App Volume Documentation

Release 0.1.0

App Volume Team

May 19, 2017

Contents

Welcome to AppVolumes Manual

This is a great product

Head

code sample

```
const appVolume = new AppVolumes(config)
```

Summary

Manager

- Dashboard
- Volumes
    - AppStacks
        * Create AppStack
        * Import AppStacks
        * Rescan
    - Writables
    - Attachments
    - Assignments
    - Applications
- Directory
- Infrastructure
- Activity
- Configuration
- Logs
- Active Directory

Agent

- Introduction

- Capture
- SVDRIVER
- SVOFFICE
- SVSERVICE

Migration

- Introduction

Recovery

- Introduction

Enterprise Scalability

- Introduction

Setup

- Introduction

Troubleshooting

- Introduction

Upgrade

- Introduction

Glossary

AppStack

A portable hard disk volume (usually a .vmdk or .vhd) that contains one or more applications. These at attached/mounted to virtual machines to instantly deliver applications.

Writable Volumes

A portable hard disk volume (usually a .vmdk or .vhd) that can persist data. The type of data and eligible directory locations are determined by the template used when a writable is created.

Storage Group

A logical grouping of hypervisor (usually vCenter/ESX datastores) storage locations/devices. This concept is mostly used when creating writable volumes. Rather than choosing a single storage location as the target destination for a writable, the storage group can be used which can contain any number of storage locations (datastores). Multiple strategies can be used to determine how items are distributed amoungst the group. This concept also works for other hypervisor types too.

VM

Virtual Machine

AD

ActiveDirectory

Administrator Group

...

Power Watcher

This is a application server process that is not receive http requests. Instead this process maintains a connection to all configured vCenters. This connection performs a long-poll request using vCenter vSphere API to monitor power changes on all virtual machines.

Background Job

Background jobs are processed by one or more background workers. These background workers are additional application server (Ruby on Rails) process that do not receive http requests. Instead they only process jobs from a queue stored in the database.

Agent

The Windows components of the App Volumes product. Installed via MSI. Assumed to be placed in a base image.

Often called the "agent" or "client-side" or "in-guest".

Testing by Deore

```
print 'hello world'
```

Capture

Often referred to as "Provisioning". This is the process of recording an application install in an AppStack.

Common Questions

Large Application Failures

When they connect an AppStack (150GB) and install a large application and it fails because the application does a pre-installation validation to look at disk space and only the c:\ disk space (50GB) is being reported. Has anyone come across this?

Matt Conover: There is a setting to determine whether we return the size of the C: drive or appstack in provisioning mode. you can create a registry setting under HKLM\SYSTEM\CurrentControlSet\services\svdriver\parameters named ReportSystemFreeSpace type REG_DWORD and set value to 0 (on the system being used for provisioning) then instead of reporting C: drive we'll report size of writable volume (or the AppStack in provisioning mode which is functionally the same as a writable volume)

SVDRIVER

This is the kernel mode filter driver that performs file system and registry virtualization.

SVOFFICE

svoffice.exe is a program that lives in the template. It was introduced around AV 2.10. It runs at post-provisioning to groom some Office-related settings on the AppStack. Prior to 2.12, post-provisioning ran the program only if the AppStack contained an Office product. Starting in 2.12.1, post-provisioning runs the program unconditionally, for obscure technical reasons. For AppStacks containing an Office product, svoffice also runs during volume attachment to groom the system volume and writable volume.

Errors

Has anyone seen the error of 'Svoffice failed. Please collect log files for VMware support.'? This dialog is presented to the customer whenever they assign a VDI desktop or NON-VDI (VM) the Office 2016 AppStack. Once you clear the error (Select 'OK') the dialog goes away and Office works great.

This is Office 2016 O365 with App Volumes 2.12.1

Art Rothstein: It's new in 2.12.1. I got tired of asking customers with problems to check their cv_startup_postsvc.log file for an error. Now when svoffice writes an error message to that file, it also displays that message box.

Please check %SVAgent%\cv_startup_postsvc.log. It's a small text file. Office may appear to be working great, but the presence of an error in that log means there's a problem lurking.

SVSERVICE

This a user-mode process that communicates over HTTP to the App Volumes Manager server.

https://blogs.vmware.com/euc/2015/06/vmware-app-volumes-microsoft-office-license-install.html

By Denis Gundarev, Application Solutions Architect, App Volumes R&D, VMware This article is the first in a series of blog posts about using Microsoft Office with VMware App Volumes. Microsoft Office and VMware App Volumes Microsoft Office is one of the most popular application suites deployed on Windows enterprise desktops. Microsoft Office applications are often implemented first in VDI installations, both in proofs of concept and in production environments. With dynamic application delivery technologies such as App Volumes and VMware ThinApp, Microsoft Office deployment and compatibility are very important. In this blog series, we will explain various scenarios using Microsoft Office with VDI, as well as use cases and best practices for deploying Microsoft Office with App Volumes. We will discuss compatibility and interoperability for different Microsoft Office versions and editions, Office activation, and support for locally installed and AppStack-provisioned Office components, as well as troubleshooting and fine-tuning AppStacks with Office components. This information applies to both View virtual desktops in VMware Horizon 6, and to Citrix XenDesktop virtual desktops. But we should start at the beginning. Before provisioning any application to an AppStack, we need to understand which scenarios are supported or allowed by the application vendor. This can be a very tricky question, and it becomes even more complicated when you start thinking about Microsoft licensing. Licensing

