VMware App Volumes User Guide

VMware App Volumes 2.12.1

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.

EN-002150-00

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

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book

The *VMware App Volumes User Guide* provides information on how to install, deploy, configure, and upgrade VMware App Volumes®. App Volumes is a real-time application delivery system that enterprises can use to dynamically deliver and manage applications.

This guide also provides information on volume creation and storage, manage infrastructure using App Volumes Manager, and create, manage, and deploy AppStacks.

Intended Audience

This information is intended for VMware App Volumes administrators, virtual infrastructure administrators, and operations engineers who track and maintain the App Volumes infrastructure.

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.

1 Introduction to VMware App Volumes

VMware App Volumes provides a system to deliver applications to desktops through virtual disks. Applications are bundled in AppStacks and delivered by attaching a standard VMDK file to a virtual machine. You can centrally manage the applications with the App Volumes Manager and there is no need to modify the desktops or individual applications. Applications delivered using App Volumes look and feel natively installed and you can update or replace the applications in real time.

All applications are provisioned during login time and App Volumes users have a persistent user experience wherein they can install their own applications and have them persist across sessions.

A typical App Volumes environment consists of a few key components that interact with each other and an external infrastructure.

Table 1-1. App Volumes Components

Component	Description
App Volumes Administrator	Active Directory (AD) or organizational unit (OU) account. User must have local administrator privileges.
App Volumes Manager	Web-based interface integrated with Active Directory (AD) and vSphere. Consists of services that orchestrate application delivery and interface the vSphere environment. You can use App Volumes Manager for the following tasks: ■ Manage assignments of volumes to users, groups, and target computers. ■ Collect AppStacks and Writable Volumes usage information. ■ Maintain a history of administrative actions. ■ Automate assignment of applications and Writable Volumes for agents during desktop startup and user login. See "Install App Volumes Manager," on page 18 and Chapter 4, "Configuring App Volumes Manager," on page 23.
App Volumes database	A Microsoft SQL or SQL Server Express database that contains configuration information for AppStacks, Writable Volumes, and users. See "Software Requirements," on page 13.
App Volumes agent	Software installed on all Windows desktops where AppStacks and Writable Volumes are assigned. See "Install App Volumes Agent," on page 19.

Table 1-1. App Volumes Components (Continued)

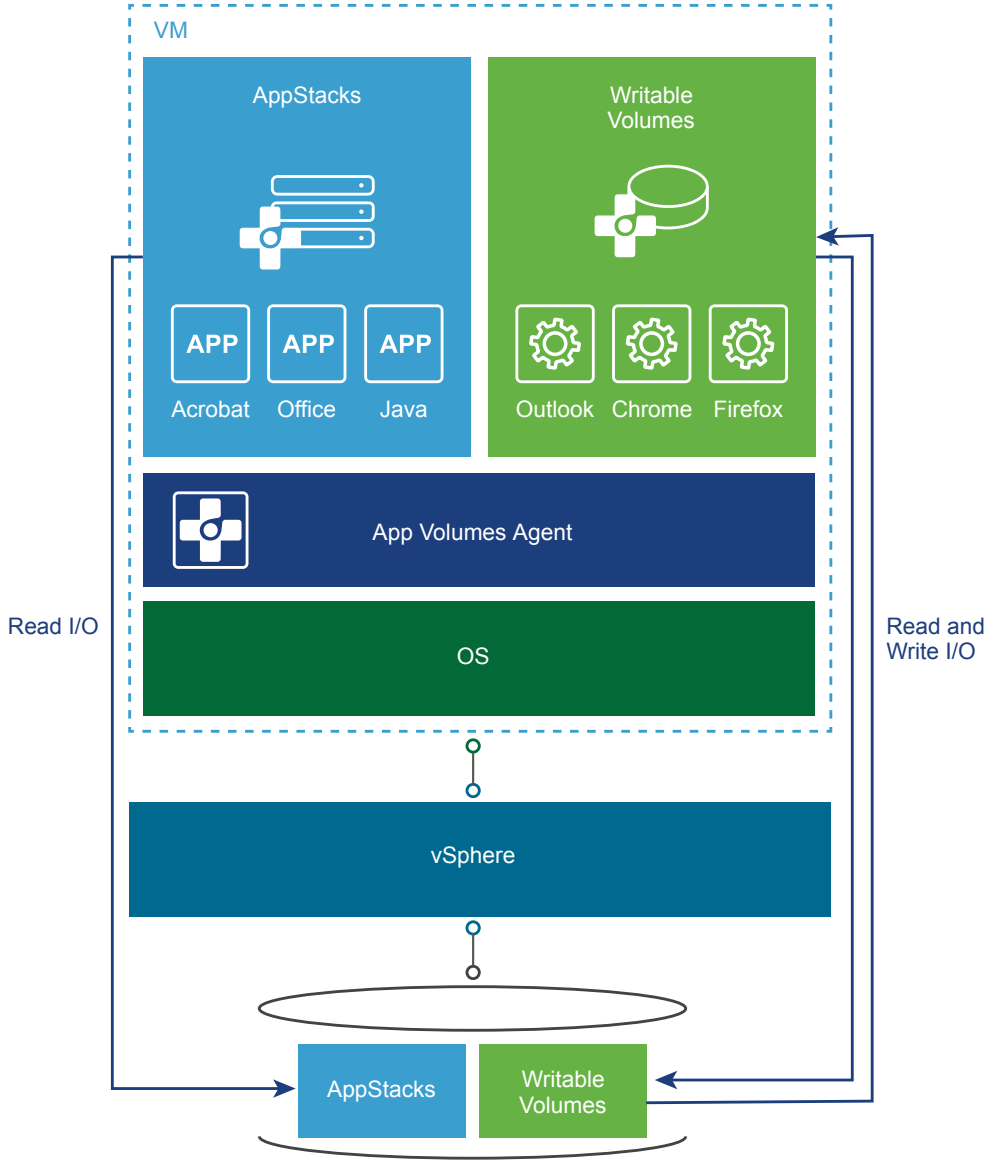
Component	Description
AppStacks	This is a read-only volume containing one or more Windows applications. Once provisioned, an individual AppStack or multiple AppStacks can be mapped to a user, a group of users, or computers at login, or in real-time and to computers only at the time of startup. See Chapter 6, "Working with AppStacks," on page 41.
Writable Volume	Read and write volume for persisting user-specific information between sessions. You can use Writable Volumes to store the following data: ■ User installed applications and application settings ■ Application licensing information ■ User and computer profile ■ Data files **Note** Users can have more than one Writable Volume assigned to them. For details about using Writable Volumes and restrictions, see Chapter 7, "Working with Writable Volumes," on page 49.
Provisioning Desktop	A clean virtual machine that contains the necessary applications for installation into AppStacks. The desktop must have the App Volumes agent installed and configured to connect to the App Volumes Manager. See "Provisioning and Assigning AppStacks," on page 41 and "Best Practices for Provisioning Virtual Machines and Applications," on page 42.
VMware vCenter Server	App Volumes uses vCenter Server to connect to resources within the vSphere environment. See "Configuring a Machine Manager," on page 26.

This chapter includes the following topics:

App Volumes Architecture

App Volumes installs an additional virtualization layer on top of the guest operating system which detaches the application, user settings, and user data layers from the virtual machine (VM). As a result, applications, user settings, and user data become independent from the VM and can be moved across data centers and shared with other VMs.

Figure 1-1. App Volumes Architecture



In a traditional vSphere deployment, a VM consists of a guest OS, applications, user settings, and user data all in a single VMDK file. A copy of the VMDK file is created on the vSphere datastore for every user of a VM. You cannot manage applications, user settings, and user data independently of the VM.

App Volumes detaches the guest OS from the applications, user settings, and user data by installing the App Volumes agent on top of the guest OS. With App Volumes, you deliver applications and user settings through two types of containers, AppStacks and Writable Volumes. AppStacks and Writable Volumes are VMDK files that reside on top of the App Volumes agent. Unlike the traditional VM architecture, only one copy of each AppStack and Writable Volume exists on the vSphere datastore. You can manage AppStacks and App Volumes independently of the VM.

AppStacks

AppStacks are read-only containers that you can use to deliver applications to your users. You can create multiple AppStacks and provision them with different sets of applications depending on the needs of your users. For example, you can create one AppStack with development tools and another one with core applications such as Microsoft Office.

You assign AppStacks to Active Directory user or computers accounts, groups or OUs . When a user logs in to a VM, the AppStack is attached to that VM and the applications on the AppStack become available to the user.

You can change or update the applications in every AppStack individually and deliver the new version of the AppStack to your users.

For information about how to create and manage AppStacks, see Chapter 6, "Working with AppStacks," on page 41.

Writable Volumes

Writable Volumes are read-write containers that you can use to enable your users to install their own applications and to store their settings. Writable Volumes can migrate with their users across different computers and systems. One user can use only one Writable Volume at a time.

For more information about Writable Volumes, see Chapter 7, "Working with Writable Volumes," on page 49.

Suggested App Volumes Workflow

After installing App Volumes, you must perform certain tasks before you can deploy and manage applications.

1. Install the App Volumes Manager. See "Install App Volumes Manager," on page 18.
2. Configure the Active Directory. See "Register an Active Directory Domain," on page 25.
3. Configure SSL and SSL certificates. See Chapter 5, "Using SSL Certificates with App Volumes Manager," on page 33.
4. Select the Active Directory group responsible for administering the App Volumes Manager. See "Add Administrators," on page 26.
5. Set up the operation mode. See "Set Up the Machine Manager Connection," on page 27.
6. Select datastores and paths to store AppStacks and writable volumes. See "Configure Storage For AppStacks and Writable Volumes," on page 29.
7. Set up roles and permissions. See "Configure VHD In-Guest Storage," on page 30.
8. Install App Volumes agents and other components. See "Install App Volumes Agent," on page 19.
9. To perform advanced configurations, see Chapter 9, "Advanced App Volumes Configuration," on page 59.

App Volumes Manager Console

The App Volumes Manager provides information about the different App Volumes components and configurations that are available to you.

Tab Name and Action	Details
Dashboard	Provides the following information: ■ The number of user and server licenses in use ■ User utilization ■ Most recent user logins ■ Computer utilization ■ Most recent computer logins ■ AppStack utilization ■ Most recent AppStack attachments
Volumes	Used to create and manage AppStacks and Writable Volumes and for monitoring currently attached volumes.
Directory	Shows information about users, computers, groups, and OUs that have assignments or were logged in to the computer that has the App Volumes agent installed. Active Directory objects are automatically synchronized with App Volumes database every 4 hours. To force synchronization, click **Sync** under the **Directory** tab.
Infrastructure	Shows information about computers and storage that are seen by the App Volumes Manager. You can also configure new storage groups and get details about existing configured groups.
Activity	Monitor the App Volumes Infrastructure: ■ **Pending Actions**: Displays actions waiting to be performed in the background and will be completed in the order submitted. ■ **Activity Log**: Displays records of system activity such as user logins, computer power-ups, volume attachments, and so forth. ■ **System Messages**: Displays messages and errors generated by internal events such as volume attachment and Active Directory access.
Configuration	Use these tabs to change the settings specified during App Volumes Manager installation: ■ **License**: Contains information about the license. A valid license issued is required to use this management console. ■ **Active Directory**: Provides information about your active directory. App Volumes uses the Active Directory to assign AppStacks to users, computers, and groups. ■ **Administrators**: Choice of the Active Directory group responsible for administering the App Volumes Manager. ■ **Machine Managers**: Login credentials for the vCenter Server. ■ **Storage**: Set the default database where AppStacks and writable volumes are stored.

