Dell EMC Avamar Virtual Edition

Version 18.2

Installation and Upgrade Guide

302-005-128
REV 02
July 2019

DELL EMC

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

FIGURES

TABLES

Preface

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 a virtual machine in a variety of environments.

This publication supersedes the following documents:

- *Avamar Virtual Edition for VMware Installation and Upgrade Guide*
- *Avamar Virtual Edition for Microsoft Azure Installation and Upgrade Guide*
- *Avamar Virtual Edition for Microsoft Hyper-V Installation and Upgrade Guide*
- *Avamar Virtual Edition for OpenStack KVM Installation and Upgrade Guide*
- *Avamar Virtual Edition for Amazon Web Services Installation and Upgrade Guide*

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 1 Revision history

Revision	Date	Description
02	July 16, 2019	Updated installation procedures for the AWS Marketplace, moved alternate installation methods to an appendix. Updates for deployment in Azure Marketplace (all methods).
01	December 14, 2018	GA release of Avamar 18.2

Related documentation

The following publications provide additional information:

- *E-lab Navigator* at https://elabnavigator.emc.com/eln/elnhome
- *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 2 Typographical conventions

Bold	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)
Italic	Used for full titles of publications that are referenced in text
`Monospace`	Used for: • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
Monospace italic	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information that is omitted from the example

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://www.dell.com/support/home/us/en/19.
2. Type a product name in the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box.
3. Select the product from the list that appears. When you select a product, the **Product Support** page loads automatically.
4. (Optional) Add the product to the **My Products** list by clicking **Add to My Saved Products** in the upper right corner of the **Product Support** 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

CHAPTER 1

Introduction

This chapter includes the following topics:

Overview of Avamar Virtual Edition

Avamar Virtual Edition (AVE) is a single-node non-RAIN (Redundant Array of Independent Nodes) Avamar server that runs as a virtual machine in a variety of environments. AVE integrates the latest version of Avamar software with SUSE Linux as a pre-packaged virtual machine, instance, or machine image, depending on the environment.

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

- Runs autonomously as a target for all Avamar client backups
- Performs a replication to a physical Avamar server or another AVE
- Some configurations of AVE support replication in the cloud

Supported environments

Supported environments include:

- VMware ESXi 5.5, 6.0, 6.5, or 6.7
- Microsoft Azure
- Windows, using Hyper-V Manager
- OpenStack KVM cloud
- Amazon Web Services (AWS) cloud

See the *E-lab Navigator* at https://elabnavigator.emc.com/eln/elnhome for specific information about supported environments and software versions.

Licensed capacity configurations

AVE supports the following licensed capacity configurations, depending on the choice of environment:

Table 3 Licensed capacity configurations by environment

Capacity configuration	AVE on VMware	AVE on Azure	AVE on Hyper-V	AVE on OpenStack KVM	AVE on AWS
0.5 TB	Yes	Yes	Yes	Yes	Yes
1 TB	Yes	Yes	Yes	Yes	Yes
2 TB	Yes	Yes	Yes	Yes	Yes
4 TB	Yes	Yes	Yes	Yes	Yes
8 TB	Yes	Yes	Yes	No	Yes
16 TB	Yes	Yes	Yes	No	Yes

Scaling and resizing AVE

AVE is not scalable to a multi-node Avamar server, and resizing the virtual machine is not supported.

You can increase storage capacity by either of the following methods:

- Deploy additional AVE virtual machines, and then divide backups among the virtual machines.
- Replicate the data to another AVE server, delete the smaller virtual machine, create a larger virtual machine, and then replicate the data back to the larger virtual machine.

Environment-specific information

AVE on VMware

AVE on VMware supports backup of both physical and virtual clients. For physical clients, install the Avamar client software on each client. For virtual clients, there are two options for backups.

Virtual clients can be backed up through:

- Guest OS backups (requires installing the Avamar client software on each virtual machine).
- Host-based backups (requires a proxy server).

AVE on Azure

AVE on Azure is certified to support Azure Government Cloud (US), which provides the ability for U.S. residents (government agencies and customers) to move sensitive workloads into the cloud. Azure Government Cloud (US) addresses specific regulatory and compliance requirements. The Azure Government Cloud (US) User Guide provides information about, and details on, setting up an Azure Government Cloud (US) account.

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

AVE on AWS

AVE on AWS is certified to support 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.

AVE on AWS supports replication in the cloud and can be used to replicate on-premises physical and virtual Avamar servers, 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.

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 the Virtual disk requirements on page 21 for the AVE virtual disk requirements 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).

Maximum change rates

The following table describes the maximum change rates that AVE supports for file server and mixed environments:

Table 4 Maximum supported change rates for file server and mixed environments

Capacity configuration	File server data	Mixed data
0.5 TB AVE	Less than 2 GB per day	Less than 5 GB per day
1 TB AVE	Less than 4 GB per day	Less than 10 GB per day
2 TB AVE	Less than 8 GB per day	Less than 20 GB per day
4 TB AVE	Less than 20 GB per day	Less than 20 GB per day
8 TB AVE[a]	Less than 40 GB per day	Less than 40 GB per day
16 TB AVE[a]	Less than 80 GB per day	Less than 80 GB per day

a. Not all environments support this licensed capacity configuration.

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.

Environment-specific notes

AVE on AWS

When you create the AWS instance for AVE, select the correct instance type for the change rates.

Preinstallation requirements and best practices

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

Note: Using third party tools to create clones or exact copies of deployed AVE servers is known to cause issues. Cloning of AVE servers is not supported.

Environment-specific notes

AVE on Azure

- The default password is no longer a fixed value. Instead, the default password is the private IPv4 address for the AVE virtual machine.
- Direct root access via SSH is not allowed before or after installation of the Avamar software.

AVE on AWS

- 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 AVE without an SSH key.

System requirements

The following topics list the minimum system requirements for an AVE instance in each virtual environment.

System requirements for AVE on AWS

When you create the AWS instance, you should select an appropriate instance type for the minimum system requirements that are listed here.

The following table defines the minimum system requirements for each AVE capacity configuration.

Table 5 Minimum system requirements for AVE on AWS

Requirement	0.5 TB AVE	1 TB AVE	2 TB AVE
Processors	Minimum two 2 GHz processors	Minimum two 2 GHz processors	Minimum two 2 GHz processors
Memory	6 GB	8 GB	16 GB
Disk space	900 GB	1,650 GB	3,150 GB
Network connection	1 GbE connection		

Table 5 Minimum system requirements for AVE on AWS

Requirement	4 TB AVE	8 TB AVE	16 TB AVE
Processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors
Memory	36 GB	48 GB	96 GB
Disk space	6,150 GB	12,150 GB	24,150 GB
Network connection	1 GbE connection		

System requirements for AVE on Azure

The following table defines the minimum system requirements for each AVE capacity configuration.

Table 6 Minimum system requirements for AVE on Azure

Requirement	0.5 TB AVE	1 TB AVE	2 TB AVE
Processors	Minimum two 2 GHz processors	Minimum two 2 GHz processors	Minimum two 2 GHz processors
Memory	6 GB	6 GB	14 GB
Disk space	850 GB	1,600 GB	3,100 GB
Azure Standard Tier	A5	A6	A5
Network connection	1 GbE connection		

Table 6 Minimum system requirements for AVE on Azure

Requirement	4 TB AVE	8 TB AVE	16 TB AVE
Processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors
Memory	28 GB	48 GB	96 GB
Disk space	6,100 GB	12,150 GB	24,150 GB
Azure Standard Tier	A6	A7	A9
Network connection	1 GbE connection		

System requirements for AVE on OpenStack KVM

Consult the *E-lab Navigator* for supported versions of OpenStack.

The following table defines the minimum system requirements for each AVE capacity configuration.

Table 7 Minimum system requirements for AVE on OpenStack KVM

Requirement	0.5 TB AVE	1 TB AVE	2 TB AVE	4 TB AVE
Processors	Minimum two 2 GHz processors	Minimum two 2 GHz processors	Minimum two 2 GHz processors	Minimum four 2 GHz processors
Memory	6 GiB (6,144 MiB)	8 GiB (8,192 MiB)	16 GiB (16,384 MiB)	36 GiB (36,864 MiB)
Disk space[a]	900 GB	1,650 GB	3,150 GB	6,150 GB
Network connection	1 GbE connection			

a. Figures include both the 128 GB nova storage for the primary bootable disk, and required amounts of Cinder storage

System requirements for AVE on VMware

Consult the *E-lab Navigator* for supported versions of VMware ESXi.

The following table defines the minimum system requirements for each AVE capacity configuration.

Table 8 Minimum system requirements for AVE on VMware

Requirement	0.5 TB AVE	1 TB AVE	2 TB AVE
Processors	Minimum two 2 GHz processors	Minimum two 2 GHz processors	Minimum two 2 GHz processors
Memory	6 GB	8 GB	16 GB
Disk space	900 GB	1,650 GB	3,150 GB
Network connection	1 GbE connection		

Table 8 Minimum system requirements for AVE on VMware

Requirement	4 TB AVE	8 TB AVE	16 TB AVE
Processors	Minimum four 2 GHz processors	Minimum eight 2 GHz processors	Minimum sixteen 2 GHz processors
Memory	36 GB	48 GB	96 GB
Disk space	6,150 GB	12,150 GB	24,150 GB
Network connection	1 GbE connection		

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 capacity 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 portion of the disk read, write, and seek usage occurs on the storage partitions. To improve performance in the storage configuration, distribute the storage partitions across high-performance logical units, where applicable.

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

Table 9 Virtual disk requirements

Capacity configuration	Number of virtual disks
0.5 TB	3 storage partitions (250 GB each)
1 TB	6 storage partitions (250 GB each)
2 TB	3 storage partitions (1000 GB each)
4 TB	6 storage partitions (1000 GB each)
8 TB[a]	12 storage partitions (1000 GB each)
16 TB[a]	12 storage partitions (2000 GB each)

a. Not all environments support this licensed capacity configuration.

The task to prepare the virtual machine instance contains steps to ensure that all of the storage partitions are the same size.

Environment-specific notes

AVE on VMware

The AVE .ova installation creates three 250 GB storage partitions along with the OS disk and so requires approximately 900 GB of free disk space at installation.

However, the AVE .ovf installation does not create storage partitions during installation and therefore requires only enough disk space for the OS disk at installation. You can subsequently create storage partitions on other datastores.

AVE on OpenStack KVM

AVE requires approximately 900 GB of free disk space at installation.

AVE on AWS

Because SSD volumes have better performance than other volume types, Dell EMC 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.

Virtual disk configuration best practices

The following topics outline best practices for creating and configuring the virtual disks, where applicable.

Virtual disk configuration best practices for AVE on VMware

ESXi supports multiple disk formats. For AVE virtual machines, the initial configuration is Thick Provision Lazy Zeroed.

Note: AVE does not support thin provisioning.

After the initial installation, if you configure the virtual disks for the Thick Provision Eager Zeroed, you will get better initial performance because the first write to the disk will require fewer operations.

Note: See the VMware documentation for information on converting Lazy zeroed virtual disks to Eager zeroed virtual disks. Converting a disk from Thick Provisioned Lazy Zeroed to Thick Provisioned Eager Zeroed is so time consuming that uses a significant number of storage I/O processes.

A virtual machine running AVE aggressively uses disk I/O and is almost never idle. VMware's recommendations for appropriate resources for high-performance database virtual machines are generally applicable to an AVE virtual machine.

Virtual disk configuration best practices for AVE on Hyper-V

Hyper-V supports multiple disk formats. For AVE virtual machines, the requirement is to use fixed disks.

The AVE on Hyper-V install file comes with a program called `createvhdfast.exe`. This program is used to quickly create one or more virtual hard disk (VHD) files for use with AVE on Hyper-V. The application creates a hard disk file quickly by not filling its contents with zeros, so the resulting file may contain fragments of previously deleted files. Since this data may be accessible by the virtual machine that uses the resulting disk file, this action may raise security issues.

The `createvhdfast.exe` program can be used in two modes.

Mode one creates a single VHD file which can then be attached to the Hyper-V virtual machine as a SCSI disk. Mode one allows greater control in how disks are created and allocated.

Mode two creates multiple VHD files which are based on the AVE virtual machine size. The resulting VHD files (three or six depending on the size of the AVE being deployed) are spread across defined datastores and can be attached to the Hyper-V virtual machine as SCSI disks (-datastore1, -datastore2, and -datastore3).

If there are security concerns, it is recommended not to use this tool but instead use the standard Microsoft Hyper-V tools to create virtual hard disk files.

The `createvhdfast.exe` is covered in the Preparing the virtual machine section.

Note: AVE does not support dynamic or differencing disks.

A virtual machine running AVE aggressively uses disk I/O and is almost never idle. Microsoft's recommendations for appropriate resources for high-performance database virtual machines are generally applicable to an AVE virtual machine. In particular, a storage pool that is allocated from a group of dedicated physical disks in a RAID 1 (mirror) or RAID 10 (combines RAID 0 with RAID 1) configuration provides the best performance.

Virtual disk configuration best practices for AVE on OpenStack KVM

AVE supports multiple disk formats for the base data disk image files (vmdk, qcow2, raw, etc). For OpenStack KVM instances, we recommend using only qcow2 or raw disks.

When attaching data disks to a KVM virtual machine, driver interface types supported for OpenStack KVM instances are:

- virtio (default)
- scsi

Software requirements

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

All environments require the software listed in the following table:

Table 10 Common AVE software installation requirements

Requirement	Description
Applications	• PuTTY[a] • WinSCP[a] Other up-to-date SSH and SCP clients are also acceptable.
Files	• AVE installation package • AVE configuration workflow package[a] • Operating system security patches (if applicable)

a. Not required for VMware .ova deployments

The following table lists any additional requirements for software that is specific to each installation environment:

Table 11 Additional environment-specific applications

AVE on Azure	Ave on Hyper-V	AVE on AWS
• Azure Cloud subscription • 7Zip • Azure Powershell	• 7Zip • Hyper-V Manager 6.2/6.3	• AWS account subscription • AWS command-line interface (CLI)[a]

a. The AWS CLI must run on a separate system from the AVE instance.

