VMware App Volumes 4 Administration Guide

VMware App Volumes 2103

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, 2021 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

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 Applications, Packages, 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 Applications, Packages, AppStacks, and Writable Volumes.

This chapter includes the following topics:

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 Applications, Packages, 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 Application, Package, 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 Packages, 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 Applications, Packages, 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 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 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.

  Note You can use LDAP channel binding with secure LDAP connections: LDAPS and LDAP over TLS. When LDAP Channel Binding is enabled in Active Directory, this security feature enables and enforces checks for the presence of channel binding information during LDAP authentication performed for the secure LDAP connections. For information about LDAP Channel binding and setting the registry key for this security feature, see the relevant Microsoft documentation.

- LDAP (insecure) - Connect to Active Directory over an insecure connection over plain LDAP. The default port number is 389.

  The initial binding however, occurs over GSS-SPNEGO.

  Note Currently, App Volumes Manager does not support LDAP Signing. To use LDAP insecure, LDAP Signing must be disabled in the Active Directory. To disable LDAP Signing, the `LDAPServerIntegrity` registry key value must be set to 1 in Active Directory. For information about setting the registry key, see the relevant Microsoft documentation.

The **Disable certificate validation(insecure)** checkbox 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 Active Directory using Domain Name. 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.
- 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 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`. **Note** When the domain name is configured to use the NETBIOS name while logging into App Volumes Manager, ensure that the NETBIOS name does not contain a period `(.)`.
Domain Controller Hosts (Optional)	IP address (`10.98.87.67`) or FQDN (`dc01.corp.example.com`). You can also provide the virtual IP address of a load balancer that is used as the front-end server of the domain controller. This option provides High Availability (HA) capability for connections to Active Directory. **Note** Do not include any non-ASCII characters in the domain controller name. You can add multiple domain controller hosts; use commas to separate the names of the hosts. **Important** If you do not add a domain controller host, the system detects the hosts that are available and connect to the nearest domain controller.
LDAP Base (Optional)	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. Example: OU=Engineering, DC=corp, DC=vmware, DC=com
Username	The user name of the service account that has access to the target Active Directory domain. For example, *admin-1*. The user can be an administrator with read-only permissions.
Password	The password for the service account. Ensure that domain policies do not enforce password expiration for the service account.
Security	Select one of the following options from the drop-down menu to configure the LDAP connection: ■ **Secure LDAP (LDAPS)** - Select this option 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)	IP address (`10.98.87.67`) or FQDN (`dc01.corp.example.com`). You can also provide the virtual IP address of a load balancer that is used as the front-end server of the domain controller. This option provides High Availability (HA) capability for connections to Active Directory. You can add multiple domain controller hosts; use commas to separate the names of the hosts. **Important** If you do not add a domain controller host, the system detects the hosts that are available and connect to the nearest domain controller.
LDAP Base (Optional)	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. Example: OU=Engineering, DC=corp, DC=vmware, DC=com
Username	The user name of the service account that has access to the target Active Directory domain. For example, *admin-1*. The user can be an administrator with read-only permissions.
Password	The password for the service account. Ensure that domain policies do not enforce password expiration for the service account.
Security	Ensure that you are aware of what security options are supported with LDAP channel binding and understand when LDAP insecure can be used. See Connecting Securely to Active Directory. Select one of the following options from the drop-down menu to configure the LDAP connection: ■ Secure LDAP (LDAPS) - Select this option 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 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 Writable Volumes.
- Inventory Administrators
  - Can perform operations related to Applications such as create, import, rescan, update, and so on.
  - Can perform operations related to Writable Volumes and Writable Volumes (2.x) such as create, import, update, rescan, and so on.

  - Has only viewing access to other resources such as Directory or Infrastructure.
  - Does not have access to Configuration resources.
- 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 and Writable Volumes (2.x) 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 Application Packages.
3. Create or import AppStacks.

4 Make storage configuration changes.

5 Add or remove Active Directory domains.

6 Add or remove Machine Managers.

7 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 monitor 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.
Writables 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.

Note the following considerations when removing role assignment:

- If only one group is assigned the Administrators role, you cannot remove the assignment because at least one administrator role must be always assigned to a group.
- If you remove the assignment of a custom role, you are only removing the assignment of that role and not the role itself.

- If you belong to one of the App Volumes Manager roles and remove the assignment of the role to the group to which you belong to, you and all other users of that group cannot log into App Volumes Manager again.

  As a workaround, any user with appropriate role privileges can reassign the role back to the group.

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	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. You can also navigate from each of the categories within a top-level privilege and choose specific individual privileges from the available subcategories. For example, if you select **Inventory** as a top-level privilege, you can select any of the privileges within **Inventory** such as **Applications**, **Application Assignments**, and so on. If you have selected **Applications**, you can further select specific individual privileges such as **View**, **Create**, and so on.

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**.

Monitoring Active Directory Entities

You can use the **DIRECTORY** tab to view the *entities* that are currently online and detailed information about each *entity*. Entity types are `Users`, `Computers`, `Groups`, and `OUs (Organizational Units)`.

On the **Managed** *Entity* page, you can view the list of *entities* and a summarized information about the number of assignments, attachments, and Writable Volumes for each *entity*.

An *entity* can be available for both App Volumes 4.0 Agent and App Volumes 2.*x* Agent. The **Entity** details page provides all entity-related information.

Note AppStacks and Writable Volumes (2.*x*) can be created only by using App Volumes Agent 2.*x* and uploading the appropriate templates. Any information related to these volumes can be viewed only when the **VOLUMES (2.X)** tab is visible in the App Volumes Manager UI. If you have installed the latest version of App Volumes Manager and want to explore App Volumes 2.*x*, see Chapter 11 Perform App Volumes 2.x Management Tasks.

View Active Directory Entities

On the *Entity* details page, depending on the *entity* type, you can view the entity name, Application and AppStack assigned to the entity, list of Packages attached to the *entity*, and Writable Volumes created for the *entity*. You can also perform assign and unassign operations.

Entity types are `Users`, `Computers`, `Groups`, or `OUs`.

For the non-computer entities (`Users`, `Groups`, or `OUs`), you can limit the delivery of an application assignment to a specific computer. For a better understanding, see Application Assignment to Specific Computers.

Similarly, you can also unassign the attachment from the entity for a specific computer. The prefix of the computer name is displayed in the **Computers** column in the **Application Assignments** table. For more information about the **Computers** column, see View Assignments.

Note AppStacks and Writable Volumes (2.x) can be created only by using App Volumes Agent 2.x and uploading the appropriate templates. Any information related to these volumes can be viewed only when the **VOLUMES (2.X)** tab is visible in the App Volumes Manager UI. If you have installed the latest version of App Volumes Manager and want to explore App Volumes 2.x, see Chapter 11 Perform App Volumes 2.x Management Tasks.

Procedure

1 From App Volumes Manager, go to **DIRECTORY > *Entity*.**

2 On the **Managed** *Entity* page, click the *entity* name.

  Entity details are displayed.

  Note For non-computer *entities* (`Users`, `Groups`, and `OUs`), the **Application Assignments** section also includes the computer prefix information.

3 (Optional) On the **Entity** details page, you can also perform the following assign and unassign tasks for an *entity*:

   a To select and assign an Application to an *entity*, click **Assign Application**.

   Only Application Packages marked `CURRENT` can be assigned to an *entity* from the **Entity** page.

   Note To only attach the assigned packages when the prefix matches the name of the computer being logged into, you can select the **Limit delivery for these assignments** text box and enter the prefix of the computer name.

   b Perform the rest of the steps in this workflow as you would while assigning an application to an entity when using the **Inventory** tab.

   c To unassign an Application from an *entity*, select the Application Assignment and click **Unassign**.

   Note If the *entity* belongs to `Users` and has received this Application as part of `Groups` or `OUs`, then you cannot unassign this Application from the entity.

   If the application assignment has a value displayed in the **Computers** column, then this value indicates that the selected application assignment is removed from that computer only.

   For more information about this task, see Unassign an Application from an Entity.

   d To assign an AppStack for an *entity*, click **Assign AppStack** and perform the rest of the steps as mentioned in Assigning and Attaching AppStacks.

   Only AppStacks in the `Enabled` status can be assigned to the *entity* from the **Entity** page.

   e To unassign an AppStack from an *entity*, select the AppStack and click **Unassign**.

   All AppStacks assigned to the *entity* are displayed.

Sync Entities with Active Directory

You can view the updated list of entities by using the Sync functionality. The **Sync** button synchronizes all entities with the Active Directory. An entity can be a User, Computer, Group, or OUs (Organizational Units).

Procedure

1 From App Volumes Manager, click **DIRECTORY**.

2 Click the desired ***Entity*** tab.

   Entity can be **Users**, **Computers**, **Groups**, or **OUs**.

3 Click **Sync**.

4 On the **Confirm Sync** window, click **Sync**.

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 Applications, Packages, 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 Applications, Packages, 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 Applications, Packages, 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\vpxd.cfg` in the vCenter Server. If it is set to false, change this to true and restart the vCenter Server service.

	Permissions
Datastore	■ Allocate space ■ Browse datastore ■ Low level file operations ■ Remove file ■ Update virtual machine files
Global	Cancel task
Host	Local Operations -> Reconfigure virtual machine **Note** ■ 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 **Note** This permission is not required for the VMware Cloud on AWS environment.
Tasks	Create task
Virtual machine	■ Configuration ■ Add existing disk ■ Add new disk ■ Add or remove device ■ Query unowned files ■ Change resource ■ Remove disk ■ Settings ■ Advanced ■ Inventory ■ Create new ■ Move ■ Register ■ Remove ■ Unregister ■ Provisioning ■ 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 `vcenter.sddc-xx.xxx-x-xx.vmc.vmware.com`
Username	The user name to access the machine. For example,`YOURDOMAIN\administrator`.
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.

Option	Description
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 `servers` entry in `clock.yml` 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.

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

You can configure storage for Packages, Writable Volumes, AppStacks (2.*x*), and Writable Volumes (2.*x*) by specifying the default storage and template paths.

Note AppStacks and Writable Volumes (2.*x*) can be created only by using App Volumes Agent 2.*x* and uploading the appropriate templates. Any information related to these volumes can be viewed only when the **VOLUMES (2.X)** tab is visible in the App Volumes Manager UI. If you have installed the latest version of App Volumes Manager and want to explore App Volumes 2.*x*, see Chapter 11 Perform App Volumes 2.x Management Tasks.

You can use the **Upload Templates** functionality to upload templates to the datastore. You can also configure VHD In-Guest Storage to use with App Volumes.

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. Some of the details displayed are as follows: Number of AppStacks, Number of Packages, Number of Writables (aggregate of Writable Volumes and Writable Volumes (2.x)), and UUID.

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 Packages

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

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 **Packages**:

Option	Description
Default Storage Location	Storage Location in VC
Default Storage Path	For example, `/appvolumes/packages`
Templates Path	For example,`/appvolumes/packages_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 AppStacks (2.*x*)

You can configure storage for AppStacks (2.*x*) by selecting the default storage locations and paths.

Note AppStacks and Writable Volumes (2.*x*) can be created only by using App Volumes Agent 2.*x* and uploading the appropriate templates. Any information related to these volumes can be viewed only when the **VOLUMES (2.X)** tab is visible in the App Volumes Manager UI. If you have installed the latest version of App Volumes Manager and want to explore App Volumes 2.*x*, see Chapter 11 Perform App Volumes 2.x Management Tasks.

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 (2.*x*):

Option	Description
Default Storage Location	Storage Location in VC
Default Storage Path	For example, `/cloudvolums/apps`
Templates Path	For example,`/cloudvolumes/apps_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 and Writable Volumes (2.*x*) by selecting the default storage locations and paths.

Note AppStacks and Writable Volumes (2.*x*) can be created only by using App Volumes Agent 2.*x* and uploading the appropriate templates. Any information related to these volumes can be viewed only when the **VOLUMES (2.X)** tab is visible in the App Volumes Manager UI. If you have installed the latest version of App Volumes Manager and want to explore App Volumes 2.*x*, see Chapter 11 Perform App Volumes 2.x Management Tasks.

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.

Note You cannot use the same storage path for Writable Volumes and Writable Volumes (2.*x*).

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
Writable Volumes	■ **Default Storage Location** Storage Location in VC ■ **Default Storage Path** For example, `/appvolumes/writables` ■ **Templates Path** For example,`/appvolumes/writables_templates` ■ **Default Backup Path** For example,`/appvolumes/writables_backup`
Writable Volumes (2.x)	■ **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 Templates

You must upload the templates to the datastore in certain scenarios. The scenarios can be as follows: you have upgraded from the previous version and want to use the latest templates, you have changed the destination of the template path, accidentally deleted, or moved a template from the datastore.

To upload the templates, use the **Upload Templates** page. On this page, you can view templates for Packages, Writable Volumes, AppStacks (2.x), and Writable Volumes (2.x).

Note AppStacks and Writable Volumes (2.x) can be created only by using App Volumes Agent 2.x and uploading the appropriate templates. Any information related to these volumes can be viewed only when the **VOLUMES (2.X)** tab is visible in the App Volumes Manager UI. If you have installed the latest version of App Volumes Manager and want to explore App Volumes 2.x, see Chapter 11 Perform App Volumes 2.x Management Tasks.

For information about types of Writable Volume templates, see Types of Writable Volume Templates.

Prerequisites

- Ensure that you have the details and login credentials of the ESX host to which you want to upload the volumes.
- Ensure that you are aware of the considerations regarding templates.

  For understanding different types of templates used in App Volumes, see Understanding Templates used in App Volumes.

Procedure

1. From the App Volumes Manager, click **CONFIGURATION > Storage**.
2. Click **Upload Templates**.
3. On the **Upload Templates** page, provide the following information:

Option	Description
Storage	Select a storage location from the drop-down menu.
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.

4. Select a source template for the volumes to be uploaded.

   The **Type** field indicates the type of volume. This could be a Package, Writable Volume, AppStack, or Writable Volume (2.x)

   The **Exists** field indicates whether the template is present at the destination path (Templates Path) and the value of this field is `Yes` or `No` accordingly.

5 Click **Upload**.

6 On the **Confirm Upload Templates** window, click **Upload**.

Understanding Templates used in App Volumes

You must specify a template when you create a volume or when you upload volumes packaged with your instance of App Volumes Manager to the selected datastore.

Note AppStacks and Writable Volumes (2.x) can be created only by using App Volumes Agent 2.x and uploading the appropriate templates. Any information related to these volumes can be viewed only when the **VOLUMES (2.X)** tab is visible in the App Volumes Manager UI. If you have installed the latest version of App Volumes Manager and want to explore App Volumes 2.x, see Chapter 11 Perform App Volumes 2.x Management Tasks.

Some of the considerations regarding templates are as follows:

- **packages_templates** and **writables_templates** are used while creating Application Packages and Writable Volumes for a user accessing a virtual machine installed with App Volumes 4.0 Agent.
- **apps_templates** and **writables_templates** (for 2.x template type) are used while creating AppStacks (2.x) and Writable Volumes for a user accessing a virtual machine installed with App Volumes 2.x Agent.
- Templates for Writable Volumes and Writable Volumes (2.x) are not compatible with each other.
- Template path for Writable Volumes and Writable Volumes (2.x) should be different.

Types of Writable Volume Templates

There are three types of Writable Volume templates available in App Volumes: Profile-only, UIA only, and UIA+profile.

The following helps you understand the types of Writable Volume templates and their usage:

- 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.

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.

The CIFS share must be created on a stable network, which can handle the applications residing on the share for VDI desktops.

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

Join the Customer Experience Improvement Program (CEIP) for App Volumes

This product participates in VMware's Customer Experience Improvement Program (CEIP). When you choose to participate in CEIP, VMware receives anonymous information to improve the quality, reliability, and functionality of VMware products and services. You can choose to join App Volumes to the program, or leave the CEIP anytime.

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are given at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

Note The **CEIP** text box is displayed the first time after you configure App Volumes Manager and you must make a selection. You can change your selection at any time by following the procedure described in this section.

Procedure

1 In the App Volumes Manager UI, navigate to **CONFIGURATIONS > Settings > Advanced Settings**.

2 To join the program, turn on the **Join the VMware CEIP** toggle switch and to leave the program, turn off the switch.

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 Packages, 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 SESSION_TIMEOUT.
General Settings	Certificate Authority File	Path of the certificate file used by machine managers. Set via the system environment variable SSL_CERT_FILE.
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 AVM_ALLOW_API_MOUNT (or CV_ALLOW_API_MOUNT).
Writable Volumes	Delete Protection	Protect volumes from getting deleted directly from storage. Set via the system environment variable AVM_NO_PROTECT (or CV_NO_PROTECT).
Writable Volumes	Force Reboot on Error	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 AVM_WRITABLE_REBOOT. **Note** The AVM_WRITABLE_REBOOT does not apply to Writable Volumes conflicts. Writable Volumes conflicts are handled by the the Block user login setting. See Create a Writable Volume (2.x) for information about this setting.
Writable Volume Backups	Regular backups	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.

