# Lab 5 - Log Management

## Introduction

• VMware Aria Operations for Logs is a part of the VMware Cloud suite of services. Use this service to develop sophisticated analytics that aid in rapid troubleshooting of your SDDC or VMware Cloud on AWS environment..

As part of the VMware Cloud suite of services, VMware Aria Operations for Logs (formerly known as vRealize Log Insight Cloud) provides a fully managed and integrated log analytics and troubleshooting service.

VMware Aria Operations for Logs includes VMware-authored SDDC (ESXi, VC, NSX, and VSAN) insight for troubleshooting, a flexible and comprehensive query facility that supports troubleshooting for novice and experienced administrators, built-in SDDC and custom alerting capability, flexible notification mechanisms, and centralized support for local or federated authentication.

## Setting up Log Insight Cloud for non- Cloud services organization



### Setting up VMware Aria Operations for Logs for VMware Cloud Subscribers



## TASKS

## Task 1 - Enabling Firewall logging and generating log entries

- 1. From your VDI Desktop, open the browser and log into your VMC on AWS SDDC <u>https://vmc.vmware.com/console/sddcs</u>
  - Username: vmcexpert#-xx@vmware-hol.com
  - Password: VMware1!
- 2. On your SDDC Tile Click View Details
- 3. Select Open NSX Manager (next to Open vCenter)
  - Select the blue box Access Via the Internet
- 4. Click the **Security** Tab
- 5. Modify the Distributed Firewall
- 6. Click Add Policy
- 7. Name the Policy Class Log Test
  - Check the box next to the policy you created, Add Rule is now available
- 8. Select Add Rule
- 9. Name the Rule Allow All HTML

Distributed Firewall				?
All Rules Category Specific Rules				
		2 Total Unpub	lished Changes ACTIONS	REVERT
ETHERNET (1) EMERGENCY (0)	INFRASTRUCTURE (0)	ENVIRONMENT (0)	• APPLICATION (4)	
+ ADD POLICY + ADD RULE		2 Unpublished Changes	Filter by Nam	e, Path and more
Name ID	Sources Destinations	Services Context Profiles	s Applied To Actio	n
Class Log Test (1) Applied To	DFW		•	Success C 🛛 🕲 🔅
New Rule	Any Any	Any None	DFW	Allow 🗸 🌑 🔅 🖂
> Default Laye (3) Applied To	DFW		•	Success C 🛛 🖉 😳

- 9. Under Sources click the pencil, select RFC1918, click Apply
- 10. Under **Destination** click the pencil, select **RFC1918**, click **Apply**

	UP				EXPAND ALL	Filter by Name, P	ath and more
			Name	Туре 🕦	Compute Members	Status	Group Type
	>	00	Connected VPC Prefixes	Generic	View Members	• Success C	System Defined
	>	00	DirectConnect Prefixes	Generic	View Members	Success C	System Defined
•	>	00	RFC1918	Generic	View Members	🔵 Success  C	User Defined
	>	88	S3 Prefixes	Generic	View Members	● Success C	System Defined
	>	88	Transit Connect DGW Prefixes	Generic	View Members	● Success C	System Defined
	>	00	Transit Connect External TGW Prefixes	Generic	View Members	● Success C	System Defined
	>	88	Transit Connect Native VPCs Prefixes	Generic	View Members	● Success C	System Defined
	>	00	Transit Connect other SDDCs Prefixes	Generic	View Members	• Success C	System Defined

- Under Services click the pencil, filter for http, select HTTP and HTTPS, click Apply
   Under Actions leave Allow selected, the rule should be enabled by default
- 13. Publish the DFW rule by clicking the blue **Publish** button

			_
Set Services		×	
Rule > Allow All HTML			
Services (2) Raw Port-Protocols (0)			
= (http ×)		CLEAR X	
Name	Service Entries	Status	
□ : > ۞ ACIM-HTTP	TCP (Source: Any   Destination: 5988)	• Success C	
🗌 : > 🗘 Асім-нттря	TCP (Source: Any   Destination: 5989)	• Success C	
☑ : > ○ AHTTP	TCP (Source: Any   Destination: 80)	• Success C	
	TCP (Source: Any   Destination: 443)	• Success C	
□ : > ۞ AHTTPS, net.tcp binding	TCP (Source: Any   Destination: 32843,32844,32845)	● Success C	
□ : > ۞ 合 Office Server Web Services,	TCP (Source: Any   Destination: 56737,56738)	● Success C	
	TCP (Source: Any   Destination: 7777)	● Success C	
□ : > ۞ 合 Oracle9iAS Web Cache HTTP	TCP (Source: Any   Destination: 7779)	● Success C	
□ : > ۞ A Oracle9iAS Web Cache HTTP	TCP (Source: Any   Destination: 4444)	● Success C	
□ : > ۞ A Oracle HTTP Server Diagnost	TCP (Source: Any   Destination: 7200)	Success C	
□ : > ۞ A Oracle HTTP Server Jserv port	TCP (Source: Any   Destination: 8007)	Success C	
2 C REFRESH		1 - 30 of 30	
Show Only Selected		CANCEL	
Distributed Firewall All Rules Category Specific Rules			?
			ACTIONS - REVERT PUBLISH
ETHERNET (1) EMERGE	NCY (0) INFRASTRUCTURE (0)	ENVIRONMENT (0)	APPLICATION (4)
+ ADD POLICY + ADD RULE			Filter by Name, Path and more
Name ID	Sources Destinations	Services Context Profiles	Applied To Action
Class Log Test (1) Ap	plied To DFW	· ·	Success C 🔘 🖗
Allow All HTML 1025	22 RFC1918 22 RFC1918	<pre>C) HTTPS None</pre> C) HTTP	DFW 🕒 Allow 🗸 🌑 🔅 🖂
Default Laye (3) Ap	plied To DFW		Success C 💿 🛞

- 14. Select the **Gear** in the far right side of the **Allow All HTML** rule
- 15. Move the **slider** next to logging to enable logging
- 16. Set the Log Label to **vmcexpert#-##\_Test** (using your Student ID)
- 17. Click **Apply**
- 18. Click **Publish**

?

