© 2021 Veeam Software.

All rights reserved. All trademarks are the property of their respective owners.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means, without written permission from Veeam Software (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright, or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

**NOTE:**
Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.
Contents

CONTACTING VEEAM SOFTWARE ........................................................................................................ 6
ABOUT THIS DOCUMENT .................................................................................................................. 7
WELCOME TO VEEAM BACKUP FOR AWS ..................................................................................... 8
SYSTEM REQUIREMENTS .................................................................................................................. 9
LICENSING .......................................................................................................................................... 11
  Installing and Removing License ...................................................................................................... 12
  Viewing License Information ............................................................................................................ 14
  Revoking License Units ................................................................................................................... 15
ARCHITECTURE OVERVIEW ............................................................................................................. 16
DEPLOYMENT ....................................................................................................................................... 19
  Installing Veeam Backup for AWS .................................................................................................... 20
  After You Install .................................................................................................................................. 27
  Uninstalling Veeam Backup for AWS ................................................................................................. 28
ACCESSING VEEAM BACKUP FOR AWS .......................................................................................... 30
CONFIGURING VEEAM BACKUP FOR AWS ...................................................................................... 33
  Managing IAM Roles .......................................................................................................................... 34
    Adding IAM Roles ............................................................................................................................. 35
    Editing IAM Role Settings ................................................................................................................. 41
    Checking IAM Role Permissions ....................................................................................................... 42
    Removing IAM Roles ......................................................................................................................... 44
  Managing Permissions ........................................................................................................................ 45
    Adding User Accounts ....................................................................................................................... 47
    Editing User Account Settings ........................................................................................................... 48
    Changing User Passwords ................................................................................................................... 49
    Configuring Multi-Factor Authentication .......................................................................................... 50
  Managing S3 Repositories .................................................................................................................. 51
    Adding S3 Repositories ...................................................................................................................... 52
    Editing S3 Repository Settings .......................................................................................................... 58
    Removing S3 Repositories .................................................................................................................. 59
  Managing Worker Instances .............................................................................................................. 60
    Configuring Worker Instance Settings .............................................................................................. 61
    Testing File-Level Restore ................................................................................................................. 63
    Editing Worker Instance Settings ...................................................................................................... 64
  Configuring General Settings ............................................................................................................ 65
    Configuring Global Retention Settings .............................................................................................. 66
    Configuring Global Email Notification Settings ............................................................................... 68
Replacing Security Certificates ................................................................. 71
Changing Time Zone .................................................................................. 72
Configuring SSO Settings .......................................................................... 73

PERFORMING BACKUP ........................................................................... 75
How Backup Works .................................................................................. 76
Snapshot Chain ......................................................................................... 77
EC2 Backup Chain .................................................................................... 79
VPC Configuration Backup Chain .............................................................. 80
Retention Policy ........................................................................................ 81
Performing EC2 Instance Backup ............................................................... 85
Creating EC2 Backup Policies ................................................................. 86
Creating Snapshots Manually ................................................................. 113
Performing RDS Instance Backup ............................................................. 115
Creating RDS Backup Policies ............................................................... 116
Creating Snapshots Manually ................................................................. 133
Performing VPC Configuration Backup ................................................... 135
Editing VPC Configuration Backup Policy ............................................. 135
Enabling and Disabling VPC Configuration Backup Policy .................... 143
Starting and Stopping VPC Configuration Backup Policy ....................... 144
Managing EC2 and RDS Backup Policies ................................................ 145
Starting and Stopping Policies ............................................................... 145
Disabling and Enabling Policies ............................................................. 146
Setting Policy Priority ............................................................................... 147
Editing Policy Settings ............................................................................. 148
Exporting and Importing Policies ............................................................ 149
Managing Backed-Up Data ...................................................................... 151
Managing Backed-Up EC2 Instance Data ................................................ 151
Managing Backed-Up RDS Instance Data ................................................ 154
Managing Backed-Up VPC Configuration Data ....................................... 157

PERFORMING RESTORE ...................................................................... 174
EC2 Instance Restore ............................................................................... 174
Performing Entire EC2 Instance Restore ................................................ 174
Performing Volume-Level Restore ......................................................... 187
Performing File-Level Restore ............................................................... 201
RDS Instance Restore ............................................................................. 211
Step 1. Launch RDS Restore Wizard ....................................................... 212
Step 2. Select Restore Point .................................................................... 212
Step 3. Specify IAM Identity ................................................................... 214
Step 4. Choose Restore Mode ............................................................... 216
Contacting Veeam Software

At Veeam Software we value feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input and build products that incorporate your suggestions.

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up-to-date information on company contacts and office locations, visit the Veeam Contacts Webpage.

Online Support

If you have any questions about Veeam products, you can use the following resources:

- Full documentation set: www.veeam.com/documentation-guides-datasheets.html
- Veeam R&D Forums at forums.veeam.com
About This Document

This guide is intended for IT managers, cloud infrastructure administrators, and other personnel responsible for the product installation and operation.

The guide contains information on Veeam Backup for AWS configuration and provides a set of tasks that are required to perform data protection and disaster recovery operations.
Welcome to Veeam Backup for AWS

Veeam Backup for Amazon Web Services (Veeam Backup for AWS) is a solution developed for protection and disaster recovery tasks for Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Relational Database Service (Amazon RDS) environments. Veeam Backup for AWS also allows you to backup and restore Amazon Virtual Private Cloud (Amazon VPC) configuration.

With Veeam Backup for AWS, you can perform the following data protection operations:

- Create cloud-native snapshots of EC2 and RDS instances.
- Replicate cloud-native snapshots to any AWS Region within any AWS account.
- Create image-level backups of EC2 instances and keep them in Amazon Simple Storage Service (Amazon S3) for high availability, cost-effective and long-term storage.
- Create backup of your Amazon VPC configuration and keep it in the Veeam Backup for AWS database and in Amazon S3.

To recover backed-up data, you can perform the following operations:

- Restore the Amazon VPC configuration.
- Restore entire EC2 and RDS instances.
- Restore EC2 instance volumes.
- Restore EC2 instance files and folders.

Integration with Veeam Backup & Replication

AWS Plug-in for Veeam Backup & Replication extends the Veeam Backup & Replication functionality and allows you to add Veeam Backup for AWS appliances into the Veeam Backup & Replication infrastructure. With AWS Plug-in for Veeam Backup & Replication, you can manage data protection and recovery operations from the Veeam Backup & Replication console. For more information, see the Integration with Veeam Backup for AWS User Guide.
System Requirements

Before you start using Veeam Backup for AWS, consider the following requirements.

- **Network ports**
- **IAM role permissions**
- **AWS services**

Network Ports

The following network ports must be open to ensure proper communication of components in the Veeam Backup for AWS infrastructure.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browser (local machine)</td>
<td>Backup appliance</td>
<td>TCP</td>
<td>443</td>
<td>Required to access the Web UI component from a user workstation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSH</td>
<td>22</td>
<td>Required to communicate with the backup service running on the backup appliance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>11005</td>
<td>Default port required to communicate with the REST API service running on the backup appliance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>For information on how to change the port number, see the Configuring Security Settings section in the Veeam Backup for AWS REST API Reference.</td>
</tr>
<tr>
<td>Worker instance</td>
<td>TCP</td>
<td>443</td>
<td></td>
<td>Required to access the File Level Recovery for Veeam Backup browser running on a worker instance during the file-level restore process.</td>
</tr>
<tr>
<td>Backup appliance</td>
<td>SMTP server</td>
<td>TCP</td>
<td>25</td>
<td>Default port used for sending email notifications.</td>
</tr>
<tr>
<td></td>
<td>Veeam Update Notification Server (repository.veeam.com)</td>
<td>TCP</td>
<td>443</td>
<td>Required to download information on available product updates.</td>
</tr>
</tbody>
</table>

To open network ports, in the AWS Management Console, you must add inbound rules to security groups associated with Veeam Backup for AWS infrastructure components.

- A security group for the backup appliance is created during the product installation. For details, see Installing Veeam Backup for AWS.
A security group for worker instances is selected per AWS Region and Availability Zone. For details, see Configuring Worker Instance Settings.

For details on how to add inbound rules to security groups, see AWS Documentation.

IAM Role Permissions

IAM roles that Veeam Backup for AWS uses to perform data protection and disaster recovery operations must have permissions to access AWS services and resources. The minimal set of permissions for IAM roles is described in the following Veeam KB articles: KB3032, KB3033, KB3034.

AWS Services

The backup appliance and worker instances must have outbound internet access to the following AWS services:

- Amazon CloudWatch
- Amazon CloudWatch Events
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Kinesis Data Streams
- Amazon Relational Database Service (RDS)
- Amazon Simple Notification Service (SNS)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Marketplace Metering Service
- AWS Resource Access Manager
- AWS Security Token Service (STS)
- AWS Service Quotas
- AWS Systems Manager (SSM), including access to the ec2messages and ssmmessages endpoints
- Elastic Load Balancing (ELB)
Licensing

Veeam Backup for AWS is licensed per protected instance. An instance is considered to be protected if it has a restore point (snapshot or backup) created by a backup policy during the past 31 days. Each protected instance consumes 1 license unit. However, if an instance has only manually created snapshots, it does not consume any license units.

Product Editions

Veeam Backup for AWS is available in 3 editions:

- **Free**
  Veeam Backup for AWS operating in the *Free* edition allows you to protect up to 10 instances free of charge.

- **Paid**
  Veeam Backup for AWS operating in the *Paid* edition allows you to protect an unlimited number of instances.

  In the *Paid* edition of the product, you are charged by AWS for instances that you actually protect. To track data protection operations on the backup appliance, Veeam Backup for AWS uses the AWS Marketplace Metering Service. Every hour, the backup server sends information on the current number of protected instances to AWS. The price for protected instances is included into the monthly AWS Cost and Usage report.

- **BYOL (Bring Your Own License)**
  Veeam Backup for AWS operating in the *BYOL* edition allows you to use a Veeam Backup for AWS license with a certain number of license units to protect instances.

  For details on how to obtain the license, contact a Veeam sales representative at Sales Inquiry. For details on how to install the license on the backup appliance, see Installing and Removing License. Note that if the license is not installed, Veeam Backup for AWS operates in the *Free* edition allowing you to protect up to 10 instances free of charge.

**TIP**

If you previously used the *Free* edition of the product for evaluation and testing purposes and want to switch to any of the commercial editions without reconfiguring the backup infrastructure, follow the steps described in this Veeam KB article.
Installing and Removing License

NOTE
This section applies only to the BYOL edition of Veeam Backup for AWS.

To install a Veeam Backup for AWS license on the backup appliance:

1. Switch to the Configuration page.
2. Navigate to Licensing > License Info.
3. Click Install License.
4. In the Upload file window, click Browse to browse to a license file, and then click Upload.

Veeam Backup for AWS will upload the license file from the local machine and install it on the backup appliance.
Removing License

You can remove an installed license if necessary.

To remove a license:

1. On the License Info tab, click Remove License.
2. In the Remove License window, click Yes to confirm that you want to remove the license.

After you remove the license, Veeam Backup for AWS will automatically switch back to the Free edition. In this case, according to the FIFO (first-in first-out) queue, only the first 10 instances registered in the configuration database will remain protected. You can revoke license units from these instances as described in section Revoking License Units.

Related Topics

Viewing License Information
Viewing License Information

To view details on the license that is currently installed on the backup appliance, do the following:

1. Switch to the Configuration page.

The licensing section provides the general information on the Veeam Backup for AWS license:

- **Status** — the license status. The status depends on the license edition, the number of days remaining until license expiration and the number of days remaining in the grace period (if any).

- **Instances** — the total number of protected instances that consume license units.
  
  Each instance that has a restore point created in the past 31 days is considered to be protected and consumes 1 license unit. To view the list of instances that consume license units, switch to the License Usage tab.

- **Expiration Date** — the date when the license will expire.

- **License Type** — the license edition (Free, BYOL).

- **License ID** — the unique identification number of the provided license file (required for contacting the Veeam Customer Support Team).

- **Licensed To** — the name of an organization to which the license was issued.

- **Support ID** — the unique identification number of the support contract (required for contacting the Veeam Customer Support Team).

![License Information Screen](image)

**Related Topics**

- **Installing and Removing License**
- **Revoking License Units**
Revoking License Units

By default, Veeam Backup for AWS automatically revokes a license unit from a protected instance if no new restore points have been created by the backup policy during the past 31 days. However, you can manually revoke license units from protected instances — this can be helpful, for example, if you remove a number of instances from a backup policy and do not want to protect them anymore.

To revoke a license unit from a protected instance, do the following:

1. Switch to the Configuration page.
2. Navigate to Licensing > License Usage.
3. Select the instance that you no longer want to protect.
4. Click Revoke License.
5. In the Revoke License window, click Yes to confirm that you want to revoke the license unit.
Architecture Overview

The Veeam Backup for AWS infrastructure includes the following components:

- **Backup appliance**
- **S3 repositories**
- **Worker instances**

Backup Appliance

The backup appliance is a Linux-based EC2 instance where Veeam Backup for AWS is installed. The backup appliance performs the following administrative activities:

- Manages infrastructure components.
- Coordinates snapshot creation, backup and recovery tasks.
- Controls backup policy scheduling.

Backup Appliance Components

The backup appliance uses the following components:

- **Backup service** — coordinates data protection and disaster recovery operations.
- **Configuration database** — stores data collected for the Veeam Backup for AWS infrastructure, backup policies, sessions and so on.
- **Web UI** — provides a web interface that allows user access to the Veeam Backup for AWS functionality.
- **Updater service** — allows to check, view and install product and package updates.
- **REST API service** — allows to perform operations with Veeam Backup for AWS entities using HTTPS requests and standard HTTP methods. For details, see the Veeam Backup for AWS REST API Reference.

To access AWS services and resources, the backup appliance uses AWS API.
S3 Repositories

An S3 repository is a folder in an Amazon S3 bucket where Veeam Backup for AWS stores image-level backups of EC2 instances and additional copies of the Amazon VPC configuration. For details on Veeam Backup for AWS communication with S3 repositories, see S3 Repositories.

Encryption on S3 Repositories

For enhanced data security, Veeam Backup for AWS allows you to enable encryption at the S3 repository level. For details, see S3 Repository Encryption. For information on how to enable encryption at the S3 repository level, see Adding S3 Repositories.

Veeam Backup for AWS also supports scenarios where data is backed up to S3 buckets with enabled Amazon S3 default encryption. You can add the S3 bucket to the backup infrastructure as an S3 repository and use it as a target for image-level backups. For information on Amazon S3 default encryption, see AWS Documentation.

Limitations for S3 Repositories

Before you add an S3 repository to the Veeam Backup for AWS configuration database, consider the following limitations:

- Veeam Backup for AWS allows you to store backups only in the S3 Standard storage class. S3 Standard-IA, S3 One Zone-IA and S3 Glacier storage classes are not supported.
- S3 buckets with S3 Object Lock enabled are not supported.

Worker Instances

A worker instance is a Linux-based EC2 instance that is responsible for the interaction between the backup appliance and other components of the Veeam Backup for AWS infrastructure. Worker instances process backup workload and distribute backup traffic when transferring data to S3 repositories.

Veeam Backup for AWS automatically launches a worker instance in Amazon EC2 for the duration of a backup or restore process and removes it immediately after the process is complete. For each AWS Region where worker instances will be launched, you can configure network settings — specify the Amazon VPC, subnet, and security group to which worker instances must be connected. If worker settings are not configured for an AWS Region, Veeam Backup for AWS will get the default settings of the AWS Region to launch worker instances and to perform data protection and disaster recovery operations.

Veeam Backup for AWS launches one worker instance per each EC2 instance specified in a backup policy or restore task. For data protection operations, the type of the worker instance is selected automatically based on the size of the largest EBS volume attached to the processed EC2 instance. For data recovery operations, Veeam Backup for AWS launches worker instances of the following type:

- c5.large — for EC2 instance restore and volume-level restore if the size of the largest EBS volume is less than 1024 GB
- c5.xlarge — for EC2 instance restore and volume-level restore if the size of the largest EBS volume is from 1024 GB to 1250 GB
- c5.2xlarge — for EC2 instance restore and volume-level restore if the size of the largest EBS volume is more than 1250 GB
- t2.medium — for file-level restore
To minimize cross-region traffic charges, depending on the data protection and disaster recovery operation, Veeam Backup for AWS launches a worker instance in the following location:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Worker Instance Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating image-level backups</td>
<td>AWS Region in which a processed EC2 instance resides</td>
</tr>
<tr>
<td>EC2 instance restore</td>
<td>AWS Region to which an EC2 instance is restored</td>
</tr>
<tr>
<td>Volume-level restore</td>
<td>AWS Region to which EC2 instance volumes are restored</td>
</tr>
<tr>
<td>File-level restore from cloud-native snapshots or snapshot replicas</td>
<td>AWS Region in which an original EC2 instance resides</td>
</tr>
<tr>
<td>File-level restore from image-level backups</td>
<td>AWS Region in which an S3 repository with backed-up data resides</td>
</tr>
</tbody>
</table>

**Worker Instance Components**

A worker instance uses the following components:

- **Veeam Data Mover** is a component that performs data processing tasks. During backup, the Veeam Data Mover retrieves EC2 instance data from snapshots and stores the retrieved data to S3 repositories. During restore, the Veeam Data Mover transfers backed-up data from S3 repositories to the target location.

- **File Level Recovery for Veeam Backup (FLR for Veeam Backup) browser** is a web service that allows you to find and save files and folders of a backed-up EC2 instance to the local machine. The FLR for Veeam Backup browser is installed automatically on worker instances that are launched for file-level restore.

**Security Certificates for Worker Instances**

Veeam Backup for AWS uses self-signed TLS certificates to establish secure communication between the web browser on the local machine and the FLR for Veeam Backup browser on the worker instance during file-level restore. A self-signed certificate is generated automatically on the worker instance when the restore session starts.
Deployment

Veeam Backup for AWS comes as an image of a Linux-based EC2 instance that you can deploy from AWS Marketplace. To install Veeam Backup for AWS, you must first configure installation settings in AWS Marketplace and then perform the initial configuration in the Veeam Backup for AWS Web UI.
Installing Veeam Backup for AWS

Veeam Backup for AWS is installed on a single EC2 instance. The EC2 instance is created during the product installation.

To install Veeam Backup for AWS:

1. Log in to AWS Marketplace using credentials of an AWS account in which you plan to install Veeam Backup for AWS.

You can install Veeam Backup for AWS in the production site — in the AWS account where resources that you plan to back up reside. It is recommended, however, that you use a separate AWS account for Veeam Backup for AWS installation. In this case, if a disaster strikes on the production site, you will still be able to access Veeam Backup for AWS and perform recovery operations.

2. Open the Veeam Backup for AWS overview page for the necessary product edition.
   - Veeam Backup for AWS Free Edition
   - Veeam Backup for AWS Paid Edition
   - Veeam Backup for AWS BYOL Edition

For more information on product editions, see Licensing.

3. Click Continue to Subscribe.

   ![Veeam Backup for AWS Paid Edition](image)

   **Product Overview**

   Veeam Backup for AWS delivers native, fully automated AWS backup and disaster recovery to effortlessly protect and manage Amazon EC2 and Amazon RDS data. Built with cost-effectiveness, security and scalability in mind, you can eliminate the risk of data loss for all your AWS data while saving big through:
   - Policy-based automation of AWS-native snapshots, backups and replicas, providing simple yet flexible protection of Amazon EC2 and Amazon RDS data, even at scale.
   - Lightning-fast recoveries in as little as seconds from entire instances, volumes, databases and VPCs to individual files and folders.
   - Cloud cost control with industry-first backup cost calculation to avoid unexpected expenses, charged block tracking and tiering to Amazon S3 for long-term retention and compliance.
   - Ransomware and cybersecurity protection, isolating backup data from production through cross-account and cross-region backup.
   
   Latest release features Amazon RDS backup, Amazon VPC backup, role-based access control, enhanced application consistency and more!

   The AMI takes just minutes to set up - see how here:
   - Deployment: https://youtu.be/pwr5FXfLDQ
   - Configuration: https://youtu.be/qlv5uAvOLxY

4. On the Subscribe to this software page, under Terms and Conditions, click Show Details.
5. Click **End User License Agreement** to view the product license agreement.

6. Click **Continue to Configuration**.
7. At the **Configure this software** page, configure installation settings:
   a. From the **Delivery Method** drop-down list, choose whether you want to connect the EC2 instance running Veeam Backup for AWS to an existing Amazon VPC and subnet, or to create a new Amazon VPC and subnet for the instance.
      - **VB for AWS Deployment - Existing VPC** — select this option if you want to use an existing Amazon VPC and subnet.
      - **VB for AWS Deployment - New VPC** — select this option if you want to create a new Amazon VPC and subnet.
   
      For details on Amazon VPCs and subnets, see [AWS Documentation](https://aws.amazon.com/documentation/vpc/).
   b. From the **Software Version** drop-down list, select the latest version of Veeam Backup for AWS.
   c. From the **Region** drop-down list, select an AWS Region in which an EC2 instance running Veeam Backup for AWS will reside.
      
      For more information on AWS Regions, see [AWS Documentation](https://aws.amazon.com/documentation/regions/).

8. Click **Continue to Launch**.

9. On the **Launch this software** page, do the following:
   a. In the **Configuration Details** section, review the product installation settings.
      
      To view information on how to access Veeam Backup for AWS, click **Usage Instructions**.
   b. From the **Choose Action** drop-down list, select **Launch CloudFormation**.
   c. Click **Launch** to launch the **Create stack** wizard.
      
      Veeam Backup for AWS is installed using AWS CloudFormation stacks. In AWS CloudFormation, a stack is a collection of AWS services and resources that you can manage as a single unit. You can create a stack in an AWS account, use resources included in the stack to run an application, or delete a stack if you no longer need it. For more information on AWS CloudFormation stacks, see [AWS Documentation](https://aws.amazon.com/documentation/cloudformation/).
In the **Create stack** wizard, you will create a stack for Veeam Backup for AWS.

10. At the **Specify template** step of the wizard, the stack template settings are preconfigured by Veeam Backup for AWS and cannot be changed.
11. At the **Specify stack details** step of the wizard, configure stack settings.

   a. In the **Stack name** field, specify a name for the created stack.

   ![Stack name](image)

   - **Stack name** field:
     - dept-01-vbaws-srv
     - Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

   b. In the **Instance Configuration** section:

      i. Select the EC2 instance type for the backup appliance.
         - The recommended EC2 instance type is `t2.medium`.

      ii. Select a key pair that will be used to authenticate against the backup appliance. For a key pair to be displayed in the **Key pair for Veeam Backup for AWS server** list, it must be created in the Amazon EC2 console. To learn how to create key pairs, see [AWS Documentation](https://aws.amazon.com/documentation).  

   ![Instance Configuration](image)

   - **Instance type for Veeam Backup for AWS server**:
     - `t2.medium`

   - **Key pair for Veeam Backup for AWS server**:
     - Select one, or create a new one at AWS console:
     - `dev_lab`  

   c. In the **Network Configuration** section:

      i. Select `true` if you want to create an Elastic IP address for the backup appliance.
         - For more information on Elastic IP addresses, see [AWS Documentation](https://aws.amazon.com/documentation).

      ii. Specify the IPv4 address range from which Veeam Backup for AWS Web UI will be accessible.
         - Make sure the IPv4 address of the local machine from which you plan to access Veeam Backup for AWS lies within the specified IPv4 range.
         
         The IPv4 address range is specified in the CIDR notation (for example, `12.23.34.0/24`). To let all IPv4 addresses access Veeam Backup for AWS, you can specify `0.0.0.0/0`. Note that allowing access from all IPv4 addresses is unsafe and thus not recommended in production environments.

         Based on the specified IPv4 range, AWS CloudFormation will create a security group for Veeam Backup for AWS with the inbound rule for HTTPS traffic. By default, port 443 is open for inbound HTTPS traffic. If you plan to change the security group for Veeam Backup for AWS upon the product installation, you will need to manually add inbound rules to the new security group and make sure this security group allows access to AWS services listed in the **Requirements** section.

   ![Network Configuration](image)

   - **Create elastic IP for Veeam Backup for AWS server?**
     - `true`

   - **Allowed source IP addresses for connection to HTTPS**
     - The IP address range in CIDR format (e.g. `12.23.34.0/24`) from which Veeam Backup for AWS Management portal will be accessible:
     - `12.23.34.0/24`
d. In the **VPC and Subnet** section, specify an Amazon VPC and subnet to which the backup appliance will be connected.

Depending on the option selected at step 7a, you can either select an existing Amazon VPC and subnet, or specify IPv4 address ranges in the CIDR notation for a new Amazon VPC and subnet.

**IMPORTANT**

Consider the following:

- The specified Amazon VPC and subnet must have the outbound internet access to AWS services listed in the **Requirements** section. Otherwise, Veeam Backup for AWS may not work efficiently and may cause unexpected errors.

- The specified Amazon VPC and subnet must allow the inbound internet access from the local machine that you plan to use to work with Veeam Backup for AWS.

To learn how to enable internet access for Amazon VPCs and subnets, see [AWS Documentation](https://aws.amazon.com/documentation/)

> **VPC and Subnet**
> **VPC CIDR**
> Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block, for example, 172.28.0.0/16. You cannot specify an IPv4 CIDR block larger than /16.
> 172.28.0.0/16

> **Subnet CIDR**
> Primary Public Subnet CIDR (Must be within VPC CIDR range).
> 172.28.0.0/20

12. At the **Configure stack options** step of the wizard, specify AWS tags, IAM role permissions and other additional settings for the stack.

For more information on available stack options, see [AWS Documentation](https://aws.amazon.com/documentation/)
13. At the **Review** step of the wizard, do the following:

a. Review the configured settings.

b. Select the **I acknowledge that AWS CloudFormation might create IAM resources** check box.

c. Click **Create stack**.

**What You Do Next**

Right after installation, you must perform the initial configuration of Veeam Backup for AWS. For details, see **After You Install**.
After You Install

To start working with Veeam Backup for AWS, you must perform the initial configuration of the backup appliance:

**IMPORTANT**

To access Veeam Backup for AWS, you can use the following web browsers: Microsoft Edge 40 or later, Mozilla Firefox 56 or later, Google Chrome 62 or later.

1. In a web browser, navigate to the Veeam Backup for AWS web address.
   
   The address consists of a public IPv4 address or DNS hostname of the backup appliance. Note that the website is available over HTTPS only.

2. Read and accept both the Veeam license agreement and the 3rd party components license agreement. If you reject the agreements, you will not be able to continue installation.
   
   To read the terms of the license agreement for the 3rd party components, click 3rd party components license agreement.

3. In the **Instance ID** field, specify the AWS ID of the EC2 instance running Veeam Backup for AWS to prove that you are the owner of this EC2 instance.
   
   You can find the EC2 instance AWS ID in the AWS Management Console.

4. Create the Default Administrator account whose credentials you will use for your first login to Veeam Backup for AWS.
   
   Veeam Backup for AWS will create the Default Administrator account and display the welcome screen where you can log in.

**NOTE**

To increase the security of the Default Administrator account, it is recommended that you enable multi-factor authentication (MFA) for the account after you first log in to Veeam Backup for AWS. To learn how to enable MFA, see Configuring Multi-Factor Authentication.
Uninstalling Veeam Backup for AWS

Veeam Backup for AWS is installed using an AWS CloudFormation stack. In AWS CloudFormation, a stack is a collection of AWS services and resources that you can manage as a single unit. To uninstall Veeam Backup for AWS, you must delete the CloudFormation stack from your AWS infrastructure. For more information on working with stacks, see AWS Documentation.

Note that backed-up data will not be removed automatically after you uninstall the solution. You can keep this data in your AWS environment and import it to a new backup appliance:

- To import cloud-native snapshots, rescan AWS Regions where the snapshots are stored. The snapshots will be automatically imported to the configuration database.
- To import image-level backups, assign the Amazon S3 bucket where the backups are stored to a new S3 repository as described in section Adding S3 Repositories.

If you do not want to keep the backed-up data, remove it manually as described in section Managing Backed-Up Data. Alternatively, you can remove the data using the AWS Management Console.

Deleting CloudFormation Stack

IMPORTANT

When you deploy Veeam Backup for AWS from the Veeam Backup & Replication console, the CloudFormation stack is not created and AWS resources cannot be managed as a single unit. Keep in mind that these resources are not automatically deleted from AWS when you remove the backup appliance from the Veeam Backup & Replication infrastructure. To learn how to manually delete resources created during Veeam Backup for AWS installation, see the Integration with Veeam Backup for AWS Guide, section Removing Appliances.

To delete the Veeam Backup for AWS CloudFormation stack, do the following:

1. Log in to the AWS Management Console using credentials of an AWS account where Veeam Backup for AWS is installed.
2. From the list of available AWS Regions in the upper-right corner of the page, select the AWS Region in which the backup appliance resides.
3. Navigate to Services > CloudFormation.
4. From the Stacks list, select the CloudFormation stack created while installing Veeam Backup for AWS.
5. Click Delete.
6. In the confirmation window, click Delete stack to acknowledge deletion.

NOTE

After you acknowledge the operation, the Veeam Backup for AWS CloudFormation stack will acquire the DELETE_IN_PROGRESS state. When all AWS resources included in the stack are successfully deleted, the stack will acquire the DELETE_COMPLETE state. By default, deleted CloudFormation stacks are not displayed in the AWS Management Console. To learn how to view deleted stacks and to troubleshoot deletion issues, see AWS Documentation.
Removing Backed-Up Data

If you no longer need the backed-up data, you can remove it manually from the AWS infrastructure:

1. Log in to the **AWS Management Console** using credentials of an AWS account where the data is stored.

2. From the list of available AWS Regions in the upper-right corner of the page, select the AWS Region in which the backed-up data is stored.

3. Remove the backed-up data:
   - To remove backups, navigate to **Services > S3**. Select an Amazon S3 bucket where the backups are stored. Navigate to **Veeam > Backup**, select the S3 repository folder, and click **Delete**.
   - To remove RDS cloud-native snapshots, navigate to **Services > RDS > Snapshots**, select the necessary Veeam snapshots, and click **Delete**.
   - To remove EC2 cloud-native snapshots, navigate to **Services > EC2 > Snapshots**, select the necessary Veeam snapshots, and click **Delete**.
Accessing Veeam Backup for AWS

To access Veeam Backup for AWS, in a web browser, navigate to the Veeam Backup for AWS web address. The address consists of a public IPv4 address or DNS hostname of the backup appliance. Note that the website is available over HTTPS only.

