Veeam Backup and Replication v12
Common Criteria Evaluated Configuration Guide (CCECG)

Version 1.0

Revision Date: July 9, 2023

Table of Contents

Introduction

The Veeam Availability Suite™ is an application suite consisting of two components: Veeam Backup & Replication and Veeam ONE. Veeam Backup & Replication provides cloud, virtual and physical backup and recovery options as well as image-based virtual machine (VM) replication from a VM or backup. Veeam ONE provides real-time monitoring, reporting and intelligent tools for Veeam Backup & Replication, VMware vSphere, and Microsoft Hyper-V.

Document Purpose and Scope

This document provides supplementary administrative guidance for the Veeam Backup & Replication v12.

- Veeam Backup & Replication Version 12, User Guide for VMware vSphere, July, 2023 [Guide]
- Veeam Backup & Replication Version 12 Quick Start Guide for VMware vSphere, February, 2023 [QuickStart]

The installation for VMware vSphere also applies to the Server 2019 installation.

This document describes procedures on how to operate and prepare the Veeam Backup & Replication v12 to meet its Common Criteria evaluated configuration. This document is referred to as the operational user guide in the Protection Profile for Application Software, v1.4 2021-10-07 [SWAPP], and supplements the other product documentation listed above to meet the required guidance assurance activities.

TOE Overview

The Veeam Backup & Replication infrastructure consists of the following core components.

- **Backup Server Component**: performs main management operations, coordinates backup, replication and restore tasks, controls job scheduling and resource allocation.
- **Backup Proxy**: a component that sits between the Backup Server and other components of the backup infrastructure. While the Backup Server Component administers tasks, the Backup Proxy processes jobs and delivers backup traffic. The Backup Proxy tasks include the following:
    - Retrieving VM data from the production storage
    - Compressing
    - Deduplicating
    - Encryption
    - Sending data to the Backup Repository (for a backup job) or another Backup Proxy (for a replication job)
    - **VBR Console**: A VBR component that provides the application user interface and allows user access to the application functionality.

- **Backup Repository**: A backup repository where backup files, backup copies and metadata of replicated VMs are stored. During installation, VBR checks volumes of the machine on which VBR is installed and identifies a volume with the greatest amount of free disk space. On this volume, VBR creates the Backup folder that is used as the default Backup Repository.

VBR's supporting environment includes the following systems.

- **VBR Configuration Database:** stores data about the backup infrastructure, jobs, sessions and other configuration data. The database instance can be located on a PostgreSQL Server installed either locally (on the same machine where the backup server is running) or remotely. **Infrastructure servers and hosts**: Servers that are source and target for backup, replication, and other activities.
- **Backup Server**: A host machine or virtual machine on which Veeam Backup & Replication is installed.

The VBR Console is invoked locally. The Administrator must have local Administrator permissions to invoke the VBR Console. Upon invocation of the VBR Console, the Administrator is prompted for which VBR the Administrator would like to connect to. The default host is the local host. The Administrator must have SeBackupPrivilege and SeRestorePrivilege to connect to the Backup Server.

Evaluated Configuration

For this evaluation, the TOE will be deployed on a single instance that provides the full functionality required to evaluate all security functions. In addition, only backup of a local file is within scope.