Click the Cloud icon in the top left corner of the App Volumes Manager to return to the home page of the console.

System Requirements 2

You must verify that your system meets the requirements for installing VMware App Volumes.

This chapter includes the following topics:

Software Requirements

Ensure that your system meets certain database and browser requirements when working with App Volumes.

Database Requirements

App Volumes Manager supports different versions of the Microsoft SQL database.

- SQL Server 2012 SP1, SP2, and SP3 (whenApp Volumes Manager is installed on Microsoft Server 2012 R2), Express, Standard, and Enterprise editions
- SQL Server 2008 R2 SP2, Express, Standard, Enterprise, and Datacenter editions
- SQL Server 2014 SP1 (supported on App Volumes 2.12 and later)

For High Availability, App Volumes supports the following database features :

- SQL Server Clustered Instances
- SQL Server Mirroring

Browser Requirements

Use App Volumes Manager on one of the following supported browsers:

- Internet Explorer 9 or later
- Mozilla Firefox 28 or later
- Safari 5.1 or later
- Google Chrome 21 or later

Infrastructure and Networking Requirements

Infrastructure and networking requirements for App Volumes include requirements for App Volumes Manager, agent, and Active Directory.

Table 2-1. Infrastructure Requirements

Component	Details
App Volumes Manager	■ Microsoft Windows Server 2008 R2, Standard, Enterprise, or Datacenter editions ■ Microsoft Windows Server 2012 R2 Standard and Datacenter editions ■ .NET 3.5 framework ■ 4 vCPU required ■ 4 GB RAM ■ 1 GB disk space
App Volumes Agent (client OS)	■ Microsoft Windows 7 SP1 Professional and Enterprise editions (Microsoft Hot fix 3033929 applied) ■ Microsoft Windows 8.1 Professional and Enterprise ■ Microsoft Windows 10 Build 1607 Current Branch & LTSB ■ Microsoft Windows 10 Build 1607 Current Branch for Business ■ Windows 10 Anniversary edition Version 1607 ■ Both 64-bit and 32-bit versions of OS are supported ■ 1 GB RAM ■ 5 MB disk space **Note** Disable the GPO Control Read and Write Access to Removable Devices or Media option.
App Volumes Agent (RDSH)	■ Microsoft Windows Server 2008 R2 Standard, Enterprise, and Datacenter editions with RDSH role enabled ■ Microsoft Windows Server 2012 R2 Standard and Datacenter editions with RDSH role enabled ■ 1 GB RAM ■ 5 MB disk space
VMware software for VMDK Direct Attached Mode (Preferred)	■ VMware ESXi 5.5.x, 6.x and vCenter Server (ESXi and vCenter Server must be the same version) ■ VMware Horizon with View 6.0.1 or later ■ ESXi 5.5 U3b or 6.0 U1 required for vMotion support (Storage vMotion is not supported)
SMB file share if using VHD mode	■ SMB 2.0 ■ SMB version 3.02 (Windows Server 2012 R2) is recommended for a better performance
Active Directory	Microsoft Active Directory domain, 2003 functional level or later. Read-only account access.

Table 2-2. Networking Requirements

Component	Purpose	Port number
App Volumes Manager	Agent and Manager communications	■ TCP 80 (HTTP) ■ TCP 443 (HTTPS) ■ TCP 5985 for PowerShell Web services
App Volumes SQL Database	Database communication	TCP 1433 (SQL)

Installing App Volumes 3

Installing App Volumes involves installing the App Volumes Manager, App Volumes agents, and related components.

Before installing App Volumes, ensure that you have created and set up the requisite user accounts and Active Directory credentials.

This chapter includes the following topics:

User Accounts and Credentials

Users and administrators require certain account permissions to install and manage App Volumes components.

User Accounts

You can create user accounts and grant privileges for different roles. User names must contain only ASCII characters:

- To integrate App Volumes with vCenter Server, you must create a service account within a vCenter Server with administrator privileges. Optionally, you can create a service account with privileges granted by a custom user role.
- If you plan to use a direct connection to the ESXi host or plan to use the **Mount to Host** option with a vCenter Server connection, you must have administrator privileges on all ESXi hosts.

Active Directory Credentials

The App Volumes Manager connects to Active Directory using the service account. To prepare for installation, you must create an account within the Active Directory domain that meets the following requirements:

- Provides read access to the Active Directory domain. Administrator privileges are not required.
- Has a password that does not expire.

If your environment contains domains that are configured for one-way or two-way trust, you can configure separate credentials to access these domains. These credentials are used when connecting to any trust instead of the primary domain credentials.

Administrators Group

Access to the App Volumes Manager is restricted to the App Volumes administrators group. When you perform the initial configuration, you must provide the name of the Active Directory security group that will have access to the App Volumes Manager.

Local administrator privileges are required for the following actions:

- Install App Volumes components on target servers.
- Use writable volumes with user-installed applications.
- Provision AppStack.

Note The Active Directory service account user is not required to be an administrator.

Install App Volumes Manager

App Volumes Manager is a Web console that is used for administration and configuration of App Volumes and assignment of AppStacks and writable volumes.

Prerequisites

- Download the App Volumes installer.
- Ensure that you have the SQL Server authentication details with you.
- Verify that your environment meets the system requirements. See "Infrastructure and Networking Requirements," on page 14 and "Software Requirements," on page 13.
- Verify that your account has local administrator privileges on the target server.

Procedure

1 Run the `setup.exe` installer file.

2 Read and accept the End-User License Agreement and click **Next**.

3 Select **Install App Volumes Manager** and click **Next**.

4 Select a database option:

Option	Description
Local installation of SQL Server Express	The database is installed automatically.
Remote SQL Server 2012	Enter the required server authentication details.

5 Select the database connection method.

Option	Description
Windows Integrated Authentication	Provide owner permissions on the new database to the App Volumes Manager server.
SQL authentication	Create a user and provide owner permissions to the user on the new database.

A new ODBC connection named svmanager is created.

6 Select the **Overwrite existing database (if any)** check box and click **Next**.

Note Ensure that the **Overwrite existing database (if any)** check box is deselected when you upgrade App Volumes or install an additional instance of App Volumes Manager.

7 Select the ports on which App Volumes Manager can listen for incoming connections.

By default, communication occurs over SSL and the default value of the port is 443. Specify the port value as 80 (or equivalent) for App Volumes Manager to listen on a HTTP port.

8 (Optional) Check the **Allow Connections over HTTP (insecure)** box.

If you have specified the App Volumes Manager to listen on a HTTP port in Step 7, you must check this box. Checking this box disables SSL and all communication with App Volumes Manager becomes insecure .

Caution Do not enable HTTP in a production environment.

9 Click **Next** and enter the path where App Volumes Manager should be installed..

10 Click **Install** to begin the installation.

What to do next

Log in to App Volumes Manager and configure the Active Directory, vCenter Server, Machine Managers, and Storage as soon as you have installed App Volumes Manager. See Chapter 4, "Configuring App Volumes Manager," on page 23. You must also perform the following additional actions:

- Configure the connection to the SQL database. See "Configure a SQL Server ODBC Connection," on page 19.
- Configure SSL for App Volumes Manager. See Chapter 5, "Using SSL Certificates with App Volumes Manager," on page 33.

Configure a SQL Server ODBC Connection

When you install App Volumes Manager, a new ODBC connection is created. You must configure a connection to the SQL database and set up the required permissions.

See the Microsoft SQL ODBC documentation for instructions about configuring the SQL Server ODBC connection.

Prerequisites

Verify that `svmanager_setup.exe` executable is located on the machine where App Volumes Manager is installed.

Procedure

1 Log in as administrator to the machine where App Volumes Manager is installed.

2 Navigate to `C:\Program Files (86)\Cloud Volumes\Manager`.

3 Run `svmanager_setup.exe`.

4 Follow the on-screen instructions to connect to the database and set up permissions.

Install App Volumes Agent

After you have installed App Volumes Manager, install the App Volumes agent on the provisioning computer and target desktops.

For improved security when using the App Volumes agent, disable weak ciphers in SSL and TLS to ensure that Windows-based machines running the agent do not use weak ciphers when they communicate using SSL/TLS protocol. See *Disable Weak Ciphers in SSL and TLS* in the Horizon 7 documentation.

Important Do not install the agent on the same machine where the App Volumes Manager is installed.

You can also install the agent silently using the Microsoft Windows Installer (MSI). See "Install App Volumes Agent Silently," on page 20 for more information.

Prerequisites

- Ensure that you have installed the App Volumes Manager and you have the host IP address and port number.
- Verify that your environment meets the system requirements. See Chapter 2, "System Requirements," on page 13.
- Verify that your account has local administrator privileges on the target computer.
- Install Windows Updates from January 2016 onwards on the target computer.
- If you intend to use this virtual machine as a provisioning computer, create a clean snapshot or take a backup of this machine. Revert to this snapshot or the backup before provisioning new AppStacks.

Procedure

1 Run the App Volumes installer.

  The same installer is used to install App Volumes Manager and the agent.

2 Read and accept the End User License Agreement and click **Next**.

3 Select **Install App Volumes Agent** and click **Next**.

4 Enter the IP address and port number.

  The default port number for App Volumes Manager is 443. Enter 80 for the port number if you have configured App Volumes Manager to listen on an HTTP port.

5 (Optional) Check the **Disable Certificate Validation with App Volumes Manager** box if you do not want the agent to validate the App Volumes Manager certificate.

  Certificate validation is enabled by default.

6 Click **Install** and follow any on-screen instructions.

7 Click **Finish** to exit the wizard after the installation is completed.

8 Restart your provisioning virtual machine to complete the agent installation.

What to do next

Configure SSL certificates for the agent. See "Import Default Self-Signed Certificate," on page 36.

You can also disable SSL communication and certificate validation between App Volumes Manager and agent. See "Disable SSL Certificate Validation in App Volumes Agent," on page 36 and "Disable SSL in App Volumes Agent," on page 39.

Install App Volumes Agent Silently

You can install App Volumes agent silently using the Microsoft Windows Installer (MSI).

You perform a silent install using the command line and you do not need to use the App Volumes installer. You can also upgrade the agent silently. See "Upgrade App Volumes Agent Silently," on page 57.

Prerequisites

- Ensure that you have installed the App Volumes Manager and you have the host IP address and port number.
- Verify that your environment meets the system requirements. See Chapter 2, "System Requirements," on page 13.

- Verify that your account has local administrator privileges on the target computer.
- Install Windows Updates from January 2016 onwards on the target computer.
- If you intend to use this virtual machine as a provisioning computer, create a clean snapshot or take a back up of this machine. Revert to this snapshot or backup before you provision new AppStacks.

Procedure

1 Open a Windows command prompt on your machine.

2 Type the following command to install the agent:

```
msiexec.exe /i "App Volumes Agent.msi" /qn MANAGER_ADDR=<Manager_FQDN/IP> MANAGER_PORT=<port>
```

Verify License

You must verify the App Volumes license information before configuring other components. A valid license is required to activate and use App Volumes.

Prerequisites

Ensure that you have downloaded and installed the App Volumes license file. The production license file can be downloaded from the VMware App Volumes product download page.

Procedure

1 From the App Volumes Manager console, click **Get Started > License**.

2 Verify the license information that is displayed.

If you have an evaluation license, you can use App Volumes until the expiration date.

3 (Optional) To apply a different license, click **Edit** and browse to the location of the license you want to upload.

4 Click **Upload** to upload the App Volumes license file.

5 Click **Next** and follow on-screen instructions.

Scaling App Volumes Manager

You can install an additional App Volumes Manager component on multiple servers and point them to a shared SQL database.

