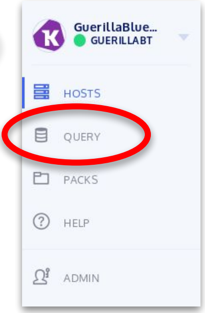
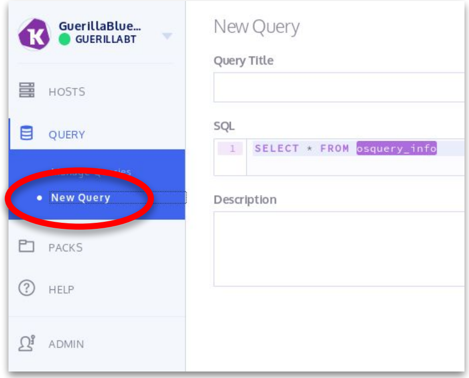
Fleet - Creating a Label

①

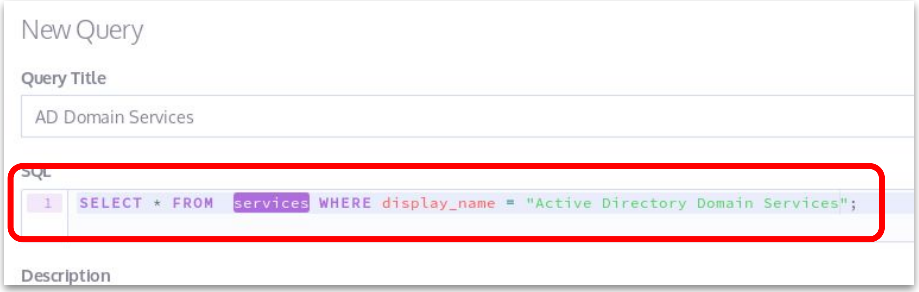


②



```
SELECT * FROM osquery_info
```

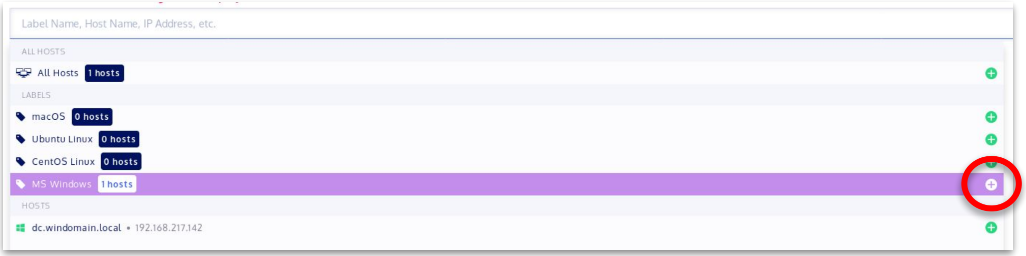
③



Query Title: AD Domain Services

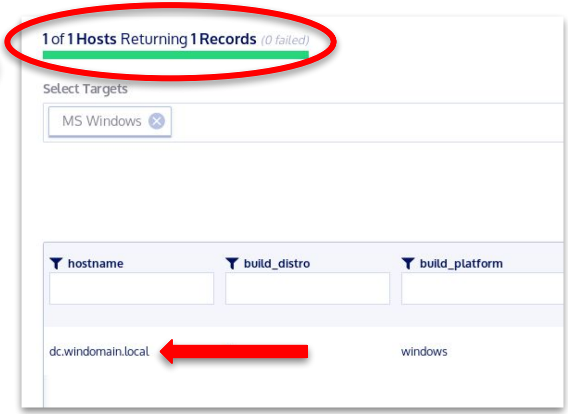
```
SELECT * FROM  services WHERE display_name = "Active Directory Domain Services";
```

④



All Hosts	1 hosts
macOS	0 hosts
Ubuntu Linux	0 hosts
CentOS Linux	0 hosts
MS Windows	1 hosts
dc.windomain.local • 192.168.217.142	