In my consulting practice, many customers have asked if application virtualization could reduce software licensing costs, and my answer has always been simple—ask your application vendor. For Microsoft Office, the answer is no. None of the application virtualization solutions for Microsoft Office will reduce Office licensing costs. All Microsoft Office applications purchased as a software product are licensed per device, where "device" is a physical or virtual system that runs Microsoft Office applications or a system that is used to access Office applications remotely. Each license permits only one user to access the software at a time. The only exception to this rule is the subscription-based model that is licensed per user. Also important to note is that neither of the following purchase scenarios permits network use: Microsoft Office retail purchase (the fully packaged product) Acquisition of Office with hardware that includes the original equipment manufacturer (OEM) licensing In other words, for most VDI scenarios you can use only Microsoft Office editions that are available with Microsoft volume licensing. These include Office Professional Plus 2013, Office Standard 2013, and Office 365 ProPlus. You cannot use Office Home & Student or Office Personal editions on VDI. Licensing Compared to Activation

Do not confuse licensing with activation. When you license software, you acquire the right to use the software according to either the end-user-licensing agreement (EULA) or the Product Usage Rights (PUR), or both. Currently,

Microsoft does not enforce license validation for Office on endpoint devices, but instead relies on compliance with the EULA. However, Microsoft requires that you activate the product on the device where it is running, although not necessarily where it is installed. When you activate the Microsoft Office product, you submit the product key for validation and, if the product key is valid and not compromised, the activation subsystem enables licensed features of the product. Activation Methods

Now that we know the difference between licensing and activation, let us talk about activation methods. Microsoft Office products acquired through Microsoft volume licensing support two activation methods: Multiple Activation Key (MAK) activation and Key Management Service (KMS) host activation. Multiple Activation Key (MAK) activation can be used to activate software on multiple devices. Using this method, information about every activated device is sent automatically to Microsoft. MAK keys must be entered on every device where Microsoft Office is installed. Each MAK has a predetermined number of allowed activations, depending on your agreement. Every time you activate the software using an MAK, the number of allowed activations for this license key decrements. If the activation limit is reached, you need to contact Microsoft to request a new license key or extend the activation limit. MAK activation status is stored on the computer where the software is installed. This means that if you are using a nonpersistent VDI deployment, a copy of Microsoft Office is activated after every reboot, and you will reach the activation limit very quickly, even in a small environment. Key Management Service (KMS) host activation works differently. You do not need to enter the product key on every device because a preinstalled Generic Volume License Key (GVLK) is used instead. When a user launches the application, the application tries to discover a Key Management Service (KMS) host. If discovery is successful and the KMS host has a KMS key for that product, the software is activated. The KMS host collects a unique client machine identification (CMID) from the client computer and saves each CMID in a KMS host table. If a client computer renews its activation within 30 days, the cached record is removed from the table, a new record is created, and the 30-day period begins again. If a KMS client computer does not renew its activation within 30 days, the KMS host removes the corresponding CMID from the table and reduces the activation count by one. If you plan to use Windows 8 with Office 2013, you can also evaluate Active Directory–Based Activation (ADBA) as a type of KMS. Active Directory–Based Activation works similarly to KMS activation but uses standard Active Directory interfaces to communicate with the KMS host. ADBA can be used for Office 2013 volume license activation using the standard KMS product key. However, neither Windows 7 nor Office 2010 is supported, which limits the use case for the ADBA activation method at the present time. VMware recommends KMS host–based activation for Microsoft Office in a nonpersistent VDI deployment because it enables a fully automated activation that does not require interaction with the user. Moreover, if you use View virtual desktops in Horizon 6, KMS is the only officially supported activation method. Office 365 ProPlus

If you are using Microsoft Office 365 ProPlus as part of your Microsoft Volume Licensing Agreement, you may use the Office 365 Click-To-Run installation package for persistent VDI desktops. Office 365 applications, in this case, will use per user activation with Microsoft Online servers. However, Office Online activation requires that the user enter credentials on every new computer or virtual machine they are using to run Microsoft Office. This means that in a nonpersistent VDI scenario, or when Office is delivered using application virtualization with App Volumes, the activation limit will be reached very quickly and Office will enter the limited functionality mode. Because of this, you should use Microsoft Office 2013 volume licensing media with traditional KMS host–based activation on nonpersistent VDI desktops and when implementing App Volumes. Note that you need to have access to the Microsoft Volume Licensing Service Center (VLSC) in order to download Microsoft Office 2013 volume licensing media. If you do not have such access, consult your Microsoft volume licensing partner. Office 32-Bit Compared to 64-Bit Versions

