

VMware App Volumes Administration Guide

17 SEP 2019

VMware App Volumes 2.18

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

<https://docs.vmware.com/>

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

Copyright © 2019, 2020 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

About This Book 6

1 Configuring App Volumes Manager 7

- Verify License 7
- Configuring and Using Active Directory 8
 - Active Directory Domains Page 9
 - Connecting Securely to Active Directory 10
 - Adding and Configuring Domain Controller Hosts 11
 - Register an Active Directory Domain 12
 - Assigning and Managing Roles and Privileges 16
- Types of Hypervisor Connections and Machine Manager Configurations 21
 - Configure and Register the Machine Manager 23
- Configuring App Volumes Manager for VMware Cloud on AWS 25
- Configuring Security Protocols and Cipher Suites 26
 - Configure TLS Connections in App Volumes Manager 26
 - TLS v1.0 Protocol Communication 27
 - Configure Cipher Suites in App Volumes Manager 27
- Configuring Storage for AppStacks and Writable Volumes 28
 - Support for Shared Datastores 28
 - Configure Storage For AppStacks 29
 - Configure Storage for Writable Volumes 30
 - Upload Prepackaged Volumes 31
 - Configure VHD In-Guest Storage 32
- Configure Asynchronous Mounting on App Volumes Manager and Agent 32
 - Enable Asynchronous Mounting On The App Volumes Agent 33
 - Enable Asynchronous Mounting On App Volumes Manager 33
- App Volumes Manager Configuration Settings Page 34

2 Registering App Volumes Manager Server 37

- Register App Volumes Manager Server 37
- Remove an App Volumes Manager Server 38
- View Status of App Volumes Manager Servers 39
- Activate Registration Security 39

3 Using SSL Certificates with App Volumes Manager 40

- Configuring SSL Certificates for Machine Managers 40
 - Establishing a Secure SQL Server Connection 40
 - Establish a Secure vCenter Server Connection 41

Managing SSL Between App Volumes Manager and Agent	42
Replace the Self-Signed Certificate with CA-signed Certificate	42
Import Default Self-Signed Certificate	43
Disable SSL Certificate Validation in App Volumes Agent	44
Enable HTTP in App Volumes Manager	45
Disable SSL in App Volumes Agent	47
Check for SSL Certificate Revocation	48

4 Working with AppStacks 49

Creating and Provisioning AppStacks	50
Preparing a Provisioning Machine	50
Best Practices for Provisioning Virtual Machines and Applications	50
Create an AppStack	51
Provision An AppStack	52
Install Applications in AppStacks	53
Assigning and Attaching AppStacks	53
Limiting AppStack Attachments	55
Assign an AppStack to a User	55
Assign an AppStack to a Computer	56
Assign an AppStack to a Group	57
Assign an AppStack to an Organizational Unit (OU)	58
Edit an AppStack	58
Update an AppStack	59
Import AppStacks to App Volumes	60
Check Datastores for Available AppStacks	60
Unassign an AppStack	61
AppStacks Precedence	61
Delete AppStacks	62

5 Working with Writable Volumes 63

Assigning and Attaching Writable Volumes	65
Create a Writable Volume	66
Import Writable Volumes	69
Enable a Writable Volume	69
Update Writable Volumes	70
Edit a Writable Volume	70
Rescan Writable Volumes	71
Expand a Writable Volume	72
Reassign a Writable Volume to a Computer	72
Disable a Writable Volume	73
Delete a Writable Volume	73

Writable Volume Exclusions	74
Specify Exclusions in a Writable Volume	74
Move, Back Up, and Restore Writable Volumes	76
Move a Writable Volume	77
Back Up a Writable Volume	78
Restore a Writable Volume	80
Protecting Writable Volumes	81
6 Configure Infrastructure	83
View Managed Machines	83
View Managed Storage Locations	84
Configure Storage	84
Configure Storage Groups	85
7 Advanced App Volumes Configuration	87
Batch Script Files	87
Configure Batch File Timeouts	87
Configuring SVdriver and SVservice	88
Configuring the SVdriver Parameters	89
Configuring the SVservice Parameters	90
Create a Custom vCenter Server Role	92
Create a Custom vCenter Server Role Using PowerCLI	93
8 Troubleshooting App Volumes	95
Configure the Interval of Background Jobs	96
Background Jobs in App Volumes Manager	96
Create a Troubleshooting Archive	98
Remove a Troubleshooting Archive	98
Reduce App Volumes Login Time on Windows 10	99
Default Storage Location on the Storage Page in the App Volumes Manager UI Is Displayed as Not Configured	99

About This Book

The *VMware App Volumes Administration Guide* provides information on how to configure and use 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 configuring SSL certificates for App Volumes Manager, and creating and managing Writable Volumes and AppStacks.

See the *VMware App Volumes Installation Guide* for information about installing and upgrading App Volumes.

Intended Audience

This information is intended for experienced IT system administrators who are familiar with virtual machine technology and datacenter operations.

Configuring App Volumes Manager

1

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:

- [Verify License](#)
- [Configuring and Using Active Directory](#)
- [Types of Hypervisor Connections and Machine Manager Configurations](#)
- [Configuring App Volumes Manager for VMware Cloud on AWS](#)
- [Configuring Security Protocols and Cipher Suites](#)
- [Configuring Storage for AppStacks and Writable Volumes](#)
- [Configure Asynchronous Mounting on App Volumes Manager and Agent](#)
- [App Volumes Manager Configuration Settings Page](#)

Verify License

You must enter 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 **CONFIGURATION > 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.

Configuring and Using Active Directory

App Volumes uses Active Directory to add domains and 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.
- Connect securely to Active Directory and optionally, validate the certificate.

Active Directory Objects Lookup

App Volumes Manager looks up Active Directory objects by their GUID instead of UPN (User Principal Name). Using GUID enables administrators to 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 Manager 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.

Active Directory Synchronization

When a user is removed and the same user logon name is added again to Active Directory, and App Volumes has not yet synchronized the directory, conflicting Writable Volumes entries might get created. The conflicted entries are displayed in the App Volumes Manager until the Active Directory is synced.

When AppStacks or Writable Volumes are attached to a user who was removed and added again to the directory, the user is considered as a new Active Directory user, and only the assignments for this user are tracked and displayed. Any old assignments are removed (if the directory was synced) or are shown as conflicted entries.

Go to **DIRECTORY > Users > Sync** to synchronize and view the latest list of users.

Multiple Active Directories with Universal Security Groups

When multiple Active Directory domains are used with Universal Security Groups for AppStacks or Writable Volumes assignments, or for administrative access either directly or using nested group membership, all the domain controllers that are accessible by App Volumes Manager must host the Global Catalog (GC). In a default setup, this means all the domain controllers in the domain must have GC enabled. If this is not possible, configure specific domain controllers in the App Volumes Manager configuration. For more details, see the *User Security Attributes* section for Active Directories on the Microsoft Developer Network site.

Active Directory Domains Page

The Active Directory Domains page in the App Volumes Manager shows information about the configured domains and certificates and displays the list of configured domain controllers.

Navigate to **CONFIGURATION > AD Domains** to view following information about the configured domains:

- Active Directory Domain Name
- Netbios
- LDAP Base
- Username
- Security (secure or insecure communication and if certificate validation was skipped in case of secure communication)
- Port
- Domain Controllers
- Date and time of creation of the domain

Click **View DCs** to see information about the configured and discovered domain controller hosts:

- Name
- connection status

- Date and time the host last connected
- Date and time the connection failed
- Failure count

Connecting Securely to Active Directory

As an App Volumes administrator, you can choose to connect to Active Directory over a secure or insecure LDAP connection.

- Secure LDAP (LDAPS) - Connect to Active Directory over a dedicated LDAPS port. The default port number for LDAPS is 636. If you choose to validate the root certificate of the domain, you must have already downloaded the CA certificate. App Volumes uses this certificate to trust the connection.
- LDAP over TLS - Connect to Active Directory over TLS. The default port number for LDAP is 389. If you choose to validate the root certificate of the domain, you must have already downloaded the CA certificate. App Volumes uses this certificate to trust the connection.
- LDAP (insecure) - Connect to Active Directory over an insecure connection over plain LDAP.

Note The initial binding however, occurs over GSS-SPNEGO.

There is a new **Disable certificate validation(insecure)** checkbox that enables you to connect securely to Active Directory over LDAPS or LDAP over TLS without validating a domain certificate. Depending on whether you are upgrading from an older version of App Volumes, and if you had connected securely to Active Directory in your earlier installation of App Volumes, or if you are performing a fresh installation, the **Disable certificate validation(insecure)** box may be checked or unchecked in the latest version of App Volumes.

Note The **Disable certificate validation(insecure)** checkbox is visible only if you select LDAPS or LDAP over TLS.

Configure CA Certificates in App Volumes Manager

You must configure the root domain CA certificates if you want to connect securely to Active Directory and also validate the certificate.

Prerequisites

- You must have downloaded root certification authority (CA) certificates of the Active Directory domains. If the certificates are not in PEM (Base64 encoded) format, see the OpenSSL or similar documentation to convert the file to PEM format.

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

- In App Volumes Manager, domain controller host names that are specified in the domain controller hosts field must match the certificate host names.

Procedure

- 1 Ensure the name of the PEM formatted certificate file is `adCA.pem`.
- 2 On each App Volumes Manager server, copy the `adCA.pem` file to the `/config` directory where the App Volumes Manager is installed.

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

- 3 Restart the App Volumes Manager servers.

What to do next

Use App Volumes Manager to connect securely to Active Directory Connection using LDAP over SSL (LDAPS) or StartTLS (LDAP over TLS).

Adding and Configuring Domain Controller Hosts

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

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 becomes unavailable, then App Volumes Manager can perform a failover and switch to a different host. This redundancy ensures that App Volumes users are unaffected by the downtime and can continue their operations without interruption.

You can select 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 connects to the AD with the domain as the host. But the manager will continue to try to connect to one of the domain controllers in the list every 5 minutes. This process slows down the system.
- Connecting to domain controller using the domain as a host only works with LDAP(insecure). The connection will fail if you use LDAPS or "LDAP over TLS" with certificate validation.
- 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.
- Do not include non-ASCII characters in the domain controller name.
- Domain controllers in the same site always have higher priority over the DCs from different sites.

You can view the list of domain controllers and their connectivity status under **CONFIGURATION > AD Domains**.

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. You must set the time in minutes.

NTLM Authentication

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

Note Domain Controller failover is not supported for NTLM-based authentication. If the first available domain controller is down, then NTLM authentication fails. However, if the App Volumes agent logs out and logs in again, NTLM authentication will go through since the App Volumes manager again queries for the first available domain controller.

Disable Microsoft Windows NTLM Authentication

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](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.

Register an Active Directory Domain

Configure and register an Active Directory domain. You can assign applications to users, computers, groups, and organizational units (OUs) using Active Directory.

Prerequisites

- If you want to connect securely from App Volumes Manager to Active Directory using a LDAPS or LDAP over TLS connection, while also validating the certificate, you must have downloaded a CA domain certificate. See [Connecting Securely to Active Directory](#) and [Configure CA Certificates in App Volumes Manager](#) .
- You can also choose to connect securely using Secure LDAPS or LDAP over TLS without validating the certificate.

Procedure

- 1 From App Volumes Manager, go to **CONFIGURATION > AD Domains**.
- 2 Click **Register Domain**.
- 3 Enter the Active Directory information on the **Register Active Directory Domain** page.