⑤

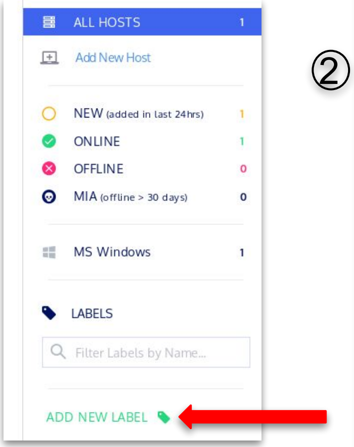


1 of 1 Hosts Returning 1 Records *(0 failed)*

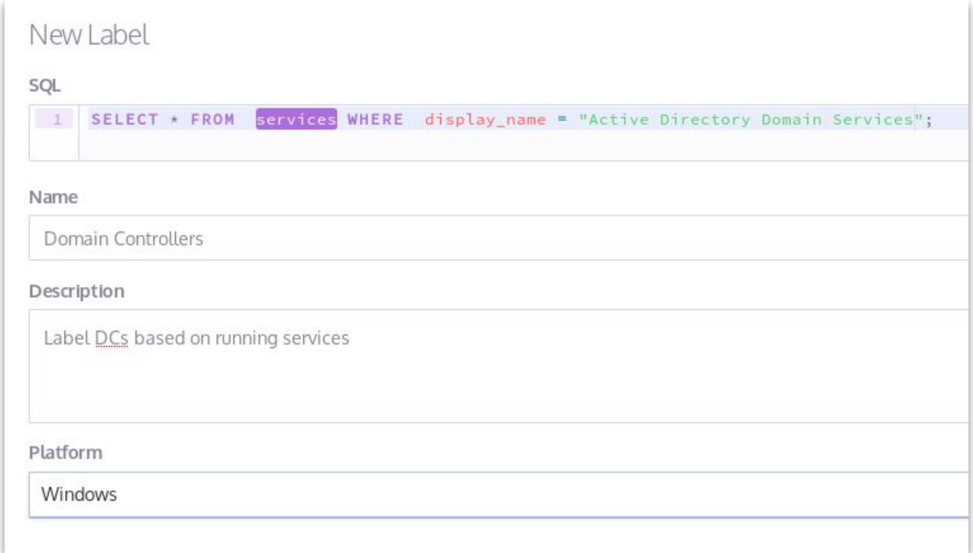
hostname	build_distro	build_platform
dc.windomain.local		windows

Fleet - Creating a Label

①



②



New Label

SQL

```
SELECT * FROM services WHERE display_name = "Active Directory Domain Services";
```

Name

Domain Controllers

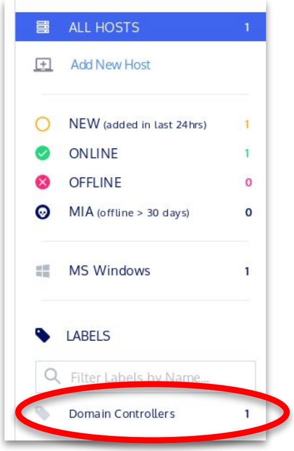
Description

Label DCs based on running services

Platform

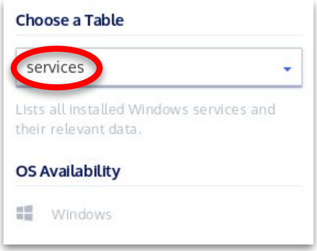
Windows

③



Fleet - Creating a Pack

①



Choose a Table

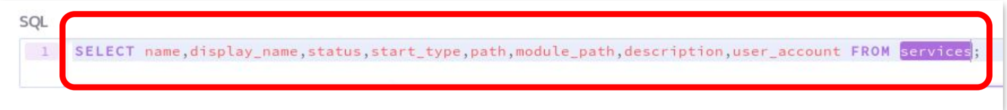
services

Lists all installed Windows services and their relevant data.