**IMPORTANT**

Internet Explorer is not supported. To access Veeam Backup for AWS, use Microsoft Edge (version 40 or later), Mozilla Firefox (version 56 or later) or Google Chrome (version 62 or later).

You can access Veeam Backup for AWS using credentials of VB for AWS user account or single sign-on (SSO) authentication. To learn how to configure SSO, see Configuring SSO Settings.

**NOTE**

The web browser may display a warning notifying that the connection is untrusted. To eliminate the warning, you can replace the TLS certificate that is currently used to secure traffic between the browser and the backup appliance with a trusted TLS certificate. To learn how to replace certificates, see Replacing Security Certificates.
Logging In Using Veeam Backup for AWS User Account

To log in using credentials of a Veeam Backup for AWS user account, do the following:

1. In the **Username** and **Password** fields, specify credentials of the Veeam Backup for AWS user account.
   
   If you log in for the first time, use credentials of the Default Administrator that was created after the product installation. You can add other user accounts to Veeam Backup for AWS. For more information, see [Managing Permissions](#).
   
   If you forgot the user password, you can reset it. To do that, click the **Forgot password?** link and follow the instructions provided in [this Veeam KB article](#).

2. Select the **Keep me logged in** to save the specified credentials in a persistent browser cookie.
   
   With this option enabled, you will not need to provide credentials when you access Veeam Backup for AWS in a new browser session.

3. Click **Log in**.
   
   If multi-factor authentication (MFA) is enabled for the user, Veeam Backup for AWS will prompt you to enter a code to verify the user identity. In the **Verification code** field, enter the temporary six-digit code generated by the authentication application running on your trusted device. Then, click **Log in**.
Logging In Using SSO

To log in using SSO authentication scheme, do the following:

1. Click **Use Single Sign-On**. You will be redirected to your identity provider portal.
2. If you have not logged in yet, log in to the identity provider portal. You will be redirected to the Veeam Backup for AWS Overview page as the authorized user.

Logging Out

To log out, at the top right corner of the Veeam Backup for AWS window, click the user name and then click **Log Out**.
Configuring Veeam Backup for AWS

To start working with Veeam Backup for AWS, perform a number of steps for its configuration:

1. **Add IAM roles to access AWS services and resources.**
2. **Add user accounts to control access to Veeam Backup for AWS.**
3. **Configure S3 repositories.**
   - This step applies if you plan to protect EC2 instances with image-level backups and to keep an additional copy of the Amazon VPC configuration backup in Amazon S3.
4. **Configure network settings for worker instances.**
   - If you do not configure settings for worker instances, Veeam Backup for AWS will use the default settings of an AWS Region where worker instances will be launched.
5. **Configure global retention, email notification and single-sign-on settings.**

**NOTE**

Even after you add IAM roles that manage your AWS resources and configure all the necessary settings, Veeam Backup for AWS will not populate the list of instances on the **Instances** page — unless you create backup policies and specify the regions where the instances belong, as described in section **Performing Backup.**
Managing IAM Roles

For each data protection and disaster recovery operation in Veeam Backup for AWS, you must specify an IAM role. Veeam Backup for AWS uses permissions of the specified IAM role to access AWS services and resources, and to perform the necessary operation.

For example, Veeam Backup for AWS requires access to the following AWS resources:

- **EC2 resources** — to display the list of EC2 instances in backup policy settings, to create cloud-native snapshots, snapshot replicas, to launch worker instances and to restore backed-up data.

- **S3 resources** — to store backed-up data to S3 repositories, to perform transform operations with backup chains, and to copy backed-up data from S3 repositories to worker instances during restore.

If you plan to back up and restore data within the initial AWS account, you can use the Default Backup Restore IAM role that is added to Veeam Backup for AWS upon the product installation. If you plan to protect data of another AWS account, or keep backed-up data in another AWS account, you must add IAM roles that have permissions to access AWS services and resources of that account.

To specify an IAM role for the necessary operation, you must first add this IAM role to Veeam Backup for AWS. You can add IAM roles that already exist in your AWS accounts, or instruct Veeam Backup for AWS to create and add IAM roles with predefined permission sets. To learn how to create and add IAM roles in Veeam Backup for AWS, see Adding IAM Roles.

**NOTE**

To grant an IAM role permissions on required AWS services and resources, in the IAM Management Console, you must create an IAM policy in the JSON format, and then attach it to the IAM role that you plan to use in Veeam Backup for AWS. Policy examples are described in these Veeam KB articles: KB3032, KB3033, KB3034.

Default Backup Restore IAM Role

Veeam Backup for AWS comes with the predefined Default Backup Restore IAM role. This IAM role has all the required permissions to perform operations within the initial AWS account — back up any instance or VPC within the account, store backups in any Amazon S3 bucket within the account, and so on.

You do not need to add the Default Backup Restore IAM to Veeam Backup for AWS. This role is created in the initial AWS account and added to Veeam Backup for AWS automatically upon the product installation.

Related Resources

This section assumes that you have a good understanding of IAM Roles, Creating IAM Policies and Adding and Removing IAM Identity Permissions.
Adding IAM Roles

To add an IAM role to Veeam Backup for AWS, complete the following steps:

1. Launch the Add IAM Role wizard.
2. Specify a name and description for the IAM role.
4. Finish working with the wizard.
Step 1. Launch Add Account Wizard

To launch the **Add IAM Role** wizard, complete the following steps:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts > IAM Roles**.
3. Click **Add**.

Step 2. Specify IAM Role Name and Description

At the **Role Name** step of the wizard, specify a name and description for the IAM role. The specified name and description will be displayed to Veeam Backup for AWS users on the **IAM Roles** tab of the **Accounts** view.

Consider the following limitations:

- An IAM role name must be unique in Veeam Backup for AWS. The length of the name must not exceed 255 characters.
- The length of a description must not exceed 512 characters.
Step 3. Specify IAM Role Type and Settings

At the Role Settings step of the wizard, choose to add an already existing IAM role, or create a new IAM role and add it to Veeam Backup for AWS.

- **IAM Role from current account** — select this option if you want to add an IAM role that has permissions on resources of the initial AWS account.

- **IAM Role from another account** — select this option if you want to add a cross-account IAM role that has permissions on resources of another AWS account.
  
  A cross-account IAM role in AWS is used to provide IAM users in the initial AWS account (trusted account) access to resources in another AWS account (trusting account). For details, see AWS Documentation.

- **Create a new IAM Role** — select this option if you want to create a new IAM role and add it to Veeam Backup for AWS.

Then specify the IAM role settings for the chosen IAM role type:

- Specifying settings for an IAM role from the initial AWS account.
- Specifying settings for a cross-account IAM from another account.
- Specifying settings for a new IAM role.

Specifying Settings for IAM Role

[This step applies if you selected the **IAM Role from current account** option]

At the Role Settings step of the wizard, specify the name of the IAM role that you want to add. You must specify the name that the IAM role has in AWS.

**NOTE**

If the IAM role was created with a path, you must specify the complete path and the name of the IAM role. For example, `dept_1/s3_role`.

Specifying Settings for Cross-Account IAM Role

[This step applies if you selected the **IAM Role from another account** option]
At the **Role Settings** step of the wizard, specify the following settings:

1. In the **Account ID** field, specify the 12-digit number (or alias) of a trusting account.
   
   The trusting account is an AWS account that owns AWS services and resources, and shares them with the initial AWS account (trusted account). To learn how to delegate access across AWS accounts, see [AWS Documentation](https://docs.aws.amazon.com/).  

2. In the **AWS Role Name** field, specify the name of the cross-account IAM role that you want to add. You must specify the name that the IAM role has in AWS.
   
   The cross-account IAM role is created in the trusting account and allows the trusting account to share AWS services and resources with the trusted account.

   **NOTE**
   
   If the cross-account IAM role was created with a path, you must specify a complete path and a name. For example, `dept_1/s3_role`.

3. In the **External ID** field, specify an external ID of the cross-account IAM role.
   
   The external ID is a property in the trust policy of the cross-account IAM role used for enhanced security. For more information, see [AWS Documentation](https://docs.aws.amazon.com/).

---

### Specifying Settings for New IAM Role

[This step applies if you selected the **Create a new IAM Role** option]

At the **Role Settings** step of the wizard, specify the following settings:

1. In the **AWS Role Name** field, specify a name for the IAM role. The IAM role will be created with the specified name in AWS.

   **NOTE**
   
   Consider the following limitations:
   
   - An AWS name of the IAM role must be unique within one AWS Account.
   - The following characters are not supported: `/ " ' [ ] : | < > ; ? * & .
   - The length of the name must not exceed 63 characters.

   For more information on limitations for an IAM role name, see [AWS Documentation](https://docs.aws.amazon.com/).
2. **Under Grant the following permissions**, select check boxes next to permission sets that must be granted to the IAM role:

   - **Service Role** — select this check box to grant permissions sufficient to launch worker instances.
   - **Policy Role** — select this check box to grant permissions sufficient to perform backup.
     
     The IAM role with this permission set will allow you to back up any instance or VPC configuration within the AWS account.
   - **Repository Role** — select this check box to grant permissions sufficient to add Amazon S3 buckets as S3 repositories.
     
     The IAM role with this permission set will allow you to add as an S3 repository any Amazon S3 bucket within the AWS account.

     If you want the IAM role to have granular permissions, do not select check boxes (for example, you may want the IAM role to have permissions only on specific EC2 instances). In this case, after the IAM role is created, you can grant the necessary permissions to it in the IAM Management Console. To learn how to gran permissions to an IAM role, see AWS Documentation.

3. Provide one-time access keys of an IAM user that is authorized to create IAM roles in an AWS account.

   The specified access keys determine in which AWS account the role will be created. For example, if you specify access keys of an IAM user from the initial AWS account, the IAM role will be created in the initial AWS account and will have permissions on AWS services and resources of the initial account.

   **NOTE**

   Veeam Backup for AWS does not store one-time access keys in the configuration database.
Step 4. Finish Working with Wizard

At the Summary step of the wizard, review summary information and click Finish.
Editing IAM Role Settings

For each IAM role added to Veeam Backup for AWS, you can modify the IAM role settings:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts > IAM Roles**.
3. Select the check box next to an IAM role whose settings you want to edit.
4. Click **Edit**.
5. Complete the **Edit IAM Role** wizard.
   a. To provide a new name and description for the IAM role, follow the instructions provided in section **Adding IAM Roles** (step 2).
   b. To edit the IAM role settings, follow the instructions provided in section **Adding IAM Roles** (step 3).
   c. At the **Summary** step of the wizard, review summary information and click **Finish**.
Checking IAM Role Permissions

You can check whether permissions of an IAM role are sufficient to perform a data protection or disaster recovery operation for which the IAM role is specified.

It is recommended that you run the IAM role permission check before you perform any operation to avoid the operation failure. For example, after you specify an IAM role in worker instance settings, you can check whether permissions of this IAM are sufficient to launch worker instances. You can also run the permission check if you made changes in your AWS account and want to ensure that permissions granted to the IAM role remain sufficient.

To run the permission check for an IAM role, do the following:

1. Switch to the Configuration page.
2. Navigate to Accounts > IAM Roles.
3. Select an IAM role and click Check AWS permissions.

Veeam Backup for AWS will display the AWS Permission Check for IAM Role window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient, the check will complete with errors. You can view the list of permissions that must be granted to the IAM role in the Missing Permissions column.

You can grant the missing permissions to the IAM role in the IAM Management Console or instruct Veeam Backup for AWS to do it. To learn how to grant permissions to an IAM Role using the IAM Management Console, see AWS Documentation.

To let Veeam Backup for AWS grant the missing permissions:

1. In the AWS Permission Check for IAM Role window, click Grant.
2. In the Grant permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of the IAM role, and then click Apply.

NOTE

Veeam Backup for AWS does not store one-time access keys in the configuration database.
3. To make sure that the missing permissions were successfully granted, click **Recheck**.
Removing IAM Roles

You can remove IAM roles from Veeam Backup for AWS. For example, you may want to remove an IAM role if it is no longer used to perform data protection and disaster recovery operations.

**IMPORTANT**

You cannot remove an IAM role that is still used to get an access to AWS resources or is specified in backup policy settings.

To remove an IAM role, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts > IAM Roles**.
3. Select the IAM role and click **Remove**.
4. In the **Confirmation** window, click **Yes** to acknowledge the operation.
Managing Permissions

Veeam Backup for AWS controls access to its functionality with the help of user roles. A role defines what operations users can perform and what range of data is available to them in the Veeam Backup for AWS UI.

There are 3 user roles that you can assign to users working with Veeam Backup for AWS. Actions a user can perform depend on the role.

- **Portal Administrator** — can perform all configuration actions and can also act as a Portal Operator and Restore Operator.
- **Portal Operator** — can create and manage backup policies, manage the protected data and perform all restore operations.
- **Restore Operator** — can only perform restore operations.

The following table describes the functionality available to users with different roles in the Veeam Backup for AWS UI.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Functionality</th>
<th>Portal Administrator</th>
<th>Portal Operator</th>
<th>Restore Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
<td>Dashboard</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td><strong>Instances</strong></td>
<td>Infrastructure</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Policies</strong></td>
<td>Backup policies</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Protected Data</strong></td>
<td>Restore</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>File-level restore</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>Remove</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Session Log</strong></td>
<td>Session log</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>Stop session execution</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Configuration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Accounts</strong></td>
<td>IAM roles, SMTP accounts, Portal Users</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Repositories</strong></td>
<td>S3 repositories</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Workers</strong></td>
<td>Worker instances</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Tab</td>
<td>Functionality</td>
<td>Portal Administrator</td>
<td>Portal Operator</td>
<td>Restore Operator</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------</td>
<td>----------------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Settings</strong></td>
<td>General settings</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Licensing</strong></td>
<td>Licensing</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Support Information</strong></td>
<td>Updates and logs</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Adding User Accounts

To add a Veeam Backup for AWS user account, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts > Portal Users**.
3. Click **Add**.
4. Complete the **Add Account** wizard.
   a. At the **Account Type** of the wizard, choose whether you want to create a new Veeam Backup for AWS user or retrieve a user identity from your Identity Provider.

**IMPORTANT**

To access Veeam Backup for AWS using the Identity Provider, you must configure single sign-on settings. For more information, see Configuring SSO Settings.

b. At the **Account Info** step of the wizard, specify a name and description for the user account. An account name can contain only lowercase Latin letters, numeric characters, underscores and dashes. You can use the dollar sign ($) as the last character of the user name.

   If you have selected the **Identity Provider account** option at step 4a, use the account format that is accepted by the Identity Provider (for example: `username@suffix`).

c. At the **Account Settings** step of the wizard, select a role for the user account. For more information on user roles, see Managing Permissions.

   If you have selected the **Veeam Backup for AWS account** option at step 4a, at the **Account Settings** step of the wizard, specify a password for the new Veeam Backup for AWS user account.

d. At the **Summary** step of the wizard, review summary information and click **Finish**.
Editing User Account Settings

For each user account added to the Veeam Backup for AWS configuration database, you can modify the settings of the account:

1. Switch to the Configuration page.
3. Select the user account and click Edit.
4. Complete the Edit Account wizard.
   a. At the Account Info step of the wizard, edit a description of the user account.
   b. At the Account Settings step of the wizard, select a new role for the user account.
   c. At the Summary step of the wizard, review summary information and click Finish.
Changing User Passwords

For Veeam Backup for AWS user accounts, you can change the password specified while creating the account:

**IMPORTANT**
You cannot change the password for a user account which user identity was obtained from an identity provider.

1. Switch to the **Configuration** page.
2. Navigate to **Accounts > Portal Users**.
3. Select the user account and click **Change Password**.
4. In the **Change Password** window, do the following:
   a. In the **Old password** field, enter the currently used password.
   b. In the **Password** field, specify a new password.
   c. In the **Repeat Password** field, confirm the new password.
   d. Click **OK**.
Configuring Multi-Factor Authentication

Multi-factor authentication (MFA) in Veeam Backup for AWS is based on the Time-based One-Time Password (TOTP) method that requires the user to verify the user identity by providing a temporary six-digit code sent by an authentication application to a trusted device.

**IMPORTANT**

You cannot enable MFA for a user account which user identity was obtained from an identity provider.

Enabling MFA

To enable MFA for a user account, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts > Portal Users**.
3. Select the user account and click **Enable MFA**.
4. Follow the instructions provided in the **MFA Settings** window:
   a. Install a supported authentication application on a trusted device. To view the list of authentication applications supported by Veeam Backup for AWS, click **See a list of compatible applications**.
   b. Scan the displayed QR code using the camera of the trusted device.
   c. Enter a verification code generated by the authentication application.
   d. Click **OK**.

Disabling MFA

To disable MFA for a user account, select the account on the **Portal Users** tab and click **Disable**.
Managing S3 Repositories

Veeam Backup for AWS uses Amazon S3 buckets as target locations for EC2 instance image-level backups and additional copies of Amazon VPC backups. To add an Amazon S3 bucket to Veeam Backup for AWS, configure an S3 repository. For more details, see Adding S3 Repositories.

To communicate with an S3 repository, Veeam Backup for AWS uses the Veeam Data Mover — the component on a worker instance that is responsible for data processing and transfer. When a backup policy addresses the S3 repository, the Veeam Data Mover establishes a connection with the S3 repository enabling data transfer. To let the Veeam Data Mover access the target Amazon S3 bucket, Veeam Backup for AWS uses permissions of an IAM role specified in S3 repository settings.
Adding S3 Repositories

You can use only existing Amazon S3 buckets as S3 repositories. Before you add an Amazon S3 bucket as an S3 repository, check limitations.

**IMPORTANT**

If you add to the Veeam Backup for AWS configuration database an S3 repository where you store VPC configuration backups created by Veeam backup service, these VPC configuration backups will be automatically added to the Veeam Backup for AWS database. For more information on the retention policy that will be applied to these backups, see [VPC Configuration Backup Retention](#).

To add an S3 repository, complete the following steps:

1. Launch the Add Repository wizard.
2. Specify an S3 repository name and description.
3. Select an IAM role to access the target Amazon S3 bucket.
4. Configure S3 repository settings.
5. Enable data encryption for the S3 repository.
6. Finish working with the wizard.
Step 1. Launch Add Repository Wizard

To launch the Add Repository wizard, complete the following steps:

1. Switch to the Configuration page.
2. Navigate to Repositories.
3. Click New.

Step 2. Specify S3 Repository Name and Description

At the Repository Name step of the wizard, specify a name and description for the new S3 repository. The name must be unique in Veeam Backup for AWS; the maximum length of the name is 255 characters.
Step 3. Select IAM Role to Access S3 Resources

At the **Account** step of the wizard, select an IAM role whose permissions Veeam Backup for AWS will use to access the target Amazon S3 bucket.

For an IAM role to be displayed in the **IAM Role** list, it must be added to Veeam Backup for AWS as described in **Adding IAM Roles**. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the **Add Repository** wizard. To add an IAM role, click **Add** and complete the **Add Account** wizard.

---

**Add Repository**

<table>
<thead>
<tr>
<th>Repository Name</th>
<th>Choose an IAM Role to connect to the repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>IAM Role:</td>
</tr>
<tr>
<td>Repository</td>
<td>S3 Access Role (Role for Dept-01 S3 repositories)</td>
</tr>
</tbody>
</table>

---

Step 4. Configure S3 Repository Settings

At the **Repository** step of the wizard, specify an Amazon S3 bucket and folder where you want to store image-level backups of EC2 instances and VPC configuration backups.

1. Click the link to the right of **Bucket**.

2. In the **Buckets** window, select the Amazon S3 bucket that will be used as a target location for image-level backups, and click **OK**.

   For an Amazon S3 bucket to be displayed in the **Bucket** list, it must be created within an AWS account to which the IAM role selected at the **Account** step of the wizard has permissions. To learn how to create an Amazon S3 bucket, see **AWS Documentation**.

---

**TIP**

It may take some time for Veeam Backup for AWS to retrieve information about existing storage buckets from AWS. To speed up the data collection process, click **Rescan**.
3. Choose whether you want to use an existing folder inside the selected Amazon S3 bucket or to create a new one to group backup files stored in the bucket.

   - To use an existing folder, click the link to the right of **Use existing folder**. In the **Select folder** window, select the necessary folder and click **Select**.

     If encryption at the S3 repository level was enabled for the selected folder, at the **Settings** step of the wizard, you will need to provide a password for this folder.

**NOTE**

If the selected folder already contains backup files, Veeam Backup for AWS import the backed-up data to the configuration database. You can then use this data to perform all disaster recovery operations described in section **Performing Restore**.

   - To create a new folder, select the **Create new folder** option, and then specify a name for the new folder. The maximum length of the name is 125 characters; the dash (/) character is not supported.

![Add Repository](image)
Step 5. Enable Data Encryption

At the **Settings** step of the wizard, use the **Enable encryption** check box to choose whether you want to encrypt backup files stored in the selected Amazon S3 bucket folder. If you enable encryption, specify a password that will be used to encrypt data.

Veeam Backup for AWS encrypts backup files in S3 repositories the same way as Veeam Backup & Replication encrypts backup files in backup repositories. For more information, see [S3 Repository Encryption](#).

If you have chosen an existing folder at the **Repository** step of the wizard, and if encryption is enabled for this folder at the S3 repository level, you must provide the currently used for encryption password to let Veeam Backup for AWS access this folder and add it as an S3 repository.
Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

As soon as you click **Finish**, Veeam Backup for AWS will start adding the S3 repository. To track the progress, click **Go to Sessions** in the **Confirmation** window to proceed to the **Sessions Log** page.
Editing S3 Repository Settings

For each S3 repository added to Veeam Backup for AWS, you can modify the S3 repository name or description, or enable encryption for the S3 repository.

**NOTE**
You cannot change an Amazon S3 bucket and folder for an S3 repository.

To edit settings of an S3 repository, do the following:

1. Switch to the Configuration page.
2. Navigate to Repositories.
3. Select the check box next to the S3 repository and click Edit.
   a. To provide a new name and description for the S3 repository, follow the instructions provided in section Adding S3 Repositories (step 2).
   b. To enable encryption for the repository, follow the instructions provided in section Adding S3 Repositories (step 5).
   c. At the Summary step of the wizard, review summary information and click Finish to confirm the changes.

As soon as you click Finish, Veeam Backup for AWS will start modifying the S3 repository settings. To track the progress, click Go to Sessions in the Confirmation window to proceed to the Sessions Log page.
Removing S3 Repositories

You can remove S3 repositories from the backup infrastructure. When you remove an S3 repository, Veeam Backup for AWS unassigns the repository role from the folder in an Amazon S3 bucket and this folder is no longer used as an S3 repository.

**NOTE**

Even though the Amazon S3 bucket is no longer used as an S3 repository, Veeam Backup for AWS preserves all backup files previously stored in the S3 repository and keeps these files in Amazon S3. You can assign the Amazon S3 bucket to a new S3 repository so that Veeam Backup for AWS imports the backed-up data to the configuration database. In this case, you will be able to perform all disaster recovery operations described in section Performing Restore.

If you no longer need the backed-up data, you can remove it as described in sections Removing Backups and Snapshots and Removing VPC Configuration Backups.

To remove an S3 repository, do the following:

1. Switch to the Configuration page.
2. Navigate to Repositories.
3. Select the check box next to the S3 repository and click Remove.
4. In the Confirmation window, click Yes to acknowledge the operation.

**IMPORTANT**

You cannot remove an S3 repository that is used by any backup policy. To remove such S3 repository, you must first delete a reference to this S3 repository in backup policy settings. For more information on backup policies, see Performing Backup.
Managing Worker Instances

To perform most data protection and disaster recovery operations (such as creating image-level backups in S3 repositories and restoring backed-up data), Veeam Backup for AWS uses worker instances. Each worker instance is launched for the duration of the backup or restore process. Veeam Backup for AWS uses the default network settings of an AWS Region where the worker instance will be launched.

To optimize infrastructure costs and to ensure better performance of the backup and restore processes, you can specify network settings for AWS Regions in which worker instances will be launched.
Configuring Worker Instance Settings

To perform image-level backup or restore backed-up data, you must first configure worker instance settings.

1. Specify an IAM role for worker instances.
2. Configure network settings for AWS Regions in which worker instances will be launched.

Specifying IAM Role

By default, Veeam Backup for AWS uses the Default Backup Restore IAM role to launch worker instances. The role is preconfigured and has all the required permissions to launch worker instances within the initial AWS account.

You can specify a different IAM role, for example, if you want Veeam Backup for AWS to launch worker instances in another AWS account. Before you specify the necessary role, make sure it is added to Veeam Backup for AWS as described in section Adding IAM Roles.

To specify an IAM role for worker instances, do the following:

1. Switch to the Configuration page.
2. Navigate to Workers > General.
3. Click the link to the right of Worker IAM Role.
4. In the Cloud Account window, click the necessary IAM role, and then click Apply.

After you specify the IAM role, it is recommended that you check whether permissions of the specified IAM role are sufficient to launch worker instances. For information on how to check IAM role permissions, see Checking IAM Role Permissions.
Configuring Network Settings

For each AWS Region in which worker instances will be launched, you must configure network settings.

To configure network settings, in the Region Network Settings section, click Add and complete the Add Region wizard.

1. At the Region step of the wizard, select the AWS Region and Availability Zone for which you want to configure network settings.

2. At the Network Settings step of the wizard, select the Amazon VPC and subnet to which you want to connect worker instances, and specify the security group. For more information on Amazon VPC, subnets and security groups, see AWS Documentation.

Veeam Backup for AWS will apply the specified network settings to all worker instances that will be launched in the AWS Region and Availability Zone selected at the Region step of the wizard.

**IMPORTANT**

Consider the following:

- The public IPv4 addressing attribute must be enabled for the selected subnet, otherwise Veeam Backup for AWS will display a warning at the Summary step of the wizard. To learn how to enable the public IPv4 addressing attribute for a subnet, see AWS Documentation.

To let Veeam Backup for AWS launch worker instances with private IPv4 addresses, the following endpoints must be configured for the selected subnet: sqs, ssm, ec2messages, ssmmessages. For information on how to configure endpoints, see AWS Documentation.

- If you select an Outpost subnet, backup and restore operations in an AWS Region to which the AWS Outpost is connected may fail. The issue occurs if the default worker instance class (c5.large) is not supported for the AWS Outpost. To work around the issue, contact Veeam Customer Support.

3. At the Summary step of the wizard, review summary information and click Finish.
# Testing File-Level Restore

Before you perform file-level restore, it is recommended that you run a file-level restore test. The file-level restore test allows you to check whether AWS Region network settings are configured properly to launch worker instances, and that you can access the File Level Recovery for Veeam Backup browser from the local machine.

To run the file-level restore test for an AWS Region, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Workers > General**.
3. In the **Region Network Settings** section, click the necessary AWS Region, and then click **Test FLR**.
4. Wait until the status of the file-level restore test in the **FLR Status** column changes to **Running**, and then click it.
   
   Veeam Backup for AWS will display the **FLR Test Log** window where you can view the progress and results of the test.

5. If network settings are configured properly for the AWS Region, Veeam Backup for AWS will launch the worker instance and display the link to the File Level Recovery for Veeam Backup browser in the **FLR Test Log** window.
   
   a. To check that you can access the File Level Recovery for Veeam Backup browser, click the displayed link.
   
   b. To finish the file-level restore test, in the File Level Recovery for Veeam Backup browser, click **End Test**.

   If you do not click **End Test** within 30 minutes after the link to the File Level Recovery for Veeam Backup browser appears, the file-level restore test will finish automatically with the **Warning** status.

### TIP

If the file-level restore test finishes with the **Warning or Error** status, and you want to run the test again after fixing issues with network settings, you can rerun the file-level restore test. To do that, in the **FLR Status** column, click the status of the file-level restore test, and then, in the **FLR Test Log** window, click **Start test**.

<table>
<thead>
<tr>
<th>Time</th>
<th>Status</th>
<th>Message</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/12/2020 5:47:00 PM</td>
<td>Success</td>
<td>Test FLR task eu-central-1 started at 06/12/2020 17:46:55</td>
<td>18 minutes 6 seconds</td>
</tr>
<tr>
<td>06/12/2020 5:47:00 PM</td>
<td>Running</td>
<td>Processing Test FLR eu-central-1.</td>
<td>18 minutes 6 seconds</td>
</tr>
<tr>
<td>06/12/2020 5:47:07 PM</td>
<td>Success</td>
<td>Preparing the worker VM.</td>
<td>7 minutes 59 seconds</td>
</tr>
<tr>
<td>06/12/2020 5:55:07 PM</td>
<td>Success</td>
<td>Configuring FLR worker</td>
<td>7 minutes 43 seconds</td>
</tr>
<tr>
<td>06/12/2020 6:02:51 PM</td>
<td>Success</td>
<td>53 endpoint url: <a href="https://s3-eu-central-1.amazonaws.com">https://s3-eu-central-1.amazonaws.com</a> ...</td>
<td></td>
</tr>
</tbody>
</table>
Editing Worker Instance Settings

You can edit settings configured in Veeam Backup for AWS to launch worker instances.

To edit worker instance settings, do the following:

1. Switch to the Configuration page.
2. Navigate to Workers > General.
2. In the Role section, you can change an IAM role whose permissions Veeam Backup for AWS will use to launch worker instances. To change the IAM role, click Change and select the necessary IAM role from the list.

**IMPORTANT**
If you change the IAM role, all previously configured network settings for AWS Regions in which Veeam Backup for AWS launches worker instances will be removed automatically.

3. In the Region Settings section, you can change network settings configured for AWS Regions in which Veeam Backup for AWS launches worker instances.

   To change network settings for an AWS Region:
   a. Select the necessary AWS Region from the list, and then click Edit.
   b. In the Edit Region window, specify new network settings for the AWS Region as described in section Configuring Worker Instance Settings.

**NOTE**
If there are any worker instances launched using the selected AWS Region network settings that are currently involved in a backup or restore process, the changes will be applied only when the process completes.
Configuring General Settings

Veeam Backup for AWS allows you to configure general settings that are applied to all performed operations and deployed infrastructure components.