Support for application databases in standalone configuration only in AVE on Azure and AWS

Backup and recovery of the following applications are supported with AVE on Azure and AWS. However, these applications are supported in standalone configuration only. Clustered configurations of application databases are not supported with AVE on Azure or AWS.

- SQL
- Exchange
- SharePoint
- Lotus
- DB2
- Sybase
- SAP
- Oracle

Verify the DNS configuration

This task applies only to AVE on VMware, Hyper-V, and OpenStack KVM.

Before you begin

For AVE on Hyper-V, an entry should be created in the DNS server with a fixed IP address for the AVE virtual machine before AVE installation.

About this task

Before you install AVE, DNS must be correctly configured. Failure to correctly configure DNS can cause runtime or configuration issues.

Procedure

1. Open a command prompt on the vCenter server, Windows server, or OpenStack controller node.
2. Type the following command on one line:

Environment	Command
AVE on VMware AVE on Hyper-V	`nslookup` *`AVE_IP_address`* *`DNS_Server_IP_address`*
AVE on OpenStack KVM	`dig -x` *`AVE_IP_address`*

The command returns the FQDN for AVE.

3. Type the following command:

Environment	Command
AVE on VMware AVE on Hyper-V	`nslookup AVE_FQDN DNS_Server_IP_address`
AVE on OpenStack KVM	`dig AVE_FQDN`

The command returns the IP address for AVE.

4. Type the following command on one line:

Environment	Command
AVE on VMware	`nslookup FQDN_of_vCenter DNS_Server_IP_address`
AVE on Hyper-V	`nslookup FQDN_of_Hyper_V_Server DNS_Server_IP_address`
AVE on OpenStack KVM	Not applicable.

The command returns the IP address of the vCenter Server or the Hyper-V Server.

5. If the commands return the proper information, close the command prompt. If the commands do not return proper information, resolve the DNS configuration before you install AVE.

Network requirements

Before you install AVE, gather the following information:

- Hostnames and IP addresses for the AVE virtual machine and the DNS server

  Note:
  AVE supports only alphanumeric characters (a-z, A-Z, and 0–9) and hyphens (-) in hostnames. Hyphens are only allowed if surrounded by other characters.

  Some workflow inputs may not accept hostnames or FQDNs with hyphens. In this case, replace the name with the corresponding IP address to complete these workflow inputs.

- Gateway, netmask, and domain of the AVE virtual machine
- Firewall openings, if applicable
  The *Avamar Product Security Guide* provides client-server data port usage and firewall requirements.

Note: AVE on OpenStack KVM supports only fixed IP addresses. NAT (floating IP addresses) is not supported.

DHCP and AVE on OpenStack KVM

Avamar servers, including AVE, require static IP addresses. Once you configure the AVE, any change to the server's IP address results in the AVE failing to function correctly.

When you start the AVE for the first time in an OpenStack KVM environment, a script performs a reverse DNS lookup and stores the result in `/etc/HOSTNAME`. The script also creates the Avamar-specific file `probe.xml` and populates `probe.xml` with the hostname from the reverse DNS lookup. If DHCP is in use, it overrides the static name

included in `/etc/HOSTNAME` and modifies `/etc/resolv.conf` to set the domain name.

- If you do not configure DHCP to always specify the correct hostname, domain, and fixed IP address, then you should use a static IP address. Follow the steps in Configure the network settings on page 40 to use the `/usr/local/avamar/bin/avenetconfig` utility.
- If DHCP is configured to always correctly specify the hostname, domain, and fixed IP address, then you do not need to use the `/usr/local/avamar/bin/avenetconfig` utility.

NTP server best practices

The following topics provide guidance for synchronizing AVE with a Network Time Protocol (NTP) server, where applicable.

NTP server best practices for AVE on VMware

AVE supports synchronizing with a Network Time Protocol (NTP) server. Best practice is to identify at least one NTP server to synchronize with the AVE host. If no NTP server is identified, the default behavior is to leave the NTP service disabled and to synchronize with the VMware host. If one or more NTP servers are identified during network configuration, synchronization with the VMware host is disabled and the NTP service is enabled.

During network configuration, you can type one or more optional NTP servers in either IPv4 or IPv6 format or in hostname format.

NTP server best practices for AVE on Hyper-V

AVE supports synchronizing with a Network Time Protocol (NTP) server. Best practice is to identify at least one NTP server to synchronize with the AVE host. If no NTP server is identified, the default behavior is to leave the NTP service disabled and to synchronize with the Hyper-V host. If one or more NTP servers is identified during network configuration, the host NTP service must be manually disabled. To perform the action:

1. Right-click the VM in **Hyper-V Manager** and select **Settings**.
2. In the **Settings** dialog box, under **Management**, go to **Integration Services**.
3. Deselect **Time synchronization**.
4. Click **OK**.

During network configuration, you can type one or more optional NTP servers in either IPv4 or IPv6 format or in hostname format.

NTP server best practices for AVE on OpenStack KVM

If you configure the AVE for DHCP and supply the DHCP server to the Network Time Protocol (NTP) server information, then NTP is enabled by default and NTP server information is obtained via DHCP.

If the DHCP server does not provide NTP information, use the `yast2` utility to configure NTP information.

Upgrade requirements and best practices

Use the procedures in this document to upgrade from AVE 7.4 and later to the current version of AVE. Upgrades from AVE 7.3.*x* and earlier require you to engage Dell EMC.

Other components in the Avamar environment

Information in this document pertains only to upgrading AVE. Other components in the environment may also require upgrades to retain compatibility after the AVE upgrade.

Check the relevant compatibility guides on the Online Support website (https://support.EMC.com) and take any necessary steps to upgrade external components separately. Some external components may require Dell EMC engagement. External components include, but are not limited to:

- All clients and database plug-ins. Customer Support can provide more information about client versions.
  - If you use the Avamar VMware or NDMP plug-ins, upgrade these plug-ins to a supported version, if necessary, before upgrading AVE.
  - If you use Avamar along with NetWorker, upgrade the NetWorker software to a supported version, if necessary, before upgrading AVE.
- Tape-out applications, such as ADT and ATO/ADMe.
  If necessary, upgrade these applications as part of the upgrade.

Stop replication tasks

An active replication session during the upgrade can cause the upgrade to fail.

Determine if there are any replication tasks running and cancel those tasks if appropriate, before upgrading AVE. The *Avamar Administration Guide* contains information about monitoring and canceling replication tasks.

PART 1

On-premises Environments

The following chapters describe instructions for installing AVE in different local virtual environments:

CHAPTER 2

Installing AVE on Hyper-V

The following topics describe how to install an AVE virtual machine in a Microsoft Hyper-V environment:

Prepare a virtual machine

Use the following instructions to install the virtual machine.

Procedure

1. Download the AVE virtual appliance file for the appropriate version of AVE you are installing to the Windows Server (on the Hyper-V host that runs AVE).

   Required software can be downloaded from https://support.emc.com/.

2. Extract the compressed `.7z` file.
3. From the `.7z` uncompressed file, extract the `createvhdfast.zip` file.

   See Virtual disk configuration best practices for AVE on Hyper-V on page 22 for information on the `createvhdfast.exe` utility and whether should be used or if the disks should be manually created. If you are manually creating the VHDs skip the following steps on `createvhdfast.exe`.

4. If you are using the `createvhdfast.exe` utility complete the following steps:

   a. Download and install the 64-bit version of `vcredist_x64.exe` (Microsoft VC++ 2015 Runtime) directly from Microsoft.

   Only 64-bit versions of the Windows operating system are supported by the `createvhdfast.exe` utility.

   b. Download and install `dotNetFx40_Full_setup.exe` (Microsoft .Net 4.0 Runtime) directly from Microsoft.

   c. Select Mode 1 or Mode 2.

   Table 12 Mode options

Mode	Command	Options
Mode 1	**createvhdfast.exe -size=*n*G -path=*path*.vhd**	• *n* is the size of the partition in GB. • *path.vhd* is the location of the path and file for the VHD.
Mode 2	**createvhdfast.exe -avetype=n -basename=*name* -datastore1=*path1* [-datastore2=*path2*] [-datastore3=*path3*]**	• *n* is one of the following values for the size of the AVE virtual machine. ▪ Use 0.5T for .5 TB AVE ▪ Use 1T for 1 TB AVE ▪ Use 2T for 2 TB AVE ▪ Use 4T for 4 TB AVE ▪ Use 8T for 8 TB AVE ▪ Use 16T for 16 TB AVE • *name* is the name of the VHD. • *pathx* is the path to the datastore.

5. Launch **Server Manager**, select **Hyper-V**, then right-click the Hyper-V host and select **Hyper-V Manager**.

6. Expand **Hyper-V Manager**, on the left side of the dialog box select the Hyper-V host. On the right side under **Actions**, click **Import Virtual Machine...**
7. From **Locate Folder** click **Browse...** and select the folder where you extracted the compressed file. Click **Select Folder** and then click **Next**.
8. From **Select Virtual Machine** highlight the **Virtual Machine**, and click **Next**.
9. From **Choose Import Type**, select **Copy the virtual machine (create a new unique ID)** and click **Next**.
10. From **Choose Destination**, accept the default settings and click **Next**.
11. From **Choose Folders to Store Virtual Hard Disks**, accept the default settings and click **Next**.
12. From **Summary**, review the selections and if correct, click **Finish**.
13. Once the system has finished importing the virtual machine, right-click the virtual machine and select **Settings...**
14. In the **Settings** window, under **Hardware**, choose **SCSI Controller**. Select **Hard Drive** and click **Add**.
15. In the **Hard Drive** window, select **Virtual hard disk:** and click **Browse**.
16. In the **Open window**, select the **File Name** and click **Open**.
17. Repeat **steps 14 to 16** for each VHD associated with the AVE virtual machine size. Click **Apply**.
18. In the **Settings** window, under **Hardware**, select **Add Hardware** and for the type choose **Network Adapter** Click **Add**.
19. Select the new **Network Adapter**. The Network Adapter settings are available on the right side of the dialog box. Under **Virtual switch**, select the network connection's virtual switch from the drop-down menu. If you need the virtual machines connection to be tagged with a VLAN ID, under the VLAN ID section, select the checkbox **Enable virtual LAN identification** and assign the VLAN ID identifier. Click **Apply**.
20. In the **Processor** window, update the number of virtual CPUs based on the size of the AVE license and click **Apply**.
    - For 0.5 TB AVE, specify **2 CPUs**.
    - For 1 TB AVE, specify **2 CPUs**.
    - For 2 TB AVE, specify **2 CPUs**.
    - For 4 TB AVE, specify **4 CPUs**.
    - For 8 TB AVE, specify **8 CPUs**.
    - For 16 TB AVE, specify **16 CPUs**.
21. In the **Memory** window, update the memory size which is based on the size of the AVE license and click **Apply** click **OK**.
    - For 0.5 TB AVE, specify **6144 MB**.
    - For 1 TB AVE, specify **8192 MB**.
    - For 2 TB AVE, specify **16384 MB**.
    - For 4 TB AVE, specify **36864 MB**.
    - For 8 TB AVE, specify **49152 MB**.
    - For 16 TB AVE, specify **98304 MB**.

22. Power on the virtual machine. The system will reboot once after initial power on.

Configure the network settings

The following procedure configures the AVE virtual machine for a single IP address or dual stack environment.

About this task

The `avenetconfig` command runs automatically when the virtual machine is first booted, in which case you should proceed to step 4 on page 34.

Procedure

1. In the Hyper-V manager, right-click the virtual machine and select **Connect**.
2. Log in as root using the password **changeme**.
3. At the command prompt, type the following command:

   avenetconfig

4. To enter the **IPv4 IP Configuration**, press **1**.
   a. Press **1** again to enter the **IPv4 Address and Prefix** (for example, 10.6.1.2/24 or 10.6.1.2/255.255.255.0).
   b. Press **2** to enter the **IPv4 Default Gateway** address.
   c. Press **4** when complete to return to the main menu.
5. To enter the **IPv6 IP Configuration**, press **2**.
   a. Press **1** to enter the**IPv6 Address and Prefix** (for example, 2000:10A::5/64).
   b. Press **2** to enter the **IPv6 Default Gateway** address.
   c. Press **4** when complete to return to the main menu.
6. Press **3** to enter the **DNS Settings**.
   a. Press **1** to enter the **Primary Nameserver** IP address. Both IPv4 and IPv6 addresses are supported. Enter additional optional nameservers by pressing **2** and **3**.
   b. Press appropriate number to enter **Alternative Search Domain(s)** (originally the number is **4**, but increases based on the number of Alternative Search Domains you enter). This action is optional and represents a list of domain names that are added to the DNS search path. By default, only the domain portion of the AVE hostname is added.
   c. Press the appropriate number to enter the **Hostname/FQDN** (originally the number is **5**, but increases based on the number of Alternative Search Domains you entered before). This action is optional and is the Fully Qualified Domain Name to be used as the hostname of this AVE. If not provided, the AVE attempts to determine its hostname from DNS using the IP addresses provided before.
   d. Press the appropriate number when complete to return to the main menu.
7. Press **4** to enter or change the **NTP Settings**.

   The **NTP Settings** is optional and can be a single IP address or comma-separated list of IP addresses for Network Time Protocol servers. If left blank, the default behavior is to use the WMware host's timesync. If one or more

addresses is included here, the VMware host's timesync is disabled and the NTP service is enabled.

a. Press **1** to enter the IP address(s) for the NTP server(s).

b. Press **3** to return to the main menu.

8. At the main menu, review the configuration and press **5** to save the changes and exit.
9. Shut down the AVE virtual machine.
10. Right-click the AVE virtual machine in **Hyper-V manager** and select **Settings**.
11. Select **Network Adapter** > **Advanced Features** from the left pane.
12. Select **Static** from the list of **MAC Address** options.

    Hyper-V populates a default MAC address in the six fields.
13. Click **OK**.

    Hyper-V saves the settings.
14. Power on the AVE virtual machine.