Microsoft Office is available in both 64-bit and 32-bit versions. The Office 64-bit version will not run on 32-bit Windows, but is it a good idea to run a 64-bit version of Office on 64-bit Windows? Do this only if your users have specific needs such as editing large Microsoft Excel or Microsoft Project files. 64-bit versions of Microsoft Office have limited compatibility with third-party products and even have limitations for built-in functionality. Microsoft recommends the use of 32-bit versions of Microsoft Office for most users. Another essential point to consider is that Office does not support running side-by-side installations of 64-bit and 32-bit versions of Office or Office components. As an example, you cannot run a 32-bit version of Microsoft Visio on a computer that has a 64-bit version of Microsoft Office installed, and vice versa. This support limitation also affects Office applications delivered with App Volumes. For example, you cannot install 32-bit Office into the base image and deliver a 64-bit version of other Office applications through an AppStack. Where to Get the Software and Product Keys

You need to purchase licenses for Microsoft Office directly from Microsoft or from a Microsoft partner. And for VDI

scenarios you can use only Office editions available through Microsoft volume licensing. However, enough about licensing...let us talk about the actual software bits that you need to use for deployment. As I mentioned before, for VDI scenarios, you need the Office Professional Plus 2013 or Office Standard 2013 installation source, even if you are using Office 365 licenses. Installation files downloaded only from a Microsoft Volume Licensing Support Center (VLSC) should be used. Do not try to use installation media that you downloaded from the TechNet Evaluation Center or from your MSDN subscription because these ISO files contain retail versions of Microsoft Office that are not allowed for use in most VDI scenarios. If you do not have access to VLSC, contact your volume licensing agreement administrator or Microsoft licensing partner to request access. If ISO files have already been downloaded for you, verify them for use with App Volumes before proceeding with deployment or AppStack provisioning. You must have a folder named Admin on your ISO; if there is no such folder, this is not a suitable ISO. Check that the name of the folder that has a .WW extension (ProPlus.WW, Visio.WW, PrjPro.WW, Standard.WW, and so on). If there is a lowercase "r" before the dot, which means retail (ProPlusr.WW, Visior.WW), then this is not a suitable ISO. The same is true for KMS product keys. They are available at VLSC, or they can be requested by phone. MSDN subscriptions come with retail keys that cannot be used for KMS activation. Important: Volume-licensed Microsoft Office comes with the Generic Volume License Key (GVLK), which is used for KMS activation. Install the KMS key only on a KMS server, and do so before you implement App Volumes. Do not enter the KMS key during or after App Volumes installation or when you provision the AppStack. Summary

To summarize the information discussed here: In most VDI deployments, you can use only Microsoft Office Professional Plus 2013, Office Standard 2013, or Office 365 ProPlus by subscription, acquired through a Volume Licensing Agreement. Retail and OEM versions of Office cannot be used for VDI. If you use nonpersistent VDI or any kind of application virtualization, or both, you need to use KMS activation. With KMS activation, you must use installation media that was downloaded from Microsoft VLSC. You should use 32-bit versions of Microsoft Office unless your users have a particular interest in editing large Excel or Project files, in which case you can use 64-bit versions. Mixing 32-bit and 64-bit Office installations on the same machine is not supported. I hope that you find this article useful. Come back for the next post of this series where I will cover supported scenarios for using Microsoft Office with App Volumes, KMS deployment and troubleshooting, procedures that you can follow to provision an AppStack with Microsoft Office, and troubleshooting Office applications delivered through App Volumes.

Do we support?

...RDSH apps on appstack?

Yes, as computer based assignments

Once apps are assigned and attached to RDSH virtual machine they can be published the same as natively installed apps

But what we are wanting to do with RDSH in Astro eventually is make that more seamless. Right now it is two unrelated flows: assign apps to RDSH VMs (probably by Active Directory organizational unit) and then publish apps. This could be one flow that when choosing to publish apps you can choose natively installed apps or App Volumes apps and if you choose an App Volumes app then we will attach that AppStack to the RDSH VMs

FAQ

#Location of VMware App Volumes log files (2091590)

This article provides details on troubleshooting an App Volumes environment using the App Volumes logs.

Note: This article references shell folders and shell folder variables. If you have performed a custom installation, your installation may differ and your log files may not be available in the path mentioned in this article. These logs location are discussed in this Knowledge Base:

- App Volumes Manager
- App Volumes Agent
- App Volumes log files

This section discusses the log files you can use to troubleshoot an App Volumes issue, and what to look for in the logs. The relevant log files are:

- App Volumes Manager logs
- App Volumes Agent log files
- ESXi logs

##App Volumes Manager logs

The App Volumes Manager log files are:

- production.log
- svmanager_server.log
- These log files are located at C:\Program Files(x86)\CloudVolumes\Manager\Log on the App Volumes Manager server. You can also access the production.log at http://AppVolumes ManagerFQDN:port number/log . You do not need to specify the port number unless it is a custom install.

###App Volumes Manager production.log

The App Volumes Manager server contains logging from the main modules of App Volumes. Use the production.log file to identify a variety of issues in an App Volumes environment.

