

# Lab 5 - Log Management

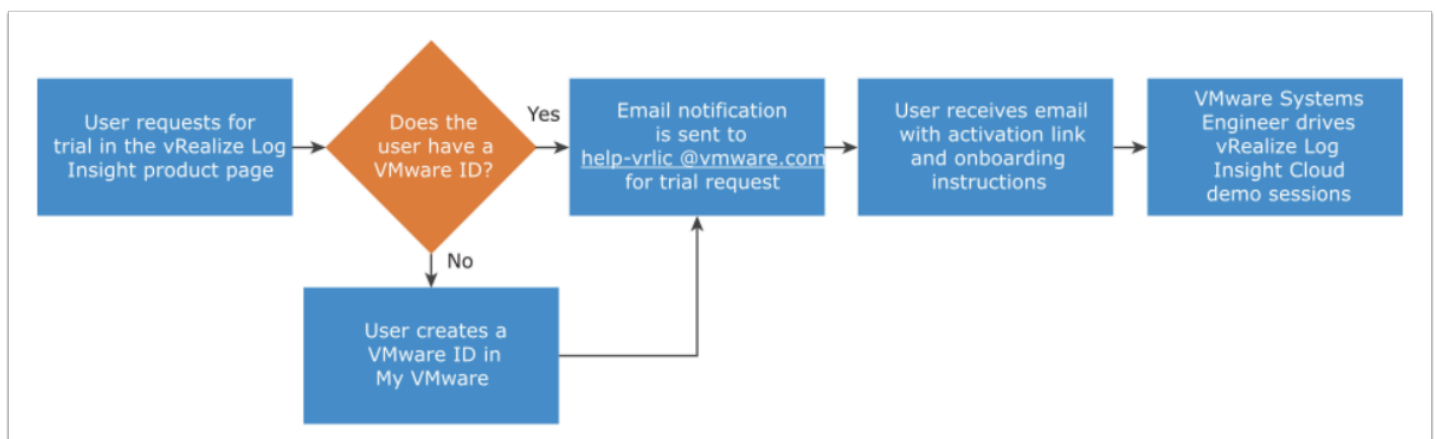
## Introduction

**i** 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..

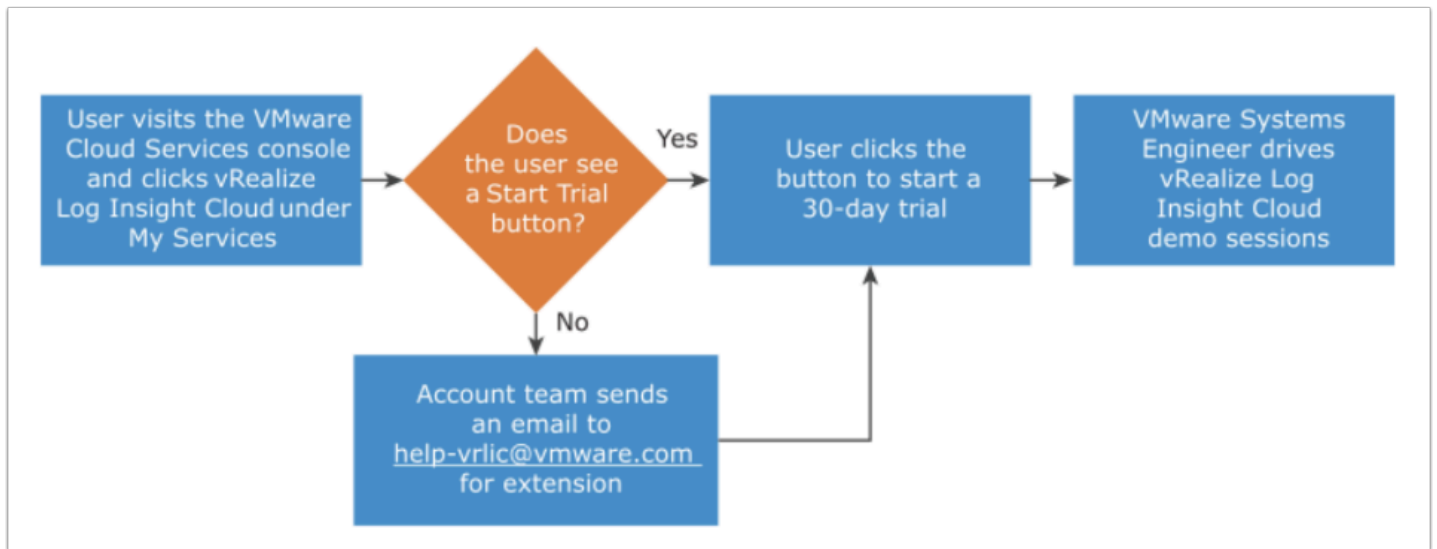
As part of the VMware Cloud suite of services, VMware Aria Operations for Logs (formerly known as vRealize Log Insight Cloud) provides a fully managed and integrated log analytics and troubleshooting service.

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  
<https://vmc.vmware.com/console/sddcs>
  - 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2 Total Unpublished Changes ACTIONS REVERT PUBLISH

ETHERNET (1) EMERGENCY (0) INFRASTRUCTURE (0) ENVIRONMENT (0) APPLICATION (4)

+ ADD POLICY + ADD RULE CLONE UNDO DELETE ... 2 Unpublished Changes Filter by Name, Path and more

	Name	ID	Sources	Destinations	Services	Context Profiles	Applied To	Action
✓	Class Log Test (1)	Applied To	DFW					Success
✓	New Rule		Any	Any	Any	None	DFW	Allow
□	Default Laye... (3)	Applied To	DFW					Success

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

**Set Source**

Rule > New Rule

Negate Selections ☐ No Negated selections will be shown as Example-Group

Groups (1) IP Addresses (0)

ADD GROUP EXPAND ALL Filter by Name, Path and more

	Name	Type	Compute Members	Status	Group Type
□	Connected VPC Prefixes	Generic	View Members	Success	System Defined
□	DirectConnect Prefixes	Generic	View Members	Success	System Defined
✓	RFC1918	Generic	View Members	Success	User Defined
□	S3 Prefixes	Generic	View Members	Success	System Defined
□	Transit Connect DGW Prefixes	Generic	View Members	Success	System Defined
□	Transit Connect External TGW Prefixes	Generic	View Members	Success	System Defined
□	Transit Connect Native VPCs Prefixes	Generic	View Members	Success	System Defined
□	Transit Connect other SDDCs Prefixes	Generic	View Members	Success	System Defined

1 REFRESH 1 - 8 of 8

Show Only Selected

CANCEL APPLY

- 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
- Publish the DFW rule by clicking the blue **Publish** button

**Set Services** ×

Rule > Allow All HTML

**Services (2)** Raw Port-Protocols (0)

× CLEAR ×

<input type="checkbox"/>	Name	Service Entries	Status
<input type="checkbox"/>	CIM-HTTP	TCP (Source: Any   Destination: 5988)	Success <span>↻</span>
<input type="checkbox"/>	CIM-HTTPS	TCP (Source: Any   Destination: 5989)	Success <span>↻</span>
<input checked="" type="checkbox"/>	HTTP	TCP (Source: Any   Destination: 80)	Success <span>↻</span>
<input checked="" type="checkbox"/>	HTTPS	TCP (Source: Any   Destination: 443)	Success <span>↻</span>
<input type="checkbox"/>	HTTPS, net.tcp binding	TCP (Source: Any   Destination: 32843,32844,32845)	Success <span>↻</span>
<input type="checkbox"/>	Office Server Web Services, ...	TCP (Source: Any   Destination: 56737,56738)	Success <span>↻</span>
<input type="checkbox"/>	ORACLE-HTTP	TCP (Source: Any   Destination: 7777)	Success <span>↻</span>
<input type="checkbox"/>	Oracle9IAS Web Cache HTTP...	TCP (Source: Any   Destination: 7779)	Success <span>↻</span>
<input type="checkbox"/>	Oracle9IAS Web Cache HTTP...	TCP (Source: Any   Destination: 4444)	Success <span>↻</span>
<input type="checkbox"/>	Oracle HTTP Server Diagnost...	TCP (Source: Any   Destination: 7200)	Success <span>↻</span>
<input type="checkbox"/>	Oracle HTTP Server Jserv port	TCP (Source: Any   Destination: 8007)	Success <span>↻</span>

☒ 2 ↻ REFRESH 1 - 30 of 30

☐ Show Only Selected

CANCEL APPLY

**Distributed Firewall** ?

All Rules Category Specific Rules

**ACTIONS** ▼ REVERT PUBLISH

ETHERNET (1) EMERGENCY (0) INFRASTRUCTURE (0) ENVIRONMENT (0) APPLICATION (4)

+ ADD POLICY + ADD RULE 📄 CLONE ↶ UNDO 🗑️ DELETE ... Filter by Name, Path and more ☰

	Name	ID	Sources	Destinations	Services	Context Profiles	Applied To	Action	
<span>⋮</span> <span>▼</span>	Class Log Test	(1)	Applied To	DFW				Success <span>↻</span>	<span>🕒</span> <span>⚙️</span>
<span>⋮</span>	Allow All HTML	1025	<span>🔗</span> RFC1918	<span>🔗</span> RFC1918	<span>🔗</span> HTTPS <span>🔗</span> HTTP	None	DFW	Allow <span>▼</span> <span>🔴</span>	<span>⚙️</span> <span>📝</span>
<span>⋮</span> <span>&gt;</span>	Default Laye...	(3)	Applied To	DFW				Success <span>↻</span>	<span>🕒</span> <span>⚙️</span>

