VMware App Volumes 3.0 Installation and Administration

VMware App Volumes 3.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Contents

App Volumes 3.0 Preface

App Volumes 3.0 Installation and Configuration provides information about using VMware® App Volumes 3.0™, including how to create application bundles ("AppStacks") and make applications available to users, as well as how to install, configure, and use the tool generally.

VMware App Volumes 3.0 enables you to deploy applications to users. These users may be widely separated in space, be using different operating systems, or using different versions of applications. VMware App Volumes 3.0 also enables you to monitor application usage.

Intended Audience

This information is intended for IT professionals intending to provision applications to users (possibly large numbers of users) on potentially geographically widely spaced sites. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

CEIP 1

VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products.

Customer Experience Improvement Program (CEIP)

This product participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html. Follow the procedure below to join or leave the CEIP for VMware App Volumes 3.0.

NOTE   The CEIP displays the first time you launch VMware App Volumes 3.0 and you must make a selection. You can change your selection at any time after that by following the procedure below.

1   Start VMware App Volumes 3.0.

2   Bring up the **Help** menu on any page in the App Volumes UI by clicking on the question mark (?) symbol.

3   Choose **CEIP** from the **Help** menu. The CEIP splash screen appears, with information about CEIP.

4   In the CEIP splash screen, there is a slider next to the prompt "Join Customer Experience Improvement Program." Move the slider to **No** to leave CEIP or **Yes** to join. (The default is Yes.)

5   Click **Save** to finish.

Introducing App Volumes 3.0

2

VMware App Volumes 3.0® is an integrated and unified application delivery and end-user management system for Horizon® and virtual environments. From the App Volumes console, admins can deploy applications and customize users' environments in real time, as well as monitor application assignment and usage, for large numbers of geographically widely separated users.

App Volumes works by bundling applications and data into specialized virtual containers called AppStacks, which are attached to each Windows user session at login or reboot, ensuring the most current applications and data are delivered to the user.

App Volumes also provides writable volumes, which are containers for persistent user profiles, settings, and user-installed applications. Writable volumes are also loaded at login.

User profile, policy, and environment settings can also be managed using the App Volumes Customizations feature.

These are some real-world examples of using VMware App Volumes 3.0:

- instantly delivery ten applications to a user who logs into his or her virtual desktop

- provide consistent user environment settings (e.g., network mappings, printer settings, etc.) to users across non-persistent environments

- update Firefox® version 39 to version 40

- determine average logon time and number of sessions in your deployment

This chapter includes the following topics:

- "App Volumes 3.0 Features," on page 10

- "App Volumes 3.0 Editions," on page 10

- "App Volumes 3.0 Components," on page 11

- "App Volumes Workflow," on page 11

- "App Volumes Best Practices," on page 12

App Volumes 3.0 Features

VMware App Volumes 3.0 provides a seamless end-user experience while reducing infrastructure and management costs and features a simple, efficient interface for deploying applications to users.

Real-Time Application Delivery and Management

App Volumes 3.0 allows administrators to dynamically deliver applications to end-users in seconds. It simplifies application management and eliminates the need to package, modify, or streamline applications.

- Instantly provision applications at scale

- Improve organizational security by dynamically delivering the most current application versions and user entitlements to the user desktop, based on organizational policies

- Reduce administrative overhead and storage costs with a "one-to-many" application-delivery model

- Implement without retraining staff on application installation; App Volumes unobtrusively builds AppStacks during standard installation processes

- Monitor end-user experience and performance of application-delivery infrastructure

Agility

- Logically manage application sets (AppStacks) based on business needs

- Deliver and integrate AppStacks across all virtual desktops

Simplicity

- Integrate into existing infrastructure

- Provision applications as easily as installing them

Flexibility

- Deliver a persistent end-user experience with the storage savings and TCO of a non-persistent environment using user environment management capabilities

- Offer persistent user customizations for user-installed apps and settings, via the writable volume feature

App Volumes 3.0 Editions

VMware App Volumes 3.0 comes in the following editions:

App Volumes Standard

- App Volumes Standard is the basic edition of VMware App Volumes 3.0, intended for SMB customers. App Volumes Standard features robust yet simple tools for managing application assignments; it also includes Customizations capabilities, which allow admins to personalize the end-user's experience and environment.

App Volumes Advanced

- App Volumes Advanced consists of App Volumes Standard plus AppIsolation (the ability to run ThinApp packages). App Volumes Advanced also provides extra management capabilities with AppToggle (the ability to dynamically deliver available applications) and AppScaling with Multizones (the ability to map multiple VMware vCenters® to a single file share).

App Volumes Enterprise

- App Volumes Enterprise includes end-user experience and performance monitoring powered by vRealize Operations for Published Applications (vROps). App Volumes Enterprise identifies and alerts you to potential issues and optimization opportunities for your deployment.

App Volumes 3.0 Components

This section lists and describes the various components associated with VMware App Volumes 3.0.

Table 2-1. VMware App Volumes 3.0 Components

Component	Description
VMware App Volumes 3.0 virtual appliance	(This product.) An OVA (Open Virtual Appliance) deployed on a vSphere
AppStack	A collection of applications on a VHD or VMDK; App Volumes 3.0 uses AppStacks to deploy applications to users
AppCapture	A standalone utility for creating AppStacks. Includes AppMerge, for merging AppStacks
App Volumes Unified Agent Installer	A standalone utility that installs the following optional agents on end-user machines: ■ App Volumes agent ■ UEM agent ■ vROps
Customizations	A feature for personalizing the user's environment, such as setting printer mappings or hard drive visibility (App Volumes Advanced and App Volumes Enterprise only)
vRealize Operations for Published Applications (vROps)	An analytics tool for monitoring performance and end-user experience (App Volumes Enterprise only)

App Volumes Workflow

The workflow for VMware App Volumes 3.0 involves installation, configuration, and usage of both VMware App Volumes 3.0 and associated standalone components.

This is a suggested workflow for using VMware App Volumes 3.0. Some components, such as AppCapture, are standalone and run outside of VMware App Volumes 3.0 itself; you don't necessarily have to run them in the order shown. However, following this sequence will ensure that all installation and configuration dependencies are taken care of.

1   Install VMware App Volumes 3.0. Refer to Chapter 4, "Installing App Volumes 3.0," on page 17.

2   Download and install the App Volumes Unified Agent Installer.

    a   Use the App Volumes Unified Agent Installer to install component agents on client machines. Refer to Chapter 5, "Installing Agents," on page 25 for information about the App Volumes Unified Agent Installer.

3   Download and install the AppCapture standalone program. Refer to Chapter 6, "Managing Applications for Deployment with AppCapture," on page 35 for information about AppCapture.

    a   Create application bundles, or AppStacks, with AppCapture.

    b   Copy the AppStacks to a file share.

4   Configure VMware App Volumes 3.0 (see Chapter 7, "Configuring App Volumes 3.0," on page 47):

    a   Configure an Active Directory. Refer to "Configure an Active Directory," on page 47.

    b   Set roles and permissions for VMware App Volumes 3.0. Refer to "Assign Roles and Permissions," on page 48.

    c   Configure a vCenter. Refer to "Configure a vCenter," on page 49.

    d   Connect to an AV Manager if needed. (You should be connected to a default AV Manager when you start up VMware App Volumes 3.0.) Refer to "Working with AV Managers," on page 52.

    e   Connect to and synchronize with the file share where you've placed the AppStacks you created with AppCapture. Refer to "Configure Application File Shares," on page 51.

    f   Set up a Customizations service location. Customizations enable you to configure the user's environment, such as setting printer access. This location points to a customization file share. Refer to "Configure Customizations File Shares," on page 51.

    g   (optional) Add vRealize Operations for Published Applications (vROps) to enable monitoring of App Volumes 3.0 end-user experience metrics. This feature is available in the App Volumes Enterprise edition only. Refer to "Configure vROps for Published Apps," on page 53.

5   Use VMware App Volumes 3.0 to perform the following tasks:

- Assign applications to users (aka "create a new App Service"). See "Assigning Applications," on page 55.

- Monitor application usage, policies, and more. "Monitoring Application Deployment and Usage," on page 62.

- Create new Customizations services. See "Customizing the User's Capabilities," on page 58.

- Examine and modify inventory of applications and Customizations. See "Working with Inventory," on page 61.

App Volumes Best Practices

Follow these guidelines to ensure that your experience with App Volumes, as well as that of your users, is as trouble-free as possible.

Stagger User On-boarding

We recommend staggering the on-boarding of users (that is, not on-boarding all users at once). Consider on-boarding not more than 100 users per vCenter per session. Staggering user on-boarding can prevent logon delays as well as problems with writable volumes. (For more information on writable volumes, see "Writable Volumes," on page 57.)

Disable (Some) Windows Services

When using Windows 10 with App Volumes, you should disable Windows Update, Indexer, and Search Service. The first-time login to a Windows 10 desktop provisioned with App Volumes is slow, as Windows configures the desktop for first-time use with this new configuration. All subsequent logins are fine as long as you attach a writable volume to the desktop. Writable volumes serve as a cache for the user's profile, which speeds up the login process.

Use a Shared Username and Password on ESX Hosts

vCenters may map to multiple ESX hosts; however, App Volumes only allows you to configure a vCenter with a single username/password for all of its associated ESX hosts. If a host has a different password from the one given in App Volumes, the vCenter will not be able to pass down AppStacks to the datastore, preventing application deployment. As a workaround, create a role on all ESX hosts with the same username and password.

For instructions on how to ensure that your ESX hosts are accessible by App Volumes, see "Problem: ESX Hosts Not Accessible," on page 63.

Do Not Delete File Shares

Deleting a file share that has applications on it will make those applications unavailable for future assignment. Therefore, we recommend not deleting file shares. For more on file shares, see "Working with File Shares," on page 50.

System Requirements for App Volumes 3.0

3

VMware App Volumes 3.0 has specific system requirements. Verify that your environment meets these system requirements before you install and configure App Volumes.

System Requirements

These are the requirements for the App Volumes 3.0 virtual appliance:

- vSphere$^®$ 6.0U1 and above (previous versions of vSphere are not supported)

- 4 vCPUs

- minimum of 80 GB disk space

- minimum of 4 GB memory

You'll also need to install the following components:

- AppCapture (requirements discussed in "AppCapture System Requirements," on page 35)

- App Volumes Unified Agent Installer (requirements discussed in "Agent Volumes Installer Requirements," on page 25)

For system requirements for separate products optionally used by App Volumes 3.0, such as vRealize Operations for Published Applications (vROps) and UEM (used for App Volumes Customizations), see the product guides for those products.

Installing App Volumes 3.0

4

Installing VMware App Volumes 3.0 is straightforward. A wizard guides you through the installation.

To use VMware App Volumes 3.0, you will need to perform the following separate installations:

- You'll deploy the App Volumes OVA, which installs App Volumes itself, including several "under the hood" components.

- You'll run the App Volumes Unified Agent Installer, which enables you to install several key agents on target machines. The Unified Agent Installer is discussed in Chapter 5, "Installing Agents," on page 25.

- You'll install AppCapture. AppCapture (including installation) is discussed in Chapter 6, "Managing Applications for Deployment with AppCapture," on page 35.

Install App Volumes 3.0

This section describes how to install VMware App Volumes 3.0.

Using the VMware App Volumes 3.0 OVA, create a VM on which App Volumes will run:

Prerequisites

Before installing VMware App Volumes 3.0, you must have virtualization software up and running. These instructions are written for vSphere® Client. These instructions also assume that you have a vCenter.

Check Chapter 3, "System Requirements for App Volumes 3.0," on page 15 to make sure that you've met the requirements for running VMware App Volumes 3.0 and its associated components.

You may wish to disable SSL Certificate Validation. See "SSL Certificate Validation," on page 19.