Here is a description of the main modules to search for in the production.log file. RADIR :RubyActiveDIRectory classes – Responsible for AD connection Cvo :App Volumes logic classes RvSphere :RubyvSphere wrapper classes SQL :Database queries (Default logging captures only errors. Debug logging captures queries and errors) PowerShell :App Volumes PowerShell interface classes NTLM :App Volumes NTLM handler Each line in the production.log file gives the Process ID (PID) and informs us whether it is a request or a delayed job. An active request is denoted by PxxxxRxx, and a delayed job is denoted by PxxxxDJ. Here are excerpts from the production.log file.

[2015-1-30 15:31:31] P3488DJ INFO Cvo: Uploading file: "C:/Program Files (x86)/CloudVolumes/Manager/ppv/writable_template..." [2015-1-30 15:31:32] P3488DJ INFO RvSphere: Connection to VMware Administrator@vcenter.vmwra.com succeeded - Took 219ms [2015-1-30 15:31:35] P3488DJ INFO RvSphere: Connection to VMware root@esxi-123.vmwra.com succeeded - Took 156ms [2015-1-30 15:31:36] P3488DJ INFO RvSphere: Copying 59392 KB thin lsiLogic disk at "[Datastore-Cluster1] cloudvolumes/writable... [2015-1-30 15:31:39] P1132R60 INFO Started GET "/cv_api/jobs/pending?_=1417390299687" for 127.0.0.1 at 2015-1-30 15:31:39 [2015-1-30 15:31:39] P1132R60 INFO Processing by CvApi::/JobsController#pending as USER

Note: This log excerpt is an example. Date, time, and environmental variables may vary depending on your environment.

For example, you can identify a certain module in the App Volumes Manager log and find the corresponding PID.

[2015-1-30 15:26:31] P2728R36INFOStarted GET "/storages?_=14717390015761" for 127.0.0.1 at 2015-1-30... [2015-1-30 15:26:31] P2728R36INFORADIR: Connection to AD ad.vmwra.com succeeded - Took 109ms [2015-1-30 15:26:31] P2728R36INFOCompleted 200 OK in 125ms...

Note: This log excerpt is an example. Date, time, and environmental variables may vary depending on your environment.

###App Volumes Manager svmanager_server.log

The svmanager_server.log file captures App Volumes Manager server actions. You can correlate these actions with the Agent log files by checking time stamps from both the server and agent logs. The svmanager_server.log file also captures information relating to the App Volumes infrastructure.

##App Volumes Agent log files

The App Volumes Agent log files are:

- svservice.log

- svdriver.log

- svcapture.log – This log file is present only on a capture machine.

###Locations for Agent log files

In releases earlier than App Volumes 2.9, the App Volumes Agent logs are located at C:\Windows on the Agent machines. The svcapture.log file is also located at C:\Windows , on the capture machine.

For App Volumes 2.9 and later, the Agent log locations have changed.

The svservice.log file is located at C:\Program Files (x86)\CloudVolumesAgent\Logs on the Agent machines.

The svcapture.log file is located at C:\Program Files (x86)\CloudVolumesAgent\Logs on the capture machine.

The App Volumes driver log is now saved in ETL format, located at C:\Windows\System32\LogFiles\WMI\AppVolumesAgent.etl. To view the AppVolumesAgent.etl file, you need to convert the ETL file to XML format.

To convert the ETL File to XML format, flush the buffers to the disk and then convert the ETL log to XML format.

To flush the buffers to the disk: Open a command prompt from the App Volumes Agent machine. Go to Start > Programs, and click Command Prompt. Run the command

logman update AppVolumesAgent -fd –ets

This command ensures that the Agent transaction data is saved to disk.

To convert the ETL log to XML format: On the App Volumes Agent machine, go to Start > Programs, and click Command Prompt. Run the command:

tracerpt.exe AppVolumesAgent.etl -of xml -gmt -tp "C:\Program Files (x86)\CloudVolumes\Agent\tmf" -o AppVolumesAgent.xml

You now have an XML file that you can open with MS Excel. For more information, see Microsoft TechNet article logman update trace command and tracerpt parameters.

Note: The preceding link was correct as of July 23, 2015. If you find the link is broken, provide a feedback and a VMware employee will update the link.

###Details on Agent log files

Here are details on the Agent log files:

svservice.log

SvService is the service responsible for communication between the App Volumes Agent and the App Volumes Manager, including the preparation of volumes, the running of post-attach scripts, refresh of variables, and registration of fonts. The log tracks this communication.

svdriver.log

SvDriver is a policy-driven driver file responsible for the virtualization of volume contents into the desktop OS. The policy file snapvol.cfg controls the files, directories, registry keys, and processes that are virtualized during application capture on each volume. The log tracks this activity.

svcapture.log

The SvCapture service performs provisioning and editing functions during application capture, such as generating policy files and metadata. The SvCapture reports this information to the App Volumes Agent and App Volumes Manager. The log tracks this activity and is available only on the capture machine.

For information to increase the logging level to debug, see Increasing Logging Level for AppVolumes Manager (2101668).

