TABLES

1  Typographical conventions................................................................. 8
2  Maximum change rates AVE supports for file server and mixed environments........ 13
3  Minimum requirements for AVE.............................................................. 13
4  AVE virtual disk requirements............................................................... 14
5  Additional AVE software installation requirements....................................... 14
6  Inbound ports for the AWS security group............................................... 19
7  Outbound ports for the AWS security group............................................. 21
8  Inbound ports for Linux gateways........................................................ 32
9  Inbound ports for Windows gateways..................................................... 32
10 EC2 instance type selection by AVE instance size....................................... 50
As part of an effort to improve the product lines, revisions of the software and hardware are periodically released. Therefore, some functions that are described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact the technical support professional when a product does not function correctly or does not function as described in this document.

Note
This document was accurate at publication time. To find the latest version of this document, go to Online Support (https://support.EMC.com).

Purpose
This guide describes how to install the Avamar Virtual Edition solution, a single-node, non-RAIN Avamar server that runs as an Amazon Web Services (AWS) instance.

Audience
The information in this guide is primarily intended for system administrators who are responsible for installing and maintaining Avamar virtual servers.

Revision history
The following table presents the revision history of this document.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>02</td>
<td>April 19, 2019</td>
<td>Updated installation procedures for the AWS Marketplace, moved alternate installation methods to an appendix</td>
</tr>
<tr>
<td>01</td>
<td>July 7, 2018</td>
<td>GA release of Avamar 18.1</td>
</tr>
</tbody>
</table>

Related documentation
The following publications provide additional information:

- Avamar Release Notes
- Avamar Administration Guide
- Avamar Operational Best Practices Guide
- Avamar Product Security Guide
- Avamar Backup Clients User Guide
Special notice conventions used in this document
These conventions are used for special notices.

⚠️ **DANGER**
Indicates a hazardous situation which, if not avoided, results in death or serious injury.

⚠️ **WARNING**
Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

⚠️ **CAUTION**
Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

⚠️ **NOTICE**
Addresses practices that are not related to personal injury.

**Note**
 Presents information that is important, but not hazard-related.

**Typographical conventions**
These type style conventions are used in this document.

**Table 1** Typographical conventions

<table>
<thead>
<tr>
<th>Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)</td>
</tr>
<tr>
<td><strong>Italic</strong></td>
<td>Used for full titles of publications that are referenced in text</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Used for:</td>
</tr>
<tr>
<td></td>
<td>• System code</td>
</tr>
<tr>
<td></td>
<td>• System output, such as an error message or script</td>
</tr>
<tr>
<td></td>
<td>• Pathnames, filenames, prompts, and syntax</td>
</tr>
<tr>
<td></td>
<td>• Commands and options</td>
</tr>
<tr>
<td><strong>Monospace italic</strong></td>
<td>Used for variables</td>
</tr>
<tr>
<td><strong>Monospace bold</strong></td>
<td>Used for user input</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets enclose optional values</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{ }</td>
<td>Braces enclose content that the user must specify, such as x or y or z</td>
</tr>
<tr>
<td>...</td>
<td>Ellipses indicate nonessential information that is omitted from the example</td>
</tr>
</tbody>
</table>
Where to get help
The Avamar support page provides access to licensing information, product documentation, advisories, and downloads, as well as how-to and troubleshooting information. This information may resolve a product issue before contacting Customer Support.

To access the Avamar support page:
1. Go to https://support.EMC.com/products.
2. Type a product name in the Find a Product by Name box.
3. Select the product from the list that appears.
4. Click the arrow next to the Find a Product by Name box.
5. (Optional) Add the product to the My Products list by clicking Add to My Saved Products in the upper right corner of the Support by Product page.

Comments and suggestions
Comments and suggestions help to continue to improve the accuracy, organization, and overall quality of the user publications. Send comments and suggestions about this document to DPAD.Doc.Feedback@emc.com.

Please include the following information:
- Product name and version
- Document name, part number, and revision (for example, 01)
- Page numbers
- Other details to help address documentation issues
PREFACE
CHAPTER 1

Introduction

This chapter includes the following topics:

- Overview of Avamar Virtual Edition for Amazon Web Services .................. 12
- Appropriate environments for AVE .......................................................... 12
- Preinstallation requirements and best practices ........................................ 13
Overview of Avamar Virtual Edition for Amazon Web Services

Avamar Virtual Edition (AVE) is a single-node non-RAIN (Redundant Array of Independent Nodes) Avamar server that runs as a virtual machine in an Amazon Web Services (AWS) cloud environment. AVE integrates the latest version of Avamar software as an Amazon Machine Image (AMI).

AVE is certified to provide support for AWS GovCloud (US) which provides the ability for U.S. residents (government agencies and customers) to move sensitive workloads into the cloud. AWS GovCloud (US) addresses specific regulatory and compliance requirements.

The AWS GovCloud (US) User Guide provides information about, and details on, setting up an AWS GovCloud (US) account.

See the compatibility guide on Online Support (http://compatibilityguide.emc.com:8080/CompGuideApp) for specific information about supported versions of AVE software.

AVE is similar to single-node Avamar servers in the following ways:

- Runs autonomously as a target for all Avamar client backups
- Supports replication in the cloud.

AVE on AWS can be used to replicate on-premises physical Avamar servers and AVEs, including non-AWS types of AVEs. However, because of security considerations, replication should be performed by using a VPN, VPC, or a direct connect link.

AVE supports the following configurations: 0.5 TB, 1 TB, 2 TB, and 4 TB licensed capacity. AVE is not scalable to a multi-node Avamar server and resizing the virtual machine is not supported. You can increase storage capacity by deploying additional AVE virtual machines, and then divide backups among them. Or you can replicate the data to another AVE server, delete the smaller virtual machine, create a larger virtual machine, and replicate the data back to the larger virtual machine.

Appropriate environments for AVE

The following factors have the most direct impact on the long-term reliability, availability, and supportability of the AVE virtual machine:

- I/O performance capability of the AVE storage subsystem
- Amount of data added daily to the AVE virtual machine (change rate)
- Capacity that is utilized within the AVE virtual machine

Specifications in this section and AVE virtual disk requirements on page 14, describe minimum or maximum requirements for these factors. AVE generally performs better when I/O performance is higher. Change rate and utilized capacity are also lower. To maximize the capacity the AVE virtual machine can use, the daily change rate of the data AVE protects must be balanced with adequate I/O performance.

The first step in determining the proper implementation of AVE is to establish which kind of customer environment AVE is used to protect, file server or mixed environment. File server environments include file system data and mixed environments include file system data and structured data (for example, database data).
The following table describes the maximum change rates that AVE supports for file server and mixed environments.

When creating the AWS instance for the AVE, you should select the appropriate instance type for the appropriate change rates for the AVE.

**Table 2 Maximum change rates AVE supports for file server and mixed environments**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>File server data</th>
<th>Mixed data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.5 TB AVE</td>
<td>Less than 2 GB per day</td>
<td>Less than 5 GB per day</td>
</tr>
<tr>
<td>1 TB AVE</td>
<td>Less than 4 GB per day</td>
<td>Less than 10 GB per day</td>
</tr>
<tr>
<td>2 TB AVE</td>
<td>Less than 8 GB per day</td>
<td>Less than 20 GB per day</td>
</tr>
<tr>
<td>4 TB AVE</td>
<td>Less than 20 GB per day</td>
<td>Less than 20 GB per day</td>
</tr>
</tbody>
</table>

Actual results depend on the retention policy and the actual data change rate. When the daily change rate exceeds the limits that are specified in the previous table, deploy a single or multi-node Avamar server.

### Preinstallation requirements and best practices

Before you install an AVE virtual machine, follow the preinstallation requirements and review the best practices in the following sections.

- The default password is no longer a fixed value. Instead, the default password is now the private IPv4 address for the AVE virtual machine.
- Direct root access via SSH is no longer allowed, before or after installation of the Avamar software.
- The SSH interface is no longer accessible via username/password authentication. Instead, authentication requires SSH keys. This restriction applies even if you install the AVE without an SSH key.

#### Note

Using third party tools to create clones or exact copies of deployed Avamar Virtual Edition systems is known to cause issues. Cloning of Avamar Virtual Edition systems is not supported.

### System requirements

The following table defines the minimum system requirements for each size of AVE. When creating the AWS instance, you should select the appropriate instance type for the minimum system requirements for the AVE.

