

Troubleshooting

Your Horizon Deployment

Chris Halstead, Senior Staff Architect, VMware

Graeme Gordon, Senior Staff EUC Architect, VMware

SESSION ID EUS1929

#vmworld #EUS1929

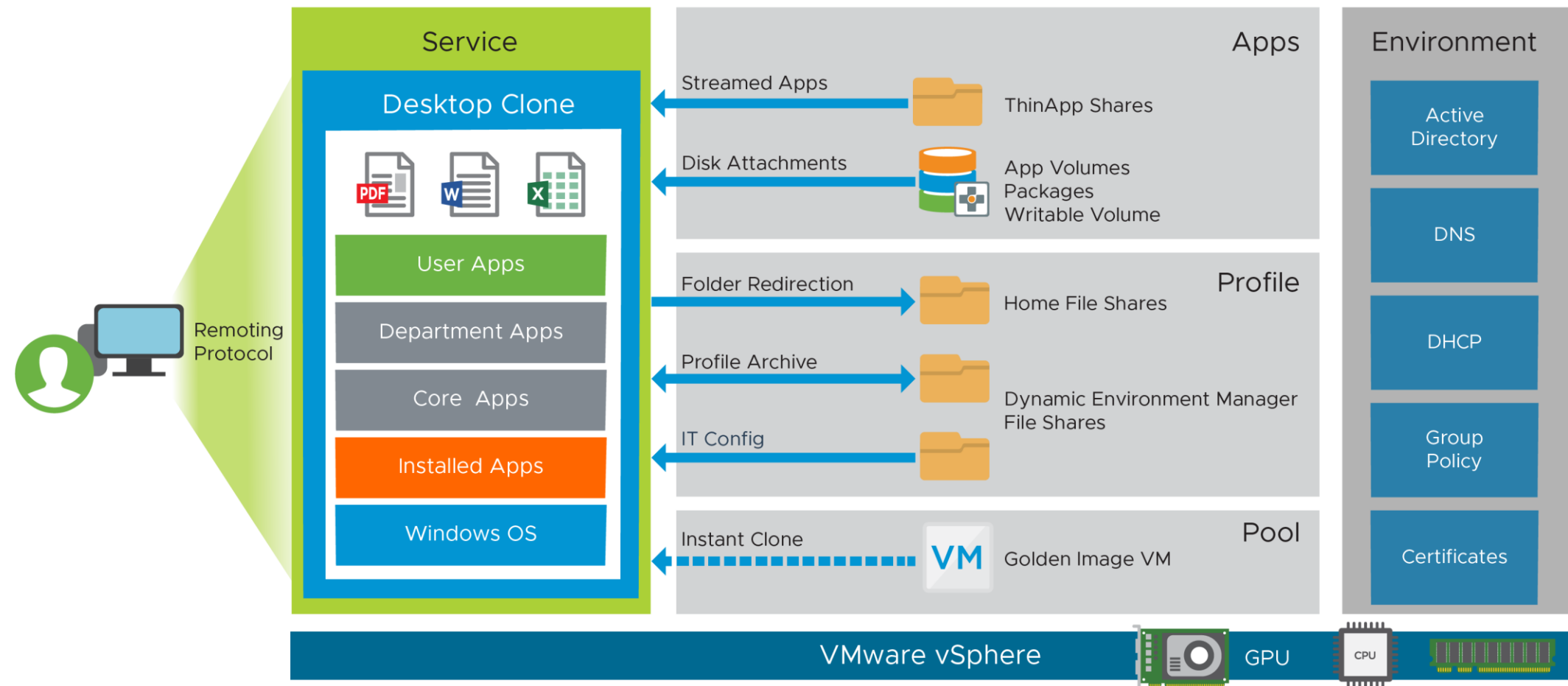


The "vmworld 2021" logo, featuring the word "vmworld" in a white, lowercase, sans-serif font with a registered trademark symbol (®) to the upper right, and the year "2021" in a larger, white, sans-serif font below it. The logo is set against a dark blue, textured background that resembles a night sky with stars and white orbital lines. A small satellite icon is visible in the upper right area of the background.

Troubleshooting Approach, Tools and Logs



Identifying the Problem Domain

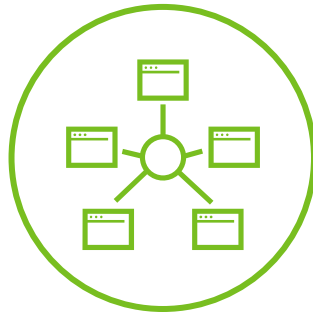


Six Step Troubleshooting

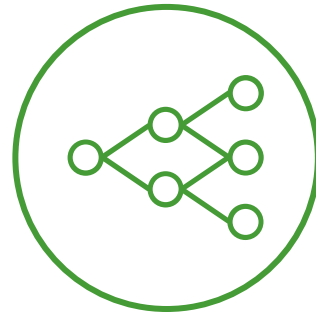
US Navy's procedure



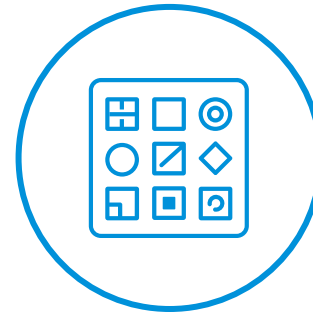
Symptom
Recognition



Symptom
Elaboration



List Probable
Faulty
Domains



Localize the
Faulty
Domain



Localize the
Faulty
Component



Failure
Analysis

<https://www.manitonetworks.com/networking/2018/7/20/six-step-troubleshooting-method>

Download Logs in Horizon Console

Centralize and Automate Log Collection (Horizon 2012 and later)

Overview

Directly download log bundles from the Horizon Console

- Connection Servers
- Desktop / RDS Agents

Log bundles

- Copied to: *C:\ProgramData\VMware\VDM\DCT*
- Purged after 60 minutes
- Can be customized in ADAM DB
 - CN=Common,OU=Global,OU=Properties,DC=vdi,DC=vmware,DC=int

Benefits

Replaces and centralizes a very manual process by the Administrator

[KB1017939](#) - collect log locations and diagnostics info

[KB1025887](#) - change log levels

Log Collection

Collect

Manage

Delete

Cancel

Last refreshed: 2:17 PM

Filter



<input type="checkbox"/>	Status	Name	Type	Initiator	Start Time	Completed Time	Download
<input type="checkbox"/>	✓	GCVE-EUC-TM-HZ3	Connection Server	vmweuc.com\chals...	12/15/2020, 2:16 PM	12/15/2020, 2:17 PM	↓ GCVE-EUC-TM-HZ3.zip
<input type="checkbox"/>	ⓘ	81-TM-1	Agent	vmweuc.com\chals...			
<input type="checkbox"/>	ⓘ	h8-ded3	Agent	vmweuc.com\chals...			

Log Monitoring

Use Tail/Grep Utilities or CMTrace

[BareTail](#)

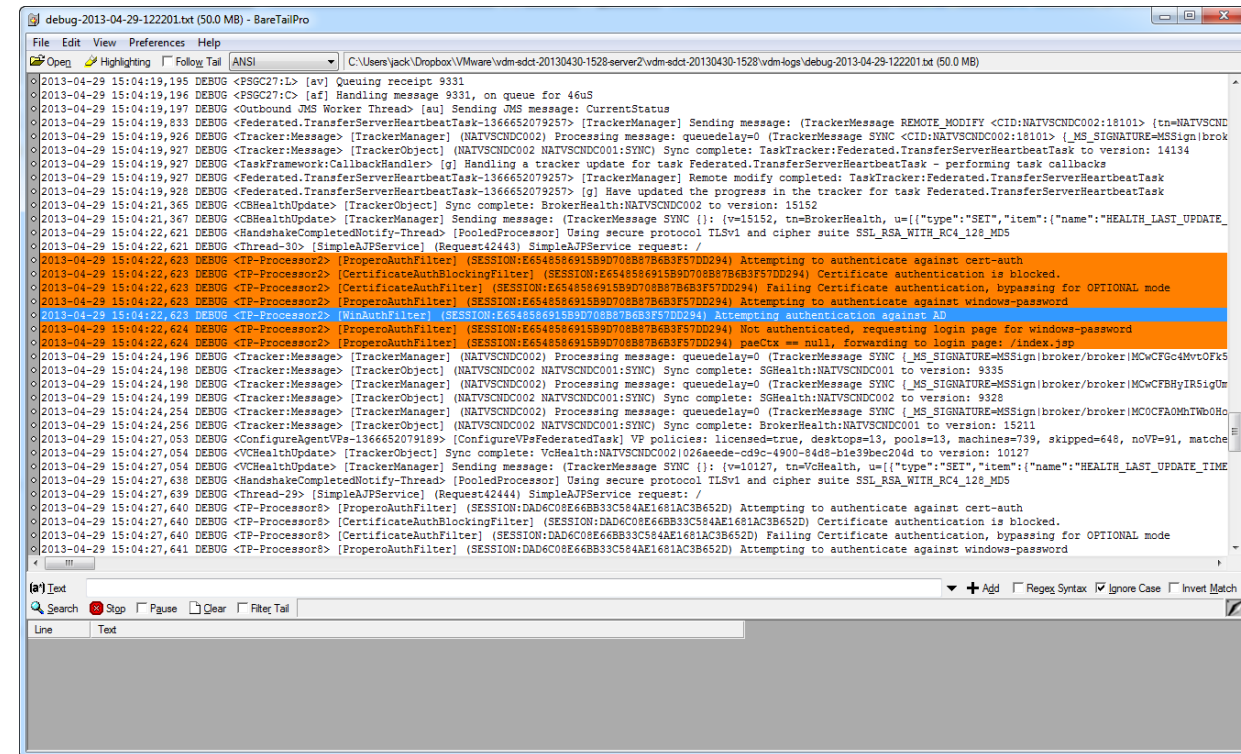
[CMTrace](#)

Filter live results

Highlight to focus attention on entries

- Color
- Session ID
- AD User ID

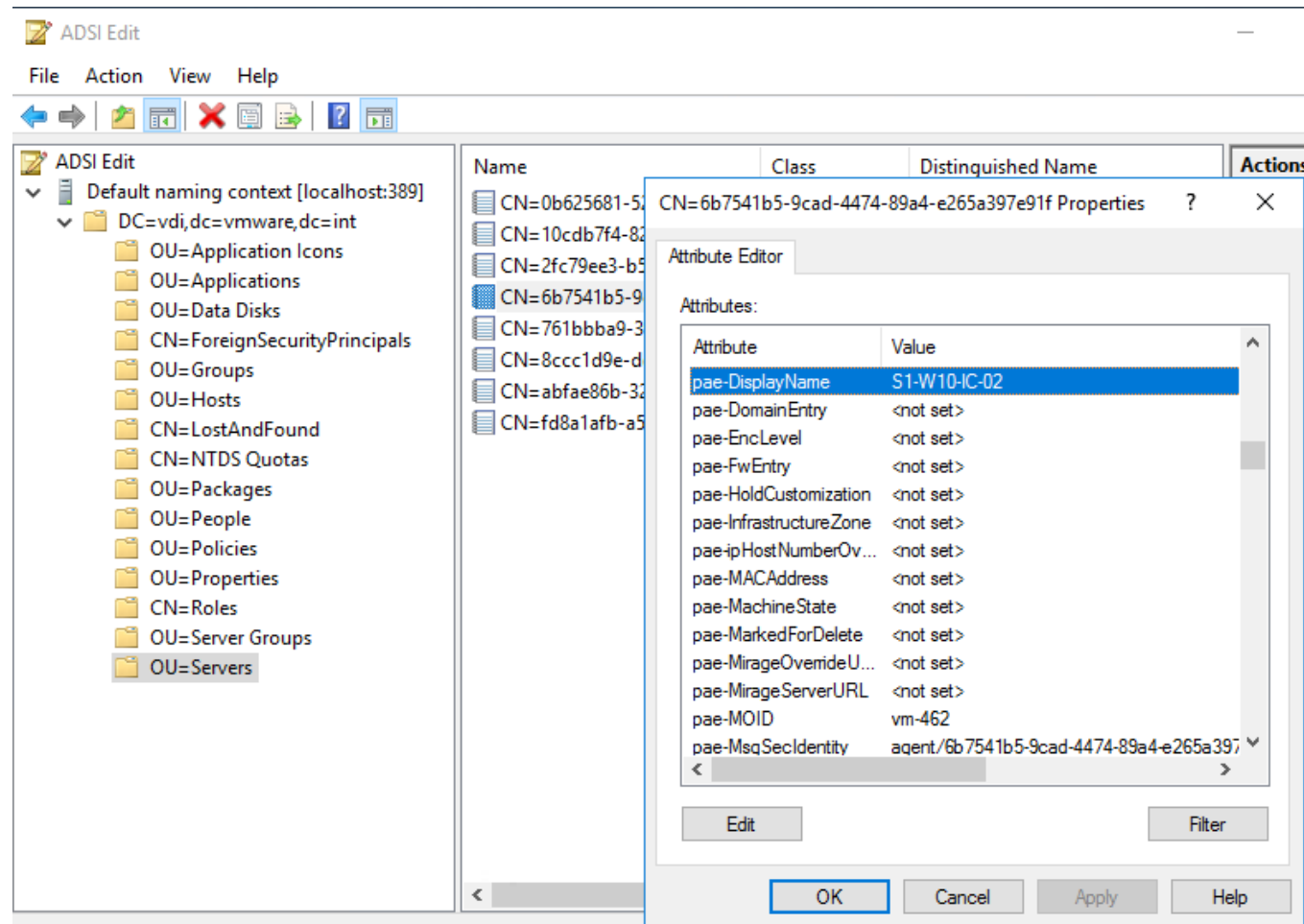
Can also follow the tail of a live log file.



ADSI Edit

Connecting to the ADAM Database:

<https://kb.vmware.com/s/article/2012377>



REST API – Horizon

Introduced in Horizon 7.12

Using the Horizon REST API:

- <https://techzone.vmware.com/resource/using-vmware-horizon-server-rest-api>

API Documentation

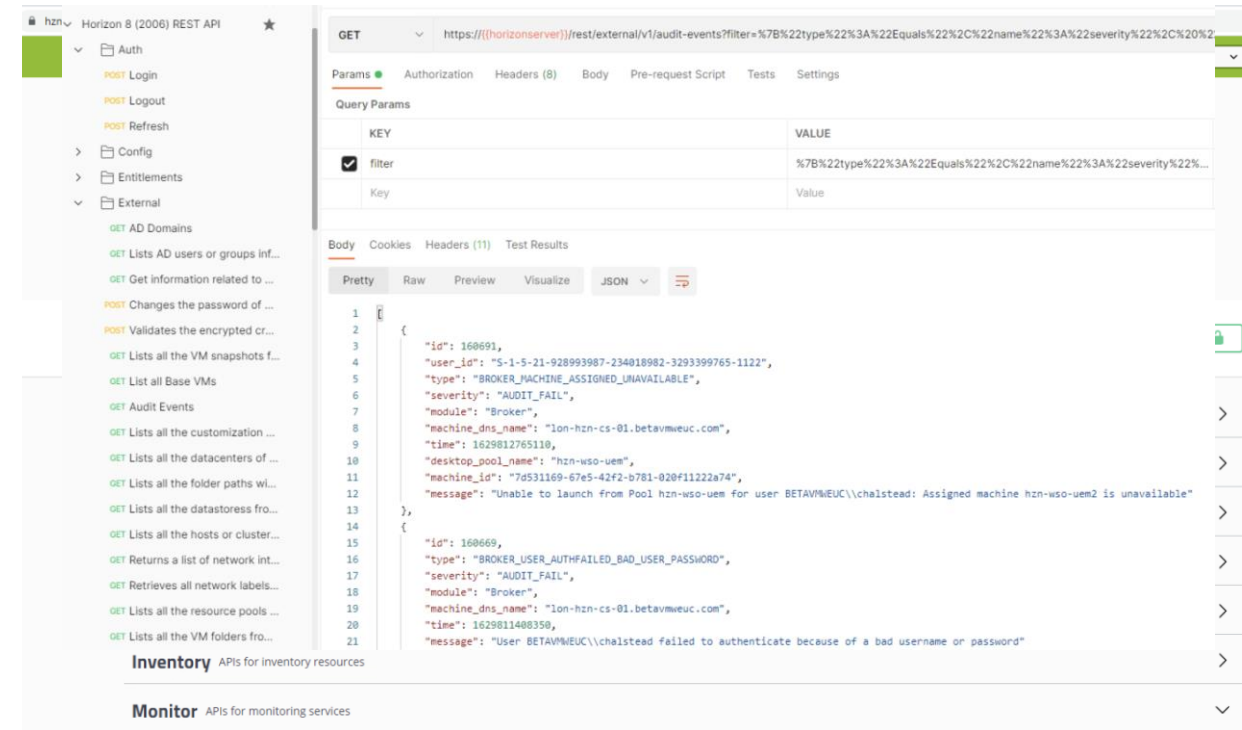
- <https://code.vmware.com/apis/1169>
- Samples: <https://code.vmware.com/samples>

Postman Collection:

- <https://code.vmware.com/samples/6432/postman-collection---horizon-rest-api>

Swagger UI:

- <https://fqdn/rest/swagger-ui.html>
- Learn about / test the API locally



GET https://(horizonserver)/rest/external/v1/audit-events?filter=%7B%22type%22%3A%22Equals%22%2C%22name%22%3A%22severity%22%2C%20%22...

Params Authorization Headers (8) Body Pre-request Script Tests Settings

Query Params

KEY	VALUE
<input checked="" type="checkbox"/> filter	%7B%22type%22%3A%22Equals%22%2C%22name%22%3A%22severity%22%2C%20%22...
Key	Value

Body Cookies Headers (11) Test Results

Pretty Raw Preview Visualize JSON

```
1 {
2   {
3     "id": 160691,
4     "user_id": "S-1-5-21-928993987-234018982-3293399765-1122",
5     "type": "BROKER_MACHINE_ASSIGNED_UNAVAILABLE",
6     "severity": "AUDIT_FAIL",
7     "module": "Broker",
8     "machine_dns_name": "lon-hzn-cs-01.betavmweuc.com",
9     "time": 1629812765110,
10    "desktop_pool_name": "hzn-wso-uem",
11    "machine_id": "7d531169-67e5-42f2-b781-020f11222a74",
12    "message": "Unable to launch from Pool hzn-wso-uem for user BETAVMWEUC\\chalsead: Assigned machine hzn-wso-uem2 is unavailable"
13  },
14  {
15    "id": 160669,
16    "type": "BROKER_USER_AUTHFAILED_BAD_USER_PASSWORD",
17    "severity": "AUDIT_FAIL",
18    "module": "Broker",
19    "machine_dns_name": "lon-hzn-cs-01.betavmweuc.com",
20    "time": 1629811488359,
21    "message": "User BETAVMWEUC\\chalsead failed to authenticate because of a bad username or password"
```

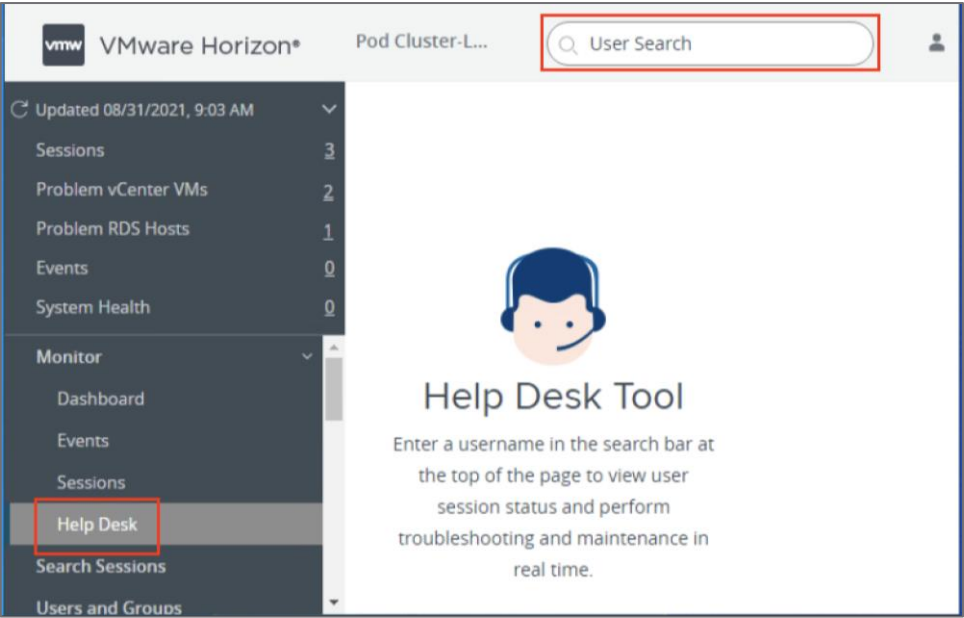
Inventory APIs for inventory resources

Monitor APIs for monitoring services

Horizon Help Desk Tool

Part of the Horizon Console
Installed by default on Connection Servers

- [https://\[CS FQDN\]/admin](https://[CS FQDN]/admin)



vdci-2.betav...