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)	<p>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.</p> <p>Note Do not include any non-ASCII characters in the domain controller name.</p> <p>You can add multiple domain controller hosts; use commas to separate the names of the hosts.</p> <p>Important If you do not add a domain controller host, the system detects the hosts that are available and connect to the nearest domain controller.</p>
LDAP Base (Optional)	<p>Distinct 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.</p> <p>Example: OU=Engineering, DC=corp, DC=vmware, DC=com</p>
Username	The user name of the service account that has access to the target Active Directory domain. For example, <i>admin-1</i> . 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
Security	<p>Select one of the following options from the drop-down menu to configure the LDAP connection:</p> <ul style="list-style-type: none"> ■ Secure LDAP (LDAPS) - Select this box if you want to connect to Active Directory over SSL. ■ LDAP over TLS - Connect to Active Directory over LDAP using TLS. You must have installed a trusted certificate from a certificate authority. ■ (Optional) Disable certificate validation (insecure) - Displayed only if you choose LDAPS or LDAP over TLS. Check the box to connect securely without validating the certificate using the root CA certificate. ■ LDAP (insecure) - Connect to Active Directory without using a secure connection.
Port (Optional)	A port number other than the default. The default port is used if this text box is left blank.

4 Click **Register**.

Edit an Active Directory

You can update and change the configuration information for a registered Active Directory.

Procedure

1 From App Volumes Manager, go to **CONFIGURATION > AD Domains**.

A list of configured domains is displayed.

2 Select a domain from the list and click **Edit**.

3 Update the information on the **Edit Active Directory Domain** page.

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)	<p>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.</p> <p>You can add multiple domain controller hosts; use commas to separate the names of the hosts.</p> <p>Important If you do not add a domain controller host, the system detects the hosts that are available and connect to the nearest domain controller.</p>
LDAP Base (Optional)	<p>Distinct 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.</p> <p>Example: OU=Engineering, DC=corp, DC=vmware, DC=com</p>
Username	The user name of the service account that has access to the target Active Directory domain. For example, <i>admin-1</i> . The user can be an administrator with read-only permissions.

Parameter	Description
Password	The password for the service account. Ensure that domain policies do not enforce password expiration for the service account.
Security	<p>Select one of the following options from the drop-down menu to configure the LDAP connection:</p> <ul style="list-style-type: none"> ■ Secure LDAP (LDAPS) - Select this box if you want to connect to Active Directory over SSL. ■ LDAP over TLS - Connect to Active Directory over LDAP using TLS. You must have installed a trusted certificate from a certificate authority. ■ (Optional) Disable certificate validation (insecure) - Displayed only if you select LDAPS or LDAP over TLS. Select the box to connect securely without validating the certificate using the root CA certificate. ■ LDAP (insecure) - Connect to Active Directory without using a secure connection.
Port (Optional)	A port number other than the default. The default port is used if this text box is left blank.

4 Click **Update**.

Remove an Active Directory

Remove an Active Directory.

Procedure

- 1 From App Volumes Manager, go to **CONFIGURATION > AD Domains**.

A list of configured domains is displayed.

- 2 Select a domain from the list and click **Remove**.
- 3 Click **Remove** on the **Confirm Remove** window.

Handling Authentication Failures

App Volumes uses Active Directory to add domains and assign applications and Writable Volumes to users, groups, computers, and Organizational Units (OUs). App Volumes thus inherits the authentication and account policies of Active Directory.

Authentication Overview and Group Policy Settings

Active Directory implements authentication measures such as inserting random delays between failed authentications, configuring the number of failed authentication attempts and so on.

See <https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/windows-authentication-overview> for an authentication overview and [https://technet.microsoft.com/en-us/library/dn751050\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn751050(v=ws.11).aspx) for information about Group Policy Settings of Active Directory.

Assigning and Managing Roles and Privileges

You can assign built-in roles or custom roles to Active Directory groups. All users within the group will inherit the privileges that have been defined for the role.

You can assign the following built-in roles from the App Volumes Manager:

- Administrators - Has permission to perform all operations including adding and settings permissions for other administrators.
- AppStacks Administrators
 - Can perform all operations related to AppStacks such as create, import, rescan, update, and so on.
 - Has only viewing access to other resources such as Directory or Infrastructure.
 - Does not have access to Configuration or Writables resource.
- Administrators (Read only) - Can only view the resources but cannot make any modifications or perform other tasks.
- Security Administrators
 - Has permission to manage roles such as create, update, and delete custom roles.
 - Manage and change role assignments.
- Writables Administrators
 - Can perform all operations related to Writable Volumes such as create, import, update, back up, and so on.
 - Has only view access to other resources such as AppStacks, Directory, Infrastructure, Storage Groups and so on.
 - Does not have access to Configuration resource.

Note To view the privileges assigned to a role, go to **CONFIGURATION > Admin Roles > Manage Roles**, select a built-in role or a custom role, and click **Show**.

Custom Roles

Note the following about custom roles and assigning multiple roles.

- You can create custom roles with specific privileges and assign them to groups. Whenever privileges are changed for the custom roles, they are dynamically updated and the members of the group receive the updated privileges immediately.

- You can assign multiple roles to a group. In such a case, the group will get the union of the privileges of the different roles assigned to it.

Note

- When a new role is assigned to a group, the users of the group must log out and log in again to the system before they can get the privileges offered by the role.
 - When creating custom administrator roles, granting view privilege to either AppStacks or applications will effectively grant view privileges to both functions.
-

Administrators (Read only)

A read-only administrator can only view the resources and configuration information but cannot perform any other tasks. Specifically, a read-only administrator cannot perform the following functions:

- 1 Make configuration changes to the App Volumes Manager.
- 2 Create or import AppStacks.
- 3 Make storage configuration changes.
- 4 Add or remove Active Directory domains.
- 5 Add or remove Machine Managers.
- 6 Create, import, or update writable volumes.

A read-only administrator can be added only by an existing administrator who has complete access to the App Volumes Manager functionality.

As an administrator, you can add a read-only account to a group of users that belong to a particular domain. For example, if you have created a domain *xyz.com*, then you can create a read-only account belonging to the domain *xyz.com*.

Note You cannot create a read-only account for a single user.

Assign a Role

You can assign built-in or custom roles to Active Directory groups. All users of the group inherit the privileges offered by the role.

An Active Directory group can have more than one role assigned to it.

Prerequisites

You must have already added the member or group to the Active Directory database.

Procedure

- 1 From App Volumes Manager, click **CONFIGURATION > Admin Roles > Assign Role**.

- 2 Select the type of role you want to add from the drop-down menu. If you had previously added a custom role, the custom role is also displayed in the drop-menu.

Option	Description
Administrators	An administrator with access to all the functions in the App Volumes Manager.
AppStacks Administrators	An administrator to manage AppStacks.
Administrators (Read only)	An administrator who can only log in to App Volumes Manager and view the App Volumes configuration details. The read-only administrator cannot make any modifications.
Security Administrators	An administrator who can manage custom and built-in roles.
Writable Administrators	An administrator who can manage Writable Volumes.

- 3 Search the domain for the administrator or group that you want to add. Select **All** to search in all domains or select a specific domain from the drop-down menu.
- 4 Enter a string to search for the administrator in the configured Active Directory Groups and click **Search**.

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

You can also leave the search field blank and click **Search**. The complete list of groups is displayed.

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

A drop-down menu with a list of groups matching your search query is displayed.

- 5 Select the Active Directory group from the list.
- 6 Click **Assign**.

Results

The selected role is assigned to the group and you can view the updated list on the Administrator Roles page.

Update Assigned Roles for an Active Directory Group

Update the privileges for an Active Directory group by changing the assigned role. You can also select a new group and assign a role to the group.

If there is only group that is assigned the Administrators role, you cannot remove the Administrators role for that group. However, you can add other built-in or custom roles to the group.

Procedure

- 1 From App Volumes Manager, click **CONFIGURATION > Admin Roles**.

A list of groups and associated roles is displayed.

- 2 Select the group whose privileges you want to edit and click **Edit**.
- 3 Select a new role on the Administrator Roles page.
- 4 (Optional) If you want to change the group, search and select the new group.

The selected role is assigned to the new group, and the original role is unassigned from the current group.

- 5 Click **Update**.

Remove an Assigned Role

You can remove privileges from an Active Directory group by removing the role that was assigned to the group.

If only one group is assigned the Administrators role, you cannot remove that role since at least one administrator must be configured at all times.

Note If you remove a custom role that is assigned to a group, you are only removing the assignment of the role and not the role itself.

Procedure

- 1 From App Volumes Manager, go to **CONFIGURATION > Admin Roles**.
A list of groups and associated roles is displayed.
- 2 Select the group for which you want to remove the role and click **Remove**.
- 3 Confirm the removal and click **Remove**.

Manage Roles

View detailed information about the existing roles and edit a custom role.

Procedure

- 1 From App Volumes Manager, click **CONFIGURATION > Admin Roles > Manage Roles**.
A list of built-in roles and any custom roles that you have created is displayed.
- 2 Select the role and click **Show** to view information about the role.
The **Show** button is visible only after you select a role.
A description of the role and the privileges associated with the role is displayed.
- 3 (Optional) If you select a custom role, click **Edit** to edit the privileges of the role.

Create a Custom Role

If you do not want to use the built-in roles with the pre-assigned privileges, you can create custom roles where you select specific privileges and assign them to the Active directory groups.

For example, you can create a role that gives privileges to perform all actions on Writable Volumes (such as create, enable, disable, rescan, and so on) and also view the online directory of users. You can edit the privileges later and the updated privileges is dynamically allocated to the members of the assigned group. That is, the members do not have to log out and log in to the system to get the new privileges.

Procedure

- 1 From App Volumes Manager, click **CONFIGURATION > Admin Roles > Manage Roles**.

A list of roles that have been created is displayed.

- 2 Click **Create Custom Role** and provide the following information:

Option	Description
Name	Name of the role.
Description	A detailed description of the custom role.
Privileges	<p>Select the list of privileges you want to assign to the role from the following top-level categories. When a top-level privilege is selected, all the privileges under it are automatically assigned to a custom role. You can also choose specific privileges under a top-level privilege, and do not have to select all the privileges.</p> <ul style="list-style-type: none"> ■ Volumes ■ Directory ■ Infrastructure ■ Activity ■ Configuration <p>You can navigate down from each of the categories and choose individual privileges from the available subcategories.</p>

- 3 Click **Create**.

Results

The new role is displayed on the **Manage Roles** page.

Remove a Custom Role

You can remove any custom roles you created.

Prerequisites

Ensure that the custom role is not assigned to any group.

Procedure

- 1 From App Volumes Manager, click **CONFIGURATION > Admin Roles > Manage Roles**.

A list of groups and associated roles is displayed.

- 2 Select the custom role you want to remove and click **Remove**.

The **Remove** button is displayed only for a custom role. You cannot remove built-in roles, you can only see the privilege details pertaining to a built-in role.

- 3 Confirm the removal and click **Remove**.

Types of Hypervisor Connections and Machine Manager Configurations

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. See [Establish a Secure vCenter Server Connection](#) to learn how to set up a secure connection to vCenter Server.

Note If you are configuring App Volumes Manager on VMware Cloud on AWS, and you select vCenter Server as the hypervisor, you must check the **vCenter on VMware Cloud on AWS** option. See [Configuring App Volumes Manager for VMware Cloud on AWS](#) for more information.

Table 1-1. 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 .

Note 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.

Reconfigure vCenter Server

If you regenerate new certificates for ESXi hosts and you have selected vCenter Server as your machine manager, with the **Mount ESXi** option, you must reconfigure your vCenter Server.

See *Regenerate Certificates for an ESXi Host* section in the *VMware vSphere ESXi and vCenter Server 5 Documentation*.

vCenter Server Permissions

The following permissions are required if you are configuring a vCenter Server as the machine manager.

You also require these permissions if you choose the **Mount ESXi** option when you are configuring the machine manager.

Note Datastore browsing must be enabled for the App Volumes Manager to enumerate volumes on the datastore. Check the `enableHttpDatastoreAccess` parameter under `C:\ProgramData\VMware\VMware VirtualCenter\vpzd.cfg` in the vCenter Server. If it is set to false, change this to true and restart the vCenter Server service.