**Table 3 Minimum requirements for AVE**

<table>
<thead>
<tr>
<th></th>
<th>0.5 TB AVE</th>
<th>1 TB AVE</th>
<th>2TB AVE</th>
<th>4 TB AVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>Minimum two 2 GHz processors</td>
<td>Minimum two 2 GHz processors</td>
<td>Minimum two 2 GHz processors</td>
<td>Minimum four 2 GHz processors</td>
</tr>
<tr>
<td>Memory</td>
<td>6 GB</td>
<td>8 GB</td>
<td>16 GB</td>
<td>36 GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>900 GB</td>
<td>1,650 GB</td>
<td>3,150 GB</td>
<td>6,150 GB</td>
</tr>
</tbody>
</table>
### Table 3 Minimum requirements for AVE (continued)

<table>
<thead>
<tr>
<th></th>
<th>0.5 TB AVE</th>
<th>1 TB AVE</th>
<th>2TB AVE</th>
<th>4 TB AVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network connection</td>
<td>1 GbE connection</td>
<td>1 GbE connection</td>
<td>1 GbE connection</td>
<td>1 GbE connection</td>
</tr>
</tbody>
</table>

### AVE virtual disk requirements

The AVE disk layout comprises one operating system disk (126 GB) and several storage partitions (250 GB, 1000 GB, or 2000 GB, depending on the AVE configuration).

The OS disk stores the operating system, Avamar application, and log files.

The storage partitions store the backup data. Backup data is evenly distributed across the storage partitions. The primary amount of the disk read, write, and seek usage occurs on the storage partitions.

In addition to the OS partition, the following table defines the number and size of virtual disks that are required for each AVE configuration.

### Table 4 AVE virtual disk requirements

<table>
<thead>
<tr>
<th>AVE configuration</th>
<th>Number of virtual disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.5 TB</td>
<td>3 storage partitions (250 GB each)</td>
</tr>
<tr>
<td>1 TB</td>
<td>6 storage partitions (250 GB each)</td>
</tr>
<tr>
<td>2 TB</td>
<td>3 storage partitions (1000 GB each)</td>
</tr>
<tr>
<td>4 TB</td>
<td>6 storage partitions (1000 GB each)</td>
</tr>
</tbody>
</table>

Because SSD volumes have better performance than other volume types, Avamar recommends SSD for all volumes. However, SSD volumes incur a larger cost to the customer. Customers should balance performance and budget when selecting the volume type.

### Software requirements

Before you install AVE, ensure that you have the software that is listed in the following table.

### Table 5 Additional AVE software installation requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>AWS account subscription</td>
</tr>
<tr>
<td></td>
<td>AWS command-line interface (CLI), running on a separate system from the AVE instance.</td>
</tr>
<tr>
<td>Files</td>
<td>AVE for AWS installation package</td>
</tr>
</tbody>
</table>

Support for application databases in standalone configuration only

Backup and recovery of the following applications are supported with AVE on AWS. However, these applications are supported in standalone configuration only. Clustered configurations of application databases are not supported with AVE on AWS.
• SQL
• Exchange
• SharePoint
• Lotus
• DB2
• Sybase
• SAP
• Oracle
CHAPTER 2

Installation and Upgrade

This chapter includes the following topics:

- Installation ................................................................. 18
- Prerequisites .............................................................. 18
- Install AVE from the AWS Marketplace ...................... 22
- Install AVE/DDVE from the AWS Marketplace with CloudFormation .... 26
- AWS security best practices .......................................... 31
- Install and configure the Avamar software ..................... 33
- Upgrading the Avamar software .................................... 34
Installation

Avamar provides multiple deployment methods for virtual machines on AWS. This chapter includes the following preferred installation methods:

- Installing AVE from the AVE Amazon Machine Image (AMI) image in the AWS marketplace.
- Installing AVE and Data Domain Virtual Edition (DDVE) together with AWS CloudFormation.

Alternate Installation Methods on page 37 contains more information about installation methods that are not covered here, but which provide additional flexibility or options. Most alternate installation methods are variations on the methods in this chapter.

Prerequisites

Before you select an installation method, complete the following items that apply to all installation methods:

Procedure

1. (Optional) Install the AWS CLI tools.
   
   Some alternate installation methods use the AWS CLI tools.

2. Open the AWS EC2 Console and select the region where you want to run the instance.

3. Create or select a virtual private cloud (VPC) to contain the AVE (and DDVE, where applicable) instance.
   
   The AWS documentation provides more information. Place the AVE and DDVE instances in the same VPC as the workloads that they protect.

   Note the name of the VPC, as well as the associated subnet and availability zone for later use.

4. If you are deploying DDVE, create a VPC endpoint for connectivity to Amazon S3 storage.
   
   The Data Domain Virtual Edition Installation and Administration Guide provides more information.

5. If you are deploying DDVE, create an S3 bucket and an identity and access management (IAM) role.
   
   The Data Domain Virtual Edition Installation and Administration Guide provides more information.

   Note the name of the S3 bucket and IAM role for later use.

6. Create a key pair by performing the following substeps:
   
   a. From the navigation pane, select Network & Security > Key Pairs.

   b. Click Create Key Pair.

   c. Type a name for the key pair and then click Create.

   The new key pair appears in the list of key pairs.
AWS automatically downloads a copy of the private key with the filename `keypair-name.pem` to the local computer. Save this file for later use.

7. Create a security group by performing the following substeps:
   a. From the navigation pane, select **Network & Security > Security Groups**.
   b. Click **Create Security Group**.
   c. Type a name and a description for the security group.
   d. From the **VPC** drop-down, select an available VPC.
   e. Add inbound and outbound rules according to the tables in Security group settings on page 19.
   f. Click **Create**.

The new security group appears in the list of security groups.

### Security group settings

The following tables describe the rules that should be added to an AWS security group with an AVE instance.

---

**Note**

Recent versions of Avamar remove support for HTTP access to TCP port 80. Use the HTTPS ports 443 to access these services instead.

---

#### Inbound ports

**Note**

If you want to restrict the source of traffic, set the source with IPv4 or IPv6 CIDR block, or a single IPv4 or IPv6 address.

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>Port Range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom ICMP Rule - IPv4</td>
<td>Time Exceeded</td>
<td>All</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom ICMP Rule - IPv6</td>
<td>Time Exceeded</td>
<td>All</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom ICMP Rule - IPv4</td>
<td>Destination</td>
<td>Unreachable</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom ICMP Rule - IPv6</td>
<td>Destination</td>
<td>Unreachable</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom ICMP Rule - IPv4</td>
<td>Echo Request</td>
<td>N/A</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom ICMP Rule - IPv6</td>
<td>Echo Request</td>
<td>N/A</td>
<td>::/0</td>
</tr>
<tr>
<td>SSH</td>
<td>TCP</td>
<td>22</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>SSH</td>
<td>TCP</td>
<td>22</td>
<td>::/0</td>
</tr>
</tbody>
</table>
Table 6 Inbound ports for the AWS security group (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>Port Range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>TCP</td>
<td>443</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP</td>
<td>443</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>161</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>161</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom UDP Rule</td>
<td>UDP</td>
<td>161</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom UDP Rule</td>
<td>UDP</td>
<td>161</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>163</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>163</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom UDP Rule</td>
<td>UDP</td>
<td>163</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom UDP Rule</td>
<td>UDP</td>
<td>163</td>
<td>::/0</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>700</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>700</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>7543</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>7543</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>7778 - 7781</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>7778 - 7781</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>8543</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>8543</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>9090</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>9090</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>9443</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>9443</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>27000</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>27000</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>28001 - 28002</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>28001 - 28002</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>28810 - 28819</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>28810 - 28819</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>29000</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>29000</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>30001 - 30003</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>
### Table 6 Inbound ports for the AWS security group (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>Port Range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>30001 - 30003</td>
<td>::/0</td>
</tr>
</tbody>
</table>

### Outbound ports

**Note**

If you want to restrict the source of traffic, set the source with IPv4 or IPv6 CIDR block, or a single IPv4 or IPv6 address.

### Table 7 Outbound ports for the AWS security group

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>Port Range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom ICMP Rule - IPv4</td>
<td>Echo Request</td>
<td>N/A</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom ICMP Rule - IPv6</td>
<td>Echo Request</td>
<td>N/A</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>7</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>7</td>
<td>::/0</td>
</tr>
<tr>
<td>SSH</td>
<td>TCP</td>
<td>22</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>SMTP</td>
<td>TCP</td>
<td>25</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>DNS (UDP)</td>
<td>UDP</td>
<td>53</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>DNS (UDP)</td>
<td>UDP</td>
<td>53</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>111</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>111</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>UDP</td>
<td>111</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>UDP</td>
<td>111</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>161</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>161</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom UDP Rule</td>
<td>UDP</td>
<td>161</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom UDP Rule</td>
<td>UDP</td>
<td>161</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>163</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>163</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom UDP Rule</td>
<td>UDP</td>
<td>163</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom UDP Rule</td>
<td>UDP</td>
<td>163</td>
<td>::/0</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>
### Table 7 Outbound ports for the AWS security group (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>Port Range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>700</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>700</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>2049</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>2049</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom UDP Rule</td>
<td>UDP</td>
<td>2049</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom UDP Rule</td>
<td>UDP</td>
<td>2052</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>2052</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom UDP Rule</td>
<td>UDP</td>
<td>2052</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>3008</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>3008</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>8443</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>8443</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>8888</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>8888</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>9443</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>9443</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>27000</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>27000</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>28001-28010</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>28001-28010</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>29000</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>29000</td>
<td>::/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>30001-30010</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>30001-30010</td>
<td>::/0</td>
</tr>
</tbody>
</table>

## Install AVE from the AWS Marketplace

The following topics describe how to install an AVE virtual machine from the AMI image in the AWS Marketplace, and then prepare the virtual machine for Avamar.
software installation. This method saves time by eliminating the need to upload and convert a virtual appliance file.