Procedure

1   Go to the VMware downloads page and download the VMware App Volumes 3.0 OVA to your machine.

2   Navigate to the folder where you downloaded it.

3   Double-click the OVA to bring up vSphere Client.

4   Enter the URL for the vCenter you are using, as well as the username and password.

5   In vSphere Client, go to **File**->**Deploy OVA Template...**

6   Browse to the location where the App Volumes OVA is located and click **Next**.

7   Confirm your system settings. In particular, make sure you have enough space for the installation. Click **Next**.

8   Accept the End User Licensing Agreement (EULA) and click **Next**.

9   Enter a name for the virtual machine.

10   Choose an inventory location. This is the location of the vCenter you'll be using. Click **Next**.

11   Choose a host or a cluster on which to run the virtual machine. If you specify a cluster, the next panel asks you to specify a host within that cluster. Click **Next**.

12   Choose a location for storing files used by this virtual machine. Make sure you choose a location with enough space. Click **Next**.

13   Choose a disk format for storing virtual disks. This may be selected for you. If not, you have the following choices:

Option	Description
Thick Provision Lazy Zeroed	Disk space is zeroed out as it's needed
Thick Provision Eager Zeroed	Disk space is pre-zeroed out
Thin Provision	Only that amount of reserved space necessary for the VM is used initially

Click **Next**.

14   Map networks in the VM to networks in your inventory.

15   Customize network properties for your virtual machine. Your vCenter administrator will have the relevant values for the requested information.

16   Review your setup and click **Finish**.

17   Once your VM has deployed, power it up and update VMware Tools as needed.

Click the Summary tab in the vSphere window. You should now see an IP address for VMware App Volumes 3.0 You may want to write this down; it's the address where you'll log in to App Volumes with a browser, once you've finished other installations.

Logging into the OVA

These are the steps for logging into the App Volumes OVA.

You may need to log into the App Volumes OVA; for example, if you're working with SSL Certificate Validation (see "SSL Certificate Validation," on page 19).

Procedure

1   Bring up the App Volumes 3.0 virtual machine in vSphere Client.

2   Click the **Console** tab.

3   For the username, enter **root**.

4   For the password, enter **123**.

You are prompted to enter a new password.

5   Enter a new password.

The password must have the following characteristics:

- minimum 10 characters in length
- must include at least 1 uppercase character
- must include at least 1 lowercase character
- must include at least 1 numeric character
- must include at least 1 special character

■ must consist only of visible ASCII characters

SSL Certificate Validation

You can choose whether to enable or disable SSL Certificate Validation.

By default, SSL Certificate Validation is enabled for XMP and microservices external communication in the OVA (for example, with vROps, vCenters, and external AV Managers).

To disable SSL Certificate Validation, run the following script:

`/etc/wemi/utils/disable_ssl_validation.sh.`

NOTE   VMware discourages disabling SSL Certificate Validation except for non-production usage.

To enable SSL Certificate Validation at any stage, run the following script:

`/etc/wemi/utils/enable_ssl_validation.sh.`

If you choose to have SSL Certificate Validation enabled, communication with external products like vCenter, vROps Manager and external AV Manager may have problems, because the default certificates of those products are either "self-signed" or "issued by private Certificate Authorities."

To work around these problems, refer to the following sections:

■ "Handling SSL Certificates for vCenters," on page 19

■ "Handling SSL Certificates for Active Directories," on page 20

■ "Handling SSL Certificates for External App Volumes Managers," on page 21

■ "Handling SSL Certificates for vROps," on page 22

■ "Enable TLSv1.0 Protocol," on page 24

See also "Enabling and Disabling SSL, SSH, and the OVA Firewall," on page 65.

Handling SSL Certificates for vCenters

This section describes the configurations for using vCenters when SSL Certificate Validation is enabled.

Your vCenter can have one of the following types of SSL certificates:

■ Default certificates (issued by VMware)

By default, vCenter certificates are issued by a private VMware Certificate Authority.

If you want to use vCenter with App Volumes 3.0 without replacing the default certificates, please follow these steps:

a Export the default vCenter CA certificate by following the instructions provided in this Knowledge Base (KB) article: https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2108294.

b Copy the certificate data from the ".0" file after following the instructions in the KB article.

This certificate data should be copied/appended to the `cacert.pem` file.

■ Single/chained corporate-signed (local/private) certificates

Steps for replacing the vCenter default SSL certificate with a corporate-signed certificate are given here: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2111219.

Be sure to copy the corporate CA's public certificate, and its contents should be copied/appended in the `cacert.pem` file. See "Handling Corporate-signed Certificates," on page 20.

- Public CA-signed certificate

  Steps for replacing the vCenter default SSL certificate with a public CA-signed certificate are given here: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2111219.

  Be sure to copy the public CA's public certificate, and its contents should be copied/appended in the `cacert.pem` file. See "Handling Public CA-signed Certificates," on page 20.

The App Volumes trusted CA certificate store will point to the file set by the environment variable `SSL_CERT_FILE`. Therefore, you should set the value of `SSL_CERT_FILE`; for example:

```
SSL_CERT_FILE=/user/local/av-manager/config/cacert.pem
```

The `SSL_CERT_FILE` environment variable and the file to which it points should be readable by "av-mgr" user in the App Volumes OVA/VM.

NOTE If you wish to disable SSL Certificate Validation only for vCenters, you can do so by setting

```
AVM_DISABLE_VCENTER_SSL_VALIDATION=1
XMP_DISABLE_VCENTER_SSL_VALIDATION=1
```

Handling Corporate-signed Certificates

These instructions show how to handle SSL Certificate Validation for vCenters, for corporate-signed (local/private) certificates.

Procedure

1   Convert the corporate CA certificate to PEM format.

    This example shows how to convert the certificate from CRT to PEM format using openSSL:

    ```
    openssl x509 -in mycert.crt -out mycert.pem -outform PEM
    ```

2   Append the converted file to the CA certificate file (e.g., `/user/local/av-manager/config/cacert.pem`).

Handling Public CA-signed Certificates

This is how to handle SSL Certificate Validation for vCenters, for public CA-signed certificates.

Procedure

1   Download the PEM file from http://curl.haxx.se/ca/cacert.pem.

2   Append the file to an App Volumes trusted CA certificate store (e.g., `/user/local/av-manager/config/cacert.pem`).

Handling SSL Certificates for Active Directories

Follow these instructions for configuring SSL for Active Directories.

Prerequisites

If your AD is configured to use LDAPS, then you have to add your Active Directory's CA file to the App Volumes trusted CA certificate store.

Procedure

1   Export the CA certificate from your AD and convert it to PEM (base 64 encoded) format.

    This example shows how to convert the certificate from CER to PEM format using openSSL:

    ```
    openssl x509 -in mycert.cer -out mycert.pem -outform PEM
    ```

2   Append the contents of the converted file to the App Volumes trusted CA certificate store.

3   Set the environment variable `SSL_CERT_FILE` to the path of the file where Active Directory certificate is copied. This file should be readable for "av-mgr" user.

If you've already created the file and set the environment variable for handling vCenter certificates (as mentioned in), just append the Active Directory certificate in the same file.

NOTE   If you wish to disable SSL Certificate Validation only for Active Directories, you can do so by setting

```
AVM_DISABLE_LDAP_SSL_VALIDATION=1
XMP_DISABLE_LDAP_SSL_VALIDATION=1
```

Handling SSL Certificates for External App Volumes Managers

These sections describe how to handle SSL certificates for AV Managers.

All external App Volumes Managers should have SSL certificates set up with a CA-signed certificate.

■

■

Replacing the Default Self-Signed Certificate of AV Manager with a CA-signed Certificate

These instructions describe how to set up an external App Volumes Manager with a CA-signed certificate.

These steps have to be followed for each external AV Manager. Note that the same CA file, once generated, can be used to further sign all AV managers.

Procedure

1   Generate a private key for CA. This key is necessary if new certificates need to be signed by the CA:

```
openssl genrsa –out rootCA.key 2048
```

2   Generate the CA certificate:

```
openssl req –x509 –new –nodes –key rootCA.key –days 365 –out rootCA.crt
```

In this example, the validity of the certificate is set to 365 days.

3   Generate a private key for the server:

```
openssl genrsa –out host.key 2048
```

4   Generate a CSR (Certificate Signing Request):

```
openssl req –new –key host.key –out host.csr
```

When prompted for "Common Name," provide the FQDN (Fully Qualified Domain Name) of the AV Manager's host server.

NOTE   The FQDN mentioned should be pingable from the primary server.

---

5   Sign the server certificate with the CA certificate:

```
openssl x509 –req –in host.csr –CA rootCA.crt –CAkey rootCA.key –CAcreateserial –out host.crt
–days 365
```

6   Copy the certificate and key file and replace it in place of the App Volumes Manager's SSL certificate and key files:

```
cp server.crt /etc/nginx/appvol_self_vmware.com.crt
```

```
cp server.key /etc/nginx/appvol_self_vmware.com.key
```

7   Restart the `nginx` service:

```
service nginx restart
```

Installing SSL Certificates of External App Volumes Managers

Follow these instructions for installing SSL for external App Volumes Managers.

Procedure

1   Copy the external AV Manager's CA certificate (e.g., `rootCA.crt`, if you've followed the procedure from "Replacing the Default Self-Signed Certificate of AV Manager with a CA-signed Certificate," on page 21) to local.

2   Make sure the file is in CRT or PEM format (Base 64-encoded text format).

3   Create a new file (for example, `avCerts.pem`) and copy the contents of the converted file in this file. Make sure this file is readable for "xmp" user.

    If you're adding multiple external AV Managers, please append their certificates in the same file.

4   Set the environment variable `XMP_SSL_CERT_FILE` to the path of the file where App Volumes certificates are copied. This environment variable and the file to which it points should be readable for "xmp" user in the App Volumes OVA/VM.

NOTE   You can't disable SSL certificate validation only for external AV Managers. However, you can disable SSL certificate validation for all external microservices connected by XMP. You can do so by setting

```
XMP_DISABLE_SERVICES_SSL_VALIDATION=1
```

Handling SSL Certificates for vROps

This section covers SSL certificates for vROps.

- "Handling SSL Certificates for vROps (Default Certificate)," on page 22
- "Handling SSL Certificates for vROps (Custom Certificate)," on page 23

Handling SSL Certificates for vROps (Default Certificate)

If you choose not to accept all certificates when setting up vRealize Operations for Published Applications (vROps), and instead are uploading the default certificate, you must export the certificate from the vROps URL.

Follow these steps to upload the default certificate for vROps into App Volumes 3.0:

Procedure

1   Use SSH to log in to vROps.

2   Go to `/storage/vcops/user/conf/ssl/`.

3   Download either the `cacert.pem` or `slice_1_cert.pem` certificate.

4   Log in to App Volumes 3.0 with your AD credential.

5   Click **Settings** in the left-hand menu bar.

6   Click **Locations**.

7   Click **vROps**.

8   Click **Configure**. Configure vROps, providing the hostname or IP address based on the issued certificate.

9   Enter a vROps username and password.

10   Set **Accept All Cert** as **No**.

11   Click **Select** (next to **Upload Cert File**) to upload the certificate that you've downloaded from vROps.

> **NOTE**   It's best to install vROps with a DNS name, and the FQDN of the vROps server should be the DNS name. However, sometimes the vROps installation doesn't have a proper FQDN name; in that case, you need to resolve the FQDN address in the `/etc/hosts` file.

Handling SSL Certificates for vROps (Custom Certificate)

If you choose not to accept all certificates when setting up vRealize Operations for Published Applications (vROps), and instead are uploading a custom certificate, you must export the certificate from the vROps URL.

If you are uploading your own certificate, you must make sure that the certificate has the following characteristics:

■   The certificate should be used as the vROps server.

■   The file must be encoded in PEM format.