Multiple App Volumes Managers can be load balanced by a hardware load balancer. Alternatively, you can configure the App Volumes agent to communicate with multiple App Volumes Manager servers.

To install additional App Volumes Manager instances, follow standard installation procedures and point a new instance to the existing SQL database. See "Install App Volumes Manager," on page 18.

Note Ensure that the **Create a new database or overwrite the existing database** check box in the installation wizard is deselected.

While configuring an App Volumes agent, you can specify the load balanced FQDN of the App Volumes Manager.

Configure the App Volumes agent to communicate with multiple managers by modifying the following registry key:

```
HKLM\SYSTEM\CurrentControlSet\Services\svservice\Parameters
```

Add string values named ManagerN (where N is number from 0 to 9) and value data of App Volumes Manager FQDN.

Configuring App Volumes Manager 4

You must configure the App Volumes Manager after installing it. Configuring the App Volumes Manager involves setting up the Active Directory, group administrative access, storage access settings, and also validating host credentials.

After configuring the App Volumes Manager, you can create and work with specialized containers known as AppStacks and Writable Volumes.

This chapter includes the following topics:

Configuring and Using Active Directory

You use Active Directory in App Volumes to assign applications and writable volumes to users, groups, computers, and Organizational Units (OUs).

As an administrator with full access to App Volumes Manager, you can configure and work with Active Directory domains and users in many ways:

- Add multiple Active Directory domains and assign unique credentials and administrator access to users from these domains.
- Assign writable volumes to a specific user.
- Filter entities based on their domain.
- Search across multiple Active Directory domains.
- Manage assignments for any user, group, or computer from any configured Active Directory domain.
- Add multiple domain controller hosts.

Active Directory Objects Lookup

App Volumes Manager looks up Active Directory objects by their GUID instead of UPN (User Principal Name). Hence administrators can move users across domains and organizational units (OUs) and even rename users and computers without affecting their AppStacks or Writable Volumes assignments .

Automatic Active Directory Synchronization

App Volumes Manager maintains a database record for any Active Directory that is seen by an App Volumes agent or assigned to an AppStack or a Writable Volume.

A background job runs every hour to synchronize up to 100 entities in the Active Directory. If there are more than 100 objects, then the next batch of 100 objects is synchronized in the hour after the first batch of objects has been synchronized.

Note GUID synchronization from Active Directory servers might take up to a week and it varies based on the number of objects that are present in the system.

Enable Secure Communication Between App Volumes Manager and Active Directory

When you configure an Active Directory, you can choose to have App Volumes Manager communicate securely with the Active Directory.

Note App Volumes Manager does not validate the SSL certificate of the Active Directory.

Prerequisites

Download the root certificate of the Active Directory to the machine where App Volumes Manager is installed.

If the root certificate is not in PEM (Base64 encoded) format, see the OpenSSL or similar documentation to convert the file to PEM format.

Procedure

1 Log in as administrator to the machine where App Volumes Manager is installed.

2 Navigate to the location where you downloaded the root certificate.

3 Rename the root certificate file to `adCA.pem`.

4 Go to the location where App Volumes Manager is installed and copy the `adCA.pem` file to the `/config` directory.

The default installation location for App Volumes Manager is `C:\Program Files (x86)\Cloud Volumes\Manager`.

When you have multiple root certificates from different domains, you can combine all the gem certificates into a single file by copying the contents of each file one by one to a single `pem` file.

You can now use LDAPs when you register an Active Directory. See "Register an Active Directory Domain," on page 25.

If you select LDAPs without configuring the `adCA.pem` file, you see the following message in App Volumes Manager: `Active Directory SSL certificate is skipped for <name-of-active-directory>, check logs for details.`. You can however still proceed with the Active Directory configuration.

Adding and Configuring Domain Controller Hosts

You can add a single domain controller host or multiple hosts when you register an Active Directory.

You might configure multiple domain controller hosts to ensure redundancy and failover operations. If the primary domain controller that App Volumes Manager is connected to goes down, then App Volumes Manager can perform a failover and switch to a different host. This ensures that App Volumes users are unaffected by the downtime and can continue their operations without interruption.

You can choose how App Volumes Manager detects domain controllers. Consider the following when you add domain controllers:

- If you provide a list of domain controllers, App Volumes Manager looks for a domain controller only in the list you provided. If the domain controllers in the list are all down, App Volumes Manager does not search for or detect any other domain controller.
- If you do not provide a list of domain controllers, App Volumes Manager detects domain controllers automatically and also assigns a priority to them.
- App Volumes Manager will search for and try to connect to domain controllers from the same site. Domain controllers from other sites are also added in order of binding time.

Note Domain controllers in the same site always have higher priority over those from different sites.

Refresh Domain Controllers

The list of available domain controllers is refreshed every 480 minutes (8 hours). Use the environment variable, TIME_TO_REFRESH_DOMAIN_CONTROLLERS, to change the default time of 8 hours.

Note You must set the time in minutes.

Register an Active Directory Domain

App Volumes uses Active Directory to assign application to users, computers, groups, and organizational units (OUs).

If you want use a secure connection to connect App Volumes Manager to the domain controller, see "Enable Secure Communication Between App Volumes Manager and Active Directory," on page 24.

Prerequisites

Procedure

1 From the App Volumes Manager console, go to **Configuration > Active Directory > Register Domain**.

2 Enter the Active Directory configuration information and click **Create**.

Parameter	Description
Active Directory Domain Name	A fully qualified domain name of the Active Directory domain where users and target computers are residing, for example **`corp.example.com`**.
Domain Controller Hosts (Optional)	IP address (**`10.98.87.67`**) or FQDN (**`dc01.corp.example.com`**). You can also provide the virtual IP address of a load balancer that is used as the front-end server of the domain controller. This option provides High Availability (HA) capability for connections to Active Directory. You can add multiple domain controller hosts; use commas to separate the names of the hosts. **Important** If you do not add a domain controller host, the system will detect the hosts that are available and connect to the nearest domain controller.
LDAP Base (Optional)	Distinguished name of the Active Directory container or organizational unit that stores required entities (if you want to limit the scope of enumeration). By default, App Volumes Manager enumerates all users, groups, OUs, and computer objects within Active Directory. Example: OU=Engineering, DC=corp, DC=vmware, DC=com
Username	The user name of the service account that has access to the target Active Directory domain. For example, *admin-1*. The user can be an administrator with read-only permissions.
Password	The password for the service account. Ensure that domain policies do not enforce password expiration for the service account.

Parameter	Description
Use LDAPs (Optional)	Check the **Use Secure Connection** box if your domain controllers are configured with TLS certificates for LDAP connections. Check the box to encrypt communication between App Volumes Manager and the domain controller.
Port (Optional)	A port number other than the default.

Add Administrators

Add an App Volumes administrator group who can log in to the App Volumes Manager and manage the users and groups.

You can create multiple administrator groups for a single Active Directory domain.

Note You cannot configure a single user an administrator, only a group can be added as an administrator.

Prerequisites

Verify that you have already added the group to the Active Directory database.

Procedure

1 From the App Volumes Manager console, click **Configuration > Administrators > Add Administrator**.

2 Search the domain for the group to which you want to provide administrator privileges and select **All** to search in all domains or select a specific domain from the drop-down menu.

You can filter the search query by Contains, Begins, Ends, or Equals.

a (Optional) Check the **Search all domains in the Active Directory forest** box to search all domains in the entire Active Directory forest.

A drop-down menu displays the groups matching your search query.

3 Select the Active Directory group from the list.

4 Click **Create**.

All users within the group are granted administrator privileges.

What to do next

After you have added the administrators, you can configure the Machine Managers and App Volumes storage. See "Configuring a Machine Manager," on page 26 and "Configure Storage For AppStacks and Writable Volumes," on page 29.

Configuring a Machine Manager

The App Volumes operation mode is determined by configuring the Machine Manager.

The Machine Manager determines the type of hypervisor connection. Three types of hypervisor connections are available. You can configure the hypervisor to connect to one of the following hosts using the App Volumes Manager console.

Table 4-1. Hypervisor Connection Types

Hypervisor Connection Type	Description
VMware vCenter Server	Preferred connection type for mid-to-large environments. Enables the use of VMDK Direct Attached operation mode . When using this connection type, you can assign AppStacks and writable volumes to the virtual machines running on multiple hypervisor hosts.
Single ESXi Host	Enables the use of VMDK Direct Attached Operation Mode, but only for a single ESXi host. Use this connection type for small deployments and proofs of concepts. You can assign AppStacks and writable volumes to the virtual machines running on a single hypervisor host.
VHD In-Guest Services	Disables other hypervisor connections and enables the use of VHD In-Guest operation mode. Use this connection type to assign AppStacks and writable volumes either to virtual machines running on an unsupported third-party hypervisor or to the physical computers. See "Configure VHD In-Guest Storage," on page 30.

You cannot change the operation mode after you configure the Machine Manager. However, if you have configured vCenter Server as the first Machine Manager, additional vCenter Server instances can be added and configured.

Set Up the Machine Manager Connection

App Volumes operation mode is determined by configuring a machine manager. You cannot change the operation mode of App Volumes after you configure the machine manager.

Prerequisites

Ensure that the domain policies do not enforce password expiration for the service account on the machine manager to be configured.

Procedure

1 From the App Volumes Manager console, click **Configuration > Machine Managers**.

2 Select and configure the machine manager.

Connection Type	Description
vCenter Server	Enter host name, user name, and password details. You can optionally enable the **Mount Local** or **Mount on Host** options. If you select a vCenter Server instance as the first configured machine manager, you can add and configure additional servers.
ESXi (Single Host)	Enter host name, user name, and password details for the ESXi host.
VHD In-Guest	Does not require any credentials.

   a (Optional) To view the permissions required by the service account, click **Required vCenter Permissions**.

3 Click **Save**.

   The configured machine manager is displayed on the Machine Managers page.

What to do next

See "Establish a Secure vCenter Server Connection," on page 33 to connect App Volumes Manager securely to a vCenter Server.

You can also create a custom role on the vCenter Server. See "Create a Custom vCenter Server Role Using PowerCLI," on page 65.

Configuring Security Protocols and Cipher Suites

You can configure the security protocols and cipher suites for App Volumes Manager so that only the TLS connections that you have specified are accepted by App Volumes Manager.

You can also configure cipher suites to add ciphers and disable weak ciphers.

Configure TLS Connections in App Volumes Manager

You can modify the Nginx configuration file to ensure that App Volumes Manager accepts connections only from specified TLS versions.

App Volumes Manager uses SSL and TLS to communicate with servers and App Volumes agents. See Chapter 5, "Using SSL Certificates with App Volumes Manager," on page 33.

Prerequisites

- You must have administrator privileges on the machine where App Volumes Manager is installed.
- Locate the `nginx.conf` file and create a backup of the file. The default location for `nginx.conf` is `C:\Program Files (x86)\CloudVolumes\Manager\nginx\conf\`.

Procedure

1. Log in to the machine where App Volumes Manager is installed.
2. Identify the `ssl_protocols` line in the `nginx.conf` file and retain only the TLS versions that you want App Volumes Manager to connect with.

   For example, if you include `TLSv1.1` and `TLSv1.2` in the `ssl_protocols` line, App Volumes Manager will accept connections only from these TLS versions.
3. Restart the App Volumes Manager service.