Physical Boundaries

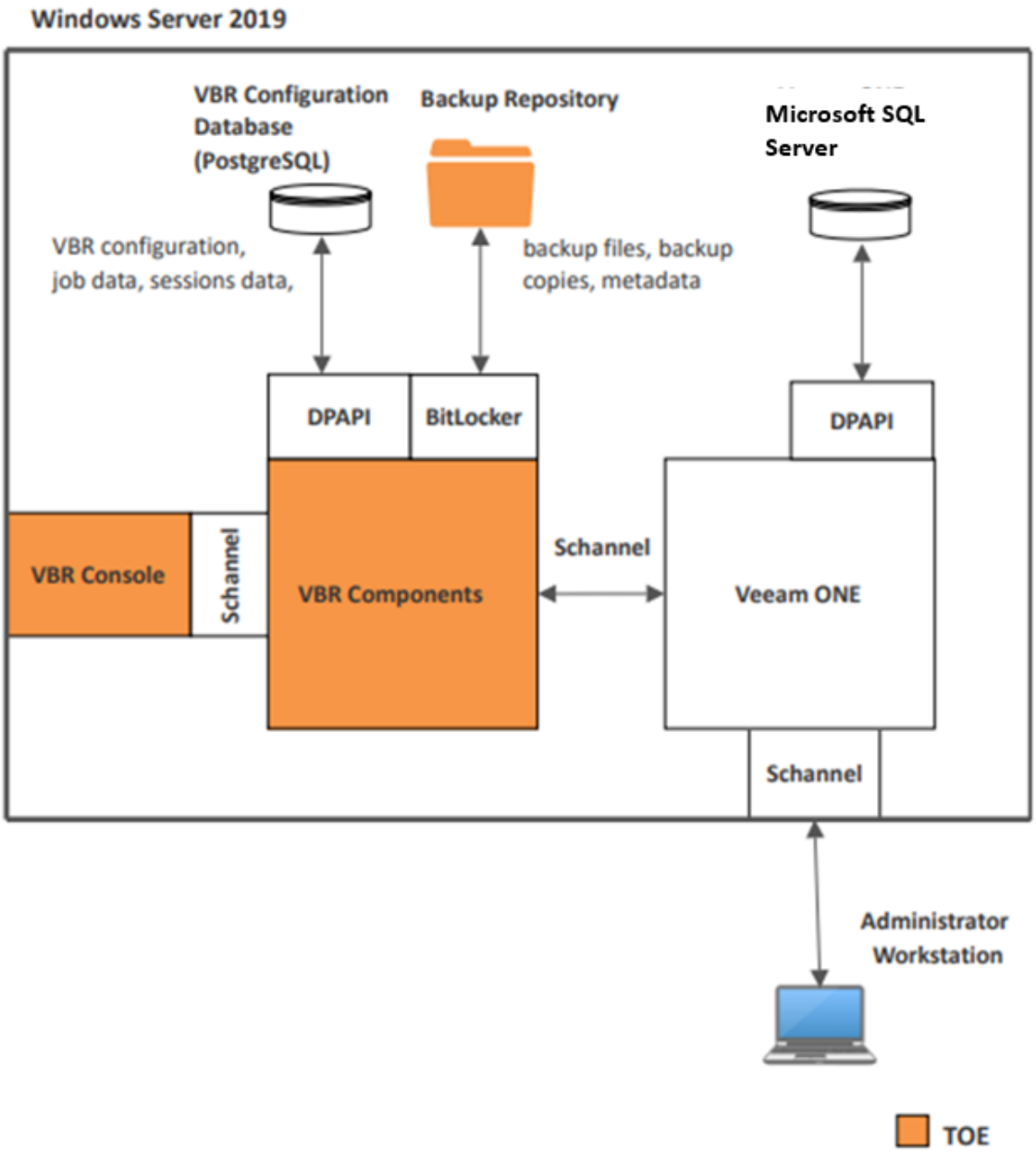
The TOE is installed on a single Microsoft Windows Server 2019 with the following minimum requirements.

Table 1 Windows Server Minimum Requirements for VBR Backup Server

Item	Minimum Requirements
CPU	x86-64 processor (minimum 4 cores recommended)
Memory	4 GB RAM plus 500 MB RAM for each concurrent job
Disk Space	5 GB for product installation and 4.5 GB for Microsoft .NET Framework 4.7.2 installation. 10 GB per 100 VM for guest file system catalog folder (persistent data)
OS	Only 64-bit versions of the following operating system: • Microsoft Windows Server 2019

Item	Minimum Requirements
Additional Software	PostgreSQL 15.1 System Center Virtual Machine Manager 2012 SP1 to 2019 Admin UI (optional, to register SCVMM server with Backup & Replication infrastructure) Microsoft .NET Framework 4.7.2 (included in the setup) Windows Installer 4.5 (included in the setup) Microsoft Windows PowerShell 5.1 (included in the setup)

The TOE in the evaluated configuration performs a backup of local files. Therefore, there are no operational environmental requirements of the evaluated configuration.