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 ⓘ

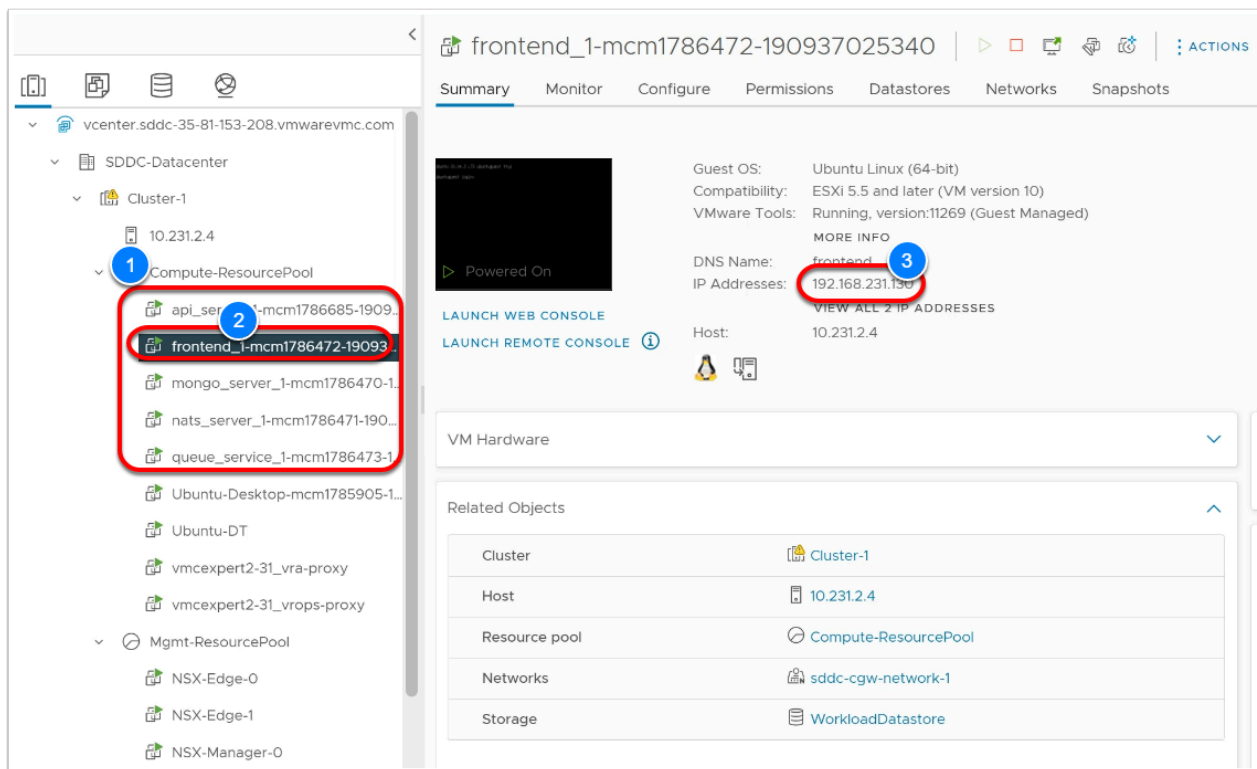
Direction In-Out ▾

Log Label vmcexpert3-03\_Test

Comments

CANCEL APPLY

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**



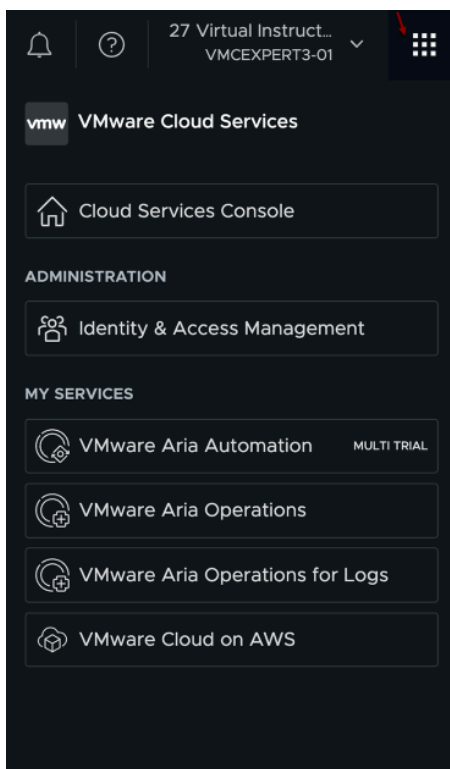
24. Select the **Ubuntu-DT** VM and click **Open Console**
25. Enter the Password of **VMware1!** if prompted
26. Launch the Firefox browser in the Ubuntu-DT VM and type in **{the address of your Frontend VM}** for the Cats & Dogs Application
27. Click the **Gato & Cachorro** buttons multiple times until 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

The image shows a dark-themed slide with six feature cards arranged in a 2x3 grid. Each card has a blue icon, a title, and a description.

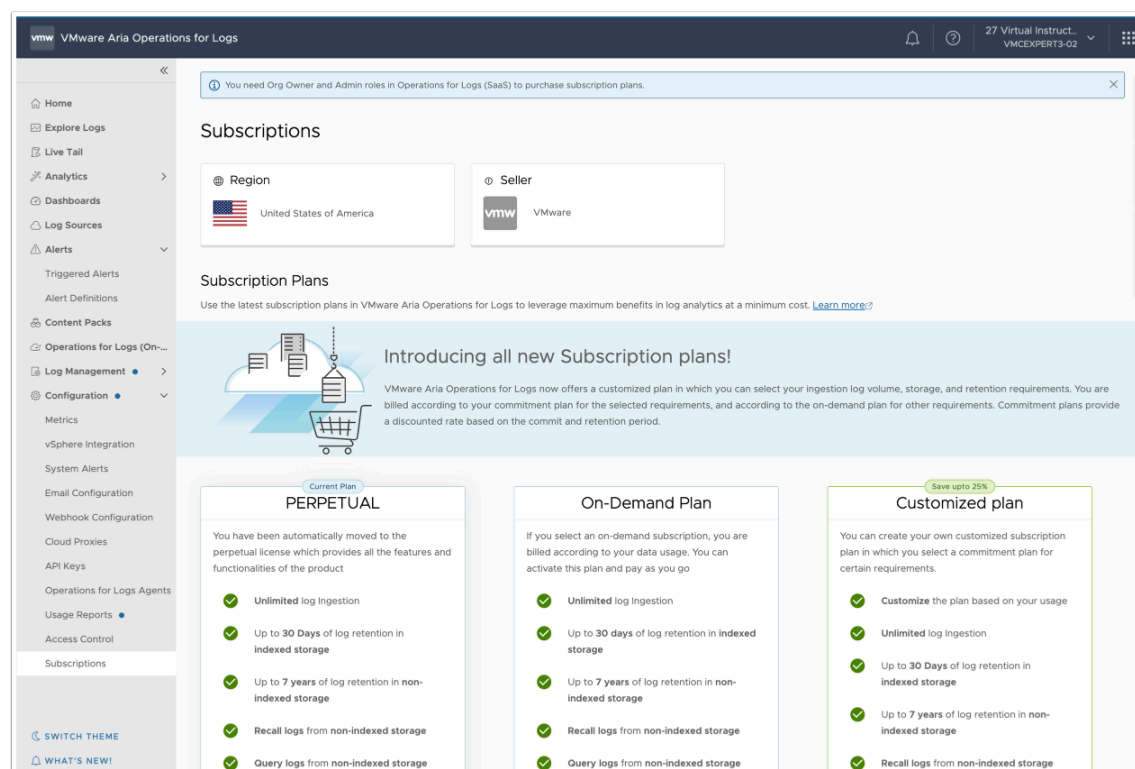
- Universal Log Collection & Analytics**: Connect to everything in your IT environment—operating systems, applications, storage, firewalls, network devices—for enterprise-wide visibility.
- Built-in VMware Cloud Knowledge**: Enable centralized analysis of your entire IT environment with built-in support for VMware Cloud technologies.
- Enterprise Scale**: In recent internal testing, Log Insight was three times faster than the leading solution in query tests across 1 billion log messages.
- Integration with vRealize Operations**: Extend operational visibility and proactive management capabilities across infrastructure and applications by integrating with [vRealize Operations](#).
- Intuitive GUI & Easy Deployment**: Easily run simple interactive searches as well as deep analytical queries for quick insights that provide immediate value and improved IT efficiency.
- Flexible Consumption**: Choose on-premises licensing or SaaS. Consume standalone, as part of [vRealize Suite](#), or as a subscription through [vRealize Cloud Universal](#).

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**

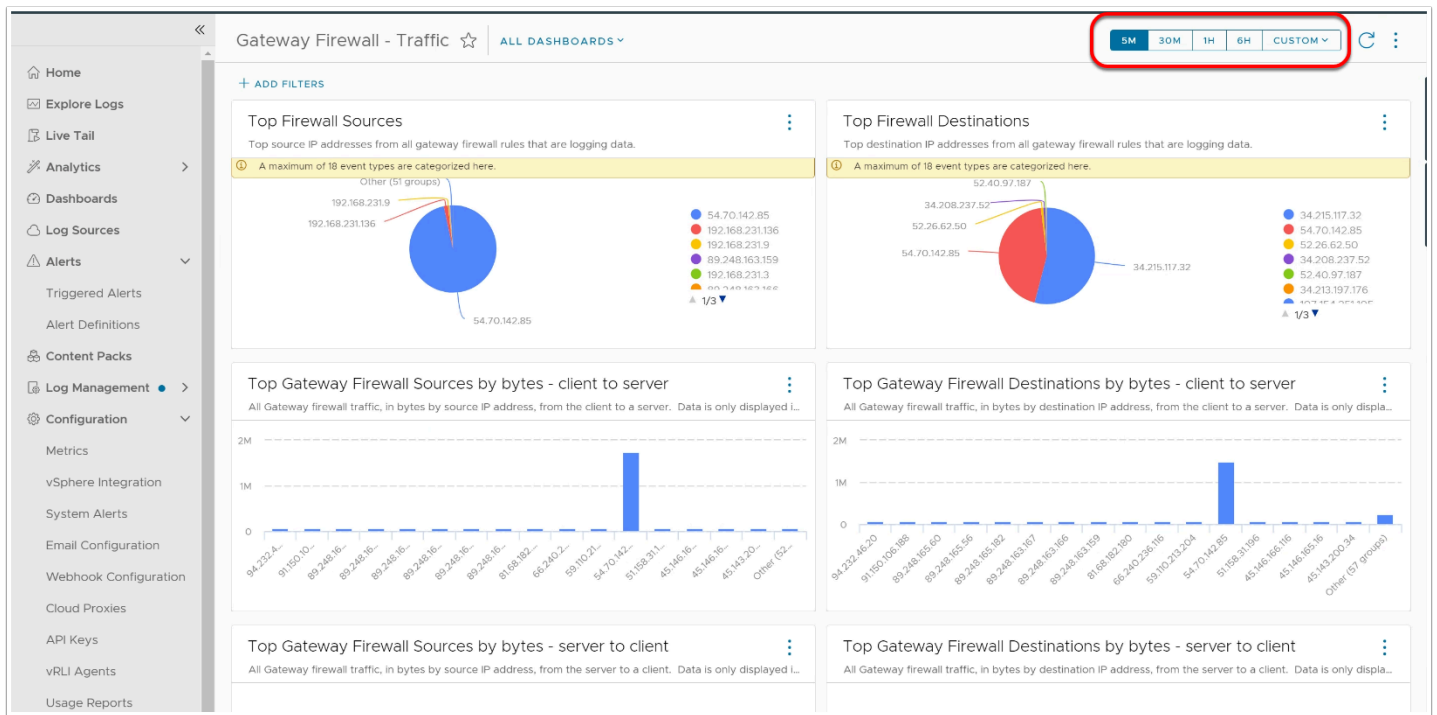
5. Notice we are using the **PERPETUAL** Subscription. This subscription comes with VMC on AWS and only allows you to view Audit logs and Firewall Logs.  
To view other types of logs (Application logs, non-SDDC logs, etc..) the subscription must be upgraded.