Example: Configure TLS v1.1 and TLS v1.2 Protocols

In this example, App Volumes Manager will accept connections only from agents that use TLS v1.1 and TLS v1.2 protocols, as specified in the `ssl_protocols` entry in the Nginx configuration file.

```
server {
            server_name 0.0.0.0;
            listen 3443;
            listen 443;
            listen [::]:443;

            ssl on;
            ssl_certificate    appvol_ca1_vmware.com.crt;
            ssl_certificate_key    appvol_ca1_vmware.com.key;
            ssl_protocols TLSv1.1 TLSv1.2
            ssl_session_cache    builtin:1000;
            ssl_session_timeout 5m;

            root ../public;
```

Configure Cipher Suites in App Volumes Manager

You can modify the Nginx configuration file to add ciphers or remove weak ciphers.

Prerequisites

- You must have administrator privileges on the machine where App Volumes Manager is installed.
- You must use the format that is defined in `https://www.openssl.org/docs/man1.0.2/apps/ciphers.html` under the section CIPHER LIST FORMAT while adding the ciphers. The ciphers are specified as a list separated by colons, spaces, or commas.
- Locate the `nginx.conf` file and create a back up of the file. `nginx.conf` is located at `C:\Program Files (x86)\CloudVolumes\Manager\nginx\conf\`.

Procedure

1 Log in to the machine where App Volumes Manager is installed.

2 Identify the line starting with `ssl_ciphers` in the `nginx.conf` file.

Add the list of ciphers before the existing list of ciphers; the order of ciphers matters.

For example, add `ECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH` to the existing list of ciphers.

3 (Optional) To disable any ciphers, remove the ciphers from the list.

4 Restart the App Volumes Manager service.

Configure Storage For AppStacks and Writable Volumes

You can select datastores and paths where AppStacks and writable volumes are stored. You can configure a Hypervisor or VHD In-Guest storage type.

Volumes are attached only for virtual machines on the host. You can add available storage only when App Volumes Manager is configured in the VHD In-Guest mode. Otherwise, the list of storage locations and datastores is populated from vCenter Server. See "Configure VHD In-Guest Storage," on page 30.

Prerequisites

Use a storage location that is accessible to all virtual machine host servers. When using VMDK Direct Attach Operation Mode, the App Volumes Manager requires local or shared storage to be configured on the hypervisor.

Procedure

1 From the App Volumes Manager console, click **Storage**.

If you have configured the storage options, click **Edit** to change the configuration.

2 Enter the **Default Storage Location**, **Default Storage Path**, and **Templates Path** for AppStacks and Writable Volumes and click **Next**.

3 Confirm your storage settings and click **Set Defaults**.

4 (Optional) Check **Import volumes immediately** to import the volumes immediately. This option does not allow you to perform administrative tasks while import is underway.

5 Verify the information you entered on the Upload Prepackaged Volumes page, select the volumes, and click **Upload**.

The volumes packaged with this App Volumes Manager are uploaded to the selected datastore.

Configure VHD In-Guest Storage

To use App Volumes with VHD In-Guest Operation mode, the machines where the App Volumes Manager and agents are installed require special permissions on the CIFS file share.

Procedure

1 On a file server, create a new empty folder.

2 Copy the contents of the `Hypervisor\In-Guest VHD` folder from the App Volumes installation media to the new folder.

3 Share the folder and grant full access permissions on the file share to everyone.

4 Configure NTFS permissions as described below.

An Active Directory domain group might be used to manage permissions for the following roles:

- Managers: App Volumes Manager
- Agents: Machines that receive App Volumes and writable volumes assignments
- Capture Agents: Machines that are used for provisioning new App Volumes agents

Table 4-2. NTFS folder permissions required for each role

Folder	Managers	Agents	Capture Agents
apps	Full	Read	Write
apps_templates	Read	None	None
writable	Full	Write or None **Note** Write permissions are required by Agents when Dynamic Permissions are not enabled.	None
writable_templates	Read	None	None

Disable Microsoft Windows NTLM Authentication

NTLM (NT LAN Manager) authentication is used to make the communication between App Volumes Manager and agent more secure.

When an App Volumes agent make an HTTP request to the App Volumes Manager, NTLM is used to authenticate the user and user account with the entry in the Active Directory.

You can disable NTLM by defining a system environment variable on the machine where App Volumes Manager is installed.

See https://technet.microsoft.com/en-us/library/jj852241(v=ws.11).aspx to understand the implications of disabling NTLM.

Procedure

1 Log in as administrator to the machine where App Volumes Manager is installed.

2 Open Control Panel and click **System > Advanced System Settings > Environment Variables > New**.

The New System Variable window appears.

3 In the **Variable name** text box, enter ***AVM_NTLM_DISABLED***.

4 In the **Variable value** text box, enter ***1***.

5 Restart the computer.

The App Volumes Manager service also restarts.

Using SSL Certificates with App Volumes Manager

5

App Volumes Manager uses SSL to communicate with Machine Managers and App Volumes agents. You can configure, replace, import, disable, and manage the SSL certificates used for SSL communication and validation.

You can add and upload trusted SSL certificates from the App Volumes Manager console to establish a secure connection to the vCenter Server and the remote SQL server.

You can also replace the default App Volumes Manager certificates that are used for communication with App Volumes agents, disable SSL and SSL certificate validation, and enable an HTTP connection.

This chapter includes the following topics:

Configuring SSL Certificates for Machine Managers

You can establish secure connections from App Volumes Manager to SQL Server and vCenter Server.

Establishing a Secure SQL Server Connection

If the instance of App Volumes Manager that you have installed connects to an SQL server, you can change the default Windows ODBC settings and connect securely to App Volumes Manager.

Ensure that you have downloaded the SSL certificate on the SQL server instance and imported the certificate as a Trusted Certificate on to the machine where App Volumes Manager is installed . Change the ODBC settings on this machine.

For detailed instructions, see https://support.microsoft.com/en-us/kb/316898.

Establish a Secure vCenter Server Connection

You can securely connect to a vCenter Server from App Volumes using an SSL certificate.

Prerequisites

Ensure that the vCenter Server you are connecting to has a domain SSL certificate.

The certificate must be verified and accepted by App Volumes.

Procedure

1 From the App Volumes Manager console, click **Machine Managers > Add Machine Manager**.

2 Enter the required Machine Manager information and click **Save**.

Option	Description
Type	Enter **vCenter Server**
Host name	The host name of the Machine Manager. For example, **server.your-domain.local**
User name	The user name with which you will access the machine. For example, YOURDOMAIN\administrator.
Password	The password for the user name.
Mount Local	Select this option if your VM's datastore has local copies of volumes and you want to mount the local copies.
Mount on Host	Select this option if you want to connect directly to the VM host. This results in increased performance and decreases the burden on the vCenter Server.

3 Verify the certificate details.

If the certificate is not trusted or verified, the following messages are seen:

- A window with details of the certificate (SHA1 fingerprint, period of validity) that is present in the vCenter Server.
- A message at the top right corner:

  ```
  Server error: SSL certificate is not verified and needs to be accepted to continue.
  ```

4 Click **Accept** to accept the certificate.

You can also log in to the vCenter Server as an administrator and verify the SHA1 code.

The Machine Manager is successfully added after the certificate is verified.

5 Click **Certificate** to view the certificate you added.

If the certificate is changed on the vCenter Server after it has established a connection with App Volumes Manager, the `Certificate not valid` message is displayed when you log in to App Volumes Manager.

Note You also see this message when you upgrade App Volumes to the latest version.

6 To validate the certificate again, select the vCenter Server under Machine Managers, click **Certificate**, and accept the certificate.

You now have a trusted SSL certificate to connect to the vCenter Server.

What to do next

When you upgrade App Volumes from an older version to the latest version, you might have to manually accept the certificates to retain the connection to vCenter Server.

Managing SSL Between App Volumes Manager and Agent

A default self-signed certificate is installed when you install App Volumes Manager. App Volumes agents use SSL to communicate with the App Volumes Manager and validate the certificate.

Replace the Self-Signed Certificate with CA-signed Certificate

A self-signed certificate is installed when you install App Volumes Manager. You can replace the default self-signed certificate by modifying the Nginx configuration file.

Note The self-signed certificate is installed in the same location as the Nginx configuration file: `C:\Program Files (x86)\CloudVolumes\Manager\nginx\conf`.

Prerequisites

- Obtain an SSL certificate from a trusted Certificate Authority (CA).
- Download the CA-signed certificate that you obtained and the corresponding key to the machine where the App Volumes Manager is installed. Note down the location where the files are downloaded.
- If you provide a passphrase while generating the private key during the Certificate Signing Request (CSR), note down the passphrase.
- Verify that the common name on the CA-signed certificate is the same as the host name or the IP address of App Volumes Manager that you configured while installing the agent.
- Verify that the SSL key and certificate are both in PEM (Base64 encoded) format.
- Verify that the certificate and key are Nginx compliant.

Procedure

1. Log in as administrator to the machine where the App Volumes Manager is installed.
2. Navigate to `C:\Program Files (x86)\CloudVolumes\Manager\nginx\conf` and make a copy of the existing Nginx configuration file, `nginx.conf`.
3. Open the Nginx configuration file.
4. Edit the *ssl_certificate* and *ssl_certificate_key* variables in the Nginx configuration file to point to the path of the certificate and key files that you downloaded.
5. (Optional) If you had provided a passphrase for the CA-signed certificate, enter the passphrase for your certificate in the Nginx configuration file.
6. Save the configuration file.
7. Restart the App Volumes Manager service.

Example: Nginx Configuration File

In this example, the *appvol_ca1_vmware.com.crt* and *appvol_ca1_vmware.com.key* are the default self-signed certificates.

```
server {
            server_name 0.0.0.0;
            listen 3443;
            listen 443;
            listen [::]:443;

            ssl on;
            ssl_certificate    appvol_ca1_vmware.com.crt;
```

```
ssl_certificate_key    appvol_ca1_vmware.com.key;
ssl_session_cache    builtin:1000;
ssl_session_timeout 5m;

root ../public;
```

What to do next

You can download and add the CA-signed certificate to the trust store of the App Volumes agent directly.

Import Default Self-Signed Certificate

If you do not want to replace the default self-signed certificate in the App Volumes Manager, you can import the certificate and add it to the local trust store of the machine where the App Volumes agent is installed.

If you have installed and configured multiple App Volumes Manager instances for use in all agent machines, then the self-signed certificates have to be imported from each App Volumes Manager instance to the agent machines.

Prerequisites

Obtain the IP address of the App Volumes Manager instance whose certificate you want to import.

Procedure

1 Log in as an administrator to the machine where the App Volumes agent is installed.

2 In a Web browser, enter the host name or IP address of the App Volumes Manager in the form of *https://hostname*.

A warning message that the SSL certificate is not validated is displayed.

3 Click the warning message and follow instructions to download the SSL certificate displayed in the browser.

4 Open the Microsoft Management Console (MMC) and import the downloaded SSL certificate.

See https://technet.microsoft.com/en-us/library/cc754841(v=ws.11).aspx#BKMK_addlocal for detailed instructions to import the SSL certificate after downloading it.

Disable SSL Certificate Validation in App Volumes Agent

SSL certificate validation is enabled by default when you install the App Volumes agent.

You can disable SSL certificate validation in the agent, either when you are installing the agent or after you have installed the agent.

Note When you disable certificate validation, untrusted App Volumes Manager certificates are not validated , but communication between App Volumes Manager and agent still occurs over SSL. If you want to disable SSL completely, see "Disable SSL in App Volumes Agent," on page 39.

Disable SSL Certificate Validation When Installing App Volumes Agent

The App Volumes agent validates the SSL certificate of the App Volumes Manager during communication with the manager. You can disable the certificate validation when you are installing the agent.

Procedure

- When you install the App Volumes agent, select the **Disable Certificate Validation with App Volumes Manager** box on the App Volumes Agent window.