- Define for how long obsolete snapshots and session records must be retained.
- Provide certificates to secure connections between Veeam Backup for AWS infrastructure components.
- Configure notification settings for automated delivery of reports.
- Change the time zone set on the backup appliance.
- Configure single sign-on settings to retrieve user identities from an identity provider.
Configuring Global Retention Settings

You can configure global retention settings to specify for how long the following data must be retained in the configuration database:

- Obsolete snapshots and replicas
- Session records

Configuring Retention Settings for Obsolete Snapshots and Replicas

If an instance is no longer processed by a backup policy (it was removed from the backup policy or the backup policy no longer exists), its cloud-native snapshots and snapshot replicas become obsolete. Retention policy settings configured when creating backup policies do not apply to obsolete snapshots — these snapshots are removed from the configuration database according to their own retention settings.

To configure retention settings for obsolete snapshots and replicas, do the following:

1. Switch to the Configuration page.
2. Navigate to Settings > Retention.
3. In the Obsolete snapshots retention section, select one of the following options:
   - Select the Never option if you do not want Veeam Backup for AWS to remove obsolete snapshots and replicas.
   - Select the After option to specify the number of days (or months) during which Veeam Backup for AWS must keep obsolete snapshots in the configuration database. The number must be between 90 and 36135.
     If you select this option, Veeam Backup for AWS will first wait for the specified period of time after an instance stops being processed by a backup policy, and then will remove its obsolete snapshots from the configuration database as soon as the period is over.
4. Click Save.

IMPORTANT
Global retention settings apply to all cloud-native snapshots and snapshot replicas. If an instance is still processed by a backup policy, but some of its cloud-native snapshots and snapshot replicas are older than the number of days (or months) specified in the global retention settings, these cloud-native snapshots and snapshot replicas will be removed from Veeam Backup for AWS.

Configuring Retention Settings for Session Records

Veeam Backup for AWS stores records for all sessions of performed data protection and disaster recovery operations. These session records are removed from the configuration database according to their own retention settings.
To configure retention settings for session records, do the following:

1. In the **Session retention** section, select one of the following options:
   
   o Select the **Keep all sessions** option if you do not want Veeam Backup for AWS to remove session records.
   
   o Select the **Keep only last** option if you want to specify the number of days (or months) during which Veeam Backup for AWS must keep session records in the configuration database.

   If you select this option, Veeam Backup for AWS will remove all session records that are older than the specified time limit.

2. Click **Save**.
Configuring Global Email Notification Settings

You can specify email notification settings for automated delivery of backup policy results and daily reports. Every daily report contains cumulative statistics for all backup policy and snapshot retention sessions run within the past 24-hour period.

To connect an SMTP server that will be used for sending email notifications:

1. Switch to the Configuration page.
2. Navigate to Settings > E-mail.
3. Select the Enable e-mail notifications check box.
4. In the SMTP Server field, specify a DNS name or an IP address of the SMTP server. All email notifications (including test messages) and daily reports will be sent by this SMTP server.
5. Click Advanced to specify an account that will be used when authenticating against the SMTP server and to configure other connection settings.

In the Advanced SMTP Options window:
   a. In the Port field, specify a communication port for SMTP traffic. The default SMTP port is 25.
   b. In the Timeout field, specify a connection timeout for responses from the SMTP server.
   c. For an SMTP server with SSL/TLS support, select the Connect using SSL check box to enable SSL data encryption.
   d. If your SMTP server requires authentication, select the This SMTP server requires authentication check box and choose the necessary account from the Log on as drop-down list.

For an account to be displayed in the Log on as list, it must be added to the configuration database as described in section Adding SMTP Accounts. If you have not set up an account beforehand, click Add and follow the steps of the Add Account wizard.

d. Click Apply.

6. In the From field, enter an email address of the notification sender. This email address will be displayed in the From field of notifications.

7. In the To field, enter an email address of a recipient. Use a semicolon to separate multiple recipient addresses. Do not use spaces after semicolons between the specified email addresses.

   For each particular policy, you can specify additional recipients.

   NOTE
   If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for AWS will send each notification twice to this recipient.

8. In the Subject field, specify a subject for notifications. You can use the following runtime variables:
   o  %JobName% — a backup policy name.
   o  [%JobResult%] — a backup policy result.
   o  (%ObjectCount% instances) — the number of instances in a backup policy.
   o  %Issues% — the number of instances in a backup policy that encountered any issues (errors and warnings) while being processed.
9. In the **Notify me immediately about** section, choose whether you want to receive email notifications in case backup policies complete successfully, complete with warnings or complete with errors.

10. To receive daily reports, select the **Send daily report at** check box and the exact time when the reports must be sent.

11. Click **Save**.

**TIP**

Veeam Backup for AWS allows you to send a test message to check whether you have configured all settings correctly. To do that, click **Send Test Email**. A test message will be sent to the specified email address.

---

### Adding SMTP Accounts

To add an account that will be used to connect to an SMTP server, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts > SMTP Accounts**.
3. Click **Add**.

Complete the **Add Account** wizard.

- **a.** At the **Account Name** step of the wizard, specify a name and description for the SMTP account. The name must be unique in Veeam Backup for AWS and the length of the name must not exceed 255 characters. The description length must not exceed 512 characters.

- **b.** At the **Account** step of the wizard, specify credentials of a user account that has permissions to access the SMTP server. Veeam Backup for AWS will use the specified credentials to authenticate against the SMTP server.
c. At the **Summary** step of the wizard, review summary information and click **Finish**.

### Editing SMTP Accounts

For each SMTP account, you can modify the settings configured while adding the account:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts > SMTP Accounts**.
3. Select the check box next to the necessary SMTP account and click **Edit**.

   Complete the **Edit Account** wizard.

   a. To provide a new name and description for the record, follow the instructions provided in section **Adding SMTP Accounts** (step 4).

   b. To specify credentials of another user account to be used to authenticate against the SMTP server, follow the instructions provided in section **Adding SMTP Accounts** (step 5).
Replacing Security Certificates

To establish secure data communications between the backup appliance and web browsers running on user workstations, Veeam Backup for AWS uses Transport Layer Security (TLS) certificates.

When you install Veeam Backup for AWS, it automatically generates a default self-signed certificate. You can replace this default certificate with your own self-signed certificate or with a certificate obtained from a Certificate Authority (CA). To replace the currently used TLS certificate, do the following:

To replace a TLS certificate, do the following:

1. Switch to the Configuration page.
2. Navigate to Settings > Certificates.
3. Click Replace Web Certificate.

Complete the New Certificate Wizard.

a. At the Certificate Source step of the wizard, do the following:
   - Select the Recreate a self-sign certificate option if you want to replace the existing certificate with a new self-signed certificate automatically generated by Veeam Backup for AWS.
   - Select the Upload certificate(s) option if you want to upload a certificate that you obtained from a CA or generated using a 3rd party tool.

b. [This step applies only if you have selected the Upload certificate(s) option] At the Upload certificate(s) step of the wizard, browse to the certificate that you want to install, and provide a password for the certificate file if required.

c. At the Summary step of the wizard, review summary information and click Finish. To allow Veeam Backup for AWS to discover the newly installed certificate, restart the backup appliance.

NOTE

If you have recreated the self-signed certificate, when you try to access Veeam Backup for AWS in a web browser, the browser will display a warning notifying that the connection is untrusted (although it is secured with SSL). To eliminate the warning, import the self-signed certificate to user workstations.
Changing Time Zone

Veeam Backup for AWS runs daily reports and performs all data protection and disaster recovery operations according to the time zone set on the backup appliance.

Since the backup appliance is deployed on an EC2 instance in Amazon EC2, the time zone is set to Coordinated Universal Time (UTC) by default. However, you can change the time zone if required. For example, you may want the time on the backup appliance to match the time on the workstation from which you access Veeam Backup for AWS.

To change the time zone set on the backup appliance:

1. Switch to the **Configuration** page.
2. Navigate to **Settings > Time Zone**.
3. Select the necessary time zone from the **Time zone** drop-down list.
4. Click **Save**.

![Configuration page](image)
Configuring SSO Settings

Veeam Backup for AWS supports single sign-on (SSO) authentication based on the SAML 2.0 protocol. SSO authentication scheme allows a user to log in to different software systems with the same credentials using the identity provider service.

To configure SSO settings for Veeam Backup for AWS, complete the following steps:

1. Switch to the Configuration page.
2. Navigate to Settings > Identity Provider.
3. In the Identity Provider Configuration section, import identity provider settings from a file obtained from your identity provider:
   a. Click Upload Metadata.
   b. In the Upload Identity Provider Configuration window, click Browse to locate the file with identity provider settings.
   c. Click Upload to import the metadata.
4. To finish SSO settings configuration, you must pass the service provider authentication settings to the identity provider. To obtain the settings, in the Veeam Backup for AWS Configuration section, click Download. Veeam Backup for AWS will download a metadata file with the service provider authentication settings to your local machine. Alternatively, you can copy the service provider settings manually:
   a. Click Copy Link to the right of SP Entity ID / Issuer.
   b. Click Copy Link to the right of Assertion Consumer URL.

TIP

If you want to sign and encrypt authentication requests sent from Veeam Backup for AWS to the identity provider, you must select a certificate with a private key that will be used for encryption and signing:

1. In the Veeam Backup for AWS Configuration section, click Select to the right of Certificate.
2. In the Upload Veeam Backup certificate window, click Browse to locate the certificate file. In the Password field, specify a password used to open the file.
3. Click Upload.
After you configure SSO settings, you can add user accounts that will be able to log in to Veeam Backup for AWS using single sign-on. For more information, see Adding User Accounts.
Performing Backup

With Veeam Backup for AWS, you can protect data in the following ways:

- **Create cloud-native snapshots of EC2 and RDS instances**
  
  A cloud-native snapshot of an EC2 instance includes point-in-time snapshots of EBS volumes attached to the processed instance. Snapshots of EBS volumes (also referred to as EBS snapshots) are taken using native AWS capabilities.

  A cloud-native snapshot of an RDS instance includes a storage volume snapshot of the instance. Snapshots of RDS instances (also referred to as DB instance snapshots) are taken using native AWS capabilities.

- **Replicate cloud-native snapshots to a remote site**

  By default, cloud-native snapshots are stored only in the AWS Region where the processed instance resides. For enhanced data safety, you can instruct Veeam Backup for AWS to create copies of cloud-native snapshots and store them in any other AWS Region within any AWS account. You can also combine the snapshot replication functionality with various data recovery options to migrate instance data between AWS Regions.

- **Create image-level backups of EC2 instances**

  In addition to cloud-native snapshots, you can protect your EC2 instances with image-level backups. An image-level backup captures the whole image of the processed EC2 instance (including OS data, application data and so on) at a specific point in time. The backup is saved as a single file to an S3 repository in the native Veeam format.

- **Create backups of your Amazon VPC configuration**

  You can back up the Amazon VPC configuration of an AWS account. By default, the Amazon VPC configuration backup is stored in the Veeam Backup for AWS database. For enhanced data safety, you can instruct Veeam Backup for AWS to create copies of Amazon VPC configuration backups and store them in the specified S3 repository.

Data protection tasks are scheduled to run automatically with backup policies. To perform a quick backup, you can also take cloud-native snapshots of EC2 and RDS instances manually when needed.

**TIP**

You can perform advanced data protection operations with image-level backups from the Veeam Backup & Replication console. For details, see the External Repository section in the Veeam Backup & Replication User Guide.
How Backup Works

Veeam Backup for AWS does not install agent software inside instances to retrieve data. To back up instance data, Veeam Backup for AWS uses native AWS capabilities. During every backup session, Veeam Backup for AWS creates a cloud-native snapshot for each instance added to a backup policy. The cloud-native snapshot is further used to create a snapshot replica (for RDS and EC2 instances) and an image-level backup (only for EC2 instances).

To protect Amazon VPC configuration, Veeam Backup for AWS retrieves configuration data through API and back up this data to the Veeam Backup for AWS database.

For more information on the backup process, see:

- EC2 instance backup
- RDS instance backup
- Amazon VPC configuration backup

EC2 Instance Backup

Veeam Backup for AWS performs EC2 instance backup in the following way:

1. Veeam Backup for AWS creates snapshots of EBS volumes that are attached to the processed EC2 instance.

2. EBS snapshots are assigned AWS tags upon creation. Keys and values of AWS tags contain encrypted metadata that helps Veeam Backup for AWS identify the related EBS snapshots and treat them as a single unit — a cloud-native snapshot.

3. If you enable snapshot replication for the backup policy, Veeam Backup for AWS copies cloud-native snapshots to the target AWS Region and AWS account specified in backup policy settings.

4. If you enable image-level backup for the backup policy, Veeam Backup for AWS performs the following operations:
   a. Launches a worker instance in an AWS Region where the processed EC2 instance resides.
   b. Re-creates the EBS volumes from the cloud-native snapshot created at step 1 and attaches them to the worker instance.

      Note that the cloud-native snapshot used as a source for image-level backup is not a temporary snapshot, and it is required to perform changed block tracking (CBT). When the backup session completes, this snapshot remains in the snapshot chain until the next image-level backup session. For more information, see CBT Impact on Snapshot Retention.

   c. Reads data from the EBS volumes on the worker instance, transfers the data to an S3 repository and stores it in the native Veeam format.

      To reduce the amount of data read from EBS volumes, Veeam Backup for AWS uses CBT: during incremental backup sessions, Veeam Backup for AWS transfers to an S3 repository only those data blocks that have changed since the previous backup session. If CBT cannot be used, Veeam Backup for AWS reads the full content of EBS volumes. For more information, see Changed Block Tracking.

      Veeam Backup for AWS encrypts and compresses data saved to S3 repositories. For more information on data encryption, see Data Encryption.

   d. When the backup session completes, Veeam Backup for AWS removes the worker instance from Amazon EC2.
RDS Instance Backup

Veeam Backup for AWS performs RDS instance backup in the following way:

1. Veeam Backup for AWS creates a storage volume snapshot of an RDS instance (DB snapshot).

   The DB snapshot is assigned AWS tags upon creation. Keys and values of AWS tags contain encrypted metadata that helps Veeam Backup for AWS identify the related DB snapshot.

2. If you enable snapshot replication for the backup policy, Veeam Backup for AWS copies the DB snapshot to the target AWS Region of the AWS account specified in the backup policy settings.

Amazon VPC Configuration Backup

Veeam Backup for AWS performs VPC configuration backup in the following way:

1. Veeam Backup for AWS sends API requests to AWS to retrieve the VPC configuration data and saves this data in the Veeam Backup for AWS database.

   To back up the VPC configuration of an AWS Region, Veeam Backup for AWS uses permissions of an IAM role specified for this AWS Region in the backup policy. For each pair of the AWS account and the AWS Region whose VPC configuration data is backed up using the IAM role created in this AWS account, Veeam Backup for AWS creates a configuration record. Every time the VPC Configuration Backup policy runs, Veeam Backup for AWS updates the record to create a new restore point for the VPC configuration. For more information, see VPC Configuration Backup Chain.

2. If you configure the VPC Configuration Backup policy to copy backup files to an S3 repository, Veeam Backup for AWS launches Veeam Data Mover service on the backup appliance to copy the restore point to the target S3 repository specified in the backup policy settings. On the S3 repository, for each backed-up AWS account, Veeam Backup for AWS creates an individual folder with VPC configuration backup files.

Snapshot Chain

During every backup session, Veeam Backup for AWS creates a cloud-native snapshot for each instance added to the backup policy. The cloud-native snapshot itself is a collection of point-in-time snapshots that Veeam Backup for AWS takes using native AWS capabilities.

A sequence of cloud-native snapshots created during a set of backup sessions makes up a snapshot chain. Veeam Backup for AWS creates the snapshot chain in the following way:

1. During the first backup session, Veeam Backup for AWS creates a snapshot of all instance data and saves it in the AWS Region where the processed instance resides. This snapshot becomes a starting point of the snapshot chain.

   The creation of the first snapshot may take significant time to complete since Veeam Backup for AWS copies the whole image of the instance.
2. During subsequent backup sessions, Veeam Backup for AWS takes snapshots of only those data blocks that have changed since the previous backup session.

The creation of subsequent snapshots typically takes less time to complete, compared to the first snapshot in the chain. Note, however, that the completion time still depends on the amount of processed data.

Each cloud-native snapshot in the snapshot chain contains metadata. Metadata stores information about the protected instance, the backup policy that created the snapshot, and the total number of snapshots in the chain. Veeam Backup for AWS uses metadata to identify outdated snapshots, to load the configuration of source instances during recovery operations, and so on.

Cloud-native snapshots act as independent restore points for backed-up instances. If you remove any snapshot, it will not break the snapshot chain — you will still be able to roll back instance data to any existing restore point.

The number of cloud-native snapshots kept in a snapshot chain is defined by retention policy settings. For details, see Snapshot Retention.

NOTE
Cloud-native snapshots created manually are not included into the snapshot chain. Therefore, such snapshots are not removed automatically according to retention policy settings. For information on how to remove them, see section Managing Backed-Up Data.

Snapshot Replica Chain

Snapshot replicas are copies of cloud-native snapshots that Veeam Backup for AWS creates during backup sessions. If you enable snapshot replication for a backup policy, Veeam Backup for AWS will make a copy of the initially created cloud-native snapshot and save it to the target AWS Region specified in backup policy settings. In the target AWS Region, snapshot replicas created during a set of backup sessions make up a snapshot replica chain.

Veeam Backup for AWS creates and maintains a snapshot replica chain in the same way as a regular snapshot chain:

- The first created snapshot replica for the processed instance becomes a starting point of the snapshot replica chain.
- Snapshot replicas created during subsequent backup sessions store only those data blocks that have changed since the previous backup session.
EC2 Backup Chain

If you enable image-level backups for an EC2 backup policy, Veeam Backup for AWS will create a new backup file in an S3 repository during every backup session. A sequence of backup files created during a set of backup sessions makes up a backup chain.

The backup chain includes backup files of the following types:

- **Full** – a full backup file stores a copy of the full EC2 image.
- **Incremental** – incremental backup files store incremental changes of EC2 images.

To create a backup chain for an EC2 instance protected by a backup policy, Veeam Backup for AWS implements the forever forward incremental backup method:

1. During the first backup session, Veeam Backup for AWS copies the full EC2 image and creates a full backup file in the S3 repository. The full backup file becomes a starting point in the backup chain.
2. During subsequent backup sessions, Veeam Backup for AWS copies only those data blocks that have changed since the previous backup session, and stores these data blocks to incremental backup files in the S3 repository. The content of each incremental backup file depends on the content of the full backup file and the preceding incremental backup files in the backup chain.

Full and incremental backup files act as restore points for a backed-up EC2 instances that let you roll back instance data to the necessary state. To recover an EC2 instance to a specific point in time, the chain of backup files created for the instance must contain a full backup file and a set of incremental backup files dependent on the full backup file.

If some file in the backup chain is missing, you will not be able to roll back to the necessary state. For this reason, you must not delete individual backup files from the S3 repository manually. Instead, you must specify retention policy settings that will let you maintain the necessary number of backup files in the backup repository. For more information, see EC2 Backup Retention.

Changed Block Tracking

The changed block tracking (CBT) mechanism allows Veeam Backup for AWS to quickly backup EC2 instances to S3 repositories.

Veeam Backup for AWS uses the CBT mechanism to reduce the amount of data read from processed EBS volumes:

- During a full backup session, Veeam Backup for AWS reads only written data blocks, while unallocated data blocks are filtered out.
- During an incremental backup session, Veeam Backup for AWS reads only those data blocks that have changed since the previous backup session.

To detect unallocated and changed data blocks, CBT relies on EBS Direct APIs.

1. During the first (full) backup session, Veeam Backup for AWS creates a cloud-native snapshot of an EC2 instance. To do that, Veeam Backup for AWS sends API requests to access the content of the snapshot and to detect unallocated data blocks.
2. During subsequent sessions, new cloud-native snapshots are created. Veeam Backup for AWS sends API requests to access and to compare the content of the snapshot created during the previous backup session and the snapshot created during the current backup session. This allows Veeam Backup for AWS to detect data blocks that have changed since the previous backup session.

Limitations for Changed Block Tracking

Veeam Backup for AWS cannot use CBT for EC2 instances that reside in AWS Regions where EBS Direct APIs are not available.

If CBT cannot be used, Veeam Backup for AWS reads the whole content of processed EBS volumes and compares it with backed-up data that already exists in the S3 repository. In this case, the completion time and cost of incremental backups may occur to grow.

VPC Configuration Backup Chain

During every backup session, Veeam Backup for AWS creates a restore point with backed-up VPC configuration data for each AWS Region protected by the VPC Configuration Backup policy. The restore point contains metadata that includes information on the date and time when the policy ran, AWS Regions whose VPC configuration settings were backed up by the policy and AWS accounts whose IAM roles were used to collect VPC configuration settings for each AWS Region.

A sequence of restore points created during a set of backup sessions makes up a VPC configuration backup chain for each configuration record.

You cannot delete specific restore points created for a configuration record - these points are removed automatically according to the specified retention policy settings. However, you can manually remove a configuration record with all restore points created for this configuration record, as described in section Removing VPC Configuration Backups.
Retention Policy

Cloud-native snapshots, snapshot replicas and image-level backups are not kept forever. They are removed according to retention policy specified in the backup schedule settings while creating a backup policy.

Depending on the data protection scenario, retention policy can be specified:

- **In restore points** — for cloud-native snapshots and snapshot replicas.
  
  The snapshot chain can contain only the allowed number of restore points. If the number of allowed restore points is exceeded, Veeam Backup for AWS removes the earliest restore point from the snapshot chain. For details, see Retention Policy for Snapshots.

- **In days/months/years** — for image-level backups.
  
  Restore points in the backup chain can be stored for the allowed period of time. If a restore point is older than the specified limit, Veeam Backup for AWS removes it from the backup chain. For details, see Retention Policy for Backups.

You can also specify global retention settings for obsolete snapshots and replicas. For details, see Configuring Global Retention Settings.

Snapshot Retention

For cloud-native snapshots and snapshot replicas, Veeam Backup for AWS retains the number of latest restore points defined in backup schedule settings.

During every successful backup session, Veeam Backup for AWS creates a new restore point. If Veeam Backup for AWS detects that the number of restore points in the snapshot chain exceeds the retention limit, the earliest restore point is removed from the chain.

Mind that Veeam Backup for AWS does not apply retention policy to cloud-native snapshots created manually. For details on how to remove them, see section Managing Backed-Up Data.

EC2 Backup Retention

For image-level backups, Veeam Backup for AWS retains restore points for the number of days defined in backup scheduling settings.

To track and remove outdated restore points from a backup chain, Veeam Backup for AWS performs the following actions once a day.

1. Veeam Backup for AWS checks the configuration database to detect S3 repositories that contain outdated restore points.
2. If an outdated restore point exists in an S3 repository, Veeam Backup for AWS transforms the backup chain in the following way:

   a. Veeam Backup for AWS rebuilds the full backup file to include in it data of the incremental backup file that follows the full backup file. To do that, Veeam Backup for AWS injects into the full backup file data blocks from the earliest incremental backup file in the chain. This way, a full backup 'moves' forward in the backup chain.

   b. Veeam Backup for AWS removes the earliest incremental backup file from the chain as redundant — this data has already been injected into the full backup file.

3. Veeam Backup for AWS repeats step 2 for all other outdated restore points found in the backup chain until all the restore points are removed. As data from multiple restore points is injected into the rebuilt full backup file, Veeam Backup for AWS ensures that the backup chain is not broken and that you will be able to recover your data when needed.

CBT Impact on Snapshot Retention

If CBT is available, Veeam Backup for AWS does not remove the cloud-native snapshot used as a source for image-level backup from the snapshot chain until the next image-level backup session completes. Therefore, at some point in time you may discover that Veeam Backup for AWS ignores retention policy settings and keeps an additional restore point in the snapshot chain.

Consider the following example. You want a backup policy to create image-level backups and to run daily according to the following schedule:

- Image-level backup creation is enabled.
- Backup policy is scheduled to run daily:
  - Cloud-native snapshots must be created at 7:00 AM, 9:00 AM, 11:00 AM, 1:00 PM, 3:00 PM, and 5:00 PM.
    Retention policy for cloud-native snapshots is set to 2 restore points.
  - Image-level backups must be created at 7:00 AM and 5:00 PM.
    Retention policy for image-level backups is set to 7 days.
Veeam Backup for AWS runs the backup policy in the following way:

1. At 7:00 AM, the first backup session will create a cloud-native snapshot, and then will use this snapshot to create a full image-level backup.

2. From 9:00 AM to 3:00 PM, subsequent sessions will create only cloud-native snapshots.
   a. After the backup session runs at 11:00 AM, the length of a snapshot chain (3 restore points) will exceed the retention limit (2 restore points). The earliest snapshot, however, will not be removed as it will be used to track changed data at 5:00 PM when the next image-level backup creation is scheduled.
   b. After the backup session runs at 1:00 PM and 3:00 PM, Veeam Backup for AWS will remove snapshots created at 9:00 AM and 11:00 AM. The length of the snapshot chain will remain 3 restore points.

3. At 5:00 PM, the backup session will create a new cloud-native snapshot. Veeam Backup for AWS will compare this snapshot with the one created at 7:00 AM to identify changed data blocks. After that, the backup session will create an incremental image-level backup based on the data obtained during the snapshot comparison.

4. After the snapshot comparison, Veeam Backup for AWS will apply the retention policy and remove the snapshot created at 7:00 AM (as it is no longer needed) and the snapshot created at 1:00 PM from the chain.
VPC Configuration Backup Retention

For VPC configuration backups, Veeam Backup for AWS retains restore points for the period of time specified in backup retention settings.

During every successful backup session, Veeam Backup for AWS creates a restore point and saves the date, time and the applied retention settings in the restore point metadata. If Veeam Backup for AWS detects that the period of time for which the restore point was stored exceeds the period specified in the retention settings, it automatically removes the restore point from the VPC configuration backup chain. You can also remove unnecessary VPC configuration backups manually as described in section Removing VPC Configuration Backups.

**NOTE**

Veeam Backup for AWS applies the retention settings configured for the VPC Configuration Backup policy both to VPC configuration backups stored in the Veeam Backup for AWS database and to VPC configuration backups stored in the S3 repository selected for the policy. For VPC configuration backups stored in S3 repositories that are not specified in the VPC Configuration Backup policy settings, Veeam Backup for AWS applies retention settings saved in the backup metadata.
Performing EC2 Instance Backup

To produce image-level backups of EC2 instances, Veeam Backup for AWS runs backup policies. A backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where backups must be stored, when the backup process must start and so on.

One backup policy can be used to process multiple EC2 instances within different regions, but you can back up each EC2 instance with one backup policy at a time. If an EC2 instance is added to more than one backup policy, it will be processed only by a backup policy that has the highest priority. Other backup policies will skip this EC2 instance from processing. For information on how to set a priority for a backup policy, see Setting Policy Priority.

To schedule data protection tasks to run automatically, create backup policies. For each protected EC2 instance, you can also take a cloud-native snapshot manually when needed.

IMPORTANT

In Veeam Backup for AWS, you can protect only EC2 instances that run in a VPC. EC2-Classic instances are not supported. For details, see this Veeam KB article.
Creating EC2 Backup Policies

One backup policy can be used to process one or more instances within one AWS account. The scope of data that you can protect in an AWS account is limited by permissions of an IAM role that is specified in backup policy settings.

Before you create an EC2 backup policy, check the following prerequisites:

- Backup infrastructure components that will take part in the backup process must be added to the backup infrastructure and properly configured. These include S3 repositories and worker instances.
- If you plan to receive email notifications on backup policy results, configure SMTP server settings first. For details, see Configuring Global Email Notification Settings.
- If you plan to create transactionally consistent backups of EC2 instances, check the requirements for application-aware processing and guest scripting.

To create an EC2 backup policy, complete the following steps:

1. Launch the Add Policy wizard.
2. Specify a backup policy name and description.
3. Configure backup source settings.
4. Enable guest processing.
5. Configure backup target settings.
6. Specify a schedule for the backup policy.
7. Review estimated cost for protecting EC2 instances.
8. Specify automatic retry settings and notification settings.
9. Finish working with the wizard.
Step 1. Launch Add Policy Wizard

To launch the **Add Policy** wizard, complete the following steps.

1. Navigate to **Policies > EC2**.
2. Click **Add**.

Step 2. Specify Policy Name and Description

At the **Policy Info** step of the wizard, use the **Name** and **Description** fields to specify a name for the new backup policy and to provide a description for future reference. The name must be unique in Veeam Backup for AWS; the maximum length of the name is 255 characters.
Step 3. Configure Backup Source Settings

At the Sources step of the wizard, specify backup source settings:

1. Select an IAM role whose permissions will be used to perform EC2 instance backup.
2. Select AWS Regions where EC2 instances that you plan to back up reside.
3. Select EC2 instances to back up.
4. Select EBS volumes of the selected EC2 instances to exclude from the backup policy.

Step 3.1 Specify IAM Role

In the IAM Role section of the Sources step of the wizard, you must specify an IAM role whose permissions will be used to access AWS services and resources, and to create cloud-native snapshots of EC2 instances. If you specify an IAM role created in another AWS account, the backup policy will process EC2 instances on which the specified IAM role has permissions in that AWS account.

For an IAM role to be displayed in the IAM Role list, it must be added to Veeam Backup for AWS as described in Adding IAM Roles. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the Add Policy wizard. To add an IAM role, click Add and complete the Add Account wizard.

It is recommended that you check whether the selected IAM role has all the required permissions to perform backup. If the IAM role permissions are insufficient, the backup policy will fail. To run the IAM role permission check, click Check permissions. Veeam Backup for AWS will display the Permissions check window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient, the check will complete with errors. You can view the list of permissions that must be granted to the IAM role in the Missing Permissions column.

You can grant the missing permissions to the IAM role in the IAM Management Console or instruct Veeam Backup for AWS to do it. To learn how to grant permissions to an IAM Role using the IAM Management Console, see AWS Documentation.

To let Veeam Backup for AWS grant the missing permissions:

1. In the Permissions Check window, click Grant.
2. In the Grant permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of the IAM role, and then click Apply.

NOTE

Veeam Backup for AWS does not store one-time access keys in the configuration database.
3. To make sure that the missing permissions were successfully granted, click `Recheck`. 
Step 3.2 Select AWS Regions

In the **Specify region** section of the **Sources** step of the wizard, select AWS Regions where EC2 instances that you plan to back up reside.

1. Click **Choose regions**.
2. In the **Choose Regions** window, select the necessary AWS Regions from the **Available regions** list, and click **Add**.
3. Click **Apply**.