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.



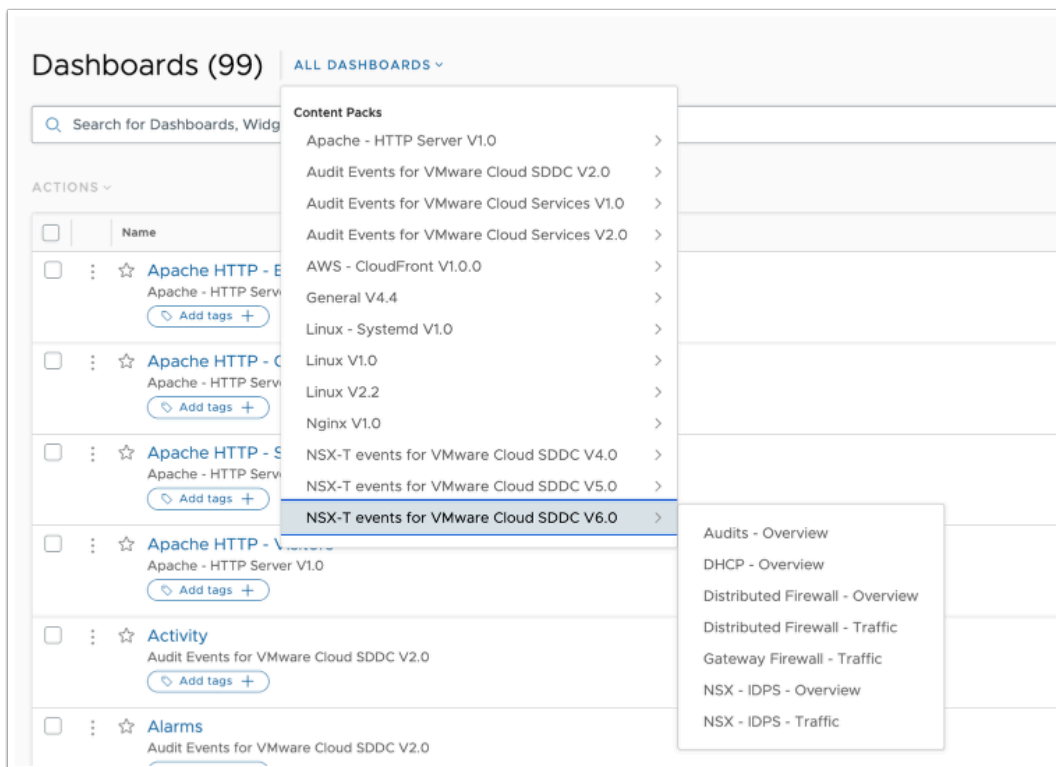


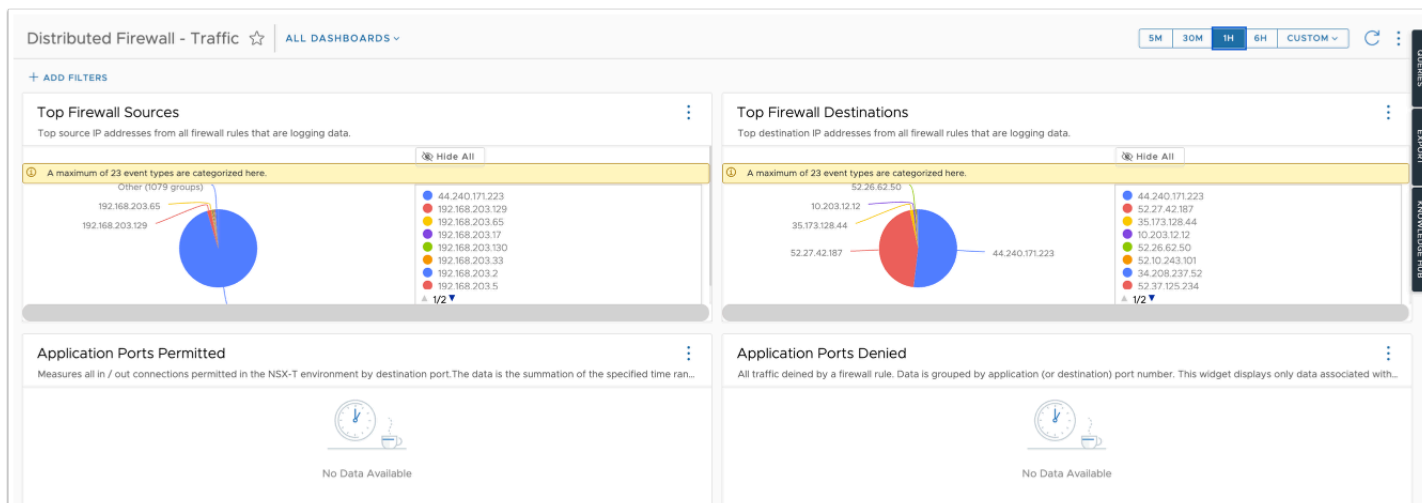
13. Select **Dashboards** in the left column

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

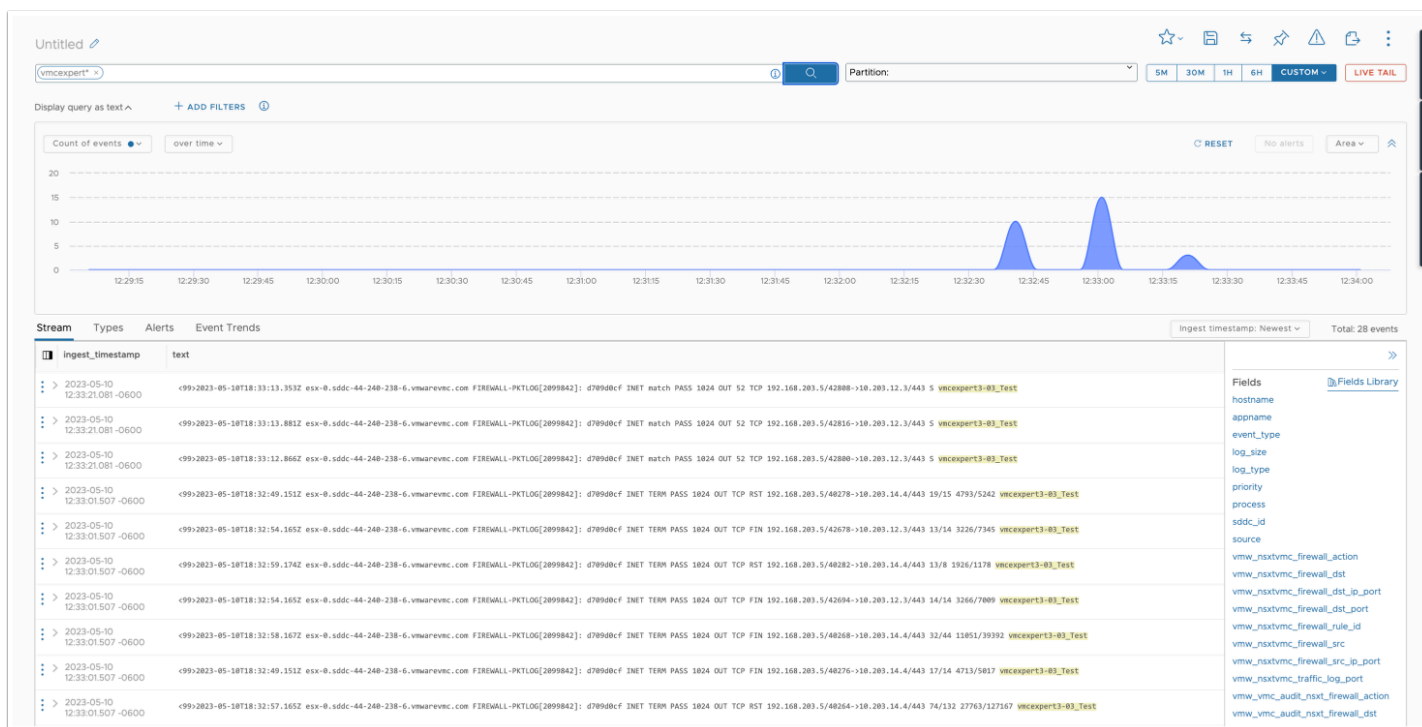




16. From the left hand navigation pane, select **Home**

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.