Settings		×
Rule > Allow All	HTML	
Logging	Enable i	
Direction	In-Out $\vee$	
Log Label	vmcexpert3-03_Test	
Comments		
		CANCEL

- 19. Click **Open vCenter** from the SDDC Console
- 20. Click Show Credentials
- 21. Copy the **Password** and Click **Open vCenter**
- 22. Log into vCenter as:
  - cloudadmin@vmc.local
    - {Paste in the copied Password}
- 23. In vCenter, Click the **frontend VM** and record its **IP address**

<	🔀 frontend_1-mcm1786472-190937025340 🛛 🖻 🖽 🖓 🐼 🕴 Actions
[] Þ = Ø	Summary Monitor Configure Permissions Datastores Networks Snapshots
<ul> <li>vcenter.sddc-35-81-153-208.vmwarevmc.com</li> <li>SDDC-Datacenter</li> <li>Cluster-1</li> <li>10.231.2.4</li> <li>Compute-ResourcePool</li> <li>api_ser_2 -mcm1786685-1909.</li> <li>frontend_i-mcm1786472-19093.</li> <li>mongo_server_1-mcm1786470-1.</li> </ul>	Guest OS: Ubuntu Linux (64-bit) Compatibility: ESXI 5.5 and later (VM version 10) VMware Tools: Running, version:11269 (Guest Managed) MORE INFO DNS Name: Instantial IP Addresses: 192.168.231.139 VIEW ALE 2 IP ADDRESSES Host: 10.231.2.4
武 nats_server_1-mcm1786471-190 武 queue_service_1-mcm1786473-1	VM Hardware 🗸
🔂 Ubuntu-Desktop-mcm1785905-1	Related Objects
wncexpert2-31_vra-proxy	Cluster (🖾 Cluster-1
vmcexpert2-31_vrops-proxy	Host 10.231.2.4
<ul> <li>Ø Mgmt-ResourcePool</li> </ul>	Resource pool O Compute-ResourcePool
NSX-Edge-0	Networks 🖾 sddc-cgw-network-1
🔂 NSX-Edge-1	Storage 🗎 WorkloadDatastore
🔂 NSX-Manager-O	

- 24. Select the Ubuntu-DT VM and click Open Console
- 25. Enter the Password of VMware1! if prompted
- 26. Launch the Firefox browser in the Ubunt-DT VM and type in **{the address of your Frontend VM}** for the Cats & Dogs Application
- 27. Click the **Gato & Cachorro** buttons multiple times until the image that appears is a hedgehog.
- 28. When this image (hedgehog) appears an error is generated and logged with log-insight and captured by vRealize Operations. You are also performing this step to generate some firewall logs
- 29. In a new Browser tab, go to VMware.com and one or more public websites

## Task 2 - VMware Aria Operations for Logs Overview



- 1. Click the **stacked squares** in the upper right-hand corner
- 2. Right-Click VMware Aria Operations for Logs
- 3. Click Open link in new tab



- 4. If Collapsed, Click the double arrows to expand the left pane
  - Expand the **Configuration** Section
  - Click Subscriptions

 Notice we are using the **PERPETUAL** Subscription. This subscription comes with VMC on AWS and only allows you to view Audit logs and Firewall Logs. To view other types of logs (Application logs, non-SDDC logs, etc..) the subscription must be upgraded.

vmw VMware Aria Operations	; for Logs		
*	(3) You need Org Owner and Admin roles in Operations for Logs (Sa	aS) to purchase subscription plans.	×
ි Home			
Explore Logs	Subscriptions		
🕼 Live Tail			
<pre>% Analytics &gt;</pre>	Region     O	Seller	
② Dashboards	Linited States of America	NW VMware	
C Log Sources			
△ Alerts ✓			
Triggered Alerts	Subscription Plans		
Alert Definitions	Use the latest subscription plans in VMware Aria Operations for L	ogs to leverage maximum benefits in log analytics at a minimum cos	t. <u>Learn more</u> r?
🗟 Content Packs			
③ Operations for Logs (On		all new Subscription plans!	
□ Log Management ● >			
Onfiguration •	billed according to your	for Logs now offers a customized plan in which you can select your commitment plan for the selected requirements, and according to th	ingestion log volume, storage, and retention requirements. You are the on-demand plan for other requirements. Commitment plans provide
Metrics	a discounted rate based	on the commit and retention period.	
vSphere Integration			
System Alerts	Countral Dian		(From units 20%)
Email Configuration	PERPETUAL	On-Demand Plan	Customized plan
Webhook Configuration	You have been extended to the	If you allock as an element extension in your as	
Cloud Proxies	perpetual license which provides all the features and	billed according to your data usage. You can	plan in which you select a commitment plan for
API Keys	functionalities of the product	activate this plan and pay as you go	certain requirements.
Operations for Logs Agents	Vnlimited log Ingestion	Unlimited log Ingestion	Customize the plan based on your usage
Usage Reports	Lin to 30 Dave of log retention in	Lin to 30 days of log retention in indexed	
Access Control	indexed storage	storage	
Subscriptions	Lin to 7 years of log retention in non-	Lin to 7 years of log retention in nor-	Up to 30 Days of log retention in
	indexed storage	indexed storage	nueved atorage
C SWITCH THEME	Recall logs from non-indexed storage	Recall logs from non-indexed storage	Up to 7 years of log retention in non- indexed storage
	Query logs from non-indexed storage	Query logs from non-indexed storage	Recall logs from non-indexed storage

- 8. Click **Dashboards** to view the available dashboards
- 9. In the Search Bar, type **Gateway Firewall**
- 10. Select Gateway Firewall Traffic (latest version)
- 11. Review the Pie Graphs for **Top Sources** and **Top Destinations** You'll see an aggregated and processed view of all network traffic leaving the SDDC in the past 5 mins.
- 12. In the Upper right corner note that you can increase the time scale to review date beyond the last 5 mins



All NSX related log events must first be enabled before those log messages will be sent to Log Insight. E.G. If you want to see DHCP, NAT or VPN related log messages then you must enable logging for those services as we did in task 1 for our firewall rule.



