ID '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5' oder ihrer Untergruppen erkannt wurden.

```
SELECT
  cat_virus.str Threat,
  COUNT(cat_virus.str) Num
FROM
  station_infection
  INNER JOIN cat_virus ON cat_virus.id = station_infection.virus
WHERE
  station_infection.infectiontime BETWEEN 20190601000000000
  AND 20190701000000000
  AND station_infection.id IN (
    SELECT
      sid
    FROM
      station_groups
    WHERE
      gid = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      OR gid IN (
        SELECT
          child
        FROM
          group_children
        WHERE
          id = '373a9afb-9c9a-4d4d-b9b1-de817b96bcc5'
      )
  )
GROUP BY
  cat_virus.str
ORDER BY
  Num DESC
LIMIT
  10;
```

5. 10 am meisten betroffene Workstations auswählen.

```
SELECT
  Station,
  Grp,
  Num
```

```
FROM
  (
    SELECT
      stations.id,
      groups_list.id,
      stations.name Station,
      groups_list.name Grp,
      COUNT(stations.id) Num
    FROM
      station_infection
      INNER JOIN stations ON station_infection.id = stations.id
      INNER JOIN groups_list ON groups_list.id = stations.gid
    GROUP BY
      stations.id,
      groups_list.id,
      stations.name,
      groups_list.name
    ORDER BY
      Num DESC
    LIMIT
      10
  ) AS t;
```

6. Alle Workstations aus benutzerdefinierten Gruppen entfernen, die für diese Workstations nicht primär sind.

```
DELETE FROM
  station_groups;
INSERT INTO station_groups(sid, gid)
SELECT
  stations.id,
  groups_list.id
FROM
  stations
  INNER JOIN groups_list ON stations.gid = groups_list.id
  AND groups_list.type NOT IN(1, 4);
```

7. Objekte des Antivirus-Netzwerks finden, in denen die angegebene Domain in der Whitelist der individuellen Einstellungen der Komponente SpIDer Gate vorhanden ist.

```
SELECT
  stations.name Station
FROM
  station_cfg
  INNER JOIN stations ON stations.id = station_cfg.id
WHERE
  station_cfg.component = 38
  AND station_cfg.name = 'WhiteVirUrlList'
  AND station_cfg.value = 'domain.tld';
SELECT
  groups_list.name Grp
FROM
  group_cfg
  INNER JOIN groups_list ON groups_list.id = group_cfg.id
WHERE
  group_cfg.component = 38
  AND group_cfg.name = 'WhiteVirUrlList'
  AND group_cfg.value = 'domain.tld';
SELECT
  policy_list.name Policy
FROM
  policy_cfg
  INNER JOIN policy_list ON policy_list.id = policy_cfg.id
WHERE
  policy_cfg.component = 38
```

```
  AND policy_cfg.name = 'WhiteVirUrlList'
  AND policy_cfg.value = 'domain.tld';
```

8. Ereignisse im Zusammenhang mit fehlgeschlagenen Anmeldungen von Administratoren am Verwaltungscenter in Kombination mit entsprechenden Anmeldungsfehlercodes auswählen.

```
SELECT
  admin_activity.login Login,
  admin_activity.address Address,
  activity_data.value ErrorCode,
  admin_activity.createtime EventTimestamp
FROM
  admin_activity
  INNER JOIN activity_data ON admin_activity.record = activity_data.record
WHERE
  admin_activity.oper = 10100
  AND admin_activity.status != 1
  AND activity_data.item = 'Error';
```

9. Windows-Workstations finden, auf denen die benötigten Sicherheitspatches installiert sind.

```
SELECT
  stations.name Station
FROM
  stations
WHERE
  id NOT IN (
    SELECT
      station_env_kb.id
    FROM
      station_env_kb
      INNER JOIN stations ON stations.id = station_env_kb.id
    WHERE
      (
        CAST(stations.lastos AS INTEGER) & 2130706432
      )= 33554432
      AND station_env_kb.name IN (
        SELECT
          id
        FROM
          env_strings
        WHERE
          str IN(
            'KB4012212', 'KB4012213', 'KB4012214',
            'KB4012215', 'KB4012216', 'KB4012217',
            'KB4012598'
          )
      )
  );
```

Kriterien der funktionalen Analyse

Legen Sie Kriterien der funktionalen Analyse bei der Konfiguration der funktionalen Analyse fest. Dies ermöglicht es Ihnen, den besten Schutz zu gewährleisten.