Permissions	
Datastore	<ul style="list-style-type: none"> ■ Allocate space ■ Browse datastore ■ Low level file operations ■ Remove file ■ Update virtual machine files
Global	Cancel task
Host	Local Operations -> Reconfigure virtual machine
	<p>Note</p> <ul style="list-style-type: none"> ■ Host permission is required when using the Mount ESXi option. ■ Mount ESXi option is not available for the VMware Cloud on AWS environment.
Sessions	View and stop sessions
	<p>Note This permission is not required for the VMware Cloud on AWS environment.</p>

Permissions	
Tasks	Create task
Virtual machine	<ul style="list-style-type: none"> ■ Configuration <ul style="list-style-type: none"> ■ Add existing disk ■ Add new disk ■ Add or remove device ■ Query unowned files ■ Change resource ■ Remove disk ■ Settings ■ Advanced ■ Inventory <ul style="list-style-type: none"> ■ Create new ■ Move ■ Register ■ Remove ■ Unregister ■ Provisioning <ul style="list-style-type: none"> ■ Promote disks

Configure and Register the Machine Manager

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.

Important If you are configuring a vCenter Server as the machine manager, ensure that you have the required vCenter Server permissions.

Procedure

- 1 From the App Volumes Manager console, click **CONFIGURATION > Machine Managers**.
- 2 Click **Register Machine Manager**.

3 Select and configure the type of machine manager.

Connection Type	Description
vCenter Server	Enter the host name, user name, and password details. If you select a vCenter Server instance as the first configured machine manager, you can add and configure additional servers. Note If the App Volumes Manager connects to the vCenter Server via an IPv6 connection, then you must provide the DNS of the vSphere as the host name.
ESXi (Single Host)	Enter the host name, user name, and password for the ESXi host.
VHD In-Guest	Does not require any credentials.

To view the permissions required by the service account, click **Required vCenter Permissions**.

4 Provide the following additional information:

Option	Description
Hostname	The host name of the Machine Manager. For example, server.your-domain.local . For App Volumes on VMware Cloud on AWS, the host name must be of the form <code>vcenter.sddc-xx.xxx-x-xx.vmc.vmware.com</code>
Username	The user name to access the machine. For example, <code>YOURDOMAIN\administrator</code> .
Password	The password for the user name.
Mount ESXi	When mounting, connect directly to ESXi servers. Note This option is not applicable for App Volumes on VMware Cloud on AWS.
Mount Local	Select this option if your VM's datastore has local copies of volumes and you want to mount the local copies.
Mount Queue	Select this option to queue requests to the VM host. Decreases the number of active connections to vCenter Server and ESXi. This results in increased performance and decreases the burden on the vCenter Server.
Mount Async	Wait for the mount request to complete in the background. Increases App Volumes Manager server throughput. Requires the Mount Queue option to be selected.
Mount Throttle	Limits the number of actively processing mount requests. Decreases load on the vCenter Server or ESXi servers. Requires the Mount Queue option to be selected.
Maximum number of concurrent mount operations per queue	The maximum number of concurrent mount operations per queue. Use the <code>servers</code> entry in <code>cLock.yml</code> to configure this field. Default value is 5. Note Each vCenter Server and ESXi server uses a separate queue for every manager process.

5 Click **Save**.

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

What to do next

See [Establish a Secure vCenter Server Connection](#) 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](#).

Configuring App Volumes Manager for VMware Cloud on AWS

You can configure App Volumes Manager on VMware Cloud on AWS. You can also transfer volumes using your vSphere Client to VMware Cloud on AWS.

Configure App Volumes Manager for VMware Cloud on AWS

- To configure App Volumes Manager for VMware Cloud on AWS, when configuring the machine manager, select vCenter Server as the hypervisor type and check the **vCenter on VMware Cloud on AWS** option. See the following links for configuring and registering a machine manager:
 - [Types of Hypervisor Connections and Machine Manager Configurations](#)
 - [Configure and Register the Machine Manager](#)
- After adding the vCenter SDDC machine manager, go to the Machine Managers tab, and click the "+" sign under the newly added machine manager to verify the details.
- Select the default storage as a Workload datastore and not as a vSAN datastore. You can edit the default storage settings under **CONFIGURATION > Storage**. See [Configuring Storage for AppStacks and Writable Volumes](#).

Transfer Writable Volumes from vSphere to VMware Cloud on AWS

You can transfer volumes using your vSphere client to the VMware Cloud on AWS environment in a two-step process:

For migration or Business Continuity Disaster Recover (BCDR) purposes, you can transfer your AppStacks or user Writable Volumes from On-Premises to the VMware Cloud on AWS environment using your vSphere client. This is a two-step process:

From the vSphere client:

- 1 Create a VM with thin provisioning and attach the volume that you want to transfer to the VM.
- 2 Select the VM and export it as an OVF template from **File > Export to OVF Template**.

From the VMware Cloud on AWS web client:

- 1 Click **Actions > Deploy OVF Template**.
- 2 Follow on-screen instructions and when you have to select the storage format, select **Thin provision**.

Once the VM is created, browse the datastore where the OVF was exported and move the VMDK file with its metadata to the `cloudvolumes` directory.

Ensure that you change the template location in the metadata file to point to the new datastore.

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 3 Using SSL Certificates with App Volumes Manager](#).

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;