- 13. Select **Dashboards** in the left column
- 14. Click on **All Dashboards**:
  - Select NSX-T events for VMware Cloud SDDC v6.0
  - Select Distributed Firewall Traffic
- 15. Observe the traffic, you may have to change the time window by selecting 30M or 1H to see relevant data

Dashboards (99)	ALL DASHBOARDS ~		
Q Search for Dashboards, Widg	Content Packs Apache - HTTP Server V1.0	>	
ACTIONS ~	Audit Events for VMware Cloud SDDC V2.0 Audit Events for VMware Cloud Services V1.0	>	
Name	Audit Events for VMware Cloud Services V2.0	>	
🗌 🚦 🔂 Apache HTTP - E	AWS - CloudFront V1.0.0	>	
Apache - HTTP Servi	General V4.4	>	
	Linux - Systemd V1.0	>	
☐ : ☆ Apache HTTP - C	Linux V1.0	>	
S Add tags +	Linux V2.2	>	
	Nginx V1.0	>	
☐ : ☆ Apache HTTP - S	NSX-T events for VMware Cloud SDDC V4.0	>	
( Add tags + )	NSX-T events for VMware Cloud SDDC V5.0	>	
	NSX-T events for VMware Cloud SDDC V6.0	>	Audits - Overview
Apache HTTP - V	- 14.0		DHCB - Overview
S Add tags +	n vi.u		Distributed Firewall - Overview
🗌 🗄 🟠 Activity			Distributed Firewall - Traffic
Audit Events for VMv	ware Cloud SDDC V2.0		Gateway Firewall - Traffic
Add tags +			NSX - IDPS - Overview
🗌 🗄 🏠 Alarms			NSX - IDPS - Traffic
Audit Events for VMv	vare Cloud SDDC V2.0		

Distributed Firewall - Traffic 🏠 🛛 ALL DA	ISHBOARDS ~	5M 3	ом тн ен сизтом - С :
+ ADD FILTERS			
Top Firewall Sources Top source IP addresses from all firewall rules that are logging	ı dətə.	Top Firewall Destinations Top destination IP addresses from all firewall rules that are logging data.	:
	ेक्क Hide All	🕅 Hide All	
A maximum of 23 event types are categorized here.     Other (079 groups)     192.168.203.05     192.168.203.129	44,240,177,223     192,163,203,69     192,163,203,69     193,163,203,69     193,163,203,10     193,163,203,10     193,163,203,10     192,163,203,2     192,163,203,5     X	<ul></ul>	223 7 14 5 5 52 34
Application Ports Permitted Measures all in / out connections permitted in the NSX-T envir	onment by destination port. The data is the summation of the specified time ran	Application Ports Denied All traffic deined by a firewall rule. Data is grouped by application (or destination) port number. Th	is widget displays only data associated with.
1	No Data Available	No Data Available	

- 16. From the left hand navigation pane, select Home
- 17. In the search bar, type **vmcexpert\*** to see traffic that has **PASS**ed the DFW rule. You may need to change the time period to 30M or 1H.
  - **HINT:** Use your full student account name (**vmcexpert#-##**) to see events for your SDDC only.

ntitled 🖉	O Q Partition:	☆~ 5м 301	Б \$	☆ ▲	
splay query as text 🔨 🕂	+ ADD FILTERS				
Count of events • v	ver time v	c	7 RESET	No alerts	Area 🗸 😞
20					
10					
0					
12:29:15 1	1229:30 1229:45 12:30:00 12:30:15 12:30:30 12:30:45 12:31:00 12:31:15 12:31:30 12:31:45 12:32:00 12:32:15 12:32:30 12:32:45 12:33:00 12	:33:15	12:33:30	12:33:45	12:34:00
tream Types Alerts	Event Trends	Inge	st timestam;	>: Newest ~	Total: 28 event
ingest_timestamp te	ent				>
> 2023-05-10 12:33:21.081 -0600	<992823-85-10718;33:13,3532 ess-0.sddc-44-240-238-6.vmarvenc.com FIRDMAL-PETLOG[2099842]; d70940ef INET natch PASS 1024 OUT 52 TCP 192.168.203.5/42208->10.203.12.3/44) 5 vmcempert3-0]_Test		Field	ds name	Fields Librar
> 2023-05-10 12:33:21.081 -0600	<99>2823-65-18118:33:13.8812 esc-8.sddc-44-248-238-6.vmarvenc.com FIRDMALL-9KTL06[2899842]: d70940ef INET natch PASS 1024 OUT 52 TCP 192.168.203.5/42816->18.203.12.3/443 5 vmcepert3-03_Test		appr	iame it_type	
> 2023-05-10 12:33:21.081 -0600	<992823-65-18118:33:12.866Z ess-0.sddc-44-240-238-6.vmarvexc.com FIREMALL-9CTLOG[2099042]: d709d0cf INET nutch PASS 1024 0UT 52 TCP 192.168.289.5/42800-310.289.12.3/443 5 mccupart3-09_Test		log_	size type	
> 2023-05-10 12:33:01.507 -0600	<992821-85-18118:12:49.1512 ess-8.s66c-44-248-238-6.vmarevec.com FIRDMUL-PKTLOG[2899842]: d7090Rcf INCT TERM PASS 1824 0UT TCP RST 192.168.289.5/48278-518.289.14.4/43 19/15 4793/5242 ymccogert3-00_Test		prior	ity ess	
> 2023-05-10 , 12:33:01.507 -0600	4992823-05-18118:32:54.165Z ess-0.sddc-44-240-238-6.vmarevec.com FIREMUL-PKTLO6[2899842]: d70908cf INET TERM PASS 1824 OUT TCP FIN 192.168.289.5/34578->10.289.12.3/443 13/14 3226/7345 succement3-00_Test		sddo	_id ce	
> 2023-05-10 12:33:01.507 -0600	4992823-65-18118:12:59.1742 ess-8.566c-44-240-238-6.vmarevec.com FIRDMLI-PKTL06[2899842]: d70908cf INIT TLBN PASS 1824 007 TCP RST 192.168.280.5/48282->10.280.14.4/40 11/8 1926/1178 mccaper13-00_Test		vmw	_nsxtvmc_firewall _nsxtvmc_firewall	Laction Ldst
> 2023-05-10 12:33:01.507 -0600	4992823-05-18118:12:14.1652 ess-0.sddc-44-240-238-6.vmarevec.com FIRDMLI-PKTL06[2099442]: d70908cf INIT TERM PASS 1824 0/T TCP FIN 192.168.280.5/4264->10.280.12.3/44) 14/14 3266/7809 <a href="https://doi.org/10.1011/j.j.ac/ac/ac/ac/ac/ac/ac/ac/ac/ac/ac/ac/ac/a</td> <td></td> <td>vmw</td> <td>_nsxtvmc_firewall _nsxtvmc_firewal</td> <td>l_dst_ip_port l_dst_port</td>		vmw	_nsxtvmc_firewall _nsxtvmc_firewal	l_dst_ip_port l_dst_port
> 2023-05-10 12:33:01.507 -0600	4992822-85-18118:12:58.1672 esx-8.s66c-44-248-238-6.vmarevec.com FIRDMAL-PCTLOG[2899842]: d70908cf INIT TERN PASS 1824 00T TCP FIN 192.168.280.5/48268-518.280.14.4/40 32/44 11851/59392 mccepert3-00_Test		vmw	_nsxtvmc_firewall	L_rule_id L_src
> 2023-05-10 12:33:01.507 -0600	(99)2822-65-18118:32:49.1512 esc-8.sddc-44-248-238-6.vmarvenc.com FIREMALL-PCTLOG[2899842]: d709d0cf INET TERN PASS 1824 0UT TCP FIN 192.168.280.5/48276-318.280.14.4/443 17/14 4713/5837 vmccmpert3-40_Test		vmw	_nsxtvmc_firewall	l_src_ip_port .log_port
> 2023-05-10 12:33:01.507 -0600	(992)822-65-18118:32:57.1652 esx-8.sdot-44-248-238-6.vmarevec.com FIRDMALL-PKTLoG[2899842]: d70940cf INET TEBM PASS 1824 00T TCP RST 192.168.200.5/40264-310.200.14.4/443 74/132 22763/122167 inccepter13-03_Test		vmw	_vmc_audit_nsxt_ _vmc_audit_nsxt,	_firewall_action _firewall_dst