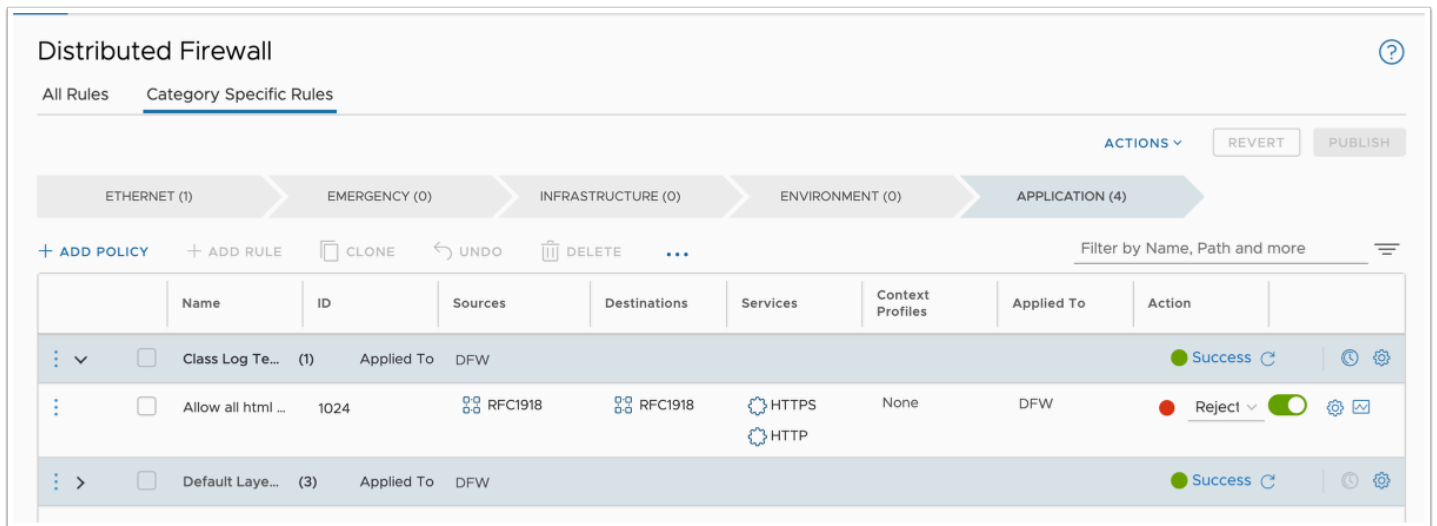
18. Return to the VMware Cloud on AWS SDDC console tab in your browser, ensuring that you are in your SDDC

- Select **Networking & Security**
- Select **Distributed Firewall** under **Security**

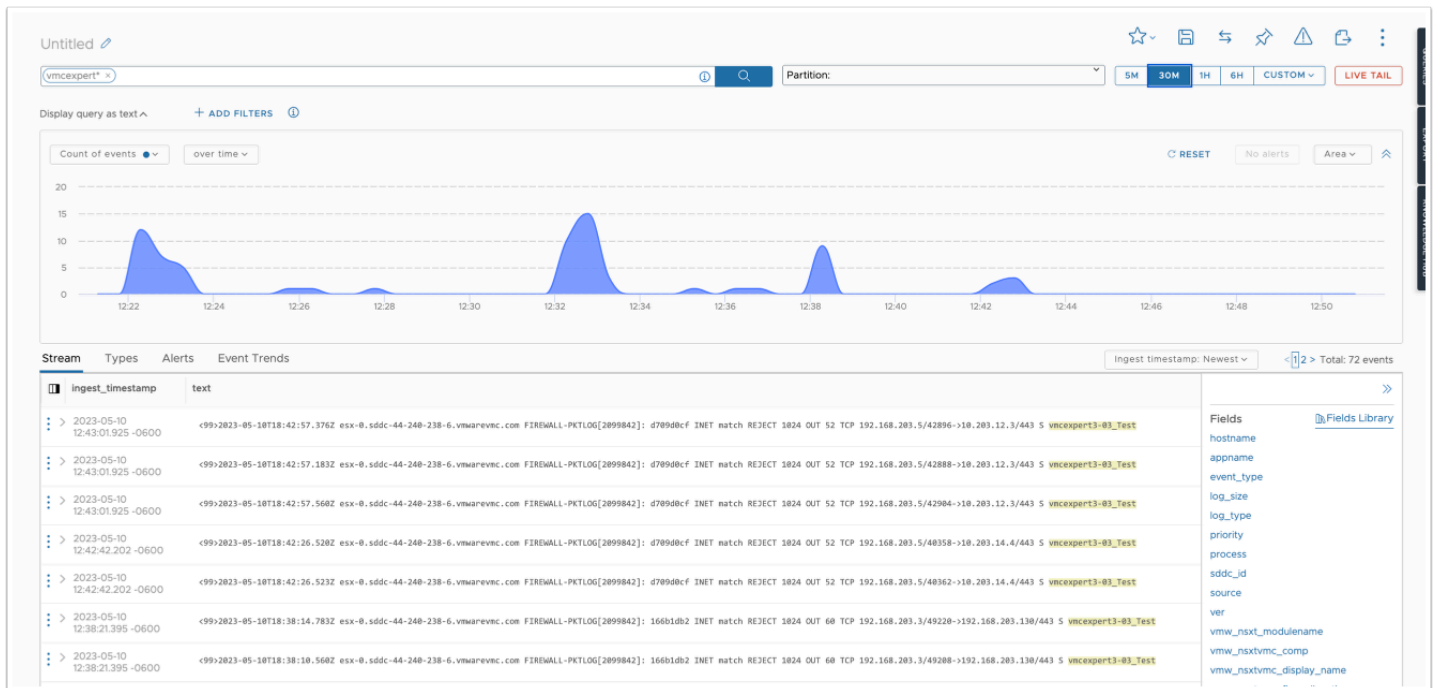
19. Open the **Class Log Test** policy to see the **Allow All HTML** rule

20. Change Allow to **Reject** under Action

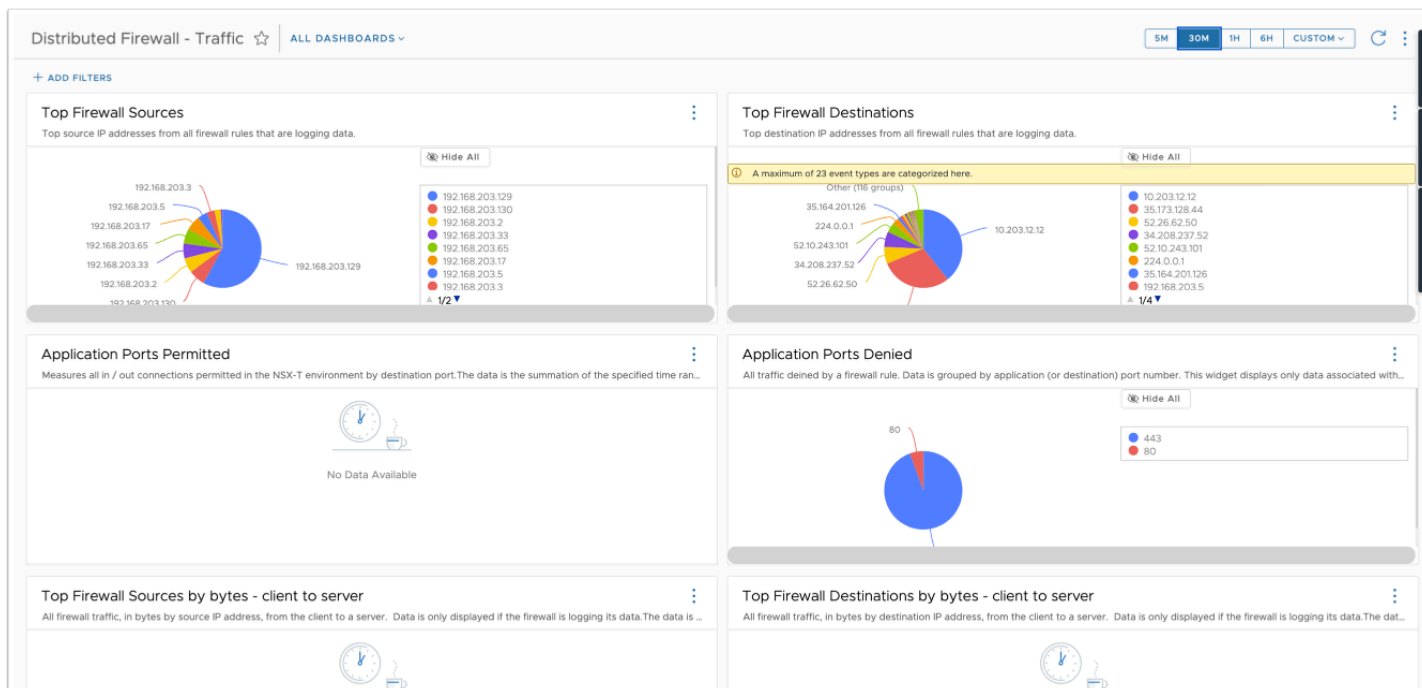
21. **Publish** the rule change



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 **REJECTED** 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



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.



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

Explore Logs

Live Tail

Analytics

Dashboards

Log Sources

Alerts

Triggered Alerts

Alert Definitions

Content Packs

Operations for Logs (On-...

Log Management

Configuration

Alert Definitions

Severity

Critical

Immediate

Warning

Info

Type

Origin

Tags

CREATE NEW


...

vcenter


ACTIONS

Sort By: Enabled First

<input type="checkbox"/>	Details	Severity	Origin	Created At
<input type="checkbox"/>	<div> <div>⌵</div> <div> <div>Audit Events for VMware Cloud SDDC   Host Connection Lost Alert</div> <div>A host that a vCenter Server system manages lost connection to vC...</div> <div> <div>⚠ Disabled forever</div> <div>Add tags</div> </div> </div> </div>	Info	Audit Events for VMware Cloud SDDC V2.0	2021-07-23 07:07:36 GMT-06:00
<input type="checkbox"/>	<div> <div>⌵</div> <div> <div>Audit Events for VMware Cloud SDDC   Host Disconnected Alert</div> <div>A host that a vCenter Server system manages got disconnected fro...</div> <div> <div>⚠ Disabled forever</div> <div>Add tags</div> </div> </div> </div>	Info	Audit Events for VMware Cloud SDDC V2.0	2021-07-23 07:07:36 GMT-06:00
<input type="checkbox"/>	<div> <div>⌵</div> <div> <div>Audit Events for VMware Cloud SDDC   Host Shut Down Alert</div> <div>A host that a vCenter Server system manages got shutdown becau...</div> <div> <div>⚠ Disabled forever</div> <div>Add tags</div> </div> </div> </div>	Info	Audit Events for VMware Cloud SDDC V2.0	2021-07-23 07:07:36 GMT-06:00
<input type="checkbox"/>	<div> <div>⌵</div> <div> <div>Audit Events for VMware Cloud SDDC   User Session Login Alert</div> <div>User logs in to a vSphere component or when a vCenter Server solu...</div> <div> <div>⚠ Disabled forever</div> <div>Add tags</div> </div> </div> </div>	Info	Audit Events for VMware Cloud SDDC V2.0	2021-07-23 07:07:35 GMT-06:00


**VMware Aria Operations for Logs**
Inbox - Comcast 6:22 PM

**Alert: [INFO] Audit Events for VMware Cloud SDDC | User Session Login Alert**  
 To: rmougey@vmware.com


**VMware Aria Operations for Logs**  
 11 May 2023 at 12:22 AM UTC  
Info **Audit Events for VMware Cloud SDDC | User Session Login Alert**

**Description**  
 User logs in to a vSphere component or when a vCenter Server solution user accesses another vCenter Server service.