DetailsProcessesApplications

Client

Less ^

User Name: User1	Client Name: Win10-Client-1	Client IP: 10.142.30.107	Client OS: Windows
Client Version: 4.8.0	Protocol: VMware Blast		

VM

Less ^

Computer Name: vdi-ic-2.betavmweuc.com	Agent Version: 7.5.0	OS Version: -	Connection Server: Horizon75-2.betavmweuc.com
Pool: Windows Desktop	vCenter: -		
Session Duration: 2 hours 5 minutes	Session State: Connected	State Duration: 2 hours 5 minutes	
Logon Time: -	Logon Duration: -	Gateway/Proxy Name: uag-9aef46e9-f062-48f5-97f9-3a555528224f	Gateway/Proxy IP: uag.betavmweuc.com

User Experience Metrics <

Less ^

Frame Rate: 16 FPS			
BLAST Session Counters		BLAST Imaging Counters	
Estimated Bandwidth (Uplink): 616 Mbps	Packet Loss (Uplink): 0%	Transmitted Bytes: 95.5 MB	Received Bytes: 462 KB
BLAST CDR Counters		BLAST Audio Counters	
Transmitted Bytes: 868 B	Received Bytes: 546 B	Transmitted Bytes: 38.7 KB	Received Bytes: 16 B

Send Message

Remote Assistance

Restart

More... ▾

Resource Consumption

Logon details

Session info

- Client and connection information
- User experience metrics
- Session control, message, remote assistance

CPU, Memory, Network, Disk

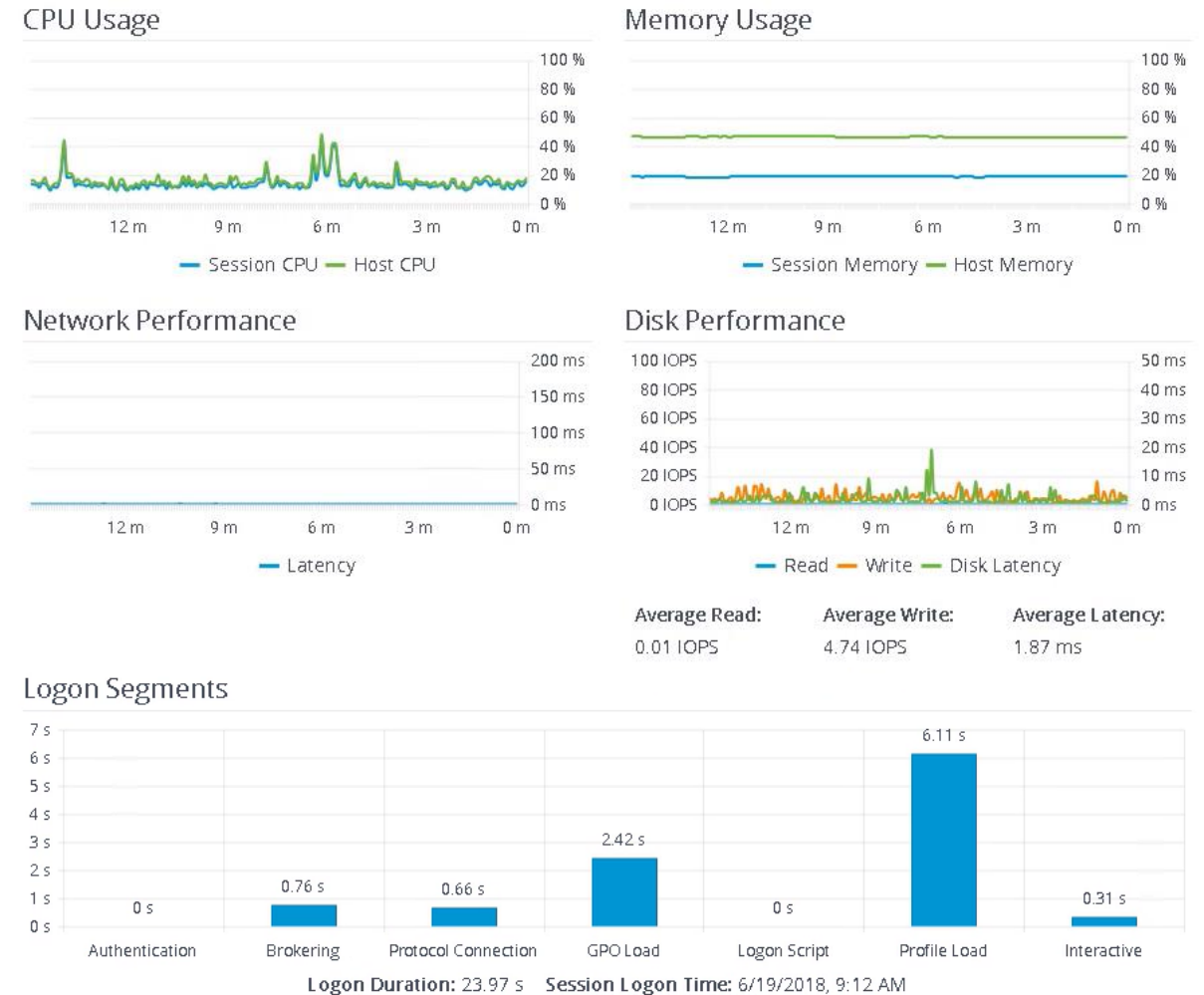
- Session metrics
- Host / VM metrics

Logon breakdown (client to broker)

- Brokering
- GPO load
- Profile load
- Interactive
- Authentication

To get logon segments enable timingProfiler writes to the event database:

- `"vdmadmin -l -timingProfiler -enable"` on each Connection Server



Horizon Performance Tracker

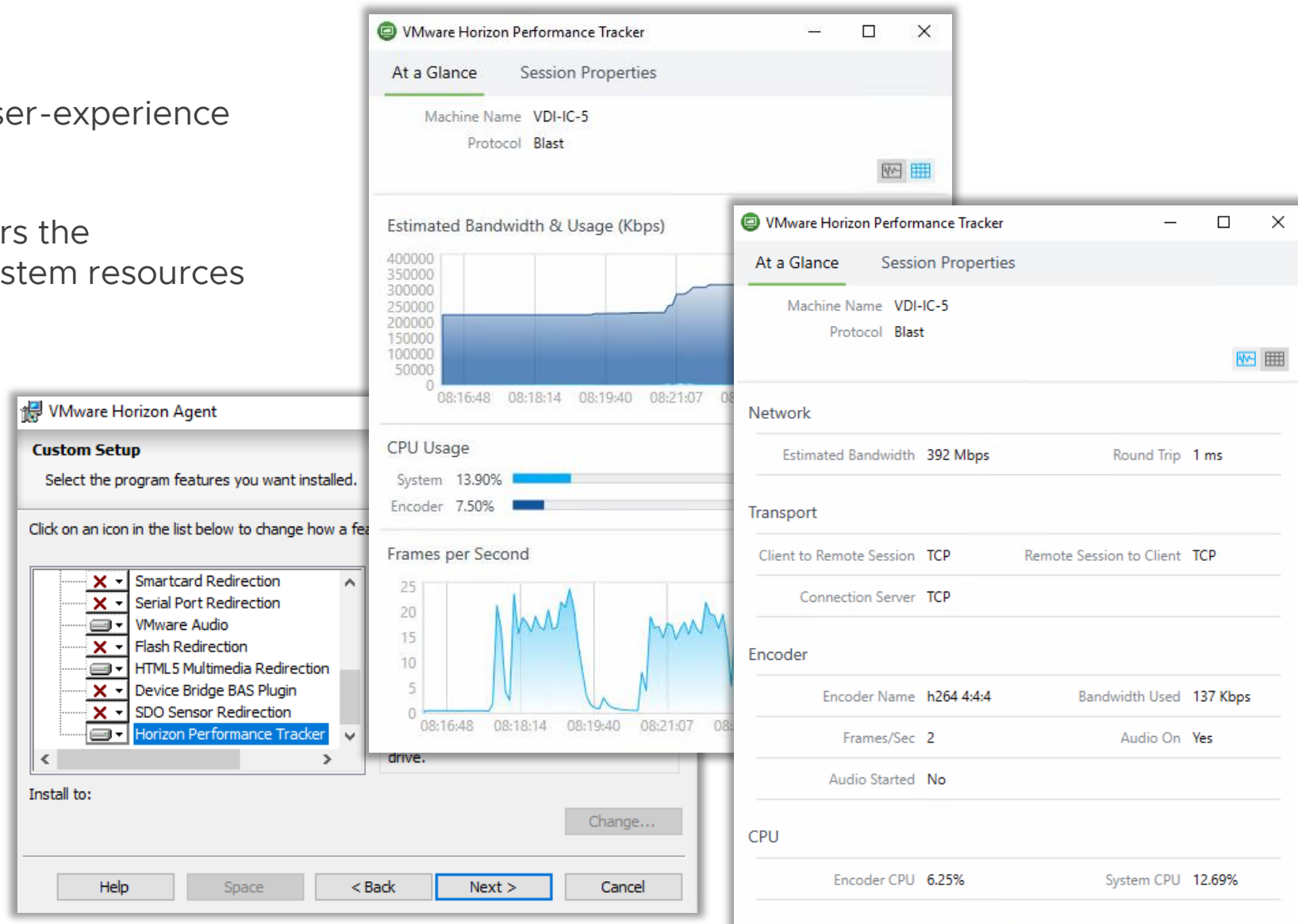
Enhanced support tool for gauging user-experience and display protocol details

Runs in a remote desktop and monitors the performance of Blast or PCoIP and system resources

Installed by the Agent Installer

GPO settings available

- Setting
- ☒ Enable Performance Tracker auto start in remote desktop connection
 - ☒ Performance Tracker basic setting
 - ☒ Enable Performance Tracker auto start in remote application connection



Troubleshooting Horizon Session Scripts

<https://code.vmware.com/samples>

Sample Scripts:

[Logoff Sessions Disconnected Longer Than a Specified Time](#)

[Manage Horizon Sessions By User](#)

[Export Horizon Sessions to .csv](#)



```
Administrator: Windows PowerShell
===== VMware Horizon PowerCLI Menu =====
Press '1' to Login to Horizon
Press '2' to Export Sessions to a .CSV
Press 'Q' to quit.
Please make a selection: 2
There are 1 total sessions

Session Start Time  Username                Pool Name  Machine Name Client Name Client Type Client Version Client IP
-----
1/20/2021 3:27:22 PM betavmweuc.com\chalstead lon-mcw-dt lon-mcw-dt-3 Chris' iMac Mac      8.1.0      192.168...

horizon session data written to: C:\Users\chalstead\Documents\Sessions_1_22_2021.csv
```

Horizon Event Notifier

VMware Fling

Overview

Connects to one or more existing Horizon Event Database(s) and allows the user to customize which types of alerts to be notified on

Can be run from any Windows based system

Collects and sends the alerts via email (SMTP) to users that are specified during the configuration process

Features

Pro-active alerting on Horizon events via SMTP directly from the one or more Horizon View Event database(s)

On VMware Fling site - <https://flings.vmware.com/horizon-event-notifier>

The screenshot shows the 'Horizon Event Notifier' application window. It has a menu bar with 'File' and tabs for 'Horizon Events' and 'Settings'. The 'Settings' tab is active, showing three main sections: 'SQL Server Settings', 'Horizon View Events', and 'SMTP Server Settings'.
SQL Server Settings: Includes a table for 'Monitored View Event DBs' with 'London' selected. To the right are fields for 'Name' (London), 'DB Server' (sql-hcs-01.betavmweuc.com), 'Database' (hcsevents), 'Username' (hcsevents), and 'Table Prefix' (lon). There are buttons for 'Test Connection', 'Save Changes', 'Add SQL Server', and 'Remove SQL Server'. A checkbox 'Test DB connection on update?' is checked.
Horizon View Events: Includes checkboxes for 'Alert on Audit Fail Events', 'Alert on Warning Events', 'Alert on Error Events', and 'Alert on Informational Events'. A 'Query Last' field is set to '60' and the unit is 'Minutes of Events'. A 'Save Changes' button is at the bottom right.
SMTP Server Settings: Includes fields for 'SMTP Server' (172.16.28.170), 'Port' (25), 'Send From' (alerts@chrisdhalstead.com), and 'Alert Recipients' (chalstead@vmware.com). A 'Send Test Email' button is at the bottom right. A checkbox 'Send Alerts via Email?' is checked, with a note 'Separate addresses with a Comma'. A 'Save Changes' button is at the bottom right.
At the bottom of the window, there is a 'Stop' button, a 'Poll Every' field set to '60' with the unit 'Seconds', and a 'Refresh' button. The status bar at the very bottom says 'Last Queried at: 8/30/2021 11:17:08 AM'.

Horizon Events Database Export Utility

VMware Fling

Overview

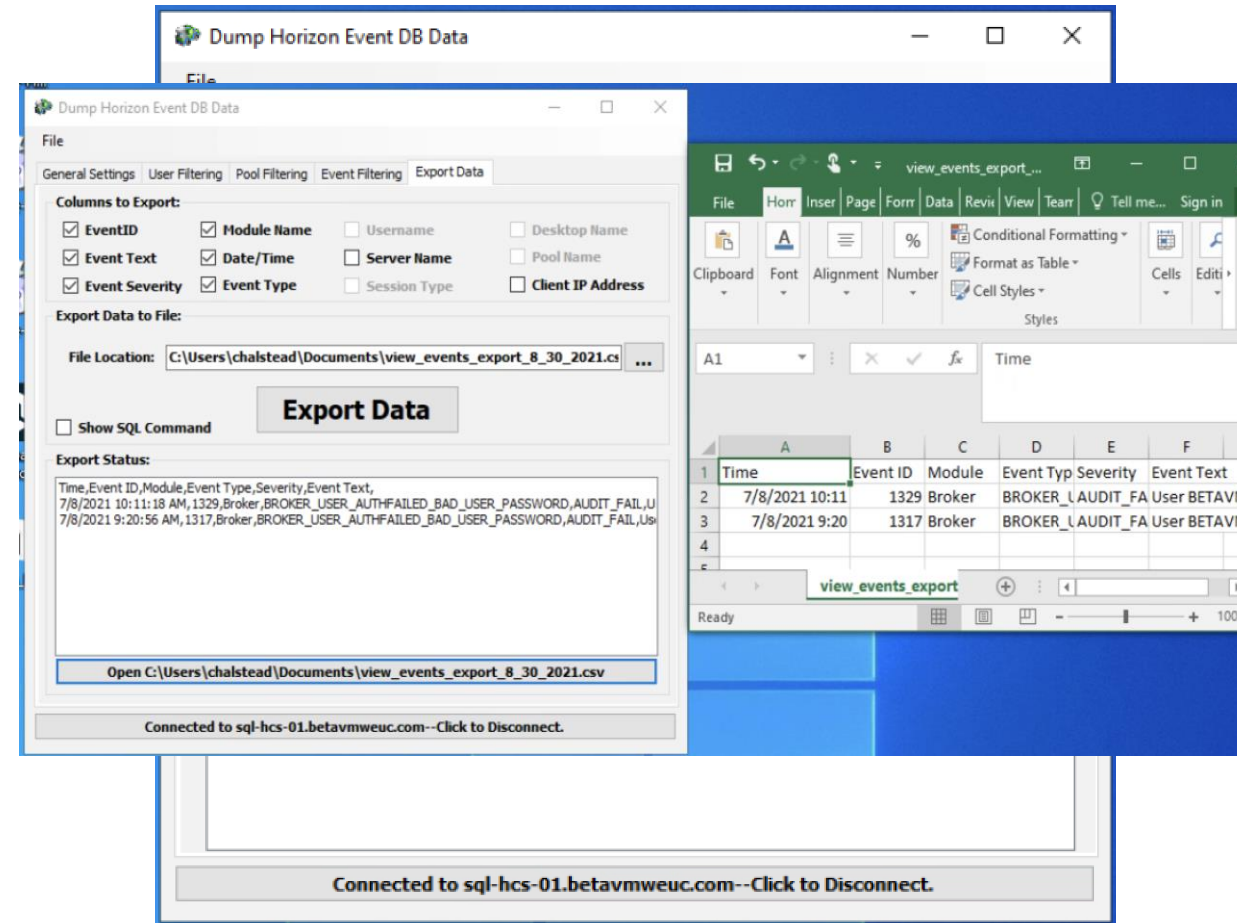
Allows administrators to easily apply very detailed filtering to the data and export it to a .CSV file

Filter on time range, event severity, event source, session type (application or desktop), usernames and event types

Features

Easily export filtered data from the Horizon Events Database to a local .CSV file

On the VMware Fling site: <https://flings.vmware.com/horizon-view-events-database-export-utility>



VMware Event Broker Fling

VMware Fling – Tech Preview of Horizon Integration

Overview

VMware Event Broker Appliance (VEBA) Fling

Unlock the hidden potential of events in the SDDC including Horizon, to easily take Events to the next level

Features

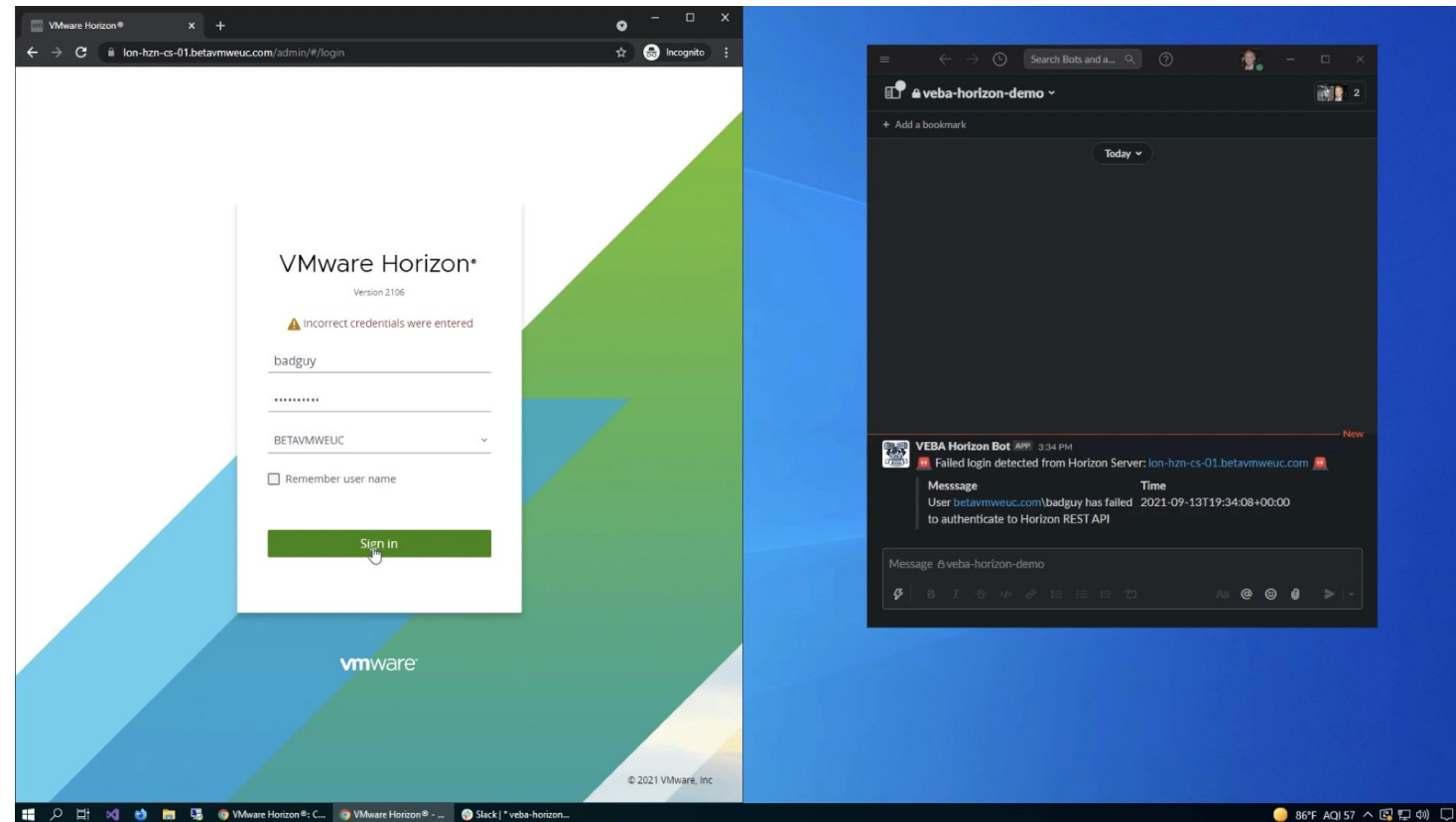
Only need to write minimal business logic without going through a steep learning curve understanding VMware APIs

Sent alerts to preferred solution (Teams, Slack, Telegram, SMS, SMTP, PagerDuty, etc.)

Take actions bases on alerts – ex. Expand Pools, etc.

On the VMware Fling site:

<https://flings.vmware.com/vmware-event-broker-appliance>



Horizon Reach

VMware Fling

Overview

Web based, monitoring and alerting fling for VMware Horizon On-Premises deployments

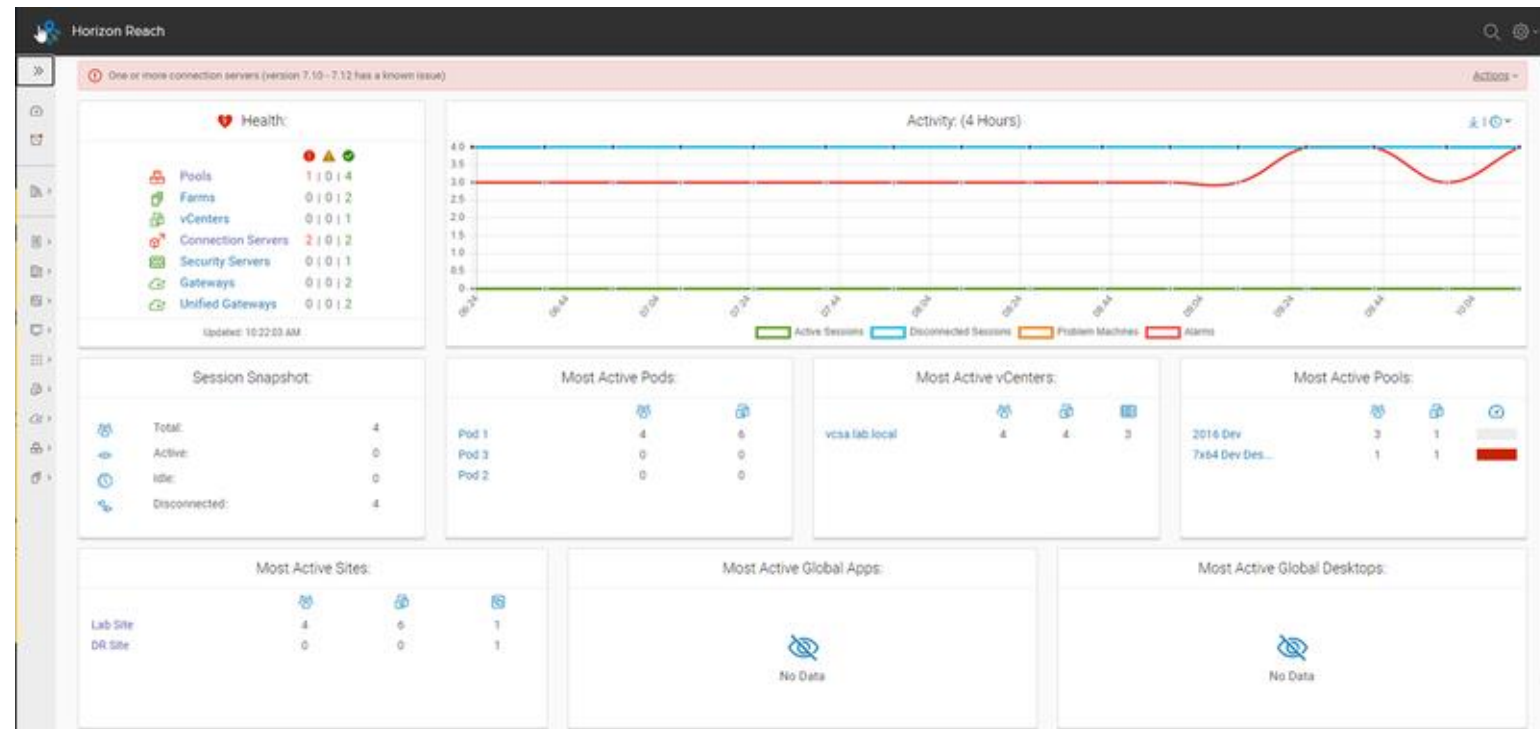
Features

Gathers pertinent errors from each separate environment

Displays them all in a single place, creating an easy location for administrators to monitor the environment

Provides detailed first step in the troubleshooting process

VMware Flings site: <https://flings.vmware.com/horizon-reach>



SSL Certificates

Horizon

Configuring Certificates for Horizon

#1 Support Ticket to GSS

Replace self-signed certs on

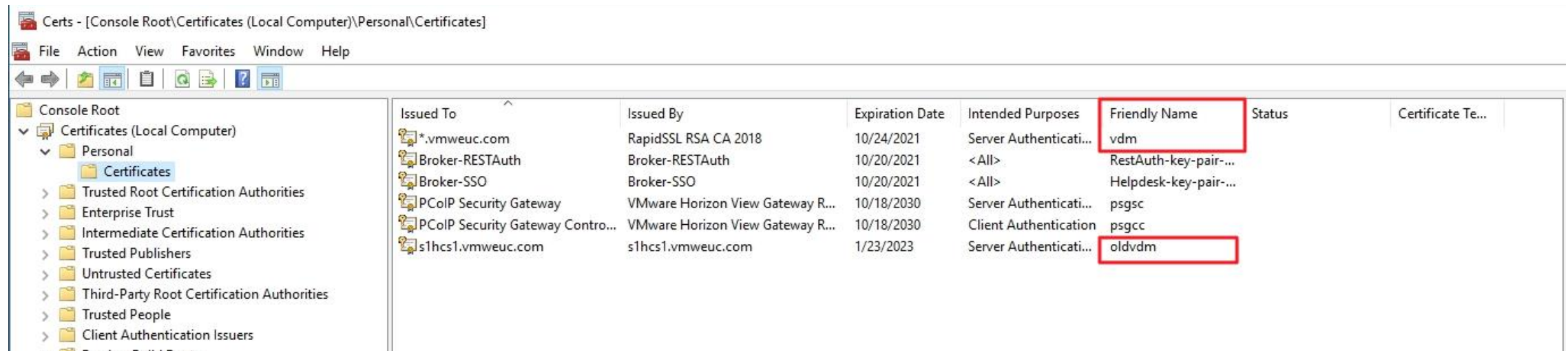
- Connection Servers
- Unified Access Gateways
- vCenters
 - Internal communications

Read the Horizon certificate documentation

- *Scenarios for Setting Up TLS Certificates for Horizon*

Use Certificate Automation Tool for vCenter

Rename the self-signed generated certificate!