- 18. Return to the VMware Cloud on AWS SDDC console tab in your browser, ensuring that you are in your SDDC
  - Select Networking & Security
  - Select Distributed Firewall under Security
- 19. Open the Class Log Test policy to see the Allow All HTML rule
- 20. Change Allow to **Reject** under Action
- 21. **Publish** the rule change

Distributed Firewall						?
All Rules Category Specific Rules						
				ACTIONS ~	REVERT	
ETHERNET (1) EMERGI	ENCY (0) INFRASTRI	JCTURE (0)	ENVIRONMENT (0)	APPLICATION (4)		
+ ADD POLICY + ADD RULE		re •••		Filter by Name,	Path and more	=
Name ID	Sources	Destinations Servi	ces Context Profiles	Applied To Action		
Class Log Te (1) Ap	plied To DFW			٠	Success C	© @
Allow all html 1024	28 RFC1918	않 RFC1918 〇 H	ITTPS None	DFW •	Reject 🗸 🌔	¢۵ ا
: > Default Laye (3) Ap	plied To DFW			•	Success C	00

- 22. Return to the Ubuntu Desktop Console window, relaunch from vCenter if it has timed out.
- 23. Open **Firefox** and connect to your **FrontEnd VM IP address** recorded earlier making sure to use **http**.
  - This should result in an immediate unable to connect message
  - If the DFW rule had been set to **DROP**, you would have to wait for the http timeout to see the failed message
  - From the Firefox web browser access vmware.com, try google.com. That access isn't blocked by the DFW.
- 24. Return to your open Aria Operations for Logs browser tab, or start a new Aria Operations for Logs session if closed
- 25. From the left hand navigation pane, select Home
- 26. In the search bar, type **vmcexpert\*** to see traffic that has been **REJECT**ed by the DFW rule. You may need to change the time period to 30M or 1H.
  - **HINT:** Use your full student account name (**vmcexpert#-##**) to see events for your SDDC only.



- 27. From the Aria Operations for Logs navigation pane, select **Dashboards**
- 28. Click the **All Dashboards** drop down
  - Select NSX-T events for VMware Cloud SDDC V6.0
  - Select Distributed Firewall Traffic
- 29. Observe **Application Ports Denied**, there should be entries from the REJECT rule. You might need to adjust the time band to 30M or 1H
- 30. When finished, return to the SDDC console, updating the DFW setting back to **ALLOW** from REJECT and **PUBLISH** the rule.
  - You can Verify that the DFW is set correctly by accessing the Cats & Dogs app from your Ubuntu Desktop

irewall rules that are logging data.
We Hide All           10.203.12.12
a is grouped by application (or destination) port number. This widget displays only data associated
by bytes - client to server on IP address, from the client to a server. Data is only displayed if the firewall is logging its data.Th
ons <sup>i</sup>

- 31. Click **Alerts** in the left hand navigation pane
- 32. Click **Alert --> Alert Definitions** to review the built-in alerts
- 33. In the search bar type **vcenter** and hit return to see the Alert definitions
- 34. Select the Audit Events for VMware Cloud SDDC | User Session Login Alert
- 35. Review the settings and notice there is currently no notification set when this alert is triggered, the rule is also disabled by default.
- 36. In the upper right hand, click the **edit Icon**, close any warning for partitions if present.