Im Bereich **Kriterien der funktionalen Analyse** finden Sie Kriterien, die Sie zum Schutz des Profils verwenden können. Wählen Sie eine Kategorie je nach Ihrem System und dem gewünschten Sicherheitsniveau aus.

Kategorien der Kriterien der funktionalen Analyse

1. **Ausführen von Anwendungen**:
   - *Ausführen von Anwendungen verhindern, die mit Zertifikaten signiert sind, die Doctor Web als Zertifikate für Adware einstuft*.
     Sperrt Anwendungen, die Werbung verbreiten.
   - *Ausführen von Anwendungen verhindern, die mit Zertifikaten signiert sind, die Doctor Web als illegal ausgestellt einstuft*.
     Sperrt Anwendungen, die mit illegal ausgestellten Zertifikaten signiert sind. Solche Zertifikate werden oft zum Signieren (potenziell) gefährlicher Anwendungen verwendet.
   - *Ausführen von Anwendungen verhindern, die mit Zertifikaten signiert sind, die Doctor Web als Zertifikate für Hacking-Tools einstuft*.
     Sperrt Anwendungen, die mit Zertifikaten signiert sind, die für Hacking-Tools verwendet werden. Die Verwendung dieses Kriteriums ist empfehlenswert.
   - *Ausführen von Anwendungen verhindern, die mit gefälschten/beschädigten Zertifikaten signiert sind*.
     Sperrt bösartige Anwendungen, die mit ungültigen Zertifikaten signiert sind. Die Verwendung dieses Kriteriums ist empfehlenswert.
   - *Ausführen von Anwendungen verhindern, die mit Zertifikaten signiert sind, die Doctor Web als Zertifikate für Schadsoftware einstuft*.
     Sperrt Anwendungen, die mit kompromittierten Zertifikaten signiert sind. Die Verwendung dieses Kriteriums ist empfehlenswert.
   - *Ausführen von Anwendungen verhindern, die mit entzogenen Zertifikaten signiert sind*.
     Sperrt Anwendungen, die mit gestohlenen oder kompromittierten Zertifikaten signiert sind. Die Verwendung dieses Kriteriums ist empfohlen, weil es die Ausführung potenziell bösartiger Anwendungen verhindert.
   - *Ausführen von Anwendungen verhindern, die mit selbstsignierten Zertifikaten signiert sind*.
     Sperrt nicht lizenzierte Software, die bösartig sein kann.
   - *Ausführen von nicht signierten Anwendungen verhindern*.
     Sperrt potenziell bösartige und nicht vertrauenswürdige Anwendungen, deren Herkunft nicht bekannt ist.
   - *Ausführen von Sysinternals-Hilfsprogrammen verhindern*.
     Schützt das System vor Kompromittierung durch Sysinternals-Hilfsprogramme.

Wenn das Kontrollkästchen **Ausführen von Systemanwendungen und Microsoft-Anwendungen zulassen** auf der Registerkarte **Erlaubnisse** aktiviert ist, können Sysinternals-Hilfsprogramme auch bei aktiviertem Ausführungsverbot gestartet werden.

   - *Ausführen von Anwendungen aus alternativen NTFS-Datenströmen (ADS) verhindern*.
     Anwendungen aus alternativen NTFS-Datenströmen (ADS) sind oft bösartig, daher ist dieses Kriterium obligatorisch.