Troubleshooting TLS Certificates for Horizon

Key issues when creating certs from 3rd parties or CA:

- Make sure key is exportable

Key issues when using your own Microsoft CA:

- Make sure the Subject name is your DNS name
- Set DNS SubjectAltNames for DNS name, including IP and localhost

Generate a Certificate Signing Request (CSR) & Private Key

- Certreq - <https://kb.vmware.com/kb/2032400>
- OpenSSL - <https://www.golinuxcloud.com/openssl-subject-alternative-name/>

Common symptoms after failed certificate replacement

- Services fail to start
- Admin console fails to load - <https://kb.vmware.com/kb/2068666>

Performance

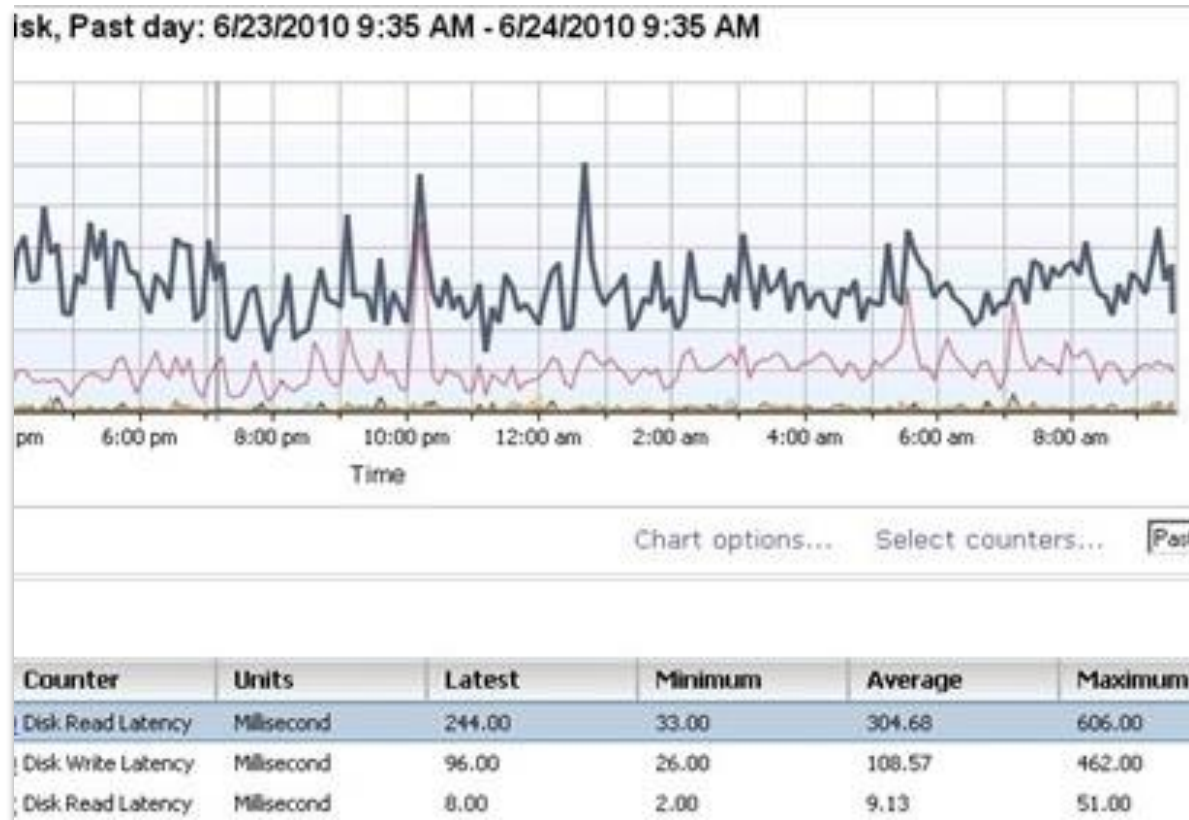
Desktop Performance

Common Issues

- Storage IO bottleneck
- Memory contention
- CPU contention
- Network issues

Where to look

- vCenter Server
- vROps
- ESXTOP
- 3rd Party Tools?



The 3 Pillars of Performance

What to look for

CPU

Cluster/Host utilization < 90%

VM utilization - %USED (ESXTOP)

VM %RDY Time (ESXTOP) < 10

Memory

Host utilization < 85%

VM utilization

Swapping / Ballooning

- SWCUR > 1
- MCTLSZ > 1 (ESXTOP)

Storage

Disk Read Latency < 25ms

ESXTOP DAVG or KAVG < 25ms
(ESXTOP)

Optimize Your Images!

<https://techzone.vmware.com/manually-creating-optimized-windows-images-vmware-horizon-vms>

VMware OS Optimization Tool 2021

vmware® OS Optimization Tool

2106 TM

Optimize Generalize Finalize Update History Templates References

System Information

OS: Microsoft Windows 10 Enterprise
Version: 21H1 (19043.1052)
Processor: AMD EPYC 7543 32-Core Processor
System Type: 64-bit
Windows Locale: United States
Display Adapter RAM: N/A

System Name: VMWAREY-ONMVIKT
User Name: Administrator
Windows Directory: C:\windows
Physical Memory: 3 GB
Display Controller: VMware SVGA 3D
Network Adapter: vmxnet3 Ethernet Adapter

Analysis Summary

600
400
200
0

Total: 483
Recommended: 482
Optional: 15

Optimization Not Applied (red bar)
Optimization Applied (green bar)

Template: VMware(Windows 10 and Server 2016 or later) Common Options

Export Analysis Result Import Selections Export Selections Search

Optimizations	ExpectedValue	Actual Value	Description
✓ Modifications to Standard Image (511 items)			Select "Disable" in the Options tab of any Task to bypass processing. Disable this entire section in the same manner.
✓ Security (108 items)			
> Defender Antivirus (16 items)			
> Firewall (1 items)			
> HVCI (7 items)			
> Security Center (6 items)			
> SmartScreen (5 items)			
> Telemetry and Privacy (37 items)			
> Windows Update (35 items)			
✓ User Experience (150 items)			
> Background (11 items)			
> Notifications (9 items)			
> Sounds (28 items)			
✓ Features (50 items)			
> Autorun (5 items)			
> Content Delivery Manager (23 items)			

Analyze Optimize

Connectivity Issues

Common Challenges

- Horizon Client can't connect
- Logon failure
- Black screen
- Poor quality display
- Randomly disconnected session



Horizon Connection Flow and Ports

Internal connection (Blast Extreme example)

Horizon connection consists of two phases:

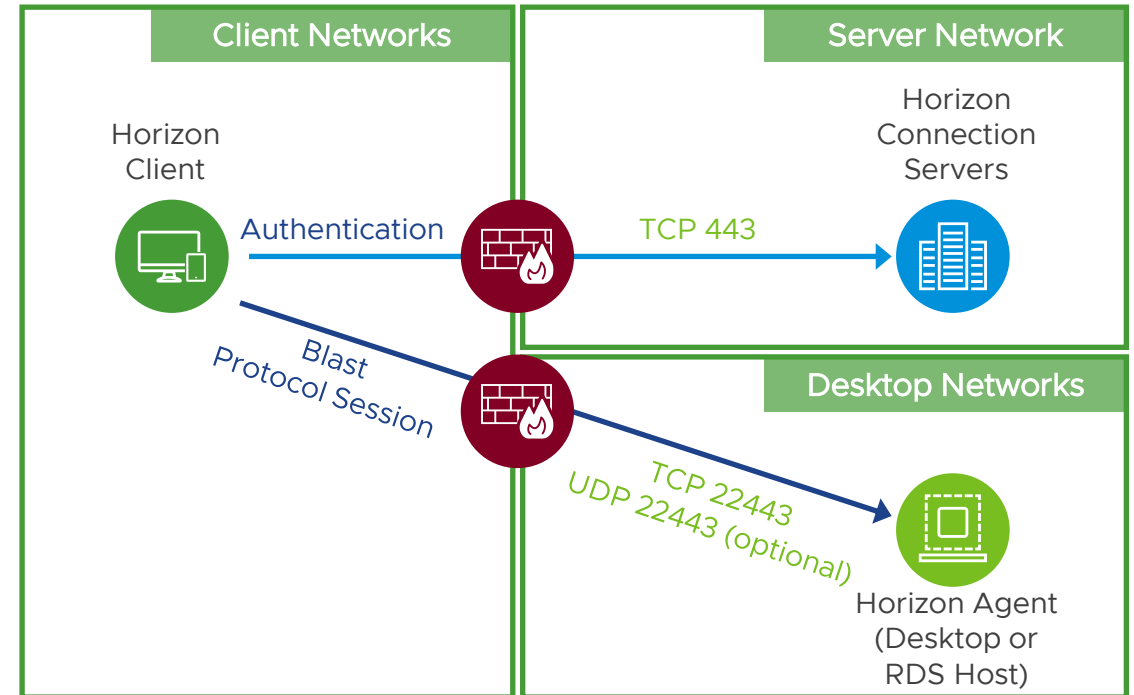
1. Authentication and session management
2. Protocol session

Internal Connection

1. Authentication = Client to Connection Server
2. Protocol = From Client to Agent

Check

- Ports are open
- Routing is correct
- Clients are allowed through firewall to
 - Connection Servers
 - Horizon Agents



Horizon Connection Flow and Ports

External connection (Blast Extreme example)

Authentication

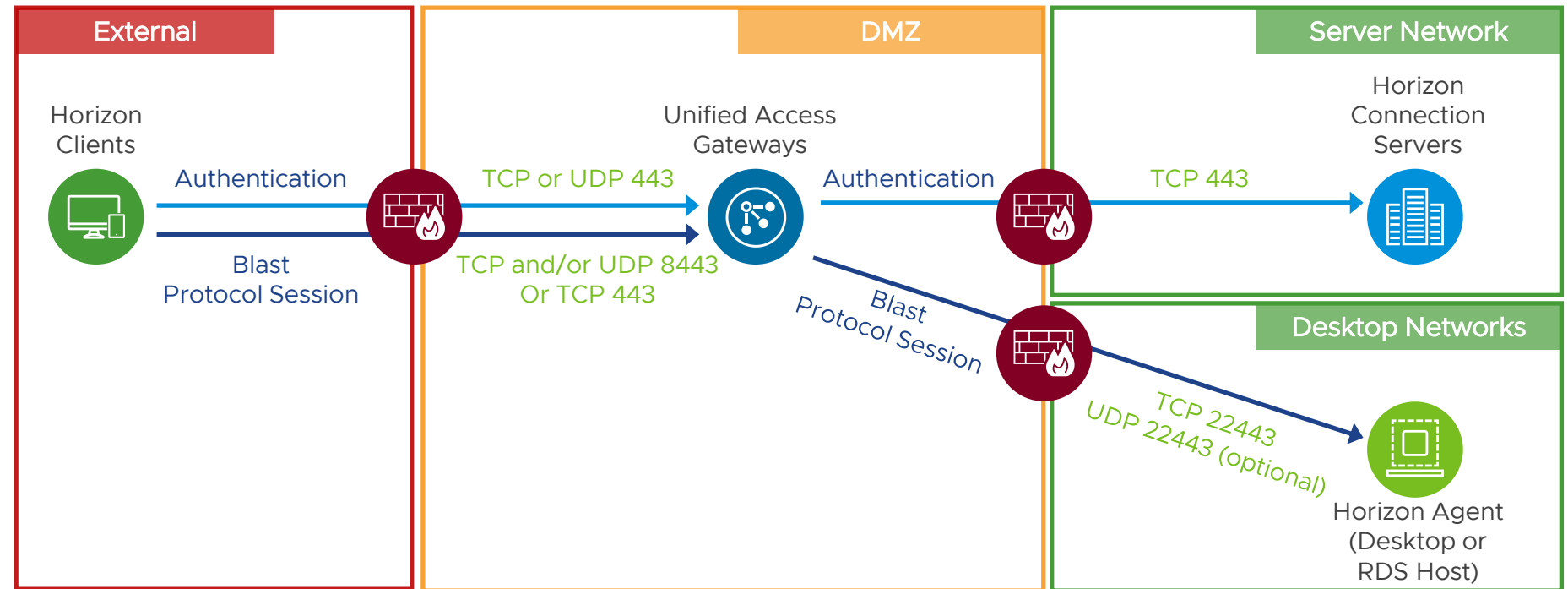
- Client to UAG
- UAG to Connection Server

Protocol

- Client to UAG
- UAG to Agent

Check

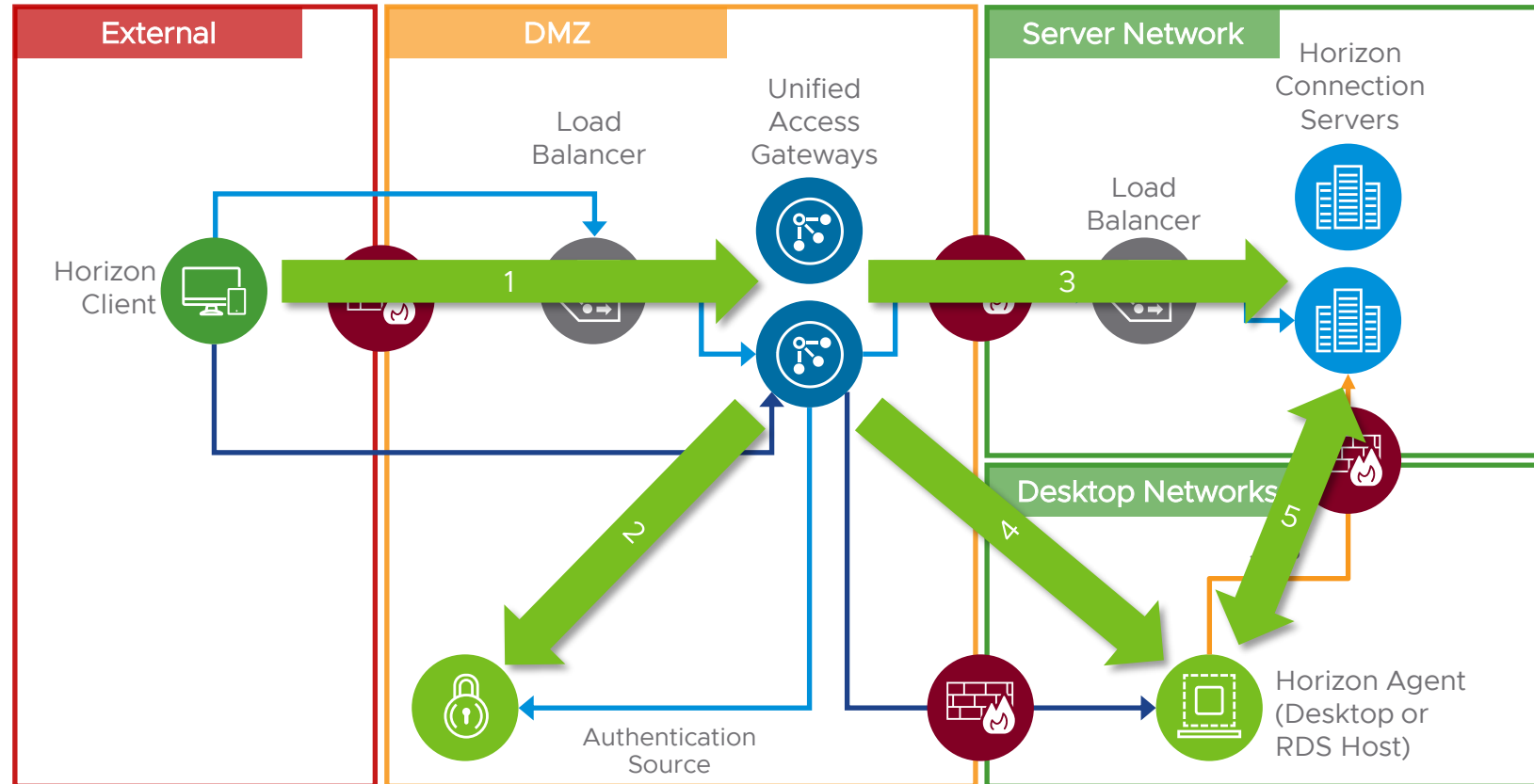
- Ports are open
- Routing is correct
- Firewall rules



<https://techzone.vmware.com/resource/network-ports-vmware-horizon>

Focus on the Right Area

What works and what doesn't



1. Horizon Client to Unified Access Gateway
2. (Optional) Unified Access Gateway to Authentication Source
3. Unified Access Gateway to Connection Server
4. Unified Access Gateway to Horizon Agent
5. Horizon Agent and Connection Server

<https://techzone.vmware.com/resource/understand-and-troubleshoot-horizon-connections>

Blast Connection never arrives at Unified Access Gateway

Blast connectivity issues

Timeout log entry in bsg.log

1. Load balancer session affinity or timeout is incorrect
 - Blast connection is misrouted to the wrong UAG appliance
2. Firewall (between the Internet and UAG) blocking Blast protocol port
 - TCP 8443 (or 443 if the blastExternalUrl specifies :443)
 - Also, optionally UDP 8443
3. Load balancer can sometimes block WebSockets (Blast uses WebSockets)
 - Issues seen with both Netscaler and Microsoft TMG
 - Enable WebSockets in these devices
4. Misconfiguration of blastExternalUrl
 - Should be set to a value usable by the client to connect to the same UAG appliance
 - Fix the blastExternalUrl config on UAG

Connection from Unified Access Gateway to Desktop or RDSH Fails

Blast connectivity issues

Firewall (between UAG and Agent) blocking Blast protocol port

- TCP 22443 (and optionally UDP 22443)

Networking routing from UAG to Agents is incorrect

- Add static routes to UAG

Connection Server configured for Blast Secure Gateway

- Error logged in bsg.log on UAG
- Multi-hop Blast Secure Gateway is not supported
- Disable gateways on Connection Servers

Other Connectivity Issues

Blast connectivity issues

Origin checking on Connection Server

Native client Blast works but HTML Access Blast fails

- With some browsers and not others

Common reason is Origin checking failure on Connection Server

- [Cross-Origin Resource Sharing \(CORS\) enabled](#) by default on 2106 and later

Look at the debug log file on Connection Server and search for "Origin" to look for origin checking failures

SSL certificate errors

Bad SSL Server Certificate on UAG

Certificate Mismatch

- Offloaded TLS/SSL handled on load balancer and the UAG appliance and load balancer have different certificates
- When Blast connection is misrouted to the wrong UAG appliance, and that appliance has a different certificate to the correct UAG appliance

Blast Protocol Logs

Agent Logs:

Location: %ProgramData%\VMware\VMware Blast

Blast-Service.log – Log data from the Blast Service

Blast-Worker-SessionId# - Log data from the Blast Worker Process

Blast-Proxy.log – Log data from the Blast Proxy Process

Adjust Logging Level:

Can accept the following strings: "all", "trace", "debug", "info", "warn", "error", "fatal", "off".

Default is "info"

```
[HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config] "LogLevel"="info"
```

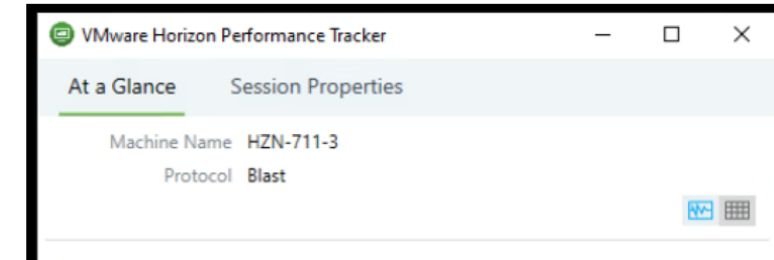

Blast Extreme Switch Encoder

Dynamic encoder switch

- Switches between video optimized encoder and text optimized encoder (Blast Codec or Adaptive)
- Helps maintain crisp text and video with reduced bandwidth usage

To enable:

- Windows Agent
HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderSwitchEnabled = 1
- Linux Agent
Under /etc/vmware/config,
set RemoteDisplay.allowSwitchEncoder=TRUE
- Or use DEM Horizon Smart Policies

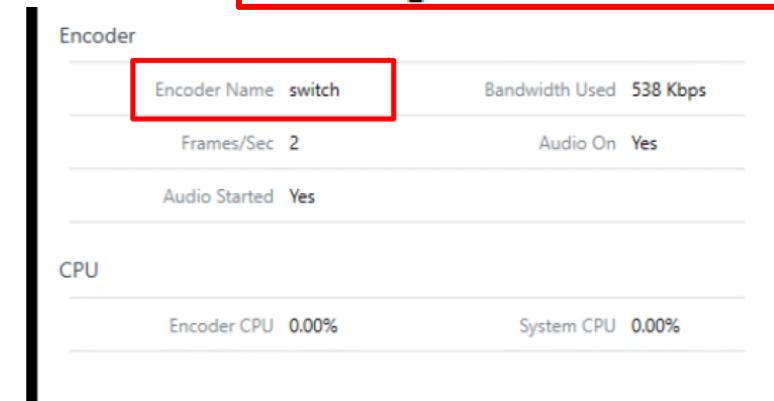


SwitchEnc: 1 Screen 0 switching to h264 4:4:4 encoder

VVC: Bandwidth stat poll logger: Rate 24251.7 KBps. Mu

VVC: Bandwidth stat poll logger: Rate 37765.9 KBps. Mu

SwitchEnc: 1 Screen 0 switching to BlastCodec encoder.



Provisioning and Customization Errors

Common Issues

- No desktop available
- Pool provisioning issues – customization
- Agent not communicating with broker
- Stuck at desktop login screen (SSO)



Loading Failed

The assigned desktop source for this desktop is not currently available. Please try again later, or contact your system administrator.