Type	Value	Description
Active Directory	Allow or Disallow	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. 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.
Writable Volume Backups	Storage Location	The location where the volumes are backed up. For example, *[xxx]AV-LUN*.
Writable Volume Backups	Storage Path	The folder name and path where the volumes are backed up. For example, *cloudvolumes/ writable_volumes_backup*
Advanced Settings	Disable Agent Session Cookie	Toggle the slider to enable or disable Agent Session Cookie. App Volumes uses a session cookie to optimize the communication between the App Volumes Manager and App Volumes Agent. If you have Agent session issues, you can use this setting to disable the session cookies.
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.

Type	Value	Description
Advanced Settings	Enable Volumes (2.x)	Toggle the slider to enable or disable the **VOLUMES (2.X)** tab. **VOLUMES (2.X)** tab is for working with AppStacks and Writable Volumes along with App Volumes Agent 2.x. For upgraded deployments, this setting can be disabled after the AppStacks and Writable Volumes are completely migrated. If you have newly installed App Volumes Manager, for more information about this setting, see Chapter 11 Perform App Volumes 2.x Management Tasks. If you have upgraded to the latest version of App Volumes Manager, for more information about this setting, see Configuring visibility and management of App Volumes Manager 2.x UI.
Advanced Settings	Allow package delivery to any operating system	Toggle the slider to allow packages to be delivered to any operating system which is different from the operating system used during packaging. By default, this setting is disabled. **Note** Enabling this setting might result in application inoperability. For optimum application compatibility, ensure that the same operating system is used to package and deliver the application. Though any operating system can be used, the package must be captured and delivered in virtual machines that have the same Windows operating system architecture. For example: if the package is captured in a virtual machine running 64-bit operating system architecture, then the package can be delivered to a machine running a 64-bit operating system architecture only. Package delivery cannot happen to a machine running 32-bit operating system architecture due to architecture mismatch.

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

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 theApp 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

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 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 backup 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;`.