###ESXi logs

You can check the ESXi host management service log (hostd) for disk locking, virtual machine state transition, and hot-add operations. The hostd.log file is located at /var/log/hostd.log on the ESXi server.

You can also check the virtual machine log (vmware.log) for virtual machine-related activities, such as user logins to a desktop, or applications not appearing on a desktop. The virtual machine log is located at /vmfs/volumes/datastore/vm_name/vmware.log .

For more information, see Location of log files for VMware products (1021806).

For more information on troubleshooting an App Volumes environment using the log files, see VMware App Volumes log analysis tools and log analysis examples (2126475).

#Outlook Search Indexing with App Volumes (2149799)

##Symptons

- User with a Writable Volume attached and trying to do an Advanced Search in Outlook by right-clicking on a message and choosing "find related messages" might cause the application to crash.

- This might also occur on other Office applications when Search Index is enabled.

- Versions of Office affected are Office 2013and Office 365 (2013 and 2016).

- The Office application can be natively installed or in an AppStack, results are the same

##Resolution

To resolve this issue, correct the error by changing / updating 3 files and adding 1 line in the snapvol.cfg file for the affected user with the writable volume.

Changing this for a single user will address the issue for that specific user. Ensure that to complete the change, the user needs to be logged off any system so that the writable volume shows as detached in the App Volumes Manager console.

As an alternative, you can also choose to change this for all your user by changing the Writable Volume template, before assigning Writable Volumes to your user.

The required modifications are needed for prestartup.bat, startup.bat, shutdown.bat and snapvol.cfg.

Note: The prestartup.bat, startup.bat and shutdown.batare present in the 2149799_OutlookIndexConfig.zip file available under attachment section of the KB.

Reminder that these changes are all done on the Writable volume.

In the file snapvol.cfg, add the following entries under the registry exclusions section

exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows Search\CrawlScopeManager_PreviousVersion

The new prestartup.bat, would look like the information below. Please note that only the lines in Italic are the lines that are added, the other lines should already exist. Also note that the mkdir and rmdir command have been updated:

```
setlocal enabledelayedexpansion
set SCRIPT_PATH=%~dp0

echo %date%-%time%>>%SCRIPT_PATH%prestartup.log
sc.exe config wsearch start= disabled >>%SCRIPT_PATH%prestartup.log
net stop wsearch >>%SCRIPT_PATH%prestartup.log

mkdir %SCRIPT_PATH%writable 2>>%SCRIPT_PATH%prestartup.log
rmdir c:\SnapVolumesTemp\writable /s /q 2>>%SCRIPT_PATH%prestartup.log
mklink /j c:\SnapVolumesTemp\writable %SCRIPT_PATH%writable >>%SCRIPT_PATH%prestartup.
↪log

reg delete "hklm\SOFTWARE\Policies\Microsoft\Windows\Windows Search" /v "DataDirectory
↪"  /F >>%SCRIPT_PATH%prestartup.log
reg add "hklm\SOFTWARE\Policies\Microsoft\Windows\Windows Search" /v "DataDirectory" /
↪d "c:\snapvolumestemp\writable\persistent" /f >>%SCRIPT_PATH%prestartup.log
```

Add the following lines to your startup.bat file, if your Writable Volume does not have a startup.bat, you need to create it, with the information below:

```
sc.exe config wsearch start= demand
sc.exe start wsearch
```

In the shutdown.bat file, you add the following lines, above the rmdir command:

```
sc.exe config wsearch start= disabled >>%SCRIPT_PATH%shutdown.log
net stop wsearch >>%SCRIPT_PATH%shutdown.log
```

All KBs

Copy them into this directory

https://confluence.eng.vmware.com/pages/viewpage.action?pageId=210253287

Active Directory

Questions

Domain Controller Auto Discovery

In 2.12 GA release does the DC Auto Discovery work as designed? Has anyone received a case of the Auto Discovery not working as expected?

It is DNS-based, not sites and services aware. So it won't do anything fancy. It is mostly just keeping track of which DC's work and which ones don't.

CHAPTER 13

Manager UI

Using the AppVolumes Manager UI

Overview

Dashboard

The dashboard contains three major sections: License utilization, usage graphs, and recently changed system objects.

Volumes

Management of AppStacks and Writable volumes. Also contains views of all assignments, attachments, and applications.

Directory

Management of system entities imported from ActiveDirectory such as Users, Computer, Groups, and Organization Units.

Infrastructure

Management of infrastructure components. Storage locations and Storage groups.

Activity

Audit and error logs.

Configuration

Management of configuration, also used as the first-time configuration mode.

Additional Capabilities

Version

```
GET http://your-manager/cv_api/version
```

Shows the current version - does not require authentication.

Health Check

```
GET http://your-manager/health-check
```

Shows some basic server information, can be used to ensure the service is up and running. Does not require authentication!

Raw Log

```
GET http://your-manager/log
```

Shows the Ruby on Rails server log. This log is a combination of logs from all internal application server processes including background workers and the power-watcher. Requires administrator to be logged in.

Cleanup

```
GET http://your-manager/cleanup
```

WARNING This is the nuclear option. Calling this url will remove all attachments from all known VMs. It also removes any orphaned assignments. Requires administrator to be logged in.