Install and configure the Avamar software

This task installs the Avamar software on a newly prepared AVE virtual machine.

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 **changeme**.

   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.

   The *Avamar Virtual Edition Configuration Workflow Guide* opens.
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**.

Note:
If you do not specify a Data Domain system when you create an 8 TB or 16 TB AVE that is intended to be used with Data Domain, you must make additional configuration changes to the Avamar subsystem settings before you can configure the Data Domain system later.

These changes improve system performance. The *Avamar Administration Guide* provides more information about system requirements for Data Domain integration.

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.

CHAPTER 3

Installing AVE on OpenStack KVM

The following topics describe how to install an AVE virtual machine in an OpenStack KVM environment:

Prepare a virtual machine

The following instructions are specific to RHEL. Ubuntu has different options.

Procedure

1. Download the AVE virtual appliance file for the appropriate version of AVE from https://support.emc.com/.
2. Log in to the OpenStack controller node with administrative rights.
3. Copy the AVE qcow2 image to the controller node.
4. Set the environment variables that the OpenStack CLI tools require.

   In the `home` directory of the root user, a file contains the environment variables that the OpenStack CLI tools require. This file may be named, for example, `keystonerc_admin` or `openrc`. The actual name of the file varies depending on the distribution. Use the shell's `source` command to pull in the environment values.

   For example:

   ```
   source keystonerc_admin
   ```

5. Create an OpenStack Glance image:

   ```
   openstack image create --disk-format qcow2 --container-format
   bare --public --property os_shutdown_timeout=900 --file AVE-
   version-disk1.qcow2 name-of-glance-image
   ```

   where *version* is the version of the AVE software and *name-of-glance-image* is the name of the Glance image.

   Record the Glance image UUID that OpenStack returns.

6. Create an OpenStack flavor to deploy the instance. System requirements on page 19 provides the required specifications.

   For example, to create a flavor for an 0.5 TB configuration:

   ```
   openstack flavor create --disk 126 --ram 6144 --vcpus 2 --swap 0
   --ephemeral 0 AVE-0.5TB --public
   ```

   Record the flavor name (for example, *AVE-0.5TB*). You use the flavor name later in this procedure to deploy the instance.

7. Create additional volumes for the AVE instance. Virtual disk requirements on page 21 provides additional information.

   For example, to create disks for a 0.5 TB AVE:

   ```
   openstack volume create --size 250 AVE-disk-1
   openstack volume create --size 250 AVE-disk-2
   openstack volume create --size 250 AVE-disk-3
   ```

   Record the Cinder volume IDs for all of the disks that you create in this step.

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

8. Create an OpenStack security group:

   ```
   openstack security group create AVESecurityGroup --description
   "AVE security group"
   ```

Record the security group ID that OpenStack returns.

9. Add TCP, ICMP, and UDP rules to the AVE security group by typing each command on one line:

   ```
   openstack security group rule create AVESecurityGroup --protocol
   icmp --dst-port -1:-1 --remote-ip 0.0.0.0/0
   ```

   ```
   openstack security group rule create AVESecurityGroup --protocol
   tcp --dst-port 1:65535 --remote-ip 0.0.0.0/0
   ```

   ```
   openstack security group rule create AVESecurityGroup --protocol
   udp --dst-port 1:65535 --remote-ip 0.0.0.0/0
   ```

10. Retrieve the network ID of the instance:

    ```
    openstack network list
    ```

    Record the network ID.

11. Deploy the AVE instance by typing the following command on one line:

    openstack server create --image *Glance-image-UUID* --security-group AVESecurityGroup --flavor *Flavor-name* --nic net-id=*Net-ID* *Name-of-AVE-instance*

    where:

    - *Glance-image-UUID* is the recorded Glance image UUID.
    - *Flavor-name* is the recorded flavor name.
    - *Net-ID* is the recorded network ID.
    - *Name-of-AVE-instance* is the name of the AVE instance.

    Record the instance ID that OpenStack returns.

12. Attach the volumes that you created to the AVE instance:

    openstack server add volume *AVE-instance-ID* *AVE-volume-ID*

    where:

    - *AVE-instance-ID* is the recorded instance ID.
    - *AVE-volume-ID* is the recorded volume ID.

    Repeat this step for all volumes that you created.

13. Verify that the AVE instance completed the initial startup by going to the Horizon Dashboard:

    openstack console url show *name*

    where *name* is the name of the Keystone server.

14. Restart the AVE instance:

    openstack server reboot *AVE-instance-ID*

    where *AVE-instance-ID* is the recorded instance ID.

Configure the network settings

The following procedure configures the AVE virtual machine for a single IP address. Use this procedure if you are configuring an AVE that uses a static IP address.

Procedure

1. Log in to the controller node.
2. From the controller node, SSH to the AVE instance as root.
3. At the command prompt, type the following command:

   ```
   avenetconfig
   ```

4. To enter the **IPv4 IP Configuration**, press **1**.
   a. Press **1** again to enter the **IPv4 Address and Prefix** (for example, 10.6.1.2/24 or 10.6.1.2/255.255.255.0).
   b. Press **2** to enter the **IPv4 Default Gateway** address.
   c. Press **4** when complete to return to the main menu.
5. To enter the **IPv6 IP Configuration**, press **2**.
   a. Press **1** to enter the**IPv6 Address and Prefix** (for example, 2000:10A::5/64).
   b. Press **2** to enter the **IPv6 Default Gateway** address.
   c. Press **4** when complete to return to the main menu.
6. Press **3** to enter the **DNS Settings**.
   a. Press **1** to enter the **Primary Nameserver** IP address. Both IPv4 and IPv6 addresses are supported. Enter additional optional nameservers by pressing **2** and **3**.
   b. Press appropriate number to enter **Alternative Search Domain(s)** (originally the number is **4**, but increases based on the number of Alternative Search Domains you enter). This action is optional and represents a list of domain names that are added to the DNS search path. By default, only the domain portion of the AVE hostname is added.
   c. Press the appropriate number to enter the **Hostname/FQDN** (originally the number is **5**, but increases based on the number of Alternative Search Domains you entered before). This action is optional and is the Fully Qualified Domain Name to be used as the hostname of this AVE. If not provided, the AVE attempts to determine its hostname from DNS using the IP addresses provided before.
   d. Press the appropriate number when complete to return to the main menu.
7. Press **4** to enter or change the **NTP Settings**.

   The **NTP Settings** is optional and can be a single IP address or comma-separated list of IP addresses for Network Time Protocol servers. If left blank, NTP is disabled. If one or more addresses are included, the NTP service is enabled. Add 127.127.1.0 to the list to create a local "hardware clock" fallback (which is the software clock of the host under `qemu-kvm`).

   a. Press **1** to enter the IP address(s) for the NTP server(s).
   b. Press **3** to return to the main menu.

8. At the main menu, review the configuration and press **5** to save the changes and exit.

Installing and configuring 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**.

Before you begin

When the AVE is deployed in a KVM environment and obtains DHCP addressing information, run the `/usr/local/avamar/bin/makeprobexml` utility before running the **ave-config** workflow.

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 **changeme**.

   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.

   The *Avamar Virtual Edition Configuration Workflow Guide* opens.
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.

CHAPTER 4

Installing AVE on VMware

The following topics describe how to install an AVE virtual machine in a VMware environment:

Prepare a virtual machine

The following instructions use vCenter Server 5.5. Other versions of vCenter Server might have different options.

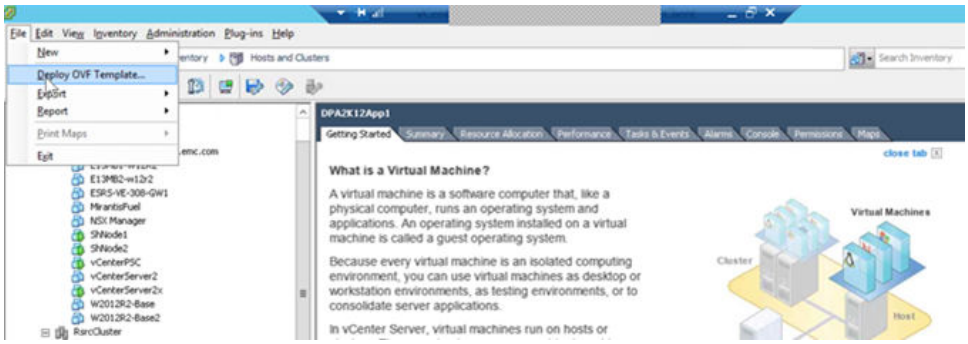
About this task

AVE on VMware supports both OVA and OVF deployment. In some cases, this task provides separate steps or variations on steps, depending on your choice of template. Where multiple options are provided, select the step or option that applies for the type of file that you use to deploy AVE.

Procedure

1. Download the AVE virtual appliance file from Dell EMC Online Support.
2. Extract the compressed `.7z` file.
3. Start a VMware web client and connect to the vCenter server, or to the ESXi host, that hosts the AVE virtual machine.
4. Log in with administrative rights.
5. If you logged in to vCenter, select the ESXi server that hosts the AVE virtual machine.
6. Select **File** > **Deploy OVF Template**.

   Figure 1 Deploying the OVF template

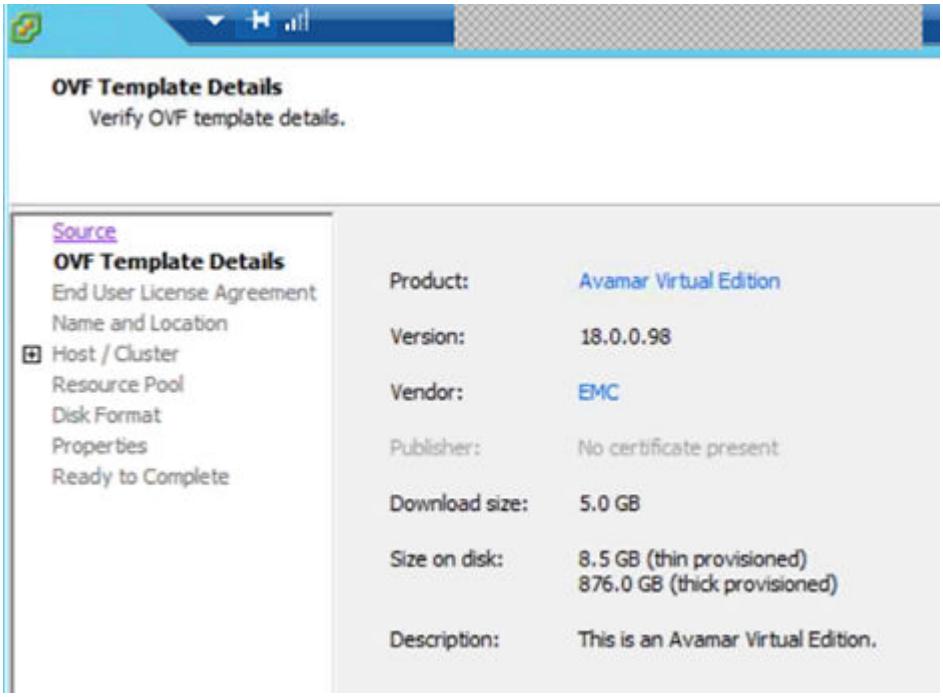
   

   The **Source** page opens.

7. Select **Deploy from a file or URL** and browse to the AVE virtual machine file (`.OVF` or `.OVA` extension), and then click **Next**.

   The **OVF Template Details** page opens.

Figure 2 OVF Template Details page



8. Verify that the template details are correct and click **Next**.

   The **End User License Agreement** page opens.

9. Click **Accept** to accept the **End User License Agreement** and click **Next**.

   The **Name and Location** page opens.

10. Type in the AVE name, select the inventory location, and then click **Next**.

    The **Storage** page opens.

11. Select the storage for AVE and click **Next**.

    The **Disk Format** page opens.

12. Select **Thick Provision Lazy Zeroed** format and click **Next**.

    AVE does not support thin provisioning.

    The **Network Mapping** page opens.

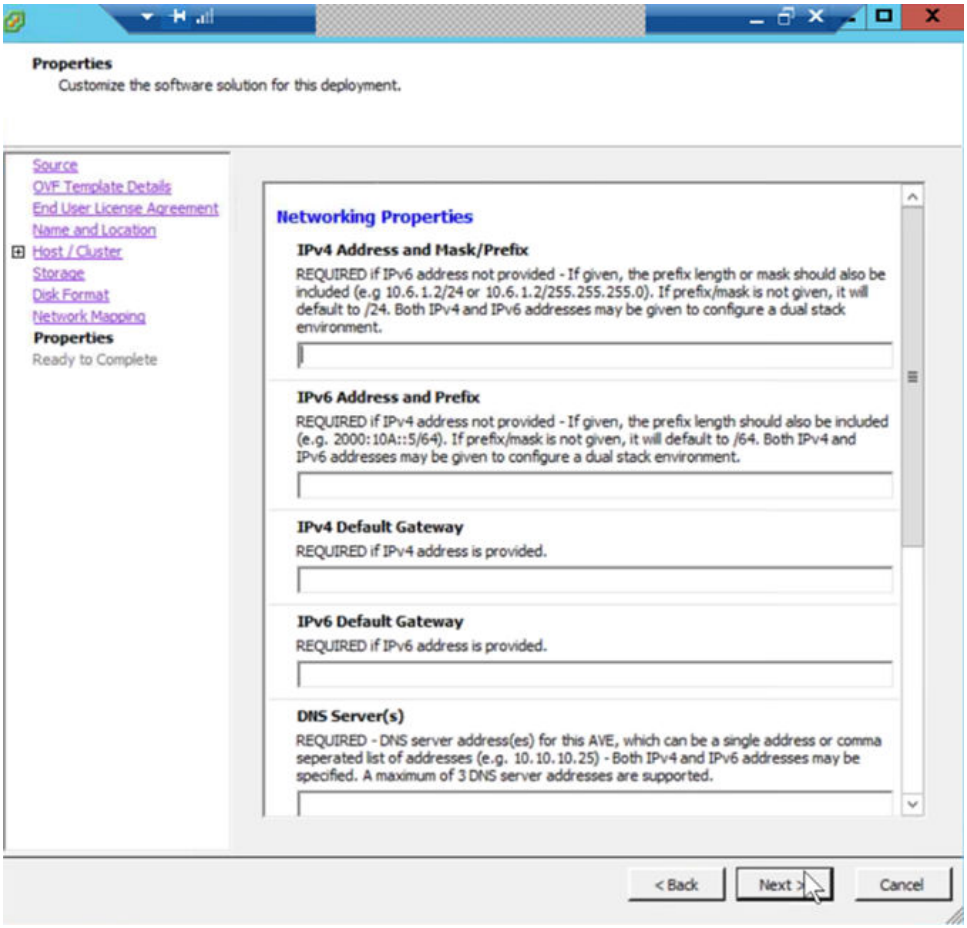
13. Select the destination network and click **Next**.