Certificate validation is disabled but communication with the manager still occurs over SSL.

Disable SSL Certificate Validation in App Volumes Agent After Installation

You can disable SSL certificate validation after you have installed the agent.

Procedure

1 Log in as administrator on the machine where the App Volumes agent is installed.

2 Click the **Start** menu in Windows and enter **`regedit`** to open the Registry editor.

3 In the Registry Editor, go to `HKLM\System\CurrentControlSet\Services\svservices\Parameters`.

4 Locate and set the `EnforceSSlCertificateValidation` key to 0.

The SSL certificate is no longer validated.

5 Restart the App Volumes service.

SSL certificate validation is disabled in App Volumes agent.

Enable HTTP in App Volumes Manager

You can enable an HTTP connection in App Volumes Manager, either when you are installing the manager or after installation.

You might want to enable an HTTP communication, for example, when you upgrade App Volumes to the latest version, and want to install and test App Volumes immediately without configuring SSL certificates.

Note Enable HTTP only in a non-production environment or if you are running App Volumes Manager behind a load balancer.

Enable an HTTP Connection in App Volumes Manager During Installation

You can enable an HTTP connection when you are installing App Volumes Manager.

Procedure

1 When you choose networks ports during App Volumes Manager installation, select the **Allow Connections Over HTTP (insecure)** option.

2 Enter a value for the HTTP port or retain the default value of 80.

HTTP is enabled in App Volumes Manager and you can now disable SSL in the agent and configure the agent to communicate over HTTP. See "Disable SSL in App Volumes Agent," on page 39.

Enable HTTP in App Volumes Manager After Installation

You can modify the Nginx configuration file in App Volumes Manager if you want to enable HTTP in the manager after it has been installed.

Important This server block is not present in the Nginx file by default; add this server block only if you have not enabled HTTP when installing App Volumes Manager.

Prerequisites

Navigate to `C:\Program Files (x86)\CloudVolumes\Manager\nginx\conf` and take a back up of the existing Nginx configuration file, `nginx.conf`.

Procedure

1 Log in as administrator to the machine where App Volumes Manager is installed.

2 Navigate to `C:\Program Files (x86)\CloudVolumes\Manager\nginx\conf`, open the Nginx configuration file, and copy the following block in the Nginx file after `include proxy/vcenter*.conf;`.

```
server {
        server_name  0.0.0.0;
        listen       80;
        listen       [::]:80;


        root   ../public;
        rewrite ^/(.*)/$ /$1 permanent;

        access_log  logs/access_http.log  main;
        error_log   logs/error_http.log  info;

        charset utf-8;
        override_charset on;

        gzip on;
        gzip_types application/json application/javascript;

        error_page  404              /404.html;
       error_page  502              /502.html;
        #error_page   500 502 503 504  /500.html;

        location ~* ^.+\.(jpg|jpeg|gif|png|ico)$ {
            expires max;
            break;
        }

        location ~* ^.+\.(css|js|htm|html|json)$ {
            #expires 0; # expire immediately
            expires 5m;
            break;
        }

        location / {
          try_files /index.html @manager;
        }

        location ^~ /ngvc/ {
            access_log logs/access_ngvc_http.log  main;
            error_log logs/error_ngvc_http.log  info;
            proxy_connect_timeout 10;
            #proxy_next_upstream off;
            proxy_next_upstream timeout;
            proxy_read_timeout 600;
            proxy_send_timeout 30;
            send_timeout 30;
            proxy_redirect off;
            server_name_in_redirect off;
            proxy_pass_header Cookie;
            proxy_pass_header Set-Cookie;
            proxy_pass_header X-Accel-Redirect;
            proxy_set_header Host $host:80;
            proxy_set_header X-Real-IP $remote_addr;
```

```
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
            add_header X-Backend $upstream_addr;
            proxy_pass http://ngvc;
        }

        location @manager {
            proxy_connect_timeout 10;
            #proxy_next_upstream off;
            proxy_next_upstream timeout;
            proxy_read_timeout 600;
            proxy_send_timeout 30;
            send_timeout 30;
            proxy_redirect off;
            server_name_in_redirect off;
            proxy_pass_header Cookie;
            proxy_pass_header Set-Cookie;
            proxy_pass_header X-Accel-Redirect;
            proxy_set_header Host $host:80;
            proxy_set_header X-Real-IP $remote_addr;
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
            add_header X-Backend $upstream_addr;
            add_header X-Frame-Options SAMEORIGIN;
            add_header X-Content-Type-Options nosniff;
            add_header X-XSS-Protection "1; mode=block";
            proxy_pass http://manager;
        }
    }
```

3 Restart the App Volumes service.

App Volumes Manager now communicates over HTTP.

Disable SSL in App Volumes Agent

You can disable SSL in App Volumes agent after you have installed the agent.

Prerequisites

Verify that you have enabled HTTP connection in App Volumes Manager. See "Enable an HTTP Connection in App Volumes Manager During Installation," on page 37.

Procedure

1 Log in as administrator on the machine where the App Volumes agent is installed.

2 Click the **Start** menu in Windows and enter **`regedit`** to open the Registry editor.

3 In the Registry Editor, go to `HKLM\System\CurrentControlSet\Services\svservices\Parameters`.

4 Set the `SSL` key in the `HKLM\System\CurrentControlSet\Services\svservices\Parameters` path to 0.

5 Restart the App Volumes service.

SSL is disabled in the App Volumes agent and all agent communication with the App Volumes Manager occurs over HTTP.

Working with AppStacks 6

You can bundle applications and data into specialized read-only containers called AppStacks. You can assign AppStacks to users, groups, or accounts, and deliver applications through them.

Using the App Volumes Manager, you can create, update, edit, and delete, and manage AppStacks.

You must be aware of the following considerations when you are creating and provisioning AppStacks:

- Physical endpoints and AppStacks are supported only under the following constraints:
  - VHD In-Guest mode is the only supported machine manager mode.
  - You must have a constant network connection.
  - The OS on the physical device must be non-persistent, streamed, or both.
- Provisioning of Internet Explorer into an AppStack is not supported. Due to the tight OS integration and dependencies, use an application isolation technology such as VMware ThinApp, and then use App Volumes for delivery of the isolated application package.

This chapter includes the following topics:

Provisioning and Assigning AppStacks

You must first create and provision an AppStack and then assign the AppStack to users and groups.

After you create an AppStack using the App Volumes Manager, you must log in to the provisioning machine where the AppStack is attached, and install the applications in the AppStack. You can then assign the AppStack to users and groups.

Preparing a Provisioning Machine

Provision the AppStacks on a clean base image, that is a virtual machine, that closely resembles the target environment to which you later plan to deploy the AppStack.

For example, the provisioning virtual machine and the target should be at the same patch and service pack level. If you have included applications in the base image, they should also be present in the provisioning virtual machine.

Perform provisioning on a virtual machine that does not have any assigned AppStacks. If you have previously assigned any AppStacks to the virtual machine, or if the virtual machine has been used for provisioning before, that virtual machine should be set back to a clean snapshot before you begin provisioning a new AppStack.

Best Practices for Provisioning Virtual Machines and Applications

You can follow some best practices while provisioning virtual machines and applications.

- Ensure that you have local administrator rights for provisioning.
- Perform only one provisioning process in each virtual machine. You can provision multiple virtual machines at the same time.
- If the provisioning virtual machine has a service pack, such as Service Pack 1, ensure that all virtual machines delivering applications are at the same or later service pack level.
- (Optional) For best performance, include application dependencies (such as Java, or .NET) in the same AppStack as the application.
- The provisioning system should not have antivirus agents, VMware Horizon with View agent, or any other filter driver applications installed or enabled.
- When provisioning an application, always install the application for all users. This ensures the application is installed under Program Files rather than a single user profile. This also creates application icons in the All Users folder.
- The provisioning virtual machine usually joins the same domain as the production virtual machine. However, this is dependent on the applications that are being provisioned. Some application requirements and licensing models require that the virtual machine shares a common SID with the production virtual machine.
- Do not deliver applications that require a common SID to a pool or to virtual machines that have had `Sysprep` run on them. These cases should be used in conjunction with VMware Horizon with View Composer or other similar OS cloning technologies that preserve the machine SID.
- Virtual machines used for provisioning should have a snapshot dedicated to the state of a user's desktop. After provisioning, virtual machines should have a clean snapshot that was made directly following the App Volumes agent installation. After the completion of provisioning, the virtual machine reverts to a clean state, that is, the snapshot.
- Provision the AppStacks on a clean base image, that is a virtual machine that closely resembles the target environment to which you later plan to deploy the AppStack. For example, the provisioning virtual machine and target should be at the same patch and service pack level and, if applications are included in the base image, they should also be present in the provisioning virtual machine.
- If you are provisioning AppStacks on a virtual machine has been used for provisioning before, the virtual machine should be set back to the clean snapshot before provisioning a new AppStack.

Create an AppStack

Create a new AppStack.

When you create an AppStack, you only provide the name, storage, path, and description of the AppStack.

Procedure

1 From the App Volumes Manager console, click **Volumes > AppStack > Create AppStack**.

2 Enter the following information for the AppStack and click **Create**:

Option	Description
Name	A name that describes the type of applications contained in the AppStack.
Storage	Name of your default datastore.
Path	The path for the volume. The path to the `apps_templates` and `writable_templates` file on the datastore is created during the initial setup process. You can change the path to further sub-categorize volumes. For example: `appvolumes/apps/your_folder.`.
Template	Select a template for the AppStack, usually in the form of a `VMDK` file.
Description	A short description of the AppStack, usually names of applications that the AppStack will contain.

What to do next

Provision the AppStack to attach it and install applications. The AppStack is not fully created until the you have completed provisioning. See "Provision An AppStack," on page 43 and "Install Applications in AppStacks," on page 44.

Provision An AppStack

After you create a new AppStack, you must provision the AppStack by attaching it to the provisioning computer and installing the applications in the AppStack .

Procedure

1 From the App Volumes Manager console, click **Volumes > AppStack**.

2 Select the AppStack you want to provision, and click **Provision**.

Note Ensure that the AppStack you have selected is not already provisioned.

3 Search for and select the provisioning computer by entering a full or partial name of the computer.

4 Click **Provision** to attach the AppStack to the virtual machine.

Note For VHD In-Guest mounting, the provisioning computer must be powered off.

5 Log in to the provisioned computer and install the applications into AppStack to complete the provisioning process.

Install Applications in AppStacks

After a new AppStack is attached to the provisioning machine, you must install the applications in the AppStack to complete the provisioning process.

Prerequisites

- Verify that the App Volumes agent is installed on the provisioning machine and is configured to connect to the App Volumes Manager. See "Install App Volumes Agent," on page 19.
- If the application you are about to install uses insecure ciphers, and if you have disabled weak ciphers in SSL and TLS while installing the App Volumes agent, the application might not function properly. If your application installs and uses its own SSL and TLS libraries, disabling weak ciphers does not impact the functioning of the application. See "Install App Volumes Agent," on page 19.

Procedure

1 Log in to the provisioning computer.

NOTE Ensure that you are now in the provisioning mode.

2 Follow the on-screen instructions to install the applications in the attached AppStack.

NOTE Do not click **OK** until you have installed all your applications. If you click **OK** before installation is completed for the first application, the AppStack is created, but it is empty.

3 After installing the applications successfully, click **OK** to return to the App Volumes Manager.

4 Restart the provisioning machine and log in to it.

What to do next

Check the applications in the provisioned AppStack to ensure that provisioning was successfully completed. The AppStack is ready to be assigned to users and groups. See "Assign an AppStack," on page 44.