OS Availability

Windows

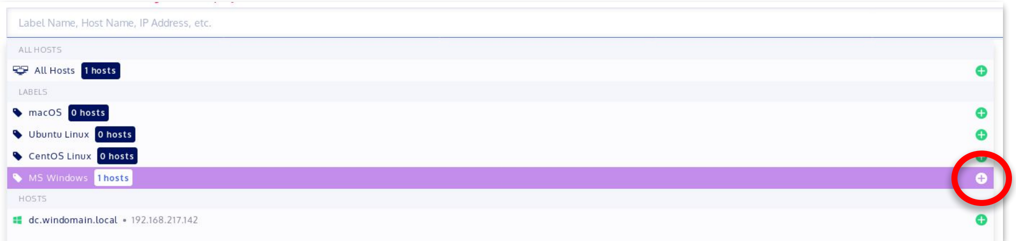
②



SQL

```
SELECT name,display_name,status,start_type,path,module_path,description,user_account FROM services;
```

③



Label Name, Host Name, IP Address, etc.

ALL HOSTS

All Hosts 1 hosts

LABELS

macOS 0 hosts

Ubuntu Linux 0 hosts

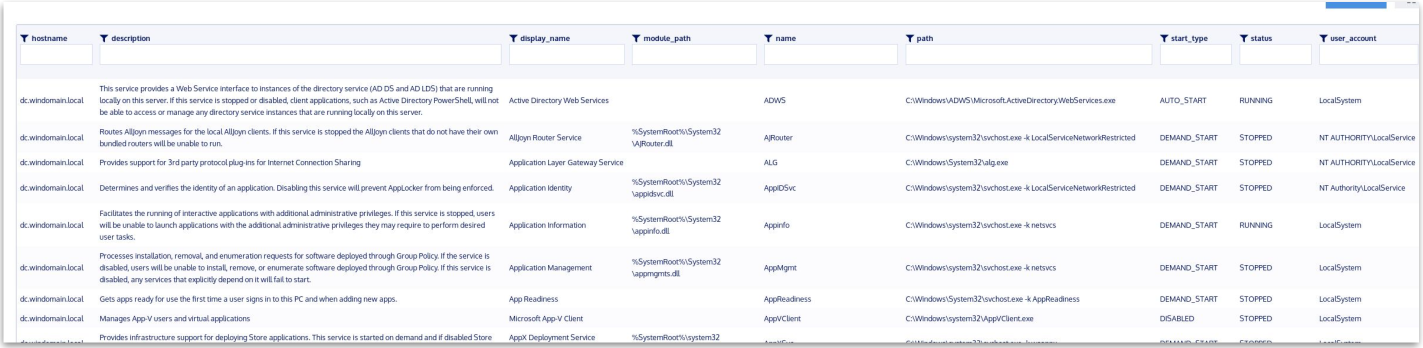
CentOS Linux 0 hosts

MS Windows 1 hosts

HOSTS

dc.windomain.local • 192.168.217.142

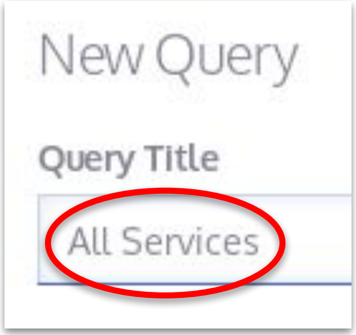
④



hostname	description	display_name	module_path	name	path	start_type	status	user_account
dc.windomain.local	This service provides a Web Service interface to instances of the directory service (AD DS and AD LDS) that are running locally on this server. If this service is stopped or disabled, client applications, such as Active Directory PowerShell, will not be able to access or manage any directory service instances that are running locally on this server.	Active Directory Web Services		ADWS	C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe	AUTO_START	RUNNING	LocalSystem
dc.windomain.local	Routes AllJoyn messages for the local AllJoyn clients. If this service is stopped the AllJoyn clients that do not have their own bundled routers will be unable to run.	AllJoyn Router Service	%SystemRoot%\System32\AJRouter.dll	AJRouter	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted	DEMAND_START	STOPPED	NT AUTHORITY\LocalService
dc.windomain.local	Provides support for 3rd party protocol plug-ins for Internet Connection Sharing	Application Layer Gateway Service		ALG	C:\Windows\System32\alg.exe	DEMAND_START	STOPPED	NT AUTHORITY\LocalService
dc.windomain.local	Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced.	Application Identity	%SystemRoot%\System32\appidsvc.dll	AppIDSvc	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted	DEMAND_START	STOPPED	NT Authority\LocalService
dc.windomain.local	Facilitates the running of interactive applications with additional administrative privileges. If this service is stopped, users will be unable to launch applications with the additional administrative privileges they may require to perform desired user tasks.	Application Information	%SystemRoot%\System32\appinfo.dll	Appinfo	C:\Windows\system32\svchost.exe -k netsvcs	DEMAND_START	RUNNING	LocalSystem
dc.windomain.local	Processes installation, removal, and enumeration requests for software deployed through Group Policy. If the service is disabled, users will be unable to install, remove, or enumerate software deployed through Group Policy. If this service is disabled, any services that explicitly depend on it will fail to start.	Application Management	%SystemRoot%\System32\appmgmts.dll	AppMgmt	C:\Windows\system32\svchost.exe -k netsvcs	DEMAND_START	STOPPED	LocalSystem
dc.windomain.local	Gets apps ready for use the first time a user signs in to this PC and when adding new apps.	App Readiness		AppReadiness	C:\Windows\System32\svchost.exe -k AppReadiness	DEMAND_START	STOPPED	LocalSystem
dc.windomain.local	Manages App-V users and virtual applications	Microsoft App-V Client		AppVClient	C:\Windows\system32\AppVClient.exe	DISABLED	STOPPED	LocalSystem
dc.windomain.local	Provides infrastructure support for deploying Store applications. This service is started on demand and if disabled Store	AppX Deployment Service	%SystemRoot%\system32	AppXSvc	C:\Windows\system32\svchost.exe -k wsappx	DEMAND_START	STOPPED	LocalSystem