    The **Networking Properties** page opens.

14. At the **Networking Properties** page, perform one of the following actions:

    - If you used the AVE `.ovf` file, do not complete the fields on this page, as the network settings are unavailable. Instead, click **Next** and configure networking with the `avenetconfig` command after deployment completes. Configure the network settings on page 48 provides more information.
    - If you used the AVE `.ova` file, complete the required and optional networking information as described in the **Networking Properties** page, and then click **Next**.

Figure 3 Networking Properties page



Note:
For the **Hostname FQDN** field, the hostname can only include alphanumeric characters (a-z, A-Z, and 0-9), hyphen (-), and period(.).

Hyphen and periods are only permitted if surrounded by other characters. Some workflow inputs may not accept hostnames or FQDNs with hyphens. In this case, replace the name with the corresponding IP address to complete these workflow inputs.

The **Ready to Complete** page opens.

15. Confirm that the deployment settings are correct and then click **Finish**.

    The installation may take several minutes. The wizard displays a `Deployment Completed Successfully` message when the installation completes.

16. Click **Close** to close the deployment dialog box.
17. If you used the AVE `.ovf` file, skip the following steps. Supply the networking properties information by using the `avenetconfig` script, as described in Configure the network settings on page 48.
18. If you used the AVE `.ova` file, and you are installing a 2 TB, 4 TB, 8 TB, or 16 TB AVE, remove the existing 250 GB virtual disks that the `.ova` file created:

    Do not perform this step for 0.5 TB and 1.0 TB AVE configurations.

    a. Right-click the AVE virtual machine and then select **Edit Settings**.

b. Select hard disk 2 from the table.

c. Select **Remove**.

d. Click **OK** to confirm drive removal.

e. Repeat for hard disks 3 and 4.

19. Right-click the AVE virtual machine and then select **Edit Settings**.

    The **Virtual Machine Properties** window opens.

20. On the **Hardware** tab, select **Memory**, and then set **Memory Size**, based on the AVE capacity configuration.

    System requirements on page 19 provides more information.

21. On the **Hardware** tab, select **CPUs**, and then change the number of virtual CPUs, based on the AVE capacity configuration.

    System requirements on page 19 provides more information.

22. On the **Hardware** tab, select **Network adapter 1**, select **Network Connection** (Network label), and then select the correct network.

23. If you are installing a 1 TB, 2 TB, 4 TB, 8 TB, or 16 TB AVE, complete the steps in Create additional virtual hard disks on page 47 to create additional virtual hard disks (VMDKs) for the AVE virtual machine, based on the AVE capacity configuration. These steps are not required for 0.5 TB AVE configurations.

24. Finish the virtual machine configuration by completing the following steps:

    a. Click **OK**.

    b. In the **Recent Tasks** status area at the bottom of the screen, observe the hard disk creation progress.

    When the virtual machine reconfiguration completes, the wizard displays a `Completed` message.

25. To start the AVE virtual machine, right-click the virtual machine and select **Power** > **Power On**.

26. Open the **Virtual Console** and monitor the installation progress.

    An insufficient licensing message at this point might indicate either a shortage of ESXi server licenses or an inability to connect to a license server. Resolve this problem with the network administrator.

27. On the **Summary** tab, verify that the status for **VMware Tools** changes to `Running`, `Unmanaged`, or `out-of-date`.

Create additional virtual hard disks

Complete this task when directed during preparation of the virtual machine. Do not perform this task for 0.5 TB AVE configurations.

About this task

Review the information in Virtual disk requirements on page 21 and repeat this task as necessary to add the required number of virtual hard disks for this AVE capacity configuration.

Procedure

1. Click the **Add** button.

   The **Add Hardware Wizard** appears.

2. Select **Hard Disk**.
3. Click **Next**.
4. Select **Create a new virtual disk**.
5. Click **Next**.
6. For **Disk Size**, type **250 GB**, **1000 GB**, or **2000 GB** as required.
7. For **Disk Provisioning**, select **Thick Provision Lazy Zeroed** format.

   Thin provisioning is not supported with AVE. If you select **Thick Provision Eager Zeroed** during the installation, the installation could take several hours. Time-out errors could also occur. Virtual disk configuration best practices on page 22 provides information about disk formatting after you complete the installation process.
8. For **Location**, select either **Store with virtual machine** or **Specify a datastore**.
9. Click **Next**.
10. For **Mode**, select **Independent**. Use the default setting for **Persistent**.
11. Click **Next**.
12. Verify the configuration and select **Finish**.

After you finish

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

Configure the network settings

This procedure configures the AVE network configuration for a single IP address or dual stack environment. Complete this task only if you used the AVE `.ovf` file to prepare the virtual machine.

About this task

If the `avenetconfig` command ran automatically when the virtual machine first booted, proceed to step 4 on page 48.

Procedure

1. In the vSphere client, right-click the virtual machine and select **Open Console**.
2. Log in as root using the password **`changeme`**.
3. At the command prompt, type the following command:

   `avenetconfig`
4. To enter the **IPv4 IP Configuration**, press **1**.
   a. Press **1** again to enter the **IPv4 Address and Prefix** (for example, 10.6.1.2/24 or 10.6.1.2/255.255.255.0).
   b. Press **2** to enter the **IPv4 Default Gateway** address.
   c. Press **4** when complete to return to the main menu.
5. To enter the **IPv6 IP Configuration**, press **2**.
   a. Press **1** to enter the**IPv6 Address and Prefix** (for example, 2000:10A::5/64).
   b. Press **2** to enter the **IPv6 Default Gateway** address.

c. Press **4** when complete to return to the main menu.

6. Press **3** to enter the **DNS Settings**.

   a. Press **1** to enter the **Primary Nameserver** IP address. Both IPv4 and IPv6 addresses are supported. Enter additional optional nameservers by pressing **2** and **3**.

   b. Press appropriate number to enter **Alternative Search Domain(s)** (originally the number is **4**, but increases based on the number of Alternative Search Domains you enter). This action is optional and represents a list of domain names that are added to the DNS search path. By default, only the domain portion of the AVE hostname is added.

   c. Press the appropriate number to enter the **Hostname/FQDN** (originally the number is **5**, but increases based on the number of Alternative Search Domains you entered before). This action is optional and is the Fully Qualified Domain Name to be used as the hostname of this AVE. If not provided, the AVE attempts to determine its hostname from DNS using the IP addresses provided before.

   d. Press the appropriate number when complete to return to the main menu.

7. Press **4** to enter or change the **NTP Settings**.

   The **NTP Settings** is optional and can be a single IP address or comma-separated list of IP addresses for Network Time Protocol servers. If left blank, the default behavior is to use the WMware host's timesync. If one or more addresses is included here, the VMware host's timesync is disabled and the NTP service is enabled.

   a. Press **1** to enter the IP address(s) for the NTP server(s).

   b. Press **3** to return to the main menu.

8. At the main menu, review the configuration and press **5** to save the changes and exit.

Install and configure the Avamar software

This task installs the Avamar software on a newly prepared AVE virtual machine.

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 **changeme**.

   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.

   The *Avamar Virtual Edition Configuration Workflow Guide* opens.
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**.

   Note:
   If you do not specify a Data Domain system when you create an 8 TB or 16 TB AVE that is intended to be used with Data Domain, you must make additional configuration changes to the Avamar subsystem settings before you can configure the Data Domain system later.

   These changes improve system performance. The *Avamar Administration Guide* provides more information about system requirements for Data Domain integration.

   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.

PART 2

Cloud Environments

The following chapters describe instructions for installing AVE in different cloud virtual environments:

CHAPTER 5

Installing AVE on AWS

The following topics describe how to install an AVE virtual machine in an Amazon Web Services (AWS) environment:

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 AWS Installation Methods on page 113 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 55.
   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 HTTPS on port 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 13 Inbound ports for the AWS security group

Type	Protocol	Port Range	Source
Custom ICMP Rule - IPv4	Time Exceeded	N/A	Anywhere (0.0.0.0/0, ::/0)
Custom ICMP Rule - IPv4	Destination Unreachable	N/A	Anywhere (0.0.0.0/0, ::/0)
Custom ICMP Rule - IPv4	Echo Reply	N/A	Anywhere (0.0.0.0/0, ::/0)
Custom ICMP Rule - IPv6	IPv6 ICMP	N/A	Anywhere (0.0.0.0/0, ::/0)
SSH	TCP	22	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	161	Anywhere (0.0.0.0/0, ::/0)
Custom UDP Rule	UDP	161	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	163	Anywhere (0.0.0.0/0, ::/0)
Custom UDP Rule	UDP	163	Anywhere (0.0.0.0/0, ::/0)

Table 13 Inbound ports for the AWS security group (continued)

Type	Protocol	Port Range	Source
HTTPS	TCP	443	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	700	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	7543	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	7778 - 7781	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	8543	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	9090	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	9443	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	27000	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	28001 - 28002	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	28810 - 28819	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	29000	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	30001 - 30003	Anywhere (0.0.0.0/0, ::/0)

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.

By default, when you create a security group, AWS adds a predefined rule that allows all outbound traffic. Remove this default rule when you create a security group.

Table 14 Outbound ports for the AWS security group

Type	Protocol	Port Range	Destination
Custom ICMP Rule - IPv4	Echo Reply	N/A	Anywhere (0.0.0.0/0, ::/0)
Custom ICMP Rule - IPv6	IPv6 ICMP	N/A	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	7	Anywhere (0.0.0.0/0, ::/0)

Table 14 Outbound ports for the AWS security group (continued)

Type	Protocol	Port Range	Destination
SSH	TCP	22	Anywhere (0.0.0.0/0, ::/0)
SMTP	TCP	25	Anywhere (0.0.0.0/0, ::/0)
DNS (UDP)	UDP	53	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	111	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	UDP	111	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	161	Anywhere (0.0.0.0/0, ::/0)
Custom UDP Rule	UDP	161	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	163	Anywhere (0.0.0.0/0, ::/0)
Custom UDP Rule	UDP	163	Anywhere (0.0.0.0/0, ::/0)
HTTPS	TCP	443	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	700	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	2049	Anywhere (0.0.0.0/0, ::/0)
Custom UDP Rule	UDP	2049	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	2052	Anywhere (0.0.0.0/0, ::/0)
Custom UDP Rule	UDP	2052	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	3008	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	8443	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	8888	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	9443	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	27000	Anywhere (0.0.0.0/0, ::/0)

Table 14 Outbound ports for the AWS security group (continued)

Type	Protocol	Port Range	Destination
Custom TCP Rule	TCP	28001-28010	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	29000	Anywhere (0.0.0.0/0, ::/0)
Custom TCP Rule	TCP	30001-30010	Anywhere (0.0.0.0/0, ::/0)

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.

   System requirements on page 19 contains details about AVE system requirements. The wizard disables any instance types that do not apply to AVE.
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.

       Virtual disk requirements on page 21 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. Virtual disk requirements on page 21 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 68 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 (https://support.emc.com/) before proceeding. You can find the template under the Downloads section for **Avamar Virtual Edition**, or by searching by product for **Avamar Virtual Edition**.

The CloudFormation template contains two files:

- `AVE_DDVE_CloudFormation.json`
- `AVE_DDVE_CloudFormation_parameters.json`

  The parameter file is only required for deployment via CLI.

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.

   This selection governs the choice of EC2 instance type and the automatic creation of virtual disks, as detailed in Virtual disk requirements on page 21.

AVE instance size	EC2 instance type
2 TB	`m4.xlarge`

AVE instance size	EC2 instance type
4 TB	m4.2xlarge
8 TB	r4.2xlarge
16 TB	r4.4xlarge

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 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*.

DDVE instance size	EC2 instance type
1 to 16 TB	`m4.xlarge`
17 to 32 TB	`m4.2xlarge`
33 to 96 TB	`m4.4xlarge`

DDVE instance size	EBS metadata disk allocation
1 to 10 TB	1 TB
11 to 20 TB	2 TB
21 to 30 TB	3 TB
31 to 40 TB	4 TB
41 to 50 TB	5 TB
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 stack**.

   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:

```
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:

```
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

The AWS documentation at https://aws.amazon.com/security/ provides more information about general AWS security recommendations.

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 15 Inbound ports for Linux gateways

Type	Protocol	Port range	Source
Custom TCP rule	TCP	7778–7781	Private subnet

Table 15 Inbound ports for Linux gateways (continued)

Type	Protocol	Port range	Source
HTTPS	TCP	443	Private subnet
SSH	TCP	22	0.0.0.0/0

Table 16 Inbound ports for Windows gateways

Type	Protocol	Port range	Source
Custom TCP rule	TCP	7778–7781	Private subnet
RDP	TCP	3389	0.0.0.0/0
HTTPS	TCP	443	Private subnet
SSH	TCP	22	Private subnet

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 54 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 55.

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.

The *Avamar Virtual Edition Configuration Workflow Guide* opens.

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.

CHAPTER 6

Installing AVE on Azure

The following topics describe how to install an AVE virtual machine in a Microsoft Azure environment:

Installation

Avamar provides multiple deployment methods for AVE virtual machines on Microsoft Azure. Select a method from the following list:

- By deploying AVE, or AVE and DDVE together, from the Azure Marketplace.