- *Ausführen von Anwendungen aus dem Netz und freigegebenen Ressourcen verhindern*.
  Die Ausführung von Anwendungen aus dem Netz und freigegebenen Ressourcen gehört nicht zu typischen Szenarien und kann das Sicherheitssystem beeinträchtigen. Die Verwendung dieses Kriteriums ist empfehlenswert.
- *Ausführen von Anwendungen von Wechselmedien verhindern*.
  Die Ausführung von Anwendungen auf Wechselmedien gehört nicht zu typischen Szenarien und kann das Sicherheitssystem beeinträchtigen. Die Verwendung dieses Kriteriums ist empfehlenswert.
- *Ausführen von Anwendungen aus temporären Verzeichnissen verhindern*.
  Sperrt die Ausführung von Anwendungen aus temporären Verzeichnissen.
- *Ausführen von Windows/Microsoft Store-Anwendungen verhindern (nur für Windows 8 und neuer)*.
  Sperrt Anwendungen, die über den Windows/Microsoft Store heruntergeladen wurden.
- *Ausführen von Anwendungen mit doppelter/nicht-regulärer Erweiterung verhindern*.
  Sperrt die Ausführung verdächtiger Dateien mit ungewöhnlichen Dateiendungen (z. B. `*.jpg.exe`).
- *Ausführen von Bash-Shells und WSL-Anwendungen verhindern (nur für Windows 10 und neuer)*.
  Sperrt die Ausführung von Bash-Shells und WSL-Anwendungen.

2. **Laden und Ausführen von Modulen**. Für die Kriterien gibt es zwei Modi:
   - *Alle Module werden geladen*.
     Dieser Modus ist ressourcenintensiv und wird nur dann empfohlen, wenn eine verstärkte Kontrolle notwendig ist.
   - *Laden und Ausführen von Modulen in Host-Anwendungen kontrollieren*.
     Dieser Modus ist weniger ressourcenintensiv. Module werden nur in Prozessen überwacht, die ausgenutzt werden können, um das System zu kompromittieren oder Malware unter dem Deckmantel einer Systemdatei oder einer vertrauenswürdigen Datei in das System zu integrieren. Falls keine verstärkte Kontrolle notwendig ist, empfehlen wir diesen Modus.

   Für die Verwendung der Kriterien **Laden und Ausführen von Modulen** gelten dieselben Empfehlungen wie für die Verwendung der Kriterien für das Ausführen von Anwendungen.
3. **Ausführen von Skriptinterpretern**:
   - *Ausführen von CMD/BAT-Skripten verhindern*.
     Sperrt die Ausführung von `cmd`- und `bat`-Dateien.
   - *Ausführen von HTA-Skripten verhindern*.
     Sperrt die Ausführung von HTA-Skripten. Solche Skripte können bösartige Skripte bearbeiten und ausführbare Dateien herunterladen, die das System beschädigen können.
   - *Ausführen von VBScript/JavaScript verhindern*.
     Sperrt Anwendungen, die in den Skriptsprachen VBScript und JavaScript geschrieben sind. Solche Anwendungen können bösartige Skripte bearbeiten und ausführbare Dateien herunterladen, die das System beschädigen können.
   - *Ausführen von PowerShell-Skripten verhindern*.
     Sperrt die Ausführung von Skripten, die in der Skriptsprache PowerShell geschrieben sind.

Solche Skripte können bösartige Skripte bearbeiten und ausführbare Dateien herunterladen, die das System beschädigen können.

- *Ausführen von REG-Skripten verhindern*.
  Sperrt die Ausführung von reg-Skripten (`reg-Dateien`). Mit solchen Dateien können Werte in der Registry geändert oder neue Werte zur Registry hinzugefügt werden.
- *Ausführen von Skripten aus alternativen NTFS-Datenströmen (ADS) verhindern*.
  Sperrt die Ausführung von Skripten aus alternativen NTFS-Datenströmen (ADS). Solche Skripte sind oft bösartig, daher ist die Verwendung dieses Kriteriums empfehlenswert.
- *Ausführen von Skripten aus dem Netz und freigegebenen Ressourcen verhindern*.
  Die Ausführung von Skripten aus dem Netz und freigegebenen Ressourcen gehört nicht zu typischen Szenarien und kann das Sicherheitssystem beeinträchtigen. Die Verwendung dieses Kriteriums ist empfehlenswert.
- *Ausführen von Skripten von Wechselmedien verhindern*.
  Die Ausführung von Skripten auf Wechselmedien gehört nicht zu typischen Szenarien und kann das Sicherheitssystem beeinträchtigen. Die Verwendung dieses Kriteriums ist empfehlenswert.
- *Ausführen von Skripten aus temporären Verzeichnissen verhindern*.
  Die Ausführung von Skripten aus temporären Verzeichnissen gehört nicht zu typischen Szenarien und kann das Sicherheitssystem beeinträchtigen. Die Verwendung dieses Kriteriums ist empfehlenswert.