Manager Threads

```
GET http://your-manager/threads
```

This will show a debug screen showing the thread usage in the Manager. Remember that the Manager is internally load-balanced across many server processes, so you will only see thread information for one of the many of those processes. Calling this on each port, such as :3001, :3002, :3003, :3004, is needed to get the whole picture.

System Environment

```
GET http://your-manager/env
```

This will show system ENV information. Requires administrator to be logged in.

CHAPTER 15

Activity

CHAPTER 16

Configuration

CHAPTER 17

Dashboard

CHAPTER 18

Directory

CHAPTER 19

Infrastructure

CHAPTER 20

Applications

CHAPTER 21

AppStacks

Create AppStacks

This is a sample image

CHAPTER 23

Import AppStacks

Rescan

Assignments

CHAPTER 26

Attachments

Volumes

CHAPTER 28

Writables

Manager Log Information

Types

There are three main logs output by the Manager.

- Application server logs (Ruby on Rails)
- HTTP server logs (Nginx)
- Service logs (STDOUT from launcher process)

Application server logs (Ruby on Rails)

Line sources

Lines in this log come from a few different sources. Request logs, background job logs, and power-watcher logs.

Process and Request numbers

Each log line starts begins with a timestamp and a process/request identifier. This identifier can be used to correlate log messages for a request. This is especially important when multiple requests happen at the same time and their log messages become intertwined.

For example, the line below came from the server process "2282" and is the 6th request to be received on that process.

```
[2016-01-13 06:58:03 UTC]    P22823R6   INFO Started GET "/login" for 127.0.0.1 at
↪2016-01-12 22:58:03 -0800
```

You can tell a log was generated by a background-job or the power-watcher by looking for "DJ" or "PW" in the request identifier.

Background job:

```
[2016-01-13 06:58:25 UTC]  P22851DJ244   INFO          Cvo: Refreshing attachments
```

Power-watcher:

```
[2016-01-13 07:21:15 UTC]     P22827PW DEBUG        Cvo: [PowerWatcher] Watching␣
↪power state changes for 1 machine managers
```

waitForUpdates()

Does AV Manager do any active state monitoring of VC? E.g. do you call waitForUpdates() to track VM or task state changes?

##Yes

Yeah, we have a separate instance of our app process that is not under nginx that monitors state changes (mostly power events).

It does a long poll to each vCenter with a waitForUpdates

We also do a waitForUpdates() for lists of ReconfigVM_Task IDs. Let's say we have a bunch of mounts happening around the same time, we take the task IDs we get back from vm.ReconfigVM_Task(...) and put them into a queue. A separate worker takes chunks from that queue and does a waitForUpdates([123,234,345,456,567,678,...])

–

Each app process (4 per VM) has up to 3 threads per host that can do the waitForUpdates() for mounts. The original idea being that if we need to wait on a bunch of task ids that we'd split it up and do them on a separate requests/connections.

The max would be: (app_processes*wait_worker_threads*vsphere_hosts) + (vsphere_hosts*power_watcher_processes)

Realistically, with 1 vCenter and 8 hosts:

ESX Mounting: (4*1*8) + (8*1) = ~45 vCenter Mounting: (4*1*1) + (1*1) = ~5

CHAPTER 31

Migration

Recovery

Developer notes for Manager release 2.10

Notable Changes:

- AVM_PROTECT_VOLUMES="1" operating system environment variable can be used to enable vMotion and to provide volumes accidental deletion protection when all ESX hosts are version 6u1 (ESX 6u1 requires vCenter 6 or later). vMotion of VMDK files is not supported.

- All templates are now created with "attributes volume set NODEFAULTDRIVELETTER" to ensure they are not automatically assigned a letter by a Windows Mountvol

- Computer identity is now verified against AD, so computer that were formerly trusted by Active Directory that have lost their trust relationship will no longer get volumes. This can happen due to default maximum machine password age of 90 days in Windows when reverting virtual machines to a snapshot after its machine password changed. See "Domain member: Disable machine account password changes" (https://technet.microsoft.com/en-us/library/jj852191.aspx) for instructions on how to disable this.

- Due to significant significant improvemsnts in the App Volumes Manager in v2.10, App Volumes Broker Integration Agent is no longer needed and is also not recommended.

No attachment to Low Performance Storage

Now storage can be marked as "Not Attachable" making manager skip it when using it for mounting volumes. This allows IT admins to better manage storage capabilities.

For example, an IT admin can setup two vCenters each with a local storage and one shared storage. The slower performing shared storage can be marked "Not Attachable" and be used solely for replication.

Expand the size of a writable volume

Admin can specify a new size for a Writable Volume (must be at least >1 gig larger than current size). The manager will grow the volume file to the new size. Next time the user logs into a VM with App Volumes Agent, it will

automatically grow the file system of the volume.

Developer notes for Manager release 2.6

Notable Changes:

- AppStack Grouping - Volume files (vmdk/vhd) on different storage locations that share a path and filename are considered to be copies of each other. They can be managed as a single AppStack in the UI.