![Choose regions window](image-url)
Step 3.3 Select EC2 Instances

In the **Resources** section of the **Sources** step of the wizard, specify the backup scope — select VM instances that Veeam Backup for AWS will back up:

1. Click **Select resources to protect**.

2. In the **Choose resource protection options** window, choose whether you want to back up all EC2 instances from AWS Regions selected at step 3.2, or only specific EC2 instances.

   If you select the **All resources** option, Veeam Backup for AWS will regularly check for new EC2 instances launched in the selected regions and automatically update the backup policy settings to include these instances in the backup scope.

   If you select the **Protect the following resources** option, you must also specify the instances explicitly:

   a. Use the **Resource type** drop-down list to choose whether you want to add individual EC2 instances or AWS tags to the backup scope.

      If you select the **Tag** option, Veeam Backup for AWS will back up only those EC2 instances that reside in the selected regions under specific AWS tags.

   b. Use the search field to the right of the **Resource type** list to find the necessary resource, and then click **Protect** to add the resource to the backup scope.

      Alternatively, you can click **Browse to select specific sources from the global list**, select check boxes next to the necessary EC2 instances or AWS tags in the list of available resources, and then click **Protect**.

**TIP**

It may take some time for Veeam Backup for AWS to access AWS resources and to populate the list of available EC2 instances or AWS tags. To speed up the data collection process, click **Rescan**.

If you add an AWS tag to the backup scope, Veeam Backup for AWS will regularly check for new EC2 instances assigned the added AWS tag and automatically update the backup policy settings to include these instances in the scope. However, this applies only to EC2 instances from the regions selected at **step 3.2**. If you select a tag assigned to EC2 instances from other regions, these instances will not be protected by the backup policy. To work around the issue, either go back to **step 3.2** and add the missing regions, or create a new backup policy.
4. To save changes made to the backup policy settings, click **Apply**.

![Veeam Backup for AWS policy settings](image)

**Step 3.4 Select EBS Volumes**

In the **Volumes exclusion** section of the **Sources** step of the wizard, you can exclude from processing EBS volumes attached to the selected EC2 instances:

1. Set the **Exclude volumes** toggle to **On**.
2. In the **Choose volumes** window, choose whether you want to exclude system volumes of the selected EC2 instances from processing.
3. To exclude specific EBS volumes, specify the EBS volumes explicitly:
   
   a. Use the **Resource type** list to choose whether you want to exclude individual EBS volumes or AWS tags from the backup scope.

   If you select the **Tag** option, Veeam Backup for AWS will exclude from processing only those EBS volumes that reside in the selected regions under specific AWS tags.

   b. Use the search field to the right of the **Resource type** list to find the necessary resource, and then click **Exclude** to exclude the resource from the backup scope.

   Alternatively, you can click **Browse to select specific sources from the global list**, select check boxes next to the necessary EBS volumes or AWS tags in the list of available resources, and then click **Exclude**.

   **TIP**

   It may take some time for Veeam Backup for AWS to access AWS resources and to populate the list of available EBS volumes or AWS tags. To speed up the data collection process, click **Rescan**.
If you exclude an AWS tag from the backup scope, Veeam Backup for AWS will regularly check for new EBS volumes assigned the excluded AWS tag and automatically update the backup policy settings to exclude these volumes from the scope.

4. To save changes made to the backup policy settings, click Apply.
Step 4. Specify Guest Processing Settings

If you back up EC2 instances that are currently running, at the Guest Processing step of the wizard, you can configure guest processing settings. These settings allow you to specify what actions Veeam Backup for AWS will perform when communicating with the instance guest OS to create transactionally consistent backups.

**NOTE**

To create transactionally consistent backups, Veeam Backup for AWS uses the AWS Systems Manager (SSM) service. For more information on the service, see AWS Documentation.

Particularly, you can specify the following guest processing settings:

- **Enable application-aware processing.** For Windows EC2 instances running VSS-aware applications, you can enable application-aware processing to ensure that the applications will be able to recover successfully, without data loss.

  Application-aware processing is the Veeam technology based on Microsoft VSS. Microsoft VSS is responsible for quiescing applications on EC2 instances and creating a consistent view of application data. For more information on Microsoft VSS, see Microsoft Docs.

- **Enable guest scripting.** For an EC2 instance running applications that do not support Microsoft VSS, you can instruct Veeam Backup for AWS to run custom scripts on the instance before and after the backup operation. For example, Veeam Backup for AWS can execute a pre-snapshot script on the instance to quiesce these applications. This will allow Veeam Backup for AWS to create a transactionally consistent snapshot while no write operations occur on the instance volumes. After the snapshot is created, a post-snapshot script can start the applications again.

**IMPORTANT**

If you plan to create transactionally consistent backups using guest scripting, consider the following:

- Scripts must be created beforehand.
- The backup appliance must have outbound internet access to the SSM service.
- The IAM role used for EC2 instance backup must have permissions to communicate with the SSM service.

Enabling Application-Aware Processing

To enable application-aware processing, at the Guest Processing step of the wizard, set the Enable application aware snapshots toggle to On.

Limitations and Requirements for Application-Aware Processing

If you plan to create transactionally consistent backups using application-aware processing, consider the following:

- Application-aware processing is available only for EC2 instances running Microsoft Windows Server 2008 R2 or later.
- The backup appliance must have outbound internet access to the SSM service.
- The IAM role used for EC2 instance backup must have permissions to communicate with the SSM service.
For more information on the SSM service, see AWS Documentation.

Enabling Guest Scripting

To enable guest scripting for processed EC2 instances, at the Guest Processing step of the wizard:

- For EC2 instances running Linux OS, set the Scripting for Linux instances toggle to On.

  The Specify scripting settings for Linux instances window will open.

- For EC2 instances running Microsoft Windows OS, set the Scripting for Microsoft Windows instances toggle to On.

  The Specify scripting settings for Microsoft Windows instances window will open.

**IMPORTANT**

Supported script formats:

- For EC2 instances running Microsoft Windows OS, Veeam Backup for AWS supports scripts in the EXE, BAT, CMD, WSF, JS, VBS and PS1 file format.

- For EC2 instances running Linux OS, Veeam Backup for AWS supports scripts in the SH file format.

In the opened window, specify pre-snapshot and post-snapshot scripts that must be executed before and after the backup operation:

1. In the Pre-snapshot script section, do the following:

   a. In the Path in guest field, specify a path to the pre-snapshot script file on an EC2 instance.

   b. In the Arguments field, specify additional arguments that must be passed to the script when the script is executed.

      You can use runtime variables as arguments for the script. To see the list of available variables, click Parameters.
NOTE

Veeam Backup for AWS will run the script residing in the specified directory for all EC2 instances added to the backup policy. If you want to execute different scripts for different EC2 instances, ensure that script files uploaded to these instances are located under the same path and have the same name.

2. Repeat step 1 for post-snapshot scripts in the **Post-snapshot script** section.

3. In the **Additional Options** section, choose whether you want to run scripts only while creating snapshot replicas, to proceed with snapshot creation even though scripts are missing on some of the processed instances, and to ignore exit codes returned while executing the scripts.

4. Click **Apply**.
Step 5. Configure Backup Target Settings

At the Targets step of the wizard, you can enable the following additional data protection scenarios:

- Instruct Veeam Backup for AWS to replicate cloud-native snapshots to other AWS accounts or AWS Regions.
- Assign AWS tags to created cloud-native snapshots.
- Instruct Veeam Backup for AWS to create image-level backups.

Configuring Snapshot Replica Settings

If you want to replicate cloud-native snapshots to other AWS accounts or regions, do the following:

1. In the Snapshots section of the Targets step of the wizard, set the Replicate snapshots toggle to On.
2. In the Replication settings window, configure the following mapping settings for each AWS Region where source instances reside:
   a. Select a source AWS Region in the list and click Edit Region Mapping.
   b. In the Edit Region Mapping window, specify the following settings:
      i. From the Target account drop-down list, select an IAM role whose permissions will be used to copy and store cloud-native snapshots in a target AWS Region.
         If you select an IAM role created in another AWS account, the cloud-native snapshot will be copied to the target AWS Region in that AWS account.
      ii. From the Target region drop-down list, select the target AWS Region to which Veeam Backup for AWS must copy cloud-native snapshots.
      iii. If you want to encrypt cloud-native snapshots copied to the target AWS Region, select the Enable encryption check box and choose the necessary AWS Key Management Service (AWS KMS) customer master keys (CMKs) from the Encryption key drop-down list. For a CMK to be displayed in the list of available encryption keys, it must be stored in the AWS Region selected at step 3 and the IAM role specified for the backup operation must have permissions to the CMK. For more information on CMKs, see AWS Documentation.
         Then use the Key Usage drop-down list to choose whether you want to encrypt snapshots for all volumes or only snapshots of the encrypted volumes.

   NOTE
   If the original EBS volume is encrypted, you must enable encryption for replicated snapshots, otherwise the replication process will fail.
iv. Click Save.

To configure mapping for all source AWS Regions at once, click Set Mapping for All Regions and specify settings as described in step 2.b.

Related Resources

AWS Key Management Service concepts

Enabling AWS Tags Assigning

If you want to assign AWS tags to the snapshots and snapshots replicas, in the Snapshots section of the Targets step of the wizard, click the Tags from source volumes will not be copied and custom tags will not be applied link.

1. In the Tags Configurations window, choose whether you want to assign already existing AWS tags or your own custom AWS tags.

   If you set the Add custom tags to created snapshots toggle to On, you must also specify the AWS tags explicitly. To do that, use the Key and Value fields to specify a key and a value for the new custom AWS tag, and then click Add.
2. To save changes made to the backup policy settings, click **Apply**.

**Configuring Image-Level Backup Settings**

If you want to create image-level backups of the selected EC2 instances, do the following:

1. In the **Backups** section of the **Targets** step of the wizard, set the **Enable backups** toggle to **On**.
2. In the **Repositories** window, select an S3 repository where the created image-level backups must be stored, and click **Apply**.

For an S3 repository to be displayed in the **Repository** list, it must be added to Veeam Backup for AWS as described in section **Adding S3 Repositories**.
Step 6. Specify Policy Scheduling Options

You can instruct Veeam Backup for AWS to start the backup policy automatically according to a specific backup schedule. The backup schedule defines how often data of the instances added to the backup policy must be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for AWS allows you to create schedules of the following types:

- **Daily** — the backup policy will create restore points repeatedly throughout a day on specific days.
- **Weekly** — the backup policy will create restore points once a day on specific days.
- **Monthly** — the backup policy will create restore points once a month on a specific day.
- **Yearly** — the backup policy will create restore points once a year on a specific day.

Combining multiple schedule types together allows you to retain restore points for longer periods of time. For more information, see Enabling Harmonized Scheduling.

**NOTE**

If you do not specify the backup schedule, after you configure the backup policy, you will need to start it manually to create EC2 instance backups. For information on how to start backup policies, see Starting and Stopping Policies.

Specifying Daily Schedule

To create a daily schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Daily retention** toggle to **On** and click **Edit daily settings**.
2. In the **Daily schedule** window, select hours when the backup policy must create cloud-native snapshots, snapshot replicas or image-level backups.

   If you want to protect EC2 instance data more frequently, you can instruct the backup policy to create multiple cloud-native snapshots per hour. To do that, click the link to the right of the **Snapshots** hour selection area, and specify the number of cloud-native snapshots that the backup policy must create within an hour.

**NOTE**

Veeam Backup for AWS does not create snapshot replicas and image-level backups independently from cloud-native snapshots. That is why when you select hours for snapshot replicas and image-level backups, the same hours are automatically selected for cloud-native snapshots. To learn how Veeam Backup for AWS performs backup, see How Backup Works.

3. Use the **Run at** drop-down list to choose whether you want the backup policy to run everyday, on workdays (Monday through Friday) or on specific days.
4. In the **Daily retention** section, configure retention policy settings for the daily schedule:
   - For cloud-native snapshots and snapshot replicas, specify the number of restore points that you want to keep in cloud-native snapshot and snapshot replica chains.

      If the restore point limit is exceeded, Veeam Backup for AWS removes the earliest restore point from the chain. For more information, see Retention Policy for Snapshots.
For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain.

If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore point from the chain. For more information, see Retention Policy for Backups.

5. To save changes made to the backup policy settings, click **Apply**.

### Specifying Weekly Schedule

To create a weekly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Weekly retention** toggle to **On** and click **Edit weekly settings**.

2. In the **Weekly schedule** window, select weekdays when the backup policy must create cloud-native snapshots, snapshot replicas or image-level backups.

**NOTE**

Veeam Backup for AWS does not create snapshot replicas and image-level backups independently from cloud-native snapshots. That is why when you select days to create snapshot replicas and image-level backups, the same days are automatically selected for cloud-native snapshots. To learn how Veeam Backup for AWS performs backup, see **How Backup Works**.

3. Use the **Create restore point at** drop-down list to schedule a specific time for the backup policy to run.

4. In the **Weekly retention** section, configure retention policy settings for the weekly schedule:

   - For cloud-native snapshots and snapshot replicas, specify the number of restore points that you want to keep in cloud-native snapshot and snapshot replica chains.

   If the restore point limit is exceeded, Veeam Backup for AWS removes the earliest restore point from the chain. For more information, see **Retention Policy for Snapshots**.
For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain. If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore point from the chain. For more information, see Retention Policy for Backups.

5. To save changes made to the backup policy settings, click Apply.

Specifying Monthly Schedule

To create a monthly schedule for the backup policy, at the Schedule step of the wizard, do the following:

1. Set the Monthly retention toggle to On and click Edit monthly settings.
2. In the Monthly schedule window, select months when the backup policy must create cloud-native snapshots, snapshot replicas or image-level backups.

NOTE

Veeam Backup for AWS does not create snapshot replicas and image-level backups independently from cloud-native snapshots. That is why when you select months to create snapshot replicas and image-level backups, the same months are automatically selected for cloud-native snapshots. To learn how Veeam Backup for AWS performs backup, see How Backup Works.

3. Use the Create restore point at and Run on drop-down lists to schedule a specific time and day for the backup policy to run.

NOTE

If you have selected a specific time for the backup policy to run at the Weekly retention section of the Schedule step of the wizard, you will not be able to change the time for the monthly schedule.
4. In the **Monthly retention** section, configure retention policy settings for the monthly schedule:
   - For cloud-native snapshots and snapshot replicas, specify the number of restore points that you want to keep in cloud-native snapshot and snapshot replica chains.
     - If the restore point limit is exceeded, Veeam Backup for AWS removes the earliest restore point from the chain. For more information, see Retention Policy for Snapshots.
   - For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain.
     - If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore point from the chain. For more information, see Retention Policy for Backups.

5. To save changes made to the backup policy settings, click **Apply**.

### Specifying Yearly Schedule

[This step applies only if you have instructed Veeam Backup for AWS to create image-level backups at the Targets step of the wizard]

To create a yearly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Yearly retention** toggle to **On** and click **Edit yearly settings**.

2. In the **Yearly schedule** window, specify a day, month and time when the backup policy must create image-level backups.
   - For example, if you select **First, Friday, January** and **06:00 PM**, the backup policy will run every first Friday of January at 06:00 PM.
3. In the **Keep backups for** field, specify the number of years for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore from the chain. For more information, see **Retention Policy for Backups**.

4. To save changes made to the backup policy settings, click **Apply**.

---

### Enabling Harmonized Scheduling

When you combine multiple types of schedules, Veeam Backup for AWS applies the harmonization mechanism that allows you to leverage restore points for long-term retentions instead of taking a new restore point every time. The mechanism simplifies the backup schedule, optimizes the backup performance and reduces the cost of retaining restore points.

With harmonized scheduling, Veeam Backup for AWS can keep restore points created according to a daily, weekly or monthly schedule for longer periods of time:

- Cloud-native snapshots and snapshot replicas can be kept for weeks and months.
- Image-level backups can be kept for weeks, months and years.

For Veeam Backup for AWS to use the harmonization mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of restore points, while another schedule will control the process of storing restore points. In terms of harmonized scheduling, Veeam Backup for AWS treats schedules of different types as tiers with the ascending priority: daily, weekly, monthly, yearly. Each restore point is marked with a flag of the related schedule type: the (D) flag is used to mark restore points created daily, (W) — weekly, (M) — monthly, and (Y) — yearly. Veeam Backup for AWS uses these flags to control the retention period for the created restore points. Once a flag of a higher-tier schedule is assigned to a restore point, this restore point can no longer be removed — it is kept for the period defined in the retention settings. When the specified retention period is over, the flag is unassigned from the restore point. If the restore point does not have any other flags assigned, it is removed according to the retention settings of a lower-tier schedule.
Consider the following example. You want a backup policy to create cloud-native snapshots of your critical workloads 3 times a day, to keep 3 daily snapshots in the snapshot chain, and also to keep one of the created snapshots for 2 weeks. In this case, you create 2 schedules when configuring the backup policy settings — daily and weekly:

- In the daily scheduling settings, you select hours and days when snapshots must be created (for example, 7:00 AM, 9:00 AM, and 11:00 AM, Working Days), and specify a number of daily restore points to retain (for example, 3).

Veeam Backup for AWS will propagate these settings to the schedule of a higher tier (which is the weekly schedule in our example).

**Add Policy**

**Daily schedule**
Select number of snapshots, replicas and backups to create.

- Select all  Clear all  Undo

<table>
<thead>
<tr>
<th>AM</th>
<th>PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>11</td>
</tr>
</tbody>
</table>

Snapshots: Total: 3 (1 per hour)
Select mode: Don't create  Create
Run at: Working Days

**Daily retention**
Due to a higher cost, snapshots and replicas are best used for short-term retention. For long-term retention, leverage more cost-effective backups.

Snapshots to keep: 3

Apply  Cancel

Previous  Next  Cancel
In the weekly scheduling settings, you specify which one of the snapshots created by the daily schedule must be retained for a longer period, and choose for how long you want to keep the selected snapshot.

For example, if you want to keep the daily restore point created at 7:00 AM on Monday for 2 weeks, you select 7:00 AM, Monday and specify 2 restore points to retain in the weekly schedule settings.

According to the specified scheduling settings, Veeam Backup for AWS will create cloud-native snapshots in the following way:

1. On the first work day (Monday), a backup session will start at 7:00 AM to create the first restore point. The restore point will be marked with the (D) flag as it was created according to the daily schedule.
   
   Since 7:00 AM, Monday is specified in weekly schedule settings, Veeam Backup for AWS will assign the (W) flag to this restore point.

2. On the same day (Monday), after backup sessions run at 9:00 AM and 11:00 AM, the created restore points will be marked with the (D) flag.
3. On the next work day (Tuesday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (D) flag.

By the moment the backup session completes, the number of restore points with the (D) flag will exceed the retention limit specified in the daily scheduling settings. However, Veeam Backup for AWS will not remove the earliest restore point (7:00 AM, Monday) with the (D) flag from the snapshot chain as this restore point is also marked with a flag of a higher-tier schedule. Instead, Veeam Backup for AWS will unassign the (D) flag from the restore point. This restore point will be kept for the retention period specified in the weekly scheduling settings (that is, for 2 weeks).

![Daily Scheduling Diagram]

4. On the same day (Tuesday), after a backup session runs at 9:00 AM, the number of restore points with the (D) flag will exceed the retention limit once again. Veeam Backup for AWS will remove from the snapshot chain the restore point created at 9:00 AM on Monday as no flags of a higher-tier schedule are assigned to this restore point.

![Daily Scheduling Diagram]

5. Veeam Backup for AWS will continue creating restore points for the next week in the same way as described in steps 1–4.

6. On week 3, after a backup session runs at 7:00 AM on Monday, the number of weekly restore points will exceed the retention limit. Veeam Backup for AWS will unassign the (W) flag from the earliest weekly restore point. Since no other flags are assigned to this restore point, Veeam Backup for AWS will remove this restore point from the snapshot chain.

![Weekly Scheduling Diagram]
Step 7. Review Estimated Cost

This step applies only if you have created a schedule for the backup policy at the **Schedule** step of the wizard.

At the **Cost Estimation** step of the wizard, review the estimated monthly cost of AWS services and resources that will be consumed to protect the instances added to the backup policy. The total estimated cost includes the following:

- The cost of creating and maintaining cloud-native snapshots of the instances.
  
  For each instance included in the backup policy, Veeam Backup for AWS takes into account the instance type, the number of EBS volumes attached, the number of restore points to be kept in the snapshot chain, and the configured scheduling settings.

- The cost of creating snapshot replicas and maintaining them in the target AWS Region.
  
  For each instance included in the backup policy, Veeam Backup for AWS takes into account the instance type, the number of EBS volumes attached, the number of restore points to be kept in the snapshot chain, and the configured scheduling settings.

- The cost of creating and storing in backup repositories image-level backups of the instances.
  
  For each instance included in the backup policy, Veeam Backup for AWS takes into account the machine type, the number of EBS volumes attached, the number of restore points to be kept in the backup chain, and the configured scheduling settings.

- The cost of transferring the instance data between AWS Regions during data protection operations (for example, if a protected instance and the target S3 repository reside in different regions).
  
  If you get a warning message regarding additional costs associated with cross-region data transfer, you can click **View details** to see available cost-effective options.

- The cost of sending API requests to Veeam Backup for AWS during data protection operations.

To calculate the estimated cost, Veeam Backup for AWS uses capabilities of the Amazon Web Services Simple Monthly Calculator.

The estimated cost may occur to be significantly higher due to the backup frequency, cross-region data transfer and snapshot charges. To reduce the cost, you can try the following workarounds:

- To avoid additional costs related to cross-region data transfer, select an S3 repository that resides in the same region as instances that you plan to back up.

- To reduce high snapshot charges, adjust the snapshot retention settings to keep less restore points in the snapshot chain.

- To optimize the cost of storing backups, configure the scheduling settings to run the backup policy less frequently.

For more information on cost estimation, see this Veeam KB article.
NOTE
You can save the cost estimation as a .CSV or .XML file. To do that, click Export and select the necessary format.

Related Resources
How AWS Pricing Works
Step 8. Specify Retry and Email Notification Settings

At the Settings step of the wizard, you can enable automatic retries and specify notification settings for the backup policy.

Automatic Retry Settings

To instruct Veeam Backup for AWS to run the backup policy again if it fails on the first try, do the following:

1. In the Retries section of the step, select the Automatic retry failed policy check box.
2. In the field to the right of the check box, specify the maximum number of attempts to run the backup policy. The time interval between retries is 60 seconds.

When retrying backup policies, Veeam Backup for AWS processes only those instances that failed to be backed up during the previous attempt.

Email Notification Settings

NOTE

To be able to specify email notification settings for the VPC Configuration Backup policy, you must configure the SMTP server settings first. For more information on how to configure the SMTP server settings, see Configuring Global Email Notification Settings.

To instruct Veeam Backup for AWS to send email notifications for the backup policy, do the following:

1. In the Notifications section of the step, set the Enabled toggle to On.
2. In the Email field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses. Do not use spaces after semicolons between the specified email addresses.
3. Use the Notify on list to choose whether you want Veeam Backup for AWS to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.
4. Select the Suppress notifications until the last retry check box to receive a notification about the final backup policy result.

   If you do not select the check box, Veeam Backup for AWS send a notification for every backup policy retry.
NOTE
If you specify the same email recipient in both backup policy notification and global email notification settings, Veeam Backup for AWS will send each notification twice to this recipient.

<table>
<thead>
<tr>
<th>Policy Info</th>
<th>Add Policy</th>
<th>Cost: $8.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Targets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schedule</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost Estimation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notifications</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Settings**
Specify retry times for the policy and email notifications.

**Schedule**
- Automatic retry failed policy: 3 Times
- Automatic retry settings are only applicable on a scheduled run of a policy

**Notifications**
- Enabled: On
- Email: ryan.smith@company.com
- Notify on:
  - Failure
  - Warning
  - Success
- Suppress notifications until the last retry
Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

It is recommended that you run the backup policy check to verify whether specified IAM roles have all the required permissions, and networks settings are configured properly to launch worker instances. To run the backup policy check, click **permissions check**. Veeam Backup for AWS will display the **Policy permissions check** window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient or worker instance settings are not configured properly, the check will complete with errors.

You can grant the missing permissions to the IAM role in the IAM Management Console or instruct Veeam Backup for AWS to do it. To learn how to grant permissions to an IAM Role using the IAM Management Console, see [AWS Documentation](https://docs.aws.amazon.com/iam/latest/reference/)

To let Veeam Backup for AWS grant the missing permissions:

1. In the **Policy permissions check** window, click the **Update role** link.
2. In the **Grant permissions** window, provide one-time access keys of an IAM user that is authorized to update permissions of the IAM role, and then click **Apply**.

**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.

3. After the required permissions are granted, close the **Policy permissions check** window, and then click **Finish** to close the **Add Policy** wizard.

Veeam Backup for AWS will save the configured backup policy.
Fixing Network Issues

If the backup policy check reveals that network settings are not configured properly, Veeam Backup for AWS will not be able to launch worker instances and thus perform image-level backup.

To fix network issues:

1. Close the Policy permissions check window, and then click Finish to close the Add Policy wizard. Veeam Backup for AWS will save the configured backup policy.

2. To prevent the backup policy from failing, disable it. For details, see Disabling and Enabling Backup Policies.

3. Depending on the error message received after the backup policy check, do the following:
   
   o Make sure that network settings are configured for each AWS Region selected at step 3.2. For information on how to configure network settings for AWS Regions, see Configuring Worker Instance Settings.
   
   o Make sure that VPCs specified in network settings for AWS Regions have access to the required AWS services. The required AWS services are listed in the Requirements section.

4. After network issues are fixed, you can enable the backup policy. For details, see Disabling and Enabling Backup Policies.

Creating Snapshots Manually

Veeam Backup for AWS allows you to manually create snapshots of EC2 instances. You can instruct Veeam Backup for AWS to store the created snapshots in the same AWS Regions where the processed EC2 instances reside, or in a different AWS Region or AWS account.

NOTE

Veeam Backup for AWS does not include snapshots created manually in the snapshot chain and does not apply the configured retention policy settings to these snapshots. This means that the snapshots are kept in your AWS environment unless you remove them manually, as described in section Managing Backed-Up EC2 Instance Data.

To manually create a cloud-native snapshot of an EC2 instance, do the following:

1. Navigate to Instances > EC2.

2. Select the necessary instance and click Take Snapshot Now.

   For an EC2 instance to be displayed in the list of available instances:
   
   o The instance must reside in any of the AWS Regions added to a backup policy as described in the section Creating EC2 Backup Policies.
   
   o The IAM role specified in the backup policy settings must have permissions to access the instance.

3. Complete the Take Snapshot wizard:

   a. At the Account step of the wizard, specify an IAM role whose permissions Veeam Backup for AWS will use to create the snapshot.

      For an IAM role to be displayed in the list, it must be added to Veeam Backup for AWS as described in section Adding IAM Roles.
b. At the **Snapshot Mode** step of the wizard, choose whether you want to store the snapshot in the same AWS Region where the processed EC2 instance resides, or in another AWS Region or AWS account.

c. [Applies if you have selected the **Remote region** option] At the **Remote Settings** step of the wizard, choose an IAM role whose permissions will be used to copy and store the snapshot in a target AWS Region, the target AWS Region and specify whether to encrypt the copied snapshot.

d. At the **Tags** step of the wizard, choose whether you want to assign AWS tags to the created snapshot.
   - To assign already existing AWS tags from the EBS volumes of the processed EC2 instance, select the **Copy Tags from source volume** check box.
   - To assign your own custom AWS tags, click **Add** and specify the tags explicitly. To do that, in the **Add additional Tag** window, specify a key and a value for the new AWS tag, and then click **Apply**.

e. At the **Summary** step of the wizard, review summary information and click **Finish**.
Performing RDS Instance Backup

Veeam Backup for AWS backs up data of RDS instances as prescribed by backup policies. A backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where backups must be stored, when the backup process must start and so on.

You can create multiple RDS backup policies. One backup policy can be used to process multiple RDS instances within different AWS Regions, but you can protect each RDS instance with one backup policy at a time. If an RDS instance is added to more than one backup policy, it will be processed only by a backup policy that has the highest priority. Other backup policies will skip this RDS instance from processing. For information on how to set a priority for a backup policy, see Setting Policy Priority.

To schedule data protection tasks to run automatically, create backup policies. For each protected RDS instance, you can also take a cloud-native snapshot manually when needed.

IMPORTANT
Veeam Backup for AWS does not support backup of RDS DB instances running the Amazon Aurora relational database engine.
Creating RDS Backup Policies

One backup policy can be used to process one or more instances within one AWS account. The scope of data that you can protect in an AWS account is limited by permissions of an IAM role that is specified in backup policy settings.

**NOTE**

Before you create an RDS backup policy, if you plan to receive email notifications on backup policy results, configure SMTP server settings first. For more information, see Configuring Global Email Notification Settings.

To create an RDS backup policy, complete the following steps:

1. Launch the Add Policy wizard.
2. Specify a backup policy name and description.
3. Configure backup source settings.
4. Configure backup target settings.
5. Specify a schedule for the backup policy.
6. Review estimated cost for protecting RDS instances.
7. Specify automatic retry settings and notification settings.
8. Finish working with the wizard.
Step 1. Launch Add Policy Wizard

To launch the Add Policy wizard, complete the following steps.

1. Navigate to Policies > RDS.
2. Click Add.

Step 2. Specify Policy Name and Description

At the Policy Info step of the wizard, use the Name and Description fields to specify a name for the new backup policy and to provide a description for future reference. The name must be unique in Veeam Backup for AWS; the maximum length of the name is 255 characters.
Step 3. Configure Backup Source Settings

At the **Sources** step of the wizard, specify backup source settings:

1. Select an IAM role whose permissions will be used to perform RDS instance backup.
2. Select AWS Regions where RDS instances that you plan to back up reside.
3. Select RDS instances to back up.

### Step 3.1 Specify IAM Role

In the **IAM Role** section of the **Sources** step of the wizard, you must specify an IAM role whose permissions will be used to access AWS services and resources, and to create cloud-native snapshots of RDS instances. If you specify an IAM role created in another AWS account, the backup policy will process RDS instances on which the specified IAM role has permissions in that AWS account.

For an IAM role to be displayed in the **IAM Role** list, it must be added to Veeam Backup for AWS as described in [Adding IAM Roles](#). If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the **Add Policy** wizard. To add an IAM role, click **Add** and complete the **Add Account** wizard.