4. **Laden von Treibern**

   - *Laden von nicht signierten Treibern verhindern*.
     Sperrt das Laden von Rootkits und Bootkits. Verhindert die Ausnutzung von Schwachstellen in Software und im Betriebssystem.
     Dieser Modus ist für 64-Bit-Versionen des Betriebssystems empfohlen. Der Modus kann auch auf Rechnern mit 32-Bit-Versionen des Betriebssystems verwendet werden – vorausgesetzt, es gibt keine unsignierten Treiber im System.
   - *Laden von anfälligen Treiberversionen gängiger Software verhindern*.
     Sperrt das Laden unsicherer Versionen von Treibern gängiger Software.

   Das Verbot des Ladens anfälliger Treiberversionen gängiger Software kann nicht mithilfe von Ausnahmen umgangen werden.

   Im Übrigen gelten dieselben Empfehlungen für die Verwendung der Kriterien **Laden von Treibern** wie für die Verwendung der Kriterien für das Ausführen von Anwendungen.

5. **Installation von MSI-Paketen**.

   Für die Verwendung der Kriterien **Installation von MSI-Paketen** gelten dieselben Empfehlungen wie für die Verwendung der Kriterien für das Ausführen von Anwendungen.

6. **Integrität von ausführbaren Dateien**

   - *Erstellen von neuen ausführbaren Dateien verhindern*.
     Sperrt Versuche, neue ausführbare Dateien zu erstellen.

- *Ändern von ausführbaren Dateien verhindern*.
  Sperrt Versuche, ausführbare Dateien zu ändern.

Die Kriterien **Integrität von ausführbaren Dateien** werden nur in Systemen verwendet, die in einer vertrauenswürdigen Umgebung arbeiten. In solchen Systemen werden alle Prozesse vom Administrator gesteuert (z. B. Geldautomaten etc.).

Das Verhalten der Kriterien **Integrität von ausführbaren Dateien** in anderen Systemen ist unberechenbar. Ihre Verwendung kann sogar zum Ausfall der Workstation führen.

Die Kriterien **Integrität von ausführbaren Dateien** können nicht mithilfe von Regeln umgangen werden.

Kapitel 4: Problembehebung

Probleme bei der Remote-Installation beheben

Installationsprinzip:

1. Der Dr.Web Server verbindet sich mit der Ressource `ADMIN$` auf dem Remote-Rechner (`\\<`*Remote-Rechner*`>\ADMIN$\Temp`) und kopiert den Netzwerk-Installier `drwinst.exe` aus dem Verzeichnis `webmin\install\windows` des Server-Installationsverzeichnisses und das SSL-Zertifikat `drwcsd-certificate.pem` aus dem Verzeichnis `etc` des Server-Installationsverzeichnisses in das Verzeichnis `\\<`*Remote-Rechner*`>\ADMIN$\Temp`.
2. Der Server führt die Datei `drwinst.exe` auf dem Remote-Rechner mit den Optionen aus, die den Einstellungen im Verwaltungscenter entsprechen.

Für eine erfolgreiche Installation müssen die folgenden Voraussetzungen erfüllt sein:

1. Die Ressource `ADMIN$\Temp` auf dem Remote-Rechner muss verfügbar sein.

   Die Verfügbarkeit kann folgenderweise überprüft werden:

   Geben Sie in die Adresszeile von `Windows Explorer` die folgende Adresse ein:

   `\\<`*Remote_Rechner*`>\ADMIN$\Temp`

   Wenn die Ressource verfügbar ist, werden Sie aufgefordert, den Benutzernamen und das Passworts zum Zugriff auf diese Ressource einzugeben. Geben Sie die Anmeldedaten ein, die Sie auf der Installationsseite angegeben haben.

   Die Ressource `ADMIN$\Temp` kann aus folgenden Gründen nicht verfügbar sein:

   a) Das Konto hat keine Administratorrechte.

   b) Der Rechner ist ausgeschaltet oder die Firewall sperrt den Zugriff auf den Port 445.

   c) Der Remote-Zugriff auf die Ressource `ADMIN$\Temp` wird unter Windows Vista oder neuer eingeschränkt, wenn der Remote-Rechner der Domäne nicht angehört.

   d) Der Besitzer des Verzeichnisses wurde nicht angegeben bzw. der Benutzer oder die Gruppe hat nicht ausreichende Zugriffsrechte.
2. Auf die Dateien `drwinst.exe` und `drwcsd.pub` kann zugegriffen werden.