- Automatic AppStack Import - Volumes files (vmdk/vhd) located at the default appstack path on storage locations in enabled StorageGroup's are automatically imported if the setting is enabled when creating the storage group.

- Automatic AppStack Replication - Volumes files (vmdk) located at the default appstack path on storage locations in enabled StorageGroup's are automatically replicated to all datastores in the storage group if the setting is enabled when creating the storage group.

- Improve internationalization support - Non-ascii text characters are now handled properly in the UI and database. Strings containing UTF-8 characters from previous versions may not appear correctly.

- Users can now receive volumes when they login to computers running a server version of Windows. Previously, only volumes were only attached to standard desktop versions.

Fixes:

- Users, Computers, Groups, and Organizational Units can be unassigned even when they are not found in AD.

- There might have been casees in v2.5.2 where the option to overwrite the database checkbox did not work properly

- When uninstalling the App Volumes Manager, attached volumes are no longer automically detached. There is now a checkbox during uninstallation that can be set if this a permanent uninstall. If the intent is to temporarily uninstall the App Volumes Manager or upgrade to a newer version, this checkbox should be left unchecked.

AppStack Grouping

Files available at the same path and filename on different datastores are considered to be copies of each other. Each AppStack now has a Locations count and pop-up display to show the child files. When mounting, only 1 file for each AppStack will be attached. This is determined by whether or not the target VM can access the storage. When multiple files are eligible, the file with the least amount of active attachments (by other users) is used. When viewing attachments, the storage location of the attached file is shown in brackets: "AppStack-Name[datastore1]".

Automatic AppStack Import

There is a new checkbox available when creating a StorageGroup called "Automatically Import AppStacks". When enabled, all storage locations in the group are checked for new volumes every 15 minutes. This is intended to be combined with AppStack Grouping so that new volume files are automatically imported and associated with their primary AppStack for scale-out use-cases.

Automatic AppStack Import

There is a new checkbox available when creating a StorageGroup called "Automatically Replicate AppStacks". When enabled, any AppStacks on one StorageGroup are replicated to the other datastores in the StorageGroup. This is intended to be combined with AppStack Grouping so that new volume files are automatically imported and replicated for scale-out use-cases.

Improve internationalization support

Due to a configuration error, strings containing UTF-8 input in previous versions were stored as single-byte ASCII characters in the database. This problem has been fixed going forward, but old strings may appear garbled.

Server VDI

Users can now receive volumes when they login to computers running a server version of Windows

Developer notes for Manager release 2.7

Notable Changes:

- Removed "Spillover" from the available Storage Group distribution options This strategy will fill up a storage because it uses actual (thin) size and not the full provisioned size

- An additional set of credentials can be provided to be used when connecting to any trusted ActiveDirectory domain This enables use of additional domains that have one-way trust relationships (see documentation for more info)

- The API route used to delete assignments has changed from POST /cv_api/assignments to DELETE /cv_api/assignments

- When configuring direct-to-host mounting using the vCenter, you will no longer be prevented from saving the ESX credentials if they are not valid (or not able to be validated) on all hosts visible to vCenter. This fixes a case when an ESX server may be down for maintenance.

- An error will be shown in System Messages when the Agent fails to attach a VHD when the Manager is configured to use InGuest (no hypervisor) mode. An error will also be recorded in the Windows Event Viewer.

- New feature for InGuest will ensure agent computers are only granted access to a VHD volume on the fly directly before the Agent can mount the file.

- Added the ability to edit a Storage Group. Look for the [Edit] button after expanding a storage group row.

- Added the ability to rescan a Storage Group. This operation contacts the hypervisor and updates storage information metadata such as free space and overall capacity. It also adds any new storage that makes the prefix (automatic-mode).

- Added the ability to manually synchronize all Users or all Computers with ActiveDirectory. New [Sync] buttons are available on the Directory->Users and Directory->Computers pages.

- Administrator can now delete AppStacks and Writables in "unreachable" and "creating" states.

- [API] Added POST /cv_api/sessions route for API login, takes "username" and "password" parameters. Once logged in this way, no CSRF-token is needed for subsequent requests.

- [API] Added DELETE /cv_api/sessions route for API logout

- [Security] Session token is re-create during UI and API login requests

- [Security] HTTP server no longer accepts RC4 or EXPORT ssl ciphers, see nginx/conf/nginx.conf for the full list

- Users can upload prepackaged VHD templates using the "Upload Prepackaged Volumes" button during storage configuration.

Trusted Domain Credentials

AV Manager automatically connects to domains trusted by the primary domain specified during configuration.

It is expected that the credentials provided can be used to authenticate to each trusted domains. This normally works because the most trusted domains have two-way trust. That means the DOMAIN1\av_manager can be used to authenticate and query DOMAIN2. However, if when there is a one-way trust, DOMAIN1 can trusts DOMAIN2, but DOMAIN1 credentials can not be used to authenticate on DOMAIN2.