  Deploying from the Azure Marketplace on page 72 provides more information.
- By deploying AVE and DDVE together via the Azure solution template.

  Deploy AVE and DDVE with an Azure solution template on page 82 provides more information, and provides instructions for the following options:

  - Azure Resource Manager
  - Azure Powershell
  - Azure CLI

Deploying from the Azure Marketplace

The AVE software and the Data Domain Virtual Edition (DDVE) software are available from the Microsoft Azure Marketplace, and can be deployed separately or together. The following topics provide instructions for each scenario:

- Deploy AVE from the Azure Marketplace on page 72
- Deploy AVE and DDVE from the Azure Marketplace on page 76

Note: For security considerations, deploy AVE in a private network and configure a secure gateway from which you can install, configure, and manage the Avamar server. Azure security best practices provides detailed information on how to set up an additional secure gateway system for AVE maintenance in the cloud.

Deploy AVE from the Azure Marketplace

This section provides information about how to deploy a stand-alone AVE VM from the Azure Marketplace.

Before you begin

Review Preinstallation requirements and best practices on page 18 and note the applicable requirements for the selected capacity configuration.

Procedure

1. Open the Azure portal at https://portal.azure.com and log in to the Azure account.
2. In the Azure Marketplace, search for the **Avamar Virtual Edition** application.
3. Locate the correct version of AVE from the Marketplace search results, and then click the listing.

   The right pane opens and presents a description of the Avamar software. Review the description.
4. From the **Select a software plan** drop-down, choose the correct version of AVE.
5. Click **Create**.

   The **Create a virtual machine** wizard opens.

Configure the basic settings for the AVE VM

With the **Create a virtual machine** wizard open to the **Basics** tab, complete the following basic configuration:

Procedure

1. Select an available Azure subscription.
2. From the **Resource group** drop-down, select an existing resource group or click **Create new**.

   Create a resource group on page 83 and the Azure portal documentation provide more information.
3. In the **Virtual machine name** field, type a name for the AVE VM. The maximum length is 10 characters.
4. From the **Region** drop-down, select an available location in which to deploy the AVE VM.
5. From the **Availability options** drop-down, select `No infrastructure redundancy required`.
6. From the **Image** drop-down, select the option for `Dell EMC Avamar Virtual Edition` that corresponds to the current version of AVE.
7. Using the information in System requirements on page 19, select a value for **Size**.
8. For **Authentication type**, select `Password` or `SSH public key`.
   a. If you selected `Password`, complete the **Username**, **Password**, and **Confirm password** fields.
   b. If you selected `SSH public key`, complete the **Username** and **SSH public key** fields.

   The installation process creates an OS-level administrative user account with this username and password.
9. For **Public inbound ports**, select one of the following options:

Option	Description
None	For environments where the protected clients reside in the Azure cloud and that require no public Internet access.
Allow selected ports	For environments where the protected clients may reside outside of the Azure cloud, or that require access from the public Internet.

   a. If you selected `Allow selected ports`, check values from the **Select inbound ports** drop-down.

   Network security group on page 93 contains information about required inbound/outbound rules for AVE.
10. Click **Next : Disks**.

Results

The **Create a virtual machine** wizard moves to the **Disks** tab.

Configure the disk settings for the AVE VM

With the **Create a virtual machine** wizard open to the **Disks** tab, complete the following configuration:

Before you begin

Because SSD volumes have better performance than other volume types, Dell EMC 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.

Procedure

1. From the **OS disk type** drop-down, select `Standard HDD` or `Standard SSD`.
2. Click **Create and attach a new disk**.

   The **Create a new disk pane** opens.
3. From the **Disk type** drop-down, select `Standard HDD` or `Standard SSD`.
4. Type a name for the data disk.
5. In the **Size** field, specify the size of the required storage partitions that you noted earlier.
6. From the **Source type** drop-down, select `None (empty disk)`.
7. Click **OK**.

   The **Create a new disk pane** closes. The **Create a virtual machine** wizard lists the new data disk.
8. Repeat steps 2 on page 74 to 7 on page 74 to create the remaining storage partitions, as listed in the virtual disk requirements table.

   Note: Verify that all of the storage partitions are the same size before continuing.
9. Click **Next : Networking**.

Results

The **Create a virtual machine** wizard moves to the **Networking** tab.

Configure the network settings for the AVE VM

With the **Create a virtual machine** wizard open to the **Networking** tab, complete the following configuration:

Procedure

1. From the **Virtual network** drop-down, select an existing virtual network or click **Create new**.

   Create a virtual network and subnet on page 85 and the Azure portal documentation provide more information.
2. If required, from the **Subnet** drop-down, select an existing subnet.

   The Azure portal automatically creates a subnet when you create a virtual network. In this case, you cannot select a value from the **Subnet** drop-down.
3. From the **Public IP** drop-down, select an available IP address block.

> **Note:** For security considerations, Dell EMC recommends that you deploy AVE in a private network and set the **Public IP** drop-down to `None`.

4. For **Network security group**, select `Advanced`.
5. From the **Configure network security group** drop-down, select an existing security group or click **Create new**.

   Creating a network security group is beyond the scope of this publication. The Azure portal documentation provides more information.

   Ensure that the selected network security group contains all of the required inbound/outbound rules. Network security group on page 93 provides more information.

6. Click **Next : Management**.

Results

The **Create a virtual machine** wizard moves to the **Management** tab.

Configure the management settings for the AVE VM

With the **Create a virtual machine** wizard open to the **Management** tab, complete the following configuration:

Procedure

1. For **Boot diagnostics**, select `On`.
2. From the **Diagnostics storage account** drop-down, select an existing diagnostics storage account or click **Create new**.

   Creating a diagnostics storage account is beyond the scope of this publication. The Azure portal documentation provides more information.

3. For **System assigned managed identity**, select `Off`.
4. For **Enable auto-shutdown**, select `Off`.
5. Click **Next : Advanced**.

   The **Create a virtual machine** wizard moves to the **Advanced** tab.

6. Click **Next : Tags**.

   The **Create a virtual machine** wizard moves to the **Tags** tab.

7. Click **Next : Review + create**.

Results

The **Create a virtual machine** wizard moves to the **Review + create** tab.

Create the AVE VM

With the **Create a virtual machine** wizard open to the **Review + create** tab, complete the following steps:

Procedure

1. Wait for the Azure portal to validate the AVE configuration.

   Review and correct any errors.

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

3. Click **Create**.

   The Azure portal starts to deploy the AVE VM. The deployment process can take considerable time to complete, depending on the selected capacity configuration.

4. Observe the output from the deployment process and respond to any problems.

   The Azure portal displays a notification when the deployment completes.

5. Create a static IP address for the AVE VM by performing the following substeps:

   a. From the network interface configuration page for the AVE VM, click **IP configurations**.

   b. Click the network name.

   c. Select **Static** for the **Private IP address** assignment.

   d. Specify a private IP address or accept the default private IP address from Azure.

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

   f. Click **Save**.

6. Install the Avamar software.

   Install and configure the Avamar software on page 97 contains instructions.

   Note: After launching the instance, the AVE initializes and restarts automatically. During this process, which takes 15 to 25 minutes, the AVE installs drivers and an updated kernel. You cannot install the Avamar software until this process is complete because the installation package, **ave-config**, is not available in the **Avamar Installation Manager**. SSH is also unavailable during this time.

Deploy AVE and DDVE from the Azure Marketplace

This section provides information on how to deploy the AVE and DDVE software together from the Azure Marketplace.

Before you begin

Review Preinstallation requirements and best practices on page 18 and the DDVE system requirements in *Data Domain Virtual Edition Installation and Administration Guide*. Note the applicable requirements for the selected capacity configurations.

Procedure

1. Open the Azure portal at https://portal.azure.com and log in to the Azure account.
2. In the Azure Marketplace, search for and deploy the Avamar and Data Domain Virtual Edition.

   Select **Avamar and Data Domain Virtual Editions**.

3. Locate the application that corresponds to the selected versions of AVE and DDVE from the Marketplace search results, and then click the listing.

   The right pane opens and presents a description of the combined software package. Review the description.

4. From the **Select a software plan** drop-down at the bottom of the right pane, choose the correct version of AVE and DDVE.
5. Click **Create**.

   The **Create Avamar and Data Domain Virtual Edition** wizard opens.

Configure the basic settings for AVE and DDVE

With the **Create Avamar and Data Domain Virtual Edition** wizard open to the **Basics** tab, complete the following basic configuration:

Procedure

1. Select an available Azure subscription.
2. From the **Resource group** drop-down, select an existing resource group or click **Create new**.

   Create a resource group on page 83 and the Azure portal documentation provide more information.
3. From the **Location** drop-down, select an available location in which to deploy AVE and DDVE.
4. Click **OK**.

Results

The **Create Avamar and Data Domain Virtual Edition** wizard moves to the **Infrastructure Configuration** tab.

Configure the infrastructure settings for AVE and DDVE

With the **Create Avamar and Data Domain Virtual Edition** wizard open to the **Infrastructure Configuration** tab, complete the following configuration:

Procedure

1. Click **Virtual network**.

   The **Choose virtual network** pane opens.
2. Select an existing virtual network or click **Create new**.

   To create a virtual network by using the wizard, complete the following substeps:

   a. Type a unique name for the new virtual network.

   b. Supply an address space in the form *<startingIP>/<subnet>*.

      For example, 10.2.3.0/24 or 192.168.0.0/16.

   c. Click **OK** to continue.

   The **Choose virtual network** pane closes.
3. Click **Subnets**.

   The **Subnets** pane opens.
4. Select a subnet from the list.

   The Azure portal automatically creates a subnet when you create a virtual network. In this case, you cannot select a value. Complete the following substeps to configure a new subnet:

   a. Type a unique name for the new subnet.

b. Supply an address prefix in the form *<startingIP>/<subnet>*.

By default, the wizard copies this field from the value that you typed for the new virtual network.

c. Click **OK** to continue.

The **Subnets** pane closes.

5. Click **Diagnostics storage account**.

The **Choose storage account** pane opens.

6. Select an existing storage account or click **Create new**.

To create a storage account by using the wizard, complete the following substeps:

a. Type a unique name for the new storage account.

b. For **Account kind**, select `Storage (general purpose v1)`.

c. For **Performance**, select `Standard`.

d. For **Replication**, select `Locally-redundant storage (LRS)`.

e. Click **OK** to continue.

The **Choose storage account** pane closes.

7. Click **OK**.

Results

The **Create Avamar and Data Domain Virtual Edition** wizard moves to the **AVE Configuration** tab.

Configure the instance settings for AVE

With the **Create Avamar and Data Domain Virtual Edition** wizard open to the **AVE Configuration** tab, complete the following configuration:

Procedure

1. From the **AVE Version** drop-down, select the available release.

Your choice of application from the Marketplace determines the available options.

2. In the **AVE Name** field, type the hostname for the AVE instance.

Note: The maximum length of the virtual machine name is 10 characters.

3. Using the information in System requirements on page 19, select a value for **AVE VM Size**.

This field offers a selection of values that correspond to the sizes that are listed in the resource requirement tables.

4. From the **AVE Capacity** drop-down, select the correct capacity configuration.

5. In the **Admin User Name** field, type the name for the administrator.

You can use this username to `ssh` into the AVE instance. The values `admin` and `root` are not permitted.

6. For **Admin Authentication Type**, select `Password` or `SSH public key`.

a. If you selected `Password`, complete the **Password** and **Confirm password** fields.

b. If you selected `SSH public key`, complete the **SSH public key** field.

The installation process creates an OS account with this username and password.

7. In the **AVE Common password** and **Confirm AVE Common password** fields, type a password for the OS admin and root accounts, and for the Avamar software.
8. From the **AVE Time Zone** drop-down, select the applicable time zone.
9. (Optional) In the **Email sender address** field, type the email address from which notification emails are sent to Dell EMC.
10. (Optional) In the **Email server** field, type the hostname or IP address of the email server that ConnectEMC uses to send email to Dell EMC. This is also the email server that sends EmailHome messages for high priority events.
11. (Optional) In the **Site name** field, type a name for the site where the Avamar server is physically located.
12. (Optional) In the **Dell EMC Site ID/CSI Party ID** field, 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 by clicking **Administration** > **View and manage company information**. An incorrect site ID may lead to delays when you contact Customer Support.
13. (Optional) In the **Company name** field, type the name of the company that owns the Avamar server.
14. (Optional) In the **Company contact name** field, type the name of the administrator managing the Avamar server.
15. (Optional) In the **Company contact phone number** field, type the phone number of the administrator managing the Avamar server.

    Valid characters are digits, plus symbol (`+`), parentheses `( )`, hyphen (`-`), spaces, and `x` for extension.
16. (Optional) In the **Company contact email address** field, type the email address of the administrator managing the Avamar server.
17. Click **OK**.

Results

The **Create Avamar and Data Domain Virtual Edition** wizard moves to the **DDVE on Hot Blob Configuration** tab.

Configure the instance settings for DDVE

With the **Create Avamar and Data Domain Virtual Edition** wizard open to the **DDVE on Hot Blob Configuration** tab, complete the following configuration:

About this task

DDVE 4.0 on Azure supports hot blob storage. The *Data Domain Virtual Edition Installation and Administration Guide* for DDVE 4.0 provides more information about hot blob storage.

Procedure

1. From the **DDVE Version** drop-down, select the available release.

   Your choice of application from the Marketplace determines the available options.

2. In the **DDVE Name** field, type the hostname for the DDVE instance.

   Note: The maximum length of the virtual machine name is 10 characters.

3. Using the information from the DDVE system requirements, select a value for **DDVE VM Size**.

   Select a size that meets or exceeds the DDVE system requirements for the chosen capacity configuration.