-0
9

- 37. Under **Trigger Condition 1**, click **Choose Notification** and Input **Your Email address** in the notify field, then click the **+**
- 38. Move the slider to **enable** the alert
- 39. Click Save
- 40. If logged into vCenter, logout. Login to your vCenter server. You should receive both user and application login notifications.
- 41. After verifying incoming email notifications, **Disable** the alert by moving the slider, edit the alert and remove your email address by clicking the '**x**' and then **Save**.

≪ ⇔ Home	Alert Definitions						CREATE NEW	e e
	vcenter						$\otimes$	
Live Tail		ACTIONS ~					Sort By: Enabled Fir	rst ~
Analytics >	∀ Filters 《		Details	Ŧ	Severity	Origin	Created At	EXPOR
② Dashboards	Severity 🗸		Audit Events for VMware Cloud SDDC   Host Connection Lost Alert		( Info )	Audit Events for VMware Cloud SDDC V2.0	2021-07-23 07:07:36 GMT-06:00	
Log Sources	Critical		A host that a vCenter Server system manages lost connection to vC					KNO
🛆 Alerts 🗸 🗸	Warning		○ Add tags +					WLEDGE
Triggered Alerts		. : 👁	Audit Events for VMware Cloud SDDC   Host Disconnected Alert		Info	Audit Events for VMware Cloud SDDC V2.0	2021-07-23 07:07:36 GMT-06:00	HUB
Alert Definitions	Туре >		A nost that a veener server system manages got disconnected iro     Disabled forever					
💩 Content Packs	Origin >		( ♦ Add tags + )					
② Operations for Logs (On			Audit Events for VMware Cloud SDDC   Host Shut Down Alert A host that a vCenter Server system manages got shutdown becau.		Info	Audit Events for VMware Cloud SDDC V2.0	2021-07-23 07:07:36 GMT-06:00	
Log Management • >	Tags 2		Disabled forever					
Onfiguration • >			( S Add tags + )					
			Audit Events for VMware Cloud SDDC   User Session Login Alert User logs in to a vSphere component or when a vCenter Server solu		Info	Audit Events for VMware Cloud SDDC V2.0	2021-07-23 07:07:35 GMT-06:00	
			▲ Disabled forever					

Edit alert 💽	CANCEL
Name: Audit Events for VMware Cloud SDDC   User S 🕦 \star	
Description:	
User logs in to a vSphere component or when a vCenter Server solution user accesses another vCenter Server service.	
Query * Select or write a query	
Audit Events for VMware Cloud SDDC   User Login Events Partition:	
Search logs to vinw_vinc_avail_event exists Alvo vinw_vinc_avail_event contains oserLoginSessionEvent SHOW CHART SHOW LOGS	
Trigger Conditions and Severity * Define Severity and Conditions  For time period of: Real Time	
Trigger Condition 1 set severity to: 100 v	
In this case, notify 🔯 rmougey@vm_ 🛞 Choose Notification 👻	
Send to VMware Aria Operations Manager (1)	
Recommendations(optional) Write down recommendations which will be shown in Notifications     No Recommendations	



Mote: You can also create custom alerts.

- 42. In the left pane, click **Content Packs** to review the available content packs for Log Insight Cloud
- 43. Notice that not all content packs are enabled. Enabling a content pack allows Log Insight to begin processing log messages for the system
- 44. If Disabled, Enable the content packs for:
  - Audit Events for VMware Cloud SDDC (v2)
  - General

Content Packs		EXPORT CONTENT
Q What content pack are you looking for?		
Enabled 🗿 Public 🚳 Private 🔕		
All  VMware Cloud  Applications Others		
VMware Cloud (6)		
Audit Events for VMware Cloud SDDC	Audit Events for VMware Cloud Services	General
This content pack provides powerful insight into audit events generated in the VMware Cloud SDDC environment allowing administrators to audit, monitor and troubleshoot activity in their environment.	This content pack provides Audit events for all the VMware Cloud Services. This includes the Governance aspect of CSP.	The Log Insight Cloud General Content Pack includes the following dashboards: • Overview - Provides generic information about any events being sent to your Log Insight instance including errors,
VERSION 2.0 Enabled Versions: V2.0	VERSION 2.0 V Enabled Versions: V2.0	VERSION 4.4 Enabled Versions: V4.4
ACTIONS ~ DETAILS	ACTIONS ~ DETAILS	ACTIONS ~ DETAILS
Disable		
Export         or VMware Cloud SDDC           This content pack provides powerful insights into the NSX-T freewal rules, packet traffic rules created in VMware cloud SDC along with audit details along and aministrators to audit, monitor and troubleshoot the behavior of configured rules in VERSION 6.0 ×           VERSION 6.0 ×         Enabled Versions: V6.0,V5.0,V4.0	VMware - Audit Events for VMware Cloud on AWS This content pack provides powerful insight into audit events generated in the VMware Cloud on AWS environment allowing administrators to audit, monitor and troubleshoot activity in their environment. VERSION 1.4 V Enabled Versions: VL4,VL0	VMware - NSX-T for VMware Cloud on AWS           Image: State of the stat
ACTIONS ~ DETAILS	ACTIONS ~ DETAILS	ACTIONS ~ DETAILS
Applications (1) Apache - HTTP Server  Abache HTTP Server, often referred to as just Apache, is an open-source web server. Like many web servers, Apache leverages the Apache leverages the Apache Like many web servers, Apache leverages the Apache Like many web servers, Apache leverages the Apache leverages the Apache leverages the Apache leverages the Apache Like many web servers, Apache leverages the Apache leverages		

- 45. Select Public, then Applications
  - NOTE: You may need to clear the search bar in order to see the desired results
- 46. Enable Apache HTTP Server and Nginx
- 47. Select Others
- 48. Enable the Linux and Linux Systemd Content Packs, if not already enabled





49. Click on **Dashboards.** In the search bar type the name of one of the content packs you enabled **(Linux, Nginx etc).** You'll now notice additional dashboards (Activity, Alerts, etc...)