It is recommended that you check whether the selected IAM role has all the required permissions to perform backup. If the IAM role permissions are insufficient, the backup policy will fail.

To run the IAM role permission check, click **Check permissions**. Veeam Backup for AWS will display the **Permissions check** window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient, the check will complete with errors. You can view the list of permissions that must be granted to the IAM role in the **Missing Permissions** column.

You can grant the missing permissions to the IAM role in the IAM Management Console or instruct Veeam Backup for AWS to do it. To learn how to grant permissions to an IAM Role using the IAM Management Console, see [AWS Documentation](#).
Step 3.2 Select AWS Regions

In the Specify region section of the Sources step of the wizard, choose AWS Regions where RDS instances that you plan to back up reside.

1. Click Choose regions.
2. In the Choose regions window, select the necessary regions, click Add to include them in the backup policy.
3. Click Apply.

Step 3.3 Select RDS DB Instances

In the Resources section of the Sources step of the wizard, specify the backup scope — select RDS instances that Veeam Backup for AWS will back up:

1. Click Select resources to protect.
2. In the Choose resource protection options window, choose whether you want to back up all RDS instances from AWS Regions selected at step 3, or only specific RDS instances.

   If you select the All resources option, Veeam Backup for AWS will regularly check for new RDS instances launched in the selected regions and automatically update the backup policy settings to include these instances in the backup scope.

   If you select the Protect the following resources option, you must also specify the instances explicitly:

   a. Use the Resource type drop-down list to choose whether you want to add individual RDS instances or AWS tags to the backup scope.

      If you select the Tag option, Veeam Backup for AWS will back up only those instances from the selected AWS Regions that are assigned specific tags.
b. Use the search field to the right of the Resource type list to find the necessary resource, and then click Protect to add the resource to the backup scope.

Alternatively, you can click Browse to select specific sources from the global list, select check boxes next to the necessary RDS instances or AWS tags in the list of available resources, and then click Protect.

**NOTE**

It may take some time for Veeam Backup for AWS to access AWS resources and to populate the list of available RDS instances or AWS tags. To speed up the data collection process, click Rescan.

If you add an AWS tag to the backup scope, Veeam Backup for AWS will regularly check for new RDS instances assigned the added AWS tag and automatically update the backup policy settings to include these instances in the scope. However, this applies only to RDS instances from the AWS Regions selected at step 3. If you select an AWS tag assigned to RDS instances from other AWS Regions, these instances will not be protected by the backup policy. To work around the issue, either go back to step 3 and add the missing AWS Regions, or create a new backup policy.

3. Click Apply.

---

**Step 4. Configure Backup Target Settings**

At the Targets step of the wizard, you can enable the following additional data protection scenarios:

- Instruct Veeam Backup for AWS to replicate cloud-native snapshots to other AWS accounts or AWS Regions.

- Assign AWS tags to created cloud-native snapshots.

**Configuring Snapshot Replica Settings**

If you want to replicate cloud-native snapshots to other AWS accounts or regions, do the following:

1. In the Snapshots section of the Targets step of the wizard, set the Replicate snapshots toggle to On.
2. In the **Replication settings** window, configure the following mapping settings for each AWS Region where source instances reside:

   a. Select a source AWS Region in the list and click **Edit Region Mapping**.

   b. In the **Edit Region Mapping** window, specify the following settings:

      i. From the **Target account** drop-down list, select an IAM role whose permissions will be used to copy and store cloud-native snapshots in a target AWS Region.

         If you select an IAM role created in another AWS account, the cloud-native snapshot will be copied to the target AWS Region in that AWS account.

      ii. From the **Target region** drop-down list, select the target AWS Region to which Veeam Backup for AWS must copy cloud-native snapshots

      iii. If you want to encrypt cloud-native snapshots copied to the target AWS Region, select the **Enable encryption** check box and choose the necessary AWS Key Management Service (AWS KMS) customer master keys (CMKs) from the **Encryption key** drop-down list. For a CMK to be displayed in the list of available encryption keys, it must be stored in the AWS Region selected at step 3 and the IAM role specified for the backup operation must have permissions to the CMK. For more information on CMKs, see AWS Documentation.

         Then use the **Key Usage** drop-down list to choose whether you want to encrypt snapshots for all instances or only snapshots of the encrypted instances.

         **NOTE**

         If the original RDS instance is encrypted, you must enable encryption for replicated snapshots, otherwise the replication process will fail.

      iv. Click **Save**.

   To configure mapping for all source AWS Regions at once, click **Set Mapping for All Regions** and specify settings as described in step 2.b.
Enabling AWS Tags Assigning

If you want to assign AWS tags to the snapshots and snapshots replicas, in the Snapshots section of the Targets step of the wizard, click the Tags from source volumes will not be copied and custom tags will not be applied link.

1. In the Tags Configurations window, choose whether you want to assign already existing AWS tags from source RDS instances or your own custom AWS tags.

   If you set the Add custom tags to created snapshots toggle to On, you must also specify the AWS tags explicitly. To do that, use the Key and Value fields to specify a key and a value for the new custom AWS tag, and then click Add.

2. To save changes made to the backup policy settings, click Apply.
Step 5. Specify Policy Scheduling Options

You can instruct Veeam Backup for AWS to start the backup policy automatically according to a specific backup schedule. The backup schedule defines how often data of the instances added to the backup policy must be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for AWS allows you to create schedules of the following types:

- **Daily** — the backup policy will create restore points repeatedly throughout a day on specific days.
- **Weekly** — the backup policy will create restore points once a day on specific days.
- **Monthly** — the backup policy will create restore points once a month on a specific day.

Combining multiple schedule types together allows you to retain restore points for longer periods of time. For more information, see Enabling Harmonized Scheduling.

**NOTE**

If you do not specify the backup schedule, after you configure the backup policy, you will need to start it manually to create RDS instance backups. For information on how to start backup policies, see Starting and Stopping Policies.

Specifying Daily Schedule

To create a daily schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Daily retention** toggle to **On** and click **Edit daily settings**.
2. In the **Daily schedule** window, select hours when the backup policy must create cloud-native snapshots and snapshot replicas.
   
   If you want to protect RDS instance data more frequently, you can instruct the backup policy to create multiple cloud-native snapshots per hour. To do that, click the link to the right of the **Snapshots hour** selection area, and specify the number of cloud-native snapshots that the backup policy must create within an hour.

   **NOTE**

   Veeam Backup for AWS does not create snapshot replicas independently from cloud-native snapshots. That is why when you select hours to create snapshot replicas, the same hours are automatically selected for cloud-native snapshots. To learn how Veeam Backup for AWS performs backup, see How Backup Works.

3. Use the **Run at** drop-down list to choose whether you want the backup policy to run everyday, on workdays (Monday through Friday) or on specific days.
4. In the **Daily retention** section, for cloud-native snapshots and snapshot replicas, specify the number of restore points that you want to keep in cloud-native snapshot and snapshot replica chains.
   
   If the restore point limit is exceeded, Veeam Backup for AWS removes the earliest restore point from the chain. For more information, see Retention Policy for Snapshots.
5. To save changes made to the backup policy settings, click **Apply**.

### Specifying Weekly Schedule

To create a weekly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Weekly retention** toggle to **On** and click **Edit weekly settings**.

2. In the **Weekly schedule** window, select weekdays when the backup policy must create cloud-native snapshots and snapshot replicas.

**NOTE**

Mind that Veeam Backup for AWS does not create snapshot replicas independently from cloud-native snapshots. That is why when you select days to create snapshot replicas, the same days are automatically selected for cloud-native snapshots. To learn how Veeam Backup for AWS performs backup, see [How Backup Works](#).

3. Use the **Create restore point at** drop-down list to schedule a specific time for the backup policy to run.

4. In the **Weekly retention** section, for cloud-native snapshots and snapshot replicas, specify the number of restore points that you want to keep in cloud-native snapshot and snapshot replica chains.

   If the restore point limit is exceeded, Veeam Backup for AWS removes the earliest restore point from the chain. For more information, see [Retention Policy for Snapshots](#).
5. To save changes made to the backup policy settings, click **Apply**.

### Specifying Monthly Schedule

To create a monthly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Monthly retention** toggle to **On** and click **Edit monthly settings**.

2. In the **Monthly schedule** window, select months when the backup policy must create cloud-native snapshots and snapshot replicas.

   **NOTE**
   
   Mind that Veeam Backup for AWS does not create snapshot replicas independently from cloud-native snapshots. That is why when you select months to create snapshot replicas, the same months are automatically selected for cloud-native snapshots. To learn how Veeam Backup for AWS performs backup, see **How Backup Works**.

3. Use the **Create restore point at** and **Run on** drop-down lists to schedule a specific time and day for the backup policy to run.

   **NOTE**
   
   If you have selected a specific time for the backup policy to run at the **Weekly retention** section of the **Schedule** step of the wizard, you will not be able to change the time for the monthly schedule.

4. In the **Monthly retention** section, for cloud-native snapshots and snapshot replicas, specify the number of restore points that you want to keep in cloud-native snapshot and snapshot replica chains.

   If the restore point limit is exceeded, Veeam Backup for AWS removes the earliest restore point from the chain. For more information, see **Retention Policy for Snapshots**.
5. To save changes made to the backup policy settings, click **Apply**.

Enabling Harmonized Scheduling

When you combine multiple types of schedules, Veeam Backup for AWS applies the harmonization mechanism that allows you to leverage restore points for long-term retentions instead of taking a new restore point every time. The mechanism simplifies the backup schedule, optimizes the backup performance and reduces the cost of retaining restore points.

With harmonized scheduling, Veeam Backup for AWS can keep restore points created according to a daily or weekly schedule for longer periods of time: cloud-native snapshots and snapshot replicas can be kept for weeks and months.

For Veeam Backup for AWS to use the harmonization mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of restore points, while another schedule will control the process of storing restore points. In terms of harmonized scheduling, Veeam Backup for AWS treats schedules of different types as tiers with the ascending priority: daily, weekly, monthly, yearly. Each restore point is marked with a flag of the related schedule type: the (D) flag is used to mark restore points created daily, (W) — weekly, (M) — monthly, and (Y) — yearly. Veeam Backup for AWS uses these flags to control the retention period for the created restore points. Once a flag of a higher-tier schedule is assigned to a restore point, this restore point can no longer be removed — it is kept for the period defined in the retention settings. When the specified retention period is over, the flag is unassigned from the restore point. If the restore point does not have any other flags assigned, it is removed according to the retention settings of a lower-tier schedule.
Consider the following example. You want a backup policy to create cloud-native snapshots of your critical workloads 3 times a day, to keep 3 daily snapshots in the snapshot chain, and also to keep one of the created snapshots for 2 weeks. In this case, you create 2 schedules when configuring the backup policy settings — daily and weekly:

- In the daily scheduling settings, you select hours and days when snapshots must be created (for example, 7:00 AM, 9:00 AM, and 11:00 AM, Working Days), and specify a number of daily restore points to retain (for example, 3).

Veeam Backup for AWS will propagate these settings to the schedule of a higher tier (which is the weekly schedule in our example).
In the weekly scheduling settings, you specify which one of the snapshots created by the daily schedule must be retained for a longer period, and choose for how long you want to keep the selected snapshot.

For example, if you want to keep the daily restore point created at 7:00 AM on Monday for 2 weeks, you select 7:00 AM, Monday and specify 2 restore points to retain in the weekly schedule settings.

According to the specified scheduling settings, Veeam Backup for AWS will create cloud-native snapshots in the following way:

1. On the first work day (Monday), a backup session will start at 7:00 AM to create the first restore point. The restore point will be marked with the (D) flag as it was created according to the daily schedule.

   Since 7:00 AM, Monday is specified in weekly schedule settings, Veeam Backup for AWS will assign the (W) flag to this restore point.

2. On the same day (Monday), after backup sessions run at 9:00 AM and 11:00 AM, the created restore points will be marked with the (D) flag.
3. On the next work day (Tuesday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (D) flag.

   By the moment the backup session completes, the number of restore points with the (D) flag will exceed the retention limit specified in the daily scheduling settings. However, Veeam Backup for AWS will not remove the earliest restore point (7:00 AM, Monday) with the (D) flag from the snapshot chain as this restore point is also marked with a flag of a higher-tier schedule. Instead, Veeam Backup for AWS will unassign the (D) flag from the restore point. This restore point will be kept for the retention period specified in the weekly scheduling settings (that is, for 2 weeks).

   ![Diagram 1](image1)

4. On the same day (Tuesday), after a backup session runs at 9:00 AM, the number of restore points with the (D) flag will exceed the retention limit once again. Veeam Backup for AWS will remove from the snapshot chain the restore point created at 9:00 AM on Monday as no flags of a higher-tier schedule are assigned to this restore point.

   ![Diagram 2](image2)

5. Veeam Backup for AWS will continue creating restore points for the next week in the same way as described in steps 1–4.

6. On week 3, after a backup session runs at 7:00 AM on Monday, the number of weekly restore points will exceed the retention limit. Veeam Backup for AWS will unassign the (W) flag from the earliest weekly restore point. Since no other flags are assigned to this restore point, Veeam Backup for AWS will remove this restore point from the snapshot chain.

   ![Diagram 3](image3)
Step 6. Review Estimated Cost

[This step applies only if you have created a schedule for the backup policy at the Schedule step of the wizard]

At the Cost Estimation step of the wizard, review the estimated monthly cost of AWS services and resources that will be consumed to protect the instances added to the backup policy. The total estimated cost includes the following:

- The cost of creating and maintaining cloud-native snapshots of the instances.
  For each instance included in the backup policy, Veeam Backup for AWS takes into account the instance class, the number of restore points to be kept in the snapshot chain, and the configured scheduling settings.

- The cost of creating snapshot replicas and maintaining them in the target AWS Region.
  For each instance included in the backup policy, Veeam Backup for AWS takes into account the instance class, the number of restore points to be kept in the snapshot chain, and the configured scheduling settings.

- The cost of sending API requests to Veeam Backup for AWS during data protection operations.

To calculate the estimated cost, Veeam Backup for AWS uses capabilities of the Amazon Web Services Simple Monthly Calculator.

The estimated cost may occur to be significantly higher due to the backup frequency, cross-region data transfer and snapshot charges. To reduce the cost, you can adjust the snapshot retention settings to keep less restore points in the snapshot chain.

For more information on cost estimation, see this Veeam KB article.

NOTE
You can save the cost estimation as a .CSV or .XML file. To do that, click Export and select the necessary format.
Step 7. Specify Retry and Email Notification Settings

At the Settings step of the wizard, you can enable automatic retries and specify notification settings for the backup policy.

Automatic Retry Settings

To instruct Veeam Backup for AWS to run the backup policy again if it fails on the first try, do the following:

1. In the Retries section of the step, select the Automatic retry failed policy check box.
2. In the field to the right of the check box, specify the maximum number of attempts to run the backup policy. The time interval between retries is 60 seconds.

When retrying backup policies, Veeam Backup for AWS processes only those instances that failed to be backed up during the previous attempt.

Email Notification Settings

**NOTE**

To be able to specify email notification settings for the VPC Configuration Backup policy, you must configure the SMTP server settings first. For more information on how to configure the SMTP server settings, see Configuring Global Email Notification Settings.

To instruct Veeam Backup for AWS to send email notifications for the backup policy, do the following:

1. In the Notifications section of the step, set the Enabled toggle to On.
2. In the Email field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses. Do not use spaces after semicolons between the specified email addresses.
3. Use the Notify on list to choose whether you want Veeam Backup for AWS to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.
4. Select the Suppress notifications until the last retry check box to receive a notification about the final backup policy result.

   If you do not select the check box, Veeam Backup for AWS send a notification for every backup policy retry.
NOTE

If you specify the same email recipient in both backup policy notification and global email notification settings, Veeam Backup for AWS will send each notification twice to this recipient.

Step 8. Finish Working with Wizard

At the Summary step of the wizard, review configuration information and click Finish.

It is recommended that you run the backup policy check to verify whether specified IAM roles have all the required permissions, and networks settings are configured properly to launch worker instances. To run the backup policy check, click permissions check. Veeam Backup for AWS will display the Policy permissions check window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient or worker instance settings are not configured properly, the check will complete with errors.

You can grant the missing permissions to the IAM role in the IAM Management Console or instruct Veeam Backup for AWS to do it. To learn how to grant permissions to an IAM Role using the IAM Management Console, see AWS Documentation.

To let Veeam Backup for AWS grant the missing permissions:

1. In the Policy permissions check window, click the Update role link.

2. In the Grant permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of the IAM role, and then click Apply.
Veeam Backup for AWS does not store one-time access keys in the configuration database.

Creating Snapshots Manually

Veeam Backup for AWS allows you to manually create snapshots of RDS instances. You can instruct Veeam Backup for AWS to store the created snapshots in the same AWS Regions where the processed RDS instances reside, or in a different AWS Region or AWS account.

Veeam Backup for AWS does not include snapshots created manually in the snapshot chain and does not apply the configured retention policy settings to these snapshots. This means that the snapshots are kept in your AWS environment unless you remove them manually, as described in section Managing Backed-Up RDS Instance Data.

To manually create a cloud-native snapshot of an RDS instance, do the following:

1. Navigate to **Instances** > **RDS**.
2. Select the necessary instance and click **Take Snapshot Now**.

   For an RDS instance to be displayed in the list of available instances:
   - The instance must reside in any of the AWS Regions added to a backup policy as described in the section Creating RDS Backup Policies.
   - The IAM role specified in the backup policy settings must have permissions to access the instance.
3. Complete the **Take Snapshot** wizard:
   a. At the **Account** step of the wizard, specify an IAM role whose permissions Veeam Backup for AWS will use to create the snapshot.
      
      For an IAM role to be displayed in the list, it must be added to Veeam Backup for AWS as described in section **Adding IAM Roles**.
   b. At the **Snapshot Mode** step of the wizard, choose whether you want to store the snapshot in the same AWS Region where the processed RDS instance resides, or in another AWS Region or AWS account.
   c. [Applies if you have selected the **Remote region** option] At the **Remote Settings** step of the wizard, choose an IAM role whose permissions will be used to copy and store the snapshot in a target AWS Region, the target AWS Region and specify whether to encrypt the copied snapshot.
   d. At the **Tags** step of the wizard, choose whether you want to assign AWS tags to the created snapshot.
      
      - To assign already existing AWS tags from the source RDS instance, select the **Copy Tags from source RDS instance** check box.
      - To assign your own custom AWS tags, click **Add** and specify the tags explicitly. To do that, in the **Add additional Tag** window, specify a key and a value for the new AWS tag, and then click **Apply**.
   e. At the **Summary** step of the wizard, review summary information and click **Finish**.

![Veeam Backup for AWS](image-url)
Performing VPC Configuration Backup

To protect the Amazon VPC configuration and settings, Veeam Backup for AWS comes with a preconfigured VPC Configuration Backup policy. With this policy, you can protect VPC configurations of AWS Regions in your AWS account.

The VPC Configuration Backup policy is disabled by default. To start protecting your Amazon VPC configuration, edit backup policy settings and enable the policy.

**IMPORTANT**
Veeam Backup for AWS does not support backup of the following VPC configuration components: VPC Traffic Mirroring, AWS Network Firewall, VPC Flow Logs, carrier gateways and customer IP pools.

Editing VPC Configuration Backup Policy

To configure the VPC Configuration Backup policy settings, complete the following steps:

1. Launch the VPC Configuration Backup wizard.
2. Select AWS Regions to protect.
3. Specify S3 repository to store an additional backup copy.
5. Specify automatic retry settings and notification settings.
6. Finish working with the wizard.
Step 1. Launch VPC Configuration Backup Wizard

To launch the VPC Configuration Backup wizard, complete the following steps.

1. Navigate to Policies > VPC.
2. Click Edit.

Step 2. Select AWS Regions

At the Regions step of the wizard, select AWS Regions whose VPC configuration you want to back up.

Veeam Backup for AWS allows you to automatically collect and back up VPC configuration data for all AWS Regions selected for EC2 and RDS backup policies. To do that, enable automatic protection for AWS Regions. To retrieve VPC configurations of all automatically protected AWS Regions, Veeam Backup for AWS will use permissions of IAM roles specified in the settings of backup policies that protect instances residing in these AWS Regions.

You can also configure the VPC Configuration Backup policy to protect configuration data for AWS Regions that are not specified in the settings of any backup policy, or choose another IAM role whose permissions Veeam Backup for AWS will use to collect the VPC configuration data of the automatically protected AWS Regions. To do that, manually add AWS Regions to the VPC Backup policy and configure backup settings for them.

Enabling Automatic Protection

To instruct Veeam Backup for AWS to protect VPC configuration of all AWS Regions specified in EC2 and RDS backup policy settings, in the Automatically Protected Regions section, set the Automatically collect VPC settings toggle to On.

To retrieve VPC configurations of all automatically protected AWS Regions, Veeam Backup for AWS will use permissions of IAM roles specified in the settings of backup policies that protect instances residing in these AWS Regions. It is recommended that you check whether IAM roles whose permissions EC2 and RDS backup policies use to perform data protection operations have all the required permissions to perform Amazon VPC configuration backup. If the IAM role permissions are insufficient, the backup policy will fail.

To run the IAM role permission check:

1. In the Automatically Protected Regions section, click the Discovered regions link.
2. In the **Discovered regions** window, select the IAM role whose permissions you want to check.

3. Click **Check permissions**.

   Veeam Backup for AWS will display the **AWS Permission Check for IAM Role** window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient, the check will complete with errors. You can view the list of permissions that must be granted to the IAM role in the **Missing Permissions** column.

   You can grant the missing permissions to the IAM role in the IAM Management Console or instruct Veeam Backup for AWS to do it. To learn how to grant permissions to an IAM Role using the IAM Management Console, see [AWS Documentation](https://aws.amazon.com). To let Veeam Backup for AWS grant the missing permissions:

   a. In the **AWS Permission check for IAM Role** window, click **Grant**.

   b. In the **Grant permissions window**, provide one-time access keys of an IAM user that is authorized to update permissions of the IAM role, and then click **Apply**.

   **NOTE**

   Veeam Backup for AWS does not store one-time access keys in the configuration database.

   c. To make sure that the missing permissions were successfully granted, click **Recheck**.

---

### Adding AWS Regions Manually

To add an AWS Region to the VPC Backup policy, or to choose another IAM role for collecting VPC configuration data, do the following:

1. In the **Additional regions** section, click **Add**.

2. In the **Configure Account Settings** window, from the **IAM Role** drop-down list, select an IAM role whose permissions Veeam Backup for AWS must use to perform Amazon VPC configuration backup. In the **Account** field, the ID of the AWS account in which the IAM role was created will be displayed.
3. In the **Regions** section, select the necessary AWS Regions from the **Available regions** list on the left, and then click **Add**.

4. Click **Apply**.

5. To check whether IAM role specified for the selected AWS Regions has all the required permissions to perform Amazon VPC configuration backup, in the **Additional regions** section, click **Check Permissions**.

You can add, edit or remove additional AWS Regions from the VPC Backup policy.
Step 3. Enable Additional Backup Copy

By default, Veeam Backup for AWS store VPC configuration backups in the Veeam Backup for AWS database. You can instruct Veeam Backup for AWS to save additional VPC configuration backup copies to an S3 repository. To do that:

1. At the Target step of the wizard, set the Enable additional copy toggle to On.
2. In the Repository window, specify an S3 repository that will be used to store the additional configuration backup copies.
3. Click Apply.

If you want to encrypt the VPC configuration data stored in an S3 repository, enable encryption on the repository level. For more information, see Adding S3 Repository.
Step 4. Configure Retention Settings

At the **Retention** step of the wizard, specify retention settings for VPC configuration backups.

1. Click the **Collect data** link.
2. In the **Daily Retention** window, specify how often the data must be backed up and for how long the backups must be stored.
Step 5. Specify Email Notification Settings

At the **Settings** step of the wizard, you can specify email notification settings for the VPC Backup policy.

**NOTE**
To be able to specify email notification settings for the VPC Configuration Backup policy, you must configure the SMTP server settings first. For more information on how to configure the SMTP server settings, see **Configuring Global Email Notification Settings**.

To instruct Veeam Backup for AWS to send email notifications for the backup policy, do the following:

1. In the **Notifications** section, set the **Receive daily report** toggle to **On**.
2. In the **Email** field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses. Do not use spaces after semicolons between the specified email addresses.
3. Use the **Notify on** list to choose whether you want Veeam Backup for AWS to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.

**NOTE**
If you specify the same email recipient in both backup policy notification and **global email notification settings**, Veeam Backup for AWS will send each notification twice to this recipient.
Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.
Enabling and Disabling VPC Configuration Backup Policy

By default, Veeam Backup for AWS comes with the disabled VPC Configuration Backup Policy. You can manually start or enable the disabled backup policy at any time you need.

To enable or disable the VPC Configuration Backup policy, do the following:

1. Navigate to Policies > VPC.
2. Click Enable or Disable.
Starting and Stopping VPC Configuration Backup Policy

You can start the VPC Configuration Backup policy manually, for example, if you want to create an additional restore point in the backup chain and do not want to modify the configured backup policy schedule. You can also stop a backup policy if the backup process is about to take long, and you do not want the policy to have an impact on the production environment during business hours.

To start or stop a backup policy, do the following:

1. Navigate to Policies > VPC.
2. Click Start or Stop.
Managing EC2 and RDS Backup Policies

You can manage and edit created EC2 and RDS backup policies, and view each backup policy details in Veeam Backup for AWS. You can also remove backup policies that you do not use anymore, export existing or import new backup policies.

Starting and Stopping Policies

You can start a backup policy manually, for example, if you want to create an additional restore point in the snapshot or backup chain and do not want to modify the configured backup policy schedule. You can also stop a backup policy if processing of an instance is about to take too long, and you do not want the policy to have an impact on the production environment during business hours.

To start or stop a backup policy, do the following:

1. Navigate to Policies.
2. Switch to the necessary tab and select check boxes next to the necessary backup policies.
3. Click Start or Stop.
Disabling and Enabling Policies

By default, Veeam Backup for AWS runs all created backup policies according to the specified schedules. However, you can temporarily disable a backup policy so that Veeam Backup for AWS does not run the backup policy automatically. You will still be able to manually start or enable the disabled backup policy at any time you need.

To enable or disable a backup policy, do the following:

1. Navigate to Policies.
2. Switch to the necessary tab and select check boxes next to the necessary backup policies.
3. Click Disable or Enable.
Setting Policy Priority

You can set priority for backup policies created in Veeam Backup for AWS. If an instance is included into several backup policies, it will be processed only by one backup policy that has the highest priority.

To set priority for backup policies:

1. In the main menu on the left, navigate to Policies.
2. Switch to the necessary tab and, at the top of the backup policies list, click Policy Priority.
3. In the Priority Order window, use the Up and Down arrows to set priority for backup policies.

   The first backup policy in the list will have the highest priority.
Editing Policy Settings

You can edit backup policies created in Veeam Backup for AWS. For example, you may want to add some instances to a backup policy, change a backup policy description and so on.

To edit backup policy settings:

1. **Navigate to Policies.**
2. Switch to the necessary tab and select the check box next to the backup policy whose settings you want to edit.
3. **Click Edit.**
4. Edit backup policy settings as described in *Creating EC2 Backup Policies* or *Creating RDS Backup Policies.*
Exporting and Importing Policies

Veeam Backup for AWS allows you to use settings of an existing backup policy as a template for creating other backup policies. You can export a backup policy to a .JSON file, modify the necessary settings in the file, and then import the policy to the same or a different backup appliance.

Exporting Backup Policies

To export a backup policy to a .JSON file:

1. Navigate to **Policies**.
2. Switch to the necessary tab and select the check box next to the backup policy you want to export.
3. Click **Advanced > Export Policy**.

Veeam Backup for AWS will save the backup policy settings as a single .JSON file to the default download directory on the local machine.

Importing Backup Policies

To import a backup policy from a .JSON file:

1. Navigate to **Policies**.
2. Switch to the necessary tab and click **Advanced > Import Policy**.
3. In the **Import Policy** window, specify a name for the imported backup policy, paste the content of the necessary .JSON file, and click **Apply**.
Managing Backed-Up Data

You can view and manage data of the backed-up EC2, RDS instances and Amazon VPC configuration backups.

Managing Backed-Up EC2 Instance Data

For each backed-up EC2 instance, Veeam Backup for AWS creates a record in the configuration database with the following set of properties:

- **Instance** — a name of an EC2 instance.
- **Policy** — a name of the backup policy that processed the EC2 instance.
- **Restore Points** — a number of restore points created for the EC2 instance.
- **Latest Restore Point** — the date and time of the latest restore point that was created for the EC2 instance.
- **Instance Size** — a size of all EBS volumes attached to the EC2 instance.
- **Region** — an AWS Region in which the EC2 instance resides.
- **File-level Recovery URL** — a link to the FLR for Veeam Backup browser.

The link appears when the restore session is started for the file-level restore process. The link contains a public DNS name of the worker instance hosting the FLR for Veeam Backup browser and authentication information used to access this worker instance.

- **Operating System** — an operating system running on the EC2 instance.
Removing Backups and Snapshots

Veeam Backup for AWS applies the configured retention policy settings to automatically remove cloud-native snapshots, snapshot replicas and image-level backups created by backup policies. If necessary, you can also remove the backed-up data manually.

**IMPORTANT**

Do not delete backup files from Amazon S3 buckets in the AWS Management Console. If some file in a backup chain is missing, you will not be able to roll back EC2 instance data to the necessary state.

To remove backed-up data manually, do the following:

1. Navigate to **Protected Data > EC2**.
2. Select EC2 instances whose data you want to remove.
3. Click **Remove** and select either of the following options:
   - **Snapshots** — to remove cloud-native snapshots created for the selected EC2 instances by backup policies.
   - **Snapshots > Manual** — to remove cloud-native snapshots created for the selected EC2 instances manually.
     