**All logs** Showing the matching result

```
<99>1 2023-05-11T00:22:04.408243+00:00 vcenter vpxd 58585 - - Event [42670] [1-1] [2023-05-11T00:22:04.405272] [vim.event.UserLoginSessionEvent] [info] [VMC.LOCAL\fleetmanagement] [] [42670] [User VMC.LOCAL\fleetmanagement@127.0.0.1 logged in as VMware vim-java 1.0]
```

[View alert in VMware Aria Operations for Logs \(SaaS\)](#)

VMware, Inc. 3401 Hillview Ave. Palo Alto CA 94304 USA Tel 1-877-486-9273  
Copyright © 2020 VMware, Inc. All rights reserved. VMware is a registered trademark of VMware, Inc. The content and links in this email contain information.



**Note:** 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

Enabled

Public

Private

All

VMware Cloud

Applications

Others

VMware Cloud (6)

Audit Events for VMware Cloud SDDC

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.

VERSION 2.0 Enabled Versions: V2.0

ACTIONS DETAILS

Disable

Export

Audit Events for VMware Cloud Services

This content pack provides Audit events for all the VMware Cloud Services. This includes the Governance aspect of CSP.

VERSION 2.0 Enabled Versions: V2.0

ACTIONS DETAILS

General

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 4.4 Enabled Versions: V4.4

ACTIONS DETAILS

NSX - Audit Events for VMware Cloud SDDC

This content pack provides powerful insights into the NSX-T firewall rules, packet traffic rules created in VMware cloud SDDC along with audit details allowing administrators to audit, monitor and troubleshoot the behavior of configured rules in their environment.

VERSION 6.0 Enabled Versions: V6.0,V5.0,V4.0

ACTIONS DETAILS

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 Enabled Versions: V1.4,V1.0

ACTIONS DETAILS

VMware - NSX-T 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 3.2 Enabled Versions: V3.2,V3.1

ACTIONS DETAILS

Applications (1)

Apache - HTTP Server

Apache HTTP Server, often referred to as just Apache, is an open-source web server. Like many web servers, Apache leverages the Apache Common Log Format (CLF) for web request logging.

VERSION 1.0 Enabled Versions: V1.0

ACTIONS DETAILS

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

Content Packs

EXPORT CONTENT

Enabled

Public

Private

All

VMware Cloud

VMware Products

Infrastructure

Applications

Cloud Services

Others

Applications (12)

Apache - CLF

This content pack supports any application that follows the Apache Common Log Format (CLF). This includes following load balancers and web servers and is not limited to only them.

VERSION 1.3

ENABLE DETAILS

Apache - HTTP Server

Apache HTTP Server, often referred to as just Apache, is an open-source web server. Like many web servers, Apache leverages the Apache Common Log Format (CLF) for web request logging.

VERSION 1.0 Enabled Versions: V1.0

ACTIONS DETAILS

HAProxy

HAProxy is an open-source load balancer. Like many load balancers, HAProxy leverages the Apache Common Log Format (CLF) for web request logging.

NOTE: This content pack is for informational purposes only.

VERSION 1.0

ENABLE DETAILS

Kubernetes auditing

Kubernetes auditing provides content for audit logs, api server logs, scheduler logs and controller logs

VERSION 1.0

ENABLE DETAILS

Microsoft - Active Directory

The content pack for Microsoft® Active Directory® provides you with information about key entities of any AD installation's health using Operations for Logs (Saas) ability to monitor Windows® Event Logs.

VERSION 3.3

ENABLE DETAILS

Microsoft - Exchange2013+

The content pack for Microsoft® Exchange® provides you with information about key entities of any Microsoft® Exchange® installation's health using Operations for Logs (Saas) ability to collect events from one or more log files and monitor

VERSION 1.1

ENABLE DETAILS

Microsoft - IIS

The content pack for Microsoft® IIS® provides you with information about key entities of any IIS installation's health using Operations for Logs (Saas) ability to collect events from one or more log files.

VERSION 3.1

ENABLE DETAILS

Microsoft - SharePoint

The content pack for Microsoft® SharePoint® (SP) provides you with information about key entities of any SharePoint server installation's health using Operations for Logs (Saas) ability to collect events from one or more log files.

VERSION 3.0

ENABLE DETAILS

Microsoft - SQL Server

The content pack for Microsoft® SQL Server® provides you with information about key entities of any Microsoft® SQL Server® installation's health using Operations for Logs (Saas) ability to collect events from one or more log files.

VERSION 3.4

ENABLE DETAILS

MySQL

MySQL, the most popular Open Source SQL database management system, is developed, distributed, and supported by Oracle Corporation

VERSION 1.0

ENABLE DETAILS

Nginx

Nginx is an open-source web server and load balancer. Like many web servers and load balancers, Nginx leverages the Apache Common Log Format (CLF) for web request logging.

NOTE: This content pack is for informational purposes only. If

VERSION 1.0 Enabled Versions: V1.0

ACTIONS DETAILS

Disable

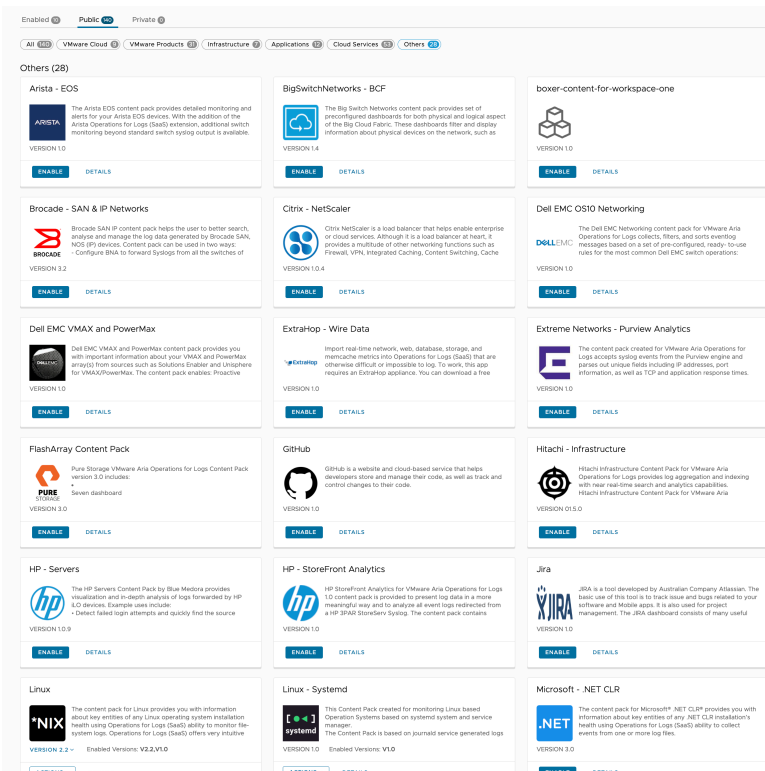
Export

Puppet Enterprise

VERSION 1.0 Enabled Versions: V1.0

ENABLE DETAILS

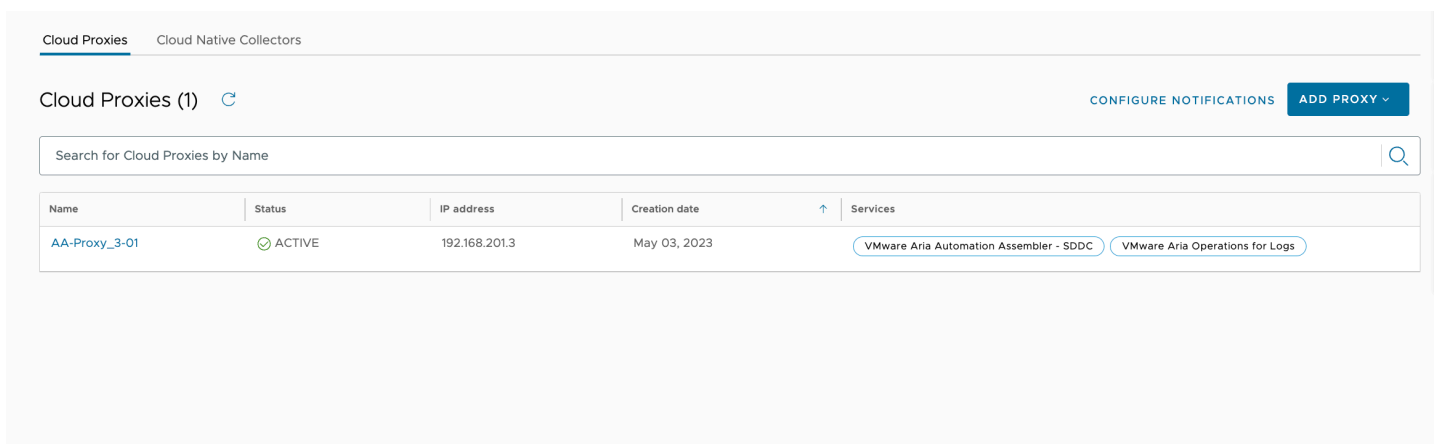
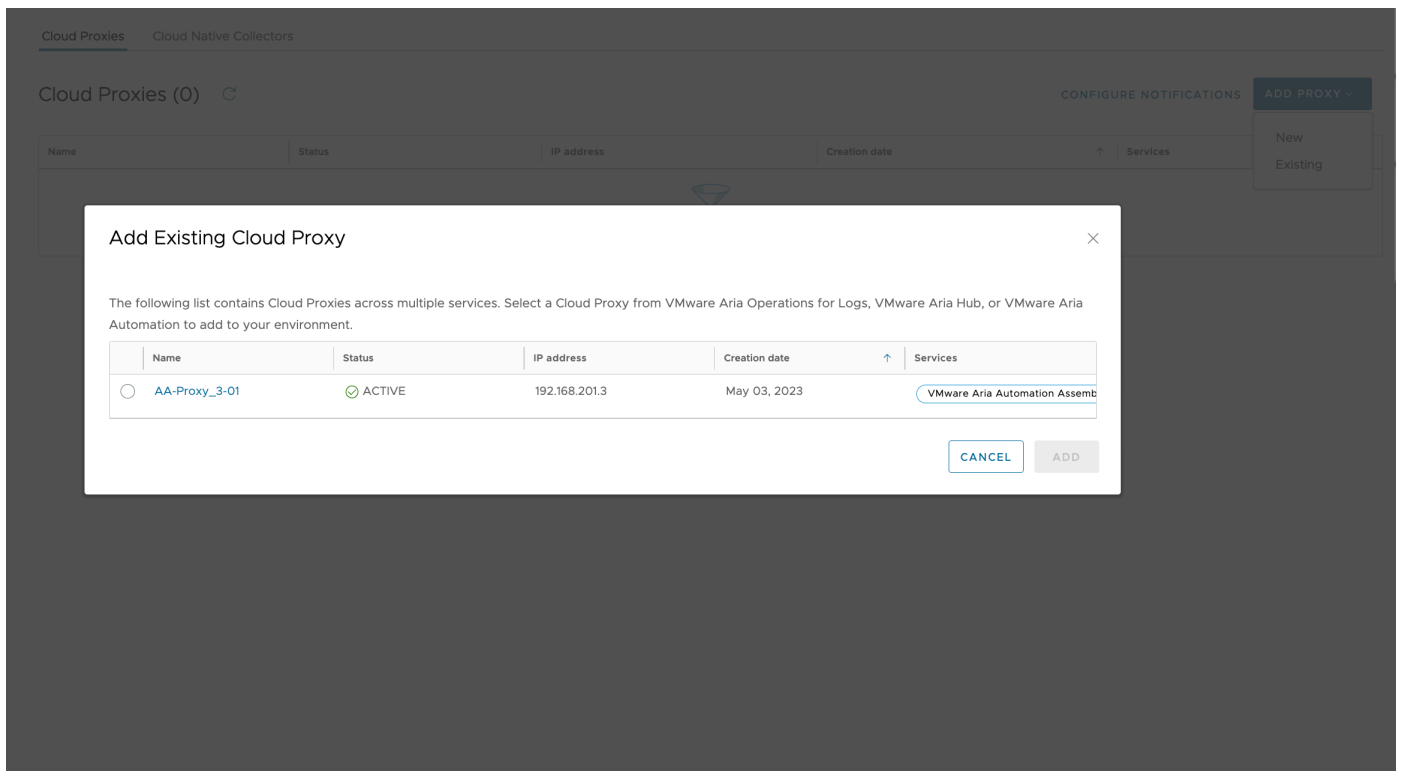