■   All certificates in the chain are included.

Follow these steps to upload a custom certificate for vROps into App Volumes 3.0:

Procedure

1   Use SSH to log in to vROps.

2   Go to `/storage/vcops/user/conf/ssl/`.

3   Download the custom certificate to be uploaded for vROps.

4   Log in to App Volumes 3.0 with your AD credential.

5   Click **Settings** in the left-hand menu bar.

6   Click **Locations**.

7   Click **vROps**.

8   Click **Configure**. Configure vROps, providing the hostname or IP address based on the issued certificate.

9   Enter a vROps username and password.

10   Set **Accept All Cert** as **No**.

11   Click **Select** (next to **Upload Cert File**) to upload the certificate that you've downloaded from vROps.

> **NOTE**   It's best to install vROps with a DNS name, and the FQDN of the vROps server should be the DNS name. However, sometimes the vROps installation doesn't have a proper FQDN name; in that case, you need to resolve the FQDN address in the `/etc/hosts` file.

Enable TLSv1.0 Protocol

Some admins who are using the TLSv1.0 protocol may want to enable its use with App Volumes 3.0.

By default, TLSv1.1 and TLSv1.2 are used for communication between App Volumes agent and AV Manager. TLSv1.0 is blocked by the AV Manager. However, if you want to re-enable the use of TLSv1.0, use the following procedure:

Procedure

1   Go to `/etc/nginx`.

2   Open the file `nginx.conf` with an editor.

3   Replace this line

   `ssl_protocols TLSv1.1 TLSv1.2;`

   with this line:

   `ssl_protocols TLSv1.0 TLSv1.1 TLSv1.2;`

4   Save the `nginx.conf` file.

5   Restart the `nginx` service with this command:

   sudo service nginx restart

Installing Agents

5

Use the App Volumes Unified Agent Installer to install the App Volumes agent, as well as optional component agents, on end-user machines.

The App Volumes Unified Agent Installer installs agents used by App Volumes:

■ the App Volumes agent

■ the Customizations agent

■ vRealize Operations for Published Applications (vROps) agent (App Volumes Enterprise only)

You have the choice of either installing using an install wizard (recommended; see "Installing Agents Using the Install Wizard," on page 28) or by entering commands on a command line (see "Installing Agents Using the Command Line," on page 30). In either case, you can perform either

■ a complete installation, in which all agents are automatically installed, or

■ a custom installation, in which you may choose which component agents to install

NOTE Use the App Volumes Unified Agent Installer to install various agents on end user's machines only. Do not use it to install on the same machine running App Volumes or AppCapture.

This chapter includes the following topics:

■ "Agent Volumes Installer Requirements," on page 25

■ "Disable Remote Desktop Session Host Windows Installer RDS Compatibility, If Applicable," on page 26

■ "Installing Agents Using the Install Wizard," on page 28

■ "Installing Agents Using the Command Line," on page 30

■ "Uninstalling," on page 31

■ "Upgrading Agents," on page 34

Agent Volumes Installer Requirements

You must meet the certain requirements in order to use the App Volumes Unified Agent Installer.

App Volumes Unified Agent Installer Requirements

The App Volumes Unified Agent Installer requires Windows 7.0 or higher (including Windows 2008 R2, Windows 2012, and Windows 2012 R2).

Disable Remote Desktop Session Host Windows Installer RDS Compatibility, If Applicable

If Remote Desktop Session Host Windows Installer RDS Compatibility is enabled on Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2, you must disable Remote Desktop Session Host Windows Installer RDS Compatibility before you install the App Volumes Unified Agent Installer.

NOTE RDS Compatibility is enabled by default. Disabling RDS Compatibility on a Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 host is necessary to prevent a Window Installer Coordinator error. See Installation can fail with Window Installer Coordinator Error.

Disable RDS Compatibility for all App Volumes Unified Agent Installer installation-related processes. For example, installation, upgrade, uninstallation, and modification.

If RDS Compatibility is not disabled, an error message appears during an attended installation of App Volumes Unified Agent Installer, instructing you to perform the procedure that follows. Even though no error message appears during a silent installation, you must still perform the procedure that follows to disable RDS Compatibility.

- Attend to this task if you will install App Volumes Unified Agent Installer on a Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 host.

- Ignore this task if you will not install App Volumes Unified Agent Installer on a Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 host.

Procedure

1   Determine if the **Enable** item exists, as in the example paths that follow, in your Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 registry and, if so, set the value to **0**.

If RDS Compatibility is enabled, the **Enable** item is set to 1 in the registry table, as in one of the following locations:

- ```
  HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Terminal
  Services\TSAppSrv\TSMSI\Enable
  ```

■   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\TSAppSrv\TSMSI\Enable

The following substeps serve as an example of how to locate the **Enable** item in the registry table.

a   On the App Volumes host machine, access the Registry Editor.

   For example, click the **Start** button, click **Run**, enter `regedit.exe`, and click **OK**.

b   Attempt to navigate to the TSMSI folder.

   If the TSMSI folder does not exist, skip the remaining substeps and proceed to the next step. As you attempt to navigate to the TSMSI folder, you might find that a folder in the potential paths provided does not exist, which prevents you from navigating farther. In this case, also, skip the remaining substeps and proceed to the next step.

   The following paths are potential paths to the TSMSI folder.

Location of the Enable Item	Description
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Terminal Services\TSAppSrv\TSMSI\Enable	Select **HKEY_LOCAL_MACHINE > Software > Policies > Microsoft > Windows NT > Terminal Services > TSAppSrv > TSMSI**
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\TSAppSrv\TSMSI\Enable	Select **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > Terminal Server > TSAppSrv > TSMSI**

c   If the TSMSI folder exists, after you navigate to it, determine the value of the **Enable** item in the right pane and take the appropriate action as follows.

Value of the Enable Item	Action
The Enable item has a value or (0)	Skip the remaining substeps and proceed to the next step.
The Enable item has a value of (1)	Proceed to the next substep.

d   If the **Enable** in the TSMSI folder has a value of (1), click the **Enable** item.

e   In the Value data text box, change the value to `0`.

f   Click **OK**.

2   Disable RDS Compatibility on the App Volumes host machine.

   The following substeps serve as an example of how to use the Local Group Policy Editor to disable RDS Compatibility.

a   Click the **Start** button, enter `gpedit.msc` in the search box, and press Enter.

   The Local Group Policy Editor dialog box appears.

b   Select **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Application Compatibility**.

c   In the right pane, click **Turn off Windows Installer RDS Compatibility**.

d   In the Turn off Windows Installer RDS Compatibility window, select **Enabled**.

   This action turns off Windows Installer RDS Compatibility.

3   In a terminal window, issue the `gpupdate /force` command to refresh the Group Policy settings.

What to do next

1   Download and install the App Volumes Unified Agent Installer. See the respective task, "Perform a Complete Installation (Wizard)," on page 28, "Perform a Custom Installation (Wizard)," on page 29 or "Perform a Complete Installation (Command Line)," on page 30.

2   If RDS Compatibility is required for your deployment, re-enable it.

The Microsoft limitation affects the installation, not the function, of App Volumes Unified Agent Installer. After installation, you can safely re-enable RDS Compatibility.

Installing Agents Using the Install Wizard

The App Volumes Unified Agent Installer wizard takes you through the steps of both a complete or custom install of App Volumes and related component agents.

If you prefer to install agents using a command line, see "Installing Agents Using the Command Line," on page 30.

Perform a Complete Installation (Wizard)

Use the App Volumes Unified Agent Installer to install the App Volumes agent and all other component agents on a target machine.

Prerequisites

For vRealize Operations for Published Applications (vROps) (App Volumes Enterprise only):

■   If you want to install vROps for Horizon View, please install the Horizon View Agent 5.0 or higher in advance.

■   If you want to install vROps for Citrix, please install the Citrix Virtual Delivery® Agent in advance.

■   You cannot install both vROps for the Horizon View agent and vROps for the Citrix Application Delivery agent.

Procedure

1   Go to the vmware.com downloads page and download the App Volumes Unified Agent Installer to your machine.

2   Navigate to the folder where you downloaded the installer and double-click the installer icon.

The installer wizard starts up.

3   Accept the terms or agreement and click **Next**.

4   Make sure that the **Complete** radio button is checked and click **Next**.

5   Enter the address of your App Volumes deployment (e.g., 123.45.67.89).

6   (optional) Change the port number if desired.

7   Follow the wizard to complete all the installation steps.

8   Restart your machine.

9   (optional) Verify that the agents have been installed. In Windows, bring up a control panel and click **Programs**, then click **Uninstall Programs.**

You will see a list of installed programs; verify that all the agents are listed.

Perform a Custom Installation (Wizard)

You can choose which agents to install with the App Volumes Unified Agent Installer.

Prerequisites

For vRealize Operations for Published Applications (vROps) (App Volumes Enterprise only):

- If you want to install vROps for Horizon View, please install the Horizon View Agent 5.0 or higher in advance.

- If you want to install vROps for Citrix, please install the Citrix Virtual Delivery® Agent in advance.

- You cannot install both vROps for the Horizon View agent and vROps for the Citrix Application Delivery agent.

Procedure

1 Go to the VMware downloads page and download the App Volumes Unified Agent Installer to your machine.

2 Navigate to the folder where you downloaded the installer and double-click the installer icon.

The installer wizard starts up.

3 Accept the terms or agreement and click **Next**.

4 Make sure that the **Custom** radio button is checked and click **Next**.

A screen showing the various available components comes up.

5 Deselect any items you don't want.

a Click the menu arrow next to the item's name.

A menu is displayed.

b Choose the menu item with a red "X" and the words "This feature will not be available."

NOTE In a custom installation, you don't select components to be installed; you select components that you don't want installed. Components are automatically installed unless you deselect them.

The deselected components will not be installed.

6 If you want to install the App Volumes Agent, enter the address of your App Volumes deployment (e.g., 123.45.67.89).

NOTE This step only applies if you want to install the App Volumes Agent.

7 If you want to install the App Volumes Agent, you can optionally change the port number if desired.

NOTE This step only applies if you want to install the App Volumes Agent.

8 Follow the wizard to complete all the installations steps.

9 Restart your machine.

10 (optional) Verify that the agents have been installed. In Windows, bring up a control panel and click **Programs**, then click **Uninstall Programs.**

You will see a list of installed programs; verify that all the agents are listed.

Installing Agents Using the Command Line

From the command line, you can perform complete or custom installations, as well as uninstall agents, view logs, and more.

As an alternative, you can install agents using the installer wizard, rather than by command line. See "Installing Agents Using the Install Wizard," on page 28 for instructions.

Perform a Complete Installation (Command Line)

You can perform a complete installation of all available components with a single command.

Prerequisites

For vRealize Operations for Published Applications (vROps) (App Volumes Enterprise only):

■ If you want to install vROps for Horizon View, please install the Horizon View Agent 5.0 or higher in advance.

■ If you want to install vROps for Citrix, please install the Citrix Virtual Delivery® Agent in advance.

■ You cannot install both vROps for the Horizon View agent and vROps for the Citrix Application Delivery agent.

Procedure

1 If you have not done so, download the App Volumes Unified Agent Installer from the VMware downloads page.

2 In Windows, open up a command console in administrator mode.

3 **cd** to the directory where you downloaded the agent installer. (In most cases this will be your `Downloads` folder.)

4 Run one of the following commands:

`VMware-appvolumes-unifiedagent-x64-3.0.0-<build>.exe [options]` (64-bit)

`VMware-appvolumes-unifiedagent-x86-3.0.0-<build>.exe [options]` (32-bit)

where *<build>* is the current build of the Unified Agent Installer. You can run this command with various options; see "Agent Installer Command-Line Options," on page 31.

5 Wait until the installer has finished.

6 (optional) Verify that the agents have been installed.

a In Windows, open up a Control Panel from the **Start** menu.

b Go to the Programs and Features panel and locate the agents in the list of installed programs.