Instant Clone – Smart Provisioning*

Mode A and Mode B Instant Clones

Mode A

Instant Clones with ParentVMs

Density > 12 VMs per host in selected cluster

- This can be on an active pool – Smart Provisioning will switch modes dynamically

On logoff forks new virtual machine from ParentVM

- On push image, does a full resync

Horizon on AVS

- vCenter permission

Mixed vCenter / vSphere versions

vTPM VMs

Mode B

Instant Clones without ParentVMs

Density <= 12 VMs per host in selected cluster

- This can be on an active pool – Smart Provisioning will switch modes dynamically

On logoff – reverts snapshot and resets VM PW

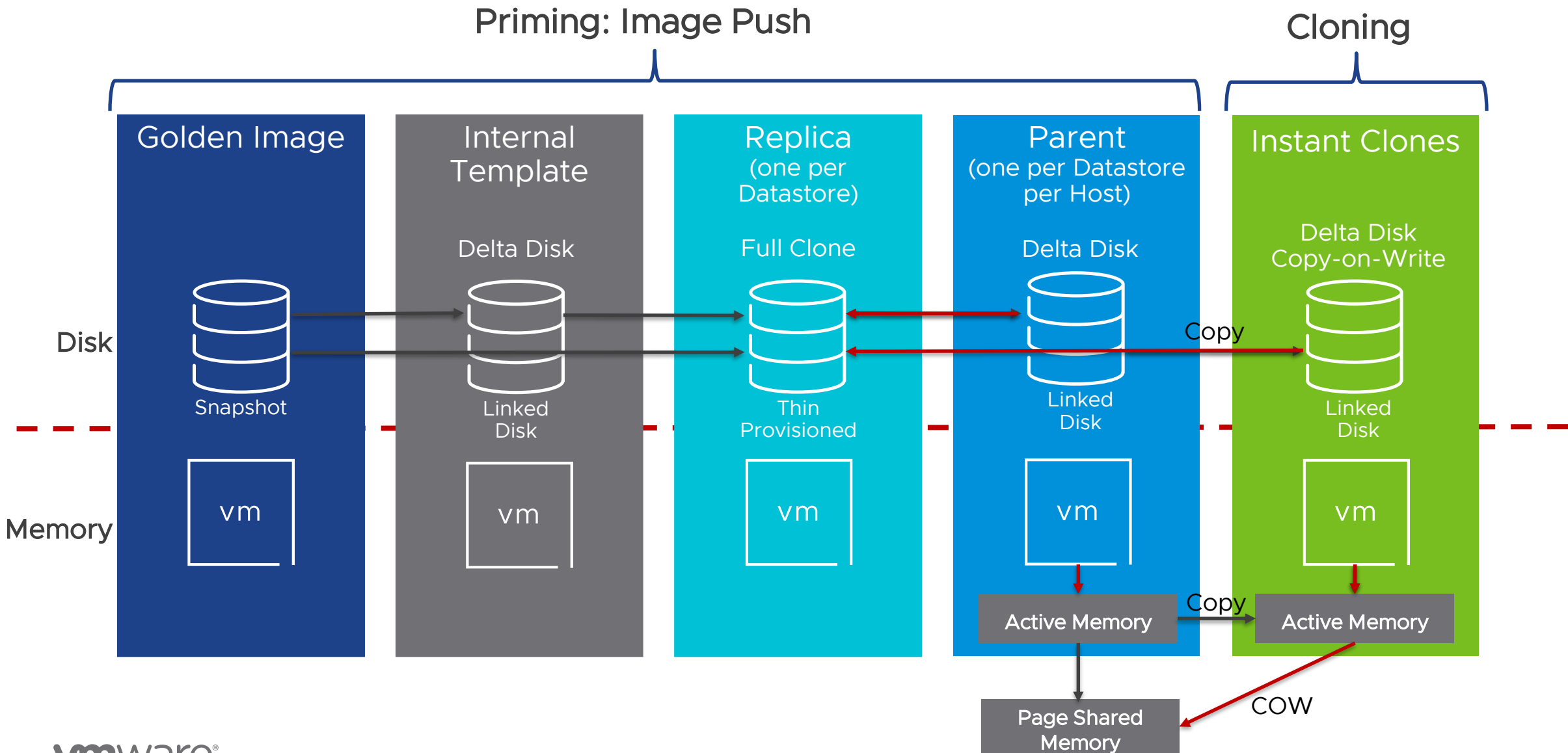
- On push image, does a full resync

Linux VMs

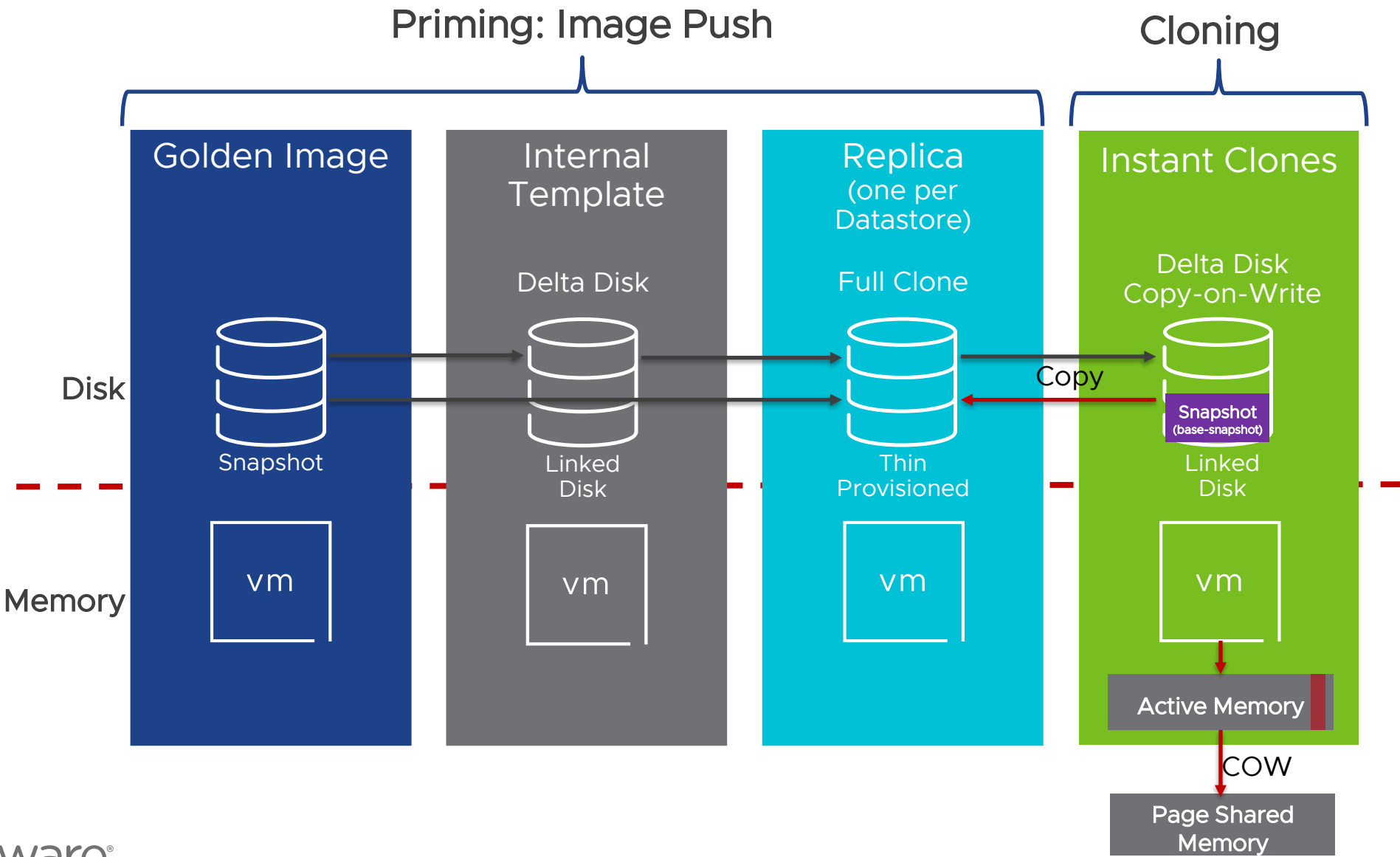
vGPU VMs

*Smart Provisioning enabled for Horizon 2006 and later and Horizon 7.13

Provisioning Instant Clones – with Parent VMs (Mode A)



Provisioning Instant Clones – without Parent VMs (Mode B)



Troubleshooting Instant Clones

Smart Provisioning

How to know if a desktop is created Mode A or Mode B

- Check virtual center to see if that desktop has a snapshot called “base-snapshot”. This is a Mode B Desktop
- This script can be run inside of the desktop to determine what kind of desktop it is (Full Clone, Instant Clone Mode A or Mode B)

– [Detect Virtual Desktop Type](#)

Force a desktop pool or farm to Mode A, Mode B or Smart Provisioning (post Horizon 2006)

- [Connect to ADAM Database](#)
- Go to OU=Server Groups, CN={name of pool} and update paeProvisionScheme
 - Mode A = ModeA
 - Mode B = ModeB
 - Smart Provisioning = blank

The screenshot shows the ADSI Edit console with a tree view on the left and a table of objects on the right. The table lists objects under the path DC=vdi,dc=vmware,dc=int, including CN=hzn-wso-uem, CN=lon-flt-mcw, CN=lon-mca-flt, CN=lon-mcw, CN=lon-mcw-dt, CN=Manual-PCOIP-Test, CN=two-nics, and CN=uem-FC. Each object is of class pae-ServerP... and has a distinguished name. Below the table, a terminal window displays the output of a script: "Horizon Agent Detected", "Instant Clone Engine Installed", "VM is an Instant Clone", and "VM is an Instant Clone with a ParentVM (Mode A)".

Name	Class	Distinguished Name
CN=hzn-wso-uem	pae-ServerP...	CN=hzn-wso-uem,OU=Server Groups,DC=vdi,DC=vmware,DC=int
CN=lon-flt-mcw	pae-ServerP...	CN=lon-flt-mcw,OU=Server Groups,DC=vdi,DC=vmware,DC=int
CN=lon-mca-flt	pae-ServerP...	CN=lon-mca-flt,OU=Server Groups,DC=vdi,DC=vmware,DC=int
CN=lon-mcw	pae-ServerP...	CN=lon-mcw,OU=Server Groups,DC=vdi,DC=vmware,DC=int
CN=lon-mcw-dt	pae-ServerP...	CN=lon-mcw-dt,OU=Server Groups,DC=vdi,DC=vmware,DC=int
CN=Manual-PCOIP-Test	pae-ServerP...	CN=Manual-PCOIP-Test,OU=Server Groups,DC=vdi,DC=vmware,DC=int
CN=two-nics	pae-ServerP...	CN=two-nics,OU=Server Groups,DC=vdi,DC=vmware,DC=int
CN=uem-FC	pae-ServerP...	CN=uem-FC,OU=Server Groups,DC=vdi,DC=vmware,DC=int

```
Horizon Agent Detected
Instant Clone Engine Installed
VM is an Instant Clone
VM is an Instant Clone with a ParentVM (Mode A)
```

Desktop Not Available

What to look for...

Provisioning Error

Check console for Pool status

Check datastore capacity

Check event database

- BROKER_PROVISIONING_ERROR_*

Check vCenter

- Instant Clone administrator accounts
- Account disabled
- Password expired

Customization Error

Check desktop status

- AGENT UNAVAILABLE

Check Horizon Dashboard

- Desktop Status > Preparing Desktops OR Problem Desktops

Check desktop connectivity to:

- DNS – Forward and reverse
- DHCP – Contactable, free leases
- AD – Credentials for LC/IC domain join
- Connection Server

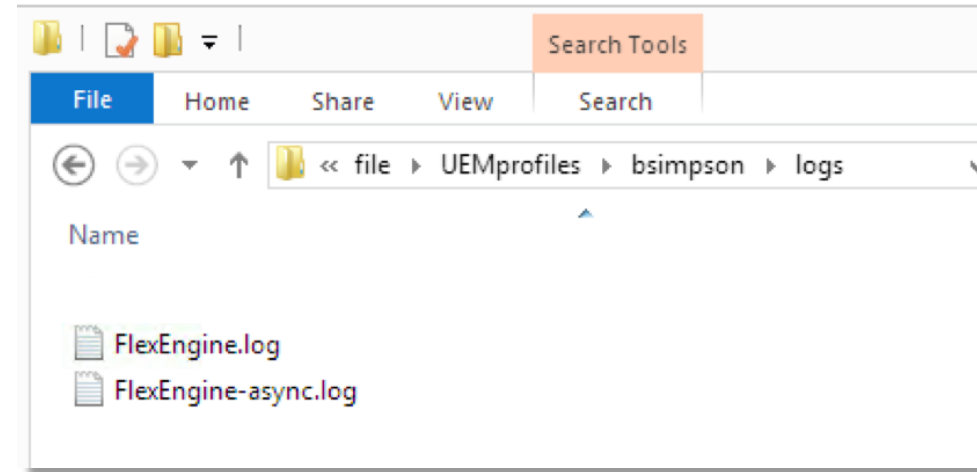
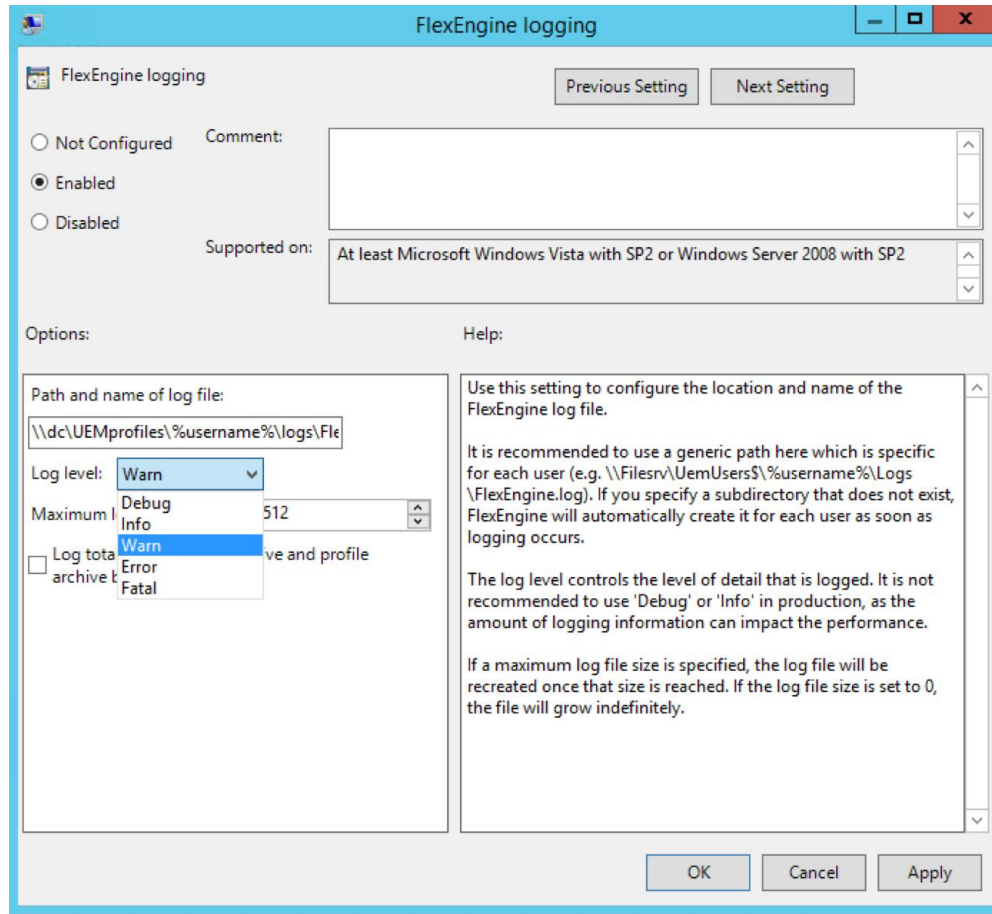
Dynamic Environment Manager

Common Issues



Dynamic Environment Manager Logs

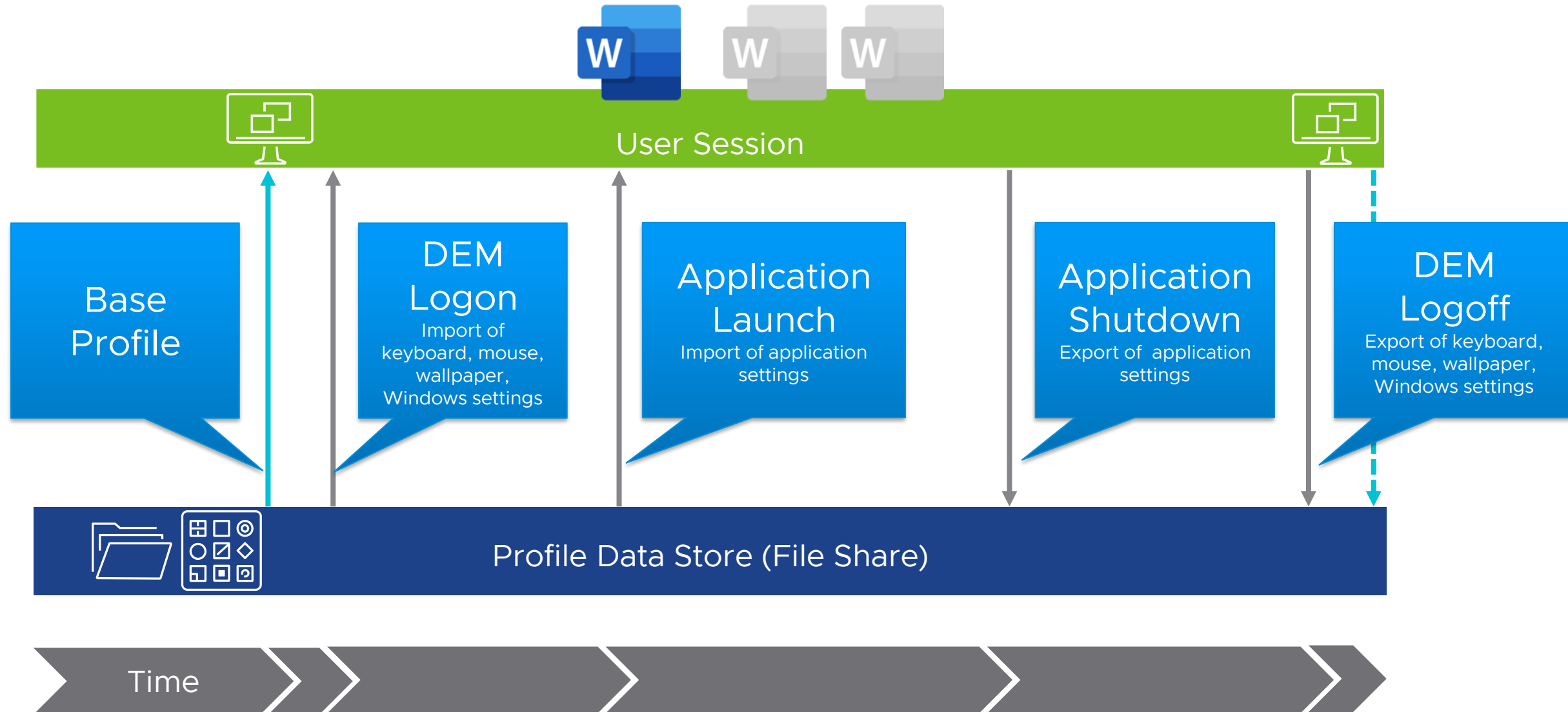
Global and Individual Debug Logs



Configure debug logging for individual user:

- <https://kb.vmware.com/kb/2113514>

Application Personalization & DirectFlex



DirectFlex Import

Directflex Import

```
2017-05-31 14:13:41.342 [INFO ] Performing DirectFlex import for config file '\\VMW-FS1\Config Files$\General\Applications\Notepad.TNT' [IFP#02e6c91a-b07538>>]
2017-05-31 14:13:41.342 [INFO ] Performing DirectFlex import for config file '\\VMW-FS1\Config Files$\General\Applications\Notepad.INI' [IFP#02e6c91a-b07538>>]
2017-05-31 14:13:41.343 [DEBUG] User: VMWARE\rwiesemann, Computer: VMW-CLIENT1, OS: x64-win7 (BuildNumber 7601, ServicePack 1, SuiteMask 100, ProductType 1/4, Lang
0409, IE 8.0.7601.17514, UEM 9.2.0.701, ProcInfo 1/2/4/4, UTC+02:00D), PTS: 3044/2872/3
2017-05-31 14:13:41.343 [DEBUG] Using profile archive '\\VMW-FS1\Userdata$\rwiesemann\Archives\Applications\Notepad.zip'
2017-05-31 14:13:41.343 [DEBUG] Triggered by 'C:\Windows\System32\notepad.exe'
2017-05-31 14:13:41.345 [DEBUG] Found flag file for '\\VMW-FS1\Config Files$\General\Applications\Notepad.INI'.
2017-05-31 14:13:41.346 [INFO ] Importing profile archive 'Notepad.zip' (\\VMW-FS1\Userdata$\rwiesemann\Archives\Applications\Notepad.zip)
2017-05-31 14:13:41.347 [DEBUG] ImportRegistry::Import: Calling '"C:\Windows\REGEDIT.EXE" /S "C:\Users\RWIESE~1\AppData\Local\Temp\FLX3F9E.tmp"' (RPAL: 1=0 (D/P), r=0)
2017-05-31 14:13:41.361 [DEBUG] Read 1 entry from profile archive (size: 788, compressed: 266)
2017-05-31 14:13:41.361 [INFO ] Completed DirectFlex import (20 ms) [<<IFP#02e6c91a-b07538]
```


FlexEngine Appears Not To Run

FlexEngine Client

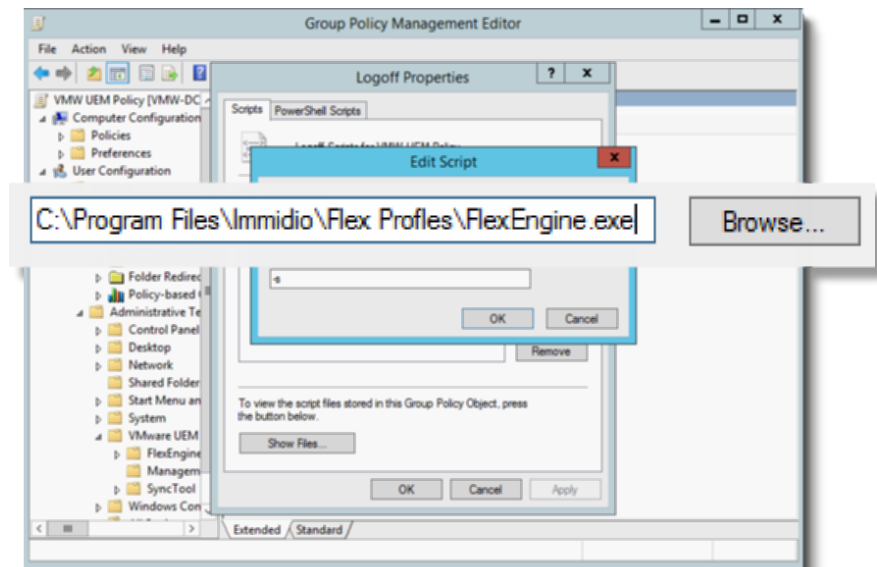
Requires use of Regedit.exe or Reg.exe to modify user-based registry keys

Must **not** be disabled via Local or Group Policy

Do not to run FlexEngine as a logon script *and* a Group Policy client-side extension

- Will show warning in log

Setting	State	Comment
Certificate support for mandatory profiles	Not configured	No
DirectFlex – advanced settings	Not configured	No
FlexEngine logging to the Windows event log	Not configured	No
Flex config files	Enabled	No
Run FlexEngine as Group Policy Extension	Enabled	No
FlexEngine logging	Not configured	No
Password support for Internet Explorer 6	Not configured	No
Profile archive backups	Not configured	No
Profile archives	Enabled	No
FlexEngine refresh settings	Not configured	No
Prevent access to Flex+ Self-Support	Not configured	No
Show Flex+ logon and logoff progress information	Not configured	No
Silo-specific Flex config files	Not configured	No



App Volumes

Common Issues



Certificates with App Volumes Manager

Replace Self-Signed Cert with CA-Signed Cert Trusted by App Volumes Agent

Options to Enable SSL

Replace self-signed certificate with a cert trusted by App Volumes Agent VMs

- See *Using SSL Certificates with App Volumes Manager* section in the [VMware App Volumes Administration Guide](#)
- Step-by-step blog with video
 - <https://blogs.vmware.com/euc/2016/12/app-volumes-2-12-certificate-replacing-self-signed.html>

Recommended for SSL

Use SSL for SQL Server Communication

Accept a CA-signed certificate from vCenter

Certificate validation for App Volumes Agent

- POC versus Production implementation



App Volumes Logs

Use Notepad++ to quickly group log entries by task.