Before you can use the AMI image in the AWS Marketplace, you must subscribe to AVE and accept the software terms. Only the first launch requires you to subscribe and accept the software terms. After you complete this task once, you do not need to complete it again.

The AWS documentation provides more information about subscribing to software and the different methods of deploying virtual machine instances.

**Subscribe to the AVE AMI image**

Locate and subscribe to the AVE AMI image in the AWS Marketplace, and accept the software terms.

**Procedure**

1. Open the AWS Marketplace.
2. Search the AWS Marketplace for Avamar, and then select Avamar Virtual Edition.
   The Product Overview page opens.
3. Click Continue to Subscribe.
   The Subscribe to this software page opens.
4. Review the software terms, and then click Accept Terms.
   The AWS Marketplace subscribes you to AVE and displays a notification.
5. Wait for AWS to complete the subscription process.
   When the subscription becomes active, the AWS Marketplace displays a confirmation message. The Continue to Configuration button becomes available.

**Deploy an AVE virtual machine from the EC2 dashboard**

Use the EC2 dashboard to configure and deploy an instance of AVE from the image in the AWS Marketplace.

**Procedure**

1. Open the AWS EC2 Console and select the correct region.
2. From the EC2 console dashboard, click Launch Instance.
   The Launch instance wizard opens to the Choose an Amazon Machine Image (AMI) tab.
3. From the navigation area on the left, select the AWS Marketplace category.
4. Search the AWS Marketplace for Avamar, and then locate Avamar Virtual Edition.
5. Click Select.
   The product information page appears.
6. Review the product details and then click Continue.
   The Launch instance wizard moves to the Choose an Instance Type tab.
7. From the list of instance types, select a type that corresponds to the system requirements for the selected capacity configuration.
8. Click **Next: Configure Instance Details**.
   The *Launch instance* wizard moves to the *Configure Instance Details* tab.

9. Click **Next: Add Storage**.
   The *Launch instance* wizard moves to the *Add Storage* tab.

10. For the root volume, from the *Volume Type* drop-down, select *General Purpose SSD (gp2)* or *Magnetic (standard)*.
    Because SSD volumes have better performance than other volume types, Avamar recommends *General Purpose SSD (gp2)* for all volumes. However, SSD volumes incur a larger cost to the customer. Customers should balance performance and budget when selecting the volume type.

11. Add the required storage volumes by completing the following substeps:
    a. Click **Add New Volume**.
       The *Launch instance* wizard adds a volume with default values.
    b. For *Size*, type the size that corresponds to the storage volumes for the selected capacity configuration.
       *AVE virtual disk requirements* on page 14 provides information about required disk sizes.
    c. For *Volume Type*, select *General Purpose SSD (gp2)* or *Magnetic (standard)*.
       Repeat this step for all required volumes. *AVE virtual disk requirements* on page 14 provides information about the number of required disks and sizes.

    **Note**
    Verify that all of the storage partitions are the same size before continuing.

12. Click **Next: Add Tags**.
    The *Launch instance* wizard moves to the *Add Tags* tab.

13. Click **Next: Configure Security Group**.
    The *Launch instance* wizard moves to the *Configure Security Group* tab.

14. For *Assign a security group*, select *Select an existing security group*.

15. From the list of security groups, select the security group that you created during the prerequisite task and then verify the port rules.

16. Click **Review and Launch**.
    The wizard validates the configuration and provides recommendations on certain selections.

17. Review the recommendations and correct any errors.
    If the wizard has no changes to recommend, continue to the next step.
    If the wizard recommends changes to the configuration, evaluate the recommendations, make any necessary changes, and then click **Next**.
18. Click Launch.
   The **Select an existing key pair or create a new key pair** dialog box opens.

19. Select **Choose an existing key pair** from the drop-down.

20. From the **Select a key pair** drop-down, select the key pair that you created during the prerequisite task.

21. Check the box to acknowledge the warning regarding access to the private key file.
   The wizard enables the **Launch instances** button.

22. Click **Launch instances**.
   The **Launch instance** wizard starts the deployment process.

23. Use the EC2 console to monitor the deployment progress and respond to any problems.
   The EC2 console displays a notification when the deployment completes.

24. (Optional) Configure an elastic IP address for the instance by completing the following substeps:
   a. From the navigation pane, select **Network & Security > Elastic IPs**.
      The EC2 console displays a list of available elastic IP addresses.
   b. If there are no available elastic IP addresses, click **Allocate new address**.
   c. For **IPv4 address pool**, select an available option that corresponds to your network environment.
   d. Click **Allocate**.
      The EC2 console displays a status notification.
   e. Click **Close**.
      The EC2 console returns to the list of elastic IP addresses.
   f. Right-click an available elastic IP address and select **Associate address**.
      The **Associate address** window opens.
   g. From the **Instance** drop-down, select the new AVE instance.
   h. From the **Private IP** drop-down, select an available private IP address.
      Note the private IP address for later use. This value is the default password for AVE.
   i. Click **Associate**.
      The EC2 console displays a status notification.
   j. Click **Close**.

25. Obtain the AVE private IPv4 address by performing one of the following substeps:
   If you configured an elastic IP address, you may already have this value.
   a. Use the AWS EC2 web console to obtain the private IPv4 address.
      The **AWS documentation** provides more information.
   b. Use the AWS CLI to obtain the private IPv4 address by typing the following command:
aws ec2 describe-instances --instance-ids instance | grep PrivateIpAddress

Record the private IPv4 address for later use. This value is the default password for AVE.

26. Install the AVE.

Install and configure the Avamar software on page 33 contains instructions.

Note

After launching the instance, the AVE initializes and reboots automatically. During this process, which takes 10 to 20 minutes, the AVE installs drivers and an updated kernel. You cannot install the AVE until this process is complete because the AVE installation package, ave-config, is not available in the Avamar Installation Manager. SSH is also unavailable during this time.

Install AVE/DDVE from the AWS Marketplace with CloudFormation

The following topics describe how to use CloudFormation to automate the installation of AVE and DDVE virtual machines from the AWS Marketplace.

The complete deployment process consists of the following steps:

1. Subscribe to AVE and DDVE in the AWS Marketplace.
2. Provide configuration parameters for AVE and DDVE.
3. Deploy AVE and DDVE using CloudFormation.
4. Configure a secure gateway system.

Configuring a secure gateway system is outside the scope of this installation guide.

CloudFormation templates are JSON files that simplify the deployment of multiple AWS resources and dependencies. In AWS, the combination of a CloudFormation template and associated resources forms a stack. Use the CloudFormation template to programmatically deploy the combined AVE and DDVE solution.

The following publications provide additional information to complete the deployment process:

- Avamar Administration Guide
- Avamar and Data Domain System Integration Guide
- Data Domain Virtual Edition in Amazon Web Services (AWS) Installation and Administration Guide
- Data Domain Virtual Edition Installation and Administration Guide
- Data Domain Operating System Initial Configuration Guide

The following AWS documentation provides additional information about using CloudFormation templates with the AWS console and for the AWS CLI:

- AWS CloudFormation Templates
- Working with AWS CloudFormation Templates
- cloudformation

If you intend to use the downloaded CloudFormation template with an alternate installation method, obtain the template for AVE and DDVE from Online Support.
Subscribe to the AVE/DDVE AMI image

The following instructions describe how to locate and subscribe to the AVE and DDVE AMI images in the AWS Marketplace, and then locate the AMI IDs for later use.

Procedure

1. Open the AWS Marketplace.
2. Search the AWS Marketplace for Avamar, and then select Avamar and Data Domain Virtual Edition.
   The Product Overview page appears.
3. Click Continue to Subscribe.
   The Subscribe to this software page appears.
4. Review the terms and conditions.
5. Click Continue to Configuration.
   The Configure this software page appears.
6. Select a region for deployment.
7. Confirm the supplied AVE and DDVE versions.
8. Review the estimated pricing.
9. Click Continue to Launch.
   The Launch this software page appears.

Configure the AVE and DDVE virtual machines

The updated CloudFormation template provided with the combined AVE/DDVE AMI image in the AWS Marketplace performs additional configuration on the deployed virtual machines, similar to completing the ave-config workflow package.

For the most part, configuration takes place in multiple sections of the Select Template tab on the CloudFormation Create stack page.

Configure common settings

The settings in the Common Configurations section apply to the new CloudFormation stack and to both virtual machines.