7 After you've verified that the agents have been installed, restart your machine.

Example: Example Full Install with Options

This example shows a complete install, using the 64-bit version of the command and the following options:

■ silent mode (/S /v/qn)

■ port specification (/V"PORT="80"")

`VMware-appvolumes-unifiedagent-x64-3.0.0-<build>.exe /S /v/qn /V"PORT="80" ADDR="192.168.0.20""`

See "Agent Installer Command-Line Options," on page 31 for all command-line options.

Agent Installer Command-Line Options

The command-line version of the Unified Agent Installer has various options that enable you to specify which agents to install, run in silent mode, and more.

Unified Agent Installer Command-Line Options

NOTE The Unified Agent Installer command line comes in two versions:

- for 64-bit machines: `VMware-appvolumes-unifiedagent-x64-3.0.0-<build>.exe`

- for 32-bit machines: `VMware-appvolumes-unifiedagent-x86-3.0.0-<build>.exe`

where *<build>* is the current build of the Unified Agent Installer. For simplicity, this documentation shows the 64-bit command; substitute the 32-bit command if you are using a 32-bit machine.

The Unified Agent Installer includes the following command-line options to the `VMware-appvolumes-unifiedagent-x64-3.0.0-<build>.exe` command.

Table 5-1. App Volumes Unified Agent Installer Command-Line Options

Task	Option
Perform a complete install of all components	*(none)*
Hide the initialization dialogue	`/S`
Specify which agents to install. The argument can be any of 'AppVolume', 'FlexUEM' (for Customizations), or 'VROPS'	`/V"AddLocal="`*agent1, agent2, agent3*`""`
Specify the address of the App Volumes machine	`/V"ADDR="`*address*`""`
Create a log	`/V"/L*V` *logName*`"`
Specify the port to use	`/V"PORT="`*port*`""`
Use silent mode	`/qn`

The following are examples of using `VMware-appvolumes-unifiedagent-x64-3.0.0-<build>.exe`. Each example is run in Silent Mode, using the `/S` and `/qn` options.

NOTE All examples must all be run in administrator mode.

Set the port and address:

`VMware-appvolumes-unifiedagent-x64-3.0.0-<build>.exe /S /v/qn /V"PORT=80 ADDR="192.168.0.20"""`

Install the App Volumes agent only, and set the port and address:

`VMware-appvolumes-unifiedagent-x64-3.0.0-<build>.exe /S /v/qn /V"AddLocal="AppVolume" PORT=80 ADDR="192.168.0.20"""`

Install Customizations and vROps for Published Apps (vROps) agents only:

`VMware-appvolumes-unifiedagent-x64-3.0.0-<build>.exe /S /v/qn /V"AddLocal="FlexUEM, VROPS"""`

Perform a complete install, and specify a log to print:

`VMware-appvolumes-unifiedagent-x64-3.0.0-<build>.exe /S /v/qn /V"PORT=80 ADDR="192.168.0.20" /L*V log.txt"`

Uninstalling

You can delete installed agents, as well as the agent installer itself.

There are multiple ways to remove either individual agents or the Unified Agent Installer itself.

You can remove:

■ Individual agents (App Volumes agent, Customizations, and /or vROps). See "Uninstalling Individual Agents," on page 32. You can do this from Windows or from the installer wizard.

■ The App Volumes Unified Agent Installer itself. See "Uninstalling the Agent Installer," on page 33. You can do this either from the installer wizard, from Windows, or from a command line.

Uninstalling Individual Agents

This section covers how to uninstall the individual agents (App Volumes, Customizations, and vROps).

You can uninstall individual agents in two ways:

■ from Windows

■ with the Unified Agent Installer wizard

Uninstall Agents from Windows

You can remove installed agents directly from Windows.

Procedure

1 In Windows, choose **Control Panel** from the **Start** menu.

2 Choose the **Programs and Features** control panel.

3 Select an agent you want to remove from the list of programs.

4 Right-click to bring up a menu, and choose **Uninstall**.

5 Repeat with any other agents you want to remove.

Uninstall Agents Using the Wizard

Use the App Volumes Unified Agent Installer to remove one or more installed agents.

Procedure

1 Navigate to the folder containing the App Volumes Unified Agent Installer. (This is often the `Downloads` folder.)

2 Double-click the agent installer.

The App Volumes Unified Agent Installer wizard starts up.

3 In the wizard, go to the Program Maintenance screen.

4 Select the **Modify** radio button and click **Next**.

The **Custom Setup** screen appears.

5 On the **Custom Setup** screen, deselect the agent(s) you want to remove. Then click the **Next** button.

6 Follow the remaining steps in the wizard to finish uninstalling the agents you've deselected.

The agents that are selected will remain. Any agents that you have not selected will be removed.

Uninstalling the Agent Installer

In addition to removing individual agents that you've installed, you can remove the agent installer itself.

There are three ways to uninstall the App Volumes Unified Agent Installer itself:

- from a command line

- from Windows

- from the App Volumes Unified Agent Installer wizard itself

Uninstall the Installer Using Windows

These are the steps to uninstall the App Volumes Unified Agent Installer from Windows.

Procedure

1   In Windows, choose **Control Panel** from the **Start** menu.

2   Choose the **Programs and Features** control panel.

3   Select the App Volumes Unified Agent Installer from the list of programs.

4   Right-click to bring up a menu, and choose **Uninstall**.

Uninstall the Installer Using the Command Line

These are the steps to uninstall the App Volumes Unified Agent Installer from a command line.

Procedure

1   Bring up a command window in administrator mode.

2   Navigate to the directory where the App Volumes Unified Agent Installer is located. For most people, this is their `Downloads` directory.

3   Enter the following command: `MsiExec.exe /x{product code} /qn`

For example, this command removes the agent installer (the numbers inside the brackets are the product code for the agent installer):

`MsiExec.exe /x{39F626B3-5D5D-492F-89D3-4498CE843D71} /qn`

To retrieve a product code:

a   In the Windows **Start** menu, click **Run**.

b   Enter `regedit.exe` to open the registry editor.

c   Go to the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall` folder.

d   Find the item whose Display Name is the App Volumes Unified Agent Installer. The 32-character GUID code is the product code, e.g.:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{11E69C13-F8AA-479F-B1FF-EDB35078440F}`.

4   Verify that the App Volumes Unified Agent Installer is no longer present.

Uninstall the Installer Using the Wizard

These are the steps to uninstall the App Volumes Unified Agent Installer using the agent installer itself.

Procedure

1   Navigate to the folder containing the App Volumes Unified Agent Installer. (This is often the `Downloads` folder.)

2   Double-click the agent installer.

The App Volumes Unified Agent Installer wizard starts up.

3   In the wizard, go to the Program Maintenance screen.

4   Select the **Remove** radio button and click **Next**.

5   Follow the remaining steps in the wizard to finish uninstalling the agent installer.

Upgrading Agents

Use the App Volumes Unified Agent Installer to upgrade agents.

To upgrade an agent, you do not need to uninstall the previously installed agent. The App Volumes Unified Agent Installer automatically deletes the old agent and installs a new one in its place.

Managing Applications for Deployment with AppCapture

<div style="text-align: right; font-size: 2em;">6</div>

Use AppCapture to create AppStacks for provisioning applications to users.

Before you can create an applications assignment (that is, assign applications to users), you must capture and package applications into AppStacks using the AppCapture utility. You then manually copy the AppStacks to a file share.

This chapter includes the following topics:

AppCapture System Requirements

This is a list of AppCapture minimum requirements.

AppCapture System Requirements

To install and run AppCapture, your system must meet the following minimum requirements:

- OS: AppCapture works on all Windows platforms from Windows 7 onward, including Windows 8.1 and Windows 10, for both x86 (32-bit) and 64-bit machines (physical, Workstation or ESX VMs).

- Disk space: The amount of disk space required depends on the number and size of the applications you are provisioning. Ensure that your system has enough disk space for all the AppStacks you are creating.

Install AppCapture

The AppCapture program enables you to bundle applications for copying to a file share.

Prerequisites

You must have administrator privileges to run AppCapture.

Procedure

1 In a browser, go to the VMware downloads page and download the AppCapture installer, `VMware–appvolumes–appcapture–3.0.0–<buildnumber>.exe` (where *<buildnumber>* is the current build of the AppCapture installer), to a copy of the Master VM that does not have the App Volumes agent installed.

> **NOTE** You cannot install AppCapture on a VM where the App Volumes agent is also installed.
>
> You can take a snapshot of the Master VM with the App Volumes agent installed, then either
>
> ■ clone that VM and uninstall the App Volumes agent, or
>
> ■ uninstall and create a second snapshot without the agent installed, allowing AppCapture to be installed
>
> See the VMware vSphere support site or the VMware Workstation support site for more information.

2 Double-click the installer and follow the instructions in the wizard.

3 (optional) Confirm that `AppCapture.exe` is installed in `C:\Program Files (x86)\VMware\AppCapture` (64-bit machines) or `C:\Program Files\VMware\AppCapture` (32-bit machines).

Using AppCapture

Before you can provide applications to users, you need to bundle the applications into AppStacks.

An AppStack is a collection of files, folders, registries, and metadata stored in `.vhd` or `.vmdk` files and accompanied by a `.json` file.

You create AppStacks on your own virtual machine with the AppCapture program. AppCapture is a standalone program; you run it outside of VMware App Volumes 3.0.

You may choose to run AppCapture either from a console command line (see "Run AppCapture from the Command Line," on page 36) or from Microsoft PowerShell® (see "Using AppCapture with Microsoft PowerShell," on page 40).

Using AppCapture with a Command Line

You can create an AppStack by running AppCapture from a command line or with Microsoft PowerShell. This section describes running AppCapture from a command line.

To run AppCapture with Microsoft PowerShell, see "Using AppCapture with Microsoft PowerShell," on page 40.

Run AppCapture from the Command Line

You can run AppCapture from a command line.

> **NOTE** You must capture applications from the same OS into which you mount them. For example, if users are operating a Win7x64 OS, then you must capture the applications using a similar or an identical base OS Win7x64 image.

Prerequisites

You must have administration privileges to run AppCapture.

Procedure

1 If you have not done so already, disable UAC (User Account Control) in Windows. Instructions for turning off UAC may be found at http://windows.microsoft.com/en-us/windows/turn-user-account-control-on-off#1TC=windows-7.

2 Take a snapshot of the system. This will allow you to revert to the snapshot after the capture session.

3   Bring up a console window.

4   If you have not yet done so, confirm that the CLI command `AppCapture.exe` is installed in `C:\Program Files (x86)\VMware\AppCapture` (64-bit machines) or `C:\Program Files\VMware\AppCapture` (32-bit machines).

5   Run the `AppCapture.exe` command: **`AppCapture.exe /n`** *your_appstack_name*

    For other options to the `AppCapture.exe` command, see "AppCapture Command-Line Options," on page 37.

    NOTE   Do not press **Enter** at this point. Run all installers first, and then return to this window.

    The AppStack (virtual machine disk) is ready in generally less than a minute.

6   Leave the console window and run normal Windows installation for each of the applications that you want to capture.

    a   Accept the default installation of all applications to the `C:` drive. The actual installation activity redirects to the virtual output disk.

    b   If an installer requires a reboot, allow the reboot to proceed.

    c   You can also run ThinApp packages (ThinApp msi's), which can be installed in a manner similar to how other application msi packages are installed. Refer to the latest ThinApp documentation on how to create ThinApp msi packages.

        NOTE   This feature is not available on all editions of App Volumes 3.0.

        ---

7   Once all installers that are required to be captured in this AppStack have run, return to the console window and press **Enter** to initiate reboot and complete virtual disk creation.

    After reboot, the console window displays content indicating that new AppStacks containing applications are available.