## Task 3 - Application Logs

- 1. In the log Insight cloud interface expand Configuration
- 2. Click Cloud Proxy

If there are any existing **inactive** Proxies, click **Delete** and confirm the deletion to remove them

- 3. Click ADD Proxy
- 4. Click **Existing**
- 5. Select the Aria Automation Proxy you deployed earlier
- 6. Click Add

Add	Existing Cloud Prox	ÿ					×	
	-	-						
The fol	lowing list contains Cloud Prox	ties across multiple services. Sel	ect a Cloud Proxy from VMware	e Aria Operations f	or Logs, VMwa	are Aria Hub, or VMwai	re Aria	
Autom	Name	Status	IP address	Creation date	<b>^</b>	Services		
0	AA-Proxy_3-01	⊘ ACTIVE	192.168.201.3	May 03, 2023		VMware Aria Automatic	on Assemb	
						CANCEL	ADD	

Cloud Proxies Cloud 1	Native Collectors			
Cloud Proxies (1)	C			CONFIGURE NOTIFICATIONS ADD PROXY ~
Search for Cloud Proxie	es by Name			Q
Name	Status	IP address	Creation date	↑ Services
AA-Proxy_3-01	⊘ ACTIVE	192.168.201.3	May 03, 2023	VMware Aria Automation Assembler - SDDC VMware Aria Operations for Logs

- 7. In the left pane under the **Configuration** section, click **Operations for Log Agents**
- 8. Under **Agent Configuration** clink **New** next to **File Logs**, add configuration settings for the following. **Note:** hit **Save** as you complete each section.
  - MongoDB
    - Directory: /var/log/mongodb
    - include files: \*.log
  - syslog
    - Directory: /var/log
    - Include files: \*.log
  - docker
    - Directory: /var/lib/docker/containers
    - Include files: \*.log

Servers General	NEW+	[filelog MongoDB]	
Common	NEW+	Directory: (var/log/mongodb ) Enabled:	
Windows Event Lo	g NEW+	Event marker: (i) Character set: UTF-8 (i)	
File Logs	NEW+	Include files: *.log ① Exclude files: hidden.log; secur?. ①	
syslog	12 X	Raw Syslog: 🗌 🧃	
docker	0 ×	Tags ()	
Journal Logs	NEW+	NEW TAG	
Parsers	NEW+	Exclude fields: EventId; ProviderName;	١
		Whitelist filter expression: level > WINLOG_LEVEL_SUCCESS and level < WINLOG_LEVEL_INFO	(i)
		Blacklist filter expression: EventID == 4688 or EventID == 5447	(i)
		Parse fields by: None (j)	

- 9. At the top of the page, in the Agents search field, click the drop-down and select **Create New Group**
- 10. Name the Group Linux\_XX (Linux\_01) matching your student number
- 11. Click **OK**

	All Agents			~		
	Search for group		<b>()</b> Au	to-update of configura	tion 🕦 🌔 Au	to-upgrade of versior
Il Agents P Address T Hostname T gent Configuration ()	Available Templates           Linux           Venion           Linux - SLES (warn)           Linux - Ubuntu (kern)           Linux - Ubuntu (kern)           Create New Group	Events Sent	Events Sent/Sec	Dropped Events	Uptime	O Agent(s Status 1 - 10 of O age
e Build tab provides prompts with a graphical user interfa	ise one of the methods below. face. Alternatively, the Edit tab allows you to edit th	ne configuration file manually.				
entropy manage agent group configurations.     Servers NEW+     General NEW+     Common NEW+     Common NEW+     Windows Event Log NEW+     Entropy Metwidth     MongoDB	ae one of the methods below.	rs Character set: UTF- DExclude files: hidde	<ol> <li>Enabled: ▼</li> <li>▲ &lt; ()</li> <li>m.log; secur?. ()</li> </ol>			

VMware Aria	Operatio	ons for Logs Agents				
		New Agent Group		×		
All Agents						
		Name Linux_31		Sent/Sec		
		Info				
		21				
			CANCEL			
		L				

- 12. Configure the Group as follows:
  - Filter
    - OS
    - Starts with
    - Ubuntu\*

### VMware Aria Operations for Logs Agents

Linux_31		✓ ₫									
Use filters to select wh	iich ager	nts receive the Agent Configu	ration below.								
OS		<ul> <li>starts with</li> </ul>	v Ubuntu*	>	<u> </u>						
+ ADD FILTERS	× CLE	AR ALL									
										23 Age	nt(s) (i)
IP Address	Ψ	Hostname T	Version	os	Last Active	Events Sent	Events Sent/Sec	Dropped Events	Uptime	Status	Υ τ
192.168.229.142		frontend	8.6.2.19075480	Ubuntu 20.04.3 LTS	May 22, 2023, 4:20:15 PM	0	0.00	0	53m 38s	Active	
192.168.229.141		queue	8.6.2.19075480	Ubuntu 20.04.3 LTS	May 22, 2023, 4:20:06 PM	0	0.00	0	55m 17s	Active	
192.168.229.36		nats	8.6.2.19075480	Ubuntu 20.04.3 LTS	May 22, 2023, 4:20:05 PM	0	0.00	0	57m 19s	Active	
192.168.229.71		api	8.6.2.19075480	Ubuntu 20.04.3 LTS	May 22, 2023, 4:20:02 PM	0	0.00	0	55m 21s	Active	
192.168.229.140		mongodb	8.6.2.19075480	Ubuntu 20.04.3 LTS	May 22, 2023, 4:20:16 PM	3	0.00	0	59m 7s	Active	
192.168.229.68		mongodb	8.0.0.14743436	Ubuntu 20.04.3 LTS	May 22, 2023, 2:26:59 PM	0	0.00	0	2h 1m	Disconnect	æd
192.168.229.18		queue	8.0.0.14743436	Ubuntu 20.04.3 LTS	May 22, 2023, 2:26:30 PM	0	0.00	0	1h 57m	Disconnect	æd
192.168.229.134		frontend	8.0.0.14743436	Ubuntu 20.04.3 LTS	May 22, 2023, 2:04:18 PM	0	0.00	0	2h 30m	Disconnect	red
192.168.229.136		api	8.0.0.14743436	Ubuntu 20.04.3 LTS	May 22, 2023, 2:26:54 PM	0	0.00	0	1h 57m	Disconnect	ed
192.168.229.35		frontend	8.0.0.14743436	Ubuntu 20.04.3 LTS	May 22, 2023, 2:26:34 PM	0	0.00	0	1h 56m	Disconnect	ed
								1-	10 of 23 agents  <	< 1/3	> >

Agent Configuration (j)

In order to centrally manage agent group configurations, use one of the methods below.