The TOE in the evaluated configuration performs a backup of local files. Therefore, there are no operational environmental requirements of the evaluated configuration.

The TOE consists of the Veeam Backup & Replication v12 application.

Logical Boundaries

The TOE provides the security functionality required by [SWAPP].

The Target of Evaluation (TOE) for the Veeam Backup & Replication v12 consists of the mandatory functionality prescribed by the [SWAPP].

The logical boundary is summarized below. In general, the following Veeam Backup & Replication v12 capabilities are considered to be within the scope of the TOE:

- **Cryptographic Support**

  The TOE invokes platform-provided cryptography to protect data at rest.

  For data at rest, the platform provided DPAPI stores configuration data, job data and session data, and the platform provided BitLocker is used to store backup files and metadata.

- **User Data Protection**
  The TOE accesses the minimum amount of Windows Server hardware and data in order to perform its function. Database connectivity information is stored in the Registry, and other TOE configuration information is saved in the PostgreSQL database.
- **Security Management**
  Both the TOE binary components themselves and the configuration settings they use are stored in locations recommended for Microsoft Windows Server.
  The TOE includes a console UI. Users must login to Windows and have permissions to access the UI in order to access the TOE.
  The console UI is used to configure the backup tasks to be performed by the TOE.
- **Privacy**
  The TOE does not handle personally identifiable information (PII) of any individuals.
- **Protection of the TSF**

  The TOE enforces various mechanisms to prevent itself from being used as an attack vector to its Windows platform. The TOE implements address space layout randomization (ASLR), does not allocate any memory with both write and execute permissions, does not write user-modifiable files to directories that contain executable files, is compiled using stack overflow protection, and is compatible with the Windows Defender security features of its host platform.

  The TOE contains libraries and invokes system APIs that are well-known and explicitly identified.

  The TOE has a mechanism to display its current software version. The TOE can be used to determine if software updates for it are available. If so, an administrator uses out of band mechanisms to securely acquire, validate, and install the update.

The TOE developer provides a secure mechanism for receiving reports of security flaws. Product vulnerabilities are tracked and addressed, and software updates are securely distributed to customers in a timely manner.

- **Trusted Path/Channels**
  The TOE does not support any network interfaces and therefore, does not provide protection of data in transit.

Assumptions

The following assumptions were drawn from the [SWAPP].

Assumption	Description
A.PLATFORM	The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

Functionality Excluded From the Evaluation Configuration

The following components/functionality/configurations/tools are excluded from the evaluated configuration.

Infrastructure

- **Off-site data** protection is excluded; only on-site data protection is supported. This excludes Veeam Cloud Connect from the evaluated configuration.
- **Veeam Agent Management**: To back up physical machines running Windows, Linux, Unix or macOS operating systems, VBR uses backup agents installed on each computer. VBR operates as a centralized control center for deploying and managing:
  - Veeam Agent for Microsoft Windows
  - Veeam Agent for Linux
  - Veeam Agent for IBM AIX
  - Veeam Agent for Oracle Solaris and

- Veeam Agent for Mac

- **Network-Attached Storage (NAS):** VBR supports backup up and restore of content of various NAS file shares. NAS backup is excluded from the evaluated configuration.
- **Tape Device Support:** Veeam provides native tape support that is fully integrated into VBR. Long-term archiving and compliance are listed as primary reasons for using tape.
- **Remote VBR Console:** Support for remote instances of the VBR Console are not included in the evaluated configuration.
- **Object Storage Repositories:** Is a repository intended for long-term data storage. It can be based on either a cloud solution or an S3 compatible storage solution. Object Storage Repositories and virtual machine backup are not supported in the evaluated configuration.