    Confirm that new `.vhd` and `.vmdk` files are in `C:\ProgramData\VMware\AppCapture\appvhds`.

8   Use the `AppCapture.exe` command to view applications in `.vhd`: **`AppCapture.exe /list`** *my_AppStack_Name.vhd* and in `.vmdk`: **`AppCapture.exe /list`** *my_AppStack_Name.vmdk*

9   Copy the AppStacks you've created to a staging file share of your choice.

10 Revert to the system snapshot that you captured before you started the first capture session.

11 Copy the AppStacks back from the staging file share to your system.

AppCapture Command-Line Options

This section describes options to the `AppCapture.exe` command.

`AppCapture.exe` Command Options

This table lists options for the `AppCapture.exe` command.

The `/meta`, `/vhd`, and `/vmdk` options are useful if you accidentally delete a `.json`, `.vhd`, or `.vmdk` file. Note that if a `.json` file is deleted, App Volumes cannot read the AppStack.

Table 6-1. `AppCapture.exe` Command Options

Task	Option
Display help for the `AppCapture.exe` command.	`/?`
Specify an author's (i.e., creator's) name for the AppStack. If the name contains at least one space, put the name in parentheses. Example: **`AppCapture.exe /n /a (IT Admin)`**	`/a`

Table 6-1. `AppCapture.exe` Command Options (Continued)

Task	Option
Specify a description for an AppStack. If the name contains at least one space, put the name in parentheses. Example: **AppCapture.exe /n /d (finance apps)**	/d
List the contents of the AppStack `.json`, `.vhd`, and `.vmdk` files. Specify the directory where the files are located, if you're not using the default. Example: **AppCapture.exe /list *filePath***	/list
Generate a `.json` file by using a `.vmdk` file as input. Specify the path containing the `.vmdk` file if not the default. Example: **AppCapture.exe /meta *appStackPath*.**	/meta
Create a new AppStack. Example: **AppCapture.exe /n**	/n
Specify an output directory for the AppStack files. The default directory is `C:\ProgramData\VMware\AppCapture\appvhds`. This option may be used with the /s option to create a new AppStack from an existing AppStack. See "Update an AppStack Using a Command Line," on page 39. Example: **AppCapture.exe /s *oldAppStackDir* /o *newAppStackDir***	/o
Specify a source directory for the AppStack files. The default directory is `C:\ProgramData\VMware\AppCapture\appvhds`. Do not use this option if you are installing a new application. This option may be used with the /o option to create a new AppStack from an existing AppStack. See "Update an AppStack Using a Command Line," on page 39. Example: **AppCapture.exe /s *oldAppStackDir* /o *newAppStackDir*** You can also use the /s option with /n to update an old AppStack with a new one. In this example, the existing *oldAppStack.vhd* AppStack is copied as a base AppStack and can be updated as *newAppstackName*: **AppCapture.exe /n *newAppstackName* /s *oldAppStack.vhd* /o *newAppStackDir***	/s
Create a `.vhd` file from a `.vmdk` file. Specify the path containing the `.vhd` file if not the default. Example: **AppCapture.exe /vhd *appStackPath*.vmdk**	/vhd
Generate a `.vmdk` file by using a `.vhd` file as input. Specify the path containing the `.vhd` file if not the default. Example: **AppCapture.exe /vmdk *appStackPath*.vhd.**	/vmdk

Merging AppStacks

You can merge two or more AppStacks from the command line using AppMerge.

Use AppMerge to merge two or more existing AppStacks into one. AppMerge takes as its input `.vhd` files associated with an AppStack.

NOTE The input AppStack files must all be of type `.vhd`. You can create a merged output AppStack of a different type with the /vhd and /vmdk options, described below.

AppMerge has the following syntax:

```
AppMerge.exe /o outputAppStack /s "inputAppStack1file","inputAppStack2file",
"inputAppStack3file",...
```

Example: Creating a Merged AppStack

In this example, we create a new AppStack `.vhd` file, called `MergedAppstack.vhd`, from three existing AppStack files, `Office.vhd`, `Notepad++.vhd`, and `Firefox.vhd`:

`AppMerge.exe /o C:\MergedAppstack.vhd /s "Office.vhd","Notepad++.vhd","Firefox.vhd"`

You can specify both input and output file paths as well as file names. In this case, the three input AppStacks are presumed to be in the default AppStack location, while the output AppStack goes into `C:\`.

Besides the `/o` and `/s` parameters, AppMerge accepts the following options:

- `/df`: delete a specific application bundle. Takes a full path of a file that contains a single GUID in each line as its arguments

- `/dl`: delete a specific application bundle. Takes comma-separated GUIDs as arguments

- `/list`: list the content of the newly created AppStack file

- `/meta`: create a `.json` file from the output AppStack file

- `/vhd`: create a `.vhd` output AppStack file from `.vmdk` AppStack input files

- `/vmdk`: create a `.vmdk` output AppStack file from `.vhd` AppStack input files

See also "AppCapture Command-Line Options," on page 37.

Update an AppStack Using a Command Line

You update an AppStack to add applications, update existing applications, or remove applications from the AppStack.

Prerequisites

Verify that you have:

- Acquired administrator privileges

- Created at least one AppStack

- Disabled User Account Control (UAC) notifications on the provisioning machine. Instructions for turning off UAC may be found at
  http://windows.microsoft.com/en-us/windows/turn-user-account-control-on-off#1TC=windows-7

Procedure

1 Open the command prompt and navigate to the AppCapture folder with either `cd "\Program Files (x86)\VMware\AppCapture"` (64-bit) or `cd "\Program Files (x86)\VMware\AppCapture"` (32-bit).

2 Update an AppStack:

a Run `AppCapture.exe /n appStackName /s sourceAppStackDir`

where *sourceAppStackDir* is the path of the AppStack that you want to update.

This example takes an existing AppStack and updates it into a new update AppStack:

```
AppCapture.exe /n AdminUser2.0 /s
"C:ProgramData\VMware\AppCapture\appvhds\AdminUser1.0" /o C:\NewFolder
```

You can include other command options that are applicable to updating an AppStack (see "AppCapture Command-Line Options," on page 37).

The AppStack is created and stored in the location you specify, or by default in the `appvhds` folder.

b Add applications, updating existing applications, or remove applications from the AppStack.

Task	Action
Add applications or update existing applications	Run the installers for the applications that you want to install or update on the AppStack.
Remove applications (optional)	1 Navigate to **Control Panel > Programs and Features**. 2 Select the applications that you want to remove from the AppStack and complete the uninstall procedure.

3 After you add or remove the applications, navigate to the command prompt and press **Enter**.

4 Press **Enter** to restart the machine and finalize the AppStack update procedure.

The machine restarts.

After the machine restarts, the `.json`, `.vhd`, and `.vmdk` files are created. When the application capture process finishes, the applications are removed from the machine.

Using AppCapture with Microsoft PowerShell

You can use Microsoft PowerShell cmdlets to capture applications, create and update AppStacks, and recreate deleted AppStacks with the AppCapture. You can use the 32-bit or 64-bit PowerShell console to run the AppCapture module.

You can also run AppCapture from the command line, as described in "Run AppCapture from the Command Line," on page 36.

NOTE You must capture applications from the same OS into which you mount them. For example, if users are operating a Win7x64 OS, then you must capture the applications using a similar or an identical base OS Win7x64 image.

Run AppCapture Using PowerShell

These are steps for running AppCapture using Microsoft PowerShell.

Prerequisites

You must run AppCapture as administrator.

Procedure

1 If you have not already done so, disable UAC (User Account Control) in Windows. Instructions for turning off UAC may be found at
http://windows.microsoft.com/en-us/windows/turn-user-account-control-on-off#1TC=windows-7.

2 Take a snapshot of the system. This will allow you to revert to the snapshot after the capture session.

3   Launch a PowerShell console (either 32- or 64-bit).

4   Import the PowerCLI module using the `import-module vmware.appcapture` command.

This imports the AppCapture module.

5   (optional) Run the `get-module` command to see a list of all modules.

You see a list of AppCapture cmdlets. These cmdlets are described in "PowerShell Options and Parameters," on page 41.

6   Run the command `Start-AVAppCapture -Name` *appStackFiile*, where *appStackFile* is the name of the AppStack `.vhd` file to create.

NOTE   IMPORTANT: Do not hit **Enter** yet!

The file *appStackFile*`.vhd` is created.

7   Leave the PowerShell console and install, on this same machine, any applications to be provisioned.

8   Once all of the applications have been installed, re-enter the PowerShell console.

9   Hit **Enter**.

10   If an installation requires you to reboot your machine, do so. You will be returned to the AppCapture console.

When your machine reboots, you should see the locations of the AppStack files (`.json`, `.vhd` and `.vmdk`). By default, these are stored in `C:\ProgramData\VMware\AppCapture\appvhds`.

11   (Optional) Go to that directory and examine the `.json`, `.vhd`, and `.vmdk` files to ensure that the applications have been bundled.

12   Copy the AppStacks you've created to a staging file share of your choice.

13   Revert to the system snapshot that you captured before you started the first capture session.

14   Copy the AppStacks back from the staging file share to your system.

PowerShell Options and Parameters

This section details some of the options available for using AppCapture with Microsoft PowerShell.

AppCapture PowerShell Options and Parameters

Use the `Start-AVAppCapture` to create an AppStack and add applications to it.

Table 6-2. `Start–AVAppCapture` Options

Start–AVAppCapture Parameter	Description
–Author *Author-name*	Specify an author associated with this AppStack.
CommonParameters	Use one or more common parameters. The common parameters are a set of cmdlet parameters implemented by Windows PowerShell. `Start–AVAppCapture` supports these common parameters: ■ Debug ■ ErrorAction ■ ErrorVariable ■ OutBuffer ■ OutVariable ■ PipelineVariable ■ Verbose ■ WarningAction ■ WarningVariable For more information about common parameters, see about_CommonParameters.
–Description *text*	Specify a description for an AppStack. If the description includes a space, type the description inside of parentheses, e.g., **–Description (HR Apps)**
–Destination *output-directory*	Specify an output directory for an AppStack. By default, AppStacks are placed in `C:\ProgramData\VMware\AppCapture\appvhds`.
–Force	Create an output directory if it does not exist. The output directory is specified by the `–Destination` parameter.
–Name *vhd-name*	Specify a name for the application(s) being captured. The output `.vhd` file will be named using the application name specified.
–Novmdk	Specify this option to prevent post-capture VMDK disk creation.
–Path *directory-path*	Specify a path to an AppStack. The AppStack will be used as a template for the current capture. Do not use this option if you are installing a new application.

You can perform several workflows with the AppCapture.

Table 6-3. AppCapture PowerShell Workflows

Workflow	Description
ConvertTo–AVVhdDisk	Generate a `.vhd` file by using the `.vmdk` file as input
ConvertTo–AVVmdkDisk	Generate a `.vmdk` file by using the `.vhd` file as input
Export–AVMetadata	Generate a `.json` file by using a `.vhd` or `.vmdk` file as input
Merge–AVAppDisks	Merge AppStack `.vhd` files into a new AppStack `.vhd`. "Merging AppStacks," on page 38 describes the command-line version, which is similar.
Remove–AVApp	Delete an AppStack from a disk.
Reset–AVConfig	Clear AppCapture configuration information from the machine
Show–AVDiskDetails	List the contents of the `.vhd` file, `.json` file, or `.vmdk` file

Table 6-3. AppCapture PowerShell Workflows (Continued)

Workflow	Description
Start–AVAppCapture	Start the procedure to capture applications
Start–AVAppUpdate	Update an AppStack

The following are examples of workflows.