...
}

```

TLS v1.0 Protocol Communication

TLS v1.0 protocol communications from App Volumes agents is disabled. All communication from the agent is done through TLS v1.1 and TLS v1.2 protocols.

App Volumes Manager can communicate with older agents only if the **Allow TLS v1.0 protocol (Not recommended)** box is selected. This box is deselected by default.

You can enable TLS v 1.0 support for App Volumes Manager during App Volumes Manager installation. Select the **Allow TLS v1.0 protocol (Not recommended)** box when you install App Volumes Manager. See the **Install App Volumes Manager** section in the *App Volumes Installation Guide*.

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.

Configuring Storage for AppStacks and Writable Volumes

You must specify the storage and template paths and select the type of storage for AppStacks and Writable Volumes before creating and using them.

Typically, the default storage path is `/cloudvolumes/writable`.

There are three types of storage templates available in App Volumes:

- Profile-only - Captures only the profile information of the users and does not include any configuration information related to user-installed applications in the Writable Volumes. The profile is delivered early in the boot process and considered only a local profile delivery. Additional profile tools like roaming profiles and VMware Dynamic Environment Manager still apply and work as expected. Use this template if a profile solution is not in place.
- UIA only - Captures all user-installed applications but does not capture any data that is written to the user profile. You can use this template with a third-party profile solution or VMware Dynamic Environment Manager.
- UIA+profile - Includes all user-installed applications and user profile data. The user profile data is only a local profile and is not a roaming profile or other managed user profiles.

You must specify the type of template when you create a volume or when you upload prepackaged volumes.

Note User profile exclusions are not supported with computer-based Writable Volumes which are attached during computer startup.

Support for Shared Datastores

App Volumes Manager is now aware of the shared physical datastores (storage) across multiple vCenter Servers that are used to connect to the datastore.

What Is a Shared Datastore

A shared datastore or location is a physical datastore that is connected to different vCenter Servers, and visible across the vCenter Servers. The datastore is identified based on the UUID of the filesystem.

A non-shared datastore, by contrast is not visible across multiple vCenter Servers. This storage might be a local storage or a LUN accessible to only one vCenter Server.

You can view a list of all the shared physical datastores from App Volumes Manager.

Identifying a Shared Datastore

You can identify a shared datastore by a unique identifier such as UUID. From App Volumes Manager, go to **INFRASTRUCTURE > Storages** and click the "+" sign next to a storage LUN. The UUID, the number of shared locations, and a link to the list of shared locations is displayed at the bottom of the description. Click the link to view the location information in a pop-up window.

Writable Volumes and Shared Datastores

When you import Writable Volumes, any Writable Volumes that are present in a shared datastore are considered to be the same Writable Volumes but from different locations. For example, when a Writable Volume is available from multiple vCenter Servers, the volume is not considered as a duplicate.

When a Writable Volume is created in a datastore, it gets created in all shared locations.

When a user logs in to a desktop, any Writable Volume that is assigned to the user can be attached from a shared datastore provided the location is reachable.

You must have a shared datastore between the source and destination vCenter Server to move and back up volumes across different vCenter Servers and if the source volumes are located in a non-shared datastore.

To back up a Writable Volume across different vCenter Servers, with the volume located in a non-shared datastore, you must first move the volume to a shared datastore, and then back up the volume to the destination datastore.

Supported Datastores

The following datastores types are supported:

- VMFS (version 3, 5, and 6)
- NFS (version 3 and 4.1)

Note When using an NFS datastore, if the same version of the datastore is not used to mount in all the vCenter Servers, then those storage locations are not considered as shared locations.

Configure Storage For AppStacks

You can configure storage for AppStacks by selecting the default storage locations and paths.

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](#).

Note Ensure that the paths for the default locations and the templates are separate from each other.

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, click **CONFIGURATION > Storage**.

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

- 2 Enter the default storage information for AppStacks:

Option	Description
Default Storage Location	Storage Location in VC
Default Storage Path	For example, /cloudvolumes/apps
Templates Path	For example,/cloudvolumes/writable_templates

- 3 Confirm your storage settings and click **Save**.

- 4 On the Confirm Storage Settings window, choose when you want to import the volumes:

- **Import volumes in the background** - App Volumes Manager dispatches a background job to import the volume and the display goes back to the manager console immediately.
- **Import volumes immediately** - App Volumes Manager waits for the import to be completed and the console is not responsive until either the process is complete or 10 minutes have elapsed.

Configure Storage for Writable Volumes

Configure storage for Writable Volumes by selecting the default storage locations and paths.

Note If local host storage is used, volumes are attached only for virtual machines on that host.

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, click **CONFIGURATION > Storage**.

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

2 Enter the following information:

Option	Description
Default Storage Location	Storage Location in VC
Default Storage Path	For example, /cloudvolumes/writable
Templates Path	For example, /cloudvolumes/writable_templates
Default Backup Path	For example, /cloudvolumes/writable_backup

3 Confirm your storage settings and click **Save**.

4 On the Confirm Storage Settings window, choose when you want to import the volumes:

- **Import volumes in the background** - App Volumes Manager dispatches a background job to import the volume and the display goes back to the manager console immediately.
- **Import volumes immediately** - App Volumes Manager waits for the import to be completed and the console is not responsive until either the process is complete or 10 minutes have elapsed.

Upload Prepackaged Volumes

Upload the volumes packaged with your instance of App Volumes Manager to the selected datastore.

There are three types of templates available in App Volumes. See [Configuring Storage for AppStacks and Writable Volumes](#) for a description of the templates.

Prerequisites

You must know the details and login credentials of the ESX host to which you want to upload the volumes.

Procedure

1 From the App Volumes Manager, click **CONFIGURATION > Storage**.

2 Provide the following storage and ESX information:

Option	Description
Storage	Select a storage location from the drop-down menu.
ESX Host	Select a host from the drop-down menu.
ESX Username	User name for the ESX host.
ESX Password	Password for the user to log in to the ESX host.
Volumes	Select a source template for the volumes to be uploaded. Select from the following templates: <ul style="list-style-type: none"> ■ Profile-only ■ UIA only ■ UIA + Profile

- 3 Click **Upload**.
- 4 Confirm the upload on the **Confirm Upload Prepackaged Volumes** window and click **Upload**.

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 1-2. 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	None
Note Write permissions are required by Agents when Dynamic Permissions are not enabled.			
writable_templates	Read	None	None

Configure Asynchronous Mounting on App Volumes Manager and Agent

You can configure asynchronous mounting on App Volumes Manager and agent to enable App Volumes Manager to handle a large number of login requests within a short time and improve scalability.

When you attach Writable Volumes or AppStacks, the App Volumes Manager has to keep a number of HTTP connections open until the volumes are all mounted. When asynchronous mounting is enabled, App Volumes Manager does not have to wait until all the volumes are mounted and can handle other requests concurrently.

Important

- When you perform a fresh installation of App Volumes, by default, asynchronous mounting is enabled on both the App Volumes Manager and agent .
- If this setting is disabled for any reason, such as, when you upgrade App Volumes, you must change the settings on both the App Volumes Manager and the agent to enable it.

Enable Asynchronous Mounting On The App Volumes Agent

Enable asynchronous mounting on the App Volumes agent.

The asynchronous mount setting is enabled by default. If it has been disabled for any reason, follow the instructions below to enable this setting.

You can also change the default time (30 seconds) the agent takes to send the mount status requests to the manager.

Procedure

- 1 Log in as administrator where the App Volumes agent is installed and change the registry key settings.

Registry Setting	Value
Path	HKLM\SYSTEM\CurrentControlSet\Services\svservice\Parameters
Key	Asyncmount
Type	DWORD
Value	1

- 2 (Optional) Change the default time (30 seconds) the agent takes to send the mount status requests to the manager.

Option	Description
Path	HKLM\SYSTEM\CurrentControlSet\Services\svservice\Parameters
Key	VolMountConfirmationReqFrequency
Type	DWORD
Value	new-time-in-seconds

Enable Asynchronous Mounting On App Volumes Manager

Enable asynchronous mounting on App Volumes Manager.

The asynchronous mount setting is enabled by default. If it has been disabled for any reason, follow the instructions below to enable this setting on the App Volumes Manager.

Procedure

- 1 Log in as administrator to App Volumes Manager.
- 2 Set the environment variable `AVM_ALLOW_ASYNC_MOUNT` to 1.

App Volumes Manager Configuration Settings Page

You can configure some of the settings directly from the Settings page, and others through the environment variables.

Configuration Settings

Go to **CONFIGURATION > Settings** to view and edit the settings.

Type	Value	Description
General Settings	UI Session Timeout	The number of seconds App Volumes Manager remains active after the user logs in. The default value is 30 minutes. Set via the system environment variable <code>SESSION_TIMEOUT</code> .
General Settings	Certificate Authority File	Path of the certificate file used by machine managers. Set via the system environment variable <code>SSL_CERT_FILE</code> .
Volume Mounting	API Mounting	Enable the user to log in even if a Writable Volume or an AppStack cannot be attached to the user at the time of login. Set via the system environment variable <code>AVM_ALLOW_API_MOUNT</code> (or <code>CV_ALLOW_API_MOUNT</code>).
Writable Volumes	Delete Protection	Protect volumes from getting deleted directly from storage. Set via the system environment variable <code>AVM_NO_PROTECT</code> (or <code>CV_NO_PROTECT</code>).

Type	Value	Description
Writable Volumes	Force Reboot on Error	<p>If a Writable Volume is assigned to a user, and the volume does not get attached to the user, the user has the option to reboot the machine. Set via the system environment variable <code>AVM_WRITABLE_REBOOT</code>.</p> <p>Note The <code>AVM_WRITABLE_REBOOT</code> does not apply to Writable Volumes conflicts. Writable Volumes conflicts are handled by the the Block user login setting. See Create a Writable Volume for information about this setting.</p>
Writable Volume Backups	Regular backups	<p>Toggle the slider to enable or disable regular backups for Writable Volumes. If enabled, Writable Volumes are backed up on a regular basis based on the recurrent interval. For example, if the recurrent interval is set to 7 days, a Writable Volume will be backed up if 7 days have elapsed since the last back up. Back up is only performed for Writable Volumes that have been used at least once since the last backup.</p>
Active Directory	Allow or Disallow	<p>The App Volumes Manager expects Computer and User accounts to be members of a registered Active Directory domain. Computer startups and user logins using local accounts are normally ignored.</p> <p>If non-domain entities are allowed, the Manager will create a record for local entities when they are first seen. That entity can then have AppStacks assigned to it from the Directory tab.</p>
Writable Volume Backups	Storage Location	<p>The location where the volumes are backed up. For example, <code>[xxx]AV-LUN</code>.</p>
Writable Volume Backups	Storage Path	<p>The folder name and path where the volumes are backed up. For example, <code>cloudvolumes/writable_volumes_backup</code></p>

Type	Value	Description
Advanced Settings	Disable Volume Cache	Toggle the slider to enable or disable volume cache. App Volumes caches AppStack or application objects to improve performance. However, if you experience increased memory usage, consider disabling volume caching.
Advanced Settings	Disable Token AD query	Toggle the slider to enable or disable token AD query. App Volumes queries for Active Directory group membership using cached object SIDs. Previous versions of App Volumes performed group membership queries against Active Directory domains directly and recursively. Disable token AD query to revert to the previous implementation.

Registering App Volumes Manager Server

2

When you install the latest version of App Volumes, the App Volumes Manager secure registration is automatically added.

When you add new App Volumes Manager servers to a fresh installation of App Volumes, you must register the newly added App Volumes Manager servers before you can use it. If it is a multi-manager setup, you must also register any existing manager servers.

If you have upgraded App Volumes from version 2.15 or earlier to the latest version, you can activate registration security for the upgraded App Volumes Manager.

This chapter includes the following topics:

- [Register App Volumes Manager Server](#)
- [Remove an App Volumes Manager Server](#)
- [View Status of App Volumes Manager Servers](#)
- [Activate Registration Security](#)

Register App Volumes Manager Server

In a multi-App Volumes Manager environment, after you upgrade App Volumes to the latest version, the first App Volumes Manager is automatically registered. You must then register other manager servers that are already in this environment. Any new manager servers that you add must also be registered.

Prerequisites

You must know the address of the registered and unregistered managers.

From the registered App Volumes Manager, go to **CONFIGURATION > Managers** to identify the unregistered managers.

Procedure

- 1 Enter the IP address of the unregistered manager server `https://<unregistered-avm-server-ip-address>/register` in a browser.

- 2 Log in to the unregistered manager with the username and password of the registered manager, and enter the following information:

Option	Description
Registered Manager Address	Address of the registered manager which also has the latest file encryption version. Note If the first App Volumes Manager is using an IPv6 connection, then you must enter the DNS of the App Volumes Manager.
Username	User name
Password	Password
Domain	Select a domain name from the drop-down menu.

If you added a manager server after upgrading App Volumes to the latest version, then you are automatically taken to the **Register App Volumes Manager Server** window.

- 3 Click **Register**.
- 4 Verify the certificate information and click **Accept** to accept the certificate.

You might see a **Untrusted Certificate** window, if the security certificate of the manager cannot not be verified. If you reject the certificate, you cannot proceed with the registration.

What to do next

Activate registration security for the App Volumes Manager instance that you just registered. Go to **CONFIGURATION > Managers** to see the updated status of the managers.

Remove an App Volumes Manager Server

Remove the record of an App Volumes Manager server that has become obsolete and is not in use.

You may want to remove an App Volumes Manager server if it has not been used for a while or if you are not sure if it is part of the manager servers cluster.

Prerequisites

You must have upgraded to or installed the latest version of App Volumes.

Procedure

- 1 From App Volumes Manager, go to **CONFIGURATION > Managers**.
A list of managers seen by this App Volumes instance is displayed.
- 2 Select the manager you want to remove and click **Remove**.
- 3 Confirm the action on the **Confirm Remove** window and click **Remove**.

Results

The record of the manager server is removed and is not seen under **CONFIGURATION > Managers**.

What to do next

You can retrieve the instance of the manager you removed. To do so, restart the App Volumes Manager service.

View Status of App Volumes Manager Servers

View the registration status of the App Volumes Manager servers.

Prerequisites

You must have upgraded to or installed the latest version of App Volumes.

Procedure

- ◆ From App Volumes Manager, go to **CONFIGURATION > Managers**.

Results

A list of manager servers with their registration status is displayed.

Activate Registration Security

After upgrading to the latest version, you can activate registration security for all servers known to this instance of App Volumes Manager.

Note Activating registration security is a one-time activity and applicable only to users upgrading from App Volumes 2.15 or earlier. This action is not required for a fresh installation of the latest version of App Volumes. You also do not need to perform this action after every App Volumes upgrade.

Prerequisites

You must have completed registration of all the manager servers for which you want to activate registration security.

Procedure

- 1 From App Volumes Manager, go to **CONFIGURATION > Managers**.

A list of App Volumes Manager servers visible to this instance of App Volumes is displayed.

- 2 Select the desired manager and click **Activate Registration Security**.
- 3 Confirm the activation and click **Activate**.

Using SSL Certificates with App Volumes Manager

3

App Volumes Manager uses SSL to communicate with Active Directory, Machine Managers, and App Volumes agents.

Using App Volumes Manager, you can perform a variety of tasks to configure and use SSL certificates. You can replace, import, disable, and manage the SSL certificates used for SSL communication and validation.