VBR Tools Excluded from the Evaluated Configuration

The VBR application includes the following utilities that enable an Administrator to perform advanced administration tasks. The following tools/utilities are excluded from the evaluated configuration.

- **Extract.exe Utility**: The VBR application includes an extract utility that can be used to recover machines from backup files. The extract utility does not require any interaction with VBR and can be used as an independent tool on Linux and Microsoft Windows machines.
- **Veeam.Backup.DBConfig.exe Utility**: VBR includes the Veeam.Backup.DBConfig.exe utility that allows an Administrator to manage connections settings for VBR and/or Veeam Backup Enterprise Manager configuration database.
- **Veeam Backup Validator**: Veeam Backup Validator is a utility that verifies the integrity of a backup file without extracting VM data. Veeam Backup Validator is a command-prompt CRC check utility that tests a backup at the file level. An Administrator may need this utility to check whether backup files were damaged.
- **Veeam Backup Configuration Tool**: The VBR application includes Veeam.Backup.Configuration.Tool.exe that enables an Administrator to manage BCO files. BCO files are backup files that contain backups of configuration databases.
- **Veeam Backup PowerShell Module** is an extension for Microsoft Windows PowerShell that adds a set of cmdlets to allow users to perform backup, replication and recovery tasks through the command-line interface of PowerShell or run custom scripts to fully automate operation of Veeam Backup & Replication.

Software Download, Installation and Configuration

Prerequisite

The application in the evaluated configuration was installed on a platform with Windows Server 2019 Standard edition. The platform processor was the Intel Xeon Gold 6126 CPU @ 2.60 GHz. The processor is included in the Skylake microarchitecture.

The application invokes platform-provided DPAPI and relies on platform provided BitLocker to protect data at rest. BitLocker must be activated before the installation of the application.

Download and Installation

See [Guide] Section *Installing Veeam Backup & Replication* provides to download and install the TOE for detailed instructions.

See [Guide] Section **Deployment > Installing Veeam Backup and Replication**

Prerequisites

A. Before You Begin
Ensure that the prerequisites are met.
The TOE will be installed as **when only backup features are used:** If you plan to use Veeam Backup & Replication for backup jobs only, the backup server should be placed in the production site.

B. Configuration Database
Veeam Backup & Replication will automatically install PostgreSQL 15.1 locally on the backup server.

Installation Steps

1. **Start Setup Wizard**
   a. Download the Veeam Backup & Replication installation image from the Download Veeam Products page. https://www.veeam.com/downloads.html
   The installation files must be manually download and installed. The installation files are packaged in .iso format. Veeam Backup & Replication installation files are signed by Veeam Software Group GmbH certificate, DigiCert is Certificate Authority in this case. Code is signed on the Veeam signing server during the build process.
   b. The installation files must be copied to the targeted platform, Autorun will open a splash screen. If Autorun is not available or disabled, run the *Setup.exe* file.
   c. In the splash screen, click *Install*.
2. **Select Component**
   At the **Select Veeam Backup & Replication Component** step of the wizard, select **Install Veeam Backup & Replication**.

3. **Read and Accept the License Agreement**
    a. At the **License Agreement** step of the wizard, read Veeam License Agreement and licensing policy as well as license agreements of 3rd party components that Veeam incorporates and license agreements of required software. To accept the license agreements and continue installing Veeam Backup & Replication, click I *Accept*.
4. **Provide License File**
    a. Follow the steps on the **License** page of the installation Wizard to install and accept the license.
5. **Install Missing Software**
    a. At the **System Configuration Check** step of the wizard, the setup wizard checks if the required software is installed on the machine. If some of the required components are missing, the setup will try to install them automatically. After the components are successfully installed, reboot is required. To reboot the machine, click *Reboot*.
    b. If the setup wizard cannot install some of the required software components automatically, install them manually and click *Retry*.
6. **Review Default Installation Settings**
    a. At the Ready to Install step of the wizard, you can select to install Veeam Backup & Replication with default installation settings or specify custom installation settings.
        i. To use the default installation settings, click Install.
        ii. To use custom installation settings, click Customize Settings. The setup wizard will include additional steps that will let you configure installation settings.