■ This example begins a new capture session. The output .vhd will be named AdobeSuite.vhd and will be generated at C:\AppCapture; the author will be set to "John" and a description is added:

Start–AVAppCapture –Name AdobeSuite –Author John –Description "This disk contains the AdobeSuite application"

■ ConverTo–AVVhdDisk: This example generates an output .vhd format file, Adobe.vhd, from a source file, Adobe.vmdk. The output file is placed in a different directory from the source file:

ConvertTo–AVVhdDisk –Path "C:\Program Files (x86)\VMware\AppCapture\appvhds\Adobe.vmdk" – Destination "C:\AppCaptures"

■ Export–AVMetadata: This example generates the output metadata file Adobe.json. The file is generated in the same place as Adobe.vhd:

Export–AVMetadata –Path "C:\Program Files (x86)\VMware\AppCapture\appvhds\Adobe.vhd"

■ Merge–AVAppDisks: This example merges all the vhd's under the .\temp and .\appstacks directories and generates a Notepad+Adobe.vhd file in C\temp:

Merge–AVAppDisks –Path .\temp*.vhd .\appstacks*.vhd –Destination c:\temp\Notepad+Adobe.vhd

■ Remove–AVApp: This example deletes both the applications Adobe and Notepad from the input disk Adobe+Notepad.vhd. Each application is identified by its unique Guid:

Remove–AVApp –Path C:\Temp\Adobe+Notepad.vhd –Destination c:\Temp\empty.vhd –Guids "{6e48d26c–6d35–44de–9674 –afa364af48b7},{8b01g60w–3e05–33wq–1274–sfa518vi94i0}"

■ Show–AVDiskDetails: This example displays the details from a .json file. The syntax is exactly the same for .vhd and .vmdk files:

Show–AVDiskDetails –Path "C:\Program Files (x86)\VMware\WEM Capture\appvhds\Adobe.json"

■ Start–AVAppUdate: This example updates the AdobeSuite.vhd with a hotfix. A copy of AdobeSuite.vhd is created and will be named AdobeHotfixUpdate.vhd. All the hotfix installations will be captured into AdobeHotfixUpdate.vhd:

Start–AVAppUpdate –Name AdobeHotfixUpdate –Path "C:\Program Files (x86)\VMware\AppCapture\appvhds\AdobeSuite.vhd"

To get help about available workflows, use the get–help command.

Table 6-4. AppCapture PowerShell Workflow Information and Examples

Command	Description
get–help *WorkFlowName*	View general information for a work flow.
get–help *WorkFlowName* –detailed	View detailed information for a work flow.
get–help *WorkFlowName* –examples	`View an example of a work flow.
get–help *WorkFlowName* –full	View technical information for a work flow .

AppCapture Folders and Files

AppCapture creates a number of files and folders.

AppCapture creates various folders in `C:\ProgramData\VMware\AppCapture\appvhds`.

Table 6-5. AppCapture Folders

Folder	Description
`appvhds`	`.vhd`, `.json`, and `.vdmk` files that are generated when you create an AppStack using AppCapture
`logs`	Log file generated by AppCapture. The log file is named `AppCapture.log` and is located in `C:\ProgramData\VMware\AppCapture\logs`
`modules`	PowerCLI `.dll` files required to perform PowerCLI operations
`plugins`	VMware App Volumes 3.0 plug-ins. Plug-ins convert the AppStack to the correct format for deployment to end users
`templates`	`.vhd` file templates that act as boilerplate `.vhds` on which AppStacks are created

The following files are created by AppCapture in the `appvhds` directory (unless you specify a different directory; see "AppCapture Command-Line Options," on page 37):

Table 6-6. AppCapture Files

File	Description
application`.vhd`	`.vhd` file that holds the application files that are part of the AppStack
application`.vmdk`	VMDK-format Virtual Hard Disk file. This is the format that VMware App Volumes 3.0 natively uses
application`.json`	The `.json` file with information about the applications that are captured in the AppStack

Copy AppStacks to File Shares

After you have created your AppStacks, you must place them in file shares. You will use App Volumes 3.0 to assign the applications in the AppStacks to users.

Procedure

1   Open a file explorer window for *share IP*\sharename

    This is the file share where the AppStacks will go. This file share is the file share that you will configure in the App Volumes 3.0 UI (if you haven't done so already).

2   Copy your AppStack .vmdk and `.json` files into this directory.

    ──────────────────────────────────────

    NOTE   AppCapture produces two types of files:

    ■   .vmdk files for mounting AppStacks on virtual machines

    ■   .vhd files for mounting them on physical machines

    VMware App Volumes 3.0 uses only .vmdk files, though you might use .vhd files to install applications on a physical machine with other VMware products.

    ──────────────────────────────────────

What to do next

After adding AppStacks to file shares, you will need to synchronize the file shares. This is done through App Volumes 3.0 and is covered in "Synchronize File Shares," on page 52.

Configuring App Volumes 3.0

7

Once you have installed VMware App Volumes 3.0 and its related components, you must configure several VMware App Volumes 3.0 features.

It is not necessary to have run AppCapture and the App Volumes Unified Agent Installer before continuing; however, by using these programs first, you will be ready to take advantage of all of the features of VMware App Volumes 3.0.

In most cases, configuration tasks use wizards to guide you.

Once you have configured VMware App Volumes 3.0, you'll be able to start deploying applications, configuring users' environments, and more. (See Chapter 8, "Using App Volumes 3.0," on page 55.)

This chapter includes the following topics:

- "Configure an Active Directory," on page 47
- "Assign Roles and Permissions," on page 48
- "Working with vCenters," on page 49
- "Working with File Shares," on page 50
- "Working with AV Managers," on page 52
- "Configure vROps for Published Apps," on page 53

Configure an Active Directory

The first step, after installation, in configuring and using VMware App Volumes 3.0 is to create an Active Directory (AD).

Prerequisites

You will need to have installed VMware App Volumes 3.0 and its constituent components before creating an Active Directory (AD). (See "Install App Volumes 3.0," on page 17.) In particular, you will need the IP address of VMware App Volumes 3.0.

We recommend that you install both the AppCapture and the App Volumes agent before creating an AD, but it's not necessary.

Procedure

1 In a browser, go to *AV_addr*\horizonadmin, where *AV_addr* is the IP address of your
   VMware App Volumes 3.0 virtual machine. (To find this address in your vSphere, click the vSphere's
   Summary tab.)

   NOTE   The first time you use App Volumes, you do not log in. A login page only appears once you have
   created an AD.

   The VMware App Volumes 3.0 Getting Started page appears, and Active Directory is listed as
   "Incomplete."

2 Click **Configure** in the Active Directory section to configure the AD.

   The Register Active Directory window appears.

3 Enter the following information:

   Table 7-1. Active Directory Basic Information

Field	Action
NETBIOS Name	Enter the name of the Active Directory you want to bind to.
DNS Domain Name	Enter the name of the Domain Name Server.
Protocol	Choose the protocol used by your Active Directory.
Bind Username	Enter the Bind Username from your Active Directory.
Bind Password	Enter the Bind Password for your Bind Username from your AD.

4 (optional) Click the down-arrow next to **Advanced Properties**. (Most users will not have to do this.)

   a   Enter the following advanced information:

   Table 7-2. Active Directory Advanced Information

Field	Action
Port	This field is pre-populated based on the default value for the "Protocol" selected. Manually change the value if desired.
Domain Controller IPs	Enter a value for the Domain Controller/IP.
Context	The field is pre-populated based on 'DNS Domain Name' you entered. Manually change the value if desired.

5 Click **Domain Bind** to finish.

If you have not already provided information on roles and permissions (i.e., if you are using
VMware App Volumes 3.0 for the first time), you are now prompted to provide role and permissions
information, as described in "Assign Roles and Permissions," on page 48.

Assign Roles and Permissions

When you first configure VMware App Volumes 3.0, you must assign at least one super-administrator role.
Additionally, you may at any later time add, delete or configure other roles and permissions.

This task will automatically come up the first time you configure an AD.

Prerequisites

Before assigning any roles and permissions, you must have previously configured an AD, as described in "Configure an Active Directory," on page 47.

Procedure

1   Enter the name of a user group containing the name of a super administrator.

    You only need to enter a partial name. App Volumes will auto-complete and present a list of matching group names. Choose a group from the list.

    The chosen group appears under Selected User Groups.

2   Click **Save** to finish.

What happens next depends on whether you are using App Volumes for the first time.

■   If you're using App Volumes for the first time, you are immediately brought to the App Volumes login page. Enter the name and password you entered in "Configure an Active Directory," on page 47 to be returned to the Getting Started page. The Active Directory and Roles and Permissions steps should appear as "Complete."

■   If you've already configured an AD and set roles and permissions, you're returned to the Getting Started page, and both the Active Directory and Roles and Permissions steps should appear as "Complete."

You can set App Volumes so it doesn't display the Getting Started page upon startup. To do so, shift the slider labeled **Getting Started Preferences / Show at Startup** on the Getting Started page to **No**.

Working with vCenters

You need to configure at least one vCenter.

vCenters allow you to manage multiple ESX hosts.

NOTE   If adding a vCenter is unsuccessful, see "Handling SSL Certificates for vCenters," on page 19.

Configure a vCenter

Follow these steps to add or configure a vCenter.

Prerequisites

You must already have a vCenter to configure.

Procedure

1   Click **Settings** in the left-hand menu bar.

    A submenu appears.

2   Click **Locations** in the submenu.

    The Locations page appears.

3   Click the **vCenter** tab.

    Information for your vCenter (if you already have one) appears.

4   Click the **New** button.

    The New vCenter panel appears.

5   Enter the following information:

Table 7-3. Configuring avCenter

Field	Action
Name	Type a friendly name of the new vCenter to be used within the system.
Hostname	Provide the hostname or IP address of the vCenter.
City Name	(optional) Enter the city where the vCenter is located.
vCenter Username	Enter a vCenter username.
vCenter Password	Enter a vCenter password for that username..
ESX Username	Enter the ESX Username. It is a required field for those that use VMDK AppStacks or other VMware Infrastructure Management. See the note below about ESX passwords.
ESX Password	Enter the ESX Password. It is a required field for those that use VMDK AppStacks or other VMware Infrastructure Management. See the note below about ESX passwords.
AV Managers	Select one or multiple AV Managers you would like this vCenter to pair with.
AppStack Datastore Prefix	Enter prefix or regular expressions for datastores where applications should be hosted from. If not specified, any datastore will be used for saving the appstack.
Writable Datastore Prefix	Enter prefix or regular expressions for datastores where writable volumes will be hosted from.

NOTE   If your vCenter manages multiple ESX hosts, it's important that all of the hosts can be accessed using the password given here; otherwise, you may find that AppStacks may not be available. See "Problem: ESX Hosts Not Accessible," on page 63 for more information.

Working with File Shares

You store AppStacks and customization information on file shares. You can map a vCenter to a file share in order to modify and configure it.

There are two types of file shares:

- An application file share contains the AppStacks that you created with AppCapture and copied to the file share. See "Assigning Applications," on page 55.

- A Customizations file share contains the configuration files for a user's custom experience (e.g., printer setup, disk hiding, and so on). See "Customizing the User's Capabilities," on page 58.

Some things to note about file shares:

- You can map multiple vCenters to a single file share. (This is known as AppScaling with Multizones.) VMware App Volumes 3.0 automatically ensures that the AppStacks in that file share are available to all mapped vCenters.

- File shares must be in the same domain as the Active Directory that is added to App Volumes.

- App Volumes must have read permissions on your file shares.

NOTE   Do not delete a file share that has applications on it, as doing so will make those applications unavailable for future assignment.

Configure Application File Shares

An application file share contains AppStacks that you created (with AppCapture) and copied there.

These steps show how to configure a new application file share. The steps are essentially the same to edit an existing file share.

Procedure

1   Click **Settings** in the left-hand menu bar.

    A submenu appears.

2   Click **Locations** in the submenu.

    The Locations page appears.