Assign an AppStack

After you create and provision an AppStack, you can assign the AppStack to users, groups, or computers.

Procedure

1 From the App Volumes Manager console, select **Volumes > AppStacks**.

2 Select the AppStack that you want to assign to a computer or user and click **Assign**.

3 Enter the following information to assign the AppStack:

Option	Description
Domain	Specify the domain to which you want to assign the AppStack.
Search String	To search the Active Directory, enter a string and select an additional option (such as Begins, Ends, Equals) to refine the search.

4 (Optional) Select the **Search all domains in the Active Directory forest** box to search all domains.

5 Click **Search**.

6 Select the user, group, or computer to which you want to assign the AppStack and click **Assign**.

7 Select one of the following methods of assignment:

Option	Description
Attach AppStack on next login or reboot	The AppStack is attached when the user logs in or reboots the machine he is logged in to.
Attach AppStack immediately	The volume is attached instantly to all computers on which the selected users are logged in. If you are assigning the AppStack to a group or organizational unit, all users or computers in that group get the attachments immediately.

After the AppStack is assigned to the selected entity, the entity becomes known to the App Volumes Manager.

What to do next

Use the **Directory** tab to manage AppStack assignments.

Edit an AppStack

You can edit an AppStack to change its name and description, and to change the type of OS to which the AppStack is attached.

Prerequisites

Verify that the AppStack you want to edit is provisioned. See "Provision An AppStack," on page 43.

Procedure

1 From the App Volumes Manager console, click **Volumes > AppStacks**.

2 Select the AppStack that you want to edit and click **Edit**.

3 Update the name, description, or OS type and click **Save**.

What to do next

Click the **Rescan** icon to view the latest information about the available AppStacks.

Update an AppStack

You can update an AppStack to add, delete, and update applications.

When you update an AppStack, App Volumes creates a clone of this AppStack and the updated AppStack is in an unprovisioned state.

Procedure

1 From the App Volumes Manager console, click **Volumes > AppStacks**.

2 Select the AppStack.

- Click the AppStack you want to update. The AppStack details are displayed.
- Select the check box next to the AppStack you want to update.

3 Click **Update**.

4 Enter the following information and click **Create**.

Field	Description
Name	The name of the AppStack.
Storage	The location where you want the AppStack to be stored.

Field	Description
Path	Path to the datastore.
Description	A description of the applications in this AppStack.

The AppStack is updated and is unprovisioned.

What to do next

Provision the updated AppStack. See "Provisioning and Assigning AppStacks," on page 41.

Import AppStacks to App Volumes

If you have preconfigured third-party AppStacks or have AppStacks from another deployment, you can import them to App Volumes.

Prerequisites

Using the vCenter Server datastore browser, select a datastore, create a new folder, and upload the AppStacks to this folder.

Procedure

1 From the App Volumes Manager console, click **Volumes > AppStack > Import AppStacks**.

2 Browse to the datastore where you uploaded the AppStacks and select the AppStack you want to import.

3 Click **Import**.

The AppStacks are imported and become known to the App Volumes Manager. You can now assign and attach the imported AppStacks.

Check Datastores for Available AppStacks

You can verify whether the AppStacks in the datastore are still present and accessible.

Procedure

1 From the App Volumes Manager console, click **Volumes > AppStacks**.

2 Click **Rescan**.

A list of all known and available App Volumes Manager is displayed.

What to do next

If you find that new AppStacks have been added to the datastore, use the **Import** option to import them, and make the AppStacks known to the App Volumes Manager that you are logged in to.

Setting AppStacks Precedence

When multiple AppStacks that share common components are assigned to a machine, you can reorder the AppStacks to give priority to oneAppStack over the others.

You can re-order AppStacks provisioned with App Volumes 2.5 or later.

As an example, you can have both Adobe 9 and Adobe 10.x App Volumes attached to a machine, although they cannot co-exist natively. When users double-click a PDF file on the desktop, only one Adobe Reader is launched. If you have assigned a higher precedence to Adobe 9 than Adobe 10.x, Adobe 9 gets the priority as the default PDF reader application. If you want to modify the default application, you can use the reordering feature in App Volumes Manager to adjust the stack order, so that Adobe 10.x becomes the default PDF reader.

See the KB article https://kb.vmware.com/kb/2146035 for information on how to provision and use Microsoft Office applications with App Volumes.

Delete AppStacks

You can delete legacy and deprecated AppStacks from the disk.

Prerequisites

Verify that the AppStacks you want to delete are not assigned to any computers, users, or groups.

Procedure

1 From the App Volumes Manager console, click **Volumes > AppStack** and select the AppStack you want to remove.

2 Click **Delete**.

Note AppStack and Writable Volume that can no longer be contacted on a datastore have their state set to `Unreachable`. You can remove AppStacks or writable volumes even when they are unreachable. This action cleans up the metadata in the App Volumes database.

What to do next

Click the **Rescan** icon to display a list of the updated and available AppStacks.

Working with Writable Volumes 7

With Writable Volumes, you can configure per-user volumes where users can install and configure their own applications and keep the data that is specific to their profile. Because you assign a Writable Volume to a specific user, the data that it stores migrates with the user to different machines.

A Writable Volume is an empty VMDK or VHD file that you assign to a specific user. It mounts to the VM when the user authenticates to the desktop. You can assign many Writable Volumes to a user, but you can attach only one Writable Volume at a time.

Examples of the data that a Writable Volume can contain are application settings, user profile, licensing information, configuration files, user-installed applications, and others.

With the latest version of App Volumes, you can also specify exclusions that are targeted for writable volumes. These exclusions do not affect AppStacks or system volumes. For more information, see Writable Volumes Exclusions.

Using Writable Volumes with User Environment Management Solutions

You can use Writable Volumes to complement a user environment management solution, for example VMware User Environment Manager. Such solutions can manage data in Writable Volumes at a more granular level and enforce policies based on different conditions or events by providing contextual rules. With ,Writable Volumes you can use containers for local user profile delivery across systems.

Using Writable Volumes with Non-Persistent Virtual Desktops

On a non-persistent virtual desktop environment, all applications that the user installs are removed after the user logs out of the desktop. Writable Volumes store the applications and settings of users and make user-specific data persistent and portable across non-persistent virtual desktops. This way, you can address use cases, such as providing development and test machines for users to install custom applications on non-persistent virtual desktops. You must reboot the desktop after you remove a Writable Volume.

Storage Configuration with Writable Volumes

When designing your environment for Writable Volumes, consider that a Writable Volume requires both read and write I/O. The input output operations per second (IOPS) for a Writable Volume might vary for each user depending on the users consume their data. IOPS might also vary depending on the type of data that the users are allowed to store on their Writable Volume.

You can manage the number of Writable Volumes that can be configured on a single storage LUN by monitoring how the users access their Writable Volumes.

Writable Volumes Exclusions

Using the Writable Volumes exclusions feature, you can exclude specific locations of user Writable Volumes, such as file paths or registry keys, from being overwritten. Use this feature only if you are an IT administrator or an advanced App Volumes administrator. See "Writable Volume Exclusions," on page 53 for more information.

This chapter includes the following topics:

Create a Writable Volume

You can create Writable Volumes for computers and users to store user-specific data such as applications installed by a user, application settings, user profile, configuration settings, and licensing information.

You can create one Writable Volume per user or computer. The Writable Volume can migrate with the user. If you create a Writable Volume for a specific computer, you can reassign it to other computers.

Prerequisites

The account that you use to log in to the App Volumes Manager must have read access to the domains that you use with App Volumes, and these domains must be configured with two-way trust. See "User Accounts and Credentials," on page 17 for details.

Procedure

1 From the App Volumes Manager console, select **Volumes > Writables > Create Writable**.

2 Select an option for searching the Active Directory domains.

- From the **Domain** drop-down menu, select an Active Directory domain that is configured with App Volumes.
- Select the **Search all domains in the Active Directory forest** check box to search the entire Active Directory forest.

> **NOTE** Searching all domains in the forest might result in slow performance.

3 In the **Search Active Directory** text box, enter a search string to locate the entity to which you want to assign the Writable Volume.

You can search for individual users, computers, groups, or OUs. User Principal Name string searches (**`search_term@domain.local`**) and Down-Level Logon Name string searches (**`domain\search_string`**) are supported.

4 Click **Search**.

A list of search results appears.

Note If you are unable to locate the entity that you need, this might be because your account might not have read access to the domains where you search, or the domains are not configured with two-way trust.

5 Select the check box on the left of the entity for which you want to create Writable Volumes.

If you select a group or OU, individual Writable Volumes are created for each member of that group or OU. Group membership is discovered by using recursion, meaning that users and computers in subgroups also receive volumes. However, when creating Writable Volumes for OUs, groups are not recursed.

6 Select either the default datastore or a different datastore for the **Destination Storage**.

The default datastore is the datastore that you configured for storing the Writable Volumes.

If you select a different datastore, verify that you have the Writable Volumes templates on that datastore in the `cloudvolumes/writable_templates` folder.

7 Select the **Destination Path**.

8 Select a template for the new Writable Volume.

9 Configure the advanced options for the Writable Volume.

Option	Description
Prevent user login if the writable is in use on another computer	Ensure that the user does not log in to a computer to which their Writable Volume is not attached, because their local profile might interfere with their profile on the Writable Volume. This option is best used to protect users from logging in to persistent desktops without their Writable Volume. It is not needed when using non-persistent pools, because the computer is reverted to a clean snapshot before use.
Limit the attachment of users writables to specific computers	Enter the prefix to a computer name. When you provide such a prefix, the Writable Volume is attached only to a computer with a name that begins with the prefix. Use this setting for users who do not need to access their Writable Volume on all computers that they use. Additionally, some users might need separate Writable Volumes that are only attached to specific computers. For example, a user that has two Writable Volumes, one limited to Win7-Dev and another limited to Win7-Test. When the user logs in to the computer named Win7-Dev-021, the user gets the first volume. When the user logs in to Win7-Testing, the user gets the second volume. If the user logs in to Win2012R2, no Writable Volume is attached.
Delay writable creation for group/OU members until they log in	Delay the creation of Writable Volumes for group and OU members until their next login. This option only affects groups and OUs. Users and computer entities that were directly selected have their volumes created immediately. Use this option when you select a group or an OU. Often these containers can have hundreds or thousands of members. This can be problematic because creating many volumes at the same time might take a long time. Some members might not need a Writable Volume.

10 Click **Create**.

Import Writable Volumes

If you have Writable Volumes from another App Volumes deployment, you can import them to your current deployment.

Prerequisites

Provide access to the files of the Writable Volumes that you want to import in one of the following ways:

- Verify that your vCenter Server instance has access to the datastore where the Writable Volumes that you want to import reside.
- Copy the VMDK files of the Writable Volumes to a different folder on the datastore that you already use for Writable Volumes on your current App Volumes deployment.

Procedure

1 From the App Volumes Manager console, select **Volumes > Writables > Import Writables**.

2 Select the datastore and path from where you want to import and click **Import**.

What to do next

Click **Rescan** to update the list of Writable Volumes in the App Volumes Manager.

Update Writable Volumes

You can upload files to the Writable Volumes VMDKs and the files are added to the Writable Volumes the next time the user logs in to the desktop. You provide the files in a ZIP format. You cannot change any of the user-installed applications on Writable Volumes.

Note After a Writable Volume is updated, you cannot reverse the updates. To make changes, use an additional update to overwrite the files.

Prerequisites

- Create a ZIP file that contains the files that you want to upload. The ZIP file must be smaller than 5 MB.
- Place the file at the root of the Writable Volumes.