Fleet - Creating a Pack

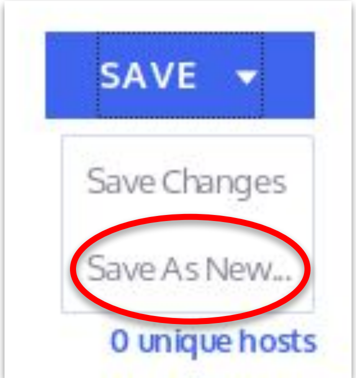
①



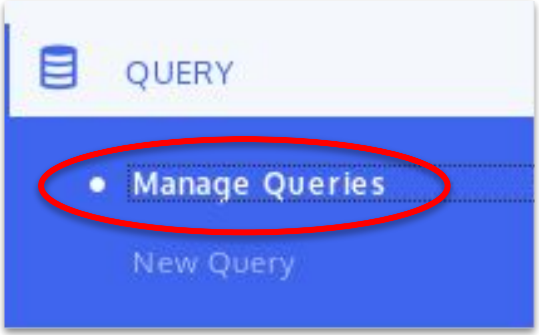
New Query

Query Title: All Services

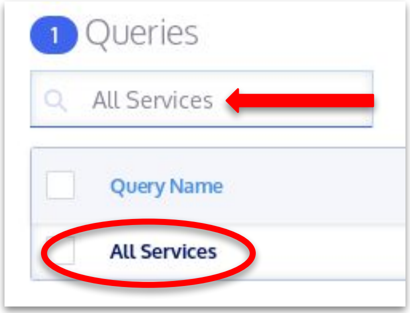
②



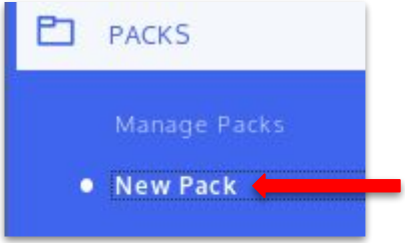
③



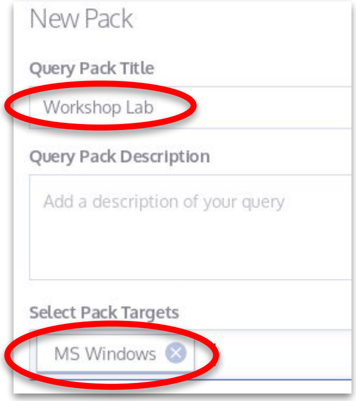