3   Click the **File Share** tab.

    Information for your file share (if you already have one) appears.

4   Click the **New** button. (Or the **Edit** button if you're editing an existing file share.)

    The New File Share panel appears.

5   Enter the following information:

Table 7-4. Application File Share Configuration

Field	Action
Name	Type a friendly name of the new file share to be used within the system.
Type	Choose **Applications** from the menu.
Source Path	Type the path of the host system to retrieve information from.
Destination vCenters:	Select one or multiple vCenters you would like Apps found on this File share to be copied to. We recommend using all vCenters.

Configure Customizations File Shares

Follow these instructions to create or modify a Customizations file share.

Procedure

1   Click **Settings** in the left-hand menu bar.

    A submenu appears.

2   Click **Locations** in the submenu.

    The Locations page appears.

3   Click the **File Share** tab.

    Information for your file share (if you already have one) appears.

4   Click the **New** button. (Or the **Edit** button if you're editing an existing file share.)

    The New File Share panel appears.

5   Enter the following information:

Table 7-5. Customizations File Share Configuration

Field	Action
Name	Type a friendly name of the new file share to be used within the system.
Type	Choose **Customization** from the menu.
Source Path	Type the path of the host system to retrieve information from.

Synchronize File Shares

File share synchronization occurs automatically at regular intervals. However, any time you add applications or Customizations to a file share, you should synchronize the file share in the App VolumesApp Volumes 3.0 console.

Procedure

1   Log in to the App Volumes 3.0 console, if you're not already logged in.

2   Go to **Settings > Locations**.

3   Click **File Share**.

4   Select the checkbox for the file share you want to sync.

You can only sync one file share at a time.

5   Click **...** and select **Sync Now**.

6   (optional) Check the sync by viewing your inventory. (See "Working with Inventory," on page 61.)

Working with AV Managers

You can add, delete, or edit connections to additional (non-default) App Volumes Managers.

App Volumes Manager (also known as AV Manager) is a VMware App Volumes 3.0 component that consists of services that orchestrate application delivery.

The installation OVA for VMware App Volumes 3.0 includes a default AV Manager.

NOTE VMware discourages using AV Manager directly, as App Volumes 3.0 enables you to perform almost all of the activities of AV Manager from the App Volumes UI, and using AV Manager directly may cause database corruption. Some expert users who have extensive experience with previous versions of App Volumes may choose to use AV Manager directly; those users should refer to "Expert: Modifying Writable Volumes," on page 57. However, most users need do nothing more than add or delete connections to AV Managers.

Add or Edit an AV Manager Connection

Use VMware App Volumes 3.0 to add, edit or delete AV Managers.

VMware App Volumes 3.0 comes with a default AV Manager. You can only add an AV Manager that is already part of the OVA you have downloaded.

NOTE   App Volumes 3.0 takes care of most of the tasks handled by AV Manager, so you should only need to add, delete, or edit a connection to an AV Manager. Using AV Manager directly may cause extensive database corruption. (Experienced, expert admins may choose to use AV Manager for configuration; see "Expert: Modifying Writable Volumes," on page 57.)

These steps are for editing an existing AV Manager; the steps for adding an AV Manager are the same, except that you don't select an existing AV Manager, and you click **New** instead of **Edit**.

Procedure

1   Click **Settings** in the left-hand menu bar.

A submenu appears.

2   Click **Locations** in the submenu.

The Locations page appears.

3   Click the **AV Manager** tab.

Information for your existing AV Manager(s) appears.

4   Select an AV Manager.

5   Click the **Edit** button.

The Edit AV Manager window appears.

6   Enter the following information:

Table 7-6. Adding or Edition an AV Manager

Field	Action
Name	Type a friendly name of the new AV Manager to be used within the system.
Path	Enter the URL for the App Volumes Manager.
Destination vCenters	Select one or multiple vCenters you would like this AV Manager to communicate with.

If adding an AV Manager is unsuccessful, see "Handling SSL Certificates for External App Volumes Managers," on page 21.

Configure vROps for Published Apps

Configure vRealize Operations for Published Applications (vROps) in order to take advantage of App Volumes's monitoring capabilities.

NOTE   vROps is only available with App Volumes Enterprise.

Installing or using vROps is optional.

Prerequisites

- Customers must have an installed and running vRealize Operations for Published Applications instance. See the vRealize Operations for Published Applications documentation for information on installing vROps.

- Customers must also have the vROps agent installed. See Chapter 5, "Installing Agents," on page 25 for information about installing agents.

Procedure

1 Click **Settings** in the left-hand menu bar.

   A submenu appears.

2 Click **Locations** in the submenu.

   The Locations page appears.

3 Click the **vROps** tab.

   Information for your vROps configuration (if you already have one) appears.

4 Click the **Configure** button.

   The Configure vROps panel appears.

5 Enter the following properties:

Table 7-7. vROps Properties

Field	Action
URL	Enter the location for the vROps center.
Username	Enter the username for the vROps center.
Password	Enter the password for the username.
Accept All Cert	Change this choice to **No** to upload your own certificate, rather than accept all certificates. You're then prompted to upload a cert file. See "Handling SSL Certificates for vROps," on page 22 for cert file requirements.
Upload Cert File	This field only appears if you're not accepting all certificates. Click **Select** to browse to the location of a certificate file to upload.

If configuring vROps is unsuccessful, see "Handling SSL Certificates for vROps," on page 22.

Using App Volumes 3.0 8

Once you have done the initial configurations for VMware App Volumes 3.0, you are ready to start deploying applications to users (via AppStacks) and to configure users' environments.

Before performing any of the basic tasks of VMware App Volumes 3.0, such as deploying applications, configuring environments, modifying inventory, or monitoring application usage, you should have performed these basic, initial configuration tasks:

- configure vCenters (see "Working with vCenters," on page 49)

- set up and/or configure one or more file shares for applications and customizations (see "Working with File Shares," on page 50)

- configure AV Managers (see "Working with AV Managers," on page 52)

- Register a vROps locale (see "Configure vROps for Published Apps," on page 53)

This chapter includes the following topics:

- "Assigning Applications," on page 55

- "Customizing the User's Capabilities," on page 58

- "Working with Inventory," on page 61

- "Monitoring Application Deployment and Usage," on page 62

Assigning Applications

Assigning applications to user is the main purpose of App Volumes.

Once you have created AppStacks and configured App Volumes, you're ready to start deploying applications.

Assign Applications

App Volumes 3.0 walks you through assigning applications to users.

These instructions are for creating a new application service. The instructions for editing an existing application assignment are nearly the same. (To edit an existing application assignment, check the box next to its name and choose **Edit**.)

Procedure

1   Bring up the Assignments page. You can do this in either of the following ways:

   a   From the Getting Started page, click **Go** in the **Create New App Assignment** section.

   b   Click **Assign** in the menu bar on the left.

   The Assignments page loads.

2   Click **New**.

   The New Assignment panel appears.

3   Click **Get Started!** under **Applications**.

   The New Applications Assignment screen appears

4   Enter the following information:

   Table 8-1. Application Assignment Definition

Field	Action
Assignment Name	Type a friendly name for this assignment.
OS	Select the target OS from the drop-down menu.
Computer Name Prefix	If you want to limit the assignment to a specific machine grouping, type a prefix for a desktop pool; e.g., "Win7."
Writable Volume	Set this to **Yes** if this user or users has an associated writable volume. See "Writable Volumes," on page 57 for more on writable volumes.

5   Click **Next** to move to the next screen.

   The Applications screen displays a list of available applications to assign.

6   (optional) Enter text in the **Filter** box to display only matching applications. For example, enter "Adobe" to display only Adobe applications (e.g., Adobe Photoshop$^®$ and Adobe Illustrator$^®$ but not Microsoft Word$^®$.

7   Select one or more applications to assign by checking the box next to the application's name.

8   Click the **Next** button.

   The Users screen appears.

9   Enter the name of a user or group in the **Users/User Groups** box. App Volumes 3.0 attempts to auto-complete the name after you type in the first few characters.

   Matching names of users and groups appear in a list. Select the one(s) you want. The new user or group is added to the list of selected users and groups.

10   Click **Next**.

   The Summary screen appears.

11   Review your choices. If you need to make any changes, click the **Back** button. If you're satisfied with your setup, click the **Submit** button. You're returned to the Assignments screen.

The applications you've selected are assigned to the users (and the users in the groups) you've designated.

Clicking on the name of an assignment on the Assignments screen takes you to a summary page for that assignment.

Writable Volumes

Writable volumes enable you to maintain users' data, settings, and profiles persistently between their login sessions.

A writable volume is an optional read/write volume for storing persistent, user-specific information between sessions. Writable volumes can be used to store the following:

■ User-installed applications and application settings

■ User data files

Users can have more than one writable volume assigned to them. However, a user can attach only one writable volume per VM.

App Volumes 3.0 handles most implementation details for writable volumes. In most cases you only need to add or delete a writable volume for a user; you will not need to modify writable volumes directly.

NOTE To prevent problems with writable volumes, do not on-board all users at once; instead, stagger their on-boarding. (See also "App Volumes Best Practices," on page 12.)

Add or Delete a Writable Volume

You can add or delete a writable volume at any time.

You have the option of adding a writable volume when you create an application assignment. (See "Assign Applications," on page 55.) You can also add or delete a writable volume by editing the assignment.

Procedure

1 In App Volumes 3.0, click **Assign** in the menu bar on the left.

2 Select the application assignment you want to modify and click the **Edit** button.

3 Switch the slider to **Yes** to add a writable volume, or **No** to delete one.

4 Continue through the wizard until the Summary page and click **Submit**.

  App Volumes 3.0 adds or deletes the writable volume and adds the user's data to it.

Expert: Modifying Writable Volumes

Most users do not need to modify writable volumes; however, for expert users, it is possible.

App Volumes 3.0 handles most implementation details about writable volumes, so in most cases you need never do more than add or delete a writable volume for an application assignment.

NOTE VMware discourages modifying writable volumes. Only admins with advanced experience using previous versions of App Volumes should attempt to modify writable volumes.

However, expert admins may want to modify a writable volume; typically, this means either expanding it or erasing it from a host. In these cases, you may do the following:

Procedure

1 In App Volumes 3.0, click **Settings** in the menu bar on the left.

2 Choose **Locations** from the submenu that appears.

3 Click the **AV Manager** tab.

4 Note the location (URL) of the AV Manager with the writable volume.

5 Log out of App Volumes 3.0.

6   Open a browser and go to the AV Manager.

7   Use the same credentials (username and password) as for App Volumes 3.0.

8   Please refer to the documentation for previous versions of App Volumes for information on how to modify writable volumes.

> NOTE   Do not modify information on any screen other than the Volumes/Writable Volumes screen.

Customizing the User's Capabilities

You can set various parameters of the user's experience, such as printer access and environment variables.

You can customize your users' environments. For example, you can set which tasks should be performed when they log on, or which drives they have access to.

> NOTE   For VMware App Volumes 3.0, Customizations are a Beta feature. When creating or editing configurations for production implementations, use the standalone UEM® console (not the App Volumes console) and a separate file share. Customizations created, edited, and assigned using the VMware App Volumes 3.0 console are intended only for non-production environments.
>
> Additionally, Customizations created with one console should not be edited with another; i.e., do not create a Customization with the standalone UEM console and edit it with the VMware App Volumes 3.0 console, or vice-versa.

Create or Edit a Customization

You can create, edit, and delete Customizations.

The instructions for creating a Customization and editing an existing Customization are virtually the same. These steps are for creating a new Customization.

Procedure

1   In App Volumes 3.0, click **Inventory** in the menu bar on the left.

    Two submenus, labeled **Applications** and **Customizations**, appear.

2   Click **Customizations**.

    The Customizations inventory page appears.