- You can configure Active Directory to reject connection with App Volumes Manager if SSL certificate validation fails. See [Configuring and Using Active Directory](#) .
- 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](#)
- [Managing SSL Between App Volumes Manager and Agent](#)

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

- Register a vCenter Server machine manager. See [Configure and Register the Machine Manager](#).
- 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 After you register a vCenter Server as a machine manager, 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.

- 2 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.

- 3 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.

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

Results

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](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](#).

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.

Results

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\svservice\Parameters.
- 4 Locate and set the EnforceSSLCertificateValidation key to 0.
The SSL certificate is no longer validated.
- 5 Restart the App Volumes service.

Results

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.

Results

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](#).

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.

Results

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](#).

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\svservice\Parameters.
- 4** Set the SSL key in the HKLM\System\CurrentControlSet\Services\svservice\Parameters path to 0.
- 5** Restart the App Volumes service.

Results

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

Check for SSL Certificate Revocation

You can configure the App Volumes agent to check if the SSL certificate used by a server to communicate with the agent is revoked or not.

App Volumes agents use SSL to communicate with App Volumes Manager and validate the certificate. By default, the App Volumes agent does not check if the SSL certificate that is used by the server to communicate with the agent is revoked or not. This can lead to decreased security in the form of persistent MITM attacks against the App Volumes agent.

Prerequisites

- You must have administrator privileges to the machine where the App Volumes agent is installed.
- SSL and SSL certificate validation must be enabled on the agent. If you have enabled HTTP on the manager, and disabled SSL on the agent, you cannot check for certificate revocation on the server.

Procedure

- 1 Log in as administrator to the machine where App Volumes agent is installed.
- 2 Run `regedit` to open the Windows registry settings, and select `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\svservice\Parameters`.
- 3 Select and set the *EnforceSSLCertificateRevocation* DWORD key to 1.

Note The *EnforceSSLCertificateRevocation* variable can be set only if the *EnforceSSLCertificateValidation* key is already enabled.

Results

If the SSL certificate is revoked on the server and SSL certificate revocation checking is enabled on the agent, the SSL connection between agent and manager is immediately terminated.

Working with AppStacks

4

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, provision, assign, update, edit, and delete, and manage AppStacks.

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

- 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.

You can have an AppStack assigned to a user and a computer concurrently. See [Assigning and Attaching AppStacks](#).

Note The App Volumes agent requires that Short File Name (SFN, aka 8dot3name) generation remain enabled for all volumes. This is the OS default. Microsoft recommends disabling SFN generation in some cases to improve performance. The App Volumes agent does not support this and any applications on the system volume or in an AppStack (especially applications belonging to the Microsoft Office Suite) may show unexpected behavior if SFNs are disabled.

This chapter includes the following topics:

- [Creating and Provisioning AppStacks](#)
- [Assigning and Attaching AppStacks](#)
- [Edit an AppStack](#)
- [Update an AppStack](#)
- [Import AppStacks to App Volumes](#)
- [Check Datastores for Available AppStacks](#)

- [Unassign an AppStack](#)
- [AppStacks Precedence](#)
- [Delete AppStacks](#)

Creating and Provisioning 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.

Note Applications installed by a non-admin user might not capture all application content. Administrators should make sure that only domain administrators or local administrators have the rights to capture applications on the provisioning VM.

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, click **Volumes > AppStack > Create AppStack**.
- 2 Enter the following information for the AppStack:

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 <code>appstacks2x_templates</code> and <code>writable_templates</code> file on the datastore is created during the initial setup process. You can change the path to further sub-categorize volumes. For example: <code>appvolumes/apps/your_folder</code> .

Option	Description
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.

3 Click **Create**.

4 Select one of the following options:

- Perform in the background - The creation takes place in the background and you can perform other tasks.
- Wait for completion - You cannot perform any other tasks until the AppStack is created.

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](#) and [Install Applications in AppStacks](#).
- You can limit the number of active attachments of the AppStack you created. See [Edit an AppStack](#).

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 it.

Prerequisites

Ensure that the AppStack you want to provision is not already provisioned. You can check the status of an AppStack on the AppStacks page under **Volumes > AppStacks**.

You cannot provision an AppStack on a computer that has a Writable Volume attached to it.

Procedure

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

A list of available AppStacks is displayed.

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

Note Check the Status column to ensure that

The **Provision AppStack:<AppStackName>** window is displayed.

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.
- 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* in the *App Volumes Installation Guide*.

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 to a User](#).

Note If you are installing Microsoft .NET Framework 2.0 or .NET Framework 3.5 on a Windows 10 machine, ensure that the application is enabled in the base and not in the AppStack. See the instructions on <https://docs.microsoft.com/en-us/dotnet/framework/install/dotnet-35-windows-10> to enable the .NET Framework 3.5 on Windows 10.

Assigning and Attaching AppStacks

You can assign AppStacks to a user, group, computer, or organizational unit (OU).

An AppStack can be either a user-assigned AppStack or a computer-based AppStack.

Note the following considerations when you assign an AppStack and a Writable Volume:

- If a user has a user-assigned AppStack and a Writable Volume, both are attached to the user.
- An AppStack that is assigned to a user does not get attached to the user if the user logs in to a computer that has a computer-based Writable Volume attached to it. However, if the Writable Volume is disabled, then the AppStack is attached to the user.
- If you assign an AppStack to a user, and the user logs in to a computer that has the same AppStack attached to it, then the user-assigned AppStack does not get attached to the user.
- You can set an attachment limit to an AppStack and limit the number of attachments. If you set an attachment limit of 1, and attach the AppStack to both a user and computer, the AppStack is attached to the computer. See [Limiting AppStack Attachments](#).
- You can attach an AppStack to a user and a computer concurrently even if auto-login is not enabled in the VM. The AppStack is attached to the user when the user logs in.
- If you have enabled the Allow non-domain entities feature, and then assign an AppStack to both a computer and a user, the AppStack is attached to the computer and not the user.
- You can allow AppStack attachments even if there is a Writable Volume conflict, such as when a volume is missing, for example.

Note This applies only to user Writable Volumes and not to system Writable Volumes.

AppStack Attachment Errors

If App Volumes Manager is unable to attach a AppStack or a Writable Volume to a user or computer, the App Volumes agent displays error messages. These messages are also displayed if the manager can attach the Writable Volume but the agent cannot access the file share (VHD configuration).

If the attachment is unsuccessful, all session data is lost and the user has to restart the session. The user can try to log in to a different VM and if the AppStack is available and attaches successfully, the user can continue with the operation.

App Volumes displays similar error messages when there are problems with attaching Writable Volumes. See [Assigning and Attaching Writable Volumes](#).

Important Due to LDAP limitations, App Volumes Manager does not support assignments that span multiple domains in the same forest. If you want to assign AppStacks to users through group membership, the user and the group that the user belongs to must be in the same domain, where the App Volumes Manager is deployed.

For example, if you assign an AppStack to a group in domain A, but a user of the group belongs to domain B, the AppStack does not get attached to the user.

However, you can assign AppStacks directly to the users in domain B, or if the group is also in domain B.

Limiting AppStack Attachments

You can limit the number of active attachments of an AppStack and configure each AppStack with the maximum number of concurrent assignments that are allowed.

Limiting attachments might be helpful when you want to enforce licensing constraints, for example.

You cannot set the attachment limit when you create an AppStack. After the AppStack is created, you can edit the AppStack to set this limit. See [Edit an AppStack](#).

Note the following considerations when you limit AppStack attachments:

- All applications that are captured within the selected AppStack are limited.
- If you want to enforce the limitation only for a specific application, the application must be captured separately and alone in an AppStack.
- If you reduce the attachment limit, the change is not reflected for the user until the user logs out and logs back in; no active attachment is removed when the limit is reduced.
- Similarly, if you increase the attachment limit, a user who was previously denied an AppStack attachment, will not receive the attachment until the user logs out and logs back in to the machine.

Assign an AppStack to a User

After you create and provision an AppStack, you can assign the AppStack to a user.

You can have an AppStack assigned to a user and computer at the same time. See [Assign an AppStack to a Computer](#).

Procedure

- 1 From the App Volumes Manager, go to **VOLUMES > AppStacks**.
A list of AppStacks are displayed.
- 2 Select an AppStack you want to assign.
- 3 Click **Assign..**
- 4 Search the Active Directory for users to assign to the selected AppStack.
 - a (Optional) Check the **Search all domains in the Active Directory Forest** to search all domains.
- 5 Select a user or users and click **Assign**.
You can assign an AppStack to multiple users at the same time.
- 6 (Optional) Select **Limit attachment of these assignments to specific computers**.
 - a If you want the selected AppStack to be attached only when the user logs into a specific computer, specify the prefix of the computer name.
- 7 Click **Assign**.

8 Select one of the following methods of assignment:

Option	Description
Attach AppStacks on next login or reboot	The AppStack is attached when the user logs in or reboots the machine.
Attach AppStacks 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.

Results

The list of users that AppStacks are attached to is displayed on the **Managed Users** page under **DIRECTORY > Users**.

What to do next

Go to **Volumes > Assignments** to view the complete list of AppStack assignments and manage them.

To assign another AppStack to the same user or users, go to **DIRECTORY > Users**, select the user from the list of Managed Users, and assign the AppStack.

Assign an AppStack to a Computer

After you create and provision an AppStack, you can assign the AppStack to a computer.

Note Real-time attachment of computer-assigned AppStacks works if the user who is logged in does not have any user or group attachments. (Writable or application)

Procedure

- 1 From the App Volumes Manager, go to **Directory > Computers**.
The **Managed Computers** page with a list of computers is displayed.
- 2 Select the computer for which you want to assign the AppStack.
Ensure that the status of the computer is set to Enabled.
- 3 Click **Assign AppStack**.
- 4 Select an available AppStack from the list.
- 5 (Optional) Select the **Detach on shutdown** if you want the assigned AppStack to be detached when the user logs off from the assigned computer.

6 Select one of the following methods of assignment:

Option	Description
Attach AppStack on next login or reboot	The AppStack is attached when the computer is started.
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

Go to **Volumes > Assignments** to view the complete list of AppStack assignments and manage them.

Assign an AppStack to a Group

After you create and provision an AppStack, you can assign the AppStack to a group.

Procedure

- 1 From the App Volumes Manager, go to **Directory > Groups**.
The **Managed groups** page with a list of groups is displayed.
- 2 Select the group for whom you want to assign the AppStack.
Ensure that the status of the group is set to Enabled.
- 3 Click **Assign AppStack**.
- 4 Select an available AppStack from the list.
- 5 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.
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

Go to **Volumes > Assignments** to view the complete list of AppStack assignments and manage them.

Assign an AppStack to an Organizational Unit (OU)

After you create and provision an AppStack, you can assign the AppStack to an organizational unit.

You can attach AppStacks to multiple OUs at the same time.

Note If you are adding an AppStack to an OU for the first time, you can assign the AppStack only from the **Volumes > AppStacks** tab. After selecting the AppStack you want to assign, you must search for and select the OU and then assign the AppStack.

Procedure

- 1 From the App Volumes Manager, go to **Directory > OrgUnits**.

The list of OUs is displayed. An OU is displayed only if it has been used at least once or assigned an AppStack.

- 2 Select an AppStack from the Assign AppStacks page.

Ensure that the AppStack is enabled.

- 3 Click **Assign AppStack**.

- a (Optional) Check the **Limit attachment of these assignments to specific computers** and specify the computer name or prefix to which you want to assign the AppStack.

You can specify a particular computer name or prefix so that the AppStack is assigned only to the specified computers.

- b Click **Assign** and select one of the following methods:

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.

- 4 Click **Assign**.

What to do next

Go to **Volumes > Assignments** to view the complete list of AppStack assignments and manage them.

Edit an AppStack

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

The *Filename* and the *Path* variables are set when the AppStack is created and cannot be updated.

Important When you specify a limit for the number of attachments for an AppStack, all applications that are captured within the AppStack are limited by this number. If you want to enforce an attachment limit for a single application, that application has to be captured separately in a separate AppStack.

Prerequisites

Ensure that the AppStack you want to edit is provisioned. See [Provision An AppStack](#).

Procedure

- 1 From the App Volumes Manager console, go to **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**.
- 4 (Optional) Check the **Limit Attachments** box to limit the number of active attachments for the AppStack.

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 that are installed in it.

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 that you want to update.
To select the AppStack, you can simply click on the AppStack, or select the checkbox next to it.
- 3 Click Update.
- 4 Enter the information you want to update 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 [Creating and Provisioning AppStacks](#).

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**.

Results

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.

Unassign an AppStack

You can unassign an AppStack that you have assigned to a user, group, computer, or organizational unit (OU).

Procedure

- 1 From App Volumes Manager, go to **Volumes > AppStacks**.
- 2 Select an AppStack that is assigned.

Select an AppStack to view the assignment details. You can also see if the AppStack is assigned and the number of assignments in the Assigned column.
- 3 Click **Unassign**.
- 4 Select the entity from which you want to unassign the AppStack and click **Unassign**.
- 5 On the **Confirm Unassign** window, select one of the following methods to unassign the AppStack:

Option	Description
Detach AppStack on next logout or reboot	The AppStack is unassigned when the user logs in or restarts the machine.
Detach AppStack immediately	The volume is detached instantly to all computers on which the selected users are logged in. If you are unassigning the AppStack from a group or organizational unit, it will be detached from all users or computers in that group immediately.

- 6 Click **Unassign**.

AppStacks Precedence

When multiple AppStacks that share common components are assigned to a machine, you can reorder the AppStacks to give priority to one AppStack over the others. Override precedence provides the ability to designate attachment priority for entities who have multiple AppStacks assigned to them.

You can reorder AppStacks provisioned with App Volumes 2.5 or later.

If you have multiple AppStacks assigned to an entity, you can use the precedence rules and the Override Precedence feature to assign priority to the AppStacks.

- Direct assignments to a user takes precedence over group or Organization Unit(OU) assignments.
- Assignments to a group take precedence over Organization Unit(OU) assignments.
- If a user is a member of multiple groups or OUs and the same AppStack is assigned to those multiple groups or OUs at different priorities, then the Override Precedence attachment priority is not guaranteed. Only the priorities within one group or OU are assured, but attachments from assignments of the other groups or OUs may be mixed in that ordering.