Note It is recommended that you set the `server_name` to the hostname URL used to access App Volumes Manager. This ensures that the HTTP request is sent to the desired App Volumes Manager server.

```
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;

         # updated by clock.rb
         location ~* ^.+\.(woff|woff2|eot|svg|ttf|jpg|jpeg|gif|png|ico|zip|css|js|html|htm|json)$
{
             expires max;
             break;
        }

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

        include location/api_redirect_location.conf;

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

        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.

Configuring Ports and Protocol for App Volumes

4

You can use the VMware Ports and Protocols Tool to configure the ports forApp Volumes. This tool enables you to view port information for a variety of VMware products on a single dashboard.

You can view the App Volumes ports and protocol information at https://ports.vmware.com/home/App-Volumes.

You can access the tool at https://ports.vmware.com/.

Working with Applications

5

Each Application represents a collection of packaged versions of that application. Users, Groups, Computers, or OUs can be entitled to receive the current package or a specific package version. You can use the **Applications** tab to create an Application or Application Package, assign an Application to an entity, and other management tasks.

Every Application has an Application details page that has information about the status of an Application, entities assigned to an Application, computer prefixes associated with non-computer entities (Users, Groups, and OUs) and a list of Application Packages.

This chapter includes the following topics:

Create an Application

By creating an Application, you can manage the lifecycle of the packages added to the Application.

Procedure

1 From App Volumes Manager, go to **INVENTORY > Applications** and click **Create**.

2 Provide the following information and click **Create**:

Option	Description
Name	Name of the Application.
Description	Include the name of the packages or programs the Application contains.
Owner	If you want to change the default option, search and select the owner from the available domains in the Active Directory.
Package (optional)	The App Volumes Manager displays the **Packages** tab after the Application is created. If this box is deselected, you must create a Package later.

3 If you want to create a package for the Application immediately after the Application is created, select the **Create a Package** box.

By default, the **Create a Package** box is selected.

4 Click **Create**.

5 On the **Confirm Create Application** window, click **Create**.

If you have selected the **Create a Package** box, App Volumes Manager displays the **Packages** tab after the Application is created.

What to do next

Create a Package for an Application.

Import an Application to App Volumes

If you have already created an application package in another App Volumes Manager deployment, you can import the files of that application package to the current App Volumes Manager deployment. You can use the import functionality to reuse pre-configured third-party application packages.

You can also import an MSIX app attach format to App Volumes. Only a single MSIX application package can be present within an MSIX app attach format. The MSIX app attach format requires Windows 10, version 2004 or later.

Note For now, you cannot use App Volumes Manager to either create or update the MSIX app attach format.

For more information about MSIX, see the relevant Microsoft documentation.

After importing the application package to the current App Volumes Manager deployment, you can perform the assign and attach activities.

For information about how App Volumes Manager associates the imported packages to their correct applications, see Understanding the Behavior of Imported Application Packages.

Prerequisites

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

Procedure

1. From the App Volumes Manager console, navigate to **INVENTORY > Applications**.
2. Click **Import**.
3. Select the datastore where you have uploaded the application package and enter the path of the application package.
4. Click **Import**.

Results

The current App Volumes Manager deployment lists the imported application package.

Understanding the Behavior of Imported Application Packages

After an import, packages are automatically associated with their application inventory item as they were related in the source App Volumes Manager.

If the application does not exist while importing, App Volumes Manager creates an application by using the application properties and then associates the package to the new application inventory item.

After an import, applications and packages are listed in the **Inventory** tab of the App Volumes Manager admin UI.

Note Imported packages follow the behavior described in this section only when they have been created or updated by App Volumes Manager 4, version 2012 or later. Any packages created before App Volumes Manager 4, version 2012, have a different import behavior even when imported to a later version. For optimal import functionality, ensure all App Volumes Manager servers are upgraded to App Volumes Manager 4, version 2012 before performing import actions. For information about upgrade, see App Volumes 4 Installation Guide.

App Volumes Manager performs the following functions to ensure that the package gets associated to the correct application:

- Any update to the package properties such as package description or package stage is applied to all storage locations of the package.

  Such an update ensures that when a package is imported, the package remains associated to the correct application.
- Any update to the application properties such as application name and description is applied to all packages of the application including to all package locations within the same App Volumes Manager instance.

- If the same package is copied to multiple storage locations, on an import, the source App Volumes Manager instance detects the package including all its duplicates and imports them to the target App Volumes Manager instance.
- Application owner information is applied to the package on import.

Note App Volumes Manager does not import an application's assignments and the assignment type, `Marker`.

If an application package is marked as `CURRENT`, though the package is imported, the package does not have the `CURRENT` marker after the import.

Rescan Applications

You can use the Rescan functionality to verify the existence and current state of each Application Package on the datastore.

The rescan operation only checks for Application Packages that are already known by the current App Volumes Manager deployment.

For new Application Packages added to the datastore from a different App Volumes Manager deployment, you can import the Application Packages to the current App Volumes Manager deployment. To import an Application Package, see Import an Application to App Volumes.

Procedure

1 From the App Volumes Manager console, navigate to **INVENTORY > Applications**.

2 Click **Rescan**.

A list of available Application Packages is displayed with its current state.

Assign an Application to an Entity

You can assign an Application to a single entity or multiple entities.

- If you select the assignment type as `Marker` and the Application package is not yet marked `CURRENT`, the Application is assigned to the entity and the assignment type is disabled until a package is marked `CURRENT`.

  For information about assignment types, see Understanding Assignment Types.
- In an Application, a Package set with the `CURRENT` marker can be assigned to multiple entities.
- By using the option of limiting delivery of assignments to specific computers, entities can have different application assignments on different computers.

  For more information about this option, see Application Assignment to Specific Computers.

Prerequisites

- Ensure that the status of the entity, to which the Application must be assigned, is `Available`.

- For the Assignment Type, `Package`, an Application must have at least one Package.
- If you are assigning an MSIX app attach format to an entity, ensure that the certificate which was used while packaging the MSIX is installed on the machine where App Volumes agent is installed.

Procedure

1. From App Volumes Manager, go to **INVENTORY > Applications**.
2. Select the Application to which needs to be assigned to an entity.
3. Click **Assign**.
4. Search the Active Directory for an entity.
5. Select the entity.

   The **Status** of the entity must be `Available`.
6. Select **Assignment Type**.

Option	Action
`Marker`	- If the Application has no Package or if the Package is not yet set with `CURRENT` marker, Application is assigned to the entity and the assignment type is disabled until a package is marked `CURRENT`. - If the Package has the `CURRENT` marker, entity receives the `CURRENT` Package version. Select **Marker**.
`Package`	Select the package that must be assigned to the entity.

7. (Optional) To only allow attachment of packages to a specific set of computers based on the computer's name, select **Limit delivery for these assignments**.
   - This option is available only for non-computer entities (`Users`, `Groups`, and `OUs`).

   a. Enter the prefix of the computer name.

      Packages are only attached to computers whose names start with the prefix specified in the text box.
8. Click **Assign**.
9. On the **Confirm Assign** window, click **Assign**.

Results

On the **Applications** page, assignment details are updated.

Understanding Assignment Types

While assigning an Application to an entity, you can either assign the latest version of an application package or a specific version of the application package. The assignment types are: `Marker` and `Package`.

At a time, only one assignment type (`Marker` or `Package`) can be selected while assigning the application package to the entity.

`Marker`

The Application Package marked as `CURRENT` is assigned to the entity. `CURRENT` implies that the entity always receives the latest version of the application package.

`Package`

A specific version of the Application package is assigned to the entity. The entity receives only this assigned version.

Priority Followed in Assigning Application Packages Based on Entity Types

When assigning an application's packages to multiple entity types, a certain priority is followed that determines what entity type receives which package.

The entity types are as follows: `Users`, `Comupters`, `Groups`, and `OU (Organizational Units)`.

If you have assigned multiple packages of an application to multiple entity types, then the assignment resolution has the following priority:

- Direct assignment to the entity types `Users` and `Computers` has more priority than an assignment to the entity types `Groups` and `OU (Organizational Units)`.
- Assignment to `Groups` has more priority than an assignment to `OU (Organization Unit)`.

Note If the entity type `Users` or `Computers` is a member of multiple `Groups` or `OUs` and the same application package is assigned to those multiple `Groups` or `OUs`, then the priority of assignment resolution might not follow the priority as mentioned previously. Only the priorities within one `Groups` or `OU` are assured, but attachments from assignments of the other groups or OUs might be mixed in that ordering.

In the examples that are listed here, John is of entity type `Users` who belongs to Engineering which is of entity type `Groups`. This group belongs to an `OU`, Employees. win_machine belongs to entity type, `Computers`. An application has multiple package versions such as package_1, package_2, package_3, and so on. None of these packages are marked `CURRENT`:

- An administrator assigns package_1 to John and package_2 to Engineering.

  When John logs into win_machine, John receives package_1 because assignment to `Users` has more priority than the assignment to `Groups`.
- win_machine belongs to the group Engineering. An administrator assigns package_4 to win_machine and package_2 to Engineering.

  When John logs into win_machine, John receives package_4 because assignment to `Computers` has more priority than the assignment to `Groups`.
- An administrator assigns package_2 to Engineering and package_3 to Employees.

When John logs into win_machine, John receives package_2 because assignment to `Groups` has more priority than the assignment to `OU`.

- An administrator assigns package_1 to John and package_4 to win_machine.

  In this case, to understand what application package John receives, see Selective Scenarios of Volume Types Delivered.

Application Assignment to Specific Computers

While assigning an Application to a non-computer entity, you can specify the prefix of a computer name by selecting the **Limit delivery for these assignments** option. This option allows you to only attach the assigned packages when the prefix matches the name of the computer being logged into.

This option is also one of the factors that determines whether an assignment is newly created, an existing assignment is updated, or a duplicate assignment is skipped. For more information, see Assignment Scenarios.

By using this option, you can also update an application assignment of an entity. When a prefix of the computer name is specified while assigning an application to a non-computer entity, then the entity receives only that application package version for that specific computer. To update the assignment, you can select the entity and use the **Limit delivery** option to specify the prefix of the computer name and assign the desired application package version.

The **Limit delivery for these assignments** option can only be used for the following *entity* types: `Users`, `Groups`, and `OUs (Organizational Units)`. This option is not applicable to `Computers`.

To view the update workflow, see Update an Application Assignment of an Entity.

Assignment Scenarios

The **Limit delivery of these assignments to specific computers option** option helps in determining the type of assignment scenario such as: an assignment is newly created, an existing assignment is updated, or a duplicate assignment is skipped. Some of the assignment scenarios are listed in this topic for a better understanding.

New Assignment

Scenario 1:

An administrator assigns Application 'X', package 1 to a non-computer entity 'user' on computer 'Dev'. The administrator can assign the same Application Package to 'user' on another computer, 'Test'.

Scenario 2:

An administrator assigns Application 'X' (`Marker` or `Package`) to a non-computer entity 'user' on computer 'Dev'. The administrator can assign Application 'Y' (`Marker` or `Package`) to the entity 'user' on 'Dev'.

Scenario 3:

An administrator assigns Application 'X', package 1 to a non-computer entity 'group' on computer 'Dev'. The administrator can assign package 2 of the same application (X) to 'group' on another computer 'Test'.

Scenario 4:

An administrator assigns Application 'Y', package 1 to a non-computer entity 'OU'. No computer prefix is specified. This results in the application being assigned to 'OU' on all computers. The administrator can assign Application 'Y', package 2 to OU on 'Dev'.

Update Assignment

Scenario 1:

An administrator assigns Application 'X', package 1 to a non-computer entity 'user' on computer 'Dev'. The administrator can assign Application 'X', package 2 to ‘user’ on ‘Dev’. As an entity can receive only one version of the Application Package at a time on a specific computer, the assignment to ‘user’ on ‘Dev’ is updated to package 2. The assignment occurs at the following login session.

Scenario 2:

An administrator assigns Application ‘Y’, package 1 to a non-computer entity ‘group’ on all computers. The administrator can assign Application ‘Y’, package 2 to ‘group’ on all computers. ‘group’ receives package 2 on all computers because an entity can be assigned only one package version of an Application at a time on a computer. As a result, ‘group’ receives the latest package version assignment.

Skip (Duplicate) Assignment

An administrator assigns Application ‘X’, package 1 to a non-computer entity ‘user’ on ‘Dev’. The administrator unintentionally selects the same entity to assign the same package version of the application on ‘Dev’. As the application package is a duplicate, the assignment to 'user' is skipped.

For more information about the **Limit delivery of these assignments to specific computers option** option, see Application Assignment to Specific Computers.

Order of Precedence for Assigning Applications

While assigning an application, an order of precedence is followed based on criteria such as entity type, assignment type (`Marker` and `Package`), computer name specified while attaching packages, and the date on which the application is assigned. This information helps you understand how application assignments take precedence over each other.

The order of precedence is as follows:

1 Active Directory entity type

   An order of priority based on the entity type is followed while assigning an application's packages to multiple entities. The entity types are as follows: `Users`, `Computers`, `Groups`, and `OU (Organizational Unit)`.

2. Computer name specified during an application assignment

   A computer name with a longer prefix takes more precedence than a computer name with a shorter prefix. For example, for the agent computer WIN10_1809, prefix WIN10_18 takes more precedence than the prefix WIN10_1.

3. Assignment type

   Specific version of the application package (`Package`), takes more precedence than the latest version of the application package (`CURRENT`).

4. Assigned date

   This criterion is applied when all other criteria listed in the order of precedence are equal. When multiple packages of the same application are assigned to an entity and no computer name is specified, then the date on which each application package is assigned to the entity determines which package is delivered to the entity. The most recent assignment takes the highest precedence.

Scenarios to Understand the Order of Precedence

For the scenarios listed in the table, the entity type examples considered are as follows: John is of entity type `Users` who belongs to two `Groups`: Engineering and Management. These groups belong to an `OU`, Employees.

Setup	Assignment Flow	Assignment Resolution
Scenario "Active Directory entity type" ■ An application has three packages: package 1, package 2, and package 3.	1 Assign package 1 to John. 2 Assign package 2 to Engineering. 3 Assign package 3 to Management. 4 John logs into a computer.	As per the order of priority in assigning application packages based on entity types, `Users` takes more precedence than `Groups` and `OU`. As a result, John receives package 1 when logged into a computer.
Scenario "Computer name" ■ An application has two packages: package 1 and package 2. ■ Package 1 is marked `CURRENT`. ■ Agent computer is WIN10_1809.	1 Assign package 1 to John and attach the package to computers whose name begins with WIN10_1. 2 Assign package 2 to John and attach the package to computers whose name begins with WIN10_18. 3 John logs into WIN10_1809.	1 Package 1 and package 2 assignments are done to the same entity, John. As a result the next criterion, which is the computer name, is checked. 2 Computer names specified while assigning the application packages are: WIN10_1 and WIN10_18. For the computer, WIN10_1809, WIN10_18 is more specific than WIN10_1. As a result, based on the order of precedence, John receives package 2.

Setup	Assignment Flow	Assignment Resolution
Scenario "Assignment type" Consider the setup of this scenario to be the same as the "Computer Name" scenario.	1 Assign the CURRENT version (package 1) of the application to Engineering. 2 Assign the specific version (package 2) of the application to Management. 3 John logs into WIN10_1809.	1 Application is assigned to two different groups, but of the same entity type, Groups. 2 Computer name is not specified in this case. As a result, the next criterion which is, assignment type is considered. 3 Assignment type: CURRENT version of the package versus specific package version of the application is considered. As per the order of precedence, John receives package 2 because a specific assignment takes more precedence than a CURRENT assignment.
Scenario "Assigned date" ■ An application has two packages: package 1 and package 2. ■ Application is assigned to the Engineering group on all computers.	1 Assign package 1 to Engineering on Monday. 2 Assign package 2 to Engineering on Tuesday. 3 John who belongs to Engineering, logs into a computer on Wednesday.	In this scenario, entity and assignment types remain the same and computer name is not specified. As a result, the "assigned date" criterion is applied while assigning the application package to any user who belongs to Engineering. Per the date on which the application package is assigned, package 2 is a more recent assignment to Engineering when compared to package 1. As a result, when John logs into a computer on Wednesday, John receives package 2.

For more information regarding the entity type criterion, see Priority Followed in Assigning Application Packages Based on Entity Types.

For more information about the assignment types criterion, see Understanding Assignment Types.

For an understanding of Active Directory Entities, see View Active Directory Entities.

Selective Scenarios of Volume Types Delivered

Users and computers can have different volume types (application packages and Writable Volumes) delivered. This section provides information about how different combinations of volumes are delivered in certain scenarios as the user logs into the computer.

In the following table, in each scenario, an application package, Writable Volume, or a combination of both is presented. The result for each of these scenarios is then listed.

	Computer		Users		
Scenario	Application	Writable Volume	Application	Writable Volume	Result
1	No	Yes	No	Yes	■ Computer Writable Volume is attached. ■ User Writable Volume is not attached.
2	No	Yes	Yes	No	■ Computer Writable Volume is attached. ■ Application package is not delivered.
3	No	Yes	Yes	Yes	■ Computer Writable Volume is attached. ■ User Writable Volume is not attached and application package is not delivered.
4	Yes	No	No	Yes	■ Computer-assigned application package is delivered. ■ User Writable Volume is not attached.
5	Yes	No	Yes	Yes	■ Computer-assigned application package is delivered. ■ User-assigned application package is not delivered and user Writable Volume is not attached.

	Computer		Users		
Scenario	Application	Writable Volume	Application	Writable Volume	Result
6	Yes	Yes	No	Yes	- Computer Writable Volume is attached and computer-assigned application package is delivered. - User Writable Volume is not attached.
7	Yes	Yes	Yes	No	- Computer Writable Volume is attached and computer-assigned application package is delivered. - User-assigned application package is not delivered.
8	Yes	Yes	Yes	Yes	- Computer Writable Volume is attached and computer-assigned application package is delivered. - User-assigned application package is not delivered and user Writable Volume is not attached.

Update an Application Assignment of an Entity

To assign a different application package version to an entity that already has an existing assignment, you can update the assignment. The update workflow can be used instead of unassigning an application from an entity and performing the assignment operation all over again.

You can also update the assignment attached to a specific computer by using the **Limit delivery for these assignments** option. For a better understanding about this option, see Application Assignment to Specific Computers.

Prerequisites

You must have already assigned an application package to an entity.

Procedure

1 To update an application assignment of an entity, navigate to the application's details page and review the assignments.

2 Click the **Assign** button.

3 On the **Assign Application** page, search for the entity whose assignment must be updated.

4 Select the entity.

5 Select the **Assignment Type**.

6 If the assignment type is `Package`, then from the **Package** window, select the desired version of the package that must be assigned to the entity.

7 (Optional) To update the assignment attached to a specific computer, perform the following:

   a Select the **Limit delivery for these assignments** option.

   b Enter the prefix of the computer name.

   Note Only those computers whose name starts with the prefix that you have entered, receive the updated assignment.

8 Click **Assign**.

9 On the **Confirm Assign** window, click **Assign**.

Unassign an Application from an Entity

You can remove an Application assigned to an entity or entities.

Procedure

1 From App Volumes Manager, go to **INVENTORY > Applications**.

2 Select an Application that must be unassigned from an entity or entities.

3 Click **Unassign**.

List of entities assigned to the Application is displayed.

4 Select the entity or entities.

5 Click **Unassign**.

6 On the **Confirm Unassign** window, click **Unassign**.

Create a Package for an Application

You can create a Package for an Application either immediately after creating the Application or at a later point in time.

When you create a Package, you only provide the metadata such as name, storage, path, template, and description of the Package from the App Volumes Manager.

For information about life cycle of a Package, see Lifecycle of a Package.

Prerequisites

- You must have already created an Application.

  Create an Application

- You must have uploaded the template for packages to the datastore.

  Upload Templates

Procedure

1 From App Volumes Manager, go to **INVENTORY > Applications**.

2 Select an Application and click **Create Package**.

3 On the **Create Package** page, provide the Package details such as `Name`, `Base Package`, `Storage`, `Path`, `Template`, `Stage`, and `Description`.

Base Package acts as reference when you opt to create a new version of a Package by using an existing version as base.

Note You cannot use the **Create** functionality to create an MSIX app attach format in App Volumes. As a result, this format is not listed in the `Base Package` dropdown box.

4 Click **Create**.

5 On the **Confirm Create Package** window, select one of the options and click **Create**.

Option	Action
Perform in the background	The Package gets created for the Application in the background and you can perform other tasks. **Note** Status of the Package is `Creating`.
Wait for completion	You must wait until the Package is created for the Application. You cannot perform any other tasks until the Package gets created.

Results

The newly created Package details are displayed in the **Packages** tab.

What to do next

Package the Application.

Lifecycle of a Package

Each Package has different stages. These stages provide information about the state of delivery of the Package. You can choose a Package stage while creating a Package.

The following are the different stages of a Package:

`New`

Package is ready to be tested. Users who are signed up for testing this Package are assigned this stage.

`Tested`

Package is ready to be published. Users have tested this Package.

`Published`

Package is published for assigned users.

`Retired`

Packages that are no longer required or updated. Entities can still be assigned to Applications with retired Packages.

To create a package, see Create a Package for an Application.

Edit an Application

You can edit an Application to change the name, description, and owner details.

Procedure

1 From App Volumes Manager, go to **INVENTORY > Applications**.

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

3 Enter the new values and click **Save**.

   The updated Application details are displayed.

Delete an Application

Depending on your requirements, you can delete an Application. When you delete an Application, the associated Packages and Assignments are also deleted.

Procedure

1 From App Volumes Manager, go to **INVENTORY > Applications**.

2 Select an Application and click **Delete**.

3 On the **Confirm Delete** window, click **Delete**.

   Status of the Application is displayed as `Pending Delete` until the action is completed.

Results

The Application is removed from the **Applications** page.

Working with Packages

6

Each Package stores one or more Programs required for the Application to run. A single Package can be delivered to multiple computers and users.

For the packaging process, you must select a computer as the packaging machine and then build the Package on the packaging machine where the programs you want to include in the Package are installed. You can provide additional Package metadata on the packaging machine such as name of the Packager and any additional notes about the Package.

You can use the **Packages** tab to view the list of Packages and perform related operations such as package an Application, update a Package, and so on. The **Package Details** page and the **Package Summary** window displays information such as package name, package format (AV, MSIX), agent version used to package the Application, and so on.

This chapter includes the following topics:

Package an Application

After adding a Package to an Application, you must select a packaging machine and build the package to finish the packaging process.