3   Click **New**. (Click **Edit** if you're editing an existing Customization.)

    The New Customization screen appears.

4   Enter a name for the new Customization.

5   Choose a type of Customization. You have the following choices:

Table 8-2. VMware App Volumes 3.0 Customizations

Customization	Description
Drive mappings	Map drives on the user's computer to remote drives
Environment variables	Set environment variables; e.g., PATH for a search path for applications
File type associations	Set which applications should be associated with specific file extensions; e.g., Word® for .docx files
Hidden drives	Set which drives (e.g., C:\) are hidden on the user's computer
Logon tasks	Set commands to be run when the user logs on
Logoff tasks	Set commands to be run when the user logs off

Table 8-2. VMware App Volumes 3.0 Customizations (Continued)

Customization	Description
Printer mappings	Map a printer, set a default printer, etc.
Shortcuts	Set shortcuts to specific programs; e.g., place a shortcut icon for Word on the user's desktop
Triggered tasks	Map certain actions to specific events; e.g., display a message when a user locks the workstation

When you select a Customization type, the Settings panel changes to present choices associated with that type of Customization.

6   (optional) Enter a description of the Customization.

7   Enter Settings information for that Customization.

8   Click **Save**.

   The new Customization appears in the Customizations inventory page.

What to do next

Now that you've created a Customization, you can assign it. See "Assign a Customization," on page 59.

Assign a Customization

Once you've created Customizations, you can assign them to users.

These instructions are for creating a new Customizations assignment. The instructions for editing an existing Customizations assignment are nearly the same. (To edit an existing Customization assignment, check the box next to its name and choose **Edit**.)

Prerequisites

You must have created at least one Customization before you can assign Customizations to users. See "Create or Edit a Customization," on page 58 to see how to create, edit, or delete Customizations.

Procedure

1   Bring up a New Customizations screen. You can do this in either of the following ways:

   a   From the Getting Started page, click **New** in the **Create a New Customizations Assignment** section.

   b   Click **Assign** in the menu bar on the left, and then click the **New** button. Then click **Get Started!** under **Customization**.

   The New Customization Assignment page loads.

2   Enter the following information:

   Table 8-3. Customizations Definition

Field	Action
Name	Enter a name for the Customizations assignment.
Description	(optional) Describe (for yourself and other admins) what this Customization assignment is for.

3   Click **Next** to move to the next screen.

   The Customizations screen displays a list of available Customizations to assign.

4   (optional) Enter text in the **Filter** box to display only matching customizations.

5 Select one or more Customizations to assign by checking the box next to the Customization's name.

6 Click the **Next** button.

The Conditions screen appears. By assigning conditions to a Customization, you can ensure that the Customization is only applied under certain circumstances. For example, you might want to set certain login tasks if the user's machine is running on a battery.

7 Select a condition from the drop-down menu.

Table 8-4. Customizations Conditions

Condition	Description
command	Runs the specified command, and compares the exit code with the specified value.
	The command should not display any UI, as there is no way for the user to interact with it.
	If no timeout is specified, the UEM agent will wait indefinitely for the command to finish. If the command never finishes, the UEM agent hangs.
	If no timeout is specified, the UEM agent will wait indefinitely for the command to finish. If the command never finishes, the UEM agent hangs.
computer battery	Checks whether the computer has a battery, or is running on a battery.
computer group	Checks if the computer or the user is a member of the specified group.
computer organization unit	Checks if the computer or user is a (direct or indirect) member of the specified organizational unit.
environment variable	Checks whether the specified environment variable matches the specified criterion. The comparison is case insensitive.
file or folder path	Checks if the specified file or folder exists. The specified path can be a directory or file name, and the last component of the path can contain wildcards. The path can contain environment variables.
file version check	Checks the file version of the specified file. This will typically be a .EXE file, but any file with a version resource can be used. The file name can contain environment variables.
IP address	Checks if one of the network adapters has an IP address in the specified range.
	Empty octets at the start of the range are interpreted as 0; at the end, 255.
OS architecture	Checks the architecture (32-bit or 64-bit) of the operating system the UEM agent is running on.
OS version	Checks the Windows version of the system the UEM agent is running on.
product version check	Checks the product version of the specified file. This will typically be a .EXE file, but any file with a version resource can be used. The file name can contain environment variables.
registry key	Checks if the specified registry key exists in the selected registry hive.
registry key value	Checks if the specified registry value matches the specified criterion.

Table 8-4. Customizations Conditions (Continued)

Condition	Description
terminal server client name	Checks if the endpoint name matches the specified criterion.
terminal server IP address	Checks if the endpoint IP address is in the specified range.
	Empty octets at the start of the range are interpreted as 0; at the end, 255.

Most of the conditions will have comparison operators associated with them. For example, the Command condition allows you to search on an exit code that is equal to, greater than, less than, and so forth, a given value.

8 Click the **Next** button.

The User Groups screen appears.

9 Enter the name of a group in the **User Groups** box. App Volumes 3.0 displays a drop-down list of groups matching the first few characters you type.

Matching names of users and groups appear in a list. Select the one(s) you want. The new group is added to the list of selected users and groups.

10 Click **Next**.

The Summary screen appears.

11 Review your choices. If you need to make any changes, click the **Back** button. If you're satisfied with your setup, click the **Submit** button.

The Customizations you've selected are assigned to the groups you've designated. The Customizations are assigned to users who both

■ match the conditions that are configured (if any)

■ are a member of any of the user groups that are configured (if any)

Clicking on the name of a Customization assignment on the Assignments screen takes you to a summary page for that assignment and displays which Customizations that assignment uses.

Working with Inventory

You can see lists of applications and Customizations available for deployment to users.

Inventory lists can provide information about the status of applications and Customizations; for example, you can see what OS an application runs on, or how many assignments it has. You can also create, edit, and delete Customizations (but not applications) from an inventory page.

Check Inventory

Inventory pages display information about available applications and Customizations.

Procedure

1 In the App Volumes 3.0 UI, click **Inventory** in the menu bar on the left.

A submenu with **Applications** and **Customizations** appears.

2 Click the inventory item (applications or Customizations) that interests you.

You can create, delete, or edit Customizations (but not applications) from an inventory page.

A list of available applications or Customizations appears.

Monitoring Application Deployment and Usage

You can monitor application deployment, data center activity, and more from the **Monitor** screen.

NOTE   Monitoring is only available after you have installed vRealize Operations for Published Applications (vROps) and the vROps agent. (See Chapter 5, "Installing Agents," on page 25 for information on installing the vROps agent.) This feature is available in the App Volumes Enterprise edition.

Monitor with the Dashboard

Use the dashboard to keep track of applications, policies, data centers, etc.

Prerequisites

You must be using App Volumes Enterprise with vROps installed to use monitoring.

Procedure

1   In the App Volumes 3.0 UI, click **Monitor** in the menu bar on the left.

The **Dashboard** submenu appears.

2   Click **Dashboard**.

The Dashboard screen appears, displaying information about data centers, assignments, policies, and more.

Dashboard Metrics

The Dashboard offers up a rich set of activity metrics: overview metrics and data center metrics.

Overview Metrics

The Overview panel displays information about application assignments, policies, and more.

Data Center Metrics

The Data Center panel displays information about data centers, including a map of data centers configured in vRealize Operations for Published Applications (vROps).

Troubleshooting App Volumes 3.0

9

This section contains solutions and workarounds for certain problems associated with App Volumes.

Be sure to check the VMware App Volumes 3.0 Release Notes for information about known issues. Also, check "App Volumes Best Practices," on page 12 for preventing common problems.

This chapter includes the following topics:

- "Problem: ESX Hosts Not Accessible," on page 63
- "Enabling and Disabling SSL, SSH, and the OVA Firewall," on page 65
- "Viewing App Volumes Logs," on page 65

Problem: ESX Hosts Not Accessible

This section describes how to make sure that all ESX hosts, and their AppStacks, are accessible.

Problem

After creating AppStacks and configuring a vCenter in App Volumes 3.0, you find that the AppStacks are not available from the ESX hosts associated with the vCenter, preventing you from deploying their applications to users.

Cause

A single vCenter may manage multiple ESX hosts. However, App Volumes only lets you set a single ESX username/password combination for all its associated hosts, and a vCenter can't pass down AppStacks to any host that has a different username/password from the one set in App Volumes. This means that App Volumes will not find and access AppStacks (and thus the applications in those AppStacks) on those hosts.

In particular, if you have set up your ESX hosts to rotate passwords, the passwords will get out of sync with those configured in App Volumes.

To work around this problem, make sure that all the ESX hosts for a given vCenter have the same username/password combination.

Solution

1 Datastore browsing needs to be enabled (this is enabled by default) for the App Volumes Manager to enumerate volumes on the datastore. Check the value of *enableHttpDatastoreAccess* in the file `C:\ProgramData\VMware\VMware VirtualCenter\vpxd.cfg` on the vCenter. If it is set to false, change it to true and restart the vCenter Server service.

2 On each ESX host, create a new role (for example "AV3") and assign it a password. The new username and password must be the same on all hosts.

3   Assign the new role the following permissions:

- Datastore
    - Allocate space
    - Browse datastore
    - Low-level file operations
    - Remove file
    - Update virtual machine files
- Folder
    - Create folder
    - Delete folder
- Global
    - Cancel task
- Host
    - Local operations
        - Reconfigure virtual machine
- Sessions
    - View and stop sessions
- Tasks
    - Create task
- Virtual machine
    - Configuration
        - Add existing disk
        - Add new disk
        - Add or remove device
        - Change resource
        - Remove disk
        - Settings
        - Advanced
- Inventory
    - Create new
    - Move
    - Register
    - Remove
    - Unregister
- Provisioning
    - Promote disks

4   Restart each ESX machine after setting up the new role.

5   In App Volumes 3.0, configure the vCenter for these ESX hosts to use the same username and password that you set up on the hosts. See "Configure a vCenter," on page 49 for more information.

Enabling and Disabling SSL, SSH, and the OVA Firewall

By default, SSL Certificate Validation is enabled for XMP and microservices external communication in the OVA; for example, with vROps, vCenters, and external AV Managers.

Problem

You may need to disable (or re-enable) SSL Certificate Validation; additionally, you may want to enable or disable the OVA firewall and the ability to SSH in to the OVA.

Solution

◆   Use the following scripts in `/etc/wemi/utils` to enable or disable SSL, SSH, and the OVA firewall:

- `enable_ssl_validation.sh`

- `disable_ssl_validation.sh`

- `enable_ssh.sh`

- `disable_ssh.sh`

- `enable_firewall.sh`

- `disable_firewall.sh`

What to do next

See "SSL Certificate Validation," on page 19.

Viewing App Volumes Logs

Information about component versions and installs is available from various App Volumes logs.

Solution

For convenience's sake, these instructions show two different ways of accessing the OVA. They are equivalent; use whichever one you prefer.

Procedure

Table 9-1. Viewing App Volumes Logs

Task	Procedure
To find the version of the App Volumes console, XMP, and App Volumes Manager:	For XMP and AV Manager: 1 Bring up a vSphere client. 2 Click the **Console** tab to bring up a console of the OVA. 3 Enter one of the following: ■ `dpkg –l xmp` (XMP) ■ `dpkg –l av–manager` (AV Manager) For the App Volumes console version, go to the following URL in a browser: `https://<IP_addr_of VM>/horizonadmin/build.json`
To view XMP/OVA logs:	1 If logging in with SSH is not enabled, enable it (see "Enabling and Disabling SSL, SSH, and the OVA Firewall," on page 65). 2 Log in to the VM using SSH: 3 `ssh root@<IP_address_of_VM>` 4 Enter the root password. For more information, see "Logging into the OVA," on page 18. 5 `cd /var/log` 6 View logs.
To view App Volumes Manager logs:	Log into `https://<IP_addr_of_VM>:3443/log`

Index