4. In the **DDVE VM Size** field, select an option from the options available in the list.
5. In the **DDVE Capacity (TB)** field, select a storage capacity from the options available in the list.
6. For **Sysadmin Authentication type**, select `Password` or `SSH public key`.
   a. If you selected `Password`, complete the **Password** and **Confirm password** fields.
   b. If you selected `SSH public key`, complete the **SSH public key** field.
7. In the **DDBoost user name** field, type the login name for the DDBoost user.
8. In the **DDVE common password** and **Confirm password** fields, type a password for the DDVE passphrase, DDBoost user account, and sysadmin account (if DDVE authentication is key-based).
9. In the **SNMP community string** field, type the SNMP community string used to monitor the DDVE. Blank spaces are not allowed.
10. In the **Resource ID of the blob storage account** field, type the resource ID for the Azure blob storage account.

    The account type must be blob storage. If you do not have an Azure blob storage account, create one before continuing.

    To obtain the resource ID from the Azure portal, click **Storage accounts**, select the storage account from the list, and then click **Properties**. A valid resource ID follows this format:

    ```
    /subscriptions/<subscription GUID>/resourceGroups/<resource
    group name>/providers/Microsoft.Storage/storageAccounts/
    <storage account name>
    ```

11. In the **Container name** field, type the name of the empty container that will store data for DDVE backups. The container must be empty or the configuration fails. If you do not have an empty container, create one before continuing.
12. Click **OK**.

Results

The **Create Avamar and Data Domain Virtual Edition** wizard moves to the **Summary** tab.

Create the AVE and DDVE VMs

With the **Create Avamar and Data Domain Virtual Edition** wizard open to the **Summary** tab, complete the following steps:

Procedure

1. Wait for the Azure portal to validate the AVE and DDVE configuration.

   Review and correct any errors.

2. Click **OK**.

   The **Create Avamar and Data Domain Virtual Edition** wizard moves to the **Buy** tab.

3. Review the estimated pricing and the terms.
4. Click **Create**.

   The Azure portal starts to deploy the AVE and DDVE VMs. The deployment process can take considerable time to complete, depending on the selected capacity configurations.

5. Observe the output from the deployment process and respond to any problems.

   The Azure portal displays a notification when the deployment completes. The output from the deployment process provides the private IP addresses for AVE and DDVE.

   After deployment completes, Azure automatically configures AVE and DDVE with the indicated selections. Deployment and configuration may take more than one hour before AVE and DDVE are ready to use.

6. Record both private IP addresses for later use.
7. Monitor the configuration process:

   a. Using SSH, connect to AVE with the private IP address that you recorded from the deployment process.

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

   ```
   tail -f /usr/local/avamar/var/ave_ddve_config.log
   ```

   After the configuration completes, the log file contains the following lines:

   ```
   Completed ave-config
   Config AVE successsfully
   ```

8. Create a static IP address for the AVE and DDVE virtual machines:

   a. From the Azure portal, select the virtual machine, and then select **Networking**.

   b. Select the network interface that is assigned to the virtual machine.

   The Azure portal opens the network interface overview.

   c. Click **IP Configurations**.

   The Azure portal lists the available IP configurations.

   d. Click the IP configuration that is currently assigned to the virtual machine.

   The IP configuration window opens.

   e. In the **Private IP address settings** section, for the **Assignment** field, select **Static**.

f. Verify the current setting or type a new static IP address for the virtual machine.

g. Click **Save**.

Repeat this step for both the AVE and DDVE virtual machines.

Deploy AVE and DDVE with an Azure solution template

The following topics describe how to deploy AVE and Data Domain Virtual Edition (DDVE) virtual machines in Azure by using a solution template. The solution template uses the DDVE 6.1.0 image in the Azure marketplace (`ddve-31-ver-060100`).

Solution templates are JSON files that simplify the deployment of multiple Azure resources and dependencies. Use the template to programmatically deploy the combined AVE and DDVE solution.

Obtain the solution template for AVE and DDVE from Online Support (https://support.emc.com/) before proceeding. The solution template contains two files:

- `AVE_DDVE_SolutionTemplate.json`
- `AVE_DDVE_SolutionTemplate_parameters.json`

  The parameter file is only required for deployment via Powershell.

The complete deployment process consists of the following steps:

1. Upload an AVE virtual machine image to Azure and configure prerequisite items.
2. Deploy AVE and DDVE using the solution template.
3. Configure a secure gateway system.
4. Configure DDVE.
5. Configure AVE.
6. Attach the DDVE system to AVE.

Steps 3–6 are outside the scope of this installation guide. The following publications provide additional information to complete the deployment process:

- *Avamar Administration Guide*
- *Avamar and Data Domain System Integration Guide*
- *Data Domain Operating System Initial Configuration Guide*
- *Data Domain Operating System Administration Guide*

This installation guide includes steps for the Azure Resource Manager, for Azure Powershell, and for the Azure CLI. The following Microsoft documentation provides additional information about using solution templates with both interfaces:

- Deploy resources with Resource Manager templates and Azure portal
- Deploy resources with Resource Manager templates and Azure CLI
- Deploy resources with Resource Manager templates and Azure PowerShell
- Parameter files

Upload the AVE image

The solution template uses this AVE image for each automatic deployment. This section also configures several important prerequisite items. Record the indicated values for later use.

Before you begin

In general, select the same resource group for each task, and select the same location.

Procedure

1. Download and decompress the AVE virtual appliance file.

   Download the required software from https://support.emc.com/.

2. Open the Azure portal at https://portal.azure.com and log in to the Azure account.

Create a resource group

Create a resource group for solution template deployment by performing the following steps:

Procedure

1. From the **Favorites** list, click **Resource groups**.
2. Click **Add**.
3. In the **Resource group name** field, type a name for the resource group.
4. Select an available Azure subscription.
5. From the **Resource group location** drop-down, select an available location.
6. Click **Create**.

After you finish

Record the name of the new resource group.

Create a storage account

The storage account holds the uploaded AVE virtual appliance file and stores the diagnostic logs from the deployment. Create a storage account for solution template deployment by performing the following substeps:

Procedure

1. From the **Favorites** list, click **Storage accounts**.
2. Click **Add**.

   The **Create storage account** wizard opens on the **Basics** tab.

3. Select an available Azure subscription.
4. From the **Resource group** drop-down, select the new resource group.
5. In the **Storage account name** field, type a name for the storage account.
6. From the **Location** drop-down, select an available location.
7. For **Performance**, select `Standard` or `Premium`.
8. From the **Account kind** drop-down, select `StorageV2 (general purpose v2)`.
9. From the **Replication** drop-down, select `Locally-redundant storage (LRS)`.

10. For **Access tier (default)**, select `Hot`.
11. Click **Review + create**.

    The remaining fields on the **Advanced** and **Tags** tabs are optional for most users.

    The **Create storage account** wizard moves to the **Review + create** tab.
12. Wait for the Azure portal to validate the storage account configuration.

    Review and correct any errors.
13. Click **Create**.

    The Azure portal starts to deploy the storage account. The deployment process can take several minutes to complete.
14. Observe the output from the deployment process and respond to any problems.

    The Azure portal displays a notification when the deployment completes.

After you finish

Record the name of the new storage account.

Create a container

Create a container for solution template deployment by performing the following steps:

Procedure

1. From the **Favorites** list, click **Storage accounts**.
2. Select the new storage account.
3. From the navigation pane for the new storage account, click **Blobs**.
4. Click **+ Container**.
5. In the **Name** field, type a name for the container.
6. For **Public access level**, select `Private (no anonymous access)`.

Results

The **Blobs** pane lists the new container.

Upload the AVE virtual appliance file

Upload the AVE virtual appliance file to the container for solution template deployment by performing the following steps:

Before you begin

Note: Transferring the AVE virtual appliance file may take considerable time.

If you encounter difficulty while uploading the AVE virtual appliance file, retry the upload with the Azure command line tool `AzCopy` or the Azure command-line interface (CLI).

- https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy provides more information about `AzCopy`, including download instructions and usage examples.
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/classic/create-upload-vhd provides more information about the Azure CLI, including usage examples.

Transfer the AVE virtual appliance file as a page blob.

Procedure

1. Select the new container.

   The Azure portal opens the contents of the container.
2. Click **Upload**.
3. Select the AVE virtual appliance file that you downloaded and decompressed earlier.
4. Click **Advanced**.
5. For **Blob type**, select `Page blob`.
6. Ensure that **Upload .vhd files as page blobs** is checked.
7. Click **Upload**.

After you finish

The upload progresses in the background. You can continue to complete tasks in the Azure portal while uploading the AVE virtual appliance file.

Create a virtual network and subnet

Create a virtual network and subnet for solution template deployment by performing the following steps:

Procedure

1. From the **Favorites** list, click **Virtual networks**.
2. Click **Add**.

   The **Create virtual network** wizard opens.
3. In the virtual network **Name** field, type a name for the virtual network.
4. In the **Address space** field, supply an address space in the form ***<startingIP>/<subnet>***.

   For example, 10.2.3.0/24 or 192.168.0.0/16.
5. Select an available Azure subscription.
6. From the **Resource group** drop-down, select the new resource group.
7. From the **Location** drop-down, select an available location.
8. In the subnet **Name** field, type a name for the new subnet.
9. Supply an address prefix in the form ***<startingIP>/<subnet>***.

   By default, the wizard copies this field from the value that you typed for the new virtual network.
10. Click **Create**.

    The Azure portal validates the virtual network settings and starts to deploy the storage account. Review and correct any validation errors. The deployment process can take several minutes to complete.

After you finish

Record the names of the new virtual network and subnet.

Create an image

Create an image for solution template deployment by performing the following steps:

Procedure

1. From the Azure portal navigation pane, click **+ Create a resource**.
2. In the **Search** field, type `image`.
3. From the search results, select the component **Image**, published by Microsoft.

   The component description pane opens on the right.
4. Click **Create**.

   The **Create image** wizard opens.
5. In the **Name** field, type a name for the new image.
6. Select an available Azure subscription.
7. From the **Resource group** drop-down, select the new resource group.
8. From the **Location** drop-down, select an available location.
9. For **OS type**, select `Linux`.
10. For the **Storage blob** field, browse to the uploaded AVE virtual appliance file.
11. For **Account type**, select `Standard HDD`.
12. For **Host caching**, select `None`.
13. Click **Create**.

After you finish

Record the resource ID for the new AVE image.

Solution template parameters

These template parameters are common to every deployment method. Use the following descriptions to provide parameters to the template:

AVE Name

Required. Type the hostname to assign to AVE. Limited to 10 characters, special characters are prohibited.

AVE Image Resource ID

Required. Provide the value that you recorded when you uploaded the AVE image.

AVE Size in TB

Select the installed capacity for this AVE instance: either **2** or **4** TB. This selection governs the choice of Azure standard tier, as detailed in System requirements on page 19, and the automatic creation of virtual disks, as detailed in Virtual disk requirements on page 21.

AVE Username

Required. Type the name of a new user with administrative privileges for AVE. Cannot be `root` or `admin`.

AVE Authentication Mode

Select the method by which users are authenticated when initiating an SSH connection: either **Password** or **SSH Public Key**.

AVE User Password

Type a password for the new user. Input must be 12–72 characters that include any three of the following: one lowercase letter, one uppercase letter, one number, and one special character. Complete this field even if using an SSH public key for authentication. The *Avamar Product Security Guide* provides more information.

The default is `Changeme123#`.

AVE Ssh Public Key

Required. Provide the representation of the new user's SSH public key. This field applies only when **SSH Public Key** authentication is selected. Complete this field even if using a password for authentication.

DDVE Name

Required. Type the hostname to assign to DDVE. Limited to 10 characters, special characters are prohibited.

DDVE Virtual Machine Size

Select the maximum installed capacity for this DDVE instance: either **Standard_F4** or **Standard_F8**. This selection governs the choice of Azure standard tier and the automatic creation of virtual disks. All virtual disks are 1000 GB.

Standard_F4 supports a maximum capacity of 7 TB. **Standard_F8** supports a maximum capacity of 15 TB.

DDVE Data Disk Size in TB

Select the actual installed capacity for this DDVE instance: integer values between 1–15 TB. The choice of **DDVE Virtual Machine Size** limits the values that are available for selection.

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

DDVE Authentication Mode

Select the method by which users are authenticated when initiating an SSH connection: either **Password** or **SSH Public Key**.

DDVE Sysadmin Password

Type a password for the `sysadmin` user. Input must be 12–72 characters that include any three of the following: one lowercase letter, one uppercase letter, one number, and one special character. Complete this field even if using an SSH public key for authentication. The *Data Domain Product Security Guide* provides more information.

The default is `Changeme123#`.

DDVE Ssh Public Key

Provide the representation of the `sysadmin` user's SSH public key. This field applies only when **SSH Public Key** authentication is selected.

Vnet Existing Resource Group

Required. Type the name of the resource group in which you created the virtual network.

Vnet Name

Required. Type the name of the new virtual network.

Vnet Subnet Name

Required. Type the name of the subnet that you created within the new virtual network.

Diagnostics Storage Account Existing Resource Group

Required. Type the name of the resource group in which you created the storage account.

Diagnostics Storage Account Name

Required. Type the name of the new storage account.

Deploy from the Azure Resource Manager

The Azure Resource manager provides a graphical interface for deployment of the appliances.

Procedure

1. Extract `AVE_DDVE_SolutionTemplate.json` to a temporary folder on the local computer.
2. Return to the Azure portal.
3. From the **Favorites** list, click **Dashboard**.
4. Click **Template deployment**.

   If you do not see **Template deployment**, complete the following substeps:

   a. Type `template deployment` in the dashboard search field.

   b. From the search results, select the Marketplace item **Template deployment**, published by Microsoft.

   The **Template deployment** description pane opens on the right.
5. Click **Create**.

   The **Custom Deployment** page opens.
6. Click **Build your own template in the editor**.

   The **Edit Template** page opens to an empty template and default values in the editor.
7. Click **Load File**.
8. Browse to `AVE_DDVE_SolutionTemplate.json` and then click **Open**.

   The AVE/DDVE solution template opens in the editor.
9. Click **Save**.

   The **Custom Deployment** page opens and displays the new template.
10. The **Basics** section is common to all Azure deployments. Choose an appropriate **Subscription**, **Resource Group**, and **Location**.
11. Provide all required AVE and DDVE parameters.