To understand some of the best practices that can be followed while packaging an application, see Best Practices for Packaging Applications.

When App Volumes and VMware Dynamic Environment Manager are used together and a Dynamic Environment Manager condition references file or registry data on an App Volumes volume, the `All AppStacks Attached` trigger must be selected. This ensures that the Dynamic Environment Manager evaluates the condition after all volumes are attached.

For information about the `All AppStacks Attached` trigger, see *Configure Triggered Tasks* in the *VMware Dynamic Environment Manager Administration Guide*.

Prerequisites

- Ensure that the status of the Package you want to build is `Unpackaged`.
- Ensure that the packaging machine meets the criteria as mentioned in Preparing a Packaging Virtual Machine.
- Ensure that you have created a clean snapshot of this virtual machine as part of the App Volumes agent installation.

Procedure

1. From the App Volumes Manager, click **INVENTORY > Packages**.
2. Click the Package with an `Unpackaged` status.
3. Click **Package**.
4. On the **Packages** page, search for the computer on which you want to perform the packaging process.

   A list of computers is displayed.
5. Select the computer you want to use as the packaging machine and click **Package**.
6. Build the Package on the packaging machine.

   a. Log in to the packaging or capture machine.

   b. Locate the installer for the program you want to capture in the Package.

   c. Install and configure the program.

      If necessary, reboot the machine.

   d. Click **Finalize**.

      The agent machine reboots.

   e. After the packaging machine restarts, click **OK** on the **Packaging is Succesful** dialog box.

      The capture process is now complete.

   f. Revert to the virtual machine's clean snapshot.
7. In App Volumes Manager, click **INVENTORY > Packages** and review the Package information to ensure that the packaging is successful.

   Package status must be `Enabled`.

What to do next

It is recommended that you test and validate the application package on a clean virtual machine different from the machine used for packaging the application.

Preparing a Packaging Virtual Machine

Before packaging an application, you must prepare the virtual machine used for packaging by following a certain criteria.

The criteria for preparing a packaging machine is as follows:

- An appropriate version of the App Volumes agent must be installed on the packaging machine.
- Application Packages must be packaged on a clean base image (virtual machine), which closely resembles the target environment to which you later plan to deploy the Applications.

  For example, the packaging virtual machine and the target environment must be at the same patch and service pack level. If you have included applications in the base image, the applications must also be present in the packaging virtual machine.
- Packaging machine must be running and must not have any attached Packages, Applications, or Writable Volumes.

  If you have previously assigned any Application to the virtual machine, or if the virtual machine has been used for packaging before, that virtual machine should be set back to a clean snapshot before you begin packaging a new Application Package.
- In the VHD In-guest operating mode, ensure that the packaging machine used for packaging applications belongs to the same domain as the App Volumes Manager.

Note Applications installed by a non-admin user might not capture all application content. Administrators must ensure that only domain administrators or local administrators have the rights to capture applications on the packaging virtual machine.

Best Practices for Packaging Applications

You can follow some best practices while packaging applications on virtual machines used for the packaging process.

- Ensure that you have local administrator rights for packaging.
- Perform only one packaging process in each virtual machine. However, you can perform packaging on multiple virtual machines at the same time.
- If the packaging 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 Package as the application.
- The packaging system must not have antivirus agents, VMware Horizon with View agent, or any other filter driver applications installed or enabled.
- When packaging an application, always install the application for all users.

This practice ensures that the application is installed under Program Files rather than a single user profile and application icons are created in the All Users folder.

- 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 must be used with VMware Horizon with View Composer or other similar OS cloning technologies that preserve the machine SID.

  Some application requirements and licensing models require that the virtual machine shares a common SID with the production virtual machine.

- Virtual machines used for packaging must have a snapshot dedicated to the state of a user's desktop.

  After the packaging process, the virtual machine must be reverted to a clean state, that is the snapshot. A clean snapshot must have been created as part of the App Volumes agent installation.

- For optimum application compatibility, ensure that the same operating system is used to package and deliver the application.

Update a Package

You can create a new version of an existing Package by updating the existing Package. The existing Package becomes the base package or acts as a reference for the new version of the Package.

- Base Package information cannot be updated.
- Currently, **Update Package** functionality is not supported for creating a new version of an imported MSIX app attach format.

Prerequisites

Ensure that the Package you want to update has finished the packaging process and the Package status shows `Enabled`.

Procedure

1. From App Volumes Manager, go to **INVENTORY > Packages**.
2. Click the Package that has the `Enabled` status and click **Update**.
3. Update the Package information as per your requirements and click **Update**.

4 On the **Confirm Update Package** window, select one of the options and click **Update**.

Option	Action
Perform in the background	The Package gets updated in the background and you can perform other tasks.
Wait for completion	You must wait until the Package is updated. You cannot perform any other tasks until the Package update is over.

The newly updated Package details are displayed.

Set the CURRENT Marker on a Package

As an App Volumes administrator, when you mark a Package as `CURRENT` and you select the Assignment Type as `Marker`, the entity to which the Packaged Application is assigned always receives the latest version of the Application.

- Only one Package in an Application can be set as `CURRENT`.
- All entities with the `Marker` assignment type receive the Package marked as `CURRENT`.

Prerequisites

The Package that you want to mark as `CURRENT` must have completed the packaging process.

Procedure

1 From App Volumes Manager, go to **INVENTORY > Packages**.

2 Click the Package that has completed the packaging process.

Status of the Package, which has completed the packaging process, is `Enabled`.

3 Review the Package information and click **Set CURRENT**.

4 On the **Confirm Set CURRENT** window, click **Set CURRENT**.

Package is marked as `CURRENT`.

Unset the CURRENT Marker on a Package

Only one Package in an Application can be marked as `CURRENT`. To mark another Package of the Application as `CURRENT`, you must unset the `CURRENT` marker on the first Package.

When a `CURRENT` marker is removed from a Package, the entities which have the assignment type as `Marker` stop receiving the `CURRENT` Package.

Procedure

1 From App Volumes Manager, go to **INVENTORY > Packages**.

2 Click the Package marked as `CURRENT`.

3 On the **Packages** page, click **Unset CURRENT**.

Edit a Package

To change the metadata information of a Package, you can edit a Package. You can change the name and description of the Package.

Procedure

1. From App Volumes Manager, click **INVENTORY > Packages**.
2. Click the Package whose details you want to edit.
3. Click **Edit**.
4. Modify the information and click **Save**.

Results

A `Package updated successfully` message is displayed.

Move a Package

Packages can be moved from one Application to another. When similar Package requirements across Applications exist, you can use the move functionality.

When you move a Package which has an assigned entity, the entity also moves to the target application.

Prerequisites

Ensure that the Package you want to move has no `CURRENT` marker.

If the Package has a `CURRENT` marker, you must first unset the marker and then move the Package. Unset the CURRENT Marker on a Package

Procedure

1. From App Volumes Manager, go to **INVENTORY > Packages**.
2. Click the Package you want to move.
3. Click **Move**.

   If the Version you are moving is the only Version of the Previous Application, you can delete the Application if you want.
4. Select the Application that you want to move the Package to from the **Application** drop-down menu.

   If there are Assignments for the Package you are moving, the Assignments are listed.
5. Click **Move**.

6 (Optional) On the **Delete Application** window, click **Delete**.

If the Package you want to move is the only Package of the previous Application, then you can delete the Application. Deleting the Application also results in deleting the assignments to the Application.

What to do next

Navigate to the Application to which you moved the Package and review the Package information.

Delete a Package

You can delete a Package if you no longer need a Package or if the Package is not being used.

When you delete a Package, the assignments to the Package of type `Package` are also deleted.

Prerequisites

Ensure that the Package you want to delete is not in use.

Procedure

1 From App Volumes Manager, click **INVENTORY > Packages**.

2 Click the Package you want to delete.

3 Click **Delete**.

4 On the **Confirm Delete** window, click **Delete**.

Results

The Package is no longer listed in App Volumes Manager.

Working with Writable Volumes 7

With Writable Volumes, you can configure per-user volumes where users can install and configure their own applications and keep the data that is specific to their profile. 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.

This chapter includes the following topics:

- Writable Volume Exclusions
- Protecting Writable Volumes
- Selective Scenarios of Volume Types Delivered

Features of Writable Volumes

You can understand how Writable Volumes can be used with VMware Dynamic Environment Manager, behavior of Writable Volumes in a non-persistent virtual desktop, how Writable Volumes are used in a shared datastore, and how to exclude specific locations of Writable Volumes from being overwritten.

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. For more information, see Considerations When Specifying Exclusions in a Policy File (snapvol.cfg) and Format for Specifying Writable Volume Exclusions in a Policy File.

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 (2.x).
- 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.
- When App Volumes and VMware Dynamic Environment Manager are used together and a Dynamic Environment Manager condition references file or registry data on an App Volumes volume, the `All AppStacks Attached` trigger must be selected. This ensures that the Dynamic Environment Manager evaluates the condition after all volumes are attached.

For information about the `All AppStacks Attached` trigger, see *Configure Triggered Tasks* in the *VMware Dynamic Environment Manager Administration Guide*.

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.

View Writable Volumes Information

You can view the Writable Volumes and associated information created for various entities on the **Writable Volumes** page. You can view information such as filename (name of the writable volume), template type used while creating the Writable Volume, and the location at which the Writable Volume is created.

Procedure

1 From App Volumes Manager, click **INVENTORY > Writables**.

   On the **Writable Volumes** page, you can view the list of entities for whom Writable Volumes are created.

2 To view the Writable Volumes information for a particular entity, click the **+** sign next to the entity.

   Information such as filename (name of the Writable Volume), template type used while creating the Writable Volume, Disk size allocated for the Writable Volume, location at which the Writable Volume is created, and so on, are displayed.

3 (Optional) To view the location (shared datastore) at which the Writable Volume is created, click ***n*** **Location**.

   n - is the number of shared datastores.

   For information about Writable Volumes and shared datastores, see Support for Shared Datastores.

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 a two-way trust if an entity is searched for in the Active Directory forest. 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.

  To synchronize users with Active Directory, see Sync Entities with Active Directory.
- You must have uploaded the required Writable Volumes template to the datastore.

  Upload Templates

Procedure

1. From the App Volumes Manager console, select **INVENTORY > Writables**.
2. Click **Create**.
3. From the **Domain** drop-down menu, select a domain that is configured with App Volumes.
4. 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.
5. Click Search.

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

   If you are unable to locate the entity that you want, your account might not have read access to the domains you are searching, or the domains are not configured with two-way trust.
6. 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.

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

There are three types of templates available in App Volumes. See Configuring Storage 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 `appvolumes/writable_templates` folder.
Destination Path	The default path is *<varname>*`/appvolumes/writable`.
Source Template	Select a source template from the drop-down menu for the new Writable Volume. **Note** After you select a Writable Volume template type, later, you cannot change this to any other template type. For example, if you select the template type as UIA-only for a Writable Volume, you cannot change this to either UIA+profile or Profile-only.

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

Option	Description
Exception Resolution	Select one of the options below to choose how to resolve login issues when Writable Volumes are unavailable for attachments: ■ **Disable virtualization and alert user** - App Volumes disables all volume virtualization and a warning message is displayed when the user logs in. **Note** You can view the warning message under **ACTIVITY > System Messages**. ■ **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. **Note** Writable Volume conflict is not considered an error. Hence, this option is not triggered when there is a Writable Volume conflict at user login. App Volumes agent does not disable volume virtualization.
Limit delivery for these user Writable Volumes	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. 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.

Option	Description
Delay writable creation for group/OU members until they log in	Delay the creation of Writable Volumes for group and OU members until their next login. This option only affects groups and OUs. Users and computer entities that were directly selected have their volumes created immediately. Use this option when you select a group or an OU. Often these containers can have hundreds or thousands of members. This can be problematic because creating many volumes at the same time might take a long time. Some members might not need a Writable Volume.

9 Click **Create**.

10 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.

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

If you have Writable Volumes (2.x) created by using App Volumes Manager 2.x, you cannot import such Writable Volumes when using the latest version of App Volumes Manager.

To import Writable Volumes (2.x), see Import Writable Volumes (2.x)

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, click **INVENTORY > Writables**.

2 On the **Writable Volumes** page, click **Import**.

3 Select the datastore from the drop-down list.

4 Provide the path from where you want to import the Writable Volumes.

5 Click **Import**.

6 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.

After a Writable Volume is created, the default status of the Writable Volume is `Enabled`.

Prerequisites

Ensure that you have already created the volume you want to enable: Create a Writable Volume.

Procedure

1 From the App Volumes Manager, go to **INVENTORY > 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 make desired changes to the configuration files, add them to a specific folder, and create a ZIP file. When you upload this ZIP file to the Writable Volume, the volume gets updated. These updates are available to the end user the next time the user logs into the desktop.

Prerequisites

Ensure that you are aware of the following considerations:

- Updates made to the Writable Volume cannot be reversed.

  If a new ZIP file is uploaded to the Writable Volume, the existing updates get overwritten.

- User-installed applications that are already in the Writable Volumes cannot be changed.
- Size of the ZIP file must be smaller than `5 MB`.
- The ZIP file must consist of the following folder structure: `\Config\writable`.

  Configuration files such as the policy file (`snapvol.cfg`) and batch scripts can be added within `writable`.

  For an understanding of configuration files (policy files and scripts), see Configuration Files.

Procedure

1. On the App Volumes Manager console, navigate to **INVENTORY > Writables > Update Writable Volumes**.
2. Determine what configuration file must be uploaded.

Option	Task
Make changes in the existing configuration file.	a Download the current ZIP file. b Make the desired changes.
Create a configuration file.	Make the desired changes. For example, you can add exclusions in the policy (`snapvol.cfg`) file.

3. Place the configuration file in the following folder structure: `\Config\writable`.
4. Create a ZIP of the folder structure mentioned in the previous step and place it in a location that can be easily accessed for uploading the file to the Writable Volume.
5. Browse to the file location that you want to upload and select the file.

   Important If you upload the newly created configuration file to the Writable Volume, the existing file's content gets overwritten. To have a copy of the existing file, you can download the current ZIP file.

6. Click **Upload**.

Results

App Volumes Manager applies the ZIP file to every Writable Volume.

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 **INVENTORY > 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	Select one of the options to choose how to resolve login issues when Writable Volumes are unavailable for attachments: ■ **Disable virtualization and alert user** - App Volumes disables all volume virtualization and the user sees an alert upon login. **Note** You can view the warning message under **ACTIVITY > System Messages**. ■ **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. **Note** Writable Volume conflict is not considered an error. Hence, this option is not triggered when there is a Writable Volume conflict at user login. App Volumes agent does not disable volume virtualization.
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 where 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 delivery for these user Writable Volumes	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. 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.
Description	Enter a description for the Writable Volume.
Operating System	Select the additional OS for which you want to attach the Writable Volume. **Note** You cannot deselect the OS to which the volume was previously attached. **Note** If you select multiple operating systems, it might result in the volume becoming inoperable.

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.

To import Writable Volumes, see Import Writable Volumes.

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` on the **Writable Volumes** page in App Volumes Manager.

Expand a Writable Volume

You can specify a new size for a Writable Volume by 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.

Disk Size (Total) indicates the total disk space allocated for the Writable Volume. Disk Size (Free) indicates the remaining disk space if the Writable Volume already has some data.

Procedure

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

2 Click the **+** sign next to the entity whose Writable Volume you want to expand.

Along with other Writable Volume information, Disk Size is displayed.

3 Click **Expand**.

A **Confirm Expand** window is displayed.

4 On the **Confirm Expand** window, 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 entity logs in to the virtual machine.

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 in the `Enabled` status.

Procedure

1 From the App Volumes Manager, go to **INVENTORY > Writables**.

2 Select a Writable Volume and click **Disable**.

3 On the **Confirm Disable** window, click **Disable**.

   The status of the Writable Volume is `Disabled`.

Delete a Writable Volume

If a Writable Volume gets corrupted or when a user for whom the Writable Volume is created leaves the organization, administrators can delete the corresponding Writable Volume by using the Delete functionality.

When a volume is deleted, the volume gets immediately removed from the computer to which it is attached. All associated data and settings are also deleted permanently.

Prerequisites

As an administrator, you must 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 **INVENTORY > Writables**.

2 Select the entity whose Writable Volume you want to delete.

3 Click **Delete**.

4 On the **Confirm Disable** window, click **Delete**.

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.

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.

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.

For more information about moving Writable Volumes, 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 **INVENTORY > Writables**.

   A list of entities is displayed.
2. Select the entity whose Writable Volume 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 back up 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 **INVENTORY > Writables**.

2 Select the entity whose Writable Volume you want to back up.

3 Click **Backup**.

4 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.

5 (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.

6 Click **Backup**.

7 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.

8 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 attached and detached 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 attached and detached at least once 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* has been attached and detached at least once between Tuesday and Friday.

Restore a Writable Volume

As administrators, you can restore any single Writable Volume that was backed up when the Writable Volume gets corrupted. You can also restore a deleted Writable Volume. 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 **INVENTORY > Writables**.

A list of entities is displayed.

2 Select the entity for whom you want to restore the volume.

3 Click **Restore**.

4 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`.

5 Click **Restore**.

6 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.

Writable Volume Exclusions

You can specify certain locations of Writable Volumes to exclude them from being persisted across sessions. `exclude_uwv_file` and `exclude_uwv_reg` are the policy keywords that can be used for specifying exclusions in Writable Volumes.

Any content present in the location within the base image or application package is accessible, but changes to the content in these excluded locations do not persist across sessions.

You can consider these as some of the use cases for using `exclude_uwv_file` and `exclude_uwv_reg`:

- 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.

- If there are locations with large unwanted content, such as temporary `downloads` folder, adding Writable Volume exclusions helps in cleaning up the unwanted content within the Writable Volume.

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

Other policy keywords such as `exclude_path` and `exclude_reg` can also be used for specifying exclusions. For more information about these keywords, see Policy Files (snapvol.cfg).

Considerations When Specifying Exclusions in a Policy File (snapvol.cfg)

You can exclude certain locations from getting persisted on a Writable Volume by adding these exclusions in the policy file (`snapvol.cfg`). For applying these exclusions, you must be aware of some considerations.

Following is the list of considerations:

- Any content created or modified in the excluded location is lost when the user logs off the machine.

- 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 exclude paths within the user profile directories so that specific applications or files can be excluded from being persisted across sessions.

- Writable Volume exclusions for user profile paths are not applicable for UIA-only Writable Volumes because user profile is already excluded on UIA-only Writable Volumes.

- Ensure that you are aware of the application's behavior and the locations where the application's data gets stored.

  This understanding is necessary to prevent your application from functioning incorrectly when exclusions are applied to the Writable Volume that contains your application.

Format for Specifying Writable Volume Exclusions in a Policy File

`exclude_uwv_file` and `exclude_uwv_reg` are the keywords that are used to specify exclusions for Writable Volumes in the policy file, `snapvol.cfg`. By applying this customization, certain locations on a Writable Volume are excluded from being persisted across sessions.

To specify an exclusion, an entry must be added to the `snapvol.cfg` file in the following formats:

- `exclude_uwv_file=path`

  <path> is the path of the folder or subfolder that is specified to be excluded.

- `exclude_uwv_reg=path`

  <path> is the path of the registry key.

If the content of the location is not required to be persisted across sessions, then to exclude only the content and not the folder itself, *<path>* must end with two trailing backslashes \\.

Important Folders such as `Desktop`, `Downloads`, `Documents`, `Pictures`, `Music`, `Videos`, and `AppData`, are necessary for the OS to function correctly and they must not be specified as exclusions. If the trailing backslashes are not provided in the path when any of these folders are used, then the folder gets excluded and the OS might not function as expected.

For example:

- `exclude_uwv_file=\users\%username%\documents\\`

  In this example, if an end user creates a file or folder within `Documents`, the file or folder persists only for that session. When the end user logs off, the file or folder gets deleted.

- `exclude_uwv_reg=\REGISTRY\MACHINE\SOFTWARE\McAfee\\`

  In this example, if a new registry key or registry value is created within the folder `McAfee`, the new key or value persists for that particular session. When the end user logs off, the key or value is deleted.

For more information about the `exclude_uwv_file` and `exclude_uwv_reg` keywords used in the policy file, see Policy Files (snapvol.cfg).

To upload the policy file that contains the exclusions to the Writable Volume, see Update Writable Volumes.

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.

Selective Scenarios of Volume Types Delivered

Users and computers can have different volume types (application packages and Writable Volumes) delivered. This section provides information about how different combinations of volumes are delivered in certain scenarios as the user logs into the computer.

In the following table, in each scenario, an application package, Writable Volume, or a combination of both is presented. The result for each of these scenarios is then listed.

	Computer		Users		
Scenario	**Application**	**Writable Volume**	**Application**	**Writable Volume**	**Result**
1	No	Yes	No	Yes	■ Computer Writable Volume is attached. ■ User Writable Volume is not attached.
2	No	Yes	Yes	No	■ Computer Writable Volume is attached. ■ Application package is not delivered.

	Computer		Users		
Scenario	**Application**	**Writable Volume**	**Application**	**Writable Volume**	**Result**
3	No	Yes	Yes	Yes	■ Computer Writable Volume is attached. ■ User Writable Volume is not attached and application package is not delivered.
4	Yes	No	No	Yes	■ Computer-assigned application package is delivered. ■ User Writable Volume is not attached.
5	Yes	No	Yes	Yes	■ Computer-assigned application package is delivered. ■ User-assigned application package is not delivered and user Writable Volume is not attached.
6	Yes	Yes	No	Yes	■ Computer Writable Volume is attached and computer-assigned application package is delivered. ■ User Writable Volume is not attached.

	Computer		Users		
Scenario	Application	Writable Volume	Application	Writable Volume	Result