④



⑤



⑥



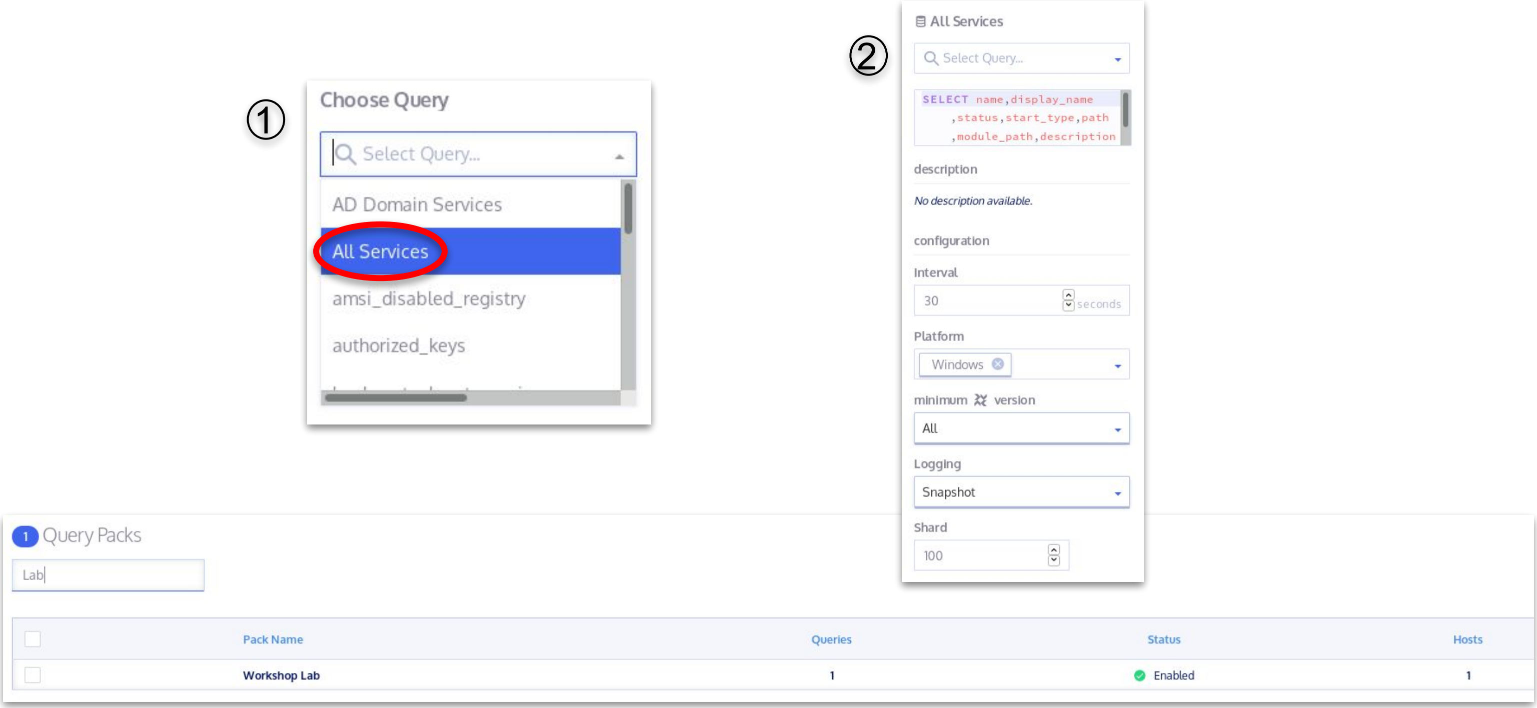
New Pack

Query Pack Title: Workshop Lab

Query Pack Description: Add a description of your query

Select Pack Targets: MS Windows

Fleet - Creating a Pack



①

Choose Query

Select Query...