     If you want to remove only specific cloud-native snapshots, follow the instructions provided in section Removing Snapshots Created Manually.
   - **Snapshots > Remote** — to remove snapshot replicas created for the selected EC2 instances by backup policies.
   - **Snapshots > All** — to remove all cloud-native snapshots and snapshot replicas created for the selected EC2 instances both by backup policies and manually.
   - **Backups** — to remove all image-level backups created for the selected EC2 instances.
   - **Snapshots and backups** — to remove cloud-native snapshots, snapshot replicas, and image-level backups created for the selected EC2 instances.
Removing Snapshots Created Manually

If you want to remove specific cloud-native snapshots created for an EC2 instance manually, do the following:

1. Navigate to Protected Data > EC2.
2. Select the necessary instance, and click the link in the Restore Points column.
3. In the Available Restore Points window, select a snapshot that you want to remove, and click Remove Manual Snapshot.
Managing Backed-Up RDS Instance Data

For each backed-up RDS instance, Veeam Backup for AWS creates a record in the configuration database with the following set of properties:

- **Instance** — a name of an RDS instance.
- **Policy** — a name of the backup policy that processed the RDS instance.
- **Snapshots** — a number of snapshots created for the RDS instance.

**NOTE**

Veeam Backup for AWS displays all existing snapshots of RDS instances, not only snapshots created by the Veeam backup service. Amazon DB snapshots created for RDS instances in AWS have the **AWS Snapshot** type and cannot be deleted from Veeam Backup for AWS.

- **Latest Snapshot** — the date and time of the latest snapshot that was created for the RDS instance.
- **Instance Size** — a size of the RDS instance storage.
- **Region** — an AWS Region in which the RDS instance resides.
- **Engine** — a database engine of the RDS instance.

Removing Snapshots

Veeam Backup for AWS applies the **configured retention policy settings** to automatically remove cloud-native snapshots and snapshot replicas created by backup policies. If necessary, you can also remove the backed-up data manually.

**NOTE**

In Veeam Backup for AWS, you can remove only snapshots created by the Veeam backup service. To delete AWS Snapshots (DB instance snapshots created in AWS), use **Amazon Management Console**.

To remove backed-up data manually, do the following:

1. Navigate to **Protected Data > RDS**.
2. Select RDS instances whose data you want to remove.
3. Click **Remove** and select either of the following options:

   - **Snapshots > Snapshots** — to remove cloud-native snapshots created for the selected RDS instances by backup policies.
   
   - **Snapshots > Manual** — to remove cloud-native snapshots created for the selected RDS instances manually.
     
   If you want to remove only specific cloud-native snapshots, follow the instructions provided in section **Removing Snapshots Created Manually**.

   - **Snapshots > Replicas** — to remove snapshot replicas created for the selected RDS instances by backup policies.
   
   - **Snapshots > All** — to remove all cloud-native snapshots and snapshot replicas created for the selected RDS instances both by backup policies and manually.
Removing Snapshots Created Manually

If you want to remove specific cloud-native snapshots created for an RDS instance manually, do the following:

1. Navigate to **Protected Data > RDS**.
2. Select the necessary instance, and click the link in the **Snapshots** column.
3. In the **Available Restore Points** window, select a snapshot that you want to remove, and click **Remove Manual Snapshot**.
Managing Backed-Up VPC Configuration Data

For each protected AWS Region within the AWS account, Veeam Backup for AWS creates a configuration record in the database. To view all existing configuration records, navigate to Protected Data > VPC.

Each configuration record is described with a set of properties:

- **Account** — a name of an AWS account whose IAM role was used to collect VPC configuration data.
- **Region** — an AWS Region whose VPC configuration data is backed up.
- **Latest Backup** — the date and time of the latest created restore point.
- **Latest Changes** — the summary of changes in the VPC configuration in comparison with the previous restore point.
- **Restore Points** — a number of restore points created for the VPC configuration.

In the **Configuration details** section, Veeam Backup for AWS displays the backed-up VPC configuration details for the selected configuration record.

You can export, compare and remove backed-up Amazon VPC configuration data.

Removing VPC Configuration Backups

Veeam Backup for AWS applies the configured retention policy settings to automatically remove VPC configuration backups created by the VPC Configuration Backup policy. If necessary, you can also remove the backed-up data manually.

**IMPORTANT**

If you remove a configuration record for an AWS Region, all VPC configuration backups for the selected AWS Region will be removed.

To remove backed-up data manually, do the following:

1. Navigate to Protected Data > VPC.
2. Select the configuration record for which you want to remove the backed-up data.

3. Click **Remove** and select either of the following options:
   - **Remove** — to remove all VPC configuration backups for the selected configuration record from the Veeam Backup for AWS database.
   - **Remove Additional Copies** — to remove all VPC configuration backups for the selected configuration record from the S3 repository, specified in the **target settings** of the VPC Configuration Backup policy.

**NOTE**

If you remove Amazon VPC configuration backups from the Veeam Backup for AWS database but leave their additional copies in any S3 repository, these backups will be added back to the Veeam Backup for AWS database when the Veeam backup service restarts or Veeam Backup for AWS rescans the S3 repository.

Comparing VPC Configuration Backups

You can compare the current Amazon VPC configuration of an AWS Region to the backed-up Amazon VPC configuration.

1. Navigate to **Protected Data > VPC**.
2. Select the configuration record for an AWS Region whose VPC configuration you want to compare.
3. Click **Compare**.

By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can compare the VPC configuration data to an earlier state. In the **Compare Attributes** window, click the link to the right of **Restore point** to select the necessary restore point.

If you want Veeam Backup for AWS to display only backed-up VPC configuration items that differ from the current VPC configuration items, set the **Show only changed attributes** toggle to **On**.
You can export or restore the VPC configuration using the selected restore point:

- To export the entire VPC configuration, click **Export** and follow the instructions provided in [Performing Entire Configuration Export](#).

- To restore the entire VPC configuration, click **Restore** and follow the instructions provided in [Performing Entire Configuration Restore](#).
Exporting VPC Configuration

You can export backed-up VPC configuration data to an AWS CloudFormation template in the JSON format using one of the following options:

- Perform the entire VPC configuration export.
- Perform the selected VPC configuration items export.

Performing Entire Configuration Export

You can export the entire VPC configuration and restore it from the CloudFormation template to the original location or to a new location.

IMPORTANT

If you plan to restore the exported VPC configuration, consider that restore to a new location is not supported for the following VPC configuration items:

- Client VPN endpoints.
- Customer gateways and load balancer listeners that use authentication certificates.
- In route tables, for routes to AWS Outpost local gateways, network interfaces, instances and carrier gateways.

To export the entire VPC configuration to a CloudFormation template, complete the following steps:

1. Launch the VPC Export wizard.
2. Select a restore point and VPCs to export.
3. Specify an IAM identity for export.
4. Choose an export mode.
5. Configure mapping for Availability Zones.
6. Configure settings for VPC peering connections.
7. Specify an Amazon S3 bucket where the Cloud Formation template must be placed.
8. Specify a reason for export.
Step 1. Launch VPC Export Wizard

To launch the **VPC Export** wizard, complete the following steps.

1. Navigate to **Protected Data > VPC**.
2. Select the configuration record for an AWS Region whose VPC configuration you want to restore.
3. Click **Export > Entire VPC**.
Step 2. Select Restore Point

At the Export List step of the wizard, select the VPC whose configuration you want to export and a restore point that will be used to export the selected VPC configuration. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can export the VPC configuration data to an earlier state.

To select a restore point, do the following:

1. In the Select restore point section, click the link to the right of Restore point.
2. In the Available Restore Points window, select the necessary restore point and click Apply.
3. In the Select VPC to restore section, select VPCs whose configuration you want to export.

![Available Restore Points Table]
Step 3. Specify IAM Identity

At the **Account** step of the wizard, specify an IAM role whose permissions Veeam Backup for AWS will use to perform the export operation.

**IMPORTANT**

Make sure, that the specified IAM role belongs to an AWS account in which you plan to restore the VPC configuration.

To specify an IAM role for export:

1. Select the **IAM Role** option.
2. Select the necessary IAM role from the list.

   For an IAM role to be displayed in the **IAM Role** list, it must be added to Veeam Backup for AWS as described in **Adding IAM Roles**. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the **VPC Restore** wizard. To add an IAM role, click **Add** and complete the **Add Account** wizard.

It is recommended that you check whether the selected IAM role has all the required permissions to perform export. To run the IAM role permission check, click **Check permissions**. Veeam Backup for AWS will display the **Permissions check** window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient, the check will complete with errors. You can view the list of permissions that must be granted to the IAM role in the **Missing Permissions** column.

You can grant the missing permissions to the IAM role in the IAM Management Console or **instruct Veeam Backup for AWS** to do it. To learn how to grant permissions to an IAM Role using the IAM Management Console, see **AWS Documentation**.
Step 4. Choose Export Mode

At the Export Mode step of the wizard, choose whether you plan to restore the exported VPC configuration to the original or to a custom location.

**IMPORTANT**

Before you choose the export mode, consider the following:

- If you plan to restore the exported VPC configuration to the original location — when you restore the VPC configuration from the CloudFormation template, all exported VPC configuration items will be newly created in the source AWS Region. If there are any already existing items with the same names in the current VPC configuration, the restored items will be created with new IDs, but with the same names.

- If you plan to restore the exported VPC configuration to a custom location — the source and target AWS Regions may have different lists of the supported AWS services. In this case, when you restore the VPC configuration from the CloudFormation template, VPC endpoints created using an AWS service that is not available in the target AWS Region will not be restored.
Step 5. Configure Availability Zone Mapping

[This step applies only if you have selected the Export to a new location option at the Export Mode step of the wizard]

At the Availability Zones step of the wizard, for each source Availability Zone, choose an Availability Zone in the target AWS Region where VPC configuration items of the source Availability Zone will be restored:

1. Choose an Availability Zone from the list and click Edit Mapping.
2. In the Map Availability Zone window, select the target Availability Zone from the Target regions dropdown list.
3. Click Apply.

**IMPORTANT**

The source and target AWS Regions may have different number of Availability Zones. In this case, Veeam Backup for AWS will automatically change subnet configuration for transit gateway VPC attachments, VPC endpoints and load balancers. After restoring, you can modify the subnet configuration manually in the AWS Management Console. To learn how to modify subnet configuration for VPC networking components, see AWS Documentation.
Step 6. Configure Peering Connection Settings

(This step applies only if you have selected the Export to a new location option at the Export Mode step of the wizard)

At the Peering Connection step of the wizard, review VPC peering connection settings. You cannot modify the VPC peering connection settings for the exported VPC. By default, Veeam Backup for AWS will export VPC peering connections as follows:

- If you export both VPCs between which you have created a peering connection, Veeam Backup for AWS will create a peering connection between the exported VPCs in the target AWS Region.

- If you export a VPC that has a peering connection to a VPC in the same AWS Region, Veeam Backup for AWS will create an inter-region peering connection between the exported VPC in the target AWS Region and the VPC with which the source VPC is peered in the source AWS Region.

- If you export a VPC that has a peering connection to a VPC in another AWS Region, Veeam Backup for AWS will create an inter-region peering connection between the exported VPC in the target AWS Region and the VPC with which the source VPC is peered in the other AWS Region.

**NOTE**

VPC peering connections will have the Pending Acceptance status after restoring from the exported CloudFormation template. To accept the restored VPC peering connections, use the AWS Management Console. For more information, see AWS Documentation.
Step 7. Specify Amazon S3 Bucket

At the **Target** step of the wizard, specify an Amazon S3 bucket where Veeam Backup for AWS will save the CloudFormation template with the exported VPC configuration data.

Choose whether you want to save the template in the root folder of the selected Amazon S3 bucket or to create a new folder for the template.

Step 8. Specify Export Reason

At the **Reason** step of the wizard, specify a reason for the export of the VPC configuration. The information you provide will be saved in the session history and you can reference it later.
Step 9. Finish Working with Wizard

At the Summary step of the wizard, review summary information and click Finish.

Performing Selected Items Export

NOTE

If you export only specific VPC configuration items, you will not be able to choose a location. By default, Veeam Backup for AWS will create a CloudFormation template to restore to the original location.

When you restore the exported items from the CloudFormation template, all exported VPC configuration items will be newly created in the source AWS Region. If there are any already existing items with the same names in the current VPC configuration, the restored items will be created with new IDs, but with the same names.

To export specific VPC configuration items to a CloudFormation template, complete the following steps:

1. Launch the VPC Export wizard.
2. Select a restore point and VPCs to export.
3. Specify an IAM identity for export.
4. Specify an Amazon S3 bucket where the CloudFormation template must be placed.
5. Specify a reason for the export.
6. Finish working with the wizard.
Step 1. Launch VPC Export Wizard

To launch the VPC Export wizard, complete the following steps.

1. Navigate to Protected Data > VPC.

2. Select the configuration record for an AWS Region whose VPC configuration you want to restore.

3. Click Export > Selected items.
Step 2. Select Restore Point

At the Export List step of the wizard, select the VPC configuration items you want to export and a restore point that will be used to export the selected VPC configuration items. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can export the VPC configuration data to an earlier state.

1. To select the restore point:
   a. In the Select restore point section, click the link to the right of Restore point.
   b. In the Available Restore Points window, select the necessary restore point and click Apply.

2. To select the VPC configuration items:
   a. In the Export list section, click Edit and select the type of VPC configuration item you want to export.
   b. In the Edit export list window, click Add.
   c. In the Item List window, select check boxes next to the items that you want to export, and click Add.
   d. In the Edit export list window, review the restore list and click Apply.

IMPORTANT

When performing the export operation, Veeam Backup for AWS does not validate the export list. If any of the VPC configuration items on which the selected items depend are missing from the current VPC configuration, the restore of the selected VPC configuration items from the created CloudFormation template will fail.
Step 3. Specify IAM Identity

At the **Account** step of the wizard, specify an IAM role whose permissions Veeam Backup for AWS will use to perform the export operation.

**IMPORTANT**

Make sure, that the specified IAM role belongs to an AWS account in which you plan to restore the VPC configuration items.

To specify an IAM role for export:

1. Select the **IAM Role** option.
2. Select the necessary IAM role from the list.

   For an IAM role to be displayed in the **IAM Role** list, it must be added to Veeam Backup for AWS as described in **Adding IAM Roles**. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the **VPC Restore** wizard. To add an IAM role, click **Add** and complete the **Add Account** wizard.

   It is recommended that you check whether the selected IAM role has all the required permissions to perform export. To run the IAM role permission check, click **Check permissions**. Veeam Backup for AWS will display the **Permissions check** window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient, the check will complete with errors. You can view the list of permissions that must be granted to the IAM role in the **Missing Permissions** column.

   You can grant the missing permissions to the IAM role in the IAM Management Console or instruct **Veeam Backup for AWS** to do it. To learn how to grant permissions to an IAM Role using the IAM Management Console, see **AWS Documentation**.
Step 4. Specify Amazon S3 Bucket

At the **Target** step of the wizard, specify an Amazon S3 bucket where Veeam Backup for AWS will save the CloudFormation template with the exported VPC configuration items.

Choose whether you want to save the template in the root folder of the selected Amazon S3 bucket or to create a new folder for the template.

![Image of Veeam Backup for AWS VPC Export wizard](image)

Step 5. Specify Export Reason

At the **Reason** step of the wizard, specify a reason for the export of the VPC configuration items. The information you provide will be saved in the session history and you can reference it later.

![Image of Veeam Backup for AWS VPC Export wizard](image)
Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.
Performing Restore

In various disaster recovery scenarios, Veeam Backup for AWS allows you to perform the following restore operations using backed-up data:

- **Restore of EC2 instances** — restore EC2 instances from cloud-native snapshots or image-level backups to the original location or to a new location.
- **Restore of RDS instances** — restore RDS instances from cloud-native snapshots to the original location or to a new location.
- **Restore of Amazon VPC configuration** — restore VPC configuration from VPC configuration backups to the original location or to a new location.

EC2 Instance Restore

Veeam Backup for AWS offers the following restore options:

- **Instance Restore** — starts an entire EC2 instance from a restore point.
- **Volume Restore** — restores EBS volumes attached to an EC2 instance.
- **File-Level Restore** — restores individual files and folders of an EC2 instance.

You can restore EC2 instance data to the most recent state or to any available restore point.

Performing Entire EC2 Instance Restore

In case of a disaster, you can restore an entire EC2 instance from a cloud-native snapshot, snapshot replica or image-level backup. Veeam Backup for AWS allows you to restore one or more EC2 instances at a time, to the original location or to a new location.

How Instance Restore Works

To restore EC2 instances from cloud-native snapshots and snapshot replicas, Veeam Backup for AWS uses native AWS capabilities. To restore EC2 instances from image-level backups, Veeam Backup for AWS performs the following steps:

1. Launches a worker instance in the AWS Region where the restored EC2 instance will reside.
2. Creates empty EBS volumes and attaches them to the worker instance.
   
   The number of empty EBS volumes equals the number of EBS volumes attached to the backed-up EC2 instance.
3. Restores backed-up data to the empty EBS volumes on the worker instance.
4. Detaches EBS volumes with restored data from the worker instance.
5. Removes the worker instance from Amazon EC2.
6. Creates an EC2 instance in the specified location.
7. Attaches EBS volumes with restored data to the target EC2 instance.
7. [This step applies only if you perform restore to the original location] Powers off the source EC2 instance and removes it from Amazon EC2.

**Before You Begin**

If you plan to restore an EC2 instance to an AWS Outpost, check the following prerequisites:

1. An IAM role you plan to specify for the restore operation must have the following permissions: `outposts:ListOutposts`, `outposts:GetOutpostInstanceTypes`. To grant the necessary permissions for the IAM role, use the AWS Management Console. For more information on how to grant permissions to an IAM role, see [AWS Documentation](https://docs.aws.amazon.com/).  

2. If an Outpost subnet is specified in the worker instance network settings, restore of an EC2 instance to an AWS Region to which the AWS Outpost is connected may fail. The issue occurs if the default worker instance class (c5.large) is not supported for the AWS Outpost. To work around the issue, contact Veeam Customer Support.

**How to Perform Instance Restore**

To restore a protected EC2 instance, complete the following steps:

1. Launch the Instance Restore wizard.
2. Select a restore point.
3. Specify IAM identity for restore.
4. Choose a restore mode.
5. Select an AWS Region.
6. Enable encryption for EBS volumes.
7. Specify an EC2 instance name and type.
8. Configure network settings.
9. Specify a restore reason.
10. Finish working with the wizard.
Step 1. Launch Instance Restore Wizard

To launch the Instance Restore wizard, complete the following steps.

1. Navigate to Protected Data > EC2.
2. Select the EC2 instance that you want to restore, and click Restore > Instance Restore.

Step 2. Select Restore Point

At the Instances step of the wizard, select a restore point that will be used to restore the selected EC2 instance. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore the EC2 instance to an earlier state.

To select a restore point, do the following:

1. Select the EC2 instance.
2. Click Restore Point.
3. In the Available Restore Points window, select the necessary restore point and click Apply.

To help you choose a restore point, Veeam Backup for AWS provides the following information on each available restore point:

- **Date** — the date when the restore point was created.
- **Size** — the size of the restore point.
- **Type** — the type of the restore point:
  - **Snapshot** — a cloud-native snapshot created by a backup policy.
  - **Replica** — a snapshot replica created by a backup policy.
  - **Manual Snapshot** — a cloud-native snapshot created manually.
  - **Backup** — an image-level backup created by a backup policy.
- **Region** — an AWS Region where the restore point is stored (for cloud-native snapshots and snapshot replicas).
- **Account name** — a name of an IAM role used to create the restore point (for cloud-native snapshots and snapshot replicas).
Step 3. Specify IAM Identity

At the **Account** step of the wizard, choose whether you want to **use an IAM role** or **one-time access keys of an IAM user** to allow Veeam Backup for AWS to perform the restore operation. For information on what permissions the IAM role or IAM user must have to perform restore, see this Veeam KB article.

**IMPORTANT**

Make sure, that the specified IAM role or one-time access keys belong to an AWS account in which you plan to restore EC2 instances.

Specifying IAM Role

To specify an IAM role for restore:

1. Select the **IAM Role** option.
2. Select the necessary IAM role from the list.

For an IAM role to be displayed in the **IAM Role** list, it must be added to Veeam Backup for AWS as described in **Adding IAM Roles**. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the **Instance Restore** wizard. To add an IAM role, click **Add** and complete the **Add Account** wizard.
Specifying One-Time Access Keys

To specify one-time access keys for restore:

1. Select the **Temporary Access Keys** option.
2. Use the **Access Key** and **Secret Key** fields to provide the access key ID and the secret access key.

**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.
Step 4. Choose Restore Mode

At the Restore Mode step of the wizard, choose whether you want to restore the selected EC2 instance to the original or to a custom location.

**IMPORTANT**
To restore to the original location, the IAM role specified at the Account step of the wizard must belong to the AWS account where the selected restore point was created.

<table>
<thead>
<tr>
<th>Instance Restore</th>
<th>Restore mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instances</td>
<td></td>
</tr>
<tr>
<td>Account</td>
<td></td>
</tr>
<tr>
<td>Restore Mode</td>
<td>□ Restore to the original location</td>
</tr>
<tr>
<td></td>
<td>Quickly initiate the restore of selected instances to their original location, with the original name and settings.</td>
</tr>
<tr>
<td></td>
<td>□ Restore to a new location, or with different settings</td>
</tr>
<tr>
<td></td>
<td>Customize the restored instance location and change its settings.</td>
</tr>
<tr>
<td>Region</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
</tr>
<tr>
<td>Instance</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
</tr>
<tr>
<td>Reason</td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td></td>
</tr>
</tbody>
</table>
Step 5. Select AWS Region

[This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard]

At the Region step of the wizard, specify the target AWS Region where restored EC2 instances will operate.

If you have AWS Outposts in your infrastructure, you can restore EC2 instances to the AWS Outpost. To do that:

1. From the Region drop-down list, select the AWS Region to which the AWS Outpost is connected.
2. In the Select AWS Outpost section, click the Not set link.
3. In the Available AWS Outposts window, select the AWS Outpost.
4. Click Ok.

NOTE
Consider the following:

- All objects residing in an AWS Outpost are encrypted.
- An AWS Outpost supports a limited list of instance types.
Step 6. Enable Encryption

[This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard]

At the Encryption step of the wizard, choose whether the restored EBS volumes of the processed EC2 instance must be encrypted with AWS Key Management Service (AWS KMS) customer master keys (CMKs):

- If you do not want to encrypt the EBS volumes or want to apply the existing encryption scheme, select the Use original encryption scheme option.

- If you want to encrypt the EBS volumes, select the Volumes will be restored as encrypted volumes option and choose the necessary CMK from the Encryption key list.

For a CMK to be displayed in the list of available encryption keys, it must be stored in the AWS Region selected at step 6 and the IAM role specified for the restore operation must have permissions to the CMK. For more information on CMKs, see AWS Documentation.

Related Resources

AWS Key Management Service concepts
Step 7. Specify Instance Name and Type

[This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard]

At the Instance step of the wizard, do the following.

1. Select the EC2 instance and click Options.

2. In the Options window, specify a name and select an instance type for the restored VM instance. For the list of all existing instance types, see AWS Documentation.

3. To save changes made to the instance settings, click Ok.
Step 8. Configure Network Settings

[This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard]

At the **Network** step of the wizard, select to which Amazon VPC a restored EC2 instance must be connected, a subnet in which the EC2 instance will be launched, and a security group — a virtual firewall for the restored EC2 instance.

1. Select the necessary EC2 instance from the list and click **Select**.
2. In the **Network** window, choose the Amazon VPC, the subnet and the security group.

For a VPC, subnet group and security group to be displayed in the lists of available network specifications, they must be created for the AWS Region specified at step 5 in the AWS Management Console as described in AWS Documentation.

If you restore EC2 instances to the AWS Outpost, for an Outpost subnet to be displayed in the **Select Subnet** drop-down list, choose the Amazon VPC that has one or more Outpost subnets.

---

**Related Resources**

- What Is Amazon VPC
- VPCs and Subnets
- Security Groups
Step 9. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring EC2 instances. The information you provide will be saved in the session history and you can reference it later.

<table>
<thead>
<tr>
<th>Instance Restore</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Instances</td>
<td></td>
</tr>
<tr>
<td>Account</td>
<td></td>
</tr>
<tr>
<td>Restore Mode</td>
<td></td>
</tr>
<tr>
<td>Region</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
</tr>
<tr>
<td>Instance</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
</tr>
<tr>
<td>Reason</td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type in the reason for performing this restore operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Reason:</td>
</tr>
<tr>
<td>Restoring failed EC2 instances</td>
</tr>
</tbody>
</table>
Step 10. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

**TIP**

If you want to start the restored EC2 instance as soon as the restore process completes, select the **Power on target instance after restoring** check box.

<table>
<thead>
<tr>
<th>Instance Restore</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instances</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Account</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Restore Mode</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Region</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Instance</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Reason</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Click Finish to Restore**

<table>
<thead>
<tr>
<th><strong>Reason</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reason:</strong></td>
<td>Restoring failed EC2 instances</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>General</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restore mode:</strong></td>
<td>Different location</td>
</tr>
<tr>
<td><strong>Location name:</strong></td>
<td>EU (London) (eu-west-2)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>IAM Role</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IAM Role Name:</strong></td>
<td>Restore Role (Role for Dept-01 restore)</td>
</tr>
</tbody>
</table>

- **Power on target instance after restoring**

---

186 | Veeam Backup for AWS | User Guide
Performing Volume-Level Restore

In case a disaster strikes, you can restore corrupted EBS volumes of an EC2 instance from a cloud-native snapshot, snapshot replica or image-level backup. Veeam Backup for AWS allows you to restore EBS volumes to the original location or to a new location.

How Volume-Level Restore Works

To restore EBS volumes from cloud-native snapshots and snapshot replicas, Veeam Backup for AWS uses native AWS capabilities. To restore EBS volumes from image-level backups, Veeam Backup for AWS performs the following steps:

1. Launches a worker instance in the AWS Region where the restored EBS volumes will reside.
2. Creates empty EBS volumes and attaches them to the worker instance.
   The number of empty EBS volumes equals the number of volumes you selected to restore.
3. Restores backed-up data to the empty EBS volumes on the worker instance.
4. Detaches EBS volumes with restored data from the worker instance.
5. Removes the worker instance from Amazon EC2.

NOTE
Veeam Backup for AWS does not attach restored EBS volumes to any EC2 instances — the volumes are placed to the specified location as standalone EBS volumes.

Before You Begin

If you plan to restore EBS volumes to an AWS Outpost, check the following prerequisites:

1. An IAM role you plan to specify for the restore operation must have the following permissions: outposts:ListOutposts, outposts:GetOutpostInstanceTypes. To grant the necessary permissions for the IAM role, use the AWS Management Console.
2. If the Outpost subnet is specified in the worker configuration settings, restore of EBS volumes to an AWS Region to which the AWS Outpost is connected may fail. The issue occurs if the default worker instance class (c5.large) is not supported for the AWS Outpost. In this case, contact Veeam Customer Support to change the type of the worker instance.

How to Perform Volume Restore

To restore EBS volumes attached to a protected EC2 instance, complete the following steps:

1. Launch the Volume Restore wizard.
2. Select a restore point.
3. Exclude EBS volumes from restore.
4. Specify IAM identity for restore.
5. Choose a restore mode.
6. Select an AWS Region and Availability Zone.
7. **Enable encryption for EBS volumes.**
8. **Specify the restored EBS volume name.**
9. **Specify a restore reason.**
10. **Finish working with the wizard.**
Step 1. Launch Volume Restore Wizard

To launch the Volume Restore wizard, complete the following steps.

1. Navigate to Protected Data > EC2.
2. Select the EC2 instance whose EBS volumes you want to restore, and click Restore > Volume Restore.
Step 2. Select Restore Point

At the **Instances** step of the wizard, select a restore point that will be used to restore EBS volumes of the selected EC2 instance. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore the EBS volumes to an earlier state.

To select a restore point, do the following:

1. Select the EC2 instance.
2. Click **Restore Point**.
3. In the **Available Restore Points** window, select the necessary restore point and click **Apply**.

To help you choose a restore point, Veeam Backup for AWS provides the following information on each available restore point:

- **Date** — the date when the restore point was created.
- **Size** — the size of the restore point.
- **Type** — the type of the restore point:
  - **Snapshot** — a cloud-native snapshot created by a backup policy.
  - **Replica** — a snapshot replica created by a backup policy.
  - **Manual Snapshot** — a cloud-native snapshot created manually.
  - **Backup** — an image-level backup created by a backup policy.
- **Region** — an AWS Region where the restore point is stored (for cloud-native snapshots and snapshot replicas).
- **Account name** — a name of an IAM role used to create the restore point (for cloud-native snapshots and snapshot replicas).
Step 3. Exclude EBS Volumes from Restore

At the **Instances** step of the wizard, specify which EBS volumes will be excluded from restore:

1. Select the EC2 instance whose EBS volumes you want to exclude and click **Exclusions**.
2. In the **Select Exclusions** window, select check boxes next to the EBS volumes that you want to exclude from restore, and click **Select**.
Step 4. Specify IAM Identity

At the **Account** step of the wizard, choose whether you want to **use an IAM role** or **one-time access keys of an IAM user** to allow Veeam Backup for AWS to perform the restore operation. For information on what permissions the IAM role or IAM user must have to perform restore, see this Veeam KB article.

**IMPORTANT**

Make sure, that the specified IAM role or one-time access keys belong to an AWS account in which you plan to restore EBS volumes.

Specifying IAM Role

To specify an IAM role for restore:

1. Select the **IAM Role** option.
2. Select the necessary IAM role from the list.

   For an IAM role to be displayed in the **IAM Role** list, it must be added to Veeam Backup for AWS as described in Adding IAM Roles. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the **Volume Restore** wizard. To add an IAM role, click **Add** and complete the **Add Account** wizard.

   ![Volume Restore Wizard](image)

   - **Select IAM role**
     - IAM Role
     - Temporary Access Keys
       - Access Key:
       - Secret Key:
   
   - We will use these keys to restore only. They are not saved or stored. See this KB for more details.
Specifying One-Time Access Keys

To specify one-time access keys for restore:

1. Select the **Temporary Access Keys** option.
2. Use the **Access Key** and **Secret Key** fields to provide the access key ID and the secret access key.

**NOTE**
Veeam Backup for AWS does not store one-time access keys in the configuration database.
Step 5. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected EBS volumes to the original or to a custom location.

**IMPORTANT**
To restore to the original location, the IAM role specified at the **Account** step of the wizard must belong to the AWS account where the selected restore point was created.
Step 6. Select AWS Region and Availability Zone

[This step applies only if you have selected the *Restore to a new location, or with different settings* option at the *Restore Mode* step of the wizard]

At the *Region* step of the wizard, select the AWS Region and Availability Zone to which Veeam Backup for AWS will place the restored EBS volumes.