7	Yes	Yes	Yes	No	■ Computer Writable Volume is attached and computer-assigned application package is delivered. ■ User-assigned application package is not delivered.
8	Yes	Yes	Yes	Yes	■ Computer Writable Volume is attached and computer-assigned application package is delivered. ■ User-assigned application package is not delivered and user Writable Volume is not attached.

Working with Programs 8

Programs are executables contained within a Package and are installed during the packaging process. You can use the **Programs** tab to view the list of Programs that are used by the Packages.

After installation on the packaging machine, Programs are available in the Programs and Features section of Windows.

By using the **Programs** tab, you can also identify duplicate Programs if installed and determine conflicts at install location of the Programs.

This chapter includes the following topics:

View Programs

You can view the list of Programs on the **Programs** page. You can view information such as name of the Program, Application version number, publisher of the Program, Package associated with the Program, and so on.

Procedure

1 From App Volumes Manager, click **INVENTORY > Programs**.

2 Click the Program name whose details you want to view.

3 View the Program details such as Package name, Publisher, install location of the Program, and Application version number.

4 (Optional) To view the Package details, click the Package name.

Working with Attachments

9

You can use the **Attachments** tab to view the list of Application Packages and Writable Volumes that are attached to a host computer (virtual machine).

When a user logs into a virtual machine to access an application, the App Volumes Agent attaches the Package and Writable Volume to the virtual machine. After these are attached, the administrator for App Volumes Manager can view the package and Writable Volume on the **Attachments** page of the **Inventory** tab.

This chapter includes the following topics:

View Attachments

By using the **Attachments** tab, you can view the list of Packages and Writable Volumes that are delivered and currently in use. You can view information such as the Application for which the Package and Writable Volume is created, host computer to which the Package or Writable Volume is attached to, mount type, assignment (type), and so on.

Procedure

1 From App Volumes Manager, click **INVENTORY > Attachments**.

2 View the details of each attached Package and Writable Volume.

Packages and Writable Volumes are listed in the **Volume** column.

Working with Assignments 10

An Application can be assigned to an entity. With the option for attaching assignments to specific computers, entities can have multiple assignments. By using the **Assignments** tab, you can view the list of Applications assigned to entities.

Entities are `Users`, `Computers`, `Groups`, or `OU (Organizational Units)`.

For more information about understanding Assignment types, see Understanding Assignment Types.

For information about the limit delivery for these assignments, see Application Assignment to Specific Computers. To gain an understanding of different assignment scenarios when entities (Users, Groups, and OUs) are associated with specific computers, see Assignment Scenarios.

This chapter includes the following topics:

View Assignments

On the **Assignments** page, you can view a list of Applications and associated Packages that are currently assigned to Users, Groups, Computers, or OUs (Organizational Units).

The **Computers** column displays a list of values that are prefixes of computer names. The value indicates that when the non-computer entity logs into a computer whose name starts with a particular prefix, then the application package gets attached only to that specific computer.

If the application package assigned to the non-computer entity applies to all computers, then the value displayed is `all`. This value indicates that the assignment is attached to any computer.

Procedure

1. From App Volumes Manager, click **INVENTORY > Assignments**.
2. To view the details of each entity assignment, click the *Entity* name.

   Entity can be a user, group, computers, or OU (Organizational Unit).

   Depending on the *Entity* that you have selected, the corresponding **Entity** details page is displayed.

Perform App Volumes 2.x Management Tasks

11

If you have upgraded from App Volumes Manager 2.x, you can skip this section. This section provides information for users who have installed the latest version of App Volumes Manager and need to enable AppStacks and Writable Volumes (2.x).

App Volumes Manager supports the co-existence of both Application Packages and AppStacks. Similar to creating and managing Application Packages and Writable Volumes, you can also create and manage AppStacks and Writable Volumes (2.x) by using the App Volumes Manager UI.

To perform tasks by using App Volumes 2.x, you must have the appropriate App Volumes Agent, templates for AppStacks and Writable Volumes (2.x), and enabled **VOLUMES (2.X)** in **Advanced Settings**:

1. Download the App Volumes 2.18 build from the VMware download page and extract the App Volumes zip file.
2. Install the Agent on a virtual machine different from the one where the latest version of App Volumes Agent has been installed.

   To install the Agent, see the *VMware App Volumes Installation Guide* at VMware Docs.
3. Download the templates for AppStacks and Writable Volumes (2.x).
4. On the virtual machine where you have installed the latest App Volumes Manager, save these templates as follows:
   - Save the AppStacks templates at `CloudVolumes\Manager\ppv\appstacks2x_templates`
   - Save the Writable Volumes (2.x) templates at `CloudVolumes\Manager\ppv\writables2x_templates`

   When creating AppStacks or Writable Volumes (2.x), these templates must be uploaded to the datastores.
5. Enable VOLUMES (2.X)

   Note If you have installed the latest version of App Volumes Manager on a new database, the 2.x toggle switch is off by default.

This chapter includes the following topics:

Enable VOLUMES (2.X)

Latest version of App Volumes Manager has a toggle switch that helps in supporting the co-existence of both Application Packages and AppStacks. When this switch is turned on, **VOLUMES (2.X)** is restored to the top navigation and other 2.x-related features required for creating and managing AppStacks and Writable Volumes (2.x) are available.

For a better understanding of when to use the toggle switch, see Chapter 11 Perform App Volumes 2.x Management Tasks.

Procedure

1. From App Volumes Manager, go to **CONFIGURATION > Settings**.
2. On the **Settings** page, click **Advanced Settings**.
3. Click the **Enable Volumes (2.x)** toggle switch.

   By default, **Enable Volumes (2.x)** is off.
4. Refresh App Volumes Manager.

   VOLUMES (2.X) tab and other 2.x-related features are enabled in the UI.

What to do next

By using **VOLUMES (2.X)**, you can now create and manage AppStacks and Writable Volumes (2.x) and view list of Attachments and Assignments.

Working with Volumes and the 2.*x* App Volumes Agent

12

After upgrading from App Volumes Manager 2.*x*, you can continue creating AppStacks and Writable Volumes (2.*x*) by using the current version of App Volumes Manager. This version of App Volumes Manager supports the co-existence of Application Packages, Writable Volumes for the current version and 2.*x*, and AppStacks.

Hence, you can use the current version of App Volumes Manager UI to create Application Packages and Writable Volumes.

When AppStacks and Writable Volumes (2.*x*) are not in use, you can disable the **VOLUMES (2.X)** tab and other 2.x-related features in the App Volumes Manager UI by using a toggle switch, **Enable Volumes (2.x)**. This switch helps you configure the visibility and management of App Volumes Manager 2.*x* UI any time. You can find this switch in the **Advanced Settings** page of the UI.

For example, this switch can be used to turn off 2.x-related features after migrating the AppStacks and Writable Volumes (2.*x*) from App Volumes Manager 2.*x*.

Note When you upgrade from App Volumes Manager 2.*x*, this switch is on by default.

For more information about how to enable or disable the App Volumes Manager 2.*x* UI features, see Configuring visibility and management of App Volumes Manager 2.x UI.

For information about creating Application Packages, see Chapter 5 Working with Applications and Chapter 6 Working with Packages. For information about creating Writable Volumes in the latest version, see Chapter 7 Working with Writable Volumes .

This chapter includes the following topics:

- Working with AppStacks
- Working with Writable Volumes (2.x)
- Working with Attachments
- Working with Assignments
- Configuring visibility and management of App Volumes Manager 2.x UI

Working with AppStacks

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.

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

Before provisioning an AppStack, you must prepare the virtual machine used for provisioning by following certain criteria.

The criteria for preparing a provisioning machine is as follows:

- AppStacks must be provisioned on a clean base image (virtual machine), which closely resembles the target environment to which you later plan to deploy the AppStack.

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

- Provisioning must be performed on a virtual machine that does not have any assigned AppStacks.

  If you have previously assigned any AppStack 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 virtual machine.

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.

Prerequisites

You must have uploaded the template for AppStacks to the datastore.

Upload Templates

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

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 canot 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 (2.X) > AppStacks**.

   A list of AppStacks are displayed.
2. Select the 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 delivery for these assignments**.
   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

View the complete list of AppStack assignments and manage them.

Working with Assignments

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

View the complete list of AppStack assignments and manage them.

Working with Assignments

Assign an AppStack to an OU (Organizational Unit)

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 (2.X) > 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 > OUs**.

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 delivery for these assignments** 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

View the complete list of AppStack assignments and manage them.

Working with Assignments

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 (2.X) > 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

View the latest information about the available AppStacks.

Check Datastores for 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 (2.X) > 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.
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 (2.X) > AppStack**.

2 Click **Import**.

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

4 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 (2.X) > 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, import the AppStacks, and make the AppStacks known to the App Volumes Manager that you are logged in to.

Import AppStacks to App Volumes

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 (2.X) > 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 oneAppStack 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 (2.X) > 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

Display a list of the updated and available AppStacks by using the Rescan functionality.

Check Datastores for Available AppStacks

Working with Writable Volumes (2.x)

An entity can have both Writable Volumes and Writable Volumes (2.*X*). Entities logging into virtual machines with App Volumes Agent 2.*x* receive only Writable Volumes (2.*x*) and entities logging into virtual machines with the latest version of App Volumes Agent receive only Writable Volumes.

With Writable Volumes (2.*X*), you can continue performing actions such as import, enable, update, move, backup, restore, and so on.

For an understanding of Writable Volumes, see Chapter 7 Working with Writable Volumes and Features of Writable Volumes.

To understand the considerations for assigning Writable Volumes to an entity, see Assigning and Attaching Writable Volumes.

To understand Writable Volumes Exclusions, see Writable Volume Exclusions and to protect Writable Volumes, see Protecting Writable Volumes.

Create a Writable Volume (2.x)

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 a two-way trust if an entity is searched for in the Active Directory forest. 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.
- You must have uploaded the required Writable Volumes template to the datastore.

  Upload Templates

Procedure

1. From the App Volumes Manager console, select **VOLUMES (2.X) > Writables**.
2. Click **Create**.
3. From the **Domain** drop-down menu, select a domain that is configured with App Volumes.
4. 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.
5. Click **Search**.

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

   If you are unable to locate the entity that you want, your account might not have read access to the domains you are searching, or the domains are not configured with two-way trust.
6. 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.

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

There are three types of templates available in App Volumes. See Configuring Storage 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 `cloudvolumes/writable_templates` folder.
Destination Path	The default path is *<varname>*`/cloudvolumes/writable`.
Source Template	Select a source template from the drop-down menu for the new Writable Volume: ■ Profile-only ■ UIA only ■ UIA+profile **Note** After you select a Writable Volume template type, later, you cannot change this to any other template type. For example, if you select the template type as UIA-only for a Writable Volume, you cannot change this to either UIA+profile or Profile-only.

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

Option	Description
Exception Resolution	Select one of the options below to choose how to resolve login issues when Writable Volumes are unavailable for attachments: ■ **Disable virtualization and alert user** - App Volumes disables all volume virtualization and a warning message is displayed when the user logs in. **Note** You can view the warning message under **ACTVITY > System Messages**. ■ **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. **Note** Writable Volume conflict is not considered an error. Hence, this option is not triggered when there is a Writable Volume conflict at user login. App Volumes agent does not disable volume virtualization.
Limit delivery for these user Writable Volumes	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. 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.

Option	Description
Delay writable creation for group/OU members until they log in	Delay the creation of Writable Volumes for group and OU members until their next login. This option only affects groups and OUs. Users and computer entities that were directly selected have their volumes created immediately. Use this option when you select a group or an OU. Often these containers can have hundreds or thousands of members. This can be problematic because creating many volumes at the same time might take a long time. Some members might not need a Writable Volume.

9 Click **Create**.

10 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 (2.X) > Writables** and verify that the volume you just created has the status set to Enabled.

Import Writable Volumes (2.x)

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 (2.X) > Writables**.

2 Click **Import**.

3 Select the datastore from the drop-down list.

4 Provide the path from where you want to import the Writable Volumes.

5 Click **Import**.

6 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

Update the list of Writable Volumes in the App Volumes Manager by using the Rescan functionality.

Check Datastores for Available AppStacks

Enable a Writable Volume (2.x)

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 (2.x).

Procedure

1 From the App Volumes Manager, go to **VOLUMES (2.X) > 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 (2.x)

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 (2.X) > Writables**.
2. Click **Update**.
3. Browse and select the ZIP file.
4. Click **Upload**.

Edit a Writable Volume (2.x)

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 (2.X) > 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	Select one of the options to choose how to resolve login issues when Writable Volumes are unavailable for attachments: ■ **Disable virtualization and alert user** - App Volumes disables all volume virtualization and the user sees an alert upon login. **Note** You can view the warning message under **ACTVITY > System Messages**. ■ **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. **Note** Writable Volume conflict is not considered an error. Hence, this option is not triggered when there is a Writable Volume conflict at user login. App Volumes agent does not disable volume virtualization.
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 where 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.

Option	Description
Limit delivery for these user Writable Volumes	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. 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.
Description	Enter a description for the Writable Volume.
Operating System	Select the additional OS for which you want to attach the Writable Volume. **Note** You cannot deselect the OS to which the volume was previously attached. **Note** If you select multiple operating systems, it might result in the volume becoming inoperable.

4 Click **Save**.

Rescan Writable Volumes (2.x)

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 (2.x) 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 (2.x)

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 (2.X) > 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 (2.x) to a Computer

If you want to rename a computer (entity) which has a Writable Volume (2.x) assigned, then you must transfer Writable Volume (2.x) 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 (2.x) 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 (2.x) that must be reassigned.
3. On the **entity_name** page, identify the Writable Volume (2.x) 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 (2.x) 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 (2.x), 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 (2.x) page in the **VOLUMES (2.X) > Writables** tab.

Disable a Writable Volume (2.x)

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 (2.X) > Writables**.

2 Select a Writable Volume and click **Disable**.

3 Click **Disable** on the **Confirm Disable** window.

Delete a Writable Volume (2.x)

You can delete a Writable Volume.

When a volume is deleted, the volume gets immediately removed from the computer to which it is attached. 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 (2.X) > 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.

Move a Writable Volume (2.x)

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 (2.X) > 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 (2.x)

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 (2.X) > 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 for 2.x

Set up App Volumes Manager to take regular backups of the Writable Volumes (2.x).

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 attached and detached 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 For **Writable Volume Backups (2.x)**, 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 attached and detached at least once 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* has been attached and detached between Tuesday and Friday.

Restore a Writable Volume (2.x)

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 (2.X) > 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.

Specify Exclusions in a Writable Volume (2.*x*) (Configuration File)

You can specify certain locations of Writable Volumes (2.*x*) to exclude them from persisting across sessions or getting overwritten.

For more information about Writable Volume Exclusions, see Writable Volume Exclusions.

Prerequisites

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

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

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

Procedure

1. Log in as administrator to the machine where the App Volumes agent is installed.
2. Locate and open the writable volumes configuration file, `snapvol.cfg`.
3. Add the following entry in the `snapvol.cfg` file, where *path* is the location of the application or registry that you want to exclude: `exclude_uwv=`*`path`*.

   You can specify multiple exclusions.

Example: Exclude an Application Location

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

- `exclude_uwv_file=\Program Files (x86)\Notepad++`
- `exclude_uwv_file=\REGISTRY\MACHINE\SOFTWARE\Notepad++`
- `exclude_uwv_file=\Users\`*`username`*`\`*`folder`*

- `exclude_uwv_file=\Users\`*`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.

Working with Attachments

You can use the **Attachments** tab to view the list of AppStacks that are attached to a host computer (virtual machine).

When a user logs into a virtual machine to access an application, the App Volumes Agent attaches an AppStack to the virtual machine. After the AppStacks gets attached to the virtual machine, the administrator for App Volumes Manager can view the AppStack on the **Attachments** page of the **VOLUMES (2.X)** tab.

View Attachments (2.x)

By using the **Attachments** tab, you can view the list of AppStacks and Writable Volumes that are attached to a host computer.

Procedure

1. From App Volumes Manager, click **VOLUMES (2.X) > Attachments**.
2. Click the Program name whose details you want to view.
3. View the Program details such as Package name, Publisher, install location of the Program, and Application version number.
4. (Optional) To view the Package details, click the Package name.

Working with Assignments

An entity can be assigned to an AppStack. Entities can be Users, Computers, Groups, or OU (Organizational Units). The **Assignments** page for **VOLUMES (2.X)** lists entities only which are assigned to AppStacks.

By using the **Assignments** tab, you can view the list of entities assigned to all the AppStacks.

For more information about assigning and attaching AppStacks to an entity, see Assigning and Attaching AppStacks.

View Assignments (2.x)

On the **Assignments (2.x)** page, you can view the list of AppStacks that are currently assigned to Users, Computers, Groups, or OUs (Organizational Units).

An entity can be a User, Computer, Group, or OU (Organizational Unit).

The AppStacks assigned to the entities are availabe while using App Volumes 2.x Agent.

Procedure

1 From App Volumes Manager, click **VOLUMES (2.X) > Assignments**.

2 View the details of each entity assignment.

Configuring visibility and management of App Volumes Manager 2.x UI

When you upgrade from App Volumes Manager 2.x, the UI supports co-existence of both Application Packages and AppStacks. If AppStacks and Writable Volumes (2.x) are not in use after migrating from 2.x, you can disable the 2.x-related features in the UI by using the **Enable Volumes (2.x)** toggle switch.

Prerequisites

If you have decided to disable the 2.x-related UI features, ensure the following:

- You have upgraded to the latest version of App Volumes Agent.
- You have migrated AppStacks and Writable Volumes (2.x) to the latest version of App Volumes template format.

Procedure

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

2 On the **Settings** page, click **Advanced Settings**.

3 To disable the **VOLUMES (2.X)** tab and other 2.x-related information, click the **Enable Volumes (2.x)** toggle switch.

By default, **Enable Volumes (2.x)** is on.

4 Refresh App Volumes Manager .

VOLUMES (2.X) tab and other 2.x-related features are disabled from the UI.

Configure Infrastructure

13

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

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.

Note AppStacks and Writable Volumes (2.*x*) can be created only by using App Volumes Agent 2.*x* and uploading the appropriate templates. Any information related to these volumes can be viewed only when the **VOLUMES (2.X)** tab is visible in the App Volumes Manager UI. If you have installed the latest version of App Volumes Manager and want to explore App Volumes 2.*x*, see Chapter 11 Perform App Volumes 2.x Management Tasks.

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 storage location.

Information such as whether the storage is attachable, used and total storage available, UUID, number of AppStacks, number of Packages, number of Writables, and so on are displayed.

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. You also have the option of marking a storage read-only so that App Volumes Manager can skip writing to that storage when updating a package or an AppStack.

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

When you configure 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 configure the slower-performing storage as **Set Not Attachable**. A storage thus configured as not attachable is ignored by the manager while mounting volumes and the storage can be used solely for replication of packages and AppStacks.

If the metadata of a package or an AppStack is updated and the package or AppStack is replicated from a read-only storage, App Volumes Manager skips writing the updates to the read-only storage, but the package or AppStack gets replicated. The replicated package or AppStack does not have the updated metadata. You have the option of removing the read-only marker on the storage.

Note AppStacks and Writable Volumes (2.x) can be created only by using App Volumes Agent 2.x and uploading the appropriate templates. Any information related to these volumes can be viewed only when the **VOLUMES (2.X)** tab is visible in the App Volumes Manager UI. If you have installed the latest version of App Volumes Manager and want to explore App Volumes 2.x, see Chapter 11 Perform App Volumes 2.x Management Tasks.

Procedure

1. To see the list of storage locations that are visible to the App Volumes Manager, click **INFRASTRUCTURE > Storages**.
2. To see the details of a storage such as the current attachable and read-only statuses and other information, click the storage name that you desire to view.
3. Select the storage whose status you want to change.
4. Depending on the current attachable status of the storage, click **Set Attachable** or **Set Not Attachable** and confirm the operation.
5. Depending on the current read-only status of the storage, click **Mark Read-only** or **Unmark Read-only** and confirm the operation.

Results

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

Configure Storage Groups

Storage groups can be used to automatically replicate Packages and AppStacks and distribute Writable Volumes across multiple datastores. You can configure storage groups by using the App Volumes Manager.

You can specify a group of datastores that contain the same application packages or AppStacks and by using the vCenter, App Volumes replicates the `.vmdk` files across the datastores for redundancy and scalability.

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.

Note AppStacks and Writable Volumes (2.*x*) can be created only by using App Volumes Agent 2.*x* and uploading the appropriate templates. Any information related to these volumes can be viewed only when the **VOLUMES (2.X)** tab is visible in the App Volumes Manager UI. If you have installed the latest version of App Volumes Manager and want to explore App Volumes 2.*x*, see Chapter 11 Perform App Volumes 2.x Management Tasks.

Procedure

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

You can directly select 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	■ Select **Automatically Import AppStacks and Packages** ■ Select **Automatically Replicate AppStacks and Packages** The **Automatically Import AppStacks and Packages** option can be used to control the automatic import of new AppStacks and Packages found in the storage locations. This option does not change the import behavior of AppStacks and Packages that are replicated within the same App Volumes Manager instance. In this scenario, the volumes are always imported after replication.
Distribution Strategy	Select how you want the files to be distributed: ■ **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	■ 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 To create a group for a specific location, select a storage location.

5 Click **Create.**

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

Advanced App Volumes Configuration

14

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:

Configuration Files

VMware provides configuration files - policy files (`snapvol.cfg`) and script files - which control how Writable Volumes and application packages function alongside the OS. You can customize these files for application and OS compatibility.