- 13. Under the Agent Configuration section add the following configuration settings:
  - Under General Click New, and add the general section logging
    - Set the logging level to **verbose**
  - Click Save
    - Under Common Click New, and add the section global
  - Click Save

	Servers	NEW+	
~	General	NEW	1]logging]
	logging	×	Debug level: verbose (1)
~	Common	NEW+	Stats report period: 15
	global	$\times$	
	Windows Event Log	NEW+	
>	File Logs	NEW+	
	Journal Logs	NEW+	
>	Parsers	NEW+	

- 14. In the Agent Configuration section, Under **Parsers**, Let's create and define 4 parsers:
  - 1. Next to Parsers Click New, name the section syslog\_appname\_parser
    - Set the Parser to use/extend to CLF (default Common Log Format)
    - Set Format to:

%{appname}i[%{thread\_id}i]

### Click to copy

### Click **Save**

- 2. Next to Parsers Click **New**, name the section syslog\_parser
  - Set the Parser to use/extend to CLF (default Common Log Format)
  - Decode Field click Add
    - set the field to **appname**
    - set the value to syslog\_appname\_parser
  - Set Format to:

%t %i %{appname}i: %M

Click to copy Click **Save** 

- 3. Next to Parsers Click **New**, name the section **auth\_Parser\_sles** 
  - Set the Parser to use/extend to CLF (default Common Log Format)
    - Set Next Parser to syslog\_parser
    - Set Format to:

```
%t %i %{appname}i[%{thread_id}i]: password changed - account=%{linux_user}i,
uid=%{uid}i, %i
```

Click to copy

Click Save

- 4. Net to Parsers Click New, name the section auth\_Parser
  - Set the Parser to use/extend to CLF (default Common Log Format)
    - Set Next Parser to syslog\_parser
    - Set Format to:

```
%t %i %{appname}i[%{thread_id}i]: password changed - account=%{linux_user}i,
uid=%{uid}i, %i
```

Click to copy

Agent Configuration (j							
In order to centrally manage agent group configurations, use one of the methods below.							
The Build tab provides prompts with a graphical user interface. Alternatively, the Edit tab allows you to edit the configuration file manually.							
Build Edit							
logging	×	[parserlauth Parser sles]					
✓ Common	NEW+						
global	×	Parser to use/extend: <u>CLF (default Common Log Format)</u> ① Verbose logs (debug):[]					
Windows Event Log	NEW+	Exclude fields: domain_name; filepaths (j)					
∽ File Logs	NEW+	Decode fields: ①					
auth	0×	No decoders added ADD+					
messages	0×	Conditional decode fields: ()					
syslog	ØΧ	No decoders added					
docker	ØΧ	ADD CONDITION+					
Journal Logs		Rename fields: () No fields added					
✓ Parsers		ADD+					
auth_parser	0×	Format:%t %i %(appname)i[%(thread_id)i]: passwoi					
auth_Parser_sles	Ø×	Next parser: syslog_parser ① ①					
syslog_parser	Ø×						
syslog_appname_parser	0 × 📮						
SAVE							

- 15. In the Agent Configuration section, Under File Logs, Let's create and define 4 log configurations:
  - 1. Next to File Log Click New, name the section auth

- Set the Directory to: /var/log
- Set Include files to: auth.log;auth.log.?
- Tag Field click **New Tag** 
  - set the field to vmc\_cp
  - set the value to **linux**
- Set Parse fields by to: auth\_parser

Build Edit	
logging ✓ Common global Windows Event Log	× NEW+ × NEW+ Event marker: ↓var/log ↓var/log ↓var/log ↓var/log ↓var/log ↓var/log ↓var/log ↓var/log ↓var/log ↓var/log ↓var/log ↓var/log ↓var/log ↓var/log
<ul> <li>✓ File Logs</li> <li>auth</li> <li>messages</li> <li>syslog</li> <li>docker</li> </ul>	NEW+     Include files: _auth.log;auth.log?     3     Exclude files: _hidden.log; secur?.       0 ×     Raw Syslog: ]     1       0 ×     Tags (1)       0 ×     No tags added       New TAG     New TAG
Journal Logs Parsers auth_parser auth_Parser_sles syslog_parser	NEW+       Exclude fields:       EventId; ProviderName;       ①         NEW+       Whitelist filter expression:       level > WINLOG_LEVEL_SUCCESS and level < WINLOG_LEVEL_INFO
syslog_appname_parser	0 ×

- 2. Next to File Log Click **New**, name the section **messages** 
  - Set the Directory to: /var/log
  - Set Include files to: messages;messages.?
  - Tag Field click **New Tag** 
    - set the field to vmc\_cp
    - set the value to **linux**
  - Set Parse fields by to: **syslog\_parser**

Agent Configuration 👔								
In order to centrally manage agent group configurations, use one of the methods below.								
The Build tab provides prompts with a graphical user interface. Alternatively, the Edit tab allows you to edit the configuration file manually.								
Build Edit								
logging       ×         Common       NEW+         global       ×         Windows Event Log       NEW+         v File Logs       NEW+         auth       Ø ×         messages       Ø ×         syslog       Ø ×         docker       Ø ×         NEW + TAG       Include files:								
Journal Logs NEW+ Exclude fields: EventId; ProviderName;								
✓ Parsers NEW+ Whitelist filter expression: level > WINLOG LEVEL SUCCESS and level < WINLOG LEVEL INFO ①								
auth_parser								
auth_Parser_sles $\partial \times$								
syslog_parser								
syslog_appname_parser 🖉 🗙 😓								
SAVE								