Procedure

1. On the Launch this software page, review the configuration details.
2. From the Choose Action drop-down list, select Launch CloudFormation.
3. Click Launch.
   The Create stack page opens to the Select Template tab.
4. For **Choose a template**, verify that the **Specify an Amazon S3 template URL** radio button is preselected, and that the URL field is prepopulated.

5. Click **Next**.

   The **Create stack** page moves to the **Specify Details** tab.

6. For **Stack name**, type a unique name for the new CloudFormation stack that forms a container for AVE and DDVE deployment.

7. For **Network**, select the ID of the VPC that you created for AVE and DDVE.

8. For **Subnet**, select the ID of the subnet that you created within the VPC.

9. For **Availability Zone**, select the availability zone that you chose for the VPC.

10. For **SSH Location**, type an IP address range from which AVE and DDVE should permit SSH access, in the format 10.2.3.4/24.

    Since AVE and DDVE receive private IP addresses, supply an IP address range within the private network to which the secure gateway provides access. Addresses outside this range are not permitted SSH access.

11. For **Key Pair**, select the name of the SSH keypair that you created for AVE and DDVE.

    **Configure the AVE instance**

    The settings in the **AVE Configurations** section apply specifically to the AVE instance.

    **Procedure**

    1. For **AVE Capacity**, select the installed capacity for this AVE instance, in TB: either **2** or **4** TB.

       This selection governs the choice of EC2 instance type and the automatic creation of virtual disks, as detailed in **AVE virtual disk requirements** on page 14.

       | AVE instance size | EC2 instance type |
       |-------------------|-------------------|
       | 2 TB              | m4.xlarge         |
       | 4 TB              | m4.2xlarge        |

    2. For **AVE Volume Type**, select the volume type for the AVE instance: either **gp2** or **st1**.

       The **AWS documentation** provides more information on the different volume types.

    3. For **AVE Common Password** and **AVE Common Password Confirmation**, type a password for the AVE OS admin and root user accounts, and for the Avamar software.

       The **Avamar Product Security Guide** provides information about password complexity rules.

    4. For **System Time Zone Name**, select the POSIX time zone name.

    5. For **Email Sender Address**, type the email address from which to send ConnectEMC notifications and alerts.

    6. For **Email Server**, type the hostname or IP address of the email server from which ConnectEMC should send emails.

       This is also the email server that sends EmailHome messages for high priority events.
7. For **Site Name**, type a description for the AVE location. For example:
   - Company name
   - Company’s site ID
   - Company’s address

8. For **Dell EMC Site ID/CSI Party ID**, type the assigned site ID or CSI party ID (maximum 32 characters).
   You can find this ID on the Service Center at [http://support.emc.com/servicecenter](http://support.emc.com/servicecenter) by clicking **Administration > View and manage company information**. An incorrect site ID may lead to delays when you contact Customer Support.
   If you cannot determine your site ID, leave the field blank. In this case, AVE does not send dial-home requests to Dell EMC.

9. For **Company Name**, type the name of the company that owns the AVE instance.

10. For **Company Contact Name**, type the name of the administrator managing the AVE instance.

11. For **Company Contact Phone Number**, type the phone number of the administrator managing the AVE instance.

12. For **Company Contact Email Address**, type the email address of the administrator managing the AVE instance.

Configure the DDVE instance

The settings in the **DDVE Configurations** section apply specifically to the DDVE instance.

**Procedure**

1. For **DDVE Capacity**, select the installed capacity for this DDVE instance, in TB.
   This selection governs the choice of EC2 instance type and the automatic creation of EBS virtual disks, as detailed in *Data Domain Virtual Edition in Amazon Web Services (AWS) Installation and Administration Guide*.

<table>
<thead>
<tr>
<th>DDVE instance size</th>
<th>EC2 instance type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 16 TB</td>
<td>m4.xlarge</td>
</tr>
<tr>
<td>17 to 32 TB</td>
<td>m4.2xlarge</td>
</tr>
<tr>
<td>33 to 96 TB</td>
<td>m4.4xlarge</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DDVE instance size</th>
<th>EBS metadata disk allocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 10 TB</td>
<td>1 TB</td>
</tr>
<tr>
<td>11 to 20 TB</td>
<td>2 TB</td>
</tr>
<tr>
<td>21 to 30 TB</td>
<td>3 TB</td>
</tr>
<tr>
<td>31 to 40 TB</td>
<td>4 TB</td>
</tr>
<tr>
<td>41 to 50 TB</td>
<td>5 TB</td>
</tr>
</tbody>
</table>
### DDVE instance size | EBS metadata disk allocation
--- | ---
51 to 60 TB | 6 TB
61 to 70 TB | 7 TB
71 to 80 TB | 8 TB
81 to 90 TB | 9 TB
91 to 96 TB | 10 TB

2. For **IAM Role for S3 Access**, type the name of the IAM role that you created during the prerequisites for access to S3 storage.

3. For **S3 Bucket Name**, type the name of the S3 bucket that you created during the prerequisites.

4. For **DDBoost Login Name**, type the login name for the DDBoost user.
   
   This name can be a new or existing account. Valid characters include letters, numbers, hyphen (-), and underscore (_).

5. For **DDVE Common Password** and **DDVE Common Password Confirmation**, type a password for the DDVE admin accounts.

   The *Data Domain Virtual Edition Installation and Administration Guide* provides information about password complexity rules.

6. For **SNMP Community String**, type the SNMP community string that is used to monitor the Data Domain systems.

   Blank spaces, colon (:), semicolon (;), dollar-sign ($), single quotes ('), and backquotes (`) are not allowed.

7. Click **Next**.

   The Create stack page opens to the **Options** tab.

---

### Deploy the AVE/DDVE stack

After you supply all of the configuration parameters, create the CloudFormation stack and use it to deploy the AVE and DDVE instances.

**Procedure**

1. On the **Options** tab, click **Next**.

   The Create stack page opens to the **Review** tab.

2. Review the parameters for AVE and DDVE, and the estimated cost.

3. Click **Create**.

   The AWS console starts the AVE and DDVE deployment process.

   CloudFormation automatically configures the AVE and DDVE instances by using the values that you provided.

4. Use the **Events** tab on the AWS portal to monitor deployment status.

   Deployment can take more than one hour.

5. (Optional) Configure an elastic IP address for the instance by completing the following substeps:

   a. From the navigation pane, select **Network & Security > Elastic IPs**.

      The EC2 console displays a list of available elastic IP addresses.
b. If there are no available elastic IP addresses, click **Allocate new address**.

c. For **IPv4 address pool**, select an available option that corresponds to your network environment.

d. Click **Allocate**.

   The EC2 console displays a status notification.

e. Click **Close**.

   The EC2 console returns to the list of elastic IP addresses.

f. Right-click an available elastic IP address and select **Associate address**.

   The **Associate address** window opens.

g. From the **Instance** drop-down, select the new AVE instance.

h. From the **Private IP** drop-down, select an available private IP address.

   Note the private IP address for later use. This value is the default password for AVE.

i. Click **Associate**.

   The EC2 console displays a status notification.

j. Click **Close**.

6. Obtain the AVE private IPv4 address by performing one of the following substeps:

   If you configured an elastic IP address, you may already have this value.

   a. Use the AWS EC2 web console to obtain the private IPv4 address.

      The AWS documentation provides more information.

   b. Use the AWS CLI to obtain the private IPv4 address by typing the following command:

      ```bash
      aws ec2 describe-instances --instance-ids instance | grep PrivateIpAddress
      ```

      Record the private IPv4 address for later use.

7. To monitor configuration status, complete the following substeps:

   a. Establish an SSH session to the AVE instance and log in as the admin user.

   b. Check the log file status by typing the following command:

      ```bash
      tail -f /usr/local/avamar/var/ave_ddve_cloud_init.log
      ```

      When configuration completes successfully, the following message appears in the log file:

      ```
      Completed ave-config
      ```

---

**AWS security best practices**

Consider the following issues when deploying AVE to an AWS environment, to create as secure an environment as possible.

**Follow AWS network security best practices**

Disable the public IP address when launching AVE
Because AVE in the cloud only backs up resources in the same Virtual Private Cloud (VPC), AVE does not need a public IP address. Isolating AVE from public network access helps to secure AVE in a cloud environment.

When creating or configuring the AVE instance, at Step 3, Configure Instance Details, select Disable for the Auto-assign Public IP option to disable the public IP address for AVE.

Set up an additional secure gateway system for AVE maintenance in the cloud
You can also set up a secure gateway system, with a public IP address, in the same VPC as AVE and the clients. Perform all operation and maintenance of AVE through this secure gateway system. Configure the gateway system for high security by, for example, defining the security group to enable only a must-have level of network access.

- For Linux gateways, enable only the SSH port, with key-based SSH access, and the VNC port range. Restrict the permitted original network address (a white-listed IP address or range is suggested).
- For Window gateways, enable only the RDP port. Restrict the permitted original network address (a white-listed IP address or range is suggested).