App Volumes can be configured with an application package, a Writable Volume, or a combination of both. The configuration files are loaded (or executed) corresponding to each volume, which gets attached to a given virtual machine.

Default and Custom Configuration Files

The configuration files are divided into two categories: Default and Custom. The Default set is created by the App Volumes agent installer. The Custom set does not exist by default, but can be created in specific folders on the base image, Writable Volume, or an application package. App Volumes has the capability to load (or execute) these files.

As the application packages are read-only, App Volumes allows the creation of custom configuration files for application packages on the base image. These files can then be used for all the application packages which get attached to the virtual machine. If configuration files are required for a particular application package, the configuration files can be placed in the application package after initiating the update package workflow in App Volumes Manager.

To upload the configuration files to all the Writable Volumes, it is recommended to use the update Writable Volumes workflow in App Volumes Manager. For more information, see Update a Package.

Note There is no support for adding custom configuration files to Writable Volumes on the base image.

A directory structure is used for default and custom configuration files on the base image, provisioning volume, Writable Volumes, and application packages. On the base image these files are located in the App Volumes installation directory, identified by %SVAgent% environment variable. This variable is created during the installation of App Volumes agent.

Default Configuration Files

The default set of configuration files might get modified with a newer version of App Volumes. Therefore, these configuration files are not preserved across App Volumes upgrades.

Important

- VMware does not recommend changing the content of the configuration files and cannot guarantee if the changes are forward compatible.

  If you must modify the content of the configuration files, create a backup of the modified files and place the files back after the upgrade, if the files are still supported.

- Deletion of the default configuration files is not supported.

  If any configuration file is deleted, the deletion can cause App Volumes to malfunction.

The following table lists the type of volumes and their corresponding default configuration directories:

Volume Type	Configuration Directory
System Volume	`%SVAgent%\Config\Default`
Profile-only Writable Volume	`%SVAgent%\Config\Default\profile`
UIA only Writable Volume	`%SVAgent%\Config\Default\uia`
UIA+profile Writable Volume	`%SVAgent%\Config\Default\uia_plus_profile`
Application Volume	`%SVAgent%\Config\Default\app`
Provisioning Volume	`%SVAgent%\Config\Default\provisioning`

Custom Configuration Files

The following table lists the type of volumes and their corresponding custom configuration directories. Any changes made to the files in the custom configuration directories are persisted across App Volumes upgrades.

Volume Type	Configuration Directories
System Volume	`%SVAgent%\Config\Custom`
Profile-only Writable Volume	`C:\SnapVolumesTemp\MountPoints\{Writable Volume Guid}\{Writable Guid}\Config\writable`
UIA only Writable Volume	`C:\SnapVolumesTemp\MountPoints\{Writable Volume Guid}\{Writable Guid}\Config\writable`
UIA+profile Writable Volume	`C:\SnapVolumesTemp\MountPoints\{Writable Volume Guid}\{Writable Guid}\Config\writable`
Application Volume	■ `C:\SnapVolumesTemp\MountPoints\{Appstack Volume Guid}\{App Guid}\Config\app` ■ `C:\SnapVolumesTemp\MountPoints\{Writable Volume Guid}\{Writable Guid}\Config\app` ■ `%SVAgent%\Config\Custom\app`
Provisioning Volume	`%SVAgent%\Config\Custom\provisioning`

Note When configuration files are created at `%SVAgent%\Config\Custom\app` or `C:\SnapVolumesTemp\MountPoints\{Writable Volume Guid}\{Writable Guid}\Config\App`, the configuration files are applicable for all the application packages which get attached to a particular VDI pool. Whereas when configuration files are created at `C:\SnapVolumesTemp\MountPoints\{Appstack Volume Guid}\{App Guid}\Config\app`, the configuration files are only applicable for that particular application package.

Policy Files (snapvol.cfg)

Policy files (`snapvol.cfg`) contain rules that control how files and registries are virtualized (or excluded from virtualization) from the base virtual machine, Writable Volumes, and application packages. These rules are specified through name-value pairs of policy keywords and their values.

These policy files also contain rules to control if processes with a specific application name or residing within a specific directory must be excluded from virtualization.

Most of the inclusion and exclusion rules are applicable for all the application packages and Writable Volumes. These rules are placed in a policy file outside the volume-specific folders located at `%SVAgent%\Config\Default\snapvol.cfg`. If you want to add inclusion or exclusion rules, you must create a custom policy file at `%SVAgent%\Config\Custom\snapvol.cfg` and add the rules in the file.

Some of the considerations when creating or modifying the policy files at `%SVAgent%\Config\Custom\snapvol.cfg` are as follows:

- A file system or registry “virtualize” policy keyword-based rules are specific to the Writable Volumes and application packages, so the policy files can only be created in the configuration directory for a Writable Volume or an application package.
- Rules present in the custom policy files are applied in addition to the rules present in the default policy files.

Definition of Terms: Virtualized and Excluded from Virtualization

The terms are defined as follows:

Virtualized

When a user or an application views the contents of a folder or registry key, the content of that folder or registry key is merged at runtime (to contain unique entities) from the base virtual machine, Writable Volumes, and all the application packages assigned to the user or virtual machine. Similarly, when a user or an application tries to access the contents of a file or a registry value, the data is fetched from the highest precedence location, where Writable Volumes have the highest precedence followed by application packages and the base virtual machine.

Excluded from Virtualization

When a user or application views a file, folder, registry key, or registry value, the content of that object is only retrieved from the base virtual machine, ignoring the presence (or absence) of that object from the Writable Volumes and application packages.

Policy Keywords

To provide more information about the rules within the policy files, the following table provides a brief description on some of the frequently used rules, which can be configured to customize a Writable Volume or an application package:

Keyword	Description	Examples
`exclude_path`	During a read or write operation, App Volumes excludes looking for any file or folder in the path specified in this keyword in either the application package or the Writable Volume. Instead, if the file or folder specified in the path is present in the base image, then the read or write operation is performed in the base image. **Note** Any file or folder starting with the prefix value specified in the keyword is excluded.	`exclude_path=\ProgramData\VMware` App Volumes excludes looking for `VMware` in either the application package or Writable Volume. Instead, if `VMware` is present in the base image then the read or write operation on the folder is performed in the base image.
`include_path`	App Volumes reads any file or folder in the path specified in this keyword in the following order: Writable Volumes, application package, and the base image. Any write operation in this path is performed on the Writable Volume. **Note** Any file or folder starting with the prefix value specified in the keyword is included.	`include_path=\Users` App Volumes reads all subfolders of `Users` from all the volumes: Writable Volume, application package, and the base image. If an end user creates a folder or file within `Users`, then the file or folder is created on the Writable Volume.
`exclude_registry`	During a read or write operation, App Volumes excludes looking for any registry key or registry value in the path specified in this keyword in either the application package or Writable Volume. Instead, if the registry key or registry value specified in the path is present in the base image, then the read or write operation is performed in the base image. **Note** Any registry key or registry value starting with the prefix value specified in the keyword is excluded.	`exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Policies` App Volumes excludes looking for any registry key or registry value specified within `Policies` in either the application package or Writable Volume. Instead if the path is present in the base image, then the read or write operation is performed on the registry key or registry value in the base image.
`include_registry`	App Volumes reads any registry key or registry value in the path specified in this keyword in the following order: Writable Volume, application package, and the base image. Any write operation in this path is performed on the Writable Volume. **Note** Any registry key or registry value starting with the prefix value specified in the keyword is included.	`include_registry=\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows Search` App Volumes reads all registry keys and registry values at `\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows Search` from all volumes: Writable Volume, application package, and base image. If a registry key or registry value is created at this path, then this operation is performed on the Writable Volume.

Keyword	Description	Examples
`exclude_process_path`	All processes that are run from an executable file in this path or subpath only see the file system and registry content from the base image. **Note** - This rule is not applicable to the child processes. - Any process name starting with the prefix value specified in the keyword is excluded.	`exclude_process_path=\Program Files\VMWare \AppCapture` Any executable file run from the `AppCapture` folder or its subfolders only sees the file system and registry content from the base image. If the process spawns a new child process, the child process sees contents from the Writable Volume, AppStack, and base image.
`include_process_name`	The process specified in this keyword sees the file system and registry content from the Writable Volume, AppStack, and base image. **Note** This rule is not applicable to the child processes.	`include_process_name=SearchIndexer.exe` The `SearchIndexer` process sees the file system and registry content from all volumes.
`exclude_process_name`	The process specified in this keyword sees the file system and registry content only from the base image. **Note** This rule is not applicable to the child processes.	`exclude_process_name=chkdsk.exe` The `chkdsk` process sees the file system and registry content only from the base image.

The following table contains keywords that can be used to customize in the policy for Writable Volumes only:

Keyword	Description	Examples
`exclude_uwv_file`	App Volumes reads any file or folder in the path specified in this keyword in the following order: Writable Volume, application package, and the base image. Any write operation to the file or folder in this path is performed on the Writable Volume, which persists for that particular session, but gets deleted when the user logs off from the computer. **Note** ■ Any file or folder starting with the prefix value specified in the keyword is excluded. ■ The path specified in this keyword must be terminated by using \\.	`exclude_uwv_file=%USERPROFILE%\AppData\Local\Temp\\` App Volumes reads any content present within the `Temp` folder from all volumes: Writable Volume, application package, and base image. If an end-user creates a file `example.txt` within `Temp`, then the file persists for that session. When the end user logs off, `example.txt` is deleted.
`exclude_uwv_reg`	App Volumes reads any registry key or registry value in the path specified in this keyword in the following order: Writable Volume, application package, and the base image. Any write operation to the registry key or registry value in this path is performed on the Writable Volume, which persists for that particular session, but gets deleted when the user logs out from the computer. **Note** ■ Any registry key or registry value starting with the prefix value specified in the keyword is excluded. ■ The path specified in this keyword must be terminated by using \\.	`exclude_uwv_reg=\REGISTRY\MACHINE\SOFTWARE\McAfee\\` App Volumes reads any registry key or registry value within `McAfee` from all the volumes: Writable Volume, application package, and the base image. If a new registry key or registry value is created within `McAfee`, the new key or value persists for that particular session. When the end user logs out, the key or value is deleted.

There are a few rules which are meant for internal purposes and required for proper functioning of App Volumes might be present in a policy file. VMware does not recommend making changes to these internal rules in either the default or custom policy files. Changes to these rules are not supported. The rules are listed as follows:

- `virtualize`
- `virtualize_registry`
- `virtualize_registry_notify_change`
- `reverse_replicate_file`
- `delete_local_profile`

Options for Adding Custom Policy Rules in App Volumes

To add the custom rules, VMware recommends that you use the policy file in the base image. App Volumes provides multiple options for modifying the policy files for Writable Volumes or application packages. Depending on your requirement, you can create or modify the policy file at the corresponding volume locations.

Note As per the security policy of App Volumes, you can access the configuration directory on a Writable Volume or an application package only through a process running with high integrity such as an elevated command prompt. You cannot access the configuration directory through Windows Explorer.

The following are the options for adding the custom policy rules:

- VMware recommends that for adding custom rules, the policy file at `%SVAgent%\Config\Custom\Snapvol.cfg` in the base image must be used.

  If the policy file does not exist, a new (empty) file must be created and custom rules must be added in the file.

- If modifying the base image is not possible and you are using a Writable Volume, then to update your policy file you can use the update Writable Volume feature in App Volumes Manager.

  The policy file is uploaded to all the Writable Volumes, as and when they get attached to a virtual machine.

  For more information about updating Writable Volumes, see Update Writable Volumes.

- If you want to have different policies within multiple Writable Volumes, you must create multiple Writable Volume templates.

  Each Writable Volume template must have a different set of custom rules in `\Config\Writable\Snapvol.cfg`, located in the root of the Writable Volume template.

  For example, consider two active directory groups: AD1 and AD2. If you want a different set of policies for each group, you can create two different Writable Volume templates with the respective policies. When assigning Writable Volumes for each group, you can select the respective Writable Volume template specifically created for each group.

- If you want the custom rules only for a particular Writable Volume or an application package, you can browse to the configuration directory of that volume and create or modify the `snapvol.cfg` in the corresponding location.

  If you want to add custom rules to an application package, the application package must be edited offline.

  For more information about the configuration directories for default and custom configuration files, see Default and Custom Configuration Files.

Batch Scripts for App Volumes workflow

Scripts files can be used to configure the App Volumes workflow before or after the virtualization of individual application packages or Writable Volumes. You can use script files to modify the application and OS compatibility and for user or enterprise-specific requirements.

The script files are only applicable to a Writable Volume or an application package, so they are located inside the volume-specific default folders. There are multiple different scripts and these scripts get triggered at different events during the virtualization of each Writable Volume and application package. Some of these scripts are run in the system service context while others are run in the context of the logged-in user.

Note Based on the content of the configuration batch scripts, executing them might have an impact on the performance of end-user login experience. Desktop and application availability might be delayed in some cases.

Internal Batch Scripts for App Volumes

The following table provides information about the default scripts which are either created by the App Volumes installer or can be created by the administrator in the default volume-specific folders (`%SVAgent\Config\Default\`*<VolumeType>*):

Important These scripts are only read from the default configuration directories. If the scripts are created in any other location on the base image, Writable Volume, or application package, then such scripts are ignored. VMware does not recommend changing these scripts because the changes are not preserved across App Volumes upgrades.

For more information about the default configuration directories, see Default and Custom Configuration Files.

Script Name	Execution Context	Description
`Prestartup.bat`	System context	Before file and registry database (index information) is read from Writable Volume or an application package.
`Startup.bat`	System context	Before virtualizing a Writable Volume or an application package. Application is still not available to the user at this stage.
`Logon.bat`	User context	Before virtualizing a Writable Volume or an application package. Application is still not available to the user at this stage.
`Shellstart.bat`	User context	After virtualization has started for a Writable Volume or an application package, but before services from that package have started.
`Startup_postsvc.bat`	System context	After virtualization has started and after services from an application package or a Writable Volume have started.

Script Name	Execution Context	Description
`Logon_postsvc.bat`	User context	After virtualization has started and after services from an application package or a Writable Volume have started.
`Allvolattached.bat`	System context	After virtualization has started for all the application packages assigned to the user.
`Allvolattached_shellstarted.bat`	User context	After virtualization has started for all the application packages assigned to the user.
`Shellstop.bat`	User context	During logoff processing, before virtualization is stopped for all the application packages and Writable Volumes.
`Logoff.bat`	User context	During logoff processing, after virtualization is stopped for all the application packages and Writable Volumes.

Customizable Batch Scripts for App Volumes

You can create or modify a different set of scripts in the custom configuration directories, which are not affected by App Volumes agent upgrades. These scripts run only in the context of the system service account. For more information about the default configuration directories, see Default and Custom Configuration Files.

The following table lists these scripts and their corresponding trigger events:

Script Name	Execution Context	Description
`OnPreLoadApp.bat`	System context	Before file and registry database (index information) is read from the Writable Volume or an application package .
`OnPostLoadApp.bat`	System context	After Writable Volume or application file/registry database (index information) is read from the Writable Volume or an application package. Application is still not available to the user at this stage.
`OnPreEnableApp.bat`	System context	Before virtualizing a Writable Volume or an application package. Application is not available to the user at this stage.
`OnPostEnableApp.bat`	System context	After virtualizing a Writable Volume or an application package. Application is already available to the user at this stage.

Script Name	Execution Context	Description
`OnPreDisableApp.bat`	System context	Before stopping virtualization for a Writable Volume or an application package. Application is still available to the user at this stage.
`OnPostDisableApp.bat`	System context	After stopping virtualization for a Writable Volume or an application package. Application is no longer available to the user at this stage.

Note To run a custom script in the user context, you can add an entry in the registry key, `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` in the base virtual machine, Writable Volume, or application package.

Precedence order of configuration directories

If a custom script file is present in multiple locations, the script file is executed only from the highest precedent configuration location and other versions of the script are ignored.

Precedence order of configuration directories when an application package is processed:

1 `C:\SnapVolumesTemp\MountPoints\{Appstack Volume Guid}\{App Guid}\Config\App`

2 `C:\SnapVolumesTemp\MountPoints\{Writable Volume Guid}\{Writable Guid}\Config\App`

3 `%SVAgent%\Config\Custom\App`

4 `%SVAgent%\Config\Default\App`

Precedence order of configuration directories when a Writable Volume is processed:

1 `C:\SnapVolumesTemp\MountPoints\{Writable Volume Guid}\{Writable Guid}\Config\Writable`

2 `%SVAgent%\Config\Custom\`*`<Writable Type>`*

The values of Writable type are `profile`, `uia`, or `uia_plus_profile`.

3 `%SVAgent%\Config\Default\`*`<Writable Type>`*

The values of Writable type are `profile`, `uia`, or `uia_plus_profile`.

Configuration of 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.

For a list of parameters that can be used to configure svdriver, see Parameters for Configuring svdriver.

For a list of parameters that can be used to configure svservice, see Parameters for Configuring svservice.

Parameters for Configuring svdriver

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

Configure svdriver with the following registry keys:

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

Configuring Drive Letter Settings

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

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

Configure this behaviour with the *DriveLetterSettings* registry value. The value for *DriveLetterSettings* is in a hexadecimal format, and any number of flags might be combined to implement multiple parameters.

Value	Description
0x0000004	DRIVELETTER_HIDE_WRITABLE. Hide drive letter for writable volumes.
0x0000008	DRIVELETTER_HIDE_READONLY. Hide drive letter for AppStack volumes.

By default, a drive letter is not assigned to either application packages or Writable Volumes.

Parameters for Configuring svservice

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

svservice Log Deletion Policy

If a backup svservice log file meets either of these policy rules, the log file is deleted:

- If the aggregate size of all the backup log files is greater than a designated number, then svservice starts the deletion from the oldest backup log file until the aggregate size is lower than the designated number.

  You can use the `BackupLogFileSizeInKB` parameter to set the designated aggregate size of all backup log files.

- If a backup log file is older than the designated number of days, the log file is deleted.

  You can use the `BackupLogFileDays` parameter to designate the number of days for the log deletion policy.

svservice Parameters

Parameter	Type	Description
`LogFileSizeInKB`	REG_DWORD	The size of the log file before rotating the log file. The default value of this parameter is `15360MB (15MB)` and the maximum value of this parameter is `51200 (50MB)`. **Note** If the parameter is set to a value greater than the maximum value or `0`, svservice uses the default value as the value of this parameter.
`BackupLogFileSizeInKB`	REG_DWORD	The aggregate size of all svservice backup log files. If the aggregate size of all backup log files is greater than the value of this parameter, svservice starts the deletion from the oldest backup log file until the aggregate size is lesser than the value of this parameter. The default value of this parameter is `768000 (750MB)` and the maximum value is `3584000 (3500MB)`. **Note** If the parameter is set to `0` or greater than the maximum value, svservice uses the default value as the value of this parameter.
`BackupLogFileDays`	REG_DWORD	The maximum age of svservice backup log files. If a svservice backup log file is older than the value of this parameter, the backup log file is deleted. The default value of this parameter is `15 days`.
`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 300 seconds (5 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.

Parameter	Type	Description
`ConnectTimeOutMs`	REG_DWORD	Defined in milliseconds for server connection requests. If a connection request takes longer than this timeout value, the request is canceled. The default is 10 seconds.
`SendTimeOutMs`	REG_DWORD	Defined in milliseconds for sending requests. If sending a request takes longer than this timeout value, the request is canceled. The default is 30 seconds.
`ReceiveTimeOutMs`	REG_DWORD	Defined in milliseconds to receive a response to a request. If a response takes longer than this timeout value, the request is canceled. The default is 5 minutes.
`ProvisioningCompleteTimeOut`	REG_DWORD	Defined in seconds to keep trying to contact the App Volumes Manager after provisioning is completed. The default is 120.
`DomainNameWaitTimeOut`	REG_DWORD	Defined in seconds how long to wait for the computer during startup to resolve Active Directory domain name. On machines that are not joined to any domain, you can set the value to 1 for faster login. The default is 60.
`DelayVirtualizationType`	REG_DWORD	Defers application virtualization at end user login and helps in improving the user login time. Values of this parameter are as follows: ■ `0` - Applications are virtualized (enabled for end user)) as soon as the end user enters the login credentials. ■ `1` - Applications are virtualized after the end user enters the login credentials. ■ `2` - Applications are virtualized just before the desktop is visible to the end user. ■ `3` - Applications are virtualized a few seconds after the desktop is visible to the end user. The default value of this parameter is `2`.
`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. **Note** When `WaitForFirstVolumeOnly` parameter is set to `0`, svservice implicitly sets the `DelayVirtualizationType` parameter value to `0`.

Configuring the Volume Behavior Parameters

You can configure the volume behavior parameters for SVservice with the `CleanSystemWritable` registry key.

Parameter	Type	Description
CleanSystemWritable	REG_DWORD	If set to 1 and no writable volumes are attached, SVservice clears any changes saved to the system during operation after a reboot. If set to 0, changes are stored in c:\SVROOT on system volume. The default value is 0.

Configuring the General Behavior Parameters

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

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

Create a Custom vCenter Server Role

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

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

You can also use PowerCLI to create a custom role. See Create a Custom vCenter Server Role Using PowerCLI.

Procedure

1 Manually create a new vCenter Server role.

2 Assign privileges to the role.

Object	Permission
Cryptographic Operations	**Direct Access** **Note** This permission is required only when the virtual machine’s storage has encryption policies.
Datastore	■ **Allocate space** ■ **Browse datastore** ■ **Low-level file operations** ■ **Remove file** ■ **Update virtual machine files**

Object	Permission
Folder	- **Create folder** - **Delete folder**
Global	**Cancel task**
Host	- **Create virtual machine** - **Delete virtual machine** - **Reconfigure virtual machine**
Resource	**Assign virtual machine to resource pool**
Sessions	**View and stop sessions**
Tasks	**Create task**
Virtual machine > Configuration	- **Add existing disk** - **Add new disk** - **Add or remove device** - **Change resource** - **Query unowned files** - **Remove disk** - **Settings** - **Advanced**
Interaction	- **Power Off** - **Power On** - **Suspend**
Inventory	- **Create from existing** - **Create new** - **Move** - **Register** - **Remove** - **Unregister**
Provisioning	- **Clone template** - **Clone virtual machine** - **Create template from virtual machine** - **Customize** - **Deploy template** - **Mark as template** - **Mark as virtual machine** - **Modify customization specifications** - **Promote disks** - **Read customization specifications**

Create a Custom vCenter Server Role Using PowerCLI

You can create custom vCenter Server roles by using PowerCLI.

CryptographicOperations.DirectAccess is required only when the virtual machine's storage has encryption policies.

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
CryptographicOperations.DirectAccess
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
   ```