Procedure

1 From the App Volumes Manager console, select **Volumes > Writables > Update Writables**.

2 Browse and select the packaged file.

3 Click **Upload**.

Rescan Writable Volumes

To get the updated list of accessible Writable Volumes in your App Volumes deployment, you can rescan the datastore where the Writable Volumes VMDK files reside.

The rescan operation only checks for Writable Volumes that are already configured to this App Volumes Manager instance.

If new Writable Volumes are added to the datastore from a different App Volumes Manager or deployment, use the **Import** option so that the current App Volumes Manager detects them. See "Import Writable Volumes," on page 52 for details.

Procedure

- From the App Volumes Manager console, click **Rescan**.

If any of the Writable Volumes VMDK files are missing from the datastore or are corrupt, they appear as Detached under Writable Volumes in App Volumes Manager.

Expand a Writable Volume

You can specify a new size for a Writable Volume using the App Volumes Manager and App Volumes increases the `.vmdk` file to the new size.

Important You cannot expand a writable volume if your Machine Manager is configured as VHD In-Guest Services. This feature is available only on vCenter Server. See "Configuring a Machine Manager," on page 26 and "Set Up the Machine Manager Connection," on page 27.

Procedure

1. From the App Volumes Manager console, select **Volumes > Writables**.
2. Select a Writable Volume from the list.
3. Enter the new size for the volume and click **Expand**.

   You must enter a size that is at least 1 GB greater than the current size of the Writable Volume.

The Writable Volume file is expanded to the new size the next time the user logs in to the virtual machine.

Writable Volume Exclusions

You can specify certain locations of Writable Volumes to exclude them from being persisted across sessions or getting overwritten.

As an administrator, you might want to prevent automatic updates of some applications and prefer to update the AppStacks that contain these applications manually.

When applications are automatically updated, multiple copies of the files might get created since the applications are also stored on the Writable Volumes. The existing applications then either do not behave as desired or stop working completely. To prevent this behavior, you can apply Writable Volumes exclusions to specific locations and registry paths.

You can also specify exclusions to prevent certain folders such as temporary download folders, from accumulating huge, unwanted files.

Important The Writable Volumes exclusions feature is for advanced IT administrators or users who are aware of application behavior with App Volumes and want to tweak the way applications are managed or how Writable Volumes are used along with AppStacks.

Keep the following considerations in mind before you apply Writable Volumes exclusions:

- If the user modifies the locations that are excluded, the changes are lost when the user logs off the machine.
- You must be aware of the application behavior and the data that gets stored in the folders you want to exclude.
- Do not use generic locations such as `\REGISTRY\MACHINE\SOFTWARE` or `\Program Files(x86)\`. Using generic locations can cause all application updates to be erased.

Prerequisites

You must have administrator privileges on the machine where the App Volumes agent is installed.

Procedure

1 Log in as administrator to the machine where the App Volumes agent is installed.

2 Locate and open the writable volumes configuration file, `SnapVol.cfg`.

3 Add the following entry in the `SnapVol.cfg` file, where *path* is the location of the application or registry that you want to exclude: `exclude_uwv=path`

You can specify multiple exclusions.

Example: Exclude an Application Location

The following examples exclude the folder and registry location of Notepad++ from being overwritten during an update.

```
exclude_uwv_file=\Program Files (x86)\Notepad++
```

```
exclude_uvw_reg=\REGISTRY\MACHINE\SOFTWARE\Notepad++
```

What to do next

You must test the application after applying any Writable Volumes exclusions to ensure that the application works as desired.

Protecting Writable Volumes

App Volumes employs a default protection mechanism to prevent accidental deletion of attached VMDK volumes.

You can override this default protection by setting the *CV_NO_PROTECT* environment variable to *1*.

Caution With the *CV_NO_PROTECT=1* setting, there is no protection in place for volumes and might result in the loss of a user's Writable Volumes.

If you delete a VM, vSphere deletes any writable disks that are attached.

Note Do not use the *CV_NO_PROTECT* variable when App Volumes is configured to use Writable Volumes.

Configuring the *AVM_PROTECT_VOLUMES* Variable

The *AVM_PROTECT_VOLUMES* environment variable provides increased volume protection and logon performance by using the updated vSphere functionality. Setting *AVM_PROTECT_VOLUMES=1* enables support for vMotion and increases VMDK attachment performance.

Note Storage vMotion is not supported.

You can use *AVM_PROTECT_VOLUMES* only with the following versions of vSphere:

- 6.0 Update 1a (or newer)
- 5.5 Update 3b (or newer)

Note If you set *AVM_PROTECT_VOLUMES=1* on unsupported versions of ESX/ESXi on all hypervisors running App Volumes, it results in protection failures.

Upgrading App Volumes Components 8

You can upgrade your App Volumes 2.12 installation to the latest version of App Volumes, 2.12.1, without uninstalling your currently installed version.

Note You must upload the prepackaged templates again manually. See "Upgrade App Volumes Templates," on page 56 for more information.

This chapter includes the following topics:

Upgrade App Volumes Manager

Download and run the latest version of the App Volumes installer to upgrade your App Volumes Manager.

You can upgrade from App Volumes 2.12 to the latest version without uninstalling the 2.12 installation.

In earlier releases of App Volumes, you had to uninstall the App Volumes Manager installation on your machine before you could upgrade to the latest version. Thus App Volumes Manager configuration details and settings were not retained and you had to reconfigure them.

With the new upgrade feature, you can upgrade to the latest version without losing your settings.

Note If you want to upgrade from a version earlier than App Volumes 2.12, you must uninstall that version before installing the latest version.

Prerequisites

- Download the latest App Volumes installer from My VMware.
- Schedule a maintenance window to ensure that there is no service degradation during the upgrade process.
- Detach all volumes.
- In the Windows **Start** menu, open **Control Panel** and click **Administrative Tools > ODBC data source**. Note down the database and server name defined in the system ODBC source *svmanager*.
- Back up the App Volumes database using SQL Server tools.
- Create a full server back up or snapshot of the App Volumes Manager server.

Procedure

1 Log in as administrator on the machine where App Volumes Manager is installed.

2 Locate the App Volumes installer that you downloaded and double-click the `setup.exe` file.

3 Select the App Volumes Manager component and click **Install**.

A notification window with the upgrade process details is displayed.

4 Click **Next** to confirm the upgrade.

5 Click **Install** to begin the installation.

A Status Bar shows the progress of the installation. The installation process takes 5 to 10 minutes to complete. During this time, configuration information is first backed-up, new files are installed, and the configuration information is restored.

6 Click **Finish** to complete the installation.

App Volumes Manager is upgraded.

Note All certificates that you had previously configured are retained and you do not need to reconfigure them.

What to do next

Upgrade the App Volumes agent and templates. See "Upgrade App Volumes Templates," on page 56 and "Upgrade App Volumes Agent," on page 57.

Upgrade App Volumes Templates

You can upgrade all available templates from an ESXi host or upload new templates for AppStacks and writable volumes.

Prepackaged AppStacks or Writable Volumes templates are VMDK files typically located in `<user>/cloudvolumes/apps_templates/`.

Important If you have upgraded App Volumes from an earlier version, you must upload the prepackaged templates again manually. You cannot upgrade the templates by copying them directly to the storage location as the location is locked by App Volumes Manager to prevent accidental deletion of volumes. However, any user-defined custom templates are automatically carried over, and you do not have to upload them again.

Procedure

1 From the App Volumes Manager console, click **Configuration > Storage > Upload Prepackaged Volumes**.

2 Enter the ESXi host information and select the volumes you want to upload.

Option	Description
Storage	The storage location where the existing or new template is stored.
ESX Host	The name of the ESX host.
ESX Username	A user name used to log in to the ESX host.
ESX Password	The password for the user name.
Volumes	The prepackaged templates that you want to upload.

3 Click **Upload**.

Upgrade App Volumes Agent

You can upgrade the App Volumes agent to the latest available version, and if your current installed version is App Volumes 2.12, you do not need to uninstall it before upgrading.

You can also upgrade the agent silently. See "Upgrade App Volumes Agent Silently," on page 57.

Prerequisites

- Download the latest App Volumes installer from My VMware.
- Schedule a maintenance window to ensure that there is no service degradation during the uninstall and subsequent upgrade process.
- Upgrade the App Volumes Manager. See "Upgrade App Volumes Manager," on page 55.
- Unassign all AppStacks and writable volumes from the target computer where you plan to upgrade the agent.

Procedure

1 Log in as administrator on the machine where the App Volumes agent is installed.

2 Locate the App Volumes installer you have downloaded and run the `setup.exe` file.

3 Select the App Volumes agent component in the Installer window and click **Install**.

4 Click **Next** to begin the installation.

The installer backs up the configuration files and services.

5 Click **Finish** when you see the confirmation message.

Upgrade App Volumes Agent Silently

You can also upgrade the App Volumes agent silently using the Microsoft Windows Installer (MSI). If your current installed version is App Volumes 2.12, you do not need to uninstall it before upgrading.

You perform a silent upgrade using the command line and you do not need to use the App Volumes installer.

Prerequisites

- Schedule a maintenance window to ensure that there is no service degradation during the uninstall and subsequent upgrade process.
- Upgrade the App Volumes Manager. See "Upgrade App Volumes Manager," on page 55.
- Unassign all AppStacks from the target computer where you plan to upgrade the agent.

Procedure

1 Open a Windows command prompt on your machine.

2 Type the following command to upgrade the agent:

```
msiexec.exe /i "App Volumes Agent.msi" /qn REINSTALLMODE=vomus REINSTALL=ALL
```

Advanced App Volumes Configuration 9

The advanced configuration methods are for advanced users and administrators, who want to perform advanced configuration, configure scripting, and configure other variable settings.

You can configure App Volumes Manager by selecting configuration options such as batch script files, called at various points during system startup and login. You can also configure registry options for services, drivers, and other parameters.

This chapter includes the following topics:

Batch Script Files

App Volumes agent executes batch script files either when an AppStack or a Writable Volume is attached dynamically or at various points during system startup and login.

The baseline configuration is defined in the AppStack and writable volume template. Not all batch script files are present by default, only the scripts present on the volume are executed.

Note Script file names are case-sensitive.

Configure Batch File Timeouts

Batch files run serially and a new script does not start until an existing script has completed. You can configure a timeout to prevent a script from blocking login or logout processes.

Wait times are defined in seconds and can be configured by creating a corresponding registry value of REG_DWORD type under the following registry key:

```
HKLM\SYSTEM\CurrentControlSet\services\svservice\Parameters
```

Configuring SVdriver and SVservice

The App Volumes agent consists of two major components, SVdriver and SVservice. SVdriver is responsible for the virtualization of volumes into the OS and SVservice is responsible for communicating system events, such as computer startup, login, logout, and shutdown, with the App Volumes Manager.

You can configure SVidriver and SVservice with the following registry values.