You can install Avamar Administrator on the secure gateway system. In this case, configure a security group for the following ports:

**Table 8 Inbound ports for Linux gateways**

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>Port range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom TCP rule</td>
<td>TCP</td>
<td>7778–7781</td>
<td>Private subnet</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>Private subnet</td>
</tr>
<tr>
<td>SSH</td>
<td>TCP</td>
<td>22</td>
<td>0.0.0.0/0</td>
</tr>
</tbody>
</table>

**Table 9 Inbound ports for Windows gateways**

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>Port range</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom TCP rule</td>
<td>TCP</td>
<td>7778–7781</td>
<td>Private subnet</td>
</tr>
<tr>
<td>RDP</td>
<td>TCP</td>
<td>3389</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>Private subnet</td>
</tr>
<tr>
<td>SSH</td>
<td>TCP</td>
<td>22</td>
<td>Private subnet</td>
</tr>
</tbody>
</table>

In these tables, the term 'private subnet' refers to the virtual network that contains AVE and related virtual machines.

Key-based SSH access is required
Use an SSH public key when launching AVE in AWS. Prerequisites on page 18 contains information about creating a key pair and selecting it when launching the instance. If you do not select a key pair when launching an instance, you cannot log in to the SSH interface with username/password authentication.

Use a security group with custom IP address ranges
In addition to the ports, restrict the source and destination network address ranges in the inbound/outbound security group. Enable only the necessary ports for both inbound and outbound network access, as defined in Security group settings on page 19.
Timely application of Avamar security patches
Avamar releases quarterly OS security patch roll-ups. Apply these patches to AVE on a regular basis.

Enable terminal protection
Accidentally terminating or deleting AVE could result in a disaster scenario with potential data loss. Therefore, it is a best practice to select the Enable terminal protection option when configuring the AVE instance.

Install and configure the Avamar software
To install the Avamar software on a new AVE virtual machine, follow the instructions that are included in the help file for the AVE installation workflow on the SW Releases page of the Avamar Installation Manager.

Procedure

1. Open a web browser and log in to the Avamar Installation Manager:
   The Avamar Administration Guide provides more information.
   a. Type the following URL:
      
      https://Avamar-server:7543/avi
      
      where Avamar-server is the IP address or the resolvable hostname of the Avamar server.
      
      The Avamar Installation Manager login page appears.
   b. Log in as the root user for the Avamar software with the default password.
      The default password is the private IPv4 address for the virtual machine.
   c. Click Login.
      
      The Avamar Installation Manager opens to the Package Selection page.

2. In the menu bar, click SW Releases, and then select the ave-config workflow package from the Package List.

3. Click the ? button next to the ave-config package.
   

4. Review the workflow guide for information about the required and optional user input fields.
   After you click Install, you are no longer able to access the workflow guide.

5. Click Install next to the AVE installation package ave-config.
   
   The Installation Setup page displays.

6. On the Installation Setup page, provide the required information in the user input fields for each tab, and then click Continue.
   
   The Installation Progress page displays.

7. On the Installation Progress page, monitor the installation and respond to any installation problems:
   a. To resolve the problem, take the appropriate action.
   b. After resolving the problem, click Call Support.
      
      The Call Support dialog box appears.
c. Click **Issue resolved, continuing the installation.**
   
   The installation resumes.

   d. Repeat these substeps for all problems that occur during the installation.

### Upgrading the Avamar software

To upgrade the Avamar software on an AVE virtual machine, follow the instructions that are included in the workflow guide for the AVE upgrade workflow package on the **SW Releases** page of the **Avamar Installation Manager**.

**Procedure**

1. **Download the AVE upgrade workflow package for the appropriate version of AVE.**
   
   Download the required software from [https://support.emc.com/](https://support.emc.com/).
   
   You can also use the Avamar Download Manager or Local Downloader Service to download the software. The *Avamar Administration Guide* contains information about configuring and using the Avamar Download Manager and the Local Downloader Service.

2. **Log in to the Avamar Installation Manager by performing the following substeps:**
   
   a. Open a web browser and type the following URL:
      
      ```
      https://Avamar-server:7543/avi
      ```
      
      where Avamar-server is the IP address or the resolvable hostname of the Avamar server.
      
      **Note**
      
      Ensure that the hostname does not contain more than 63 characters.
      
      The Avamar Installation Manager login page appears. The *Avamar Administration Guide* contains information about the **Avamar Installation Manager**.
   
   b. Log in as the Avamar software root user.
      
      The root user password is typically created with the `ave_config` workflow when you install the Avamar software.
   
   c. Click **Login**.

3. **Upload the AVE upgrade workflow package that you downloaded in step 1 on page 34 by performing the following substeps:**
   
   a. Click **Repository**.
      
      The **Repository** tab appears.
   
   b. For **Package Upload**, click **Browse** and select the package to upload.
      
      Once the package upload completes, it automatically appears in the **Repository** table.

4. **Click **SW Upgrade**.**
   
   The **SW Upgrade** tab appears.

5. **Click the ? button for the AVE upgrade workflow package (AvamarUpgrade-version.avp) to open the workflow guide.**
6. Click **Upgrade**.

7. Monitor the upgrade progress on the **Installation Progress** page and respond to any problems:
   
a. To resolve the problem, take the appropriate action.

b. After resolving the problem, click **Call Support**.
   
The **Call Support** dialog box appears.

c. Click **Issue resolved, continuing the installation**.
   
The upgrade resumes.

d. Repeat these substeps for all problems that occur during the upgrade.

8. When the upgrade is complete, run the following optional, but recommended, packages:
   
   - `AvPlatformOsRollup_<year>-Q<q>-R<r>.avp`
   - `UpgradeClientDownloads-<version>.avp`
   - `UpgradeClientPluginCatalog-<version>.avp`
This appendix contains the following topics:

- Overview of alternate installation methods ........................................................ 38
- Install an AVE virtual machine from the AWS Marketplace (manual launch method) ............................................................................................................. 38
- Install an AVE virtual machine from a manually uploaded virtual appliance file .... 41
- Alternate CloudFormation installation methods for AVE/DDVE virtual appliances ................................................................. 46
Overview of alternate installation methods

This appendix provides instructions to install AVE virtual machines or combined AVE/DDVE virtual appliances by methods that are not covered in the Installation chapter. Use this appendix for environments where the methods are not available or are otherwise undesirable.

Perform the Prerequisites on page 18 before you start the procedures in this appendix.

Install an AVE virtual machine from the AWS Marketplace (manual launch method)

This section describes how to use the manual launch method to install an AVE virtual machine where you have already subscribed to the AVE AMI image in the AWS Marketplace. Use the procedures in this section if you do not want to use the EC2 dashboard.

The manual launch method creates an AVE instance without attached data disks or storage partitions, only a root disk for the operating system. A subsequent task configures and then attaches additional disks, which are composed of Elastic Block Storage (EBS) volumes, to the AVE instance.

Before you start the procedures in this section, subscribe to the AVE image in the AWS Marketplace.

AVE virtual disk requirements on page 14 provides information about the number of required disks and sizes. The AWS documentation provides more information about EBS volumes.

Deploy the AVE virtual machine (manual launch method)

From the AWS Marketplace, deploy an instance of AVE without attached data disks or storage partitions.

Procedure

1. Open the AWS Marketplace.
2. Locate the Hello, YourName menu in the upper right corner of the window.
3. From the Hello, YourName menu, select Your Marketplace Software.
   The Your Software Subscriptions page opens.
4. Locate Avamar Virtual Edition in the list of subscriptions and then click Launch More Software.
   The Configure this software page opens.
5. From the Software Version drop-down, select the correct version of AVE.
6. From the Region drop-down, select the correct AWS region.
7. Click Continue to Launch.
   The Launch this software page opens.
8. From the Choose Action drop-down, select Launch from Website.
9. From the EC2 Instance Type drop-down, select a type that corresponds to the system requirements for the selected capacity configuration.
Configure the AVE virtual machine (manual launch method)

Configure and attach additional virtual disks to the new AVE instance, perform final configuration, and then install the Avamar software.

Procedure

1. Stop the new AVE instance.

Wait for the instance to stop before continuing.

2. From the navigation pane, select Elastic Block Store > Volumes.

The EC2 console displays a list of available volumes.

3. Add the required storage volumes by completing the following substeps:

   a. Click Create Volume.

      The Create Volume window opens.

   b. For Volume Type, select General Purpose SSD (gp2) or Magnetic (standard).

      Because SSD volumes have better performance than other volume types, Avamar recommends General Purpose SSD (gp2) for all volumes. However, SSD volumes incur a larger cost to the customer. Customers should balance performance and budget when selecting the volume type.

   c. For Size, type the size that corresponds to the storage volumes for the selected capacity configuration.