"DJ" indicates
Manager
background
job

```
5415 P2928DJ5732 INFO Rendered text template (0.0ms)
5416 P2928DJ5732 INFO Completed 200 OK in 15.6ms (Views: 0.5ms | ActiveRecord: 0.0ms)
5417 P2928DJ5732 INFO
5418
5419
5420 P2928DJ5735 INFO Cvo: Starting job: Update Gra
5421 P2928DJ5735 INFO Cvo: Background worker updati
5422 P2928DJ5735 INFO Cvo: Background worker update
5423 P2928DJ5735 INFO Cvo: Finished job: Update Gra
5424 P2928DJ5736 INFO Cvo: Starting job: Expire Ses
5425 P2928DJ5736 INFO Cvo: Background worker expiri
5426 P2928DJ5736 INFO Cvo: Background worker removed 1 old session(s)
5427 P2928DJ5736 INFO Cvo: Finished job: Expire Sessions #<Thread:0x00000000accec0>
5428 P2928DJ5737 INFO Cvo: Starting job: Import Storage Groups #<Thread:0x00000000accec0>
5429 P2928DJ5737 INFO Cvo: Importing volumes from storage groups
5430 P2928DJ5737 INFO Cvo: Finished job: Import Storage Groups #<Thread:0x00000000accec0>
```

```
C:\Program Files (x86)\CloudVolumes\Manager\log\production000014.log - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
clock.yml production000014.log production000011.log
5666 P3312R2864 INFO Cvo: Re-using "Hypervisor <VMware vCenter#27893280 betavmweuc.com\svc-appvol@v
5667 P3312R2864 INFO Cvo: Acquired 'vcenter' adapter 1 of 16 for 'vcenter512961563' in 0.0 seconds
5668 P3312R2864 INFO Cvo: Volumes will be mounted synchronously
5669 P3312R2864 INFO RvSphere: Mounting 1 volume(s) in VM "vmworld-4" (503aeee7-5138-6ef9-3f4e-393245d15
5670 P3312R2864 INFO RvSphere: Attaching read-only volume "[t3600-01-Beta-VDI-2-2] cloudvolumes213EA/app
5671 P3312R2864 INFO RvSphere: Preparing to reconfigure VM "vmworld-4" (503aeee7-5138-6ef9-3f4e-393245d1
5672 P3312R2864 INFO RvSphere: ReconfigVM_Task task: task-10827
5673 P3312R2864 INFO RvSphere: Task total time: 0.330568s (execution time 0.32532s)
5674 P3312R2864 INFO RvSphere: vCenter operation failed: File [/vmfs/volumes/58d1816c-5526a246-f3cf-14f
5675 P3312R2864 ERROR RvSphere: Failed to reconfigure VM "vmworld-4" (503aeee7-5138-6ef9-3f4e-393245d15e
5676 -Found)
5677 P3312R2864 INFO Cvo: Incrementing unmount count for volume #2, now 1
5678 P3312R2864 INFO Cvo: Unsuccessful mount result appended to response: Volumes were not mounted
5679 P3312R2864 INFO Rendered text template (0.0ms)
5680 P3312R2864 INFO Completed 400 Bad Request in 1140.6ms (Views: 0.5ms | ActiveRecord: 93.7ms)
5681 P3312R2864 INFO
5682
5683
5684
5685 INFO Started GET "/log_fileshares/active?name=svservice&uuid=423af27b-71f3-101a-5f89-aa01f
5686 INFO NTLM: Authenticating URL "/log_fileshares/active"
5687 INFO NTLM: Received NTLM authentication to "/log_fileshares/active" (type 1)
5687 INFO NTLM: There are "0" NTLM authentication threads
```

"R" indicates
dynamic
Ruby job

Log files are
created daily

Degraded Performance or Slow User Logon

Check Logon Segments in Horizon to determine where the delay is

Optimize `clock.yml`

- If performance decreases as deployment scales
- Increasing `servers`, `workers`, and `thread_pool` requires additional CPU and RAM
- Involve GSS to ensure optimal settings
- Frequency of background jobs should be tuned/optimized

APP VOLUMES ITEM	FOR <=2,000 USERS	FOR >2,000 TO <5,000 USERS	FOR >=5,000 USERS
Number of App Volumes Manager servers	2	3	3+1 for each 2,500 users
Number of CPUs on each App Volumes server	4	6	8
RAM on each App Volumes server	4	8	
Changes to Manager\clock.yml (section medium:)	workers: 1	servers: 6 workers: 1	

```
clock.yml
17  small:
18    servers: 2
19    workers: 2
20    watcher: true
21    thread_pool: 25
22  jobs:
23    check_servers: 00:00:30
24
25  medium: # default
26    servers: 4
27    workers: 2
28    watcher: true
29    thread_pool: 35
30  jobs:
31    check_servers: 00:00:30
32
33  large:
34    servers: 6
35    workers: 4
36    watcher: true
37    thread_pool: 50
38  jobs:
39    check_servers: 00:00:30
40
```

<https://techzone.vmware.com/resource/vmware-app-volumes-2x-database-best-practices>

Unified Access Gateway

Certificates, logs, and integration

Certificates for Unified Access Gateway

Simplifying and troubleshooting

Replace the default self-signed certificate

Certificates must be trusted by client machines

Must also be applicable to

- All instances of Unified Access Gateway
- Load balancer

Use either

- Wildcard certificates
- Subject Alternative Name (SAN) certificates

Certificate can be in PFX or PEM format

Automate UAG deployment, including certificate

- Use PowerShell method
- Production-ready deployment in minutes
- Scripts now part of product download

Guide to scripted deployment

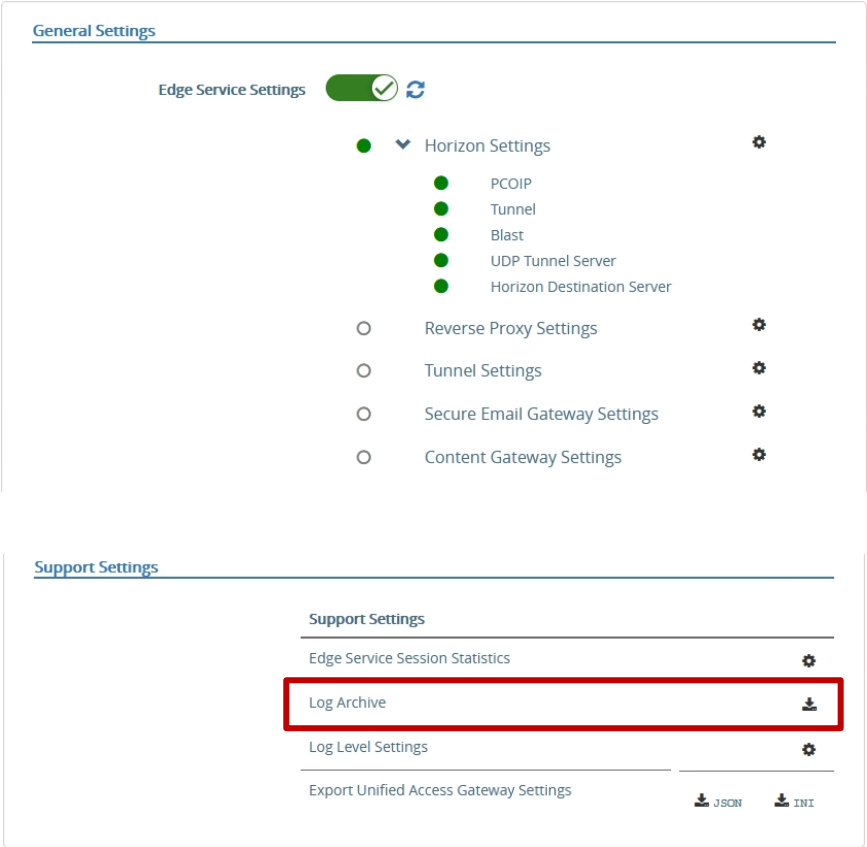
- <https://communities.vmware.com/docs/DOC-30835>
- Includes troubleshooting examples

How to guides and videos

- <https://techzone.vmware.com/mastering-unified-access-gateway#deploy>

Monitoring and Logs

Monitor services from the Admin UI



Log Files

- Default log level is INFO

Export from Admin UI or

- <https://uag.domain.com:9443/rest/v1/monitor/support-archive>

Downloads a zip file of multiple logs

Service Logs	Appliance Logs
<ul style="list-style-type: none">• appliance-agent.log• authbroker.log• bsg.log• esmanager.log• haproxy.conf• proxy.log• psg.log• securityGateway_*.log• tunnel.log• utserver.log• vpnd.log	<ul style="list-style-type: none">• UAG Config• Linux logs

Register UAGs in Horizon Console

Name should match UAG Name

- Not necessarily the same as the appliance name or DNS name

The screenshot shows the VMware Horizon Console interface. On the left is a navigation pane with options like Sessions, Problem vCenter VMs, Problem RDS Hosts, Events, System Health, Monitor, Dashboard, Events, Sessions, Help Desk, Users and Groups, Inventory, Desktops, Applications, Farms, Machines, Settings, and Servers. The main area is titled 'Servers' and has tabs for 'vCenter Servers', 'Gateways', and 'Connection Servers'. The 'Gateways' tab is active, showing a table of registered gateways. Below the table are 'Register' and 'Unregister' buttons. A 'Components' dialog box is open in the foreground, showing a list of components with a count of 1.

Gateway	Version	IP Address	Location
s1huag1.vmweuc.com	21.06	172.16.74.80	External
s1huag2.vmweuc.com	21.06	172.16.74.81	External
s1huag3.vmweuc.com	21.06	172.16.74.82	External
s1huag4.vmweuc.com	21.06	172.16.74.83	External

Status	ID	Version	IP Address	Location	Type
✓	s1huag1.vmweuc.com	21.06	172.16.74.80	External	Unified Access Gat.
✓	s1huag2.vmweuc.com	21.06	172.16.74.81	External	Unified Access Gat.
✓	s1huag3.vmweuc.com	21.06	172.16.74.82	External	Unified Access Gat.
✓	s1huag4.vmweuc.com	21.06	172.16.74.83	External	Unified Access Gat.
✓	s1huag5.vmweuc.com	21.06	172.16.74.84	External	Unified Access Gat.

Can be set in the UAG Console

The screenshot shows the 'System Configuration' window in the UAG Console. It has two input fields: 'UAG Name' and 'Locale *'. The 'UAG Name' field is highlighted with a red box and contains the value 's1huag1.vmweuc.com'. The 'Locale' field is set to 'en_US'.

Or as **UAGName** parameter in PowerShell INI file

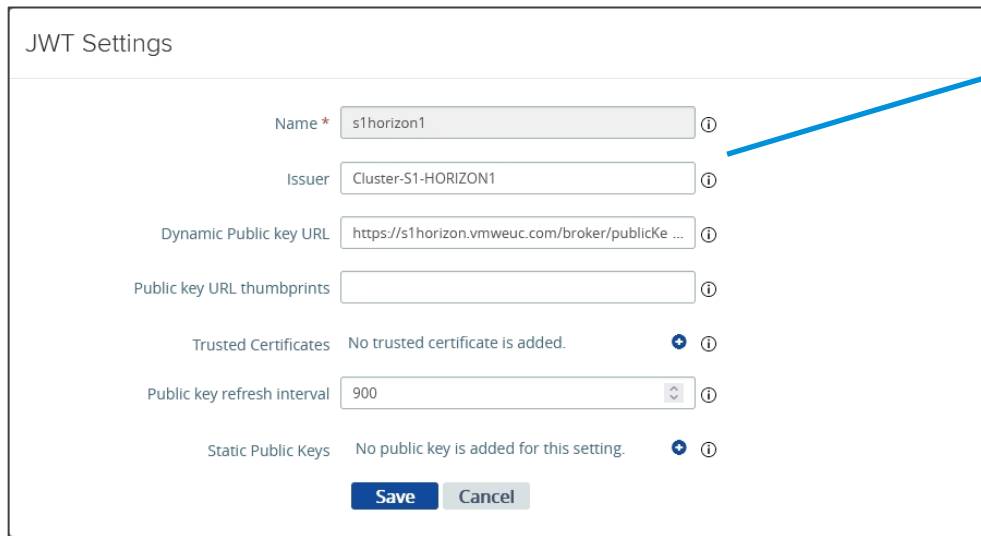
```
s1huag1 - Notepad
File Edit Format View Help
[General]
#
# UAG virtual appliance unique name (between 1 and 32 characters).
# If name is not specified, the script will prompt for it.
#
name=s1huag1
uagName=s1huag1.vmweuc.com
adminPasswordExpirationDays=365
#
```

Universal Broker Integration

<https://techzone.vmware.com/resource/horizon-configuration#universal-broker-configuration>

JWT (JSON Web Token) settings required on Unified Access Gateways

Issuer = Horizon pod cluster name



JWT Settings

Name * ⓘ

Issuer ⓘ

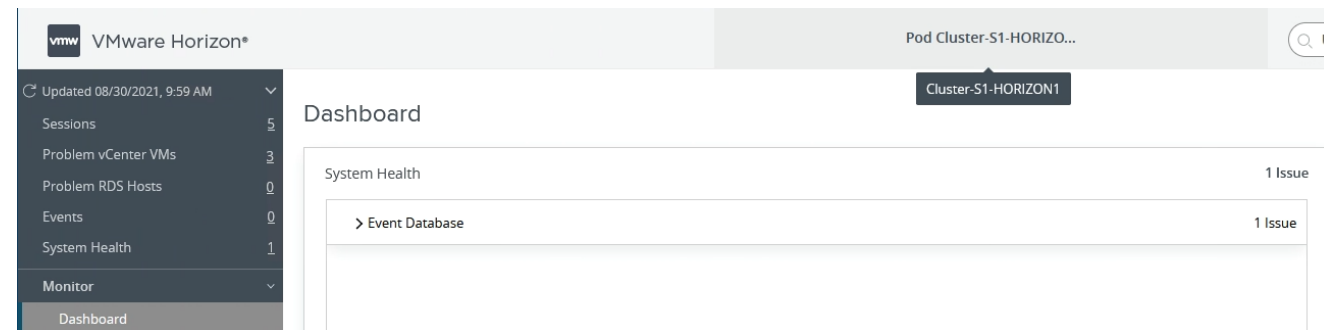
Dynamic Public key URL ⓘ

Public key URL thumbprints ⓘ

Trusted Certificates No trusted certificate is added. ⓘ

Public key refresh interval ⓘ

Static Public Keys No public key is added for this setting. ⓘ



Workspace ONE Access

Integration and Troubleshooting



Workspace ONE Access Integration

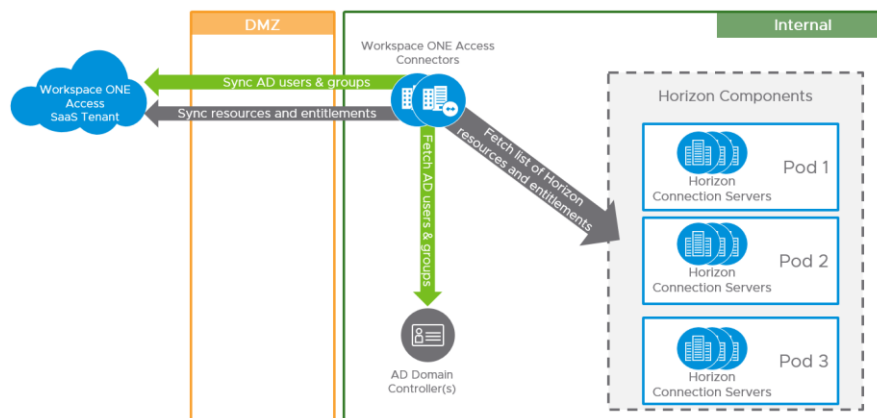
<https://techzone.vmware.com/resource/platform-integration#horizon-and-workspace-one-access-integration>

Desktop and app entitlements not syncing

- Time sync
- Timing issues

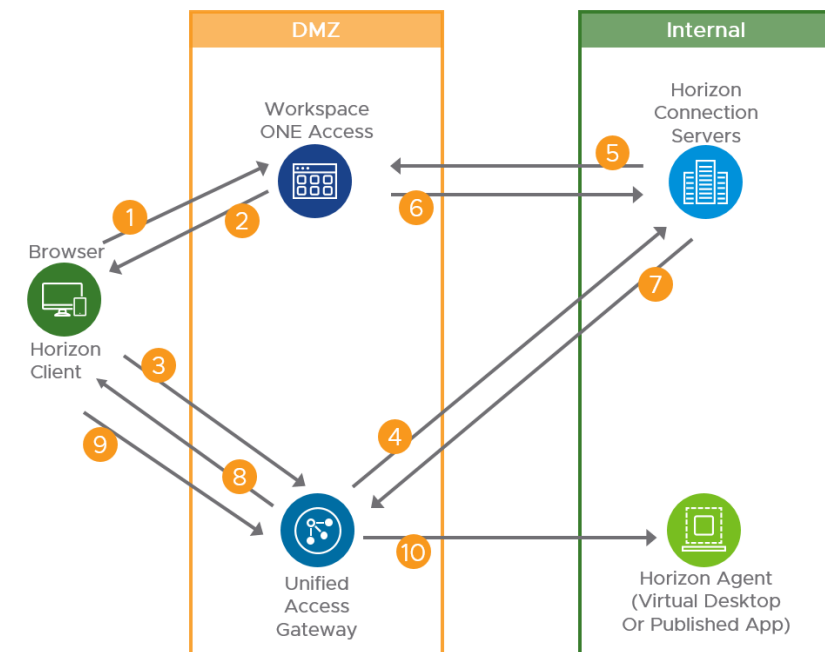
Active Directory sync issues

- Safeguards will require manual intervention for first time sync
- And/or when making large changes
- Anything that exceeds thresholds



Resource launch fails

- Wrong Client Access FQDN
- Time sync
- SAML metadata on Connection Server expired after last sync



True SSO

Enrollment Server Architecture

Separate server and role

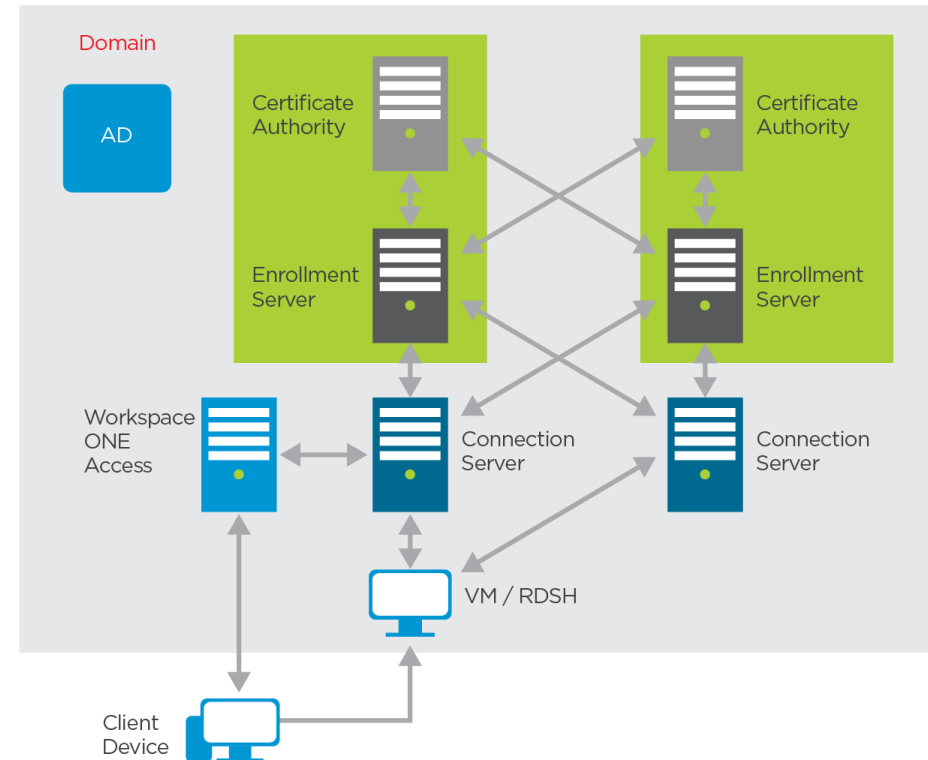
- Not supported on a Domain Controller
- Cannot be co-located with Horizon Connection Server
- Can co-locate on Certificate Authority (CA) Server

Resilience per Pod

- Deploy two Enrollment servers
 - Primary / Failover or internal load balance (round robin)
- Deploy two Certificate Authority servers

Networking

- Requires IPv4 static IP address
- True SSO Channel (TCP 32111) between Enrollment Server & Broker



Common Problems

<https://techzone.vmware.com/resource/horizon-configuration#setting-up-true-sso>

Pairing Issues between Enrollment Server and Broker

- Look for errors for “CERTSSL” in Connection Server and Enrollment Server logs
- Most common error involves around CS/Cluster certificate not being copied to the Enrollment Server

Certificate Template not setup properly

- Template security settings doesn't have Enroll permissions for the Enrollment Server
- Certificate expired

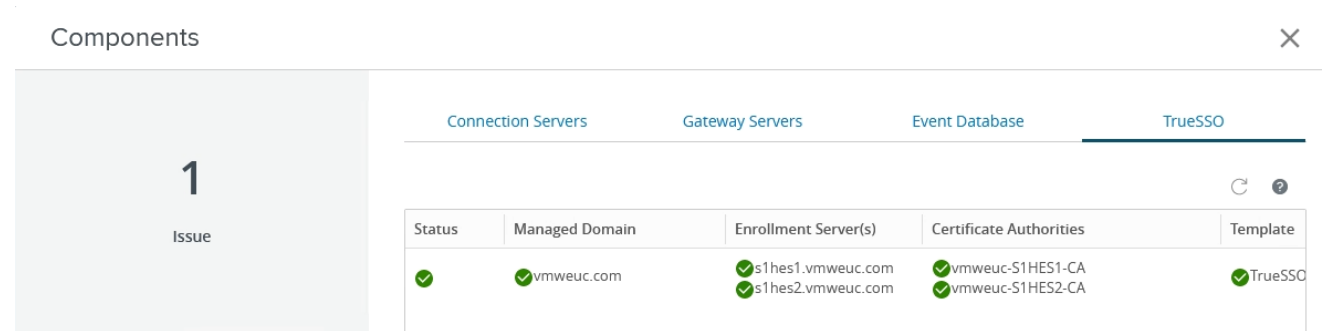
Enrollment Agent (Computer) Certificate Template not issued to Enrollment Server

No “True SSO” entry in dashboard

- Connector is not configured or not setup properly
- Or Connection Server cannot connect to the Enrollment Server

Troubleshooting and Log Files

Horizon Dashboard contains information on configuration errors



The screenshot shows the 'Components' window in the Horizon Dashboard. On the left, a grey box displays '1 Issue'. The main area has tabs for 'Connection Servers', 'Gateway Servers', 'Event Database', and 'TrueSSO'. The 'TrueSSO' tab is active, showing a table with the following data:

Status	Managed Domain	Enrollment Server(s)	Certificate Authorities	Template
✓	✓vmweuc.com	✓s1hes1.vmweuc.com ✓s1hes2.vmweuc.com	✓vmweuc-S1HES1-CA ✓vmweuc-S1HES2-CA	✓TrueSSO

True SSO Diagnostic Utility

Log files: Usual debug log files on Agent, Connection Server and Enrollment Server

- Path: `%PROGRAMDATA%\VMware\VDM\logs\debug-xxxxxx.txt`

Keywords in logfiles:

- Agent: certlogon, startSession, CertSso, CERTIFICATESSOID
- Connection Server: CertSso:, CERTSSL, startSession

vmware® DIGITAL WORKSPACE
TECH ZONE

techzone.vmware.com

Your Fastest Path to Understanding,
Evaluating and Deploying VMware Products

Other Tech Zone Sites

go.techzone.vmware.com

CARBON BLACK
TECH ZONE

carbonblack.vmware.com

THE CLOUD PLATFORM
TECH ZONE

core.vmware.com

NETWORKING AND
SECURITY TECH ZONE

nsx.techzone.vmware.com

VMWARE CLOUD
TECH ZONE

vmc.techzone.vmware.com

vmware®



vmworld®
IMAGINE
that



Thank you!

vmworld[®]

IMAGINE
that

Additional Material

Extra slides and information that we couldn't fit into the actual session

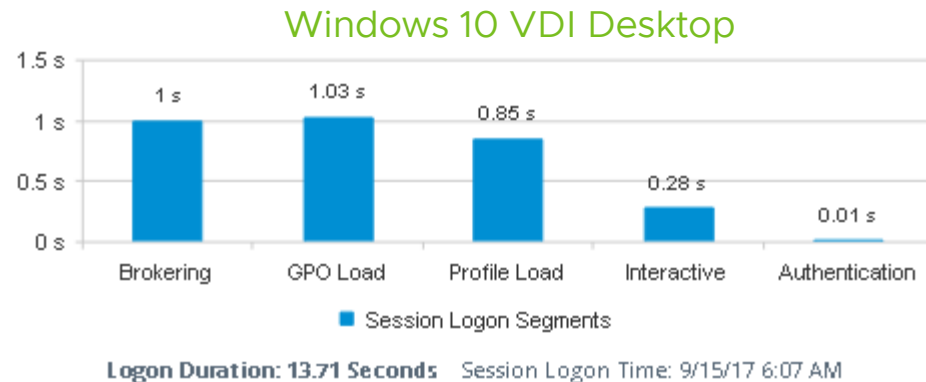
Horizon

Additional Material

Session Logon Segments

Logon Duration

- Calculated from the time the user clicks the desktop or app pool to the time when Windows Explorer starts



Brokering

- Total time for Connection Server to process a session connect or reconnect

GPO load

- Total time for Windows group policy processing

Profile load

- Total time for Windows user profile processing

Interactive

- Total time for Horizon Agent to process a session connect or reconnect

Authentication

- Total time for Connection Server to authenticate the session

Desktop Not Available

What to look for...

Broker starts session on VM

- [DesktopSessionImp] (SESSION:7072-***-a79c) startSession – sending StartSession message

Agent responds...