Script Name	Triggers	Security Context	Wait Time Registry Parameter
prestartup.bat	Called when a volume is dynamically attached, or during system startup but before virtualization is activated.	System account	WaitPrestartup (default do not wait)
startup.bat	Called when a volume is dynamically attached, or when system starts up.	System account	WaitStartup (default do not wait)
startup_postsvc.bat	Called as and called after services have been started on the volume (not called if there are no services on volume).	System account	WaitStartupPostSvc (default do not wait)
logon.bat	Called when the user logs in and before Windows Explorer starts.	User account	WaitLogon (default wait until it finishes)
logon_postsvc.bat	Called after services have been started and not called if no services are running on volume.	User account	WaitLogonPostsvc (default do not wait)
shellstart.bat	Called when a volume is dynamically attached or when Windows Explorer starts.	User account	WaitShellstart (default do not wait)
shellstop.bat	Called when the user logs out before Windows Explorer is closed.	User account	WaitShellstop (default do not wait)
logoff.bat	Called when the user logs out and Windows Explorer is closed.	User account	WaitLogoff (default do not wait)
shutdown_presvc.bat	Called when the computer is shutting down before services are stopped.	System account	WaitShutdownPresvc (default do not wait)
shutdown.bat	Called when the computer is shutting down after services are stopped.	System account	WaitShutdown (default do not wait)
allvolattached.bat	Called after all volumes are processed. For example, if the user has 3 AppStacks, this is called after all 3 have loaded.	System account	WaitAllvolattached (default do not wait)
allvolattached_shellstarted.bat	Called after all volumes are processed and the user session is started.	User account	None
post_prov.bat	Called at the end of provisioning to perform any one-time steps required at the end of provisioning. Invoked when clicking the provisioning complete pop-up window while the volume is still virtualized.	System account	WaitPostProv (default wait forever)
prov_p2.bat	Called at phase 2 of the provisioning process after the machine is rebooted, but before App Volumes Manager has been notified that provisioning is complete. This is the last chance to perform any actions on the provisioned volume with virtualization disabled.	System account	WaitProvP2 (default wait forever)

Configuring the SVdriver Parameters

You can configure SVdriver with registry keys and optionally by configuring the values in the `HKLM\SYSTEM\CurrentControlSet\services\svdriver\Parameters` registry key.

Configure SVdriver with the following registry keys:

Registry Key	Type	Description
LogFileSizeInKB	REG_DWORD	Configure the size of the log file before rotating the log file. The default value is 51200 (50 MB).
ReorderTimeOutInSeconds	REG_DWORD	Configure the wait time for all volumes to be attached and processed based on Order Precedence set from within App Volumes Manager. The timeout is defined in seconds.
MinimizeReplication	REG_DWORD	Configure how changes are preserved in a writable volume. If this value is 1, only changes to data are preserved in a writable volume. If this value is 0, changes to data and file attributes (hidden, Read Only, and so on) permissions are preserved in writable volume.
EnableShortFileName	REG_DWORD	For legacy AppStacks created earlier than App Volumes 2.3, set this parameter to 0 to disable DOS short names.
EnableRegValueMerging	REG_DWORD	If this value is 1, merge certain registry values such as AppInitDlls across volumes. This action is additive across the volumes.
DriveLetterSettings	REG_DWORD	The value for DriveLetterSettings is in a hexadecimal format, and any number of flags might be combined to implement multiple parameters.

Configuring Drive Letter Settings

You can configure the App Volumes agent to interact with mapped volumes by using a system path to the volume, instead of mapping it to a drive letter.

Most modern applications are compatible with this behavior, but some applications might require a drive letter to access program or application files. To support such situations while maintaining the familiar user interface, App Volumes can hide the drive from Windows Explorer after it is mapped.

Configure this behaviour with the *DriveLetterSettings* registry value. The value for *DriveLetterSettings* is in a hexadecimal format, and any number of flags might be combined to implement multiple parameters. For example, if you want to use the 0x00000001 and 0x00000008 flags, the result is 0x00000009. Enter this as 9 because you only work with the significant digits.

Value	Description
0x0000001	DRIVELETTER_REMOVE_WRITABLE. Do not assign drive letter for writable volumes.
0x0000002	DRIVELETTER_REMOVE_READONLY. Do not assign drive letter for AppStack volumes.
0x0000004	DRIVELETTER_HIDE_WRITABLE. Hide drive letter for writable volumes.
0x0000008	DRIVELETTER_HIDE_READONLY. Hide drive letter for AppStack volumes.

The default registry value is 3. This means that for writable volumes, the drive letter is hidden, and for AppStackvolumes, the drive letter is not assigned.

Configuring the SVservice Parameters

You can SVservice configure with the following registry keys and optionally by configuring the values in the `HKLM\SYSTEM\CurrentControlSet\services\svservice\Parameters` registry key.

Parameter	Type	Description
`LogFileSizeInKB`	REG_DWORD	The size of the log file before rotating the log file. The default is 51200 (50MB).
`MaxDelayTimeOutS`	REG_DWORD	The maximum wait for a response from the App Volumes Manager, in seconds. If set to 0, the wait for response is forever. The default is 2 minutes.
`ResolveTimeOutMs`	REG_DWORD	Defined in milliseconds for name resolution. If resolution takes longer than the timeout value, the action is canceled. The default is 0, which waits for completion.
`ConnectTimeOutMs`	REG_DWORD	Defined in milliseconds for server connection requests. If a connection request takes longer than this timeout value, the request is canceled. The default is 10 seconds.
`SendTimeOutMs`	REG_DWORD	Defined in milliseconds for sending requests. If sending a request takes longer than this timeout value, the request is canceled. The default is 30 seconds.
`ReceiveTimeOutMs`	REG_DWORD	Defined in milliseconds to receive a response to a request. If a response takes longer than this timeout value, the request is canceled. The default is 5 minutes.
`ProvisioningCompleteTimeOut`	REG_DWORD	Defined in seconds to keep trying to contact the App Volumes Manager after provisioning is completed. The default is 120.
`DomainNameWaitTimeOut`	REG_DWORD	Defined in seconds how long to wait for the computer during startup to resolve Active Directory domain name. On machines that are not joined to any domain, you can set the value to 1 for faster login. The default is 60.
`WaitInstallFonts`	REG_DWORD	Defines how long to wait in seconds for fonts to be installed. The default is to not wait for completion.
`WaitUninstallFonts`	REG_DWORD	Defines how long to wait in seconds for fonts to be removed. The default is to not wait for completion.
`WaitForFirstVolumeOnlyValue`	REG_DWORD	Defined in seconds, only hold logon for the first volume. After the first volume is complete, the remaining are handled in the background, and the logon process is allowed to proceed. To wait for all volumes to load before releasing the logon process, set this value to 0. The default is 1.

Configuring the Volume Behavior Parameters

You can configure the volume behavior parameters for SVservice with the VolWaitTimeout, VolDelayLoadTime, and CleanSystemWritable registry keys.

Parameter	Type	Description
`VolWaitTimeout`	REG_DWORD	Defined in seconds. The time required for a volume to be processed before ignoring the volume and proceeding with the login process. The default value is 180.
`VolDelayLoadTime`	REG_DWORD	Defined in seconds. The time required after logon process to delay volume attachments. This value is ignored if a writable volume is used. You must attach writable volumes before attaching any AppStacks. If the value is greater than VolWaitTimeout, it will be reduced to the value of VolWaitTimeout. This might speed up the login time by delaying the virtualizing of applications until after logon is complete. The default value is 0 (do not delay load time).
`CleanSystemWritable`	REG_DWORD	If set to 1 and no writable volumes are attached, SVservice clears any changes saved to the system during operation after a reboot. If set to 0, changes are stored in `c:\SVROOT` on system volume. The default value is 0.

Configuring the General Behavior Parameters

You can configure the services, drivers, and general behavior parameters values for SVservice with the following registry keys.

Value	Type	Description
RebootAfterDetach	REG_DWORD	If set to 1, the system automatically reboots after a user logs off. The default is 0.
DisableAutoStartServices	REG_DWORD	If set to 1, services on volumes do not automatically start after attachment. The default is 0.
HidePopups	REG_DWORD	If set to 1, `svservice.exe` does not generate pop-up messages. The default is 0.
DisableRunKeys	REG_DWORD	If set to 1, applications in the `Run` key are not called. The default is 0.

Create a Custom vCenter Server Role

As a vCenter Server administrator, you can create a custom vCenter Server role and assign privileges to it.

A service account is used by the App Volumes Manager to communicate with vCenter Server. The default administrator role can be used for this service account, but you can create a vCenter Server role with certain privileges, specifically for the App Volumes service account.

You can also use PowerCLI to create a custom role. See "Create a Custom vCenter Server Role Using PowerCLI," on page 65.

Procedure

1 Manually create a new vCenter Server role.

2 Assign privileges to the role.

Object	Permission
Datastore	■ **Allocate space** ■ **Browse datastore** ■ **Low-level file operations** ■ **Remove file** ■ **Update virtual machine files**
Folder	■ **Create folder** ■ **Delete folder**
Global	**Cancel task**
Host	■ **Create virtual machine** ■ **Delete virtual machine** ■ **Reconfigure virtual machine**
Resource	**Assign virtual machine to resource pool**
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**
Interaction	■ **Power Off** ■ **Power On** ■ **Suspend**
Inventory	■ **Create from existing** ■ **Create new** ■ **Move** ■ **Register** ■ **Remove** ■ **Unregister**
Provisioning	■ **Clone template** ■ **Clone virtual machine** ■ **Create template from virtual machine** ■ **Customize** ■ **Deploy template** ■ **Mark as template** ■ **Mark as virtual machine** ■ **Modify customization specifications** ■ **Promote disks** ■ **Read customization specifications**

Create a Custom vCenter Server Role Using PowerCLI

You can create custom vCenter Server roles by using PowerCLI.

Procedure

1 Create a text file called `CV_role_ids.txt` and add the following content:

```
System.Anonymous
System.View
System.Read
Global.CancelTask
Folder.Create
Folder.Delete
Datastore.Browse
Datastore.DeleteFile
Datastore.FileManagement
Datastore.AllocateSpace
Datastore.UpdateVirtualMachineFiles
Host.Local.CreateVM
Host.Local.ReconfigVM
Host.Local.DeleteVM
VirtualMachine.Inventory.Create
VirtualMachine.Inventory.CreateFromExisting
VirtualMachine.Inventory.Register
VirtualMachine.Inventory.Delete
VirtualMachine.Inventory.Unregister
VirtualMachine.Inventory.Move
VirtualMachine.Interact.PowerOn
VirtualMachine.Interact.PowerOff
VirtualMachine.Interact.Suspend
VirtualMachine.Config.AddExistingDisk
VirtualMachine.Config.AddNewDisk
VirtualMachine.Config.RemoveDisk
VirtualMachine.Config.AddRemoveDevice
VirtualMachine.Config.Settings
VirtualMachine.Config.Resource
VirtualMachine.Provisioning.Customize
VirtualMachine.Provisioning.Clone
VirtualMachine.Provisioning.PromoteDisks
VirtualMachine.Provisioning.CreateTemplateFromVM
VirtualMachine.Provisioning.DeployTemplate
VirtualMachine.Provisioning.CloneTemplate
VirtualMachine.Provisioning.MarkAsTemplate
VirtualMachine.Provisioning.MarkAsVM
VirtualMachine.Provisioning.ReadCustSpecs
VirtualMachine.Provisioning.ModifyCustSpecs
Resource.AssignVMToPool
Task.Create
Sessions.TerminateSession
```

2 Modify the vCenter Server location in the following PowerShell script and run it:

The `CV_role_ids.txt` file must be in the same folder as the PowerShell script.

```
$cvRole = "App Volumes Role"
$cvRolePermFile = "CV_role_ids.txt"
$viSserver = "your-vcenter-server-FQDN"
Connect-VIServer -server $viServer
$cvRoleIds = @()
Get-Content $cvRolePermFile | Foreach-Object{
    $cvRoleIds += $_P
}
New-VIRole -name $cvRole -Privilege (Get-VIPrivilege -Server $viserver -id $cvRoleIds) -
Server $viserver
Set-VIRole -Role $cvRole -AddPrivilege (Get-VIPrivilege -Server $viserver -id $cvRoleIds) -
Server $viserver
```

Index