    Note: The TOE in the Common Criteria evaluated configuration does not have network access. The TOE cannot provide automatic checks for updates. The administrator must manually check for updates.
7. **Specify Service Account Settings**
    a. The **Service Account** step of the wizard is available if you have selected to configure installation settings manually.
    b. You can select an account under which you want to run the Veeam Backup Service:
        i. LOCAL SYSTEM account (recommended, used by default)
        ii. Another user account
    c. Select the default **LOCAL SYSTEM account (Recommended)** setting and click *Next*.
8. **Specify Database Engine and Instance**
    a. Accept the default settings and click *Next*.

Protection of Stored Data

The TOE invokes platform-provided DPAPI and relies on platform provided BitLocker to protect data at rest. The sensitive data consists of backup files, backup copies and metadata of replicated VMs.

Access to Platform Resources

The TOE does not access any hardware resources. The application restricts access to VBR event logs, VBR job information, and VBR infrastructure information.

Network Communications

The TOE does not require Internet access.

Management

The TOE provides authorized administrators with the ability to enable/disable backup functionality for localhost files. The administrator may create jobs to perform backups. Management functions are performed by invoking the application on the system on which the TOE is installed

Follow the following instructions to back up and restore the configuration database that Veeam Backup & Replication uses:

See [Guide] Section **Backup Infrastructure > Configuration Backup and Restore > Configuration Backup**

By default, Veeam Backup & Replication is configured to create a configuration backup daily. You can change the schedule or run the backup manually.

Configuration Backup Files

When you perform configuration backup, Veeam Backup & Replication retrieves data for the backup server from the configuration database, writes this data into a set of XML files and archives these XML files to a backup file of the BCO format.

Veeam Backup & Replication exports information about the following objects:

- **Backup infrastructure components and objects**: hosts, servers, backup proxies, repositories, WAN accelerators and jobs, global settings configured on the backup server and so on.
- **Backups**: backups, replicas and backup copies created on the backup server.
- **Sessions**: job sessions performed on the backup server.

Backup Repository Target

The resulting configuration backup file is stored in the \VeeamConfigBackup\%BackupServer% folder on the default backup repository.

When you configure a new backup repository, Veeam Backup & Replication offers you to change the configuration backup file location from the default backup repository to the new backup repository. Click **Yes**, and Veeam Backup & Replication will automatically change the backup target in the configuration backup job settings and will use this target in future.

Running Configuration Backups Manually

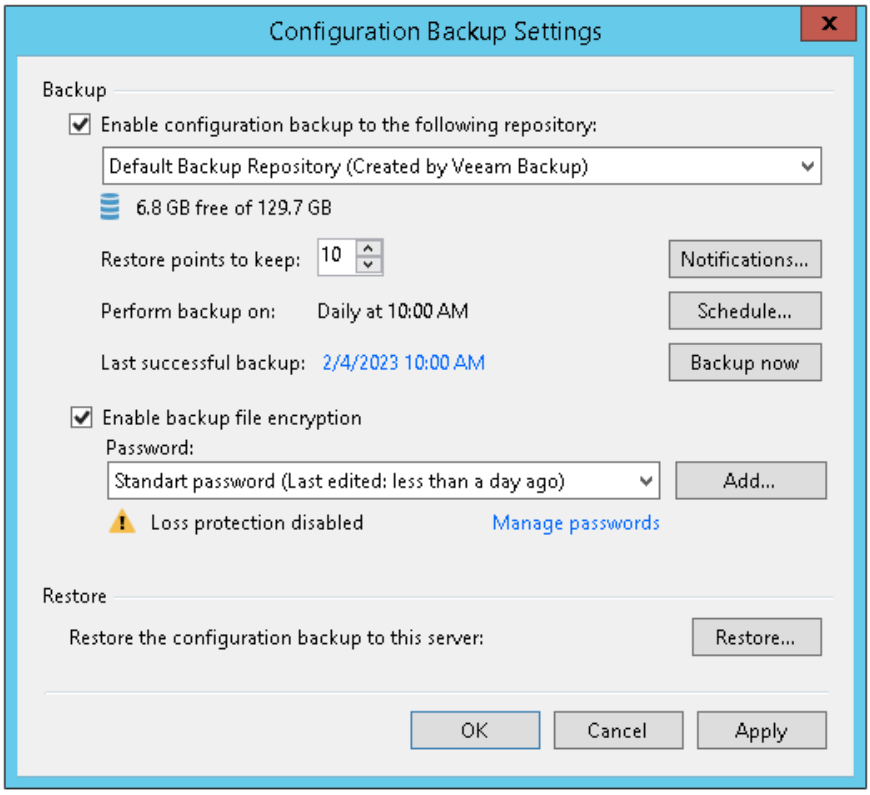
To create a configuration backup manually:

1. From the main menu, select **Configuration Backup**.
2. Make sure that the **Enable configuration backup to the following repository** check box is selected.
3. From the **Backup repository** list, choose a backup repository on which the configuration backup must be stored.
4. In the **Restore points to keep** field, specify the number of restore points that you want to maintain in the backup repository.
5. To create an encrypted backup, select the **Enable backup file encryption** check box. From the **Password** field, select a password you want to use for encryption. If you have not created a password beforehand, click **Add** or use the **Manage passwords** link to specify a new password.

   Note: Step 5 is skipped since the backup file encryption in the elevated configuration relies on the platform provided BitLocker.
6. Click **Backup now**.

Veeam Backup & Replication will back up the configuration database and store a new restore point to the selected backup repository.

See the screenshot below.



Scheduling Configuration Backups

You can instruct Veeam Backup & Replication to perform configuration backup automatically by schedule.

To schedule a configuration backup:

1. From the main menu, select **Configuration Backup**.
2. Make sure that the **Enable configuration backup to the following repository** check box is selected.
3. From the **Backup repository** list, choose a backup repository on which the configuration backup must be stored.
4. In the **Restore points to keep** field, specify the number of restore points that you want to maintain in the backup repository.

5. Click **Schedule** next to the **Perform backup on** field and specify the time schedule according to which the configuration backup must be created.
6. Do not select "**Enable backup file encryption**".

   Note: Step 6 is skipped since the backup file encryption in the elevated configuration relies on the platform provided BitLocker.

Refer to the screenshot above.

Disabling and Deleting Jobs

See [User] Section **Backup > Managing Backup Jobs > Disabling and Deleting Jobs**

You can temporary disable scheduled jobs. The disabled job is paused for some period of time and is not run by the specified schedule. You can enable a disabled job at any time. You can also permanently delete a job from Veeam Backup & Replication and from the configuration database.

Disabling Job

To disable a job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the job and click **Disable** on the ribbon or right-click the job and select **Disable**.

To enable a disabled job, select it in the list and click **Disable** on the ribbon once again.