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

5

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. A Writable Volume is assigned to a specific user and becomes available to the user from any machine.

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 attach only one Writable Volume at a time per-user per OS. For example, if a user logs into a Windows 7 machine and a Windows 10 machine at the same time, one volume is attached to the user on Windows 7 and another one on Windows 10.

A Writable Volume can contain data such as application settings, user profile, licensing information, configuration files, and user-installed applications.

Using App Volumes Manager, you can create, import, edit, expand, and disable Writable Volumes.

Writable Volumes with User Environment Management Solutions

You can use Writable Volumes to complement a user environment management solution such as VMware Dynamic 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.

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.

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 how 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 and Shared Datastores

You can create, import, and attach Writable Volumes from shared datastores. See [Support for Shared Datastores](#).

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. The exclusions do not affect AppStacks or system volumes. See [Specify Exclusions in a Writable Volume](#) for more information.

Move, Backup, and Restore Writable Volumes

You can move Writable Volumes from one storage to another. You can also take backups of the volumes and restore them. See [Move, Back Up, and Restore Writable Volumes](#).

This chapter includes the following topics:

- [Assigning and Attaching Writable Volumes](#)
- [Create a Writable Volume](#)
- [Import Writable Volumes](#)
- [Enable a Writable Volume](#)
- [Update Writable Volumes](#)
- [Edit a Writable Volume](#)
- [Rescan Writable Volumes](#)
- [Expand a Writable Volume](#)
- [Reassign a Writable Volume to a Computer](#)
- [Disable a Writable Volume](#)
- [Delete a Writable Volume](#)

- [Writable Volume Exclusions](#)
- [Move, Back Up, and Restore Writable Volumes](#)
- [Protecting Writable Volumes](#)

Assigning and Attaching Writable Volumes

You can assign Writable Volumes to a user, group, computer, or organizational unit (OU).

Note the following considerations and limitations when you assign and attach Writable Volumes:

- When a Writable Volume is created for a user, it is assigned to the user immediately. When the volume is assigned to a group, it is created when a user belonging to the assigned group logs in to the machine.
- A user can have more than one Writable Volume attached at the same time if the volume is OS-specific, or created for a computer with a specific prefix. For example, suppose that you create a Writable Volume for each of the following:
 - A Windows 7 machine
 - A Windows 10 machine
 - A computer with Win2012-dev prefix to its name
 - A computer with Win2012-test prefix to its name

Then, when the user logs in to these different machines at the same time, each Writable Volume that is assigned to the specific machine is attached to the user at the same time.

- A machine can have only one Writable Volume attached to it at a given point in time.
- A Writable Volume must be enabled before it can be attached. See [Enable a Writable Volume](#).
- Automatic Windows updates must be disabled.
- Detach the volume before performing any update to the OS.
- Detach all Writable Volumes when performing any revert, recompose, or refresh of the virtual machines.

Note A user can also have multiple volumes attached to the same OS if there are two separate nodes and the user logs in to the desktop on both nodes.

Writable Volume Attachment Errors

If a Writable Volume that is assigned to a user or a computer does not attach correctly or if an assigned volume is running out of space, an error message is displayed and the user may have to restart the session.

The user may also see attachment errors when an assigned Writable Volume is disabled by the administrator or if the App Volumes agent is unable to access the volume due to permission issues, for example.

In such cases, the user can try to log in to a different VM and retry the operations. If the volume becomes available, the user can continue with the operations.

Similar errors are displayed if AppStacks are unable to get attached. See [Assigning and Attaching AppStacks](#).

Create a Writable Volume

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

Prerequisites

- Your account must have read access to the domains that you use with App Volumes, and the domains must be configured with two-way trust. See the *User Accounts and Credentials* section in the *VMware App Volumes Installation guide* for more information.
- If you are creating a Writable Volume for a group or OU, sync the users in the group or OU so that any changes to group or OU membership for the user are reflected in the App Volumes database. Go to **DIRECTORY > Users** and click **Sync** to see the updated list of users.

Procedure

- 1 From the App Volumes Manager console, select **Volumes > Writables > Create Writable**.
- 2 From the **Domain** drop-down menu, select a domain that is configured with App Volumes.
- 3 Enter a search string in the **Search Active Directory** text box domain 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. You can filter your search query by Contains, Begins, Ends, or Equals.

- a (Optional) Select the **Search all domains in the Active Directory forest** check box to search the entire Active Directory forest.
- 4 Click Search.

Searching all domains in the forest might result in slow performance.

If you are unable to locate the entity that you want, it your account might not have read access to the domains you are searching, or the domains are not configured with two-way trust.

5 Select the entity for which you want to create the Writable Volume.

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 Enter the destination storage and path, and the source template.

There are three types of templates available in App Volumes. See [Configuring Storage for AppStacks and Writable Volumes](#) for a description of the templates.

Option	Description
Destination Storage	Select either the default datastore or a different datastore. The default datastore is the one 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 <code>cloudvolumes/writable_templates</code> folder.
Destination Path	The default path is <code><varname>/cloudvolumes/writable</code> .
Source Template	<p>Select a source template from the drop-down menu for the new Writable Volume:</p> <ul style="list-style-type: none"> ■ Profile-only ■ UIA only ■ UIA+profile <p>Note If you select a UIA only or UIA+profile as a source template, you cannot later change this Writable Volume to a Profile-only template.</p>

- 7 (Optional) Select the appropriate box to configure additional settings for the Writable Volume.

Option	Description
Exception Resolution	<p>Select one of the options below to choose how to resolve login issues when Writable Volumes are unavailable for attachments:</p> <ul style="list-style-type: none"> ■ Disable virtualization and alert user - App Volumes disables all volume virtualization and an warning message is displayed when the user logs in. AppStacks can be attached even if volume is unavailable. <p>Note You can view the warning message under ACTIVITY > System Messages.</p> <ul style="list-style-type: none"> ■ Block user login - Use this setting to handle Writable Volumes conflicts. When there is a conflict due to a Writable Volume being attached elsewhere, App Volumes will prevent the user from logging into any additional computers. This will protect users from conflicts that arise when a local profile interferes with their profile on the Writable Volume. ■ Disable virtualization and alert user (errors only) - App Volumes agent will disable all volume virtualization and an alert will be displayed to the user of the desktop. This excludes conflicts stemming from users who have more than one active session at a time.
Limit the attachment of users writables to specific computers	<p>Use this setting for users who do not need to access their Writable Volume on all computers that they use. Also, some users might need separate Writable Volumes that are only attached to specific computers.</p> <p>For example, a user has two Writable Volumes assigned, 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.</p>
Delay writable creation for group/OU members until they log in	<p>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.</p> <p>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.</p>

- 8 Click **Create**.

- 9 On the **Confirm Create Writable Volumes** window, select when you want to create the selected volume:

- **Create volume in the background** - App Volumes Manager dispatches a background job to create the volume and the display goes back to the manager console immediately.
- **Create volume immediately** - App Volumes Manager waits for the volume to be created and the console is not responsive until either the process is complete or 10 minutes have elapsed.

What to do next

Confirm that the Writable Volume has been created for the user. From the App Volumes Manager console, select **Volumes > Writables** and verify that the volume you just created has the status set to Enabled.

Import Writable Volumes

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

Prerequisites

Ensure that you have access to the Writable Volumes that you want to import. You can verify access 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, select **Volumes > Writables > Import Writables**.
- 2 Select the datastore from the drop-down list.
- 3 Provide the path from where you want to import the Writable Volumes.
- 4 Click **Import**.
- 5 On the **Confirm Import Writable Volumes** window, choose when you want to import the selected volume:
 - **Import volumes in the background** - App Volumes Manager dispatches a background job to import the volume and the display goes back to the manager console immediately.
 - **Import volumes immediately** - App Volumes Manager waits for the import to be completed and the console is not responsive until either the process is complete or 10 minutes have elapsed.

What to do next

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

Enable a Writable Volume

You must enable a Writable Volume before you can attach it to a user or computer.

Prerequisites

Ensure that you have already created the volume you want to enable. See [Create a Writable Volume](#).

Procedure

- 1 From the App Volumes Manager, go to **Volumes > Writables**.
- 2 Select a Writable Volume and click **Enable**.

- 3 Click **Enable** on the **Confirm Enable** window.

What to do next

You can now assign the enabled volume to a user or computer.

Update Writable Volumes

You can upload ZIP files to the Writable Volumes VMDKs and update the volume. The uploaded files become available to the user the next time the user logs in to the desktop.

You cannot change any user-installed applications that are already in the Writable Volumes.

Note After a Writable Volume is updated, you cannot reverse the updates.

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 or any location that is accessible to the App Volumes Manager.

Procedure

- 1 From the App Volumes Manager console, select **Volumes > Writables > Update Writables**.
- 2 Browse and select the ZIP file.
- 3 Click **Upload**.

Edit a Writable Volume

You can edit some settings of a Writable Volume, such as specifying whether AppStack attachments should be allowed when volumes are unavailable, and limiting volume attachment to specific computers.

The Name, Filename, and Path text boxes are not editable.

Procedure

- 1 From App Volumes Manager, go to **Volumes > Writables**.
A list of entities is displayed.
- 2 Select the user or entity for whom you want to edit the Writable Volume.
A list of operations that can be performed on the volume is displayed.

3 Click **Edit** to update the available settings.

Option	Description
Exception Resolution	<p>Select one of the options to choose how to resolve login issues when Writable Volumes are unavailable for attachments:</p> <ul style="list-style-type: none"> ■ Disable virtualization and alert user - App Volumes disables all volume virtualization and the user sees an alert upon login. AppStacks can be attached even if volume is unavailable. <p>Note You can view the warning message under ACTIVITY > System Messages.</p> <ul style="list-style-type: none"> ■ Block user login - When there is a conflict due to a Writable Volume being attached elsewhere, App Volumes will prevent the user from logging into any additional computers. This will protect users from conflicts that arise when a local profile interferes with their profile on the Writable Volume. ■ Disable virtualization and alert user (errors only) - App Volumes agent will disable all volume virtualization and an alert will be displayed to the user of the desktop. This excludes conflicts stemming from users who have more than one active session at a time.
Prevent user login if the writable is in use on another computer	Select this option to ensure that the user does not log in to a computer to which their Writable Volume is not present. Using a desktop without an attached Writable Volume may result in the user working on a machine where the data is not saved to the Writable Volume.
Limit the attachment of users writables to specific computers	<p>Select this setting for users who do not need to access their Writable Volume on all computers that they use. Also, some users might need separate Writable Volumes that are only attached to specific computers.</p> <p>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.</p>
Description	Enter a description for the Writable Volume.
Operating System	<p>Select the additional OS for which you want to attach the Writable Volume.</p> <p>Note You cannot deselect the OS to which the volume was previously attached.</p> <p>Note If you select multiple operating systems, it might result in the volume becoming inoperable.</p>

4 Click **Save**.

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](#) for details.

Procedure

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

Results

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 [Types of Hypervisor Connections and Machine Manager Configurations](#) and [Configure and Register the Machine Manager](#).

Procedure

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

- 2 Select a Writable Volume from the list and click **Expand**.

A **Confirm Expand** window is displayed.

- 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.

Results

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

Reassign a Writable Volume to a Computer

If you want to rename a computer (entity) which has a Writable Volume assigned, then you must transfer the Writable Volume to another computer. You can perform the Writable Volume transfer by using the **Reassign** button, available in the **DIRECTORY > Computers** tab.

Only computer-owned Writable Volumes can be reassigned to another computer.

Prerequisites

Ensure that the computer selected for the reassign operation is in the Available status.

Procedure

- 1 In the App Volumes Manager UI, navigate to **DIRECTORY > Computers**.

- 2 On the **Managed Computers** page, identify and select the computer which has Writable Volumes that must be reassigned.
- 3 On the **entity_name** page, identify the Writable Volume that must be reassigned.
entity_name - name of the computer
- 4 Click **Reassign**.
- 5 To select a new computer, search the Active Directory.
If you used the **Search** button, a list of computers is displayed.
- 6 Select the computer to which the Writable Volume must be reassigned.
Status of the computer must be Available.
- 7 Click **Reassign**.
- 8 On the **Confirm reassign of Writable Volume** window, click **Reassign**.
- 9 To view the computer which has the reassigned Writable Volume, navigate to **DIRECTORY > Computers**.
The new computer is listed in the **Managed Computers** page.
Alternately, you can also view the computer listed as one of the entities on the Writable Volumes page in the **VOLUMES > Writables** tab.

Disable a Writable Volume

You can disable an assigned Writable Volume.

When you disable a Writable Volume, and the user does not have any other volumes on the datastore, the user will not have any volume attached.

A new Writable Volume will not be created to replace a disabled Writable Volume unless you have also deleted the volume from the datastore. In such a case, a new volume is created.

Prerequisites

Ensure that the Writable Volume you want to disable is enabled and assigned to a user or computer.

Procedure

- 1 From the App Volumes Manager, go to **Volumes > Writables**.
- 2 Select a Writable Volume and click **Disable**.
- 3 Click **Disable** on the **Confirm Disable** window.

Delete a Writable Volume

You can delete a Writable Volume.

A volume that is deleted is immediately detached from all computers. All associated data and settings are also deleted permanently.

Prerequisites

Ensure that the Writable Volume you want to delete is not in use by any user or computer.

Procedure

- 1 From the App Volumes Manager, go to **Volumes > Writables**.
- 2 Select a Writable Volume and click **Delete**.
- 3 Click **Delete** on the **Confirm Disable** window.

What to do next

If you chose to delete more than one volume, the deleted volume may still be displayed in the App Volumes Manager. Refresh the App Volumes Manager to see the updated list of available volumes.

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 might also want to specify exclusions for the following reasons:

- Prevent certain folders such as temporary download folders, from accumulating huge, unwanted files.
- Exclude certain applications or paths. You can do this by including paths within the users' profile directories.

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.

Specify Exclusions in a Writable Volume

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

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 know what application behavior and data will get 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.
- You can include paths within the users profile directories so that specific applications or files can be excluded from being captured.
- If the Writable Volume is UIA-only, all user profile paths are excluded and you do not have to explicitly specify any user profile paths for exclusion.

Note This feature is enabled by default and is applicable only when the Writable Volume is assigned.

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_file=path`
 - You can specify multiple exclusions.
 - While specifying user environment variables such as `%username%` and `%userprofile%` to exclude folders in `exclude_uwv_file`, the user profile must not be present on the base image.