Update Database Credentials For App Volumes Manager

You can update the connection details for App Volumes Manager by updating the database credentials. Your database connection can use either the Windows Integrated authentication method or the SQL Authentication method.

App Volumes Manager UI displays ODBC errors, which can help you troubleshoot `database.yml` file syntax issues.

When the App Volumes Manager service starts, the cleartext password is replaced by an encrypted stamp.

Prerequisites

While editing the `.yml` file, ensure that you follow the YAML syntax.

Procedure

1. On the virtual machine that runs the App Volumes Manager service, stop the service.
2. In the **Control Panel**, open the **ODBC Data Source Administrator (32-bit)** tool.

   Attention You must perform the rest of the procedure for the ODBC Data Source Administrator (64-bit). Only then the database connection details get updated.

3. In the **System DSN** tab, select `svmanager`.
4. Click **Configure**.

5 Depending on the mechanism used by your database to connect to the App Volumes Manager server, perform the following steps:

Option	Steps
Integrated Windows Authentication	a On the **Microsoft SQL Server DSN Configuration** window, select the Server. b Click **Next**. c Select **With Integrated Windows authentication**. d Click **Next**. e Continue verifying the settings as per your requirement. f Click **Finish**. g Test the connection and save the settings.
SQL Authentication	a On the **Microsoft SQL Server DSN Configuration** window, select the Server. b Click **Next**. c Select **With SQL Server authentication using a login ID and password entered by the user**. d Click **Next**. e Make changes as per your requirement and click **Finish**. f Test the connection and save the settings. g In the location where you have installed App Volumes, navigate to the `config` folder. For example: `C:\Program Files (x86)\CloudVolumes\Manager\config` h Make a copy of the `database.yml` file as `database.yml.bkp`. i Edit the `database.yml` file by using a text editor. j In the file, after `production`, add the new *username* and *password*. k Start the App Volumes Manager service.

6 Follow the same procedure for ODBC Data Source Administrator (64-bit).

Using the App Volumes Application Capture Command-Line Program

15

The App Volumes Application Capture Command-Line Program is a standalone, Windows command-line software program. Use this program to easily automate the process of capturing applications by working with packages outside of App Volumes Manager console.

This program allows you to capture application installs into a package as a `.vhd` and `.vmdk` (monolithic sparse) file outside of App Volumes Manager and App Volumes agent. Before delivering the package to the end users, you can use the program to test and validate the application package.

After the capture and validation, you can manually transfer the application package into App Volumes Manager to assign and deliver the package to the end users.

Using the program's command-line arguments, you can create a `.json` metadata file as required by App Volumes to process an MSIX app attach format and convert this package to `.vmdk` (monolithic sparse). You can transfer the `.vhd` and `.vmdk` files along with the `.json` file to App Volumes Manager and import the packages into the admin UI. Further, you can deliver these packages to the end user.

This chapter describes some of the workflows that you can run using the command-line arguments of the program.

To install the software, see the *VMware App Volumes Installation Guide*.

This chapter includes the following topics:

How to Run the App Volumes Application Capture Command-Line Program

You can run the App Volumes Application Capture Command-Line Program using the `appcapture.exe` command on the Windows command line. To run the command-line capture program, you can also use the Microsoft PowerShell commands.

Using this program, you can capture an application install, update an existing application, and test and validate the application package before delivering the package to the end users.

Capture an Application

A standard capture workflow constitutes of starting a command-line capture program session, installing the application, and completing the capture session. To start and end the capture, `appcapture.exe /new` and `appcapture.exe /end` commands are used respectively.

After the capture completes, the program creates an application package in the `.vmdk` (monolithic sparse) and `.vhd` formats. In addition to the package file formats, the program also generates a `.json` file which has the metadata for the generated packages. Later, you can manually transfer this application package into App Volumes Manager and deliver the package to the end users.

You can use the `/noauto` argument with `/new` and `/end`. For more information about these command-line arguments and others, see Windows Command-Line Arguments for the App Volumes Application Capture Command-Line Program . Alternately, you use `appcapture.exe /help` on the command line.

Prerequisites

- Ensure that you start a new capture every time on a clean virtual machine.
- Ensure that the User Account Control (UAC) in Windows is disabled.

  To disable UAC, see Microsoft Windows documentation.
- You must run the command-line capture program as an administrator.
- Ensure that the command-line capture program utility is installed at `C:\Program Files (x86)\VMware\AppCapture`.

  Note Do not use the command-line capture program's executable located at `C:\Program Files (x86)\CloudVolumes\Agent`. This copy of the executable is meant for internal purpose only.
- Ensure that you have downloaded the installer of the application that must be captured.
- Ensure that you are aware of the command-line arguments that can be used with the `appcapture.exe` command.

Procedure

1 Take a snapshot of your virtual machine.

  You can revert to the snapshot after the capture session.

2 Open a command-line window.

3 Start a new capture session from the location where the command-line capture program is installed by using the following command: `appcapture.exe /new <package_name>`.

   package_name - name of the application package that is captured.

4 Install the application that you want to capture.

   a If your application install requires a virtual machine reboot, perform the reboot or wait for the reboot to complete.

      The command-line capture program session automatically restarts.

5 Finish the capture session by using the following command: `appcapture.exe /end`.

   Machine reboots and the command-line capture program session automatically restarts.

   The capture process is complete and the application package is created in the `vhd` and `.vmdk` (monolithic sparse) formats.

6 Ensure that the following outputs *package_name*`.vhd`, *package_name_workstation*`.vmdk`, and *package_name*`.json` are generated at `C:\ProgramData\VMware\AppCapture\appvhds`.

7 Revert to the virtual machine's snapshot taken before you started the capture session.

What to do next

- To import the `*_workstation.vmdk` package into App Volumes Manager, place the `.vmdk` and `.json` files on the App Volumes Manager server at `<installation_directory>\CloudVolumes\Manager\ppv\packages`, upload these files to the desired datastore from the **Storage** page in the admin UI by using Upload Templates, and follow the Import an Application to App Volumes procedure.
- To import the `.vhd` application package into App Volumes Manager, copy the package (including the `.json` file) to a file share and follow the Import an Application to App Volumes procedure.

After the package is successfully imported into App Volumes Manager, you can assign the application and deliver the package to the end users.

Update an Application

To update an existing application which has been captured, use the `/s` argument in the `appcapture.exe` command. The command-line capture program creates a copy of the existing package's disk (`.vhd` format) and updates the disk.

You can use the `/noauto` argument with `/new` and `/end`. For more information about these and other command-line arguments, see Windows Command-Line Arguments for the App Volumes Application Capture Command-Line Program . Alternately, you can use `appcapture.exe /help` on the command line.

Prerequisites

- Ensure that you perform this task on a clean virtual machine.

- Ensure that the User Account Control (UAC) in Windows is disabled.

  To disable UAC, see Microsoft Windows documentation.
- You must run the command-line capture program as administrator.
- Ensure that the command-line capture program utility is installed at `C:\Program Files (x86)\VMware\AppCapture`.

  Note Do not use the command-line capture program's executable located at `C:\Program Files (x86)\CloudVolumes\Agent`. This copy of the executable is meant for internal purpose only.
- Ensure that you have the path of the `.vhd` file of the existing, captured application.

  This path is used as the source when starting the capture session.

  See Capture an Application.
- Ensure that you have downloaded the installer of the application that needs to be updated.
- Ensure that you are aware of the command-line arguments that can be used with the `appcapture.exe` command.

Procedure

1 Take a snapshot of your virtual machine.

You can revert to the snapshot after the capture session.

2 Open a command-line window.

3 Update the existing application package from the location where the command-line capture program is installed by using the following command: `appcapture.exe /new <package_name> /s <source_vhd_filepath>`.

- *package_name* - name of the application package that is updated.

  Important *<package_name>* must be different from the name provided during the application's initial capture session.
- *source_vhd_filepath* is the source path of the captured application's `.vhd` file.

4 Install the application updates.

a If your application install requires a virtual machine reboot, perform the reboot or wait for the reboot to complete.

The command-line capture program session automatically restarts.

5 Finish the capture session by using the following command: `appcapture.exe /end`.

Machine reboots and the command-line capture program session automatically restarts.

This completes the update process and the application package is created in the `vhd` and `.vmdk` formats.