Im Verwaltungscenter werden detaillierte Informationen (Schritt und Fehlercode) angezeigt, die bei der Fehlerdiagnose hilfreich sein können.

Liste der Fehler, die bei einer Remote-Installation des Dr.Web Agent auftreten können

Schritt	Fehler	Ursache
SMB-Verbindung mit der Workstation <*host*> wird hergestellt	Falsche Adresse der Workstation <*host*>	Die IP-Adresse der Workstation, die für die Installation des Agents festgelegt wurde, ist keine IPv4/IPv6-Adresse oder der DNS-Name konnte nicht in eine Adresse konvertiert werden: Dieser DNS-Name ist nicht vorhanden bzw. der Namensserver ist falsch konfiguriert.
	Fehler beim Herstellen der SMB-Verbindung mit der Workstation <*host*>	SMB-Verbindung mit der Workstation konnte nicht hergestellt werden. Mögliche Ursachen: • Der Server-Dienst auf der Workstation ist deaktiviert. • TCP-Port 445 ist nicht verfügbar auf dem Remote-Rechner. Mögliche Ursachen: ▫ Der Rechner ist ausgeschaltet. ▫ Die Firewall sperrt den angegebenen Port. ▫ Auf dem Remote-Rechner ist ein Nicht-Windows-Betriebssystem installiert. • Das Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten sind nicht konfiguriert. • Der Autorisierungsserver (Domänencontroller) ist nicht verfügbar. • Unbekannter Benutzer oder ungültiges Passwort.
	Nicht genügend Rechte zum Öffnen der freigegebenen Ressource <*share*> auf der Workstation <*host*>	Die Ressource `ADMIN$` ist nicht vorhanden auf dem Remote-Rechner bzw. es sind nicht genügend Rechte zum Öffnen der Ressource vorhanden.
Dateien werden an die Workstation <*host*> übertragen	Der Pfad <*path*> konnte nicht in der freigegebenen Ressource <*share*> auf der Workstation <*host*> gefunden werden	Das Verzeichnis `ADMIN$/TEMP` fehlt.

Schritt	Fehler	Ursache
	Fehler beim Erstellen des temporären Ordners <*path*> in der freigegebenen Ressource <*share*> auf der Workstation <*host*>	Der erforderliche temporäre Ordner unter `ADMIN$/TEMP` konnte nicht erstellt werden. Mögliche Ursache: Es sind nicht genügend Schreibrechte vorhanden.
	Fehler beim Löschen des temporären Ordners <*path*> in der freigegebenen Ressource <*share*> auf der Workstation <*host*>	Der Ordner `ADMIN$/TEMP` konnte nach dem Vorgangsabschluss nicht gelöscht werden. So kann dies der Fall sein, wenn der Dienst nicht abgeschlossen ist oder wenn jemand eine Datei in diesem Ordner geöffnet hat.
	Die Datei <*path*> konnte auf dem Server nicht zum Lesen geöffnet werden Fehler beim Lesen der Datei <*path*> auf dem Server	Die Datei des Installationsprogramms fehlt auf dem Server selbst oder der Datei des Installationsprogramms wurden falsche Zugriffrechte zugewiesen.
	Die Datei <*path*> konnte in der freigegebenen Ressource <*share*> auf der Workstation <*host*> nicht zum Schreiben geöffnet werden Fehler beim Schreiben der Datei <*path*> in der freigegebenen Ressource <*share*> auf der Workstation <*host*>	Unzureichende Rechte zum Lesen/Schreiben der entsprechenden Dateien oder für die entsprechenden Ordner.
Service auf der Workstation <*host*> wird erstellt	Fehler beim Herstellen der Verbindung mit dem Server-Dienst (srvsvc RPC) auf der Workstation <*host*>	Dienste lassen sich remote nicht verwalten.
	Fehler beim Herstellen der Verbindung mit SCM auf der Workstation <*host*> Fehler beim Erstellen des Service auf der Workstation <*host*> Fehler beim Starten des Service auf der Workstation <*host*> Fehler beim Beenden des Service auf der Workstation <*host*>	Unzureichende Rechte zum Verwalten der Dienste.