    Some fields are preconfigured. Mandatory fields have red names and an `*`. Validated fields have a purple border and a green check mark.

    Solution template parameters on page 86 provides additional information on parameter values.

12. Review the terms and conditions, and then check **I agree to the terms and conditions stated above**.
13. Click **Purchase**.

    Deployment may take 15–30 minutes. Note all of the return values from the deployment process.

Deploy from the Azure Powershell

You can also deploy the appliances from the command line by using Azure Powershell. This method provides the required parameters in the `AVE_DDVE_SolutionTemplate_parameters.json` file.

Procedure

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

   Solution template parameters on page 86 provides additional information. Each parameter in this file corresponds to an input field in the Azure Resource Manager method.

   For example:

```
{
  "$schema": "https://schema.management.azure.com/schemas/
2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "AVEName": {
      "value": "AVE-test"
    },
    "AVEImageResourceID": {
      "value": "/subscriptions/azure-test/resourceGroups/rg-
test/providers/provider-test/vm-image/ave-image"
    },
    "AVESizeInTB": {
      "value": "2"
    },
    "AVEUsername": {
      "value": "test"
    },
    "AVEAuthenticationMode": {
      "value": "Password"
    },
    "AVEUserPwd": {
      "value": "S3cure#P@ssW0rd!"
    },
    "AVESshPublicKey": {
      "value": "Input only when SSH Public Key is selected as
the authentication mode."
    },
    "DDVEName": {
      "value": "DDVE-test"
    },
    "DDVEVirtualMachineSize": {
      "value": "Standard_F4"
    },
    "DDVEDataDiskSizeInTB": {
      "value": "1"
    },
    "DDVEAuthenticationMode": {
      "value": "Password"
    },
```

```
    "DDVESysadminPwd": {
      "value": ".DdV3#P@ssW0rd%"
    },
    "DDVESshPublicKey": {
      "value": "Input only when SSH Public Key is selected as
the authentication mode."
    },
    "vnetExistingResourceGroup": {
      "value": "rg-test"
    },
    "vnetName": {
      "value": "vnet-test"
    },
    "vnetSubnetName": {
      "value": "subnet-test"
    },
    "diagnosticsStorageAccountExistingResourceGroup": {
      "value": "rg-test"
    },
    "diagnosticsStorageAccountName": {
      "value": "storage-test"
    }
  }
}
```

3. Save and close the file.
4. In the Azure Powershell interface, log in and select an appropriate subscription.
5. In the Azure Powershell interface, type the following command on one line:

   New-AzureRmResourceGroupDeployment -Name *<DeploymentName>* -ResourceGroupName *<ResourceGroupName>* -TemplateFile AVE_DDVE_SolutionTemplate.json -TemplateParameterFile AVE_DDVE_SolutionTemplate_parameters.json

   where:

   - *<DeploymentName>* is a unique name for this AVE and DDVE deployment.
   - *<ResourceGroupName>* is a resource group in which to place the new instances of AVE and DDVE.

   Deployment may take 15–30 minutes. Note all of the return values from the deployment process.

Deploy from the Azure CLI

You can also deploy the appliances from the command line by using Azure Command Line Interface (CLI). This method provides the required parameters in the `AVE_DDVE_SolutionTemplate_parameters.json` file.

Procedure

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

   Solution template parameters on page 86 provides additional information. Each parameter in this file corresponds to an input field in the Azure Resource Manager method.

   For example:

```
{
  "$schema": "https://schema.management.azure.com/schemas/
```

```
2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "AVEName": {
      "value": "AVE-test"
    },
    "AVEImageResourceID": {
      "value": "/subscriptions/azure-test/resourceGroups/rg-
test/providers/provider-test/vm-image/ave-image"
    },
    "AVESizeInTB": {
      "value": "2"
    },
    "AVEUsername": {
      "value": "test"
    },
    "AVEAuthenticationMode": {
      "value": "Password"
    },
    "AVEUserPwd": {
      "value": "S3cure#P@ssW0rd!"
    },
    "AVESshPublicKey": {
      "value": "Input only when SSH Public Key is selected as
the authentication mode."
    },
    "DDVEName": {
      "value": "DDVE-test"
    },
    "DDVEVirtualMachineSize": {
      "value": "Standard_F4"
    },
    "DDVEDataDiskSizeInTB": {
      "value": "1"
    },
    "DDVEAuthenticationMode": {
      "value": "Password"
    },
    "DDVESysadminPwd": {
      "value": ".DdV3#P@ssW0rd%"
    },
    "DDVESshPublicKey": {
      "value": "Input only when SSH Public Key is selected as
the authentication mode."
    },
    "vnetExistingResourceGroup": {
      "value": "rg-test"
    },
    "vnetName": {
      "value": "vnet-test"
    },
    "vnetSubnetName": {
      "value": "subnet-test"
    },
    "diagnosticsStorageAccountExistingResourceGroup": {
      "value": "rg-test"
    },
    "diagnosticsStorageAccountName": {
      "value": "storage-test"
    }
  }
}
```

3. Save and close the file.
4. In the Azure CLI, log in and select an appropriate subscription.
5. In the Azure CLI, type the following command on one line:

   az group deployment create --name *<DeploymentName>* -ResourceGroupName *<ResourceGroupName>* -TemplateFile

```
AVE_DDVE_SolutionTemplate.json -TemplateParameterFile
AVE_DDVE_SolutionTemplate_parameters.json
```

where:

- *<DeploymentName>* is a unique name for this AVE and DDVE deployment.
- *<ResourceGroupName>* is a resource group in which to place the new instances of AVE and DDVE.

Deployment may take 15–30 minutes. Note all of the return values from the deployment process.

Complete post-deployment configuration

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

Before you begin

Note and record the deployment status, and the **AVAMARURL** and **DDSMURL** values from the deployment task. Access to these URLs requires a secure gateway system, which is beyond the scope of this installation guide.

Procedure

1. Create a static IP address for the AVE VM by performing the following substeps:
   a. From the network interface configuration page for the AVE VM, click **IP configurations**.
   b. Click the network name.
   c. Select **Static** for the **Private IP address** assignment.
   d. Specify a private IP address or accept the default private IP address from Azure.
   e. Record the private IPv4 address for future use. This value is the default password for AVE.
   f. Click **Save**.
2. Obtain the AVE private IPv4 address by performing one of the following substeps:
   a. Use the Azure Portal to obtain the private IPv4 address.

      The Microsoft documentation for the Azure Portal provides more information.

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

      ```
      az vm list-ip-addresses --name vm-name
      ```

   c. Record the private IPv4 address for future use. This value is the default password for AVE.
3. Configure a secure gateway system.
4. Install the Avamar software.

   Install and configure the Avamar software on page 97 contains instructions.

   Note: After launching the instance, the AVE initializes and restarts automatically. During this process, which takes 15 to 25 minutes, the AVE

installs drivers and an updated kernel. You cannot install the Avamar software until this process is complete because the 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.

Network security group

The following tables describe the rules that should be added to an Azure network security group.

Inbound ports for the Azure network security group

The following tables describe the rules that should be added to an Azure network security group.

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.

Note: Avamar no longer supports HTTP access to TCP port 80. Use the HTTPS ports 443 to access these services instead.

For all table entries:

- The **Source** and **Destination** fields are `Any`.
- The **Source port range** field is `*`
- The **Action** is `Allow`.
- Assign a unique priority value to each rule, starting at 100.
- Type a unique description for each rule. The value must be unique for both inbound and outbound rules.

Table 17 Inbound ports for the Azure network security group

Type	Protocol	Destination port range
SSH	TCP	22
Custom TCP Rule	TCP	161
Custom UDP Rule	UDP	161
Custom TCP Rule	TCP	163
Custom UDP Rule	UDP	163
HTTPS	TCP	443

Table 17 Inbound ports for the Azure network security group (continued)

Type	Protocol	Destination port range
Custom TCP Rule	TCP	700
Custom TCP Rule	TCP	7543
Custom TCP Rule	TCP	7778 - 7781
Custom TCP Rule	TCP	8543
Custom TCP Rule	TCP	9090
Custom TCP Rule	TCP	9443
Custom TCP Rule	TCP	27000
Custom TCP Rule	TCP	28001 - 28002
Custom TCP Rule	TCP	28810 - 28819
Custom TCP Rule	TCP	29000
Custom TCP Rule	TCP	30001 - 30010

Outbound ports for the Azure network security group

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.

By default, Azure has a rule AllowInternetOutBound with priority `65001` to allow all outbound internet traffic. Override this rule by adding a rule with a priority (that is, an integer number) that is greater than all customized rules' priority, and less than 65000: `source: *, destination: *, protocol: *, action: Deny`. Azure documentation contains information about creating a firewall rule.

For all table entries:

- The **Source** and **Destination** fields are `Any`.
- The **Source port range** field is `*`
- The **Action** is `Allow`.
- Assign a unique priority value to each rule, starting at 100.
- Type a unique description for each rule. The value must be unique for both inbound and outbound rules.

Table 18 Outbound ports for the Azure network security group

Type	Protocol	Destination port range
Custom TCP Rule	TCP	7
SSH	TCP	22
SMTP	TCP	25
DNS (UDP)	UDP	53
Custom TCP Rule	TCP	111
Custom UDP Rule	UDP	111

Table 18 Outbound ports for the Azure network security group (continued)

Type	Protocol	Destination port range
Custom TCP Rule	TCP	161
Custom UDP Rule	UDP	161
Custom TCP Rule	TCP	163
Custom UDP Rule	UDP	163
HTTPS	TCP	443
Custom TCP Rule	TCP	700
Custom TCP Rule	TCP	2049
Custom UDP Rule	UDP	2049
Custom TCP Rule	TCP	2052
Custom UDP Rule	UDP	2052
Custom TCP Rule	TCP	3008
Custom TCP Rule	TCP	8443
Custom TCP Rule	TCP	8888
Custom TCP Rule	TCP	9090
Custom TCP Rule	TCP	9443
Custom TCP Rule	TCP	27000
Custom TCP Rule	TCP	28001-28010
Custom TCP Rule	TCP	29000
Custom TCP Rule	TCP	30001-30010

Azure security best practices

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

Follow the Azure network security best practices

Follow the Azure network security best practices at https://docs.microsoft.com/en-us/azure/best-practices-network-security to define an Information Security Management System (ISMS). Build a set of security policies and processes for the organization to protect the Avamar server and clients in the Azure cloud.

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 the virtual machine, select **None** for the public IP address setting 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 19 Inbound ports for Linux gateways

Type	Protocol	Port range	Source
Custom TCP rule	TCP	7778-7781	Subnet IPv4 CIDR
HTTPS	TCP	443	Subnet IPv4 CIDR
SSH	TCP	22	0.0.0.0/0

Table 20 Inbound ports for Windows gateways

Type	Protocol	Port range	Source
Custom TCP rule	TCP	7778-7781	Subnet IPv4 CIDR
RDP	TCP	3389	0.0.0.0/0
HTTPS	TCP	443	Subnet IPv4 CIDR
SSH	TCP	22	Subnet IPv4 CIDR

Use only key-based SSH access

Use an SSH public key when launching AVE in Azure. Select **SSH public** key as the **Authentication type** when creating the virtual machine.

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 Network security group on page 93.

Timely application of Avamar security patches

Avamar releases quarterly OS security patch roll-ups. Apply these patches to AVE on a regular basis.

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.

   The *Avamar Virtual Edition Configuration Workflow Guide* opens.
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.

PART 3

Common Procedures

The following chapters describe instructions that are common to all virtual environments.

CHAPTER 7

Completing post-installation activities

Review the following activities after you install the Avamar software and complete any that apply:

Verify the Avamar services

As a best practice, verify that the Avamar services have started.

Procedure

1. Open a command shell and log in to the server as admin.
2. Verify that all services are online by typing the following command:

   ```
   dpnctl status
   ```

   Information similar to the following is displayed in the command shell:

   ```
   Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/
   admin_key)
   dpnctl: INFO: gsan status: up
   dpnctl: INFO: MCS status: up.
   dpnctl: INFO: emt status: up.
   dpnctl: INFO: Backup scheduler status: up.
   dpnctl: INFO: Maintenance windows scheduler status: enabled.
   dpnctl: INFO: Unattended startup status: enabled.
   dpnctl: INFO: avinstaller status: up.
   dpnctl: INFO: ConnectEMC status: up.
   dpnctl: INFO: ddrmaint-service status
   ```

(Optional) Add EMC Secure Remote Services

EMC Secure Remote Services (ESRS) is a two-way connection between Dell EMC products and solutions and Dell EMC Customer Support. ESRS provides:

- Proactive remote monitoring and repair
- 5x faster issue resolution times
- 15 percent higher levels of availability

Documentation, downloads and product information for ESRS, including installation instructions, are available on Online Support.

Test the Data Domain integration

If you configured AVE with Data Domain, verify the status of the Data Domain integration and open any necessary service requests with Customer Support when problems occur.

Note: The *Avamar and Data Domain System Integration Guide* contains information about how to add a Data Domain system to the Avamar server and then verify it. This document also contains information about replication.

Store Avamar server checkpoints on a Data Domain system

You can store checkpoints for Avamar on a Data Domain system. Checkpoints are system-wide backups that are taken for disaster recovery of the Avamar server.

About this task

Restoring checkpoints from a Data Domain system requires assistance from Dell EMC Professional Services. The *Avamar Administration Guide* provides details about checkpoints.

To store checkpoints, perform the following steps:

Procedure

1. In Avamar Administrator, click the **Server** launcher link.

   The **Server** window is displayed.
2. Click the **Server Management** tab.
3. Select a Data Domain system.
4. Click **Actions** > **Edit Data Domain System**.

   The **Edit Data Domain System** window opens.
5. Click the **System** tab and then select **Use system as target for Avamar Checkpoint Backups**.
6. Click **OK**.
7. Click **Close**.

Upgrade the Avamar client downloads

The *Avamar Client Downloads and Client Manager Installer Upgrades Technical Note*, which is available on Online Support contains information about the procedures to install the client installation packages.