6 Ensure that the following outputs *package_name*.vhd, *package_name_workstation*.vmdk, and *package_name*.json are generated at C:\ProgramData\VMware\AppCapture\appvhds.

7 Revert to the virtual machine's snapshot taken before you started the capture session.

What to do next

- To import the *_workstation.vmdk package into App Volumes Manager, place the .vmdk and .json files on the App Volumes Manager server at <installation_directory>\CloudVolumes\Manager\ppv\packages and upload these files to the desired datastore from the **Storage** page in the admin UI.

  For more information about uploading these files, see Upload Templates.

- To import the .vhd application package into App Volumes Manager, copy the package (including the .json file) to a file share and follow the Import an Application to App Volumes procedure.

After the package is successfully imported into App Volumes Manager, you can assign the application and deliver the package to the end users.

Test a Captured Application

Using the App Volumes Application Capture Command-Line Program, you can test and validate the captured application before delivering the application package to the end users. To test the captured application, the appcapture.exe /test command uses the .vhd format of the application package.

When the appcapture.exe /test runs, the application is dynamically available on the virtual machine used for testing purpose. At a time, only one application package can be tested per session.

Prerequisites

- Ensure that you perform this task on a clean virtual machine.
- Ensure that the User Account Control (UAC) in Windows is disabled.

  To disable UAC, see the relevant Microsoft Windows documentation.

- You must have already captured the application that you want to test and validate.

  See Capture an Application.

- Copy the .vhd format of the application package to a file share accessible by the virtual machine used for testing.
- Ensure that you test and validate the application package on a clean virtual machine different from the machine used for capturing the application.

- Ensure that the command-line capture program is installed at `C:\Program Files (x86)\VMware\AppCapture`.

  Note Do not use the command-line capture program's executable located at `C:\Program Files (x86)\CloudVolumes\Agent`. This copy of the executable is meant for internal purpose only.

- You must run the command-line capture program as administrator.
- Ensure that you are aware of the command-line arguments that can be used with the `appcapture.exe` command.

  For more information about the command-line arguments, see Windows Command-Line Arguments for the App Volumes Application Capture Command-Line Program . Alternately, you can use `appcapture.exe /help` on the command line.

Procedure

1. Take a snapshot of your virtual machine.

   You can revert to the snapshot after testing and validating the application. It is recommended that you revert to this snapshot between two successive test sessions.

2. Open a command-line window.
3. Start the test session for an application package from the location where the command-line capture program is installed by using the following command: `appcapture.exe /test <source_path_.vhd_file>`.

   <source_path_.vhd_file> is the path of the `.vhd` file of the application package that is tested.

   Application is now enabled for testing.

4. Test and validate the application.
5. To end the test session, use the following command: `appcapture.exe /testend`.

   Application is removed from the virtual machine and is no longer available for testing.

6. If you intend to test and validate another application, then revert to the snapshot taken before you started the test session for this application.

Windows Command-Line Arguments for the App Volumes Application Capture Command-Line Program

This section lists the command-line arguments that are used with `appcapture.exe` to achieve tasks such as create a capture, update an existing application, end a capture session, and so on, using the command-line capture program. Some of these arguments are mandatory while few are optional.

The following table lists the command-line arguments and tasks accomplished using these arguments:

Note Command-line arguments for an MSIX app attach format are not supported for capturing packages in the App Volumes format.

Command-line Argument	Task	Examples
/help	Displays the list of arguments and their description that can be used with the `appcapture.exe` command.	`appcapture.exe /help`
/new *<package_name>*	Start a capture session for a new application or update an existing application. This argument is mandatory. Following files are created in a capture session: `.vmdk`, `.vhd`, and `.json`. By default, the files are located at `C:\ProgramData\VMware\AppCapture\appvhds`. **Note** Only the following arguments can be used with /new: `/d, /s, /a, and /novmdk`. To see the usage of `/new`, see Capture an Application.	Example: `appcapture.exe /new MyApp` `MyApp` is the name of the package generated when the MyApp application is captured.
/d *<disk_description>*	Specify comments that identify the content in the output file while running a new capture session or updating an existing application. The disk description can be viewed in the App Volumes Manager admin UI as part of the package description. This argument is optional.	Example: `appcpature.exe /new MyApp /d "This package contains the MyApp application."`

Command-line Argument	Task	Examples
/s *<source_vhd_filepath>*	Update an existing (already captured) application by using the captured application's `.vhd` file as the source. This argument is optional. **Note** Do not use this argument when capturing a new application. To see the usage of /s, see Update an Application	Example: `appcapture.exe /new MyApp_update /s C:\ProgramData\VMware\AppCapture\appvhds\MyApp.vhd` - `MyApp_update` - name of the package. **Note** This name must be different from the name provided during the initial application capture. - `MyApp.vhd` - existing application package created during the application's initial capture. The command-line capture program uses this file as the source and creates an updated package (`MyApp_update.vhd`).
/o *output_dir*	Customize the location of the output files created in a capture session by specifying the path to the directory where the files must be saved. This argument is optional. By default, the output files are located at `C:\ProgramData\VMware\AppCapture\appvhd`. **Note** /o can be used only with the following: `/new, /meta, /vmdk, /vhd`.	Example: `appcapture.exe /new MyApp /o C:\ProgramData\VMware\AppCapture\appvhds\MyApp_dir` After the capture session, `MyApp_dir` contains `MyApp_workstation.vmdk`, `MyApp.vhd`, and `MyApp.json`.
/novmdk	Prevents the creation of the `.vmdk` format of the application package. This argument is optional and can be used when you need only the `.vhd` format of the application package. By default, after a capture session, the program creates a `.vmdk` file for the captured application. When this argument is provided, the `.vmdk` file is not created.	Example: `appcapture.exe /new MyApp /novmdk` `MyApp.vhd` and `MyApp.json` are created.

Command-line Argument	Task	Examples

/end	Completes the capture session which was started by using `/new`.
	When `/end` is used, the machine reboots and the command-line capture program automatically restarts. This completes the capture process. `.vhd` and `.vmdk` package formats are generated along with the `.json` metadata file.
	This argument is mandatory.
	To see the usage of this argument, see Capture an Application.
		Example:
		`appcapture.exe /new MyApp`
		`.........................`
		`.........................`
		`appcapture.exe /end`
		By default, `MyApp.vhd`, `MyApp_workstation.vmdk`, and `MyApp.json` are created at `C:\ProgramData\VMware\AppCapture\appvhds`.

/noauto	Prevents the program from automatically restarting after a machine reboot. This argument is optional and can be used only with `/new` and `/end`. In some scenarios such as during capture completion and at times during application installation, the machine reboots. In either case, the command-line capture program automatically restarts on its own. At times you might want to perform some custom initialization task and prevent the automatic restart of the program. In such cases, you can use the `/noauto` argument. After the machine reboots, to restart the program and complete the capture session, `/resume` must be used.	Examples: ■ `appcapture.exe /new MyApp /noauto` ■ `appcapture. exe /end /noauto`

/resume	Resumes the command-line capture program after a machine reboot.
	This argument is mandatory if you have used the `/noauto` argument while starting (`/new`) or ending (`/end`) a capture session.
		Example:
		`appcapture.exe /new MyApp_test /noauto`
		`...............................`
		`....`
		`...............................`
		`....`
		`appcapture.exe /resume`

/cancel	Cancels the capture session that was started using `/new`.
	The capture session gets cancelled and the machine reboots. It is recommended that you revert to a clean snapshot before you start a new capture session.
		Example:
		`appcapture.exe /new MyApp`
		`.........................`
		`.........................`
		`appcapture.exe /cancel`

Command-line Argument	Task	Examples
/test *source_vhd_filepath*	Tests and validates the captured application using the application's `.vhd` package format. When this argument is used, the program attaches the package to the virtual machine and enables the application bundles in the package for testing. To use the `/test` parameter, you must revert to a clean snapshot, different from the one used for application capture. To see the usage of this argument, see Test a Captured Application.	Example: `appcapture.exe /test C:\ProgramData\VMware\AppCapture\appvhds\test_dir\MyApp.vhd` The application package, `MyApp.vhd` at `C:\ProgramData\VMware\AppCapture\appvhds\test_dir` is attached to the virtual machine and enabled for testing.
/testend	Ends the test session. If you intend to test and validate another application, then revert to the snapshot taken before you started the test session for this application.	Example: `appcapture.exe /testend`
/list *<vhd, vmdk, or json filepath>*	Prints the package information.	Example: `appcapture.exe /list C:\ProgramData\VMware\AppCapture\appvhds\MyApp_workstation.vmdk`
/meta *<vhd or vmdk filepath>*	Creates a `.json` metadata file for a captured application using the application's `.vmdk` or `.vhd` file as the source. By default, the `.json` file is created in the same path as that of the source.	Examples: `appcapture.exe /meta C:\ProgramData\VMware\AppCapture\appvhds\MyApp_workstation.vmdk` `MyApp.json` is created at `C:\ProgramData\VMware\AppCapture\appvhds\`.
/vmdk *vhd_filepath*	Creates a `.vmdk` file using the application's `.vhd` file as the source.	Example: `appcapture.exe /vmdk C:\ProgramData\VMware\AppCapture\appvhds\MyApp.vhd` Using `MyApp.vhd` as the source, the program creates `MyApp_workstation.vmdk`. By default, the `.vmdk` file is located at the same path as the `.vhd` file. In the example, `MyApp_workstation.vmdk` is created at `C:\ProgramData\VMware\AppCapture\appvhds`.

Command-line Argument	Task	Examples
/vhd *vmdk_filepath*	Creates a `.vhd` file using the application's `.vmdk` file as the source. In case you have misplaced or accidentally deleted the `.vhd` file, you can use this argument to create the file.	Example: `appcapture.exe /vhd C:\ProgramData\VMware\AppCapture\appvhds\MyApp_workstation.vmdk` Using `MyApp_workstation.vmdk` as the source, the program creates `MyApp.vhd`. By default, the `.vhd` file is located at the same path as the `.vmdk` file. In the example, `MyApp.vhd` is created at `C:\ProgramData\VMware\AppCapture\appvhds`.
/addmeta *vhd_filepath*	Creates a `.json` metadata file as required by App Volumes to process an MSIX app attach format. **Note** Prior to using the `/addmeta` argument, ensure that the VHD is not already mounted. If the VHD is mounted, you must unmount the VHD and then run the argument. After creating the metadata for the MSIX app attach format, you can copy the `.vhd` and `.json` files to a file share and import the package to App Volumes Manager by following the Import an Application to App Volumes procedure.	

Command-line Argument	Task	Examples
/msix *root_path*	Specifies the location of the unpacked MSIX inside the MSIX app attach format. **Note** This argument must be used with `/addmeta <vhd_filepath>` while creating the `.json` file.	Example: `appcapture.exe /addmeta "C:\VHDs\MyApp.vhd" /msix "WindowsApps \MyApp_1.0.0.0_x64__97zz0k7g87g 9t"` A `.json` metadata file is created for the `MyApp.vhd` package, which is an MSIX app attach format. This metadata file is created at `C:\VHDs`. `WindowsApps \MyApp_1.0.0.0_x64__97zz0k7g87g9t` specifies the location of the unpacked MSIX inside the MSIX app attach format.
/msixvmdk *vhd_filepath*	Converts the MSIX app attach format to `.vmdk` (monolithic sparse). To import the `.vmdk` into App Volumes Manager, you must rename the file to `*_workstation.vmdk` and follow the procedure that is similar to importing a `.vmdk` package after capturing an application. For more information, see the *What to do next* section in Capture an Application.	Example: `appcapture.exe /msixvmdk "C:\VHDs\MyApp.vhd"` Converts `MyApp.vhd` to `.vmdk`.

Microsoft PowerShell Cmdlets for the App Volumes Application Capture Command-Line Program

You can use the 32-bit or the 64-bit PowerShell console to run the App Volumes Application Capture Command-Line Program. This section lists the PowerShell cmdlets that can be used to run the program.

The following table lists the cmdlets and tasks accomplished using these cmdlets. Some of these cmdlets have multiple parameters. For more information about the cmdlets, use `get-help <cmdlet_name>` on the PowerShell console.

Command-line Argument	Task
`ConvertTo-AVVhdDisk`	Converts a `.vmdk` format file to a `.vhd` format file.
`ConvertTo-AVVmdkDisk`	Converts a `.vhd` format file to a `.vmdk` format file.
`Export-AVMetadata`	Exports the metadata associated with the `.vhd` or `.vmdk` file.

Command-line Argument	Task
`Reset-AVConfig`	Resets the configuration information stored on the machine. `Start-AVAppCapture` and `Start-AVAppUpdate` stores some configuration information on the machine as part of their workflow.
`Reset-AVTask`	Cancels a running capture or update session started with `Start-AVAppCapture` and `Start-AVAppUpdate` respectively. **Note** The machine automatically reboots after the session is cancelled.
`Reset-AVTest`	Cancels the test session started with `Start-AVTest`.
`Resume-AVTask`	If `NoAuto` switch is specified with `Start-AVAppCapture`, `Start-AVAppUpdate`, or `Stop-AVTask`, then the command-line capture program does not restart automatically after a machine reboot. To manually continue the program, this cmdlet must be used.
`Show-AVDiskDetails`	Displays the application and disk details of the given file (`.vhd`, `.vmdk`, or `.json`).
`Start-AVAppCapture`	Captures an application into a `.vhd` file.
`Start-AVAppUpdate`	Updates a previously captured (using `Start-AVAppCapture`) application.
`Start-AVTest`	Attaches the application package (`.vhd`) and enables application bundles for user guided testing.
`Stop-AVTask`	Finish and finalize a session started with either `Start-AVAppCapture` or `Start-AVAppUpdate`.
`Stop-AVTest`	Finish the test session initiated with `Start-AVTest`.

Troubleshooting App Volumes 16

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:

- [VHD] Future Logins for Users Is Blocked When Deleted Volume Attachments Are Not Removed from App Volumes Manager
- Disable Restarting the Spooler Service When Using VMware Integrated Printing

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.

Firewall Rules in Application Package or Writable Volume displayed twice

When a Firewall rule is present in the application package or Writable Volume, the firewall console might display the same rule twice. This is redundant and does not have any impact on the functionality of App Volumes.

Reduce End-User Login Time If There Is a Connection Failure with App Volumes Manager

If there is a consistent connection failure between the agent machine and App Volumes Manager, the end-user login time can be reduced by setting the registry value of `RetryStartupRequestFrequency` parameter to `0` in the agent base image.

The parameter’s registry value indicates the interval in seconds between retries. Setting the value to zero stops the agent machine from retrying the communication.

KeyName	`HKLM\SYSTEM\CurrentControlSet\Services\svservice\Parameters`
ValueName	`RetryStartupRequestFrequency`
ValueType	DWORD
ValueData	`0`

After setting the registry value, to deploy the base image in the Horizon pool, you must restart the agent machine.

[VHD] Future Logins for Users Is Blocked When Deleted Volume Attachments Are Not Removed from App Volumes Manager

In VHD In-Guest Operation mode, sometimes when instant-clone desktops are deleted, the application packages and Writable Volumes attached to these desktops are not removed from App Volumes Manager. This prevents future user logins to new instant-clone desktops.

The issue occurs when App Volumes Manager is unavailable and at the same time an instant-clone desktop sends a request to App Volumes Manager during a user logout or computer shutdown. By the time App Volumes Manager comes online, the desktops are deleted and new desktops are created. As a result, App Volumes Manager does not receive these requests.

So, the volume attachments and online desktop entries in the App Volumes Manager database do not get updated and the application packages and Writable Volumes continue to appear as attached to the deleted desktops. This prevents future login of users to newly created instant-clone desktops and the following error is displayed to the end user: `You may be logged in more than once. please try logging in again , or contact administrator. Virtualization is disabled.`

Workaround

Blocked entries must be removed from the `snapvol_attachments` table present in the configured database.

Note The deleted desktops might still be listed in the **DIRECTORY > Online** tab of the App Volumes Manager UI. However, the listed entries do not affect the App Volumes Manager operations.

Disable Restarting the Spooler Service When Using VMware Integrated Printing

When using VMware Integrated Printing, if the spooler service takes a long time to restart, the local printer to remote desktop mapping fails on a user's second login. As a result, printers are not redirected to the remote desktops and the end users are unable to see any local printers.

Problem

This problem occurs in a Horizon VDI environment with a remote desktop running App Volumes agent that has Writable Volumes.

Cause

This problem occurs because the spooler service takes a long time to restart.

Solution

To stop the spooler service from restarting, set the registry value of `DisableSpoolerRestart` to `DWORD`, 1 at `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\svservice\Parameters`.