49. Click on **Dashboards**. In the search bar type the name of one of the content packs you enabled (**Linux, Nginx etc**). You'll now notice additional dashboards (Activity, Alerts, etc...)

## 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**



7. In the left pane under the **Configuration** section, click **Operations for Log Agents**
8. Under **Agent Configuration** click **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**

Build Edit

Servers NEW+  
General NEW+  
Common NEW+  
Windows Event Log NEW+  
File Logs NEW+  

MongoDB  
syslog  
docker

Journal Logs NEW+  
Parsers NEW+

### [filelog|MongoDB]

Directory: /var/log/mongodb Enabled: ☒

Event marker: Character set: UTF-8

Include files: \*.log Exclude files: hidden.log; secur?.

Raw Syslog: ☐

Tags  
mongodb log  
NEW TAG

Exclude fields: EventId; ProviderName; ...

Whitelist filter expression: level > WINLOG\_LEVEL\_SUCCESS and level < WINLOG\_LEVEL\_INFO

Blacklist filter expression: EventID == 4688 or EventID == 5447

Parse fields by: None

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**

VMware Aria Operations for Logs Agents

Search for group

Available Templates

- Linux
- Linux
- Linux - SLES (warn)
- Linux - SLES (warn)
- Linux - Systemd
- Linux - Ubuntu (kern)
- Linux - Ubuntu (kern)

Create New Group

0 Agent(s)

IP Address	Hostname	Version	Events Sent	Events Sent/Sec	Dropped Events	Uptime	Status
No agents found							

1 - 10 of 0 agents

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

Servers NEW+  
General NEW+  
Common NEW+  
Windows Event Log NEW+  
File Logs NEW+  

MongoDB  
syslog  
docker

Journal Logs NEW+  
Parsers NEW+

### [filelog|docker]

Directory: /var/lib/docker/containers Enabled: ☒

Event marker: Character set: UTF-8

Include files: \*.log Exclude files: hidden.log; secur?.

Raw Syslog: ☐

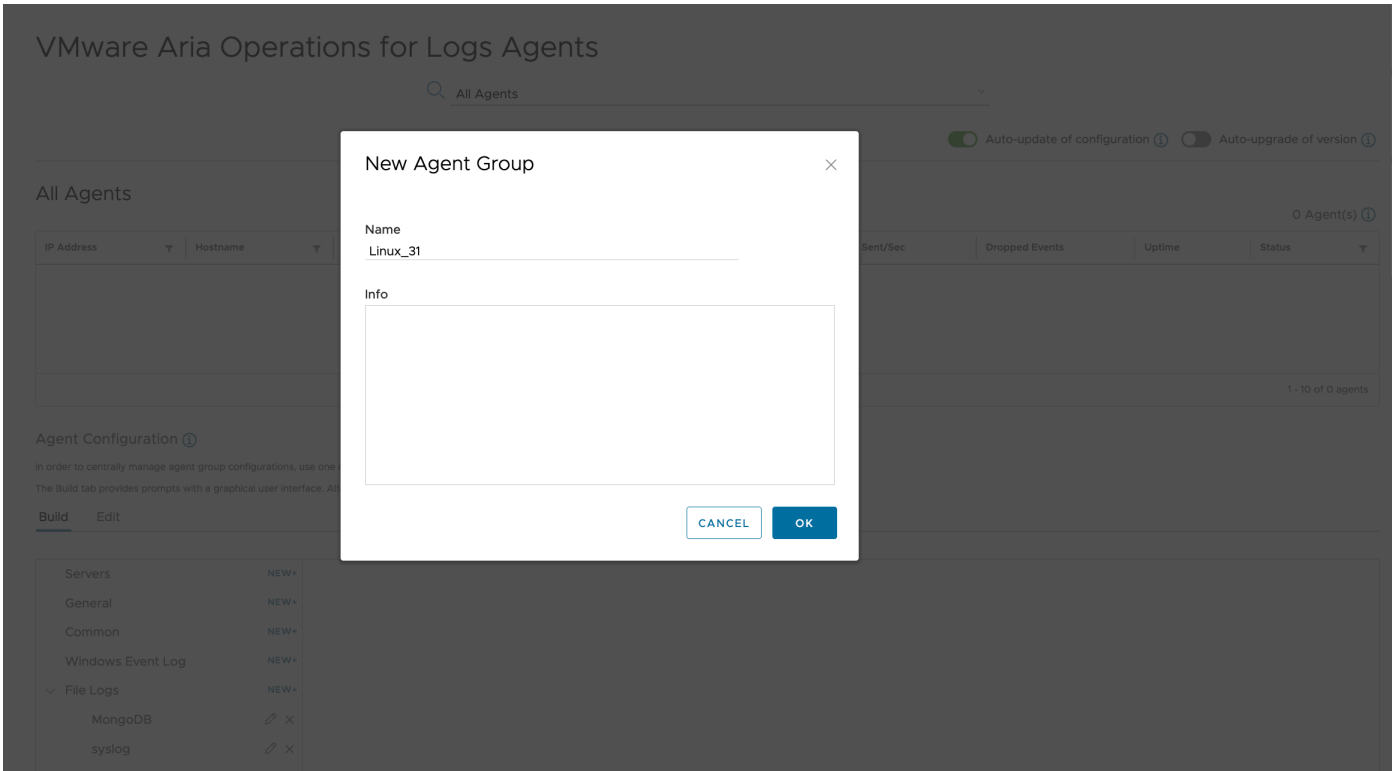
Tags  
No tags added  
NEW TAG

Exclude fields: EventId; ProviderName; ...

Whitelist filter expression: level > WINLOG\_LEVEL\_SUCCESS and level < WINLOG\_LEVEL\_INFO

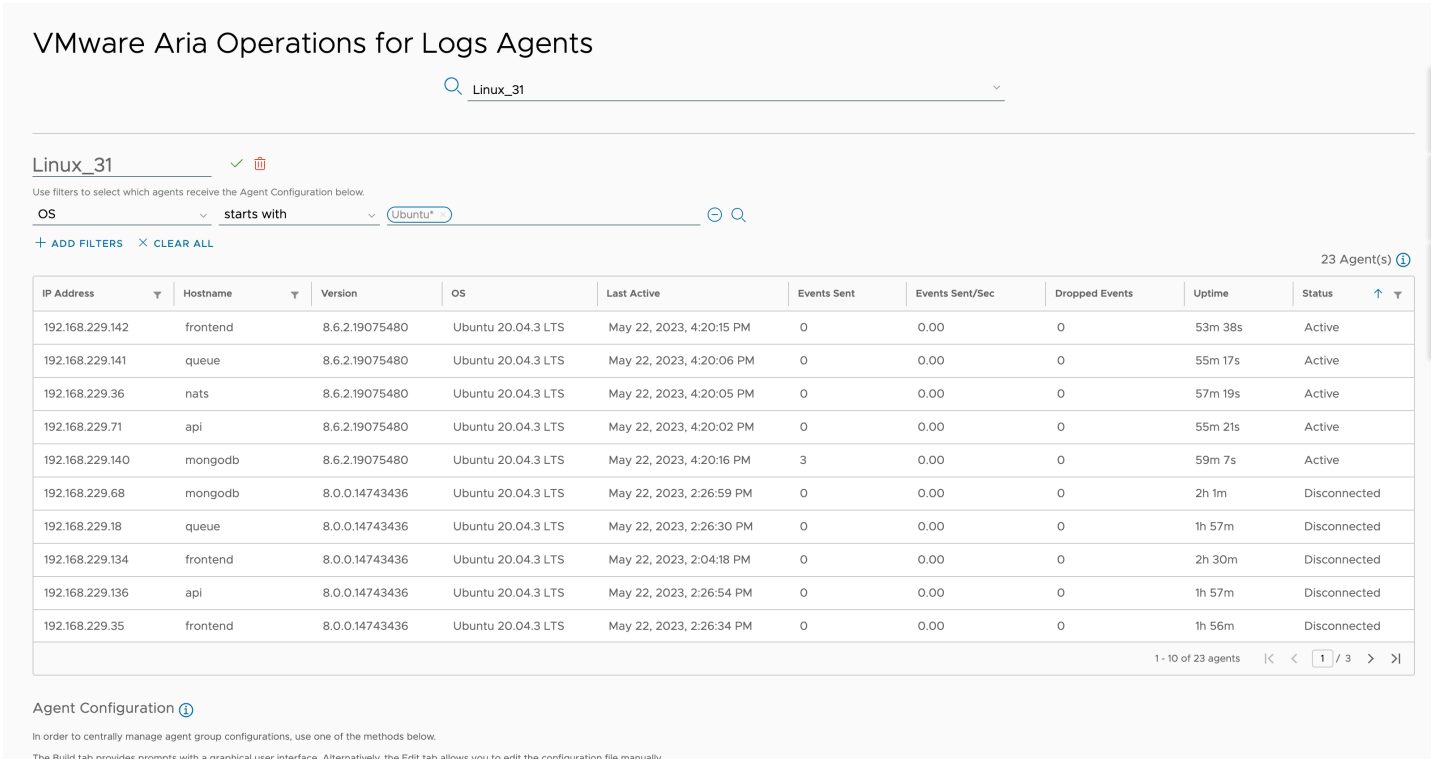
Blacklist filter expression: EventID == 4688 or EventID == 5447