Install server hotfixes and the security patch rollup

Dell EMC releases server hotfixes and the Avamar platform OS security patch rollup on a periodic basis. When available, you should install hotfixes and the security patch rollup on new and existing AVE systems.

The *Avamar Administration Guide* contains information about installing hotfixes. KB article https://support.emc.com/kb/335359 provides instructions for installing the Avamar platform OS security patch rollup.

Select a Data Domain target for backups

To select a Data Domain system as the storage for a backup, select the **Store backup on Data Domain system** checkbox in the plug-in options for the backup, and then select the Data Domain system from the list.

Allow only Data Domain backups

To prevent accidental backups to the Avamar metadata node, you can choose to store all backups on Data Domain.

About this task

By default, all Avamar and Data Domain integrations enable client backups to be stored on either the Avamar or Data Domain system. To only store backups on the Data Domain, complete the following procedure.

Note: Ensure that you want all backups stored on Data Domain. Not all Avamar backup clients and plug-ins are supported with Data Domain. After you complete this procedure, backups that are not supported with Data Domain fail. Additionally, these changes cannot be easily reversed without assistance from Dell EMC Professional Services.

Procedure

1. Open a command shell and log in by using one of the following methods:
   - For a single-node server, log in to the server as admin.
   - For a multi-node server, log in to the utility node as admin.
2. Load the admin OpenSSH key by typing:

   ```
   ssh-agent bash
   ssh-add ~admin/.ssh/admin_key
   ```

3. Change directory by typing the following:

   ```
   cd /usr/local/avamar/var/mc/server_data/prefs/
   ```

4. Back up the current `mcserver.xml` file by typing:

   ```
   cp -p mcserver.xml x-mcserver.xml-<YYYYMMDD>
   ```

   where *YYYYMMDD* is the current year, month, and day.

5. Edit the `mcserver.xml` file by typing:

   ```
   vi mcserver.xml
   ```

6. Search for a line that is similar to the following:

   ```
   <entry key="dd_only_mode" value="DATASET" />
   ```

7. Set the value to `ALL` so that the line is similar to the following:

   ```
   <entry key="dd_only_mode" value="ALL" />
   ```

8. Save and exit the file.
9. Restart the MCS by typing the following:

   ```
   dpnctl stop mcs
   dpnctl start mcs,sched
   ```

10. Verify that all services are up and running by typing the following:

    ```
    dpnctl status
    ```

11. Take an MCS flush or backup by typing the following:

    ```
    mcserver.sh --flush
    ```

12. If there are no errors or issues that are seen in the `flush` command, log out of the command line.
13. (Optional) To verify that the changes were successful, perform a test backup:
    a. Log in to the Avamar Administrator GUI.
    b. Perform an on-demand backup using any client.

       Ensure that you specify **Avamar** as the backend storage.

    If the backup fails with an error, the changes were successful.

Results

Information similar to the following appears in the `mcserver.xml` file:

```
admin@avamarave1:/usr/local/avamar/var/mc/server_data/prefs/>: grep
"dd_only_mode" mcserver.xml
```

```
                <entry key="dd_only_mode" value="ALL" />
                <entry key="dd_only_mode_plugin_exclusions"
value="" />
```

CHAPTER 8

Upgrading AVE

The following topics describe how to upgrade AVE in any supported virtual environment:

Upgrade the Avamar software

The AVE upgrade workflow package provides a customer-enabled way to upgrade the Avamar software on an AVE virtual machine. Review the instructions in the workflow guide for the workflow package, on the **SW Releases** page of the **Avamar Installation Manager**.

Procedure

1. Download the AVE upgrade workflow package from https://support.emc.com/.

   You can also use the Avamar Downloader Service or Local Downloader Service (LDLS) to download the workflow package. The *Avamar Administration Guide* contains information about configuring and using the Avamar Downloader Service and the LDLS.

2. 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.

      The root user password is typically set as part of the **ave_config** workflow during Avamar software installation.

   c. Click **Login**.

   The **Avamar Installation Manager** opens to the **Package Selection** page.

3. Upload the AVE upgrade workflow package 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 upload completes, the workflow package automatically appears in the **Repository** table.

4. Click **SW Upgrade**.

   The **SW Upgrade** tab appears.

5. Click the **?** button next to the AVE upgrade workflow package (`AvamarUpgrade-version.avp`).

   The workflow guide opens.

6. Review the workflow guide for information about the required and optional user input fields.

   After you click **Upgrade**, you are no longer able to access the workflow guide.

7. Click **Upgrade** next to the AVE upgrade workflow package.

   The **Installation Setup** page displays.

8. On the **Installation Progress** page, monitor the upgrade 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.
9. After the upgrade completes, install the following optional, but recommended, workflow packages:
   - Avamar platform OS security patch rollup (`AvPlatformOsRollup_<year>-Q<q>-R<r>.avp`)
   - Upgrade client downloads (`UpgradeClientDownloads-<version>.avp`)
   - Upgrade client plugin catalog (`UpgradeClientPluginCatalog-<version>.avp`)

   The *Avamar Administration Guide* provides more information.

Post-upgrade activities

Review the following activities after you upgrade the Avamar software and complete any that apply:

Start the Avamar schedulers

Ensure that the backup and maintenance schedulers are active after the upgrade.

Procedure

1. Open a command shell and log in to the server as admin.
2. Start the backup scheduler by typing the following command

   dpnctl start sched

   Information similar to the following is displayed in the command shell:

   ```
   Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/
   admin_key)
   dpnctl: INFO: Resuming backup scheduler...
   dpnctl: INFO: Backup scheduler resumed.
   ```

3. Start the maintenance scheduler by typing the following command

   dpnctl start maint

   Information similar to the following is displayed in the command shell:

   ```
   Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/
   admin_key)
   dpnctl: INFO: Resuming maintenance windows scheduler...
   dpnctl: INFO: maintenance windows scheduler resumed.
   ```

Verify the Avamar services

As a best practice, verify that the Avamar services have started.

Procedure

1. Open a command shell and log in to the server as admin.
2. Verify that all services are online by typing the following command:

   dpnctl status

   Information similar to the following is displayed in the command shell:

```
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/
admin_key)
dpnctl: INFO: gsan status: up
dpnctl: INFO: MCS status: up.
dpnctl: INFO: emt status: up.
dpnctl: INFO: Backup scheduler status: up.
dpnctl: INFO: Maintenance windows scheduler status: enabled.
dpnctl: INFO: Unattended startup status: enabled.
dpnctl: INFO: avinstaller status: up.
dpnctl: INFO: ConnectEMC status: up.
dpnctl: INFO: ddrmaint-service status
```

Restart the Avamar proxy clients

If Avamar proxy clients are installed, complete the following steps.

Procedure

1. Switch user to root by typing the following command:

   su -

2. Restart the proxy clients by typing the following command:

   mccli mcs reboot-proxy --all=true

   Information similar to the following is displayed in the command shell:

   ```
   0,22357,Initiated request to recycle proxy power.
   ```

   Note: The *Avamar for VMware User Guide* contains information about deploying proxies.

3. Switch user to admin by typing **exit**.

Test the Data Domain integration

If you configured AVE with Data Domain, verify the status of the Data Domain integration and open any necessary service requests with Customer Support when problems occur.

Note: The *Avamar and Data Domain System Integration Guide* contains information about how to add a Data Domain system to the Avamar server and then verify it. This document also contains information about replication.

Generate new certificates for Data Domain systems

When you upgrade an AVE that is connected to a Data Domain system, and session ticket authentication is enabled during the upgrade, you must generate new certificates on the Data Domain system. The *Avamar Product Security Guide* contains more information.

Set a passphrase on the Data Domain systems

When you upgrade an AVE that is connected to a Data Domain system, enable a passphrase for the DD Boost user by performing the following steps:

About this task

Note: The DD Boost user must have admin rights.

Procedure

1. Log in to the Data Domain system.
2. Type the following command at the Data Domain CLI:

   ```
   system passphrase set
   ```

3. When prompted, type a passphrase.

Test replication

If you perform an AVE upgrade and replication was configured before the upgrade, verify the status of replication and open any necessary service requests with Customer Support when problems occur. The *Avamar Administration Guide* contains information about replication.

Upgrade the Avamar client downloads

The *Avamar Client Downloads and Client Manager Installer Upgrades Technical Note*, which is available on Online Support contains information about the procedures to install the client installation packages.

Install server hotfixes and the security patch rollup

Dell EMC releases server hotfixes and the Avamar platform OS security patch rollup on a periodic basis. When available, you should install hotfixes and the security patch rollup on new and existing AVE systems.

The *Avamar Administration Guide* contains information about installing hotfixes. KB article https://support.emc.com/kb/335359 provides instructions for installing the Avamar platform OS security patch rollup.

Alternate AWS Installation Methods

This appendix contains the following topics:

Overview of alternate AWS installation methods

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

Perform the Prerequisites on page 54 before you start the procedures in this appendix.

AWS Marketplace AVE manual launch

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.

Virtual disk requirements on page 21 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.

   System requirements on page 19 contains details about AVE system requirements. The wizard disables any instance types that do not apply to AVE.

10. From the **VPC Settings** drop-down, select the correct virtual private cloud (VPC).
11. From the **Subnet Settings** drop-down, select a corresponding subnet from that VPC.
12. From the **Security Group Settings**, select the security group that you created during the prerequisite task.
13. From the **Key Pair Settings** drop-down, select the key pair that you created during the prerequisite task.
14. Click **Launch**.

    EC2 starts the deployment process.
15. Record the ID for the new AVE instance for later use.
16. Use the EC2 console to monitor the deployment progress and respond to any problems.

    The EC2 console displays a notification when the deployment completes.

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.

      Virtual disk requirements on page 21 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. Virtual disk requirements on page 21 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 68 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.

AVE manual upload

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>"
         },
         "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:

`aws ec2 describe-import-image-tasks --import-task-ids` ***`IMPORT_TASK_ID`*** **`--region`** ***`REGION`***
where:

- *IMPORT_TASK_ID* 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:

```
{
  "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 19 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.

      Virtual disk requirements on page 21 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. Virtual disk requirements on page 21 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:

       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 68 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 AVE/DDVE installation methods

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 roadmaps and complete the associated additional tasks.

AWS CLI

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

- Locate the AWS Marketplace AVE and DDVE machine image IDs on page 122.
- Review the CloudFormation template parameters on page 126.
- Deploy AVE/DDVE via CloudFormation from the AWS CLI on page 128.

Manual upload and installation

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

- Upload and convert the AVE/DDVE virtual appliance file on page 123.
- Review the CloudFormation template parameters on page 126.
- One of the following:
  - Deploy AVE/DDVE via CloudFormation from the AWS console (alternate) on page 127.
  - Deploy AVE/DDVE via CloudFormation from the AWS CLI on page 128.

Locate the AWS Marketplace AVE and DDVE machine image IDs

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 provides additional information.

2. Create a subnet for the VPC and specify an availability zone.

   The AWS 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.

About this task

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:

   ```
   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>"
      },
      "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:

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

where:

- *IMPORT_TASK_ID* 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:

```
{
  "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.

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:

AVE AMI ID (AVEAMIID)

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

DDVE AMI ID (DDVEAMIID)

Required. Provide the value that you recorded when you uploaded the DDVE image.

AVE Instance Size (AVEInstanceSize)

Select the installed capacity for this AVE instance, in TB, from the left column of the following table. This selection governs the choice of EC2 instance type and the automatic creation of virtual disks, as detailed in Virtual disk requirements on page 21.

Table 21 EC2 instance type selection by AVE instance size

AVE instance size	EC2 instance type
2TB	m4.xlarge
4TB	m4.2xlarge
8TB	r4.2xlarge
16TB	r4.4xlarge

AVE EBS volume type for all disks (AVEDiskType)

Select the volume type for this AVE instance: either **gp2** or **st1**. The AWS documentation provides more information on the different volume types.

DDVE Instance Type (DDVEInstanceType)

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 (DDVEDataDisk1Size)

Select the virtual disk size for this DDVE instance, 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.

Table 22 EC2 volume size by DDVE instance size

DDVE instance size	EBS metadata disk allocation
1 to 10 TB	1 TB
11 to 20 TB	2 TB

Table 22 EC2 volume size by DDVE instance size (continued)

DDVE instance size	EBS metadata disk allocation
21 to 30 TB	3 TB
31 to 40 TB	4 TB
41 to 50 TB	5 TB
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

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

VPC ID (`VpcId`)

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

Subnet ID (`SubnetId`)

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 (`AvailabilityZoneName`)

Required. Select the availability zone that you chose for the new VPC.

Key Pair Name (`KeyName`)

Required. Select the name of the new SSH keypair that you created for AVE and DDVE.

Deploy AVE/DDVE via CloudFormation from the AWS console (alternate)

The AWS console provides a graphical interface for deployment of the virtual appliances. This topic forms part of the alternate CloudFormation installation method, and is intended for use with the CloudFormation template.

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 file**.
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 126 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 129.

Deploy AVE/DDVE via CloudFormation 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 126 provides additional information. Each parameter in this file corresponds to an input field in the AWS console method.

   For example:

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

```
    "ParameterValue": "m4.xlarge"
  },
  {
    "ParameterKey": "AVEInstanceType",
    "ParameterValue": "t2.xlarge"
  },
  {
    "ParameterKey": "DDVEDataDisk1Size",
    "ParameterValue": "1TB"
  },
  {
    "ParameterKey": "VpcId",
    "ParameterValue": "vpc-abcdef03"
  },
  {
    "ParameterKey": "SubnetId",
    "ParameterValue": "subnet-abcdef04"
  },
  {
    "ParameterKey": "AvailabilityZoneName",
    "ParameterValue": "us-west-2a"
  },
  {
    "ParameterKey": "KeyName",
    "ParameterValue": "AVE_DDVE_Keypair"
  }
]
```

3. Save and close the file.
4. In the AWS CLI, type the following command on one line:

   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 129.

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 **DDSMURL** 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 68 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.