Schritt	Fehler	Ursache
	Fehler beim Löschen des Service auf der Workstation <*host*>	
Service auf der Workstation <*host*> wird ausgeführt	Fehler beim Abrufen des Service-Status auf der Workstation <*host*>	Ein liegt möglicherweise ein Problem mit SCM vor.
	Installation auf der Workstation <*host*> wurde aufgrund einer Zeitüberschreitung abgebrochen	Das Installationsprogramm konnte den Agent innerhalb des angegebenen Zeitraums nicht installieren. Mögliche Gründe: geringe Kapazität des Übertragungskanals zwischen dem Server und der Workstation, Zeitüberschreitung beim Laden der erforderlichen Daten.
	Fehler beim Abrufen des lokalen Pfads zur freigegebenen Ressource <*share*> auf der Workstation <*host*>	Der Pfad zur Ressource `ADMIN$` auf der Workstation konnte nicht ermittelt werden.
	Service ist mit einem Fehler auf der Workstation <*host*> fehlgeschlagen. Abschlussstatus: <*state*>. Fehlercode: <*rc*>.	Fehler im Installationsprogramm des Agents.

Probleme mit dem BFE-Dienst bei der Installation des Dr.Web Agents für Windows beheben

Das Basisfiltermodul (BFE) ist Voraussetzung für den Start einiger Komponenten des Dr.Web Antivirus für Workstations unter Windows. Wenn der BFE-Dienst deaktiviert ist bzw. fehlt, ist die Installation des Dr.Web Agents unter Windows nicht möglich. Die Tatsache allein, dass der DFE-Dienst nicht aktiviert bzw. defekt ist, kann auf einen Virenbefall oder eventuelle Sicherheitsprobleme im System hindeuten.

Gehen Sie so vor, wenn die Installation des Dr.Web Agents aufgrund eines Problems mit dem BFE-Dienst nicht möglich ist:

1. Scannen Sie das System der betreffenden Workstation mit dem Desinfektions-Tool CureNet! von Doctor Web.

   Die kostenfreie Testversion mit einem eingeschränkten Funktionsumfang (kein Desinfizieren möglich) kann unter dem folgenden Link angefordert werden: https://download.drweb.com/curenet/.

   Die Nutzungsbedingungen und Preisinformationen zur Vollversion des Tools finden Sie unter https://estore.drweb.com/utilities/.
2. Starten Sie den BFE-Dienst manuell. Falls sich der BFE-Dienst auch manuell nicht starten lässt oder gar nicht in der Dienste-Liste vorhanden ist, wenden Sie sich an den Microsoft-Support.
3. Starten Sie das Installationsprogramm des Dr.Web Agents für Windows und führen Sie die Installation wie in der **Installationsanleitung** beschrieben durch.

   Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support von Doctor Web.

Technischer Support

Sollten Sie Probleme mit der Installation oder beim Betrieb unserer Software haben, nutzen Sie bitte folgende Möglichkeiten, bevor Sie sich an den technischen Support wenden:

- Konsultieren Sie zunächst die aktuelle Produktdokumentation unter https://download.drweb.com/doc/.
- Stöbern Sie in unseren Antworten auf die häufig gestellten Fragen unter https://support.drweb.com/show_faq/.
- Besuchen Sie das Forum von Doctor Web unter https://forum.drweb.com/. Möglicherweise wurde Ihre Frage hier schon von anderen Nutzern gestellt und beantwortet.

Wenn Sie es nicht geschafft haben, das Problem selbst zu lösen, dann können Sie sich an den technischen Support von Doctor Web über folgende Wege wenden:

- Stellen Sie eine Frage in einem entsprechenden Abschnitt unter https://support.drweb.com/.
- Rufen Sie unser deutsches Support-Team unter der Telefonnummer +49 (0) 170 4884028 oder unser internationales Support-Team unter +7 (495) 789 45 86 an. Nutzer aus Russland erreichen unsere Hotline unter der kostenlosen Rufnummer 8 800 333 7932.

Detaillierte Kontaktinformationen der Regionalvertretungen von Doctor Web finden Sie auf der offiziellen Website unter https://company.drweb.com/contacts/offices/.

Schlagwortregister