      AVE virtual disk requirements on page 14 provides information about required disk sizes.

   d. From the Availability Zone drop-down, select a zone within the current region.

   e. Click Add tag.

   f. For Key, type Name.
g. For Value, type a unique name for the data disk so that you can identify it later.

h. Click Create Volume.
   The EC2 console displays a status notification.

i. Click Close.
   The EC2 console returns to the list of volumes.

Repeat this step for all required volumes. AVE virtual disk requirements on page 14 provides information about the number of required disks and sizes.

Note
Verify that all of the storage volumes are identical before continuing.

4. For each new volume, attach the volume to the instance by performing the following substeps:
   a. Right-click the volume and then select Attach Volume.
      The Attach Volume dialog box opens.
   b. Type the name or ID of the new AVE instance.
   c. Verify the default device mount point that AWS proposes.
   d. Click Attach.

5. From the navigation pane, select Instances > Instances.
   The EC2 console displays a list of available instances.

6. Start the new instance.
   Wait for the instance to start before continuing.

7. (Optional) Configure an elastic IP address for the instance by completing the following substeps:
   a. From the navigation pane, select Network & Security > Elastic IPs.
      The EC2 console displays a list of available elastic IP addresses.
   b. If there are no available elastic IP addresses, click Allocate new address.
   c. For IPv4 address pool, select an available option that corresponds to your network environment.
   d. Click Allocate.
      The EC2 console displays a status notification.
   e. Click Close.
      The EC2 console returns to the list of elastic IP addresses.
   f. Right-click an available elastic IP address and select Associate address.
      The Associate address window opens.
   g. From the Instance drop-down, select the new AVE instance.
   h. From the Private IP drop-down, select an available private IP address.
      Note the private IP address for later use. This value is the default password for AVE.
i. Click **Associate**.
   The EC2 console displays a status notification.

j. Click **Close**.

8. Obtain the AVE private IPv4 address by performing one of the following substeps:
   If you configured an elastic IP address, you may already have this value.
   a. Use the AWS EC2 web console to obtain the private IPv4 address.
      The [AWS documentation](#) provides more information.
   b. Use the AWS CLI to obtain the private IPv4 address by typing the following command:
      ```
      aws ec2 describe-instances --instance-ids instance | grep PrivateIpAddress
      ```
      Record the private IPv4 address for later use. This value is the default password for AVE.

9. Install the AVE.
   [Install and configure the Avamar software](#) on page 33 contains instructions.

---

**Note**

After launching the instance, the AVE initializes and reboots automatically. During this process, which takes 10 to 20 minutes, the AVE installs drivers and an updated kernel. You cannot install the AVE until this process is complete because the AVE installation package, `ave-config`, is not available in the **Avamar Installation Manager**. SSH is also unavailable during this time.

---

### Install an AVE virtual machine from a manually uploaded virtual appliance file

This section describes how to manually upload an AVE virtual appliance file and convert the upload to the Amazon Machine Image (AMI) format. You can then use the AWS EC2 console to deploy an AVE instance from the AMI.

Use these instructions to install a specific AVE build that may not be available in the [AWS Marketplace](#).

**Upload and convert the AVE virtual appliance file**

Obtain the AVE virtual appliance file from Support Zone, transfer the file to an AWS S3 bucket, and then convert the file to an AMI for deployment.

**Procedure**

1. Download the AVE virtual appliance file (`AWS-AVE-version-disk1.vmdk`) from [support.EMC.com](#), where `version` is the release and build number of the software to be installed.

   You can find the AVE virtual appliance file under the [Downloads](#) section for [Avamar Virtual Edition](#), or by searching by product for [Avamar Virtual Edition](#) and browsing for [Avamar Virtual Edition for Amazon Web Service Cloud](#).
2. Open the AWS Console Identity and Access Management (IAM) page.

3. Create or select a group. The group must have a minimum of the following permissions:
   - AmazonEC2FullAccess
   - AmazonS3FullAccess

4. Create or select a user with a minimum of Programmatic access and AWS Management Console access.

   Download a .csv file and save the Access key ID and Secret access key values. These values are very important.

   **NOTICE**

   You must have the Access key ID and Secret access key available later in this procedure. When creating a user, save these values locally by selecting Download csv.

5. Upload the virtual appliance file by performing the following substeps:
   a. Open the AWS S3 Console and select the region where you want to run the instance.
   b. Click Create Bucket.
   c. Type a name and click Create.
   d. Click the bucket name to open it.
   e. Click Upload.
   f. Click Add files and select the virtual appliance file that you downloaded in a previous step.

6. Import the virtual appliance file from the S3 bucket to an Amazon Machine Image (AMI) by performing the following substeps:
   a. From the command line, type the following command:

   ```
   aws ec2 import-image --architecture x86_64 --platform Linux --region REGION --disk-containers "[{ "Format" : "vmdk", "UserBucket" : {"S3Bucket" : "<BUCKET_NAME>", "S3Key": "<VMDK_FILENAME>"}}]"
   ```

   where:
   - **REGION** is the region where you want to run the instance. For example, us-west-1.
   - **BUCKET_NAME** is the name of the S3 bucket.
   - **VMDK_FILENAME** is the name of the virtual appliance file that you downloaded in a previous step.

   Output similar to the following appears:

   ```
   "Status": "active",
   "Platform": "Linux",
   "Architecture": "x86_64",
   "SnapshotDetails": [{
      "UserBucket": {
        "S3Bucket": "<BUCKET_NAME>",
        "S3Key": "<VMDK_FILENAME>"
      }
    ]
   ```

   Alternate Installation Methods
b. Use the **ImportTaskID** to monitor the task status by typing the following command on one line:

```bash
aws ec2 describe-import-image-tasks --import-task-ids
IMPORT_TASK_ID --region REGION
```

where:
- **BUCKET_NAME** is the ImportTaskID from the previous command.
- **REGION** is the region where you want to run the instance. For example, `us-west-1`.

Output similar to the following appears:

```json
{
  "ImportImageTasks": [
    {
      "Status": "completed",
      "LicenseType": "BYOL",
      "ImageId": "ami-2bbd994b",
      "Platform": "Linux",
      "Architecture": "x86_64",
      "SnapshotDetails": [
        {
          "UserBucket": {
            "S3Bucket": "<BUCKET_NAME>",
            "S3Key": "<VMDK_FILENAME>"
          },
          "SnapshotId": "snap-0b8fdb6bc5ace3d61",
          "DiskImageSize": 5740812288.0,
          "DeviceName": "/dev/sda1",
          "Format": "VMDK"
        }
      ],
      "ImportTaskId": "import-ami-ffmbx7hu"
    }
  ]
}
```

When the `import-image` task completes, the **Status** field changes to `completed` and **ImageId** provides the AMI ID.

## Deploy AVE from the converted AMI image

Use the EC2 console to deploy an AVE virtual machine from the AMI image, and then install the Avamar software.

**Procedure**

1. Open the **AWS EC2 Console** and select the correct region.
2. From the navigation pane, select **Images > AMIs**.
   The EC2 console displays a list of available AMIs.
3. Select the correct AMI from the list, based on the AMI ID returned from the previous command.
4. Click Launch.

The **Launch instance** wizard opens to the **Choose an Instance Type** tab.

5. From the list of instance types, select a type that corresponds to the system requirements for the selected capacity configuration.

  **System requirements** on page 13 contains details about AVE system requirements. The wizard disables any instance types that do not apply to AVE.

6. Click **Next: Configure Instance Details**.

The **Launch instance** wizard moves to the **Configure Instance Details** tab.

7. Click **Next: Add Storage**.

The **Launch instance** wizard moves to the **Add Storage** tab.

8. For the root volume, from the **Volume Type** drop-down, select **General Purpose SSD (gp2)** or **Magnetic (standard)**.

Because SSD volumes have better performance than other volume types, **Avamar recommends** General Purpose SSD (gp2) for all volumes. However, SSD volumes incur a larger cost to the customer. Customers should balance performance and budget when selecting the volume type.

9. Add the required storage volumes by completing the following substeps:
   a. Click **Add New Volume**.

   The **Launch instance** wizard adds a volume with default values.
   
   b. For **Size**, type the size that corresponds to the storage volumes for the selected capacity configuration.

   **AVE virtual disk requirements** on page 14 provides information about required disk sizes.
   
   c. For **Volume Type**, select **General Purpose SSD (gp2)** or **Magnetic (standard)**.

   Repeat this step for all required volumes. **AVE virtual disk requirements** on page 14 provides information about the number of required disks and sizes.

   **Note**

   Verify that all of the storage partitions are the same size before continuing.

10. Click **Next: Add Tags**.

   The **Launch instance** wizard moves to the **Add Tags** tab.

11. Click **Next: Configure Security Group**.

   The **Launch instance** wizard moves to the **Configure Security Group** tab.

12. For **Assign a security group**, select **Select an existing security group**.

13. From the list of security groups, select the security group that you created during the prerequisite task and then verify the port rules.