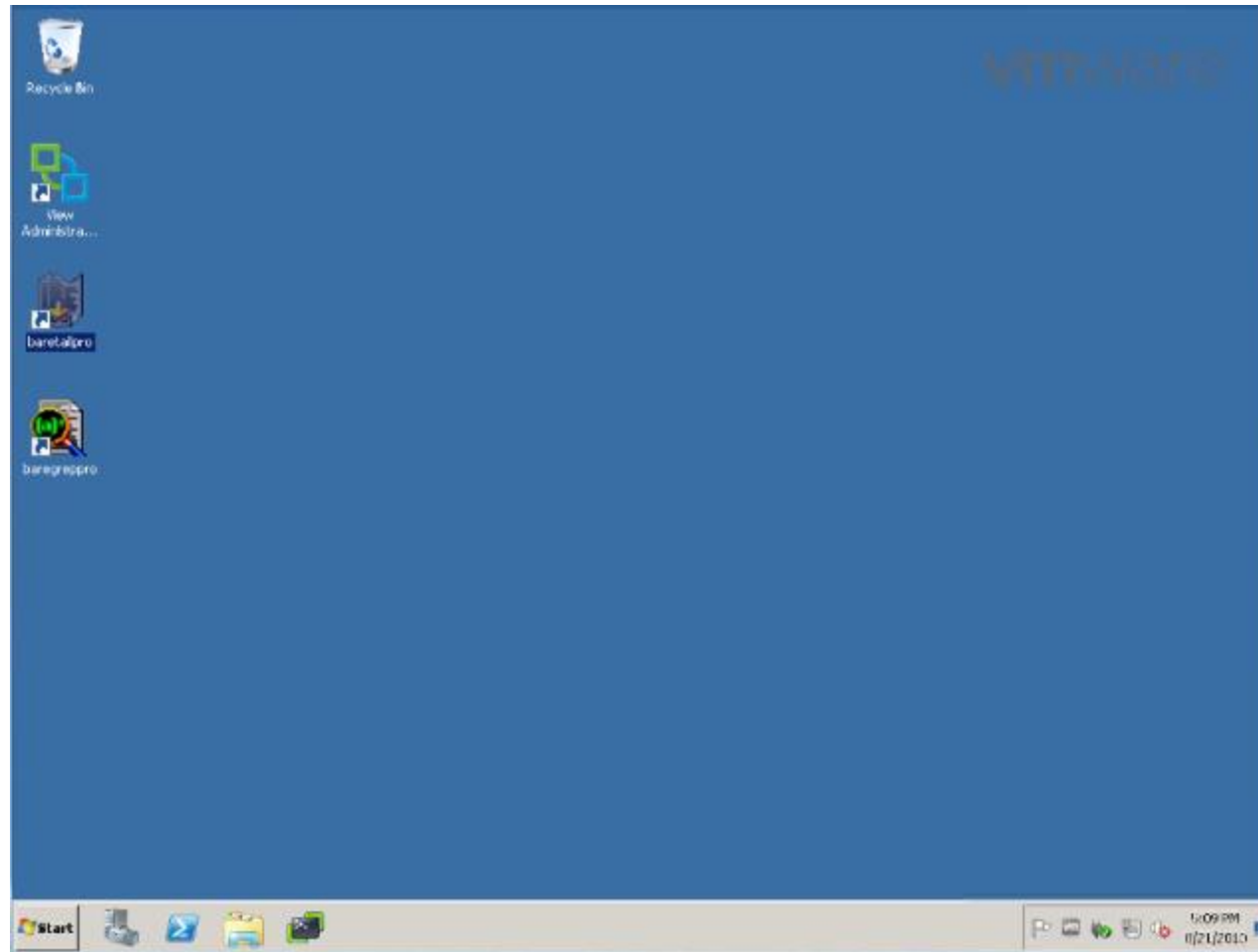
- "DesktopManager got a StartSession message"
- Client Info should be in Agent Log along with PCoIP launch

Event Database: AGENT_PENDING

Client connects to VM (Agent)

- "PCoIPCnx::OnConnectionComplete Begin (PCOIP)"
- "WTS_SESSION_LOGON"
- Event Database: AGENT_CONNECTED

Demo – Log Monitoring with BareTail/BareGrep



Horizon Connectivity Issues

Where to look

- Connection Broker logs - *C:\ProgramData\VMware\VDM\logs*
- Event Database
- Data Collection Tool (DCT Bundle)

What to look for

- (Client connects) [SimpleAJPService] (ajp:broker:Request9) Request from /192.168.2.1: POST /broker/xml
- (Broker authentication) [WinAuthFilter] (SESSION:7072-***-a79c mattc) Attempting to authenticate user 'mattc' in domain 'FUTUREOFFICE'
- (User has authenticated to Broker) [AuthorizationFilter] (SESSION:7072-***-a79c) User FUTUREOFFICE\mattc has successfully authenticated to VDM
- (Audit Entry) [Audit] (SESSION:7072-***-a79c) BROKER_LOGON:USER:FUTUREOFFICE\mattc;USERSID:S-1-5-21-326850759-2560684469-1780228732-1113;USERDN:CN=S-1-5-21-326850759-2560684469-1780228732-1113,CN=ForeignSecurityPrincipals,DC=vdi,DC=vmware,DC=int;
- Event Database: BROKER_USERLOGGEDIN

User Experience Issues

Black screen of death

- Protocol ports blocked
- Protocol incorrectly routed
- SVGA driver issue
- Insufficient vRAM

Poor quality display

- Bandwidth, latency, or QoS
- Pcoip_server logs report
 - *VGMAC :Stat frms: Loss=0.45%/0.21% (R/T)*
 - *MGMT_PCOIP_DATA :BW: Decrease (loss) old = 234.9982 new = 176.8438*

Randomly disconnected session

- 15 min after established
 - wssm process hasn't started on desktop
- Agent logs (<DriveLetter>:\ProgramData\VMware\VDM\logs)
 - PENDING_EXPIRED
- Sometimes caused by daisy-chaining the GINA

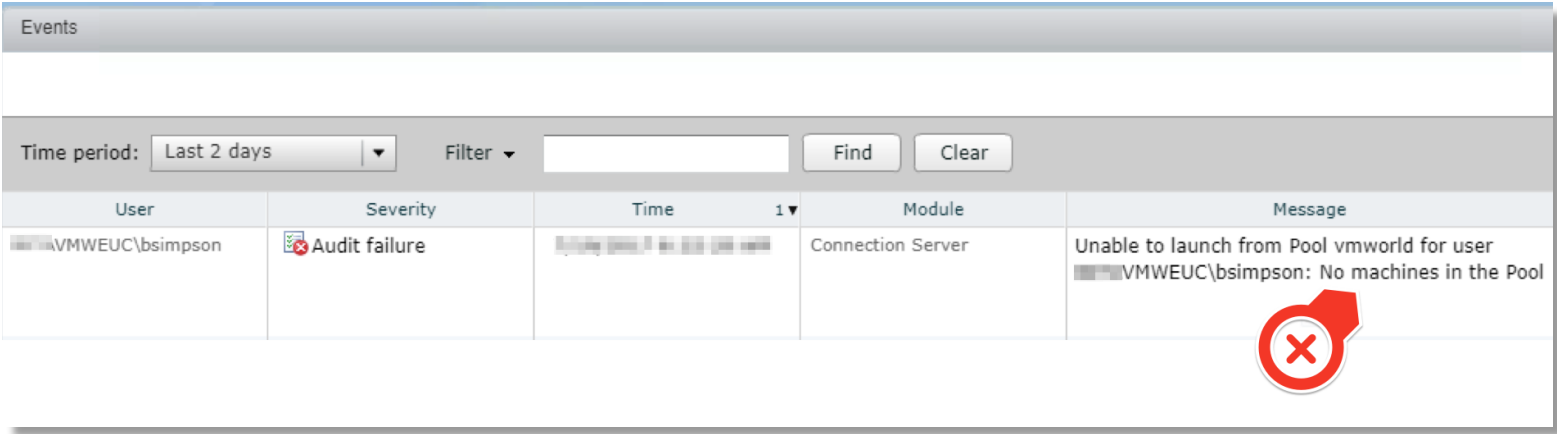
<https://techzone.vmware.com/resource/blast-extreme-display-protocol-vmware-horizon-7>

Desktop Source Not Available

Where to look

Event database

Connection server logs



Events				
Time period: Last 2 days Filter Find Clear				
User	Severity	Time	Module	Message
VMWEUC\bsimpson	Audit failure		Connection Server	Unable to launch from Pool vmworld for user VMWEUC\bsimpson: No machines in the Pool

What to look for

[SessionLaunchContext] (SESSION:40a7_***_6cbd) VMWEUC\bsimpson, Desktop=vmworld: Session request failed.

(SESSION:40a7_***_6cbd) [VMWEUC\bsimpson, Desktop=vmworld] (5ms): The following servers were blocked for new sessions: [cn=5162cf76-8d8a-4ac0-9185-845a540d24e5,ou=servers,dc=vdi,dc=vmware,dc=int]

(SESSION:40a7_***_6cbd) [VMWEUC\bsimpson, Desktop=vmworld] (5ms): Application launch failed, exception was: The desktop sources for this desktop are not responding. Please try again later.

Desktop Not Available

What to look for... - walk through successful connection

Client requests desktop

- Event Database: BROKER_DESKTOP_REQUEST

Broker allocates session to user

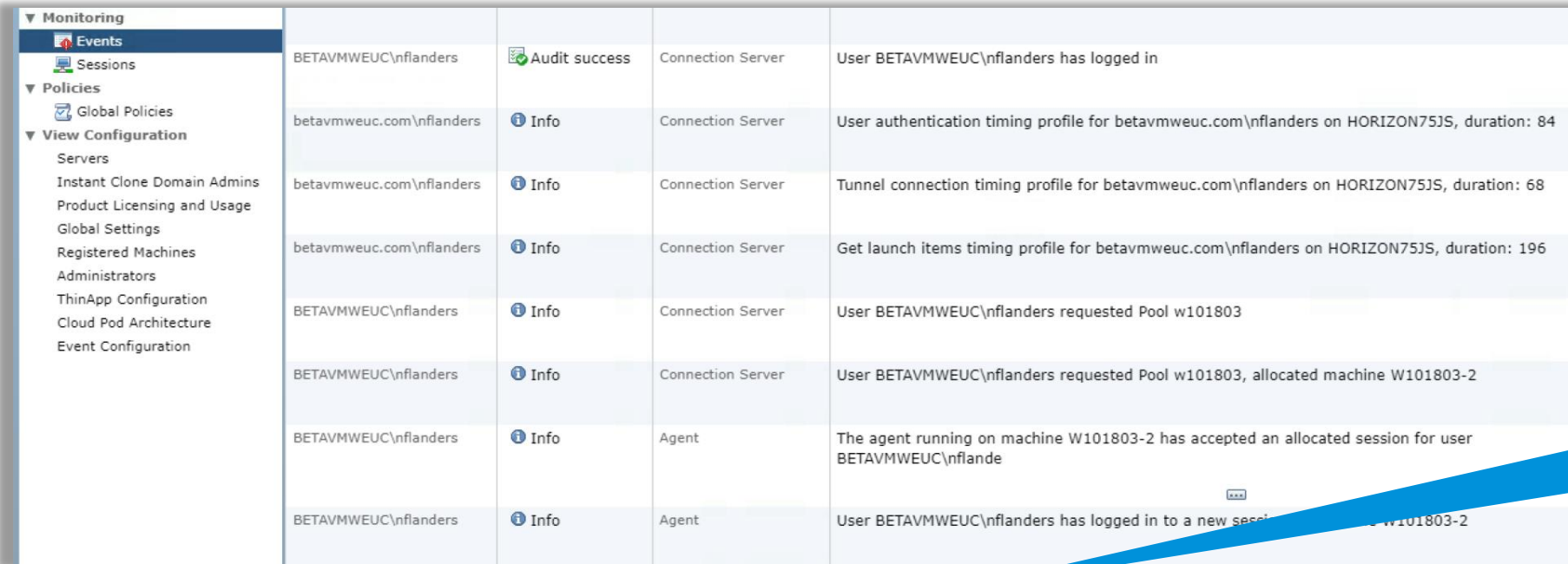
- *[FarmImp] (SESSION:7072-***-a79c) cn=3f974017-409f-4912-83bc-2ee794f22fab,ou=servers,dc=vdi,dc=vmware,dc=int, total session count: 0*
- *[FarmImp] (SESSION:7072-***-a79c) allocateNewSession - identified server for application CN=GOLD-NP,OU=Applications,DC=vdi,DC=vmware,DC=int*
- Event Database: BROKER_MACHINE_ALLOCATED

Broker attempts SSO

- *[FarmImp] (SESSION:7072-***-a79c) Using domain for SSO: FUTUREOFFICE***
- User won't be logged on to the VM without this!

Desktop Not Available

What to look for... - walk through successful connection



▼ Monitoring				
Events	BETAVMWEUC\nflanders	Audit success	Connection Server	User BETAVMWEUC\nflanders has logged in
Sessions				
▼ Policies				
Global Policies				
▼ View Configuration				
Servers	betavmweuc.com\nflanders	Info	Connection Server	User authentication timing profile for betavmweuc.com\nflanders on HORIZON75JS, duration: 84
Instant Clone Domain Admins	betavmweuc.com\nflanders	Info	Connection Server	Tunnel connection timing profile for betavmweuc.com\nflanders on HORIZON75JS, duration: 68
Product Licensing and Usage	betavmweuc.com\nflanders	Info	Connection Server	Get launch items timing profile for betavmweuc.com\nflanders on HORIZON75JS, duration: 196
Global Settings				
Registered Machines	BETAVMWEUC\nflanders	Info	Connection Server	User BETAVMWEUC\nflanders requested Pool w101803
Administrators	BETAVMWEUC\nflanders	Info	Connection Server	User BETAVMWEUC\nflanders requested Pool w101803, allocated machine W101803-2
ThinApp Configuration	BETAVMWEUC\nflanders	Info	Agent	The agent running on machine W101803-2 has accepted an allocated session for user BETAVMWEUC\nflande
Cloud Pod Architecture				
Event Configuration	BETAVMWEUC\nflanders	Info	Agent	User BETAVMWEUC\nflanders has logged in to a new session on W101803-2

Active Directory
objectSid
for user account

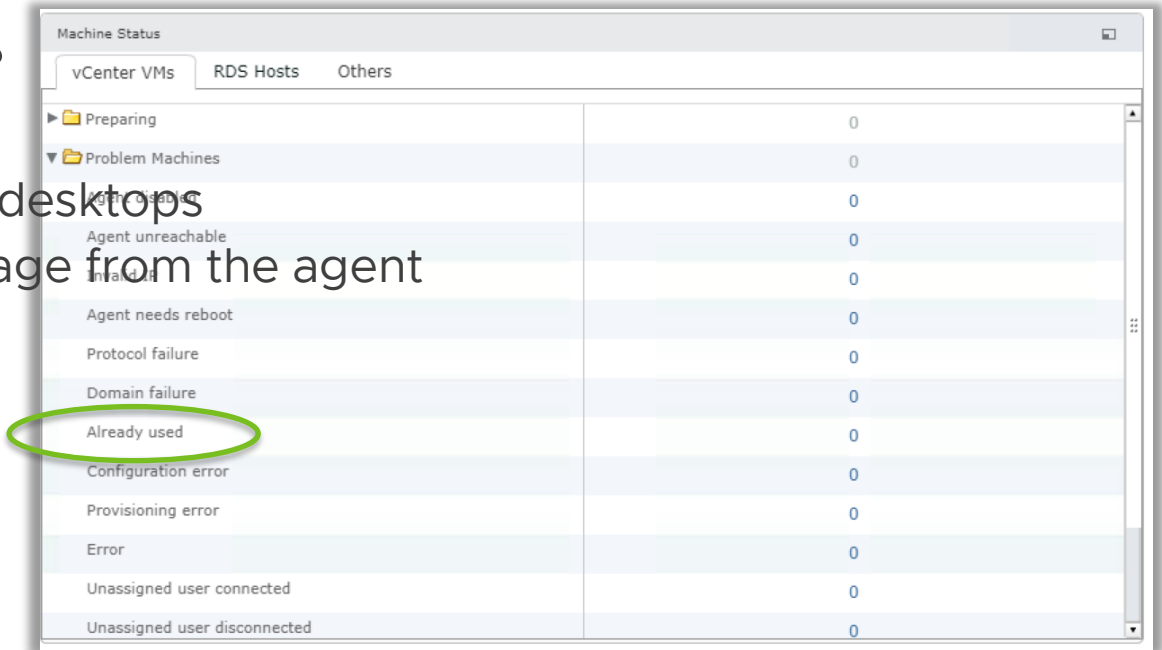
[FarmImp] (SESSION:ceca_***_c2c9) getSessionForApplication, userDn: CN=S-1-5-21-XYZ,CN=ForeignSecurityPrincipals,DC=vdi,DC=vmware,DC=int
[FarmImp] (SESSION:ceca_***_c2c9) Found 0 existing user sessions for userDn: CN=S-1-5-21-XYZ,CN=ForeignSecurityPrincipals,DC=vdi,DC=vmware,DC=int
[FarmImp] (SESSION:ceca_***_c2c9) Creating new session for launch item cn=w101803,ou=applications,dc=vdi,dc=vmware,dc=int from pool cn=w101803,ou=server groups,dc=vdi,dc=vmware,dc=int for userDn: CN=S-1-5-21-XYZ,CN=ForeignSecurityPrincipals,DC=vdi,DC=vmware,DC=int
[FarmImp] (SESSION:ceca_***_c2c9) Selecting server from single session machines for userDn: CN=S-1-5-21-XYZ,CN=ForeignSecurityPrincipals,DC=vdi,DC=vmware,DC=int
[FarmImp] (SESSION:ceca_***_c2c9) allocateNewSession - identified server for launch item cn=w101803,ou=applications,dc=vdi,dc=vmware,dc=int from pool cn=w101803,ou=server groups,dc=vdi,dc=vmware,dc=int for userDn: CN=S-1-5-21-XYZ,CN=ForeignSecurityPrincipals,DC=vdi,DC=vmware,DC=int

Desktop Not Available

What to look for...

Desktop not available due to VM reset/crash?

- Check Desktop status – ALREADY USED
- Typical on refresh-on-logout or delete-on-use desktops
- Broker never received an explicit logout message from the agent
- Missing AGENT_ENDED event in DB for VM



Machine Status	
vCenter VMs	RDS Hosts Others
Preparing	0
Problem Machines	0
Agent unreachable	0
Invalid	0
Agent needs reboot	0
Protocol failure	0
Domain failure	0
Already used	0
Configuration error	0
Provisioning error	0
Error	0
Unassigned user connected	0
Unassigned user disconnected	0

View Composer Issues associated with incorrect domain credentials

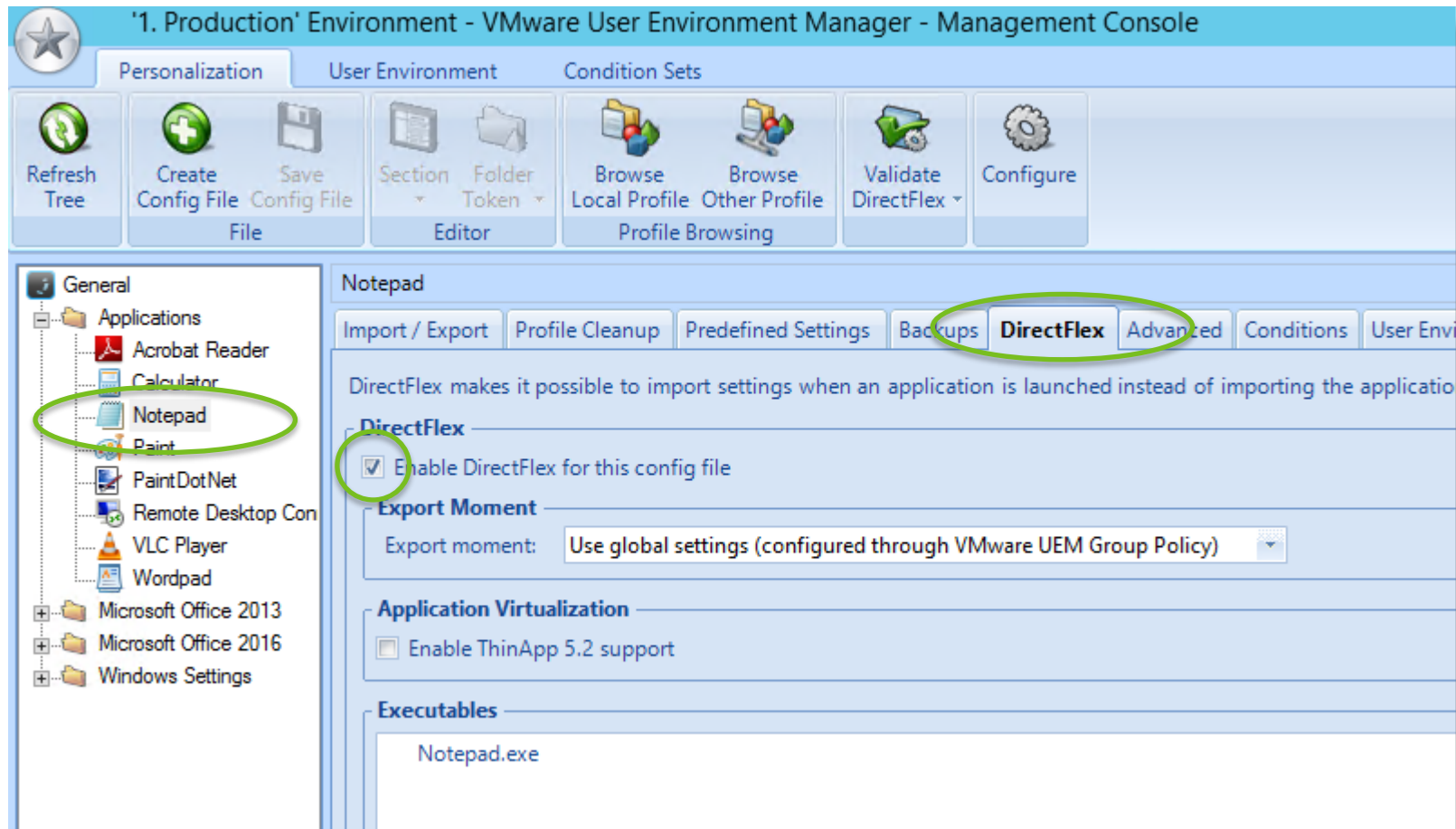
- *C:\ProgramData\VMware\View Composer\Logs*
- *FATAL CSvmGaService - [svmGaService.cpp, 116] Domain join failed Error 5 (0x5): Access is denied.*

<https://kb.vmware.com/s/article/1000590>

Dynamic Environment Manager

Additional Material

DirectFlex Logging



DirectFlex Export

Directflex Export

```
2017-05-31 14:13:50.362 [INFO] Performing DirectFlex export for config file '\\VMW-FS1\Config Files$\General\Applications\Notepad.INI' [TFP#1a66475f-b07538>>]  
2017-05-31 14:13:50.362 [INFO] Exporting profile archive for config file '\\VMW-FS1\Config Files$\General\Applications\Notepad.INI' [TFP#1a66475f-b07538>>  
2017-05-31 14:13:50.363 [DEBUG] User: VMWARE\rwiesemann, Computer: WMV-CRINT1, OS: x64-win7 (BuildNumber 7601, ServicePack 1, SuiteMask 100, ProductType 1/4, Lang  
0409, IE 8.0.7601.17514, UEM 9.2.0.701, ProcInfo 1/2/4/4, UTC+02:00D), PTS: 3044/2872/3  
2017-05-31 14:13:50.363 [DEBUG] Using profile archive '\\VMW-FS1\Userdata$\rwiesemann\Archives\Applications\Notepad.zip'  
2017-05-31 14:13:50.363 [DEBUG] Triggered by 'C:\Windows\System32\notepad.exe'  
2017-05-31 14:13:50.364 [INFO] Exporting profile using config file 'Notepad.INI' (\\VMW-FS1\Config Files$\General\Applications\Notepad.INI)  
2017-05-31 14:13:50.364 [INFO] Binary Settings: Applied Application Template 'Microsoft Notepad'  
2017-05-31 14:13:50.365 [INFO] Exporting Registry information  
2017-05-31 14:13:50.365 [DEBUG] ExportRegistry: Exporting tree 'HKCU\Software\Microsofft\Notepad'  
2017-05-31 14:13:50.365 [INFO] Exported Registry information successfully  
2017-05-31 14:13:50.365 [DEBUG] Stored 1 entry in profile archive (size: 788; compressed: 267)  
2017-05-31 14:13:50.366 [DEBUG] Backing up '\\VMW-FS1\Userdata$\rwiesemann\Archives\Applications\Notepad.zip' to '\\VMW-FS1\Userdata$\rwiesemann\Backups\Applications  
v \Notepad 2017-05-22 132012.zip'  
2017-05-31 14:13:50 Completed DirectFlex export (9 ms) [<<IFP#1a66475f-b07538]
```