If you have AWS Outposts in your infrastructure, you can restore EBS volumes to the AWS Outpost. To do that:

1. From the *Region* drop-down list, select the AWS Region to which the AWS Outpost is connected.
2. From the *Availability zone* drop-down list, select the Availability Zone that the AWS Outpost is homed to.
3. In the *Select AWS Outpost* section, click the *Not set* link.
4. In the *Available AWS Outposts* window, select the AWS Outpost.
5. Click *Ok*.

**NOTE**

Consider the following:

- All objects residing in an AWS Outpost are encrypted.
- An AWS Outpost supports a limited list of EBS volume types. If the type of the restored EBS volume is not supported in the selected AWS Outpost, the restore operation will fail.
Step 7. Enable Encryption

(This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard)

At the Encryption step of the wizard, choose whether the restored EBS volumes must be encrypted with AWS Key Management Service (AWS KMS) customer master keys (CMKs):

- If you do not want to encrypt the EBS volumes or want to apply the existing encryption scheme, select the Use original encryption scheme option.

- If you want to encrypt the EBS volumes, select the Volumes will be restored as encrypted volumes option and choose the necessary CMK from the Encryption key list.

For a CMK to be displayed in the list of available encryption keys, it must be stored in the AWS Region selected at step 6 and the IAM role specified for the restore operation must have permissions to the CMK. For more information on CMKs, see AWS Documentation.
Step 8. Specify EBS Volume Name

[This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard]

At the Volumes step of the wizard, you can specify a name for each restored EBS volume:

1. Select the necessary EBS volume and click Edit.
   Veeam Backup for AWS will open the Volume Properties window.

2. In the Volume Properties window, specify a name for the restored EBS volume and click Ok.
Step 9. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring EBS volumes. The information you provide will be saved in the session history and you can reference it later.

- **Reason**: Restoring corrupted EBS volumes
Step 10. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

<table>
<thead>
<tr>
<th>Volume Restore</th>
<th>Click Finish to Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restore Summary</strong></td>
<td></td>
</tr>
<tr>
<td>Reason:</td>
<td>Restoring corrupted EBS volumes</td>
</tr>
<tr>
<td>Restore mode:</td>
<td>Different location</td>
</tr>
<tr>
<td>Location name:</td>
<td>EU (London) (eu-west-2)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>c2-Tgt-01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore point:</td>
</tr>
<tr>
<td>Disk name:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>c2-Tgt-02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore point:</td>
</tr>
<tr>
<td>Disk name:</td>
</tr>
</tbody>
</table>
Performing File-Level Restore

In case a disaster strikes, you can recover corrupted or missing files of an EC2 instance from a cloud-native snapshot or image-level backup. Veeam Backup for AWS allows you to download the necessary files and folders to a local machine or restore the files and folders to the source EC2 instance using the File Level Recovery for Veeam Backup browser.

**IMPORTANT**

You can restore files and folders from the following file systems:
- Microsoft Windows systems — FAT, FAT32, NTFS.
- Linux systems — ext2, ext3, ext4, XFS, Btrfs.

Veeam Backup for AWS supports file-level restore only for Microsoft Windows basic volumes and dynamic simple volumes with disabled data deduplication.

How File-Level Restore Works

To recover files and folders of a backed-up EC2 instance, Veeam Backup for AWS performs the following steps:

1. Launches a worker instance in either of the following AWS Regions:
   - To restore files and folders from a cloud-native snapshot or a snapshot replicas, Veeam Backup for AWS launches the worker instance in the AWS Region where the source EC2 instance resides.
   - To restore files and folders from an image-level backup, Veeam Backup for AWS launches the worker instance in the AWS Region where the target S3 repository resides.

2. Attaches and mounts EBS volumes of the EC2 instance to the worker instance.
   EBS volumes are not physically extracted from the backup — Veeam Backup for AWS emulates their presence on the worker instance. The source backup itself remains in the read-only state.

3. [This step applies only if you perform restore to the original location] Installs the Veeam restore tool to the source EC2 instance.

4. Launches the File Level Recovery for Veeam Backup browser.
   The File Level Recovery for Veeam Backup browser displays the file system tree of the backed-up EC2 instance. In the browser, you select the necessary files and folders to restore.

5. Saves the selected files and folders to the local machine or restores them to the original EC2 instance if the Additional restore mode is enabled.

6. Unmounts and detaches EBS volumes of the backed-up EC2 instance from the worker instance.

7. [This step applies only if you perform restore to the original location] Removes the Veeam restore tool from the original EC2 instance if the Keep the restore tool at the target instance option is not selected.

8. Removes the worker instance from Amazon EC2.
Before You Begin

Before you start file-level restore, check the following prerequisites:

- The machine from which you plan to open the File Level Recovery for Veeam Backup browser must be allowed to access the worker instances over the internet. To enable internet access for a worker instance, update the security group specified in worker instance settings to add an inbound rule for HTTPS traffic on the port 443. To learn how to add rules to security groups, see AWS Documentation.
- If you plan to perform file-level restore to the original location, make sure that:
  - The IAM role attached to the source EC2 instance has permissions to communicate with the SSM.
  - If the source EC2 instance and backup appliance reside in the same AWS account, the IAM role attached to the source EC2 instance has the following permissions: sqs:ListQueues, sqs:GetQueueUrl, kinesis:List*, kinesis:Describe*, kinesis:Get*, sqs:GetQueueAttributes, sqs:ListDeadLetterSourceQueues.
  - If the source EC2 instance and backup appliance reside in different AWS accounts, the IAM role attached to the source EC2 instance has permissions to assume the following role:
    arn:aws:iam::<service-account-id>:role/veeam_rto_<original-instance-id>, where the <service-account-id> is an AWS ID of the trusted AWS account, <original-instance-id> is an AWS ID of the source EC2 instance.

How to Perform File-Level Recovery

To recover files and folders of a protected VM instance, do the following:

1. Launch the File-level Recovery wizard.
2. Select a restore point.
3. Choose a restore mode.
4. Specify a restore reason.
5. Finish working with the wizard — start a recovery session.
6. Choose files and folders to recover.
7. Stop the recovery session.
Step 1. Launch File-level Recovery Wizard

To launch the File-level Recovery wizard, do the following:

1. Navigate to Protected Data > EC2.
2. Select the EC2 instances whose files and folders you want to recover, and click File-level Recovery.

Step 2. Select Restore Point

At the Instances step of the wizard, select a restore point that will be used to recover files and folders of the selected EC2 instance. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can recover the items to an earlier state.

To select a restore point, do the following:

1. Select the EC2 instance.
2. Click Restore Point.
3. In the Available Restore Points window, select the necessary restore point and click Apply.

To help you choose a restore point, Veeam Backup for AWS provides the following information on each available restore point:

- **Date** — the date when the restore point was created.
- **Size** — the size of the restore point.
- **Type** — the type of the restore point:
  - Snapshot — a cloud-native snapshot created by a backup policy.
  - Replica — a snapshot replica created by a backup policy.
  - Manual Snapshot — a cloud-native snapshot created manually.
  - Backup - an image-level backup created by a backup policy.
- **Region** — an AWS Region where the restore point is stored (for cloud-native snapshots and snapshot replicas).
- **Account name** — a name of an IAM role used to create the restore point (for cloud-native snapshots and snapshot replicas).
Step 3. Choose Restore Mode

At the **Restore Mode** step of the wizard, set the **Additional restore mode** toggle to *On* if you want to restore files and folders to the source EC2 instance. Before you enable the additional restore mode, ensure that the IAM role attached to the source EC2 instance has all the required permissions to perform restore to the original location.

To restore files and folders to the source EC2 instance, Veeam Backup for AWS uses Amazon Kinesis Data Streams. For more information on Kinesis Data Streams, see [AWS Documentation](https://aws.amazon.com/documentation/kinesis/). Kinesis Data Streams are charged on a per-shard basis. By default, Veeam Backup for AWS specifies for the Kinesis Data Stream 1 shard with data transfer rate equal to 1 MB per second. You can change the number of shards to be used in the stream using the **Restore rate** slider.

**TIP**

If you perform file-level restore to the original location for the selected EC2 instance frequently, you can select the **Keep the restore tool at the target instance** check box. In this case, Veeam Backup for AWS will not remove the Veeam restore tool from the EC2 instance, which will reduce the time of future recovery operations.

---

**File-level Recovery**

<table>
<thead>
<tr>
<th>Instances</th>
<th>Configure additional restore mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore mode</td>
<td>By default, we provide the option to download restored files. To restore files to the original location, enable the additional restore mode option. You can configure the restore rate by choosing the speed for the restore operation.</td>
</tr>
</tbody>
</table>

**Reason**

**Summary**

Additional restore mode: [On]

Restore rate:

- 0.225 $/hour
- 15 MB/sec

[Keep the restore tool at the target instance]
Step 4. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for recovering files and folders. This information will be saved to the session history and you will be able to reference it later.

![Restore Reason](image-url)
Step 5. Start Recovery Session

At the Summary step of the wizard, review summary information and click Start.

As soon as you click Start, Veeam Backup for AWS will close the File-level Recovery wizard, start a recovery session and display the FLR Running Sessions window. During the recovery session, Veeam Backup for AWS will launch a worker instance and attach EBS volumes of the processed EC2 instance to it.

**TIP**

If you accidentally close the FLR Running Sessions window, navigate to Protected Data > EC2 and click the link in the File-Level Recovery URL column to open the window again.

In the FLR Running Sessions window you can track the progress of the recovery session. In the URL column of the window, Veeam Backup for AWS will display a link to the File Level Recovery for Veeam Backup browser. You can use the link in either of the following ways:

- Click the link to open the File Level Recovery for Veeam Backup browser on your local machine while the recovery session is running.
- Copy the link, close the FLR Running Sessions window and open the File Level Recovery for Veeam Backup browser on another machine.

**IMPORTANT**

When you click Copy FLR URL, Veeam Backup for AWS copies the following information to the clipboard:

- A link to the File Level Recovery for Veeam Backup browser the includes a public DNS name of the worker instance hosting the browser and authentication information used to access the browser.
- A thumbprint of a TLS certificate installed on the worker instance hosting the File Level Recovery for Veeam Backup browser.

To avoid a man-in-the-middle attack, before you start recovering files and folders, check that the certificate thumbprint displayed in the web browser from which you access the File Level Recovery for Veeam Backup browser matches the provided certificate thumbprint.
Step 6. Choose Items to Recover

In the File Level Recovery for Veeam Backup browser, you can find and recover items (files and folders) of the selected EC2 instance. All recovered items are saved as a single .ZIP archive to the default download directory on a machine from which you access the browser.

To recover files from a specific folder, follow the steps:

1. In the File Level Recovery for Veeam Backup browser, navigate to the folder that contains the necessary files.
2. In the working area, select check boxes next to the files that you want to restore and do the following:
   - To download the files to the local machine, click **Download**.
   - To download the files to the source EC2 instance, click **Restore > Keep**.
     Veeam Backup for AWS will save the files with the `restored-` prefix to the same directory where the source files are located.
   - To restore the files to the source EC2 instance, click **Restore > Overwrite**.
     Veeam Backup for AWS will overwrite the source files.

To recover files from multiple folders all at once, follow the steps:

1. In the File Level Recovery for Veeam Backup browser, navigate to a folder that contains the necessary files.
2. In the working area, select check boxes next to the files and click **Add to Recovery List**.
3. Repeat steps 1-2 for all other folders whose files you want to recover.
4. Click **Pending Recovery**.
5. In the **Recovery List** window, review the list of items to recover and do the following:
   - To download the files to the local machine, click **Download**.
   - To download the files to the source EC2 instance, click **Restore > Keep**.
     Veeam Backup for AWS will save the files with the `restored-` prefix to the same directory where the source files are located.
To restore the files to the source EC2 instance, click **Restore > Overwrite**. Veeam Backup for AWS will overwrite the source files.
Step 7. Stop Recovery Session

After you finish working with the File Level Recovery for Veeam Backup browser, it is recommended that you stop the recovery session so that Veeam Backup for AWS can unmount and detach EBS volumes of the processed EC2 instance from the worker instance and remove the worker instance from Amazon EC2.

To stop the recovery session, click **Stop recovery session** in the **FLR Running Sessions** window. If you do not perform any actions in the File Level Recovery for Veeam Backup browser for 30 minutes, Veeam Backup for AWS will stop the recovery session automatically.

**TIP**

If you accidentally close the **FLR Running Sessions** window, navigate to **Protected Data > EC2** and click the link in the **File-Level Recovery URL** column to open the window again.

<table>
<thead>
<tr>
<th>Restore Point</th>
<th>URL</th>
<th>Certificate Thumbprint</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/01/2020 2:00:18 PM</td>
<td><a href="https://ec2-3-101-37-195.us-w">https://ec2-3-101-37-195.us-w</a>...</td>
<td>67F9E02F5EF375BAF484F291...</td>
</tr>
<tr>
<td>05/15/2020 12:00:15 PM</td>
<td><a href="https://ec2-3-101-24-75.us-we">https://ec2-3-101-24-75.us-we</a>...</td>
<td>59B67061BABB9AE20EF65B...</td>
</tr>
</tbody>
</table>
RDS Instance Restore

In case of a disaster, you can restore an RDS instance from a cloud-native snapshot, snapshot replica or an AWS snapshot. Veeam Backup for AWS allows you to restore only one RDS instance at a time, to the original location or to a new location.

How RDS DB Instance Restore Works

To restore RDS instances from a snapshot, Veeam Backup for AWS performs the following steps using native AWS capabilities:

1. Creates an RDS instance in the specified location.
2. Modifies the configuration setting values of the created RDS instance.
3. Restores backed-up databases to the restored RDS instance.

How to Perform Instance Restore

To restore a protected RDS instance, complete the following steps:

1. Launch the RDS Restore wizard.
2. Select a restore point.
3. Specify an IAM identity for restore.
4. Choose a restore mode.
5. Enable encryption.
6. Configure RDS instance settings.
7. Configure network settings.
8. Specify a restore reason.
9. Finish working with the wizard.
Step 1. Launch RDS Restore Wizard

To launch the RDS Restore wizard, complete the following steps.

1. Navigate to Protected Data > RDS.
2. Select the RDS instance you want to restore.
3. Click Restore Instance.

Step 2. Select Restore Point

At the Instance step of the wizard, select a restore point that will be used to restore the selected RDS instance. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore the RDS instance data to an earlier state.

To select a restore point, do the following:

1. Select the RDS instance and click Restore Point.
2. In the Available Restore Points window, select the necessary restore point and click Apply.

   To help you choose a restore point, Veeam Backup for AWS provides the following information on each available restore point:
   
   - **Date** — the date when the restore point was created.
   - **Size** — the size of the restore point.
   - **Type** — the type of the restore point:
     - **Snapshot** — a cloud-native snapshot created by a backup policy.
     - **Replica** — a snapshot replica created by a backup policy.
     - **Manual Snapshot** — a cloud-native snapshot created manually.
     - **AWS Snapshot** — an Amazon DB instance snapshot created in AWS.
**IMPORTANT**

If you select a restore point of the AWS snapshot type, you will not be able to restore an RDS instance to the original location.

- **Region** — an AWS Region where a restore point is stored (for cloud-native snapshots and snapshot replicas).
- **Account name** — a name of an IAM role used to create a restore point (for cloud-native snapshots and snapshot replicas).
Step 3. Specify IAM Identity

At the Account step of the wizard, choose whether you want to use an IAM role or one-time access keys of an IAM user to allow Veeam Backup for AWS to perform the restore operation.

**IMPORTANT**

Make sure, that the specified IAM role or one-time access keys belong to an AWS account in which you plan to restore the RDS instance.

Specifying IAM Role

To specify an IAM role for restore:

1. Select the IAM Role option.
2. Select the necessary IAM role from the list.

   For an IAM role to be displayed in the IAM Role list, it must be added to Veeam Backup for AWS as described in Adding IAM Roles. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the RDS Restore wizard. To add an IAM role, click Add and complete the Add Account wizard.

   It is recommended that you check whether the selected IAM role has all the required permissions to perform restore. To run the IAM role permission check, click Check permissions. Veeam Backup for AWS will display the Permissions check window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient, the check will complete with errors. You can view the list of permissions that must be granted to the IAM role in the Missing Permissions column.

   You can grant the missing permissions to the IAM role in the IAM Management Console or instruct Veeam Backup for AWS to do it. To learn how to grant permissions to an IAM Role using the IAM Management Console, see AWS Documentation.
Specifying One-Time Access Keys

To specify one-time access keys for restore:

1. Select the **Temporary Access Keys** option.
2. Use the **Access Key** and **Secret Key** fields to provide the access key ID and the secret access key.

**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.
Step 4. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected RDS instance to the original or to a custom location.

**IMPORTANT**

You cannot restore to the original location if the restore point selected at the **Instance** step of the wizard has the **AWS snapshot** type, or if the IAM role specified at the **Account** step of the wizard belongs to the AWS account other than the AWS account where the restore point was created.
Step 5. Enable Encryption

[This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard]

At the Encryption step of the wizard, choose whether the restored RDS instance must be encrypted with AWS Key Management Service (AWS KMS) customer master keys (CMKs):

- If you do not want to encrypt the RDS instance or want to apply the existing encryption scheme, select the Use original encryption scheme option.
- If you want to encrypt the RDS instance, select the Restore as encrypted instance option and choose the necessary CMK from the Encryption key list.

For a CMK to be displayed in the list of available encryption keys, it must be stored in the AWS Region selected at step 4 and the IAM role specified for the restore operation must have permissions to the CMK. For more information on CMKs, see AWS Documentation.

Related Resources

AWS Key Management Service concepts
Step 6. Configure Instance Settings

[This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard]

At the Settings step of the wizard, specify:

- An instance identifier (name) for the restored RDS instance.
- An option group and a parameter group that must be applied to the restored RDS instance.

TIP

The Instance specification and Advances options sections of the Settings step contain preconfigured settings retrieved from the source instance. If you want to specify advanced configuration settings for the restored RDS instance, click Edit in the necessary section. For more information on all available settings that can be specified for an RDS instance, see AWS Documentation.

Specifying Instance Identifier

To specify an identifier for the restored RDS instance:

1. In the Settings section, click Edit Instance Settings.
2. In the Instance settings window, enter the identifier in the Instance Identifier field. Consider the following limitations:
   - The instance identifier must be unique for each AWS Region within one AWS Account.
   - The instance identifier can contain only lowercase Latin letters or hyphens, but cannot contain two consecutive hyphens. You cannot use a hyphen as the last character of the identifier.
   - The maximum length of the instance identifier is 63 characters.
   For more information on limitations for RDS instance identifiers, see AWS Documentation.
3. Click Apply.

Specifying Parameter Group and Option Group

To specify a parameter group and an option group:

1. In the Instance options section, click Edit Instance Options.
2. In the Instance options window, do the following:
   a. From the Parameter group drop-down list, select the parameter group with database engine configuration values that will be applied to the restored RDS instance.
   b. From the Option group drop-down list, select the option group with database configuration values and security settings that will be applied to the restored RDS instance.

NOTE

If you select Use default group, Veeam Backup for AWS will associate the restored RDS instance with the default parameter group and the default option group automatically created by AWS.
For a parameter group and an option group to be displayed in the lists, the groups must be created in the Amazon RDS console. To learn how to create parameter and option groups, see AWS Documentation.

3. Click Apply.

Step 7. Configure Network Settings

[This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard]

At the Network step of the wizard, configure network and security settings for the restored RDS instance.

1. In the Network section, specify the network settings for the restored RDS instance:

   a. Click Edit Network Settings.

   b. In the Network specifications window, choose an Amazon VPC to which the restored RDS instance will be connected, a subnet group that will be assigned to the instance, an Availability Zone where the instance will reside, and port that must be used to access the RDS instance. Note that Veeam Backup for AWS will display only Amazon VPCs that have one or more subnet groups in the VPC drop-down list.

   For a VPC and a subnet group to be displayed in the lists of available network specifications, they must be created for the AWS Region specified at step 4 in the AWS Management Console as described in AWS Documentation.

   **TIP**

   If you want to create a passive secondary replica (standby instance) of the restored RDS instance, set the Multi-AZ deployment toggle to On. However, keep in mind that Multi-AZ deployments are not supported for RDS instances running MS SQL Server Express Edition or MS SQL Server Web Edition. For more information on Multi-AZ deployments, AWS Documentation.
c. Click **Apply**.

2. In the **Security** section, specify security settings to control what IP addresses will be able to connect to databases on the restored RDS instance.
   a. Click **Edit Security Settings**.
   b. In the **Security settings** window, from the **VPC security group** drop-down list, select a VPC security group that will control access to the RDS instance.

   If you want to make the restored RDS instance accessible outside the Amazon VPC, set the **Public accessible** toggle to *On*. Note that the RDS instance must belong to a public subnet group to become publicly accessible.

   c. Click **Apply**.
Step 8. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring the RDS instance. This information will be saved to the session history and you will be able to reference it later.

```
Specify the reason for performing the restore operation

Restore reason:
- Restoring the failed RDS instance
```

Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.
VPC Configuration Restore

Veeam Backup for AWS offers the following disaster recovery operations:

- **VPC Configuration Restore** — starts an entire VPC configuration from a restore point.
- **Selected Items Restore** — restores the selected VPC configuration items.

You can restore the VPC configuration data to the most recent state or to any available restore point.
Performing Entire Configuration Restore

In case of unexpected configuration changes, you can restore entire Amazon VPC configuration from a VPC configuration backup. Veeam Backup for AWS allows you to restore the VPC configuration to the original location or to a new location.

**IMPORTANT**

Restore to a new location is not supported for the following VPC configuration items:

- Client VPN endpoints.
- Customer gateways and load balancer listeners that use authentication certificates.
- In route tables, for routes to AWS Outpost local gateways, network interfaces, instances and carrier gateways.

How Entire VPC Configuration Restore Works

To restore the entire VPC configuration from a backup, Veeam Backup for AWS performs the following steps:

1. Retrieves the backed-up VPC configuration from the Veeam Backup for AWS database.
2. Validates the restore operation: sends API requests to AWS to verify that AWS service quotas are not exceeded and there are no subnet CIDR block conflicts.
3. Retrieves information on existing items and their settings in the current Amazon VPC configuration.
4. Restores the backed-up VPC configuration:
   a. Creates the missing VPC configuration items.
   b. Modifies settings of the existing items that do not match the backed-up settings.

How to Perform Entire VPC Configuration Restore

To restore the entire VPC configuration, complete the following steps:

1. Launch the VPC Restore wizard.
2. Select a restore point and VPCs to restore.
3. Specify an IAM identity for restore.
4. Choose a restore mode.
5. Configure mapping for Availability Zones.
7. Specify a restore reason.
8. Finish working with the wizard.
Step 1. Launch VPC Restore Wizard

To launch the VPC Restore wizard, complete the following steps.

1. Navigate to Protected Data > VPC.

2. Select the configuration record for an AWS Region whose VPC configuration you want to restore.

3. Click Restore > Entire VPC.
Step 2. Select Restore Point

At the **Restore List** step of the wizard, select a restore point that will be used to restore the selected VPC configuration. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore the VPC configuration data to an earlier state.

To select a restore point, do the following:

1. In the **Select restore point** section, click the link to the right of **Restore point**.
2. In the **Available Restore Points** window, select the necessary restore point and click **Apply**.
3. In the **Select VPC to restore** section, select VPCs whose configuration you want to restore.

Step 3. Specify IAM Identity

At the **Account** step of the wizard, choose whether you want to use an IAM role or one-time access keys of an IAM user to allow Veeam Backup for AWS to perform the restore operation.

**IMPORTANT**

Make sure, that the specified IAM role or one-time access keys belong to an AWS account in which you plan to restore the VPC configuration.

**Specifying IAM Role**

To specify an IAM role for restore:

1. Select the **IAM Role** option.
2. Select the necessary IAM role from the list.

For an IAM role to be displayed in the **IAM Role** list, it must be added to Veeam Backup for AWS as described in **Adding IAM Roles**. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the **VPC Restore** wizard. To add an IAM role, click **Add** and complete the **Add Account** wizard.
It is recommended that you check whether the selected IAM role has all the required permissions to perform restore. To run the IAM role permission check, click Check permissions. Veeam Backup for AWS will display the Permissions check window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient, the check will complete with errors. You can view the list of permissions that must be granted to the IAM role in the Missing Permissions column.

You can grant the missing permissions to the IAM role in the IAM Management Console or instruct Veeam Backup for AWS to do it. To learn how to grant permissions to an IAM Role using the IAM Management Console, see AWS Documentation.

Specifying One-Time Access Keys

To specify one-time access keys for restore:

1. Select the Temporary Access Keys option.
2. Use the Access Key and Secret Key fields to provide the access key ID and the secret access key.

**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.
Step 4. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected VPC configuration to the original or to a custom location.

**IMPORTANT**

If you select the **Restore to a new location, or with different settings** option, consider that AWS Regions have different lists of the supported AWS services. VPC endpoints created using an AWS service that is not available in the target AWS Region will not be restored.

![Veeam Backup for AWS VPC Restore screen](image)
Step 5. Configure Availability Zone Mapping

[This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard]

At the Availability Zones step of the wizard, for each source Availability Zone, choose an Availability Zone in the target AWS Region to which VPC configuration items of the source Availability Zone will be restored:

1. Choose an Availability Zone from the list and click **Edit Mapping**.
2. In the **Map Availability Zone** window, select the target Availability Zone from the Target regions dropdown list.
3. Click **Apply**.

**IMPORTANT**

The source and target AWS Regions may have different number of Availability Zones. In this case, Veeam Backup for AWS will automatically change subnet configuration for transit gateway VPC attachments, VPC endpoints and load balancers. After restoring, you can modify the subnet configuration manually in the AWS Management Console. To learn how to modify subnet configuration for VPC networking components, see AWS Documentation.
Step 6. Review Peering Connection Settings

[This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard]

At the Peering Connection step of the wizard, review preconfigured VPC peering connection settings. You cannot modify the settings for the restored VPC configuration — by default, Veeam Backup for AWS will restore VPC peering connections as follows:

- If you restore both VPCs between which you have created a peering connection, Veeam Backup for AWS will create a peering connection between the restored VPCs in the target AWS Region.

- If you restore a VPC that has a peering connection to a VPC in the same AWS Region, Veeam Backup for AWS will create an inter-region peering connection between the restored VPC in the target AWS Region and the VPC with which the source VPC is peered in the source AWS Region.

- If you restore a VPC that has a peering connection to a VPC in another AWS Region, Veeam Backup for AWS will create an inter-region peering connection between the restored VPC in the target AWS Region and the VPC with which the source VPC is peered in the other AWS Region.

NOTE

VPC peering connections will have the Pending Acceptance status after restoring. To accept the restored VPC peering connections, use the AWS Management Console. For more information, see AWS Documentation.
Step 7. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring VPC configuration. The information you provide will be saved in the session history and you can reference it later.

![Reason Step](image)

Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

![Summary Step](image)
Performing Selected Items Restore

In case of unexpected configuration changes, you can restore only specific items of the Amazon VPC configuration from a VPC configuration backup.

**NOTE**

If you restore only specific VPC configuration items, you will not be able to choose a location. By default, Veeam Backup for AWS will restore these items to the original location.

How Selected Items Restore Works

To restore specific items of the VPC configuration from a backup, Veeam Backup for AWS performs the following steps:

1. Retrieves from the Veeam Backup for AWS database the backed-up VPC configuration data on items added to a restore list.
2. Validates the restore operation: sends API request to AWS to verify that AWS service quotas are not exceeded and there are no subnet CIDR block conflicts.
3. Retrieves information on existing items and their settings in the current Amazon VPC configuration.
4. Validates the restore list: sends API requests to AWS to check whether any of the selected VPC configuration items depend on other items that are missing from the current VPC configuration.
   
   In case any VPC configuration items on which the selected items depend are missing, Veeam Backup for AWS allows the user to add the missing items to the restore list.
5. Restores the selected items of the backed-up VPC configuration:
   
   - Creates the missing VPC configuration items.
   - Modifies settings of the existing items that do not match the backed-up settings.

**IMPORTANT**

Consider the following:

- VPC peering connections will have the *Pending Acceptance* status after restoring. To accept the restored VPC peering connections, use the AWS Management Console. For more information, see [AWS Documentation](https://aws.amazon.com/documentation).
- If restore of any selected item fails, Veeam Backup for AWS will stop the restore operation and initiate a rollback. During the rollback, Veeam Backup for AWS will delete all newly created items, but will retain all changes made to the existing VPC configuration items.

How to Perform Selected Items Restore

To restore specific items of the VPC configuration, complete the following steps:

1. **Launch the VPC Restore wizard.**
2. **Select a restore point and items to restore.**
3. **Specify an IAM identity for restore.**
4. Specify a restore reason.
5. Finish working with the wizard.

Step 1. Launch VPC Restore Wizard

To launch the VPC Restore wizard, complete the following steps.

1. Navigate to Protected Data > VPC.
2. Select the configuration record for an AWS Region whose VPC configuration you want to restore.
3. Click Restore > Selected Items.
Step 2. Select Restore Point

At the **Restore List** step of the wizard, select VPC configuration items you want to restore and a restore point that will be used to restore the selected items. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore the VPC configuration data to an earlier state.

1. To select the restore point:
   a. In the **Select restore point** section, click the link to the right of **Restore point**.
   b. In the **Available Restore Points** window, select the necessary restore point and click **Apply**.

2. To select the VPC configuration items:
   a. In the **Restore list** section, click **Edit** and select an Amazon VPC resource that you want to restore.
   b. In the **Edit restore list** window, click **Add to restore list**.
   c. In the **Item List** window, select check boxes next to the items that you want to restore, and click **Add**.
   d. In the **Edit restore list** window, review the restore list and click **Apply**.
Step 3. Specify IAM Identity

At the **Account** step of the wizard, choose whether you want to use an IAM role or one-time access keys of an IAM user to allow Veeam Backup for AWS to perform the restore operation.

**IMPORTANT**

After you click **Next**, Veeam Backup for AWS will use the permissions of the specified IAM role or IAM user to validate the restore list created at step 2. If any of the VPC configuration items on which the selected items depend are missing from the current VPC configuration, Veeam Backup for AWS will open the **Missing Configuration Items** window with the list of the missing items. To proceed to the next step, click **Add**. The missing items will be automatically added to the restore list.