14. Click **Review and Launch**.

   The wizard validates the configuration and provides recommendations on certain selections.
15. Review the recommendations and correct any errors.  
   If the wizard has no changes to recommend, continue to the next step.  
   If the wizard recommends changes to the configuration, evaluate the  
   recommendations, make any necessary changes, and then click **Next**.

16. Review the summary of the AVE configuration, including the estimated pricing  
   and the terms.

17. Click **Launch**.  
   The **Select an existing key pair or create a new key pair** dialog box opens.

18. Select **Choose an existing key pair from the drop-down**.

19. From the **Select a key pair** drop-down, select the key pair that you created  
   during the prerequisite task.

20. Check the box to acknowledge the warning regarding access to the private key  
   file.  
   The wizard enables the **Launch instances** button.

21. Click **Launch instances**.  
   The **Launch instance** wizard starts the deployment process.

22. Use the EC2 console to monitor the deployment progress and respond to any  
   problems.
   The EC2 console displays a notification when the deployment completes.

23. (Optional) Configure an elastic IP address for the instance by completing the  
   following substeps:
   a. From the navigation pane, select **Network & Security > Elastic IPs**.  
      The EC2 console displays a list of available elastic IP addresses.
   b. If there are no available elastic IP addresses, click **Allocate new address**.
   c. For **IPv4 address pool**, select an available option that corresponds to your  
      network environment.
   d. Click **Allocate**.  
      The EC2 console displays a status notification.
   e. Click **Close**.  
      The EC2 console returns to the list of elastic IP addresses.
   f. Right-click an available elastic IP address and select **Associate address**.  
      The **Associate address** window opens.
   g. From the **Instance** drop-down, select the new AVE instance.
   h. From the **Private IP** drop-down, select an available private IP address.  
      Note the private IP address for later use. This value is the default password  
      for AVE.
   i. Click **Associate**.  
      The EC2 console displays a status notification.
   j. Click **Close**.

24. Obtain the AVE private IPv4 address by performing one of the following  
   substeps:
If you configured an elastic IP address, you may already have this value.

a. Use the AWS EC2 web console to obtain the private IPv4 address.
   The AWS documentation provides more information.

b. Use the AWS CLI to obtain the private IPv4 address by typing the following command:
   ```bash
   aws ec2 describe-instances --instance-ids instance | grep PrivateIpAddress
   ```

Record the private IPv4 address for later use. This value is the default password for AVE.

25. Install the AVE.
   
   Install and configure the Avamar software on page 33 contains instructions.

   **Note**
   After launching the instance, the AVE initializes and reboots automatically. During this process, which takes 10 to 20 minutes, the AVE installs drivers and an updated kernel. You cannot install the AVE until this process is complete because the AVE installation package, **ave-config**, is not available in the Avamar Installation Manager. SSH is also unavailable during this time.

---

**Alternate CloudFormation installation methods for AVE/DDVE virtual appliances**

Alternate CloudFormation installation methods provide additional flexibility, such as instructions for the AWS CLI, and for manually uploading a combined AVE/DDVE virtual appliance file.

Select one of the following methods and complete the associated additional tasks.

To use the AWS CLI to install AVE and DDVE from the AWS Marketplace:

- **Locate the AVE and DDVE machine image IDs from the AWS Marketplace** on page 47.
- Review the CloudFormation template parameters on page 50.
- **Deploy AVE and DDVE from the AWS CLI** on page 52.

To manually upload and install a AVE and DDVE virtual appliance file:

- **Upload and convert the AVE/DDVE virtual appliance file** on page 48.
- Review the CloudFormation template parameters on page 50.
- One of the following:
  - **Deploy the converted AVE/DDVE AMI image from the AWS console** on page 51.
  - **Deploy AVE and DDVE from the AWS CLI** on page 52.
Locate the AVE and DDVE machine image IDs from the AWS Marketplace

Locate and subscribe to the AVE and DDVE AMI images in the AWS Marketplace, and then locate the AMI IDs for later use.

**Procedure**

1. Create a virtual private cloud (VPC) for AVE and DDVE.
   The [AWS documentation](https://aws.amazon.com/documentation) provides additional information.

2. Create a subnet for the VPC and specify an availability zone.
   The [AWS documentation](https://aws.amazon.com/documentation) provides additional information.

3. Open the AWS Console Identity and Access Management (IAM) page.

4. Create or select a group. The group must have a minimum of the following permissions:
   - AmazonEC2FullAccess
   - AmazonS3FullAccess

5. Create or select a user with a minimum of Programmatic access and AWS Management Console access.
   Download a .csv file and save the Access key ID and Secret access key values. These values are very important.
   
   **NOTICE**
   
   You must have the Access key ID and Secret access key available later in this procedure. When creating a user, save these values locally by selecting Download csv.

6. Open the AWS Marketplace.

7. Search the AWS Marketplace for Avamar, and then select Avamar Virtual Edition.
   The Product Details page appears.

8. Click Continue to Subscribe.
   The Launch on EC2 page appears.

9. Click Continue to Configuration.
   The Configure this software page appears.

10. Select a region for deployment.

11. Record the AVE AMI ID for later use.

12. Search the AWS Marketplace for Data Domain, and then select Data Domain Virtual Edition.
    The Product Details page appears.

13. Click Continue to Subscribe.
    The Launch on EC2 page appears.

14. Click Continue to Configuration.
    The Configure this software page appears.
15. For DDVE 4.0, select **Amazon Machine Image** from the list of fulfilment options.

16. Select a region for deployment.

17. Record the DDVE AMI ID for later use.

**After you finish**

Use the recorded AMI IDs to complete the CloudFormation template.

---

**Upload and convert the AVE/DDVE virtual appliance file**

CloudFormation uses this image for each automatic deployment. This task also configures several important prerequisite items. Record the indicated values for later use.

Uploading the virtual appliance file takes approximately 40 minutes. Converting the virtual appliance file to AMI format takes approximately 40 minutes.

**Procedure**

1. Download and decompress the AVE/DDVE virtual appliance file.
   
   Download the required software from https://support.emc.com/.

2. Open the AWS Console Identity and Access Management (IAM) page.

3. Create or select a group. The group must have a minimum of the following permissions:
   
   - AmazonEC2FullAccess
   - AmazonS3FullAccess

4. Create or select a user with a minimum of **Programmatic access** and **AWS Management Console** access.
   
   Download a .csv file and save the **Access key ID** and **Secret access key** values. These values are very important.

   **NOTICE**

   You must have the **Access key ID** and **Secret access key** available later in this procedure. When creating a user, save these values locally by selecting **Download csv**.

5. Upload the virtual appliance file by performing the following substeps:
   
   a. Open the **AWS S3 Console** and select the region where you want to run the instance.
   
   b. Click **Create Bucket**.
   
   c. Type a name and click **Create**.
   
   d. Click the bucket name to open it.
   
   e. Click **Upload**.
   
   f. Click **Add files** and select the virtual appliance file that you downloaded in a previous step.

6. Import the virtual appliance file from the S3 bucket to an Amazon Machine Image (AMI) by performing the following substeps:
a. From the command line, type the following command:

```bash
aws ec2 import-image --architecture x86_64 --platform Linux --region REGION --disk-containers "[{
  "Format" : "vmdk",
  "UserBucket" : {
    "S3Bucket" : "BUCKET_NAME",
    "S3Key" : "VMDK_FILENAME"}
}]
```

where:
- **REGION** is the region where you want to run the instance. For example, `us-west-1`.
- **BUCKET_NAME** is the name of the S3 bucket.
- **VMDK_FILENAME** is the name of the virtual appliance file that you downloaded in a previous step.

Output similar to the following appears:

```json
{
  "Status": "active",
  "Platform": "Linux",
  "Architecture": "x86_64",
  "SnapshotDetails": [
    {
      "UserBucket": {
        "S3Bucket": "<BUCKET_NAME>",
        "S3Key": "<VMDK_FILENAME>"
      },
      "DiskImageSize": 0.0,
      "Format": "VMDK"
    }
  ],
  "Progress": "2",
  "StatusMessage": "pending",
  "ImportTaskId": "import-ami-12mbx7hu"
}
```

b. Use the `ImportTaskID` to monitor the task status by typing the following command on one line:

```bash
aws ec2 describe-import-image-tasks --import-task-ids IMPORT_TASK_ID --region REGION
```

where:
- **BUCKET_NAME** is the `ImportTaskID` from the previous command.
- **REGION** is the region where you want to run the instance. For example, `us-west-1`.