Path-Based Import Runs Slow

Be careful not to run FlexEngine as a logon script *and* a Group Policy client-side extension.

```
2017-05-31 15:13:38.678 [INFO ] Starting FlexEngine v9.2.0.701 [IFP#02e9d2df-27018bd>>]
2017-05-31 15:13:38.678 [DEBUG] Running as child of process #3312
2017-05-31 15:13:38.678 [DEBUG] Performing path-based import
2017-05-31 15:13:38.678 [DEBUG] User: VMWARE\rwiesemann, Computer: VMW-CLIENT1, OS: x64-win7 (BuildNumber 7601, ServicePack 1, SuiteMask 100, ProductType 1/4, Lang
0409, IE 8.0.7601.17514, UEM 9.2.0.701, ProcInfo 1/2/4/4, UTC+02:00), PTS: 3320/3900/5
2017-05-31 15:13:38.678 [DEBUG] Profile state: local (0x00000204)
2017-05-31 15:13:38.678 [DEBUG] Recursively processing config files from path '\\VMW-FS1\Config Files$\General'
2017-05-31 15:13:38.678 [DEBUG] Using profile archive path '\\VMW-FS1\Userdata$\rwiesemann\Archives'
2017-05-31 15:13:38.678 [DEBUG] Logging to file '\\VMW-FS1\Userdata$\rwiesemann\Logs\Flexengine.log'
2017-05-31 15:13:38.678 [DEBUG] Log file will be overwritten when larger than 512 kilobytes
2017-05-31 15:13:38.678 [DEBUG] Support for removing local profile at logoff is enabled
```

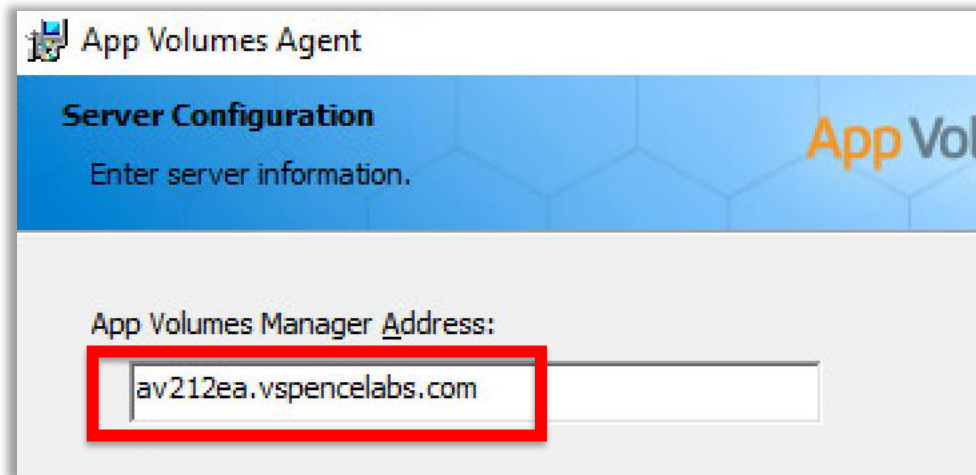
2017-05-31 15:13:38.678 [WARN] Found import status flag. This does not necessarily indicate a problem, but be careful not to accidentally run FlexEngine multiple times (for instance both as a Group Policy client-side extension and from a logon script).

App Volumes

Additional Material

Avoiding Certificate Issues

Be Consistent with App Volumes Manager Name



App Volumes Agent

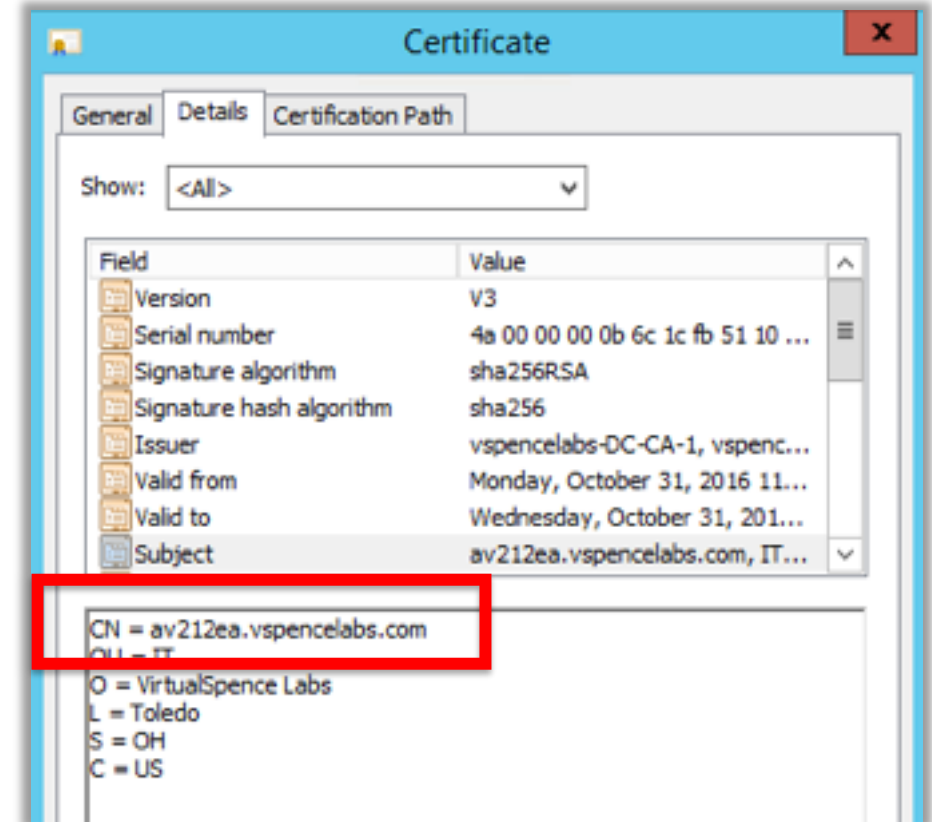
Server Configuration

Enter server information.

App Volumes Manager Address:

av212ea.vspencelabs.com

Name	Type	Data
(Default)	REG_SZ	(value not set)
EnforceSSLCertificateValidation	REG_DWORD	0x00000001 (1)
Hypervisor	REG_SZ	vcenter
Manager1	REG_SZ	av212ea.vspencelabs.com:443
RebootAfterDetach	REG_DWORD	0x00000000 (0)
SSL	REG_DWORD	0x00000001 (1)
VolAttachMessageOn	REG_DWORD	0x00000000 (0)



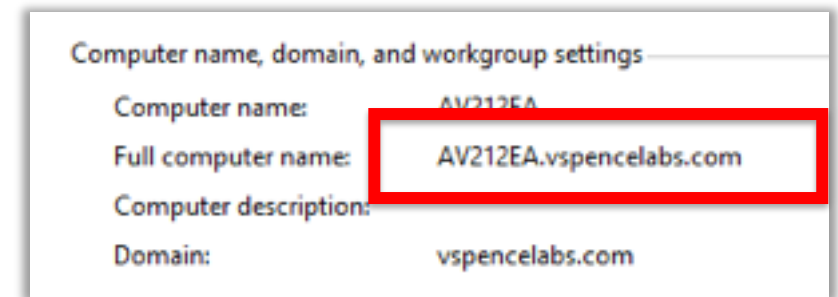
Certificate

General Details Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	4a 00 00 00 0b 6c 1c fb 51 10 ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	vspencelabs-DC-CA-1, vspenc...
Valid from	Monday, October 31, 2016 11...
Valid to	Wednesday, October 31, 201...
Subject	av212ea.vspencelabs.com, IT...

CN = av212ea.vspencelabs.com
OU = IT
O = VirtualSpence Labs
L = Toledo
S = OH
C = US



Computer name, domain, and workgroup settings

Computer name: AV212EA

Full computer name: AV212EA.vspencelabs.com

Computer description:

Domain: vspencelabs.com

AppStack Not Attaching at Logon

One host in vSphere cluster does not have access to the shared datastore where the AppStack resides

- Common oversight, especially with Storage Groups

Conflicting Minifilter driver

- DLP software
- Be aware of app altitude
- More info from Microsoft:
 - <https://docs.microsoft.com/en-us/windows-hardware/drivers/ifs/load-order-groups-and-altitudes-for-minifilter-drivers>

OS Compatibility

```
gvc-desktops.betavmware.com"
P3312R2864 INFO RvSphere: Attaching read-only volume "[t3600-01-Beta-VDI-2-2] cloudvolumes213EA/apps/VLC
P3312R2864 INFO RvSphere: Preparing to reconfigure VM vmworld-4" (503aeee7-5138-6ef9-3f4e-393245d15e64)
P3312R2864 INFO RvSphere: ReconfigVM_Task task: task-10827
P3312R2864 INFO RvSphere: Task total time: 0.330568s (execut 0.32532s)
P3312R2864 INFO RvSphere: vCenter operation failed: File
526a246-f3cf-14feb50cefc5/cloudvolumes213EA/apps/VLC.vmdk was not found
P3312R2864 ERROR RvSphere: Failed to reconfigure VM "vmworld-4" (503aeee7-5138-6ef9-3f4e-393245d15e64):
tFound)
P3312R2864 INFO Cvo: Incrementing unmount count for volume #2, now 1
P3312R2864 INFO Cvo: Unsuccessful mount result appended to response: Volumes were not mounted due t
```

```
C:\Windows\system32>fltmc
```

Filter Name	Num Instances	Altitude	Frame
immflex	4	385910	0
vsepflt	4	328200	0
WdFilter	4	328010	0
storqosflt	0	244000	0
svdriver	2	190000	0
FileCrypt	0	141100	0
luafv	1	135000	0
npsvcrtig	1	46000	0
FileInfo	4	45000	0
Wof	3	40700	0

Operating Systems:

<input type="checkbox"/> Windows 7 (x64)	<input type="checkbox"/> Windows 7 (x86)
<input type="checkbox"/> Windows 8 (x64)	<input type="checkbox"/> Windows 8 (x86)
<input type="checkbox"/> Windows 8.1 (x64)	<input type="checkbox"/> Windows 8.1 (x86)
<input type="checkbox"/> Windows 10 (x64)	<input type="checkbox"/> Windows 10 (x86)
<input type="checkbox"/> Windows Server 2008 (x64)	<input type="checkbox"/> Windows Server 2008 (x86)
<input type="checkbox"/> Windows Server 2008 R2 (x64)	
<input type="checkbox"/> Windows Server 2012 (x64)	
<input type="checkbox"/> Windows Server 2012 R2 (x64)	
<input checked="" type="checkbox"/> Windows Server 2016 (x64)	

8.3 Naming Convention on NTFS Partitions

Some customers disable 8.3 file naming as described here:

<https://support.microsoft.com/en-us/help/121007/how-to-disable-8-3-file-name-creation-on-ntfs-partitions>

If you have MS Office installed on the system volume, do not disable 8.3 file naming

“Some folders on the system volume retain their 8.3 names. These 8.3 names are saved in the registry by Office products during their installation and are often validated at program launch. If these 8.3 names are inconsistent with the 8.3 names on AppStacks or Writable Volumes, whether because the names differ or because some volumes have no 8.3 names, the validation fails and the program initiates reconfiguration.”



SSL Certificates and vCenter Server Connection

Accept vCenter Certificate

- By default, certificate validation is required between App Volumes Manager and vSphere
- Accept vCenter cert (self-signed or CA-signed) while creating the Machine Manager in App Volumes Manager
- No custom certificate work required

The screenshot displays the 'Machine Managers' configuration page in the App Volumes Manager interface. The top navigation bar includes 'DASHBOARD', 'VOLUMES', 'DIRECTORY', 'INFRASTRUCTURE', 'ACTIVITY', and 'CONFIGURATION'. The 'CONFIGURATION' tab is active, showing sub-tabs for 'License', 'Active Directories', 'Administrators', 'Machine Managers', and 'Storage'. The 'Machine Managers' sub-tab is selected, and an 'Add Machine Manager' button is visible. Below the sub-tabs, a message states: 'Add and configure in-guest services or leverage the performance of VMware vCenter Servers to deliver volumes.' A 'Show' dropdown is set to '10'. A table lists the machine managers with columns for 'Host', 'Username', and 'Type'. One entry is shown: 'vcsa.vspencelabs.com' with username 'vspencelabs\svc-horizon' and type 'VMware vCenter'. Below the table, a detailed view of the selected machine manager shows its type, hostname, and description. A green checkmark icon and a message indicate that the App Volumes manager is connected to the vCenter server with a manually accepted (trusted) certificate. The bottom of the page shows 'Showing 1 to 1 of 1 machine managers' and navigation links: 'First', 'Previous', '1', 'Next', 'Last'.

Host	Username	Type
vcsa.vspencelabs.com	vspencelabs\svc-horizon	VMware vCenter

Type: VMware vCenter
Hostname: vcsa.vspencelabs.com
Description: VMware vCenter Server 6.0.0 build-3634794

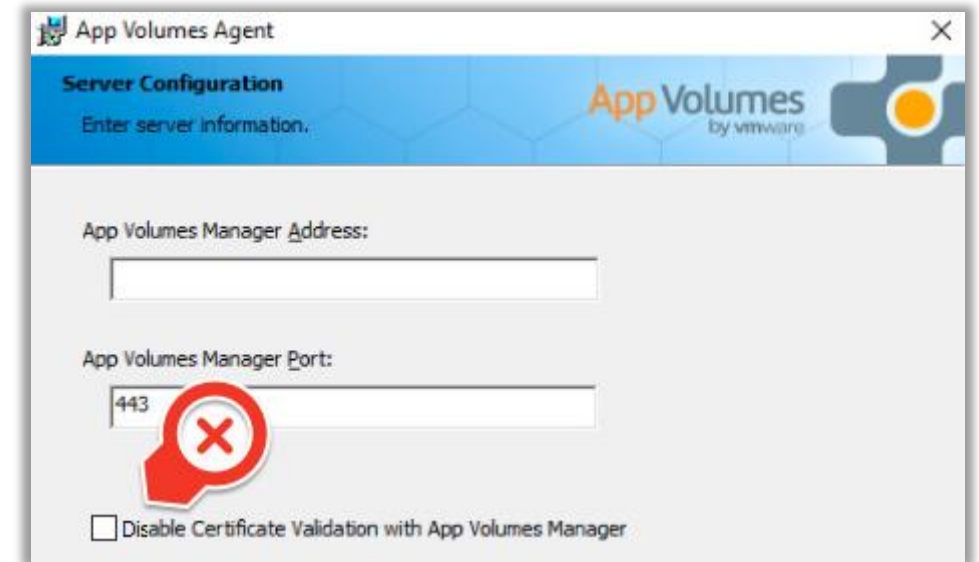
App Volumes manager connected to vcsa.vspencelabs.com with manually accepted (trusted) certificate.

Certificate Options for Production

Enable Certificate Validation on the App Volumes Agent








Options to Enable SSL

- SSL is enabled by default
- Don't disable certificate validation during Agent installation
- Enable SSL in the registry after App Volumes Agent install



HKLM\System\CurrentControlSet\Services\svservices\Parameters

- EnforceSSLCertificateValidation = 1
- SSL = 1

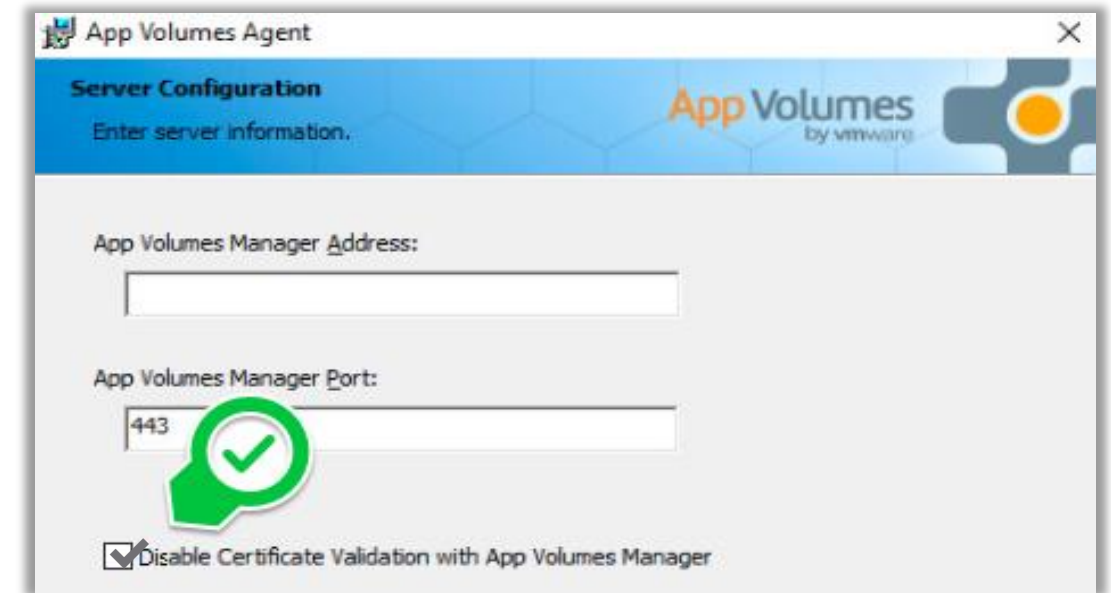
Name	Type	Data
 (Default)	REG_SZ	(value not set)
 EnforceSSLCertificateValidation	REG_DWORD	0x00000001 (1)
 Hypervisor	REG_SZ	vcenter
 Manager1	REG_SZ	10.10.10.1:443
 RebootAfterDetach	REG_DWORD	0x00000000 (0)
 SSL	REG_DWORD	0x00000001 (1)
 VolAttachMessageOn	REG_DWORD	0x00000000 (0)

Certificate Options for a POC

Disable SSL Certificate Validation on the Agent

Options to Disable SSL

- *Disable Certificate Validation with App Volumes Manager* during App Volumes Agent install
- *EnforceSSLCertificateValidation* in the registry after App Volumes Agent install



HKLM\System\CurrentControlSet\Services\svservices\Parameters

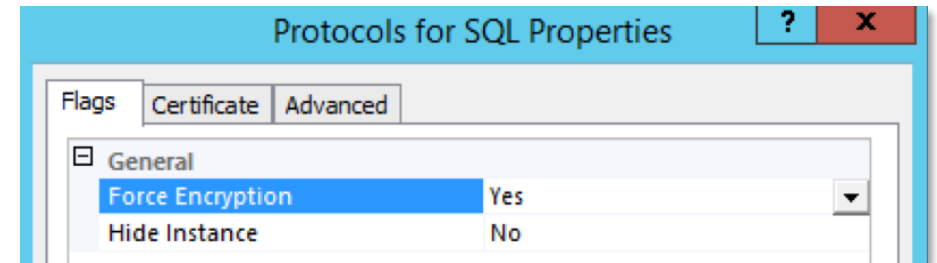
- EnforceSSLCertificateValidation = 0

Name	Type	Data
(Default)	REG_SZ	(value not set)
EnforceSSLCertificateValidation	REG_DWORD	0x00000000 (0)
Hypervisor	REG_SZ	vcenter
Manager1	REG_SZ	10.10.10.10:443
RebootAfterDetach	REG_DWORD	0x00000000 (0)
SSL	REG_DWORD	0x00000001 (1)
VolAttachMessageOn	REG_DWORD	0x00000000 (0)

SSL Certificates and SQL Server Communication

Securing Communications Between App Volumes Manager and SQL Server

- 2.12 User Guide references [MS Support](#)
 - Note the differences for a SQL Server clustered installation
- Encryption is configured on the SQL Server *instance*, so *all* databases on a shared SQL Server will be affected
- From the SQL Server, use SQL Server Configuration Manager to configure **Force Encryption** and specify the SQL certificate



SQL Server service account must have **Read** permissions to the **Private Key** of the SQL Server SSL certificate.

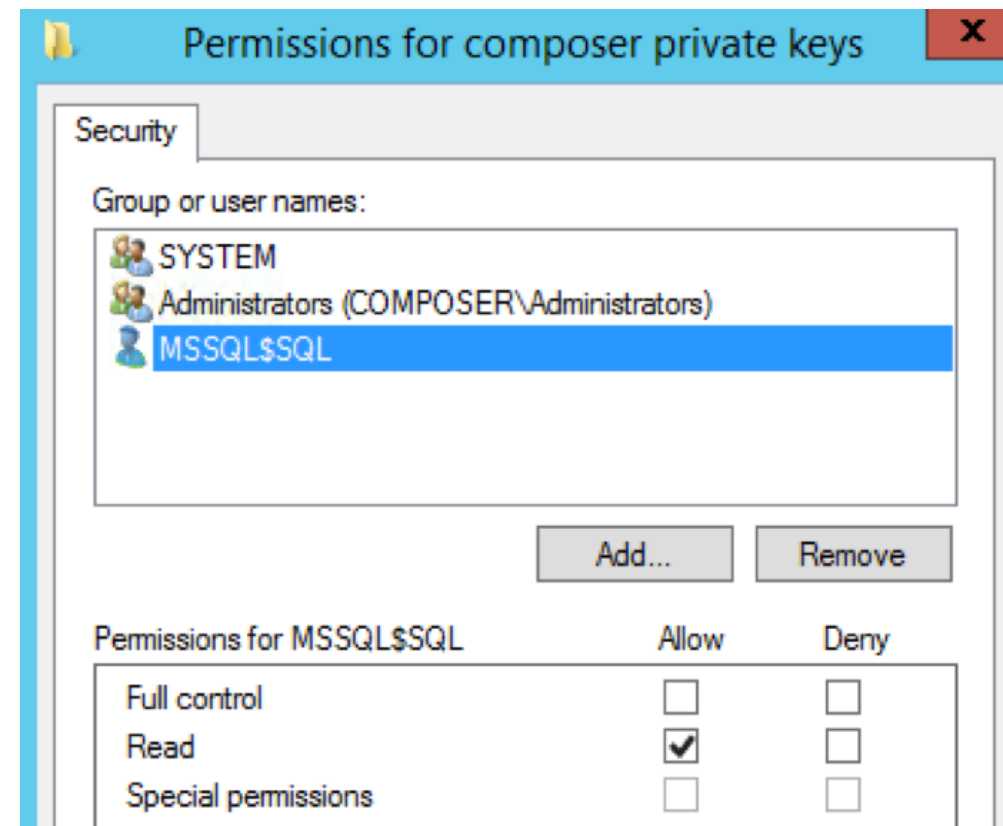
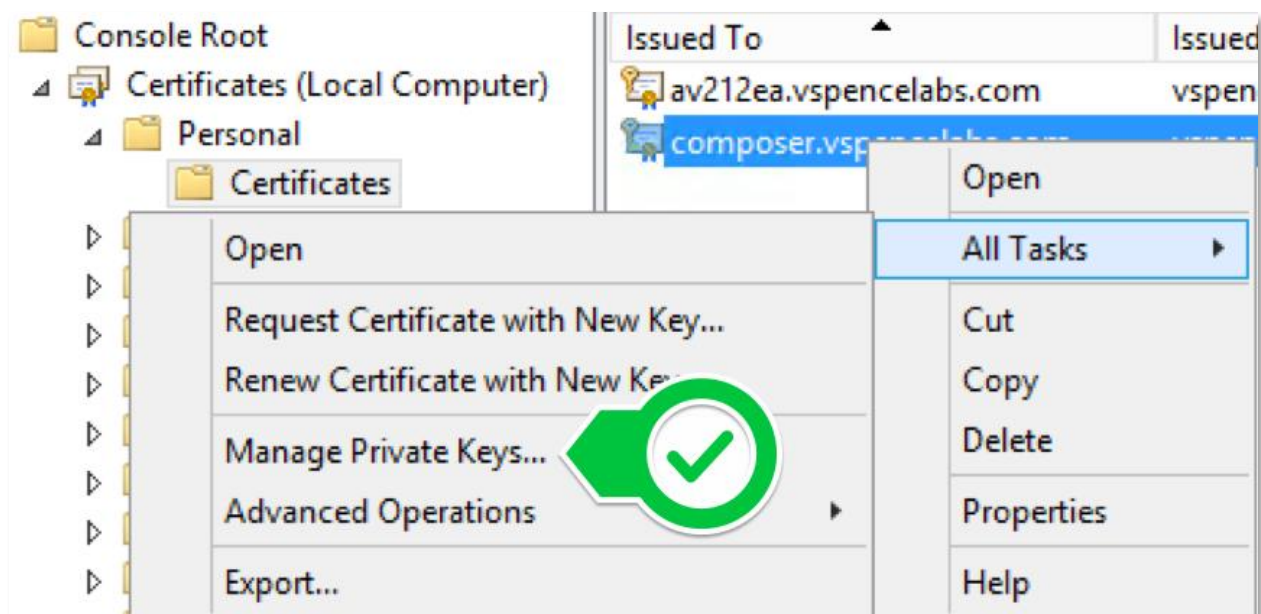
- Check SQL Server Configuration Manager > SQL Server Services > SQL Server (SQL) > Log On
- Default is **NT Service\MSSQL\$SQL** which does *not* have the necessary permissions.