### Specifying IAM Role

To specify an IAM role for restore:

1. Select the **IAM Role** option.
2. Select the necessary IAM role from the list.

   For an IAM role to be displayed in the **IAM Role** list, it must be added to Veeam Backup for AWS as described in **Adding IAM Roles**. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the **VPC Restore** wizard. To add an IAM role, click **Add** and complete the **Add Account** wizard.

   It is recommended that you check whether the selected IAM role has all the required permissions to perform restore. To run the IAM role permission check, click **Check permissions**. Veeam Backup for AWS will display the **Permissions check** window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient, the check will complete with errors. You can view the list of permissions that must be granted to the IAM role in the **Missing Permissions** column.

   You can grant the missing permissions to the IAM role in the IAM Management Console or instruct Veeam Backup for AWS to do it. To learn how to grant permissions to an IAM Role using the IAM Management Console, see **AWS Documentation**.

![Veeam Backup for AWS VPC Restore](image-url)
Specifying One-Time Access Keys

To specify one-time access keys for restore:

1. Select the **Temporary Access Keys** option.
2. Use the **Access Key** and **Secret Key** fields to provide the access key ID and the secret access key.

**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.
Step 4. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for the restore of VPC configuration items. The information you provide will be saved in the session history and you can reference it later.

![Reason step of the wizard](Image)

Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

![Summary step of the wizard](Image)
Enabling Data Encryption

For enhanced data security, Veeam Backup for AWS allows you to encrypt backed-up EC2 instance data in S3 repositories using Veeam encryption mechanisms. Additionally, Veeam Backup for AWS supports native AWS encryption of EC2 and RDS instance volumes — AWS Key Management Service (AWS KMS) customer master keys (CMKs).

S3 Repository Encryption

Veeam Backup for AWS allows you to enable encryption at the S3 repository level. Veeam Backup for AWS encrypts backup files stored in S3 repositories the same way as Veeam Backup & Replication encrypts backup files stored in backup repositories. To learn what algorithms Veeam Backup & Replication uses to encrypt backup files, see the Veeam Backup & Replication User Guide, section Encryption Standards.

To enable encryption for an S3 repository added to the Veeam Backup for AWS infrastructure, configure the repository settings as described in section Adding S3 Repositories. After you create a backup policy and specify the backup repository as a target location for image-level backups, as described in section Creating EC2 Backup Policies, Veeam Backup for AWS performs the following steps:

1. Generates an encryption key to protect instance data stored in the S3 repository, and stores the key in the configuration database on the backup appliance.

2. Uses the generated key to encrypt backed-up data transferred to the S3 repository when running the backup policy.
AWS CMK Encryption

Veeam Backup for AWS allows you to back up, replicate and restore data of EC2 and RDS instance volumes encrypted with AWS Key Management Service (AWS KMS) customer master keys (CMKs). Additionally, you can encrypt unencrypted data and change CMKs used to encrypt data when performing the following operations:

- Create EC2 instance snapshot replicas.
- Create RDS instance snapshot replicas.
- Create cloud-native snapshots of EC2 instances manually in another location.
- Create cloud-native snapshots of RDS instances manually in another location.
- Restore entire EC2 instances to another location.
- Restore entire RDS instances to another location.
- Restore EC2 instance volumes to another location.

If you back up, replicate and restore data of an unencrypted RDS instance or EC2 instance, and want to encrypt the backed-up or restored data, the IAM role that Veeam Backup for AWS uses to perform the operation requires permissions to access a CMK with which you want to encrypt the data.

If you back up, replicate and restore data of an encrypted RDS instance or an EC2 instance that has encrypted EBS volumes, depending on the operation performed with the instance, the IAM role that Veeam Backup for AWS uses for the operation requires specific permissions on CMKs. To learn what permissions must be assigned to the IAM role, see:

- Creating cloud-native snapshots
- Creating snapshot replicas
- Restoring from cloud-native snapshots
- Creating image-level backups
- Restoring from image-level backups

To learn how to grant permissions on a CMK to an IAM role, see this Veeam KB article.
Creating Cloud-Native Snapshots

The process of creating cloud-native snapshots of an EC2 instance with encrypted EBS volumes and an encrypted RDS instance does not differ from the same process for an instance with unencrypted volumes. The IAM role used to create cloud-native snapshots does not require any additional permissions — Veeam Backup for AWS encrypts these snapshots with the same CMKs with which the source instance or volume is encrypted.

Creating Snapshot Replicas

The process of creating a snapshot replica of an encrypted RDS instance and an EC2 instance with encrypted EBS volumes differs depending on whether you create snapshot replicas within the same AWS account where the instance resides or not:

- Creating the snapshot replica in the same AWS account where the instance resides.
- Creating the snapshot replica in an account that is different from the AWS account where the EC2 instance resides.
- Creating the snapshot replica in an account that is different from the AWS account where the RDS instance resides.
Creating Snapshot Replica in Same AWS Account

If you create a snapshot replica within the same AWS account where the encrypted EC2 or RDS instance resides, Veeam Backup for AWS performs the following steps:

1. Creates an encrypted cloud-native snapshot of the instance.
2. Copies the created snapshot to the target AWS Region.

To copy the encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for copying and storing cloud-native snapshots in a target AWS Region. To learn how to specify this IAM role, see sections Creating EC2 Backup Policies (step 5) and Creating RDS Backup Policies (step 4). The IAM role must have permissions to access the following CMKs:

- CMKs with which data of the source instance is encrypted (source CMKs).
- A CMK with which you want to encrypt instance data in the snapshot replica (target CMK).

**IMPORTANT**

Note that if you do not specify the target CMK, the snapshot replica of an encrypted instance will not be created, and the backup session will complete with warnings. To learn how to specify the target CMK, see Creating EC2 Backup Policies (step 5) and Creating RDS Backup Policies (step 4).

Creating Cross-Account Snapshot Replica of EC2 Instance

If you create a snapshot replica in an AWS account different from the AWS account where the EC2 instance with encrypted EBS volumes resides, Veeam Backup for AWS performs the following steps:

1. Creates an encrypted cloud-native snapshot of the EC2 instance.
2. Shares the created snapshot with the target AWS account.

To share the encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for creating cloud-native snapshots. To learn how to specify this IAM role, see Creating EC2 Backup Policies (step 3.1). The IAM role must have permissions to access CMKs with which EBS volumes of the EC2 instance are encrypted (source CMKs).
If EBS volumes of the EC2 instance are encrypted with the default key for EBS encryption (aws/ebs alias), Veeam Backup for AWS will not be able to share the snapshot with another AWS account and the replication process will fail. For more information, see this Veeam KB article.

3. Copies the shared snapshot to the target AWS Region in the target AWS account.

To copy the shared encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for copying and storing cloud-native snapshots in a target AWS Region. To learn how to specify this IAM role, see Creating EC2 Backup Policies (step 5). The IAM role must have permissions to access the following CMKs:

- The CMKs with which EBS volumes of the EC2 instance are encrypted (source CMKs).
- A CMK with which you want to encrypt EBS volume data in the snapshot replica (target CMK).

If the RDS instance is encrypted with the default encryption key (aws/rds alias), Veeam Backup for AWS will not be able to share the snapshot with another AWS account and the replication process will fail. For more information, see this Veeam KB article.

Creating Cross-Account Snapshot Replica of RDS Instance

If you create a snapshot replica in an AWS account different from the AWS account where the encrypted RDS instance resides, Veeam Backup for AWS performs the following steps:

1. Creates an encrypted cloud-native snapshot of the RDS instance.

2. Shares the created snapshot with the target AWS account.

To share the encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for creating cloud-native snapshots. To learn how to specify this IAM role, see Creating RDS Backup Policies (step 3.1). The IAM role must have permissions to access a CMK with which the RDS instance is encrypted (source CMK).

If the RDS instance is encrypted with the default encryption key (aws/rds alias), Veeam Backup for AWS will not be able to share the snapshot with another AWS account and the replication process will fail. For more information, see this Veeam KB article.
3. In the target AWS account, copies the shared encrypted snapshot to the same AWS Region where the RDS instance resides in the source AWS account. Then, if the target AWS Region differs from the source AWS Region, copies the shared cloud-native snapshot to the target AWS Region.

To copy the shared encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for copying and storing cloud-native snapshots in a target AWS Region. To learn how to specify this IAM role, see Creating RDS Backup Policies (step 4). The IAM role must have permissions to access the following CMKs:

- The CMK with which the RDS instance is encrypted (source CMK).
- A CMK with which you want to encrypt RDS instance data in the snapshot replica (target CMK).

**IMPORTANT**

Note that if you do not specify the target CMK, the snapshot replica of an encrypted RDS instance will not be created, and the backup session will complete with warnings. To learn how to specify the target CMK, see Creating RDS Backup Policies (step 4).
Restoring From Snapshots and Replicas

The process of restoring an RDS or EC2 instance from an encrypted cloud-native snapshot differs depending on whether you perform restore to the same location where the cloud-native snapshot resides or not:

- Restoring the EC2 or RDS instance to the same location where the snapshot resides.
- Restoring the EC2 instance to a different AWS Region in the same AWS account where the snapshot resides.
- Restoring the EC2 instance in a different AWS account to the same AWS Region where the snapshot resides.
- Restoring the EC2 instance in a different AWS account to a different AWS Region.
- Restoring the RDS instance to a different AWS Region in the same AWS account where the snapshot resides.
- Restoring the RDS instance in a different AWS account to the same AWS Region where the snapshot resides.
- Restoring the RDS instance in a different AWS account to a different AWS Region.

**NOTE**

Consider the following:

- An AWS account in which the cloud-native snapshot resides is also referred to as the source AWS account.
- An AWS account to which you restore the instance is also referred to as the target AWS account.
Restore to Snapshot Original Location

To restore an EC2 or RDS instance to the location where the snapshot resides, Veeam Backup for AWS uses an IAM role specified for the restore operation. To learn how to specify this IAM role, see Performing Entire EC2 Instance Restore (step 3) and Performing RDS Instance Restore (step 3). The IAM role must have permissions to access the following CMKs:

- CMKs with which the cloud-native snapshot is encrypted.
- A CMK with which you want to encrypt data of the restored instance.

Restore of EC2 Instance to Different AWS Region

To restore an EC2 instance to a different AWS Region in the same AWS account where the cloud-native snapshot resides, Veeam Backup for AWS performs the following steps:

1. Copies the encrypted cloud-native snapshot to the target AWS Region.
2. Creates an EC2 instance in the target AWS Region.
3. Creates encrypted EBS volumes from the copied encrypted snapshot and attaches them to the created EC2 instance.

To copy the encrypted snapshot, and to create and encrypt EBS volumes, Veeam Backup for AWS uses an IAM role specified for the restore operation. To learn how to specify this IAM role, see Performing Entire EC2 Instance Restore (step 3). The IAM role must have permissions to access the following CMKs:

- CMKs with which the cloud-native snapshot is encrypted (source CMKs).
- A CMK with which you want to encrypt EBS volumes of the restored EC2 instance (target CMK).
Cross-Account Restore of EC2 Instance to Same AWS Region

To restore an EC2 instance in a different AWS account to the same AWS Region where the cloud-native snapshot resides, Veeam Backup for AWS performs the following steps:

1. Shares the encrypted cloud-native snapshot with the target AWS account.
   To share the encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for creating cloud-native snapshots (if you restore from a snapshot) or for copying and storing snapshot replicas (if you restore from a snapshot replica). The IAM role must have permissions to access CMKs with which the cloud-native snapshot is encrypted (source CMKs).

   **IMPORTANT**
   According to AWS limitations, cloud-native snapshots encrypted with the default key for EBS encryption (aws/ebs alias) cannot be shared between AWS accounts. Thus, if the cloud-native snapshot is encrypted with the default key for EBS encryption, Veeam Backup for AWS will not be able to share the snapshot and the restore process will fail. For more information, see this Veeam KB article.

2. Creates an EC2 instance in the target AWS account in the same AWS Region where the snapshot resides in the source AWS account.

3. Creates encrypted EBS volumes from the shared encrypted snapshot and attaches them to the created EC2 instance.
   To create and encrypt EBS volumes, Veeam Backup for AWS uses an IAM role specified for the restore operation. To learn how to specify this IAM role, see Performing Entire EC2 Instance Restore (step 3). The IAM role must have permissions to access the following CMKs:
   - The CMKs with which the cloud-native snapshot is encrypted (source CMKs).
   - A CMK with which you want to encrypt EBS volumes of the restored EC2 instance (target CMK).
Cross-Account Restore of EC2 Instance to Different AWS Region

To restore an EC2 instance to a different AWS Region in a different AWS account, Veeam Backup for AWS performs the following steps:

1. Shares the encrypted cloud-native snapshot with the target AWS account.

   To share the encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for creating cloud-native snapshots (if you restore from a snapshot) or for copying and storing snapshot replicas (if you restore from a snapshot replica). The IAM role must have permissions to access the following CMKs:
   - CMKs with which the cloud-native snapshot is encrypted (source CMKs).
   - A CMK with which you want to encrypt EBS volumes of the restored EC2 instance (target CMK).

   **IMPORTANT**

   According to AWS limitations, cloud-native snapshots encrypted with the default key for EBS encryption (aws/ebs alias) cannot be shared between AWS accounts. Thus, if the cloud-native snapshot is encrypted with the default key for EBS encryption, Veeam Backup for AWS will not be able to share the snapshot and the restore process will fail. For more information, see this Veeam KB article.

2. Copies the shared snapshot to the target AWS Region in the target AWS account.

3. Creates an EC2 instance in the target AWS Region in the target AWS account.

4. Creates encrypted EBS volumes from the shared encrypted snapshot and attaches them to the created EC2 instance.

   To copy the snapshot, create and encrypt EBS volumes, Veeam Backup for AWS uses an IAM role specified for the restore operation. To learn how to specify this IAM role, see Performing Entire EC2 Instance Restore (step 3). The IAM role must have permissions to access the following CMKs:
   - The CMKs with which the cloud-native snapshot is encrypted (source CMKs)
   - The CMK with which you want to encrypt EBS volumes of the restored EC2 instance (target CMK).
Restore of RDS Instance to Different AWS Region

To restore an RDS instance to a different AWS Region in the same AWS account where the cloud-native snapshot resides, Veeam Backup for AWS performs the following steps:

1. Copies the encrypted cloud-native snapshot to the target AWS Region.
2. Creates an RDS instance from the copied encrypted snapshot in the target AWS Region.

To copy the encrypted snapshot, and to create the RDS instance, Veeam Backup for AWS uses an IAM role specified for the restore operation. To learn how to specify this IAM role, see Performing RDS Instance Restore (step 3). The IAM role must have permissions to access the following CMKs:

- A CMK with which the cloud-native snapshot is encrypted (source CMK).
- A CMK with which you want to encrypt the restored RDS instance (target CMK).

Cross-Account Restore of RDS Instance to Same AWS Region

To restore an RDS instance in a different AWS account to the same AWS Region where the cloud-native snapshot resides, Veeam Backup for AWS performs the following steps:

1. Shares the encrypted cloud-native snapshot with the target AWS account.

To share the encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for creating cloud-native snapshots (if you restore from a snapshot) or for copying and storing snapshot replicas (if you restore from a snapshot replica). The IAM role must have permissions to access an CMK with which the cloud-native snapshot is encrypted (source CMK).

**IMPORTANT**

According to AWS limitations, cloud-native snapshots encrypted with the default encryption key (aws/rds alias) cannot be shared between AWS accounts. Thus, if the cloud-native snapshot is encrypted with the default encryption key, Veeam Backup for AWS will not be able to share the snapshot and the restore process will fail. For more information, see this Veeam KB article.
2. In the target AWS account, copies the shared snapshot to the same AWS Region where the snapshot resides in the source AWS account, and re-encrypts the snapshot with the CMKs that you specified to encrypt the restored RDS instance.

To copy the shared encrypted snapshot and to re-encrypt it, Veeam Backup for AWS uses an IAM role specified for the restore operation. To learn how to specify this IAM role, see Performing RDS Instance Restore (step 3). The IAM role must have permissions to access the following CMKs:

- The CMK with which the cloud-native snapshot is encrypted (source CMK).
- A CMK with which you want to encrypt the restored RDS instance (target CMK).

3. Creates an encrypted RDS instance from the copied encrypted snapshot in the target AWS account in the same AWS Region where the snapshot resides in the source AWS account.

To create and encrypt the RDS instance, Veeam Backup for AWS uses an IAM role specified for the restore operation. To learn how to specify this IAM role, see Performing RDS Instance Restore (step 3). The IAM role must have permissions to access the CMK with which you want to encrypt the restored RDS instance (target CMK).

Cross-Account Restore of RDS Instance to Different AWS Region

To restore an RDS instance to a different AWS Region in a different AWS account, Veeam Backup for AWS performs the following steps:

1. Shares the encrypted cloud-native snapshot with the target AWS account.

To share the encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for creating cloud-native snapshots (if you restore from a snapshot) or for copying and storing snapshot replicas (if you restore from a snapshot replica). The IAM role must have permissions to access the following CMKs:

- A CMK with which the cloud-native snapshot is encrypted (source CMK).
- A CMK with which you want to encrypt the restored RDS instance (target CMK).
According to AWS limitations, cloud-native snapshots encrypted with the default encryption key (aws/rds alias) cannot be shared between AWS accounts. Thus, if the cloud-native snapshot is encrypted with the default encryption key, Veeam Backup for AWS will not be able to share the snapshot and the restore process will fail. For more information, see this Veeam KB article.

2. In the target AWS account, copies the shared snapshot to the same AWS Region where the snapshot resides in the source AWS account.

To copy the shared encrypted snapshot, Veeam Backup for AWS uses an IAM role specified for the restore operation. To learn how to specify this IAM role, see Performing RDS Instance Restore (step 3). The IAM role must have permissions to access the CMK with which the cloud-native snapshot is encrypted (source CMK).

3. Copies the copied encrypted snapshot to the target AWS Region in the target AWS account and re-encrypts the snapshot with the CMK specified to encrypt the restored RDS Instance.

5. Creates an encrypted RDS instance in the target AWS Region in the target AWS account.

To copy and re-encrypt the snapshot, create and encrypt the RDS instance, Veeam Backup for AWS uses an IAM role specified for the restore operation. To learn how to specify this IAM role, see Performing RDS Instance Restore (step 3). The IAM role must have permissions to access the CMK with which you want to encrypt the restored RDS instance (target CMK).
Creating Image-Level Backups

The process of creating an image-level backup of an EC2 instance with encrypted EBS volumes differs depending on whether a worker instance processing EBS volume data is launched in the same AWS account or not:

- Creating the image-level backup in the same AWS account where the worker instance is launched.
- Creating the image-level backup in an AWS account that is different from the AWS account where the worker instance is launched.

Creating Image-Level Backup in Same AWS Account

If a worker instance is launched in the same AWS account where the processed EC2 instance resides, Veeam Backup for AWS performs the following steps:

1. Creates an encrypted cloud-native snapshot of the EC2 instance.
2. Creates encrypted EBS volumes from the snapshot, and then attaches them to the worker instance to read and further transfer EBS volume data to an S3 repository.

To access the data, Veeam Backup for AWS uses an IAM role specified to launch worker instances. To learn how to specify this IAM role, see Configuring Worker Instance Settings. The IAM role must have permissions to access CMKs with which EBS volumes of the EC2 instance are encrypted (source CMKs).
Creating Cross-Account Image-Level Backup

If a worker instance is launched in an AWS account different from the AWS account where the processed EC2 instance resides, Veeam Backup for AWS performs the following steps:

1. Creates an encrypted cloud-native snapshot of the EC2 instance.
2. Shares the created snapshot with the AWS account where the worker instance is launched.
   
   To share the encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for creating cloud-native snapshots. To learn how to specify this IAM role, see Creating EC2 Backup Policies. The IAM role must have permissions to access CMKs with which EBS volumes of the EC2 instance are encrypted (source CMKs).

   **IMPORTANT**
   
   If EBS volumes of the EC2 instance are encrypted with the default key for EBS encryption (aws/ebs alias), Veeam Backup for AWS will not be able to share the snapshot with another AWS account and the backup process will fail. For more information, see this Veeam KB article.

3. Creates encrypted EBS volumes from the shared encrypted snapshot, and then attaches them to the worker instance to read and further transfer EBS volume data to an S3 repository.

   Note that according to AWS requirements, EBS volumes created from encrypted snapshots must also be encrypted. Thus, Veeam Backup for AWS encrypts re-created EBS volumes with the default encryption key specified for the AWS Region where the worker instance is launched.

   To access the data, Veeam Backup for AWS uses an IAM role specified to launch worker instances. To learn how to specify this IAM role, see Configuring Worker Instance Settings. The IAM role must have permissions to access the following CMKs:

   - The CMKs with which EBS volumes of the EC2 instance are encrypted (source CMKs).
   - The default encryption key specified for the AWS Region where the worker instance is launched.

![Diagram of Creating Cross-Account Image-Level Backup](image.png)
Restoring From Image-Level Backups

The process of restoring an EC2 instance with encrypted EBS volumes from an image-level backup differs depending on whether a worker instance is launched in the same AWS account to which you perform restore or not:

- Performing restore from the image-level backup to the AWS account where the worker instance is launched.
- Performing restore from the image-level backup to an AWS account that is different from the AWS account where the worker instance is launched.

NOTE
Consider the following:

- An AWS account that owns an IAM role specified for launching worker instances is also referred to as the source AWS account.
- An AWS account to which you restore an instance is also referred to as the target AWS account.
- Veeam Backup for AWS always launches a worker instance in a target AWS Region specified in restore settings. For more information, see Managing Worker Instances.

Restore to Same AWS Account

If a worker instance is launched in the same AWS account where the restored EC2 instance will reside, to encrypt EBS volumes of the restored EC2 instance, Veeam Backup for AWS uses an IAM role specified to launch worker instances. To learn how to specify this IAM role, see Configuring Worker Instance Settings. The IAM role must have permissions to access to the CMK with which you want to encrypt EBS volumes of the restored EC2 instance.

Cross-Account Restore

If a worker instance is launched in an AWS account that is different from the AWS account where the restored EC2 instance will reside, Veeam Backup for AWS performs the following steps:

1. Creates empty EBS volumes in the target AWS Region in the source AWS account and attaches them to the worker instance. To protect data that will be restored to these volumes, Veeam Backup for AWS encrypts the created EBS volumes with the default encryption key specified for the target AWS Region.
   
   To encrypt the volumes, Veeam Backup for AWS uses an IAM role specified to launch worker instances. To learn how to specify this IAM role, see Configuring Worker Instance Settings. The IAM role must have permissions to access to the default encryption key specified for the target AWS Region in the source AWS account.

2. Restores backed-up data to the empty EBS volumes on the worker instance.

3. Creates an encrypted cloud-native snapshot of the EBS volumes with the restored data.

4. Shares the created snapshot with the target AWS account.
According to AWS limitations, snapshots encrypted with the default key for EBS encryption (aws/ebs alias) cannot be shared between AWS accounts. Thus, if the default encryption key specified for the target AWS Region in the source AWS account is the default key for EBS encryption, Veeam Backup for AWS will not be able to share the snapshot and the restore process will fail. For more information, see this Veeam KB article.

5. Creates an EC2 instance in the target AWS Region within the target AWS account.

6. Creates encrypted EBS volumes from the shared encrypted snapshot and attaches them to the created EC2 instance.

To create and encrypt EBS volumes, Veeam Backup for AWS uses an IAM role specified for the restore operation. To learn how to specify this IAM role, see Performing Entire EC2 Instance Restore (step 3). The IAM role must have permissions to access the following CMKs:

- The default encryption key specified for the target AWS Region in the source AWS account.
- A CMK with which you want to encrypt EBS volumes of the restored EC2 instance (target CMK).
Viewing Session Statistics

For each performed data protection or disaster recovery operation, Veeam Backup for AWS starts a new session and stores its records in the configuration database. You can track real-time statistics of all running and completed operations on the Sessions Log page.

To view the full list of tasks executed during an operation, click the link in the Status column. To view the full list of instances processed during an operation, click the link in the Items column.

TIP

If you want to specify the time period during which VB for Google must keep session records in the configuration database, follow the instructions provided in section Configuring Global Retention Settings.
Collecting Object Properties

You can export properties of objects managed by Veeam Backup for AWS as a single file in the CSV or XML format. To do that, navigate to the necessary tab and click Export. Veeam Backup for AWS will save the file with the exported data to the default download directory on the local machine.

**NOTE**

Even if you try to export properties of a specific object, Veeam Backup for AWS will still export all properties of all objects present on the currently opened tab.
Updating Veeam Backup for AWS

Veeam Backup for AWS allows you to check for new product versions and available package updates, download and install them from the Web UI.

It is recommended that you timely install available package updates to avoid performance issues while working with the product. For example, timely installed security updates may help you prevent potential security issues and reduce the risk of compromising sensitive data.

- Checking for Updates
- Installing Updates
- Viewing Updates History

Checking for Updates

Veeam Backup for AWS automatically notifies you about newly released product versions and package updates available for the operating system running on the backup appliance. However, you can check for available updates manually if required:

1. Switch to the Configuration page.
2. Navigate to Support Information > Updates.
3. Click Check and view updates.
If new updates are available, Veeam Backup for AWS will display them on the Updates tab of the Veeam Backup for AWS Updater page. To view detailed information on an update, select the check box next to the update and click What’s new?

### Installing Updates

To download and install new product versions and available package updates, you can use either of the following options:

- **Install updates immediately**
- **Schedule update installation**

You can also set a reminder to send update notifications.

### Installing Updates

**IMPORTANT**

Before you install a product update, make sure all backup policies are disabled and restore tasks are finished. Otherwise, the update process will interrupt running activities, which may result in data loss.

To download and install available product and package updates:

1. Open the Veeam Backup for AWS Updater page:
   a. Switch to the Configuration page.
   b. Navigate to Support Information.
   c. On the Updates tab, click Check and view updates.
2. On the **Veeam Backup for AWS Updater** page, do the following:

   a. In the **Updates are available for this system** section, select check boxes next to the necessary updates.

   b. In the **Choose action** section, select the **Install updates now** option, select the **Reboot automatically after install if required** check box to allow Veeam Backup for AWS to reboot the backup appliance if needed, and then click **Install Updates Now**.

**NOTE**

The updater may require you to read and accept the Veeam license agreement and the 3rd party components license agreement. If you reject the agreements, you will not be able to continue installation.

---

Veeam Backup for AWS will download and install the updates; the results of the installation process will be displayed on the **History** tab. Keep in mind that it may take several minutes for the installation process to complete.

**NOTE**

When installing product updates, Veeam Backup for AWS restarts all services running on the backup appliance, including the Web UI service. That is why Veeam Backup for AWS will log you out when the update process completes.
Scheduling Update Installation

You can instruct Veeam Backup for AWS to automatically download and install available product versions and package updates on a specific date at a specific time:

1. On the Veeam Backup for AWS Updater page, in the Updates are available for this system section, select check boxes next to the necessary updates.

2. In the Choose action section, do the following:

   a. Select the Schedule updates installation option and configure the necessary schedule.

   IMPORTANT

   When selecting a date and time when updates must be installed, make sure no backup policies are scheduled to run on the selected time. Otherwise, the update process will interrupt the running activities, which may result in data loss.

   b. Select the Reboot automatically after install if required check box to allow Veeam Backup for AWS to reboot the backup appliance if needed.

   c. Click Schedule Updates.

Veeam Backup for AWS will automatically download and install the updates on the selected date at the selected time; the results of the installation process will be displayed on the History tab.
Setting Update Reminder

If you have not decided when to install updates, you can set an update reminder — instruct Veeam Backup for AWS to send an update notification later.

To do that, on the Veeam Backup for AWS Updater page, in the Choose action section, do the following:

1. Select the Remind me later option and choose when you want to receive the reminder.
   - If you select the Next Week option, Veeam Backup for AWS will send the reminder next Monday.
2. Click Remind me later.
Viewing Updates History

To see the results of the update installation performed on the backup appliance, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Support Information > Updates**.
3. Click **Check and view updates**.
4. On the **Veeam Backup for AWS** page, switch to the **History** tab.

For each date when an update was installed, the **Veeam Backup for AWS Updater** page will display the name of the update and its status (whether the installation process completed successfully, completed with warnings or failed to complete).

To download logs for the installed updates, select the necessary date in the **Date** section, and click **View Full Log**. Veeam Backup for AWS will save the logs as a single file to the default download directory on the local machine.

<table>
<thead>
<tr>
<th>Updates</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update sessions history</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Package</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 14, 2020, 02:30 PM</td>
<td>Common CA certificates (20190110-18:04:1)</td>
<td>Success</td>
</tr>
<tr>
<td>June 4, 2020, 08:10 PM</td>
<td>Microsoft .NET Core SDK 3.1.300 (3.1.300-1)</td>
<td>Success</td>
</tr>
<tr>
<td>May 30, 2020, 06:02 PM</td>
<td>JSON manipulation library - shared library (0.12.1-1:3ubuntu0.3)</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>Secure Sockets Layer toolkit - cryptographic utility (1.1.1-1:3ubuntu2.1-18.04.6)</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>Veeam Backup for AWS (2.0.0.601)</td>
<td>Success</td>
</tr>
</tbody>
</table>
Getting Technical Support

If you have any questions or issues with Veeam Backup for AWS, you can search for a resolution on Veeam R&D Forums or submit a support case in the Veeam Customer Support Portal.

When you submit a support case, it is recommended that you provide the Veeam Customer Support Team with the following information:

- Version information for the product and its infrastructure components
- The error message or an accurate description of the problem you are facing
- Log files

Viewing Product Details

To view the product details:

1. Switch to the Configuration page.
2. Navigate to Support Information.

The About section of the Updates tab displays the following information:

- Server Version — the currently installed version of Veeam Backup for AWS.
- AWS ID — the ID of the AWS account where Veeam Backup for AWS is installed.
- Support ID — the ID of the Veeam support contract.
Downloading Product Logs

To download the product logs, do the following:

1. Switch to the **Download Logs** tab.
2. Click **Download Logs**.
3. In the **Download Logs** window, specify a time interval for which logs must be collected:
   - Select the **Collect logs for the last** option if you want to collect data for a specific number of days in the past.
   - Select the **Collect logs for the time period from** option if you want to collect data for a specific period of time in the past.
4. Click **OK**.

Veeam Backup for AWS will collect logs for the specified time interval and save them to the default download folder on the local machine in a single log.zip archive.