Parse fields by: None



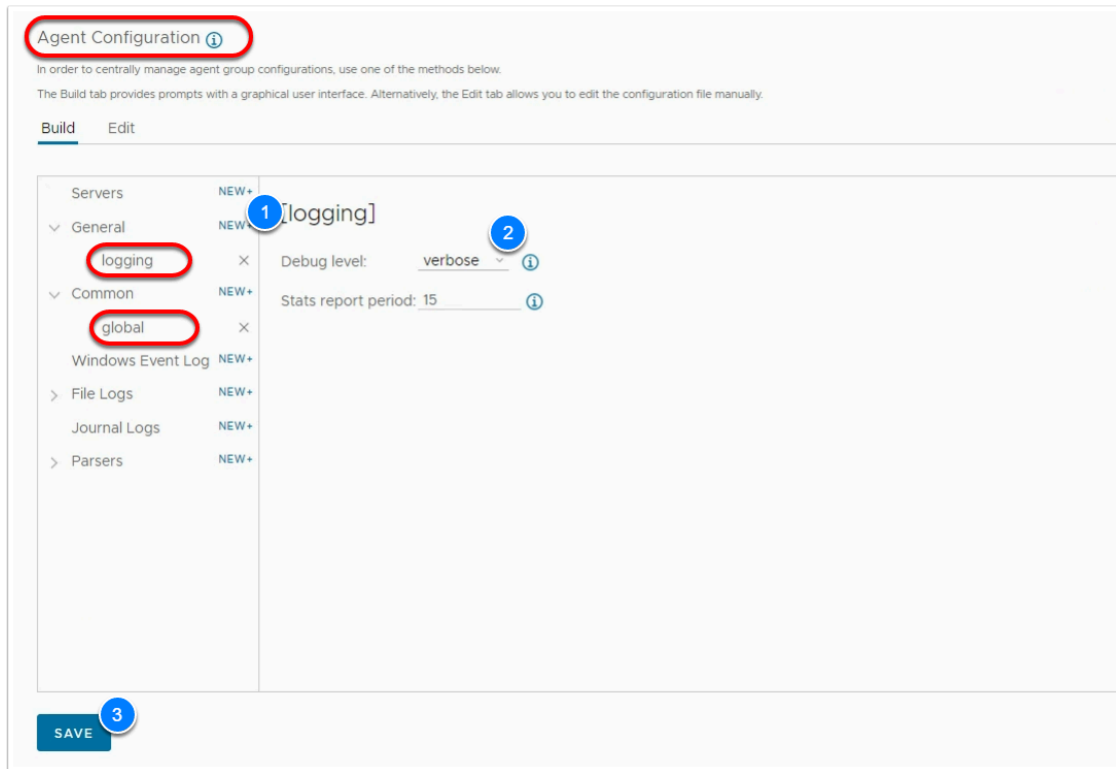
12. Configure the Group as follows:

- Filter
  - OS
  - Starts with
  - Ubuntu\*



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**



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:

```
<p>{%appname}i[%{thread_id}i]</p>
```

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:

```
<p>%t %i {%appname}i: %M</p>
```

Click to copy  
Click **Save**

- 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:

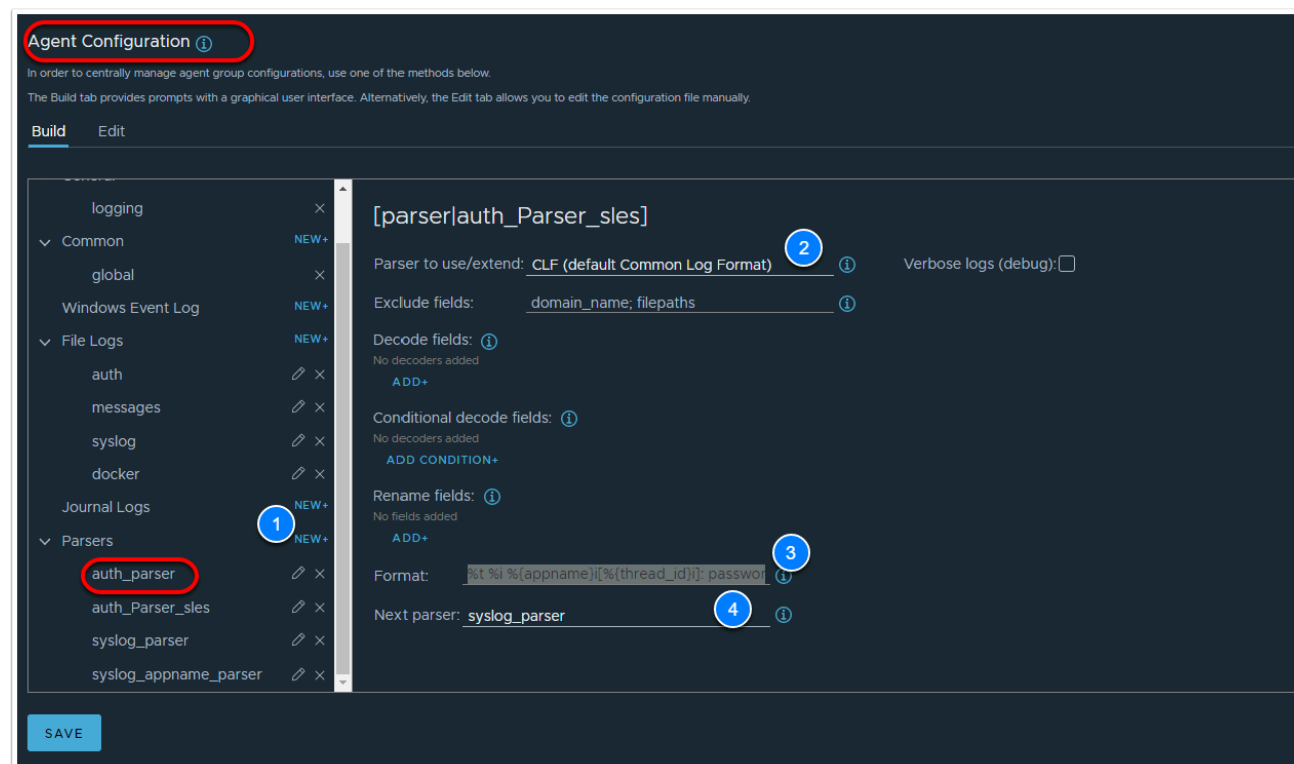
```
<p>%t %i %{appname}i[%{thread_id}i]: password changed - account=%{linux_user}i, uid=%{uid}i, %i</p>
```

Click to copy  
Click **Save**

- 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:

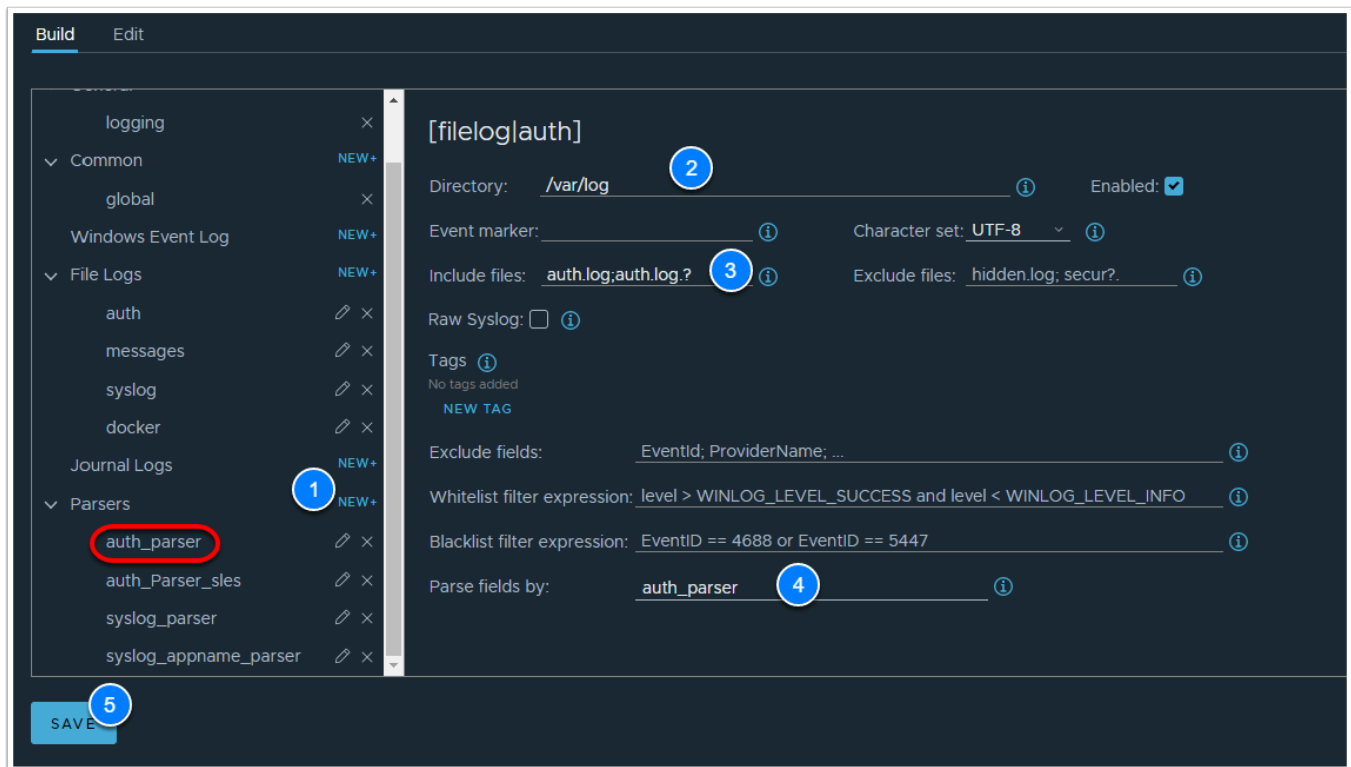
```
<p>%t %i %{appname}i[%{thread_id}i]: password changed - account=%{linux_user}i, uid=%{uid}i, %i</p>
```