Note When a user profile is specified to be excluded in `exclude_uwv_file` and if an existing user profile is present on the base image or the profile does not exist, the exclusions do not occur and appropriate error messages are logged in `svservice` logs.

The following messages are logged in `svservice`: `User profile already exists.` and `User environment variable policies will not be enforced.`

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_uwv_reg=\REGISTRY\MACHINE\SOFTWARE\Notepad++\`
- `exclude_uwv_file=\Users\%username%\folder\`
- `exclude_uwv_file=%userprofile%\folder\`

What to do next

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

Move, Back Up, and Restore Writable Volumes

You can move Writable Volumes from one storage to another. You can also take backups of the volumes and restore them.

You can back up a single volume, or multiple volumes, but you can only restore a single volume. You can also schedule App Volumes Manager to take regular backups of the Writable Volumes.

Note Storage Groups are not supported for the move, back up, and restore operations.

Thin Provisioning and Writable Volumes

If you move or back up a writable to a storage that does not support thin provisioning, the volume is expanded and becomes a flat VMDK on the destination storage. You can see the expanded size on the **Backup Writable** and **Move Writable** screens. For example, Move Writable Volume for *user1* – 400.00 MB (expanded: 10.00 GB)

If you restore a volume that is flat, it will remain flat, and will not get converted back to a sparse volume.

Using Shared Datastores for Writable Volumes Operations

You must have a shared datastore between the source and destination vCenter Server to move and back up volumes across different vCenter Servers and if the source volumes are located in a non-shared datastore.

To back up a Writable Volume across different vCenter Servers, with the volume located in a non-shared datastore, you must first move the volume to a shared datastore, and then back up the volume to the destination datastore.

See [Support for Shared Datastores](#) for information about shared datastores.

Moving a Large Number of Writable Volumes

If you are moving a large number of Writable Volumes, the operation could take a long time depending on the underlying infrastructure. You can reduce the time taken to move this large number of Writable Volumes by changing the default value of the `max_marshall_writable_jobs` and `marshal_writables_downtime` variables.

For example, if you want move 30 volumes in 6 minutes (360 seconds), set the following variables in the database settings table:

- `max_marshall_writable_jobs = 30`
- `marshal_writables_downtime = 6`

In the above case, it takes 12 seconds (360/30) to move each Writable Volume. However, the speed of the movement depends on the total size of the Writable Volume and the infrastructure configuration. The infrastructure includes the underlying datastore, target datastore, and network bandwidth. If the infrastructure does not support the speed set by the variables, the move jobs will pile up and will be completed in a time supported by the underlying infrastructure.

The actual time taken to complete the operation in the above example is also slightly more than 6 minutes since App Volumes might perform a refresh on the existing Writable Volumes or perform other sync jobs, while completing the move.

Therefore, set the values depending on the number of Writable Volumes to be moved and the underlying infrastructure.

Note The `worker_threads_count` variable also may need to be modified depending on your setting.

Move a Writable Volume

You can move a single Writable Volume or multiple volumes from one storage to another.

There are other considerations to note when you are moving multiple volumes:

- If the volumes are still attached at the time of the move, the move will occur after the volumes get detached.
- If you are moving multiple volumes, the move will always occur in the background.
- Other operations such as sync, refresh, or rescan of volumes have a higher priority than the move operation. As a result, if these operations are queued at the same time as the move operation, the time taken to move the volumes is affected.
- The time taken to move the volumes is also affected by the number of volumes. If you are moving a large number of volumes, the operation might take a long time. See [Move, Back Up, and Restore Writable Volumes](#).

Prerequisites

- Ensure that the source and destination storage are visible from the same vCenter Server.
- If you are moving a single volume and choose to move the volume immediately, ensure that the volume is detached.

Procedure

- 1 From App Volumes Manager, go to **VOLUMES > Writables**.

A list of users is displayed.

- 2 Select the volume or volumes you want to move.
- 3 Click **Move**.
- 4 On the **Move Writable Volume** page, provide the following information:

Option	Description
Destination Storage	Select a storage from the drop-down menu.
Destination Path	Enter the destination path.

The size of the destination storage and the expanded size (if thin provisioning is not supported) is displayed.

- 5 Click **Move**.
- 6 If you are moving a single volume, on the **Confirm Move Writable Volume** window, select when you want to move the selected volume:
 - **Move volumes in the background** - App Volumes Manager dispatches a background job to move the volume and the display goes back to the manager console immediately.
 - **Move volumes immediately** - App Volumes Manager waits for the move to be completed and the console is not responsive until either the process is complete or 10 minutes have elapsed.
- 7 Click **Move** to confirm.

Results

Go to **ACTIVITY > Activity Log** to see detailed information about the operation. Go to **ACTIVITY > System Messages** to see any warnings or error messages.

Back Up a Writable Volume

You can back up a single Writable Volume or multiple volumes from the App Volumes Manager.

If you choose to backup the volumes in the background, and they are still attached at the time of the back up, the back up will occur after the volumes get detached.

Note Multiple volumes can only be backed up as a background job.

You can also schedule regular backups in App Volumes Manager. See [Set Up Regular Writable Volumes Backups](#).

Prerequisites

If you are backing up a single volume and choose to back up the volume immediately, ensure that the volume is detached.

Procedure

- 1 In App Volumes Manager, go to **VOLUMES > Writables**.

- 2 Select the Writable Volume that you want to back up and click **Backup**.
- 3 On the **Backup Writable Volume** page, provide the following information:

Option	Description
Destination Storage	Select a storage from the drop-down menu.
Destination Path	Enter a path for the backup.

The size of the destination storage and the expanded size (if thin provisioning is not supported) is displayed.

- 4 (Optional) Select **Delete writable volumes after backup** if you want to delete the original Writable Volume after the back up is completed.

Important This operation cannot be undone.

- 5 Click **Backup**.
- 6 On the **Confirm Backup Writable Volumes** window, select when you want to back up the selected volume:
 - **Backup volume in the background** - App Volumes Manager dispatches a background job to back up the volume and the display goes back to the manager console immediately.
 - **Backup volume immediately** - App Volumes Manager waits for the backup to be completed and the console is not responsive until either the process is complete or 10 minutes have elapsed.
- 7 Click **Backup**.

Results

Go to **ACTIVITY > Activity Log** to see detailed information about the operation. Go to **ACTIVITY > System Messages** to see any warnings or error messages.

Set Up Regular Writable Volumes Backups

Set up App Volumes Manager to take regular backups of the Writable Volumes.

When a new volume is created and attached, the volume is backed up immediately. The next backup is only performed for volumes that have been used at least once since the last backup, and the duration is defined by the backup interval.

Procedure

- 1 From App Volumes Manager, go to **CONFIGURATION > Settings**.

- 2 Under **Writable Volume Backups**, provide the following information:

Option	Description
Regular Backups	Toggle the slider to enable regular backups. Enter the number of days (interval) after which you want to back up the volumes. Note The backup interval is defined as the time between the last back up and the number of days for the next backup, during which the volume was used. So, different volumes can be backed up on different days, even though the interval is the same.
Storage Location	Select a location from the drop-down menu.
Storage Path	Enter a default path for the volume backups.

- 3 Click **Save**.

Example: Back Up Volumes Every 3 Days

If the backup interval is set up for 3 days, and if a volume *Vol1* was backed up on Monday, the next back will occur on Thursday, if *Vol1* has been used between Monday and Thursday.

Now, if a new volume *Vol2* is created and attached on Tuesday, *Vol2* is backed up when the user logs off, and the next back up will occur on Friday, if *Vol2* is used between Tuesday and Friday.

Restore a Writable Volume

You can restore any single volume that was backed up. When you restore a volume, the existing volume is overwritten by default.

Prerequisites

Ensure that the volume you want to restore is detached.

Procedure

- 1 From the App Volumes Manager, go to **VOLUMES > Writables**.
A list of users is displayed.
- 2 Select the user for whom you want to restore the volume.
A list of actions that can be performed for the selected user is displayed on the right.
- 3 On the **Restore Writable** page, provide the following information:

Option	Description
Source Storage	Select a source storage from the drop-down menu.
Source Path	Enter the path from the volume is to be restored. The default path is /cloudvolumes/writable.

- 4 Click **Restore**.

5 On the **Confirm Restore Writable Volumes** window, select when you want to restore the selected volume:

- **Restore volume in the background** - App Volumes Manager dispatches a background job to restore the volume and the display goes back to the manager console immediately.
- **Restore volume immediately** - App Volumes Manager waits for the restore to be completed and the console is not responsive until either the process is complete or 10 minutes have elapsed.

Results

Go to **ACTIVITY > Activity Log** to see detailed information about the operation. Go to **ACTIVITY > System Messages** to see any warnings or error messages.

Note After a volume is restored, the volume ID of the restored volume is different since the original volume is either deleted or replaced. The activity logs do not display the new ID and the entity and target columns are shown as empty.

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.

Configure Infrastructure

6

You can view and configure App Volumes infrastructure elements such as machines, storage, and storage groups.

The App Volumes Manager periodically checks for and cleans-up machines and storage locations which do not exist on the vCenter Server.

This chapter includes the following topics:

- [View Managed Machines](#)
- [View Managed Storage Locations](#)
- [Configure Storage Groups](#)

View Managed Machines

You can view both existing and deleted machines that are seen and recognized by this instance of App Volumes Manager.

The App Volumes Manager periodically checks for and cleans-up machines and storage locations which do not exist on the vCenter Server. These cleaned-up machines and storage locations are marked as deleted in the App Volumes database.

Procedure

- 1 From App Volumes Manager, click **INFRASTRUCTURE > Machines**.
- 2 From the drop-down filter, select the required option.

Option	Description
Active Only	Lists existing machines in the App Volumes database.
Show All	Lists both existing and cleaned-up or deleted machines in the App Volumes database.

- 3 (Optional) If you have added or deleted any machine managers recently, click **Rescan** to view the latest list of machines.

View Managed Storage Locations

You can view the list of storage locations including shared datastores that are seen by this instance of App Volumes Manager.

The App Volumes Manager periodically checks for and cleans-up machines and storage locations which do not exist on the vCenter Server. These cleaned-up machines and storage locations are marked as deleted in the App Volumes database.

Procedure

- 1 From App Volumes Manager, click **INFRASTRUCTURE > Storages**.
- 2 From the drop-down filter, select the required option.

Option	Description
Active Only	Lists active datastores in the App Volumes database.
Show All	Lists both active and cleaned-up or deleted datastores in the App Volumes database.

- 3 Click the '+' sign next to a location to view the detailed information about the storage such as whether it is attachable, used and total storage available and so on.

The UUID, the number of shared locations, and a link to the list of shared locations is displayed at the bottom of the description. Click the link to view the location information in a pop-up window.

- 4 (Optional) If you have added or deleted any storage locations recently, click **Rescan** to view the latest list of locations.

Configure Storage

Manage storage groups by configuring the storage to make it attachable or non-attachable.

The list of storage locations and their status is displayed on the Managed Storage Locations page.

When you mark a storage as **Not Attachable**, the App Volumes Manager ignores the storage while mounting volumes.

For example, if you have set up two vCenter Server instances. Each instance can have a local storage and shared storage capability. You can mark the slower-performing storage as **Not Attachable**. A storage thus marked is ignored by the manager while mounting volumes and the storage can be used solely for replication of AppStacks.

Procedure

- 1 Click **INFRASTRUCTURE > Storages** to see the list of storage locations that are visible to the App Volumes Manager.

- 2 Click the storage whose status you want to change.

The Attachable and Status columns of the selected storage provide the relevant information.

- 3 Click **Make as Attachable** or **Make as Not Attachable** depending on the existing status of the storage.
- 4 Confirm the operation.

Results

The updated status is seen on the Managed Storage Locations page.

Configure Storage Groups

You can view and create storage groups using the App Volumes Manager.

You can define storage groups to automatically replicate AppStacks or distribute Writable Volumes across many datastores. They are also used to define a group of datastores that should all contain the same AppStacks. Some of the attributes for the group, such as template location and distribution strategy, only apply when using the group for distributing Writable Volumes. The distribution strategy setting controls how Writable Volumes are distributed across the group.

Procedure

- 1 Click **INFRASTRUCTURE > Storage Groups > Create Storage Group**

You can directly choose the storage to add or specify a name prefix to automatically add new matching storage.

- 2 Provide the following information:

Option	Description
Group Name	Name for the storage group.
Automation	<ul style="list-style-type: none"> ■ Select Automatically Import AppStacks to ■ Select Automatically Replicate AppStacks to
Distribution Strategy	Select how you want the files to be distributed: <ul style="list-style-type: none"> ■ Spread - Distribute files evenly across all the storage locations. When a file is created, the storage with the most available space is selected. ■ Round-robin - Distribute files by sequentially using the storage locations. When a file is created, the storage with the oldest used time is selected.
Template Storage	Select a storage location from the drop-down menu.
Storage Selection	<ul style="list-style-type: none"> ■ Direct - select from the list of storage options that are displayed. ■ Automatic - You can specify a storage name prefix to filter the options. Leave the Storage Name Prefix box blank to see all storage options.

- 3 Select a prefix for the storage name. Leave it blank to see all possible storage locations.

This field is visible only for Automatic storage selection.

- 4 Select a storage location to create a group for a specific location.

- 5 Click **Create**.
- 6 A list of locations that was selected is displayed. Confirm the operation and click **Create**..

Advanced App Volumes Configuration

7

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](#)
- [Configure Batch File Timeouts](#)
- [Configuring SVdriver and SVservice](#)
- [Create a Custom vCenter Server Role](#)
- [Create a Custom vCenter Server Role Using PowerCLI](#)

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 SVdriver 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

Script Name	Triggers	Security Context	Wait Time Registry Parameter
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 ApplnitDlls 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
0x00000001	DRIVELETTER_REMOVE_WRITABLE. Do not assign drive letter for writable volumes.
0x00000002	DRIVELETTER_REMOVE_READONLY. Do not assign drive letter for AppStack volumes.
0x00000004	DRIVELETTER_HIDE_WRITABLE. Hide drive letter for writable volumes.
0x00000008	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 configure SVservice with the following registry keys and optionally 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.

Parameter	Type	Description
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.
WaitForFirstVolumeOnly	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:\SVR00T 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](#).

Procedure

- 1 Manually create a new vCenter Server role.
- 2 Assign privileges to the role.

Object	Permission
Datastore	<ul style="list-style-type: none"> ■ Allocate space ■ Browse datastore ■ Low-level file operations ■ Remove file ■ Update virtual machine files
Folder	<ul style="list-style-type: none"> ■ Create folder ■ Delete folder
Global	Cancel task
Host	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Add existing disk ■ Add new disk ■ Add or remove device ■ Change resource ■ Remove disk ■ Settings
Interaction	<ul style="list-style-type: none"> ■ Power Off ■ Power On ■ Suspend

Object	Permission
Inventory	<ul style="list-style-type: none"> ■ Create from existing ■ Create new ■ Move ■ Register ■ Remove ■ Unregister
Provisioning	<ul style="list-style-type: none"> ■ 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"
$viserver = "your-vcenter-server-FQDN"
Connect-VIServer -server $viServer
$cvRoleIds = @()
Get-Content $cvRolePermFile | Foreach-Object{
    $cvRoleIds += $_
}
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