Trusted Update

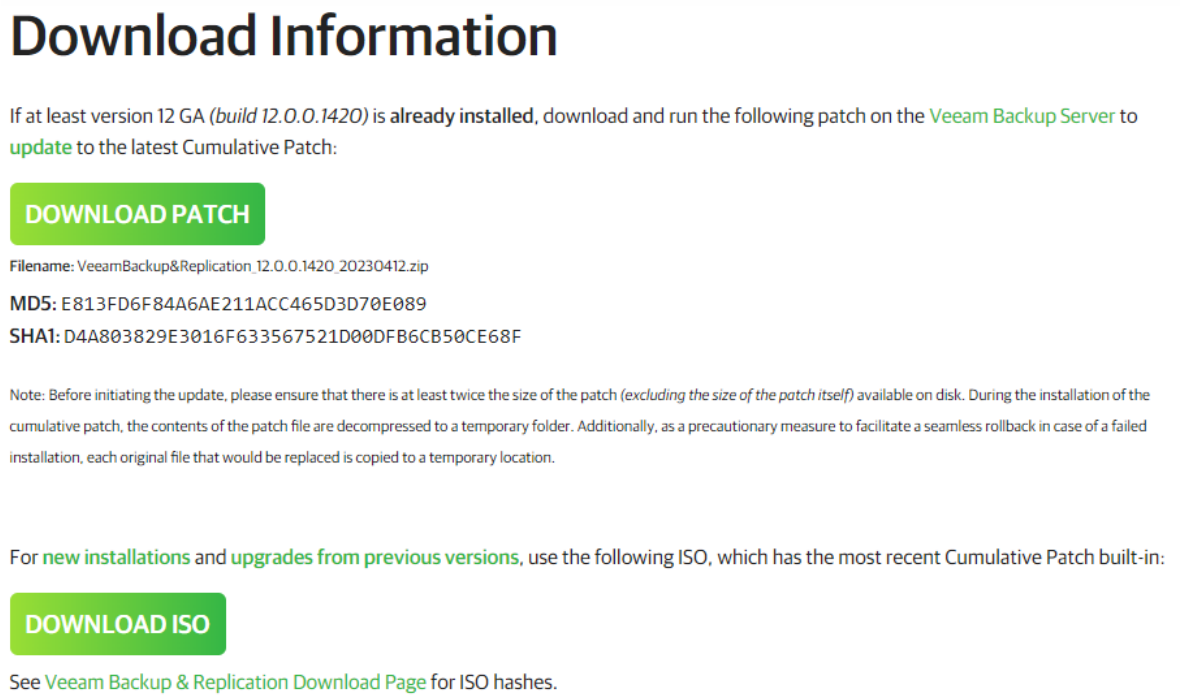
Performing Update

The TOE provides the ability for authorized administrators to check for available updates. The current version of the TOE is verified by selecting the Help menu and then selecting About.

Updates must be manually downloaded and installed. Because the TOE does not support a network interface, administrators are required to check and download updates from another system and then manually load the update on the TOE hosted system.

To install the latest update for Veeam Backup & Replication 12, perform the following steps:

1. Navigate to the Veeam KB article. https://www.veeam.com/kb4420.
   Compare the published latest version to that of the installed TOE. If the published version is later than the TOE version, proceed to download the latest cumulative patch.



Download Information

If at least version 12 GA *(build 12.0.0.1420)* is **already installed**, download and run the following patch on the Veeam Backup Server to update to the latest Cumulative Patch:

DOWNLOAD PATCH

Filename: VeeamBackup&Replication_12.0.0.1420_20230412.zip

MD5: E813FD6F84A6AE211ACC465D3D70E089

SHA1: D4A803829E3016F633567521D00DFB6CB50CE68F

Note: Before initiating the update, please ensure that there is at least twice the size of the patch *(excluding the size of the patch itself)* available on disk. During the installation of the cumulative patch, the contents of the patch file are decompressed to a temporary folder. Additionally, as a precautionary measure to facilitate a seamless rollback in case of a failed installation, each original file that would be replaced is copied to a temporary location.

For new installations and upgrades from previous versions, use the following ISO, which has the most recent Cumulative Patch built-in:

DOWNLOAD ISO

See Veeam Backup & Replication Download Page for ISO hashes.

2. In the **Download Information** section of the Veeam KB article, click **DOWNLOAD PATCH**.
3. Extract the executable file from the downloaded archive.
4. Copy the executable file onto the platform which the Veeam Backup and Replication v12 is installed.
5. Run the executable file to launch the update wizard.
6. In the update wizard, click **Next**, the click Install.

The Veeam VBR update package is signed by Veeam Software Group GmbH certificate, DigiCert is the Certificate Authority. Code is signed on the Veeam signing server during the build process.

The update package digital signature is verified by the Windows OS. The digital signature of the executable is also verified by the Windows platform. If something is wrong with the signature, Windows

displays a message with the issue and asks if the installation should proceed The administrator should terminate the installation.