SSL Certificates and SQL Server Communication

Setting Custom Private Key Permissions for SQL Service Account

Start on the SQL Server

MMC > Certificates



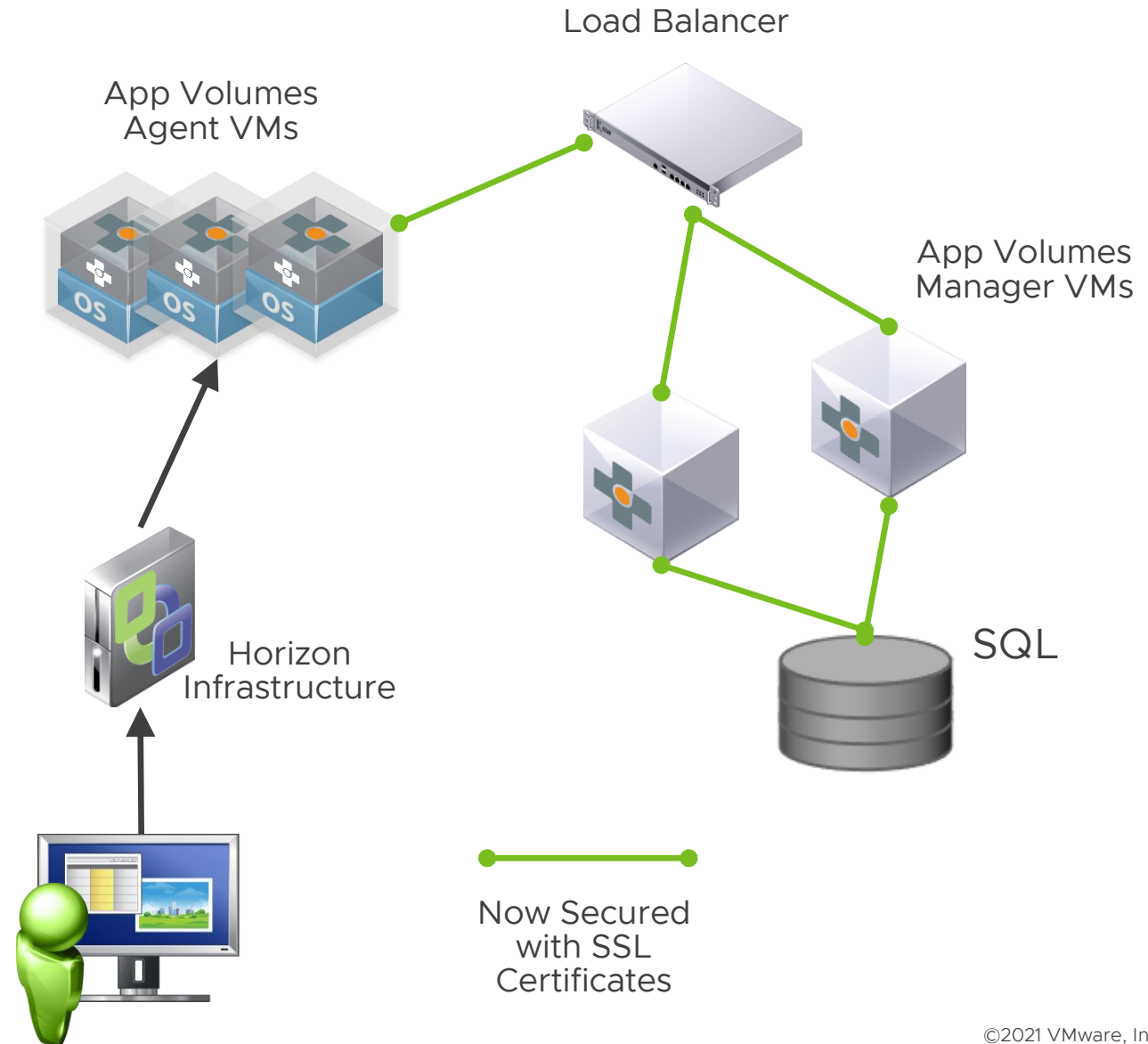
SSL Certificates and Load Balancers

Typical Deployment

- SSL is terminated at load balancer
- HTTP between LB and AV Manager
- SSL between AV Agents and LB
- If trusted CA-signed cert is used for LB, be sure all agents trust the CA

Alternative Deployment

- To keep SSL between LB and AV Manager, signed AV Manager certificate(s) should be added to trust list of the LB



Unified Access Gateway

Additional Material

Unified Access Gateway Logs (1/2)

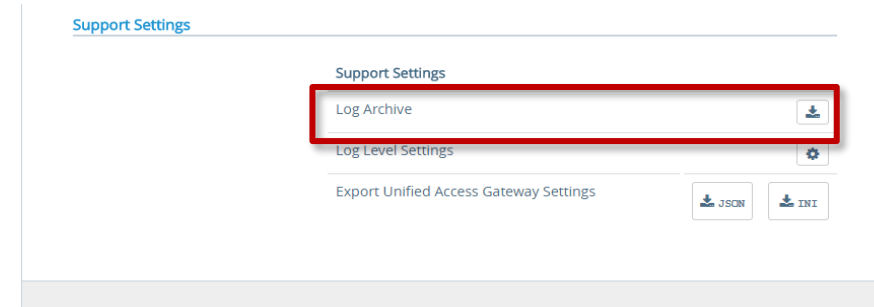
Service Logs

Admin UI

- or <https://uag.domain.com:9443/rest/v1/monitor/support-archive>

Downloads a zip file of multiple logs

- **appliance-agent.log** - VMware Tunnel agent (which starts up server and proxy) logs
- **authbroker.log** - Messages from the authbroker service which handles authentication adapters
- **bsg.log** - Blast Security Gateway logs
- **esmanager.log** - Log messages from the Edge Service monitor listener on ports 80 & 443
- **haproxy.conf** - HA proxy configuration for TLS port sharing, if configured
- **proxy.log** - VMware Tunnel proxy logs
- **psg.log** - PCoIP secure gateway logs
- **securityGateway_*.log** - Messages from the PCoIP Security Gateway
- **tunnel.log** - Messages from the tunnel process that is used as part of the XML API processing
- **utserver.log** - UDP Tunnel Server logs
- **vpnd.log** - VMware Tunnel server logs



Unified Access Gateway Logs (2/2)

Appliance Logs

UAG Config

- admin.log – Messages from the process that provides UAG REST API on port 9443
- admin-zookeeper.log – Messages related to the data layer that is used to store UAG config info
- rpm-version.log - Version of the UAG appliance
- uag_config.ini – current configuration settings in ini format.
- uag_config.json – current configuration settings in json format.

Linux logs

- df.log - Disk space usage
- Free.log – Information on memory usage
- ifconfig.log – Information on network interfaces
- ipv4-forwardrules - IPv4 forwarding rules
- netstat.log – Network configuration
- netstat-r.log – Static routes
- netstat-s.log - Network stats (bytes sent/received etc) from the time of creation of the appliance
- ps.log – Process list
- top.log - Sorted list of processes by memory usage at the time of downloading logs
- vami.log - Logs from running vami commands to set network interfaces during deployment

Log File Descriptors (1/2)

Aplogarchive.zip included files

Log	Log filename	Description	Linux Command (if applicable)
UAG configuration	uag_config.json, uag_config.ini	Entire configuration of the UAG appliance, showing all the settings as a json and an ini file	
UAG version	rpm-version.log	Version of the UAG appliance (2.8, 2.9, 3.0 etc)	
Process list	ps.log	Processes running at the time of downloading logs	ps -elf --width 300
IP forwarding rules	ipv4-forwardrules	IPv4 forwarding rules configured on the appliance	
Memory usage	top.log	Sorted list of processes by memory usage at the time of downloading logs	top -b -o %MEM -n 1
Free memory present	free.log	RAM availability at the time of downloading logs	free
Network information	netstat.log	Information on open ports and existing TCP connections	netstat -an
Network interface	ifconfig.log	Network interface configuration for the appliance	ifconfig -a
Network stats	netstat-s.log	Network stats (bytes sent/received etc) from the time of creation of the appliance	netstat -s
Disk usage	df.log	Disk usage on the appliance	df -a -h --total
Static routes	netstat-r.log	Static routes created on the appliance	netstat -r
Uptime	w.log	Information about uptime, the users currently on the machine, and their processes.	w
Supervisor	supervisord.log	Supervisor (manager for ES manager, admin and auth broker) log	
Edge service manager	esmanager-x.log, esmanager-std-out.log	Edge service manager log, showing backend processes performed on the appliance	
Admin	admin.log, admin-std-out.log	Admin GUI logs	
Auth Broker	authbroker.log	Auth Broker for Radius and RSA SecurID authentication	
BSG	bsg.log	Blast secure gateway logs	
PSG	psg.log	PCOIP secure gateway logs	
UT Server	utserver.log	UDP Tunnel Server logs	
VMware Tunnel server	vpnd.log	VMware Tunnel server logs	
VMware Tunnel proxy	proxy.log	VMware Tunnel proxy logs	
Tunnel agent	appliance-agent.log	VMware Tunnel agent (which starts up server and proxy) logs	
TLS port sharing configuration	haproxy.conf	HA proxy configuration for TLS port sharing, if configured.	
VAMI commands	vami.log	Logs from running vami commands to set network interfaces during deployment	

Log File Descriptors (2/2)

Log	Log filename	Description	Linux Command (if applicable)
Supervisor	supervisord.log	Supervisor (manager for ES manager, admin and auth broker) log	
Edge service manager	esmanager-x.log, esmanager-std-out.log	Edge service manager log, showing backend processes performed on the appliance	
Admin	admin.log, admin-std-out.log	Admin GUI logs	
Auth Broker	authbroker.log	Auth Broker for Radius and RSA SecurID authentication	
BSG	bsg.log	Blast secure gateway logs	
PSG	psg.log	PCOIP secure gateway logs	
UT Server	utserver.log	UDP Tunnel Server logs	
VMware Tunnel server	vpnd.log	VMware Tunnel server logs	tail -f /var/log/vmware/proxy/tunnel.log
VMware Tunnel proxy	proxy.log	VMware Tunnel proxy logs	tail -f /var/log/vmware/proxy/proxy.log
Tunnel agent	appliance-agent.log	VMware Tunnel agent (which starts up server and proxy) logs	
TLS port sharing configuration	haproxy.conf	HA proxy configuration for TLS port sharing, if configured.	
VAMI commands	vami.log	Logs from running vami commands to set network interfaces during deployment	

True SSO

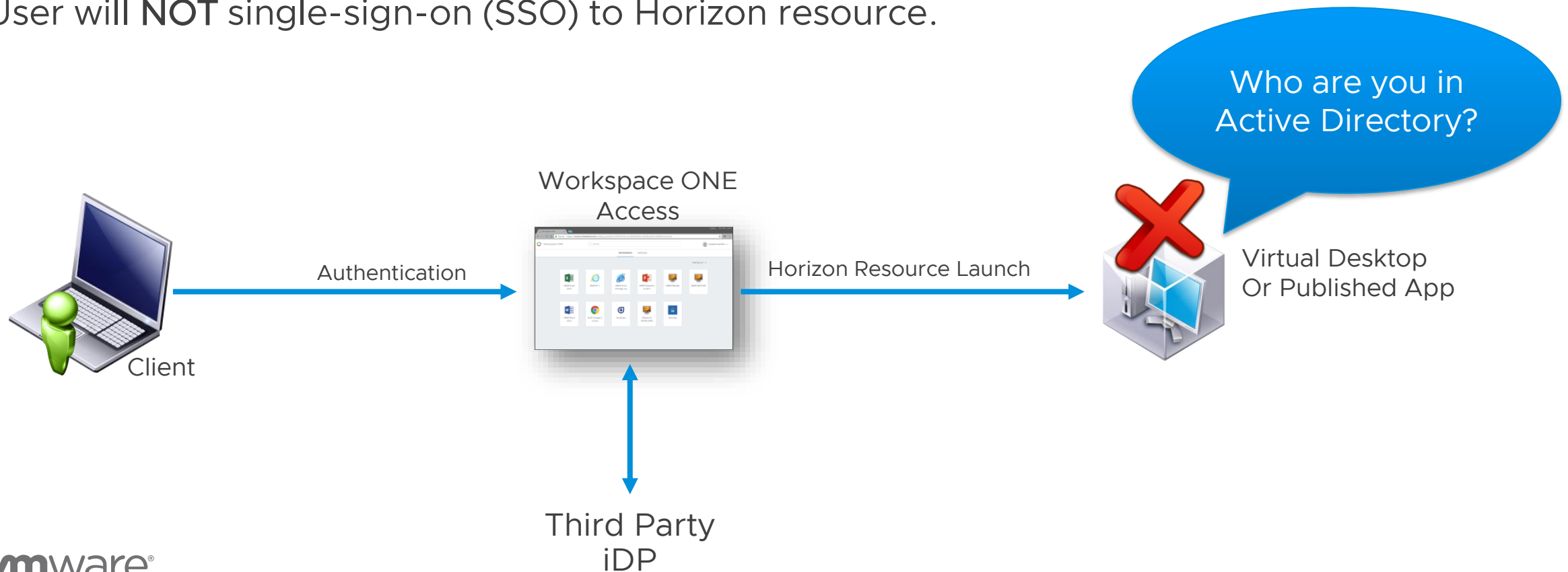
Additional Material

Third Party Authentication through WS1 Access

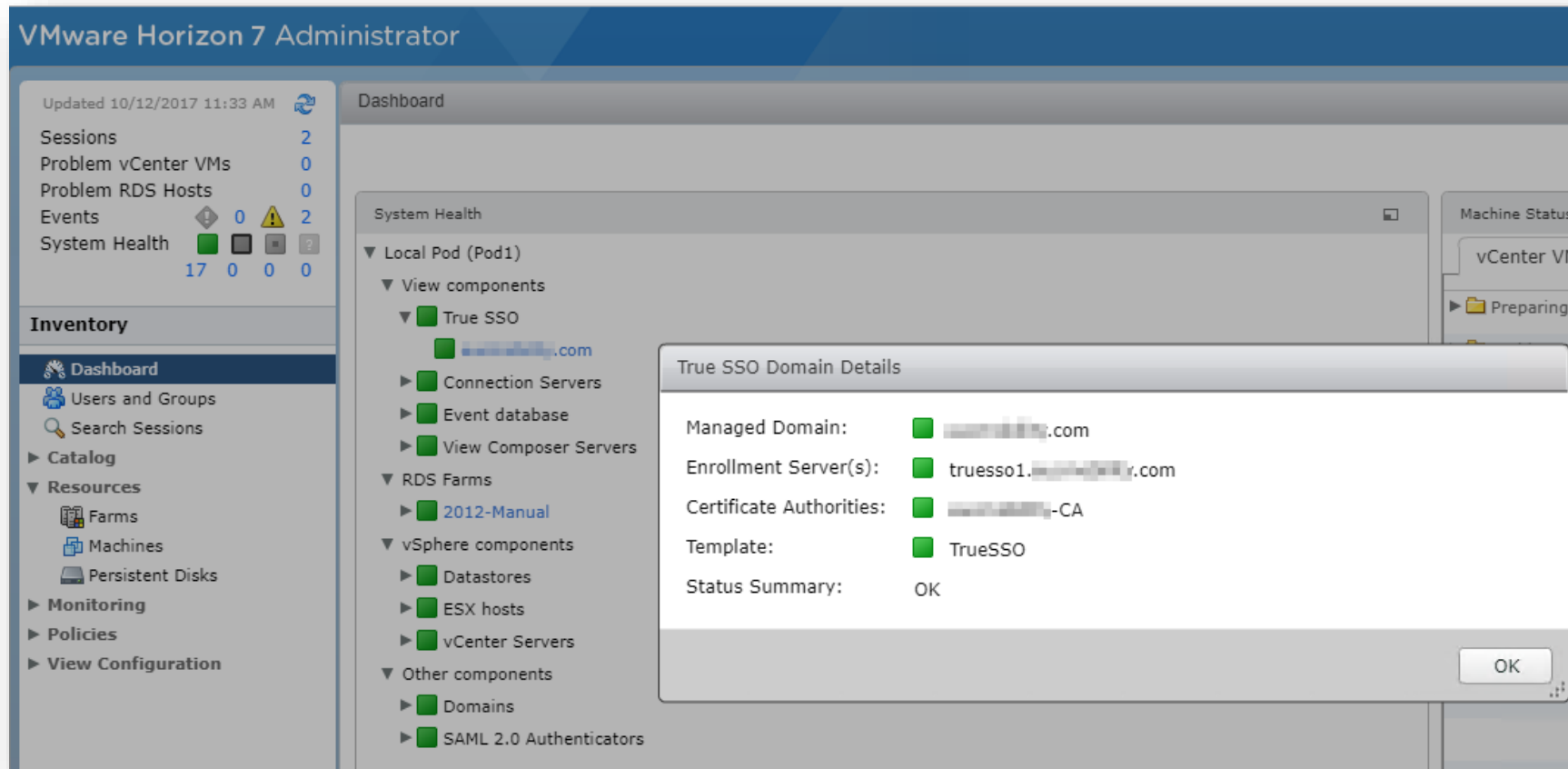
Authentication process to Workspace ONE Access can use many credential options.

- May not include Active Directory credentials

User will **NOT** single-sign-on (SSO) to Horizon resource.



True SSO in Horizon Dashboard



TrueSSO Status
displayed within
the Dashboard

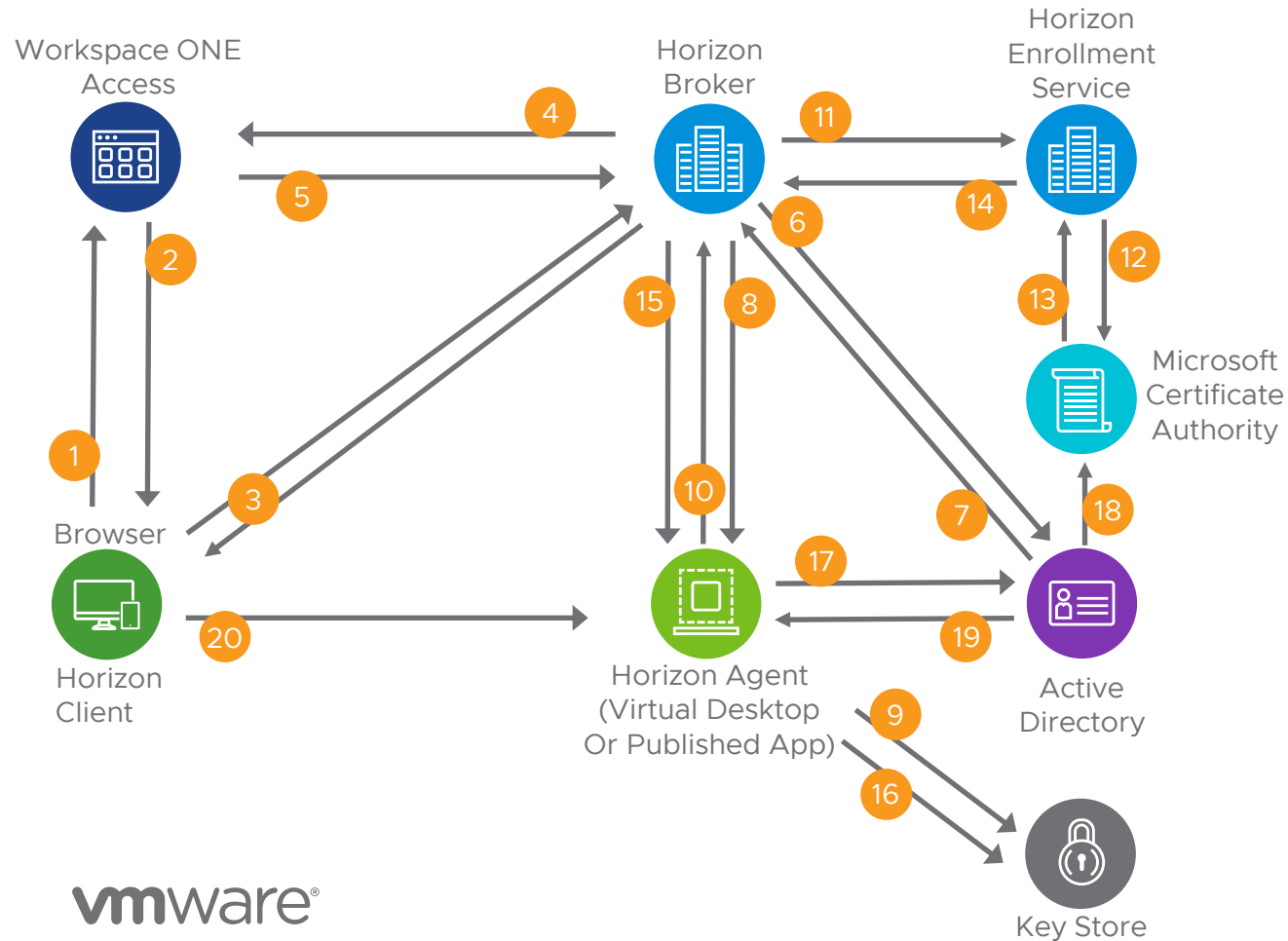
Displays
configured
Components

Dynamic status
summary
information

Dashboard
update interval is
60 seconds

Detailed TrueSSO Communication Flow

Identity Manager Launch of Horizon Resource without AD credentials



1. In Browser, user launches Horizon resource from Workspace ONE Access
2. Workspace ONE Access generates SAML assertion and artifact. Generates view URL containing artifact and returns to Browser: `vmware-view://URL SAMLArt=<saml-artifact>`
3. Horizon Client is launched from view URL. XML-API request `do-submit-authentication <saml-artifact>`
4. Connection Server performs SAML resolve against Workspace ONE Access `<saml-artifact>`
5. Workspace ONE Access validates artifact and returns assertion. `<saml-assertion>`
6. Connection Server performs a UPN Lookup (if UPN not provided in assertion) to a Domain Controller
7. Corporate UPN returned from AD to Connection Server
8. Connection Server performs a Certificate Logon Request to the virtual desktop or RDSH
9. Key Gen to Key Store
10. CSR returned from desktop or RDSH
11. Connection Server to Enrollment Server – Certificate Logon Request (providing key and UPN)
12. Enrollment Server generates a certificate request to the Microsoft Certificate Authority.
13. The CA returns a certificate to the Enrollment Server.
14. The Enrollment passes the certificate to the Connection Server.
15. The Connection Server presents the Certificate to the virtual desktop or RDSH
16. Cert Logon to Key Store.
17. The desktop does a Kerberos Certificate Logon.
18. The Domain Controller performs a certificate revocation check with the Certificate Authority
19. AD returns a Kerberos Token.
20. The protocol session connects.