Click to copy  
Click **Save**



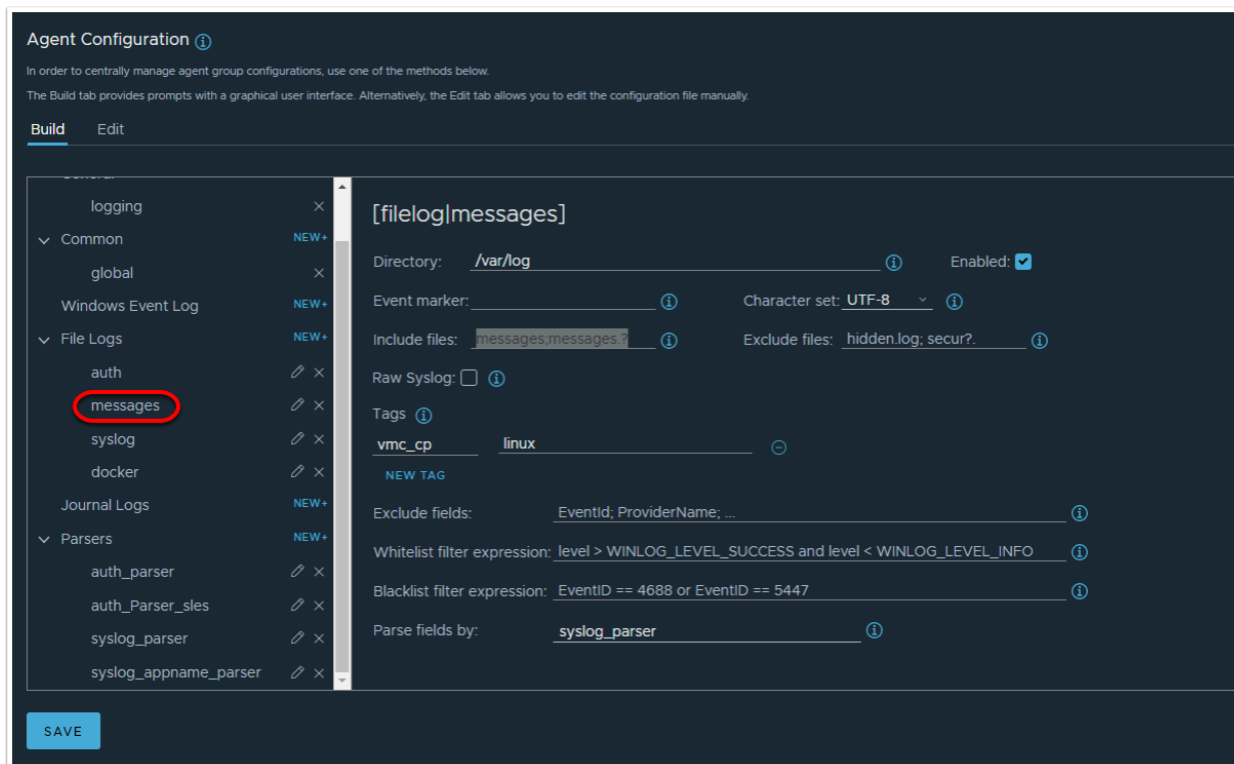
- In the Agent Configuration section, Under File Logs, Let's create and define 4 log configurations:
  - Next to **File Log** Click **New**, name the section **auth**

- 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**



Click **Save**

- 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**



Click **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 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

global

Windows Event Log

File Logs

auth

messages

**syslog**

docker

Journal Logs

Parsers

auth\_parser

auth\_parser\_sles

syslog\_parser

syslog\_appname\_parser

[filelog]syslog]

Directory: /var/log

Event marker:

Character set: UTF-8

Include files: syslog.syslog?

Exclude files: hidden.log; secur?

Raw Syslog:

Tags

vmw\_cp linux

NEW TAG

Exclude fields: EventId; ProviderName; ...

Whitelist filter expression: level > WINLOG\_LEVEL\_SUCCESS and level < WINLOG\_LEVEL\_INFO

Blacklist filter expression: EventID == 4688 or EventID == 5447

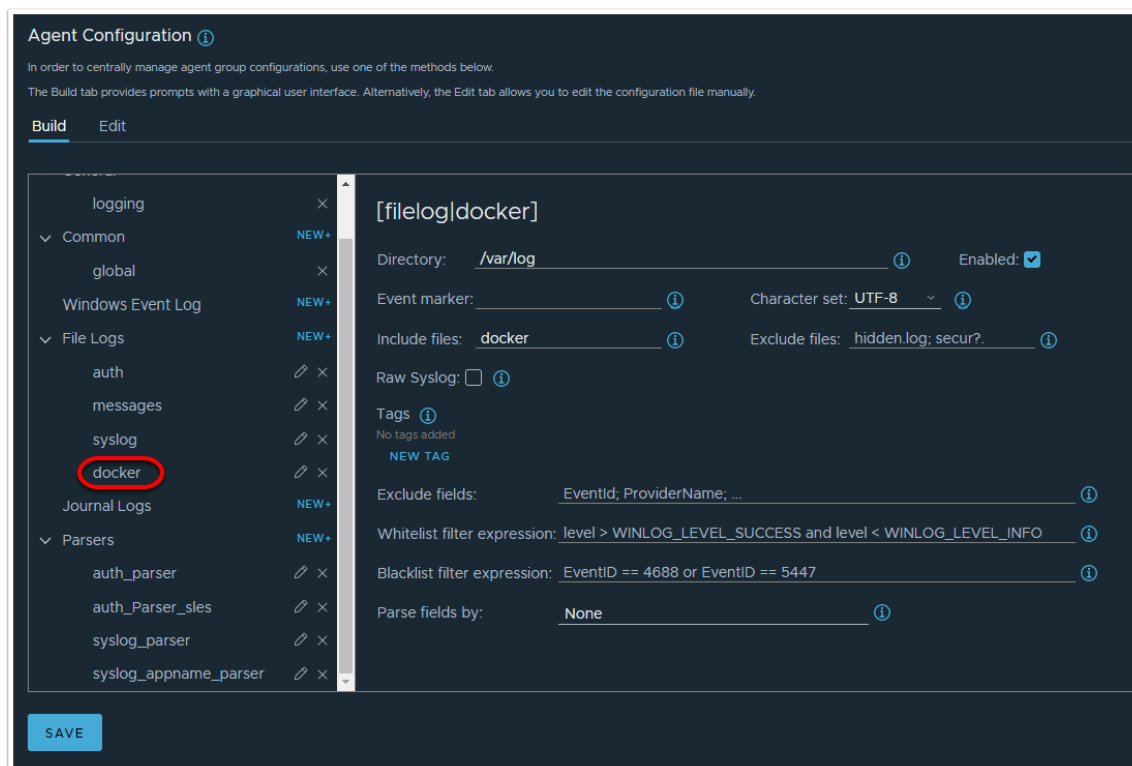
Parse fields by: syslog\_parser

SAVE

Click **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**



Click **Save**

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

VMware Aria Operations for Logs Agents

Search for group: **All Agents**

Auto-update of configuration ☒ Auto-upgrade of version ☐

**All Agents** 23 Agent(s)

IP Address	Hostname	Version	Events Sent	Events Sent/Sec	Dropped Events	Uptime	Status
192.168.229.142	frontend	8.6.2.19075480	0	0.00	0	55m 35s	Active
192.168.229.141	queue	8.6.2.19075480	0	0.00	0	57m 15s	Active
192.168.229.36	nats	8.6.2.19075480	0	0.00	0	59m 16s	Active
192.168.229.71	api	8.6.2.19075480	0	0.00	0	57m 18s	Active
192.168.229.140	mongodb	8.6.2.19075480	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

🔍 All Agents

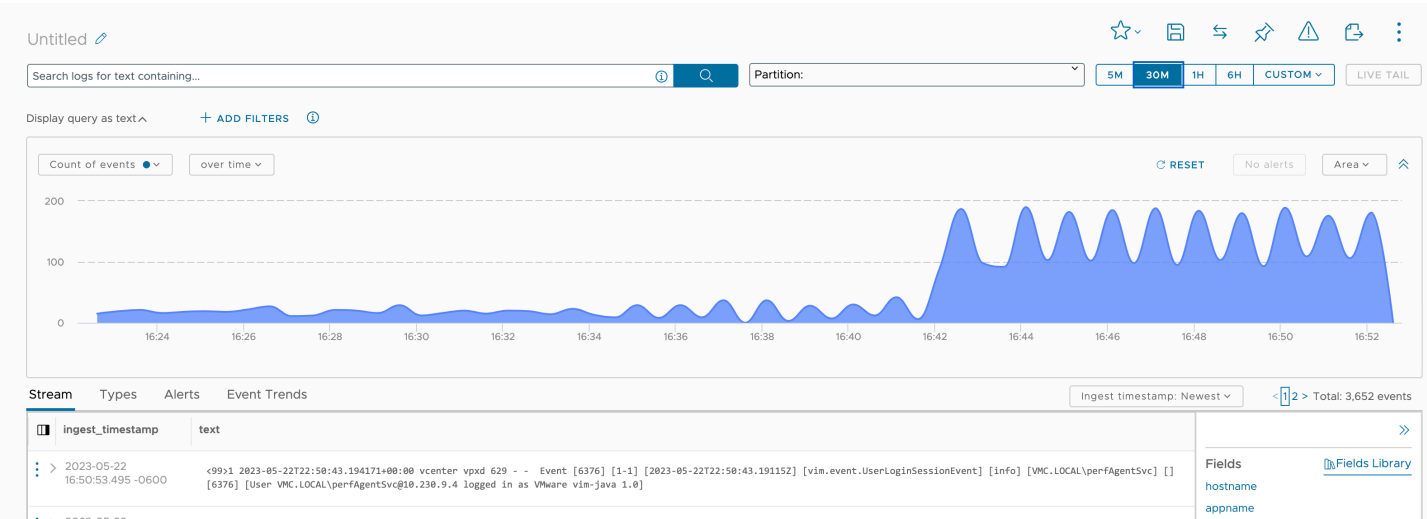
🟢 Auto-update of configuration ⓘ ⚙️ Auto-upgrade of version ⓘ

## All Agents

23 Agent(s) ⓘ

IP Address	Hostname	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	api	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