You can now specify a second set of credentials that will be used whenever connecting to a trust during ActiveDirectory configuration. These credentials will be used when connecting to any trust instead of the primary domains credentials. A list of domains to use the new trust credentials can be provided. Instead of using the credentials on all trusted domains, they are only used on the specified domains. The list should be separated by spaces: domain2.local domain3.com.

If the domain controller can not be automatically detected from DNS, you can add that to a domain in the list using a semi-colon. For example: domain2.local;10.0.0.1 domain3.com;ldap.domain3.com. Such a configuration will even allow you to use a domain that is not trusted by the primary domain.

vCenter Direct-to-Host Mounting

Volume mounts are performed using vSphere's VM reconfigure API. The time it takes to run this command can is shorter when it is performed directly on an ESX host. The AV Manager allow an administrator to enable this functionality when configuring a vCenter hypervisor.

To use this feature, each ESX server being managed by a vCenter must have an identical system/service account. We suggest creating an account on each ESX with limited permissions.

If enabled, the AV Manager will attempt to connect to every ESX server before saving the hypervisor configuration. Prior to the v2.7 release, the configuration would not be considered valid unless every ESX server could be reached. In v2.7 and beyond, the administrator will receive a warning message if any of the ESX servers can not be contacted but the configuration settings will still be saved. The administrator may want some ESX servers not to be included or some of the servers may be offline for maintenance.

VHD: Dynamic File Permissions

Files located on SMB based file shares can be accessed from multiple computers. Enabling this feature for InGuest will ensure agent computers are only granted access to VHD file on the fly directly before the Agent can mount the file. Upon logoff (User Assignments) and shutdown (Computer Assignments) the rights are then revoked from the agent computer.

To enable this feature, from the Configuration > Hypervisor tab select "Hypervisor: None [VHD] In-Guest Mounting" and check the "Security: [ ] Dynamic File Permissions" checkbox.

Note: An administrator must also configure the minimal file permissions as follows:

manager_server$ | Full Control Domain Computers | List Folder Contents

Synchronize ActiveDirectory Entities

The AppVolumes Manager keeps a database record for any ActiveDirectory that has been seen by the Agent or assigned an AppStack or Writable Volume. A background job is run every hour to synchronize up to 1000 entities. If you have more than 1000 items, the a new batch of 1000 will be synchronized the next hour and so on.

Synchronization mainly updates human-readable information like name. It also checks the entry's enabled or disabled state.

You can force a manual synchronization in two ways. First you can use the [Sync] button on the detail view for an individual user or computer. You can also use the Sync button on the Users or Computers index pages. These buttons will schedule a background job to synchronize every User or Computer in the Manager database.

Deletion of AppStacks and Writables in "Unreachable" and "Creating" states

AppStacks and Writables that exists on a datastore that can no longer be contacted have their state set to "unreachable". Previously these volumes were unable to be deleted from the Manager interface. This was restricted so that volumes were not removed from the Manager unless the underlying volume files could be deleted. When a datastore can not be contacted, we are unable to delete the volume file. However, if a datastore is removed and is never going to return, the administrator was left with stale records. Administrators can now remove an AppStack or Writable even when it is "unreachable".

New interface for managing VHD file shares

Previously users would blindly add UNC paths with no information regarding if the path would function. Now an administrator can enter in a UNC (or partial UNC) path to browse shares. The administrator will also be given a warning message if the App Volumes Manager is unable to write to the share alerting the administrator that further action may need to be taken. Also, as a convenience, the administrator can quickly view the file share permissions.

Developer notes for Manager release 2.9

Notable changes

- Hypervisor configuration is now called Machine Managers.
- Multiple vCenters can be used with the App Volumes Manager concurrently.
- When more than one vcenter is added, multiple datacenters can be used.
- All json responses returned from /cv_api/ always have the Content-Type of application/json
- /cv_api/appstacks is no longer nested under a "currentappstack" and "appstacks" objects - it returns a flat array
- Storage replication will not work across multiple vCenters and is unsupported.

Machine Managers - Multiple vCenter

Three types of Machine Managers are available and only one type may be selected by the App Volumes Manager database.

The three types are:

- VMware vCenter Server
- VMware ESX Server
- VHD In-guest Services

System Administrators can add more than one vCenter to the Machine Manager configuration.

Note: VMs must be unique across all vCenters. Datastore names must be unique across all vCenters.

Deleting a Machine Manager - vCenter Server Only

Deleting a machine manager will result in removal of related records. Detaching logging users off and powering down machines managed on the machine manager being deleted will ensure Appstacks and Writable Volumes are not left attached.

The following records will be removed when a related Machine Manager is deleted:

- machine references
- file references
- storage locations
- members of storage groups
- snapvol file references of multi-file snapvols
- snapvols with no more files

CHAPTER 37

Scale

CHAPTER 38

Setup

CHAPTER 39

Troubleshooting

CHAPTER 40

Uncategorized

This is temporary location to dump yet to be categorized documents. Please try best to find `duplication` or `best path` before putting document to here.

All docs under this directory is not exposed, and will be manually selected and categorized by maintainers.

Upgrade

CHAPTER 42

Indices and tables

- genindex
- modindex
- search