- 3. Next to File Log Click **New**, name the section **syslog** 
  - Set the Directory to: /var/log
  - Set Include files to: syslog;syslog.?
  - Tag Field click **New Tag** 
    - set the field to vmc\_cp
    - set the value to **linux**
  - Set Parse fields by to: **syslog\_parser**

Agent Configuration (	
In order to centrally manage agent group config	urations, use one of the methods below.
The Build tab provides prompts with a graphical	user interface. Alternatively, the Edit tab allows you to edit the configuration file manually.
Build Edit	
logging	× [filelog syslog]
∽ Common	NEW+
global	X Directory: /var/log (1) Enabled: V
Windows Event Log	NEW+ Event marker: ① Character set: UTF-8 ①
∽ File Logs	NEW+ Include files: syslog;syslog;? (i) Exclude files: hidden.log; secur?. (i)
auth	
messages	ℓ × Tags (j)
syslog	Ø× vmw_cp linux ⊙
docker	
Journal Logs	NEW+ Exclude fields: EventId; ProviderName;
✓ Parsers	NEW+ Whitelist filter expression: level > WINLOG LEVEL SUCCESS and level < WINLOG LEVEL INFO ①
auth_parser	
auth_Parser_sles	Blacklist filter expression: <u>EventiD == 4688 or EventiD == 5447</u> (1)
syslog_parser	Parse fields by:     syslog_parser     ①
syslog_appname_parser	
SAVE	

- 4. Next to File Log Click **New**, name the section **docker** 
  - Set the Directory to: /var/log
  - Set Include files to: docker
  - Tag Field click **New Tag** 
    - set the field to vmc\_cp
    - set the value to **linux**
  - Set Parse fields by to: **syslog\_parser**

Agent Configuration ()									
In order to centrally manage agent group configurations, use one of the methods below.									
The Build tab provides prompts with a graphical user interface. Alternatively, the Edit tab allows you to edit the configuration file manually.									
Build Edit									
logging	×	[filelog docker]							
V Common	NEW+								
global	×	Directory: (i) Enabled: 🗹							
Windows Event Log	NEW+	Event marker: () Character set: UTF-8 · ()							
✓ File Logs	NEW+	Include files: docker (i) Exclude files: hidden.log; secur?. (j)							
auth	$\mathscr{O}$ ×	Raw Syslog: 🗌 🚯							
messages	0×	Tags ()							
syslog	0×	No tags added							
docker	0×								
Journal Logs	NEW+	Exclude fields:EventId; ProviderName; (1)							
✓ Parsers	NEW+	Whitelist filter expression: <u>level &gt; WINLOG_LEVEL_SUCCESS</u> and level < WINLOG_LEVEL_INFO	)						
auth_parser	0×	Blacklist filter expression: EventID == 4688 or EventID == 5447	>						
auth_Parser_sles	$\mathscr{O}$ ×	Parse fields by: None ①							
syslog_parser	$\mathscr{O}$ ×								
syslog_appname_parser	0 × 📮								
SAVE									

16. At the top of the VMware Aria Operations for Logs Agents page choose **All Agents** in the search field

VMware A	ria Operat	tions for L	ogs Agents								
All Agents          ✓					~						
			Search for group Active Groups				C Aut	) Auto-update of configuration () Auto-upgrade of version ()			
All Agents			All Agents								
			Linux_29					:			3 Agent(s) 🚺
IP Address	Hostname T	Version	Available Templates		ve	Events Sent	Events Sent/Sec	Dropped Events	Uptime	Status	1 τ
192.168.229.142	frontend	8.6.2.19075480	Linux	10	, 2023, 4:23:15 PM	0	0.00	0	55m 35s	Active	
192.168.229.141	queue	8.6.2.19075480	Linux - Systemd	10 10	, 2023, 4:23:06 PM	0	0.00	0	57m 15s	Active	
192.168.229.36	nats	8.6.2.19075480	Linux - Ubuntu (kern)	į 🗅	, 2023, 4:23:05 PM	0	0.00	0	59m 16s	Active	
192.168.229.71	api	8.6.2.19075480	Create New Group		, 2023, 4:23:02 PM	0	0.00	0	57m 18s	Active	
192.168.229.140	mongodb	8.6.2.19075480	Obuntu 20.04.3 LTS	May ∠∠	, 2023, 4:23:16 PM	3	0.00	0	1h 1m	Active	

You should now see the agents from your Cats & Dog application, there would also be more than 10 events recorded. Click on the Status field to sort by Active if you see multiple Disconnected agents.

#### VMware Aria Operations for Logs Agents

			Q All Agents			~			
						<b>(</b> ) A	uto-update of configura	tion į 🔵 A	uto-upgrade of version 🕦
All Agents									23 Agent(s) 🕕
IP Address	▼ Hostname	T Version	OS	Last Active	Events Sent	Events Sent/Sec	Dropped Events	Uptime	Status 🔨 🕇
192.168.229.142	frontend	8.6.2.19075480	Ubuntu 20.04.3 LTS	May 22, 2023, 4:44:15 PM	99	0.82	0	1h 15m	Active
192.168.229.141	queue	8.6.2.19075480	Ubuntu 20.04.3 LTS	May 22, 2023, 4:44:06 PM	99	0.83	0	1h 17m	Active
192.168.229.36	nats	8.6.2.19075480	Ubuntu 20.04.3 LTS	May 22, 2023, 4:44:05 PM	98	0.82	0	1h 19m	Active
192.168.229.71	арі	8.6.2.19075480	Ubuntu 20.04.3 LTS	May 22, 2023, 4:44:03 PM	99	0.83	0	1h 17m	Active
192.168.229.140	mongodb	8.6.2.19075480	Ubuntu 20.04.3 LTS	May 22, 2023, 4:44:16 PM	102	0.82	0	1h 21m	Active

Return to the Aria Operations for Logs **Explore Logs** and observe a change in the data stream. You can adjust the time band as necessary, 5M - 30M - 1H etc.



## Conclusion