Output similar to the following appears:

```json
{
  "ImportImageTasks": [
    {
      "Status": "completed",
      "LicenseType": "BYOL",
      "ImageId": "ami-2bbd994b",
      "Platform": "Linux",
      "Architecture": "x86_64",
      "SnapshotDetails": [
        {
          "UserBucket": {
            "S3Bucket": "<BUCKET_NAME>",
            "S3Key": "<VMDK_FILENAME>"
          },
          "SnapshotId": "snap-0b8f9db56bc5ace3d61",
          "DiskImageSize": 5740812288.0,
          "DeviceName": "/dev/sda1",
          "Format": "VMDK"
        }
      ],
      "DiskImageSize": 5740812288.0,
      "DeviceName": "/dev/sda1"
    }
  ],
  "StatusMessage": "complete",
  "ImportTaskId": "import-ami-12mbx7hu"
}
```
When the import-image task completes, the Status field changes to completed and ImageId provides the AMI ID.

7. Create a virtual private cloud (VPC) for AVE and DDVE.
   The AWS documentation provides additional information.

8. Create a subnet for the VPC and specify an availability zone.
   The AWS documentation provides additional information.

CloudFormation template parameters

These template parameters are common, whether you deploy the solution through the AWS Portal or through the AWS CLI. Use the following descriptions to provide parameters to the template:

- **Stack name**
  Required. Type a unique name for the new CloudFormation stack that forms a container for AVE and DDVE deployment.

- **VPC ID**
  Required. Select the ID of the new VPC that you created for AVE and DDVE.

- **Subnet ID**
  Required. Select the ID of the subnet that you created within the new VPC. AVE and DDVE are both deployed in this subnet.

- **Availability Zone**
  Required. Select the availability zone that you chose for the new VPC.

- **Key Pair Name**
  Required. Select the name of the new SSH keypair that you created for AVE and DDVE.

- **AVE AMI ID**
  Required. Provide the Amazon host ID that you recorded when you uploaded the AVE image.

- **AVE Instance Size**
  Select the installed capacity for this AVE instance, in TB: either 2 or 4 TB. This selection governs the choice of EC2 instance type and the automatic creation of virtual disks, as detailed in AVE virtual disk requirements on page 14.

<table>
<thead>
<tr>
<th>AVE instance size</th>
<th>EC2 instance type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 TB</td>
<td>m4.xlarge</td>
</tr>
<tr>
<td>4 TB</td>
<td>m4.2xlarge</td>
</tr>
</tbody>
</table>

- **AVE EBS volume type for all disks**
  Select the volume type for this AVE instance: either gp2 or st1. The AWS documentation provides more information on the different volume types.
**DDVE AMI ID**
Required. Provide the value that you recorded when you uploaded the DDVE image.

**DDVE Instance Type**
Select the EC2 instance type for the DDVE instance: either `m4.xlarge`, `m4.2xlarge`, or `m4.4xlarge`. The AWS documentation provides more information on the different EC2 instance types.

- `m4.xlarge` supports an 8 TB DDVE.
- `m4.2xlarge` and `m4.4xlarge` support a 16 TB DDVE.

**EBS volume size for the first data disk**
Select the virtual disk size for this DDVE instance: either `0.5TB`, `1TB`, `2TB`, or `3TB`, based on the available licensed capacity.

This value is only for the first data disk. Create additional disks, if required, after deployment via CloudFormation and before the DDVE configuration process.

The `0.5 TB` value is only for use with the evaluation license. Do not use this value for any other installations.

---

**Deploy the converted AVE/DDVE AMI image from the AWS console**

The AWS console provides a graphical interface for deployment of the virtual appliances.

**Procedure**

1. Extract `AVE_DDVE_CloudFormation.json` to a temporary folder on the local computer.
2. Return to the AWS console.
3. Click **Management Tools > CloudFormation**.
   The CloudFormation portal opens.
4. Click **Create Stack**.
   The Select Template page opens.
5. Click **Upload a template to Amazon S3**.
6. Click **Choose File**.
7. Browse to and select `AVE_DDVE_CloudFormation.json`.
8. Click **Next**.
   The Specify Details page opens.
9. Provide all required AVE and DDVE parameters.
   Some fields are preconfigured. CloudFormation template parameters on page 50 provides additional information on parameter values.
10. Click **Next**.
    The Options page opens. Do not define any tags or additional permissions on the Options page.
11. Click **Next**.
    The Review page opens.
12. Review the selections, values, and cost estimate.
13. Click Create.
Deployment may take 15–30 minutes. The CloudFormation console describes the progress of the stack creation process. Note all of the outputs from the stack creation process.

After you finish

Complete post-deployment configuration on page 53.

**Deploy AVE and DDVE from the AWS CLI**

This CloudFormation deployment method provides the required parameters in the AVE_DDVE_CloudFormation_parameters.json file.

**Procedure**

1. Extract AVE_DDVE_CloudFormation.json and AVE_DDVE_CloudFormation_parameters.json to a temporary folder on the local computer.
2. Edit AVE_DDVE_CloudFormation_parameters.json with a text editor and provide the required values.

CloudFormation template parameters on page 50 provides additional information. Each parameter in this file corresponds to an input field in the AWS console method.

For example:

```json
{
   "ParameterKey": "AVEAMIID",
   "ParameterValue": "ami-abcdef01"
},
{
   "ParameterKey": "DDVEAMIID",
   "ParameterValue": "ami-abcdef02"
},
{
   "ParameterKey": "AVEInstanceSize",
   "ParameterValue": "4TB"
},
{
   "ParameterKey": "AVEDiskType",
   "ParameterValue": "gp2"
},
{
   "ParameterKey": "DDVEInstanceType",
   "ParameterValue": "m4.xlarge"
},
{
   "ParameterKey": "AVEDiskType",
   "ParameterValue": "gp2"
},
{
   "ParameterKey": "DDVEInstanceType",
   "ParameterValue": "m4.xlarge"
},
{
   "ParameterKey": "AVEAMIID",
   "ParameterValue": "ami-abcdef01"
},
```

Alternate Installation Methods

52

Avamar Virtual Edition for Amazon Web Services 18.1 Installation and Upgrade Guide
3. Save and close the file.

4. In the AWS CLI, type the following command on one line:

```bash
aws cloudformation create-stack --stack-name <StackName> --template-body file://AVE_DDVE_CloudFormation.json --parameters file://AVE_DDVE_CloudFormation_parameters.json
```

where `<StackName>` is a unique name for this AVE and DDVE stack.

**Note**

You can also store the JSON files in an AWS S3 bucket and supply the URL of each file. The AWS documentation provides additional information.

Deployment may take 15–30 minutes. The CloudFormation console describes the progress of the stack creation process. Note all of the outputs from the stack creation process.

**After you finish**

Complete post-deployment configuration on page 53.

---

## Complete post-deployment configuration

These steps prepare the deployed AVE for installation of the Avamar software.

**Before you begin**

Note and record the stack creation status, and the AVIURL and DDSTMURL values from the stack creation task. Access to these URLs requires a secure gateway system, which is beyond the scope of this installation guide.

**Procedure**

1. (Optional) Configure an elastic IP address for the instance by completing the following substeps:
   a. From the navigation pane, select **Network & Security > Elastic IPs**.
      The EC2 console displays a list of available elastic IP addresses.
   b. If there are no available elastic IP addresses, click **Allocate new address**.
   c. For **IPv4 address pool**, select an available option that corresponds to your network environment.
   d. Click **Allocate**.
      The EC2 console displays a status notification.
   e. Click **Close**.
      The EC2 console returns to the list of elastic IP addresses.
   f. Right-click an available elastic IP address and select ** Associate address**.
      The **Associate address** window opens.
   g. From the **Instance** drop-down, select the new AVE instance.
h. From the **Private IP** drop-down, select an available private IP address.
   
   Note the private IP address for later use. This value is the default password for AVE.

i. Click **Associate**.
   
   The EC2 console displays a status notification.

j. Click **Close**.

2. Obtain the AVE private IPv4 address by performing one of the following substeps:
   
   If you configured an elastic IP address, you may already have this value.

   a. Use the AWS EC2 web console to obtain the private IPv4 address.
      
      The **AWS documentation** provides more information.

   b. Use the AWS CLI to obtain the private IPv4 address by typing the following command:
      
      ```
      aws ec2 describe-instances --instance-ids instance | grep PrivateIpAddress
      ```
      
      Record the private IPv4 address for later use. This value is the default password for AVE.

3. Configure a secure gateway system.

4. Configure the AVE instance.

   *Install and configure the Avamar software* on page 33 contains instructions.

---

**Note**

After launching the instance, the AVE initializes and reboots automatically.

During this process, which takes 10–20 minutes, the AVE installs drivers and an updated kernel. You cannot install the AVE until this process is complete because the AVE installation package, **ave-config**, is not available in the **Avamar Installation Manager**. SSH is also unavailable during this time.

5. Configure the DDVE instance.

   If you cannot access the DDVE instance from the secure gateway via HTTP or HTTPS, perform the following substeps:

   a. SSH to the DDVE instance and log in as the sysadmin user.

   b. Type the following command:
      
      ```
      adminaccess enable http/https
      ```

6. Attach the DDVE system to AVE.