```

Troubleshooting App Volumes

8

You can view background jobs, system activity, server logs, and error messages, and create and download troubleshooting log files from the **ACTIVITY** tab in App Volumes Manager.

The ACTIVITY tab consists of the following subcategories:

- **Pending Actions** - Displays a list of actions waiting to be performed. The actions are processed in the background and are completed in the order they are submitted. Select the **Auto Refresh** box to automatically show the latest list of actions.
- **Jobs** - Displays a list of background jobs running in App Volumes Manager . Jobs run automatically at scheduled intervals. Users can configure these intervals.
- **Activity Log** - Displays information about user logins, computer power-ups, and volume attachments. System messages include messages and errors generated from internal events such as polling for domain controllers, Active Directory access, and so on.
- **System Messages** - Displays messages and errors generated from internal events such as volume attachment, Active Directory access, and so on.

If the administrator has opted to continue with application mounting despite a Writable Volume conflict, a warning message is displayed under **System Messages**, during AppStack for example.

- **Server Log** - Shows the end of the current log file with the option to refresh in real time. Click **Play** to view the logs in real time.
- **Troubleshooting Archives** - Archive and manage configuration settings and logs. You can create, download, and delete the archives.

This chapter includes the following topics:

- [Configure the Interval of Background Jobs](#)
- [Create a Troubleshooting Archive](#)
- [Remove a Troubleshooting Archive](#)
- [Reduce App Volumes Login Time on Windows 10](#)
- [Default Storage Location on the Storage Page in the App Volumes Manager UI Is Displayed as Not Configured](#)

Configure the Interval of Background Jobs

You can use the **Jobs** page to configure the intervals and downtime of a background job running in the App Volumes Manager. The ability to configure the interval and downtime helps ease background job queues.

You can also use the **Jobs** page to enable or disable a job depending on your requirements.

Interval

Interval is the time duration between successive running of each background job.

Downtime

Downtime is the duration for which the job does not run.

Note Use this feature only when there is a requirement in your environment.

Prerequisites

If you want to configure the **Interval** and **Downtime** of a job, ensure that you make a note of the default values.

Procedure

- 1 From the App Volumes Manager console, go to **ACTIVITY > Jobs** .
Background jobs running in the App Volumes Manager are displayed.
- 2 Identify the background job whose values you want to configure and click the **+** sign.
Background job details are displayed.
- 3 Depending on your requirements, configure the **Interval** and **Downtime** values.
Each job has default **Interval** and **Downtime** values.
- 4 Click **Save**.
- 5 To disable or enable a job, select the job and click **Enable** or **Disable** respectively.
By default, the status of a job is Enabled.

Background Jobs in App Volumes Manager

App Volumes Manager has jobs running in the background. These jobs perform a specific task and run automatically at scheduled intervals.

The following background jobs run within App Volumes Manager :

Import Storage Groups

Imports volumes from any Storage Group which has auto import configured.

Refresh Domains

Discovers and updates the state of domain controllers.

Audit Vms

Checks the virtual machine state and ensures that the attachments are in sync.

Collect Logs

Collects logs periodically.

Expire Sessions

Closes stale agent sessions and user-interface sessions that have been idle for more than 30 minutes.

Fulfill Writables

Checks Groups and Organizational Units (OUs) for new members and schedules creation of writable volumes for the new members.

License Extension

Checks for license extension.

Marshal Writables

Schedules jobs to marshal Writable Volumes

Refresh Attachments

Ensures that the volume for each attachment remains attached.

Refresh Computers

Ensures that the state of each computer is online.

Refresh Machines

Ensures that each virtual machine exists. Removes the virtual machines if they no longer exist and are not in use.

Remove Stale Storage Locations

Ensures that each storage location (datastore) is online and accessible. Removes stale storage locations that no longer exist in the vCenter and are no longer in use.

Replicate Storage Groups

Starts replication jobs for StorageGroups.

Sweep Vms

Ensures that each available virtual machine exists. Removes the virtual machine if they no longer exist.

Sync Ad

Verifies the state of Active Directory entities such as users, computers, groups, and organizational units and keep these entities in sync.

Synchronize Storage

Synchronizes Hypervisor Storage on Hypervisor <Multiple vCenters>"

Update Timeseries

Collects usage statistics for dashboard graphs.

Create a Troubleshooting Archive

The App Volumes Manager archives logs and configuration files and you can view and download these files for troubleshooting purposes.

Procedure

- 1 From App Volumes Manager, go to **ACTIVITY > Troubleshooting** and click **Create**.
- 2 On the **Create Troubleshooting Archive** window, select the configuration data and log files you want to archive.
- 3 Click **Create**.

The archived file is created. By default, the files are saved in C:/Program Files (x86)/CloudVolumes/Manager/public/troubleshooting on the current server.

What to do next

To download an archived file, select the file. A zipped file is downloaded.

Note If you are running App Volumes Manager behind a load balancer, you will not be able to download the archived file. Log in directly to the App Volumes Manager to access the archived file.

Remove a Troubleshooting Archive

You can delete a troubleshooting archive. You might want to delete the archive to clear up disk space on the server.

Note Removing an archive removes the file from its physical location along with the record of the file. But if App Volumes Manager is behind a load balancer, the archive may continue to exist on the physical server.

Prerequisites

Ensure you have permissions to modify files in the location where the archives are saved. By default, the files are saved in C:/Program Files (x86)/CloudVolumes/Manager/public/troubleshooting.

Procedure

1 From App Volumes Manager, go to **ACTIVITY > Troubleshooting** tab.

2 Click the '+' sign next to the archive you want to delete and click **Remove**.

By default, the archives belonging to the manager on the current server are displayed. To view the list of archives from all managers, select the **All Servers** option from the drop-down list.

3 Confirm that you want to remove the file on the **Confirm Remove** window and click **Remove**.

Reduce App Volumes Login Time on Windows 10

The Windows Modules Installer service affects the App Volumes login time on Windows 10.

If the VMs on which App Volumes is installed remain idle, the Windows Modules Installer service becomes enabled and causes the App Volumes login time to increase.

Disable the Windows Modules Installer service completely to prevent the service from starting automatically.

See the relevant Microsoft documentation to learn how to disable the Windows Modules Installer service.

Default Storage Location on the Storage Page in the App Volumes Manager UI Is Displayed as Not Configured

When the background job for removing stale storage locations in the App Volumes Manager runs and any location that belongs to the vCenter is not reachable, then the job identifies the location as stale and removes the location from App Volumes Manager.

Problem

When the storage location is removed from App Volumes Manager, the **Default Storage Location** information on the **Configuration -> Storage page** is displayed as Not configured.

Cause

This problem occurs if the vCenter is not reachable when the background job for removing the stale storage locations is running in App Volumes Manager.

Solution

To retrieve the deleted storage locations, navigate to the **Configuration > Storage** page in the App Volumes Manager admin UI and click **Rescan**.