AD Domain Services

All Services

amsi_disabled_registry

authorized_keys

②

All Services

Select Query...

```
SELECT name,display_name
    ,status,start_type,path
    ,module_path,description
```

description

No description available.

configuration

Interval

30 seconds

Platform

Windows

minimum version

All

Logging

Snapshot

Shard

100

③

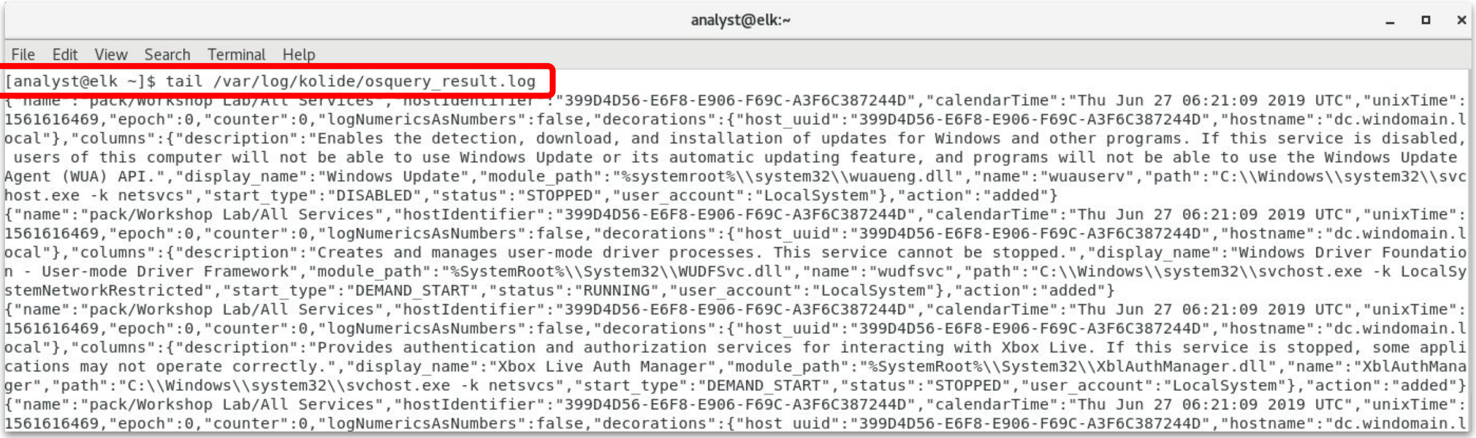
1 Query Packs

Lab

□	Pack Name	Queries	Status	Hosts
□	Workshop Lab	1	✓ Enabled	1

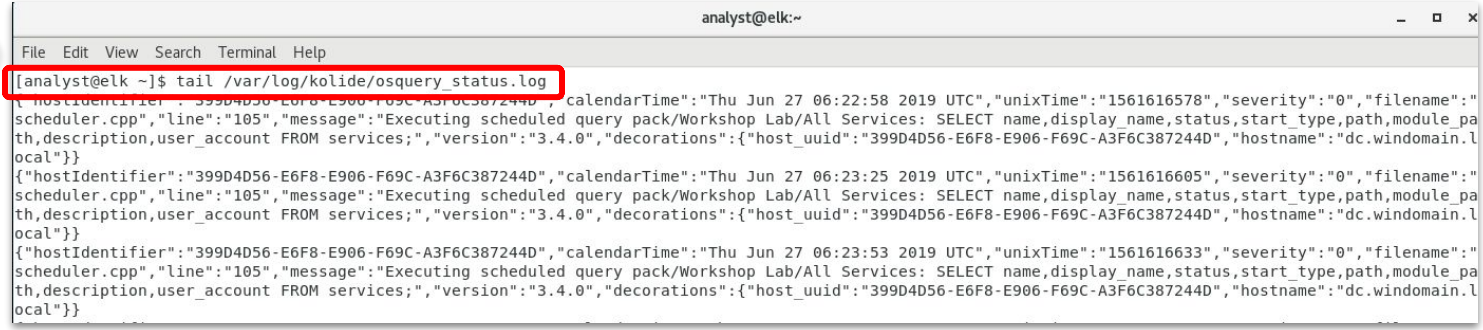
Fleet - Logging Query Results

①



```
[analyst@elk ~]$ tail /var/log/kolide/osquery_result.log
{"name":"pack/Workshop Lab/All Services","hostIdentifier":"399D4D56-E6F8-E906-F69C-A3F6C387244D","calendarTime":"Thu Jun 27 06:21:09 2019 UTC","unixTime":
1561616469,"epoch":0,"counter":0,"logNumericsAsNumbers":false,"decorations":{"host_uuid":"399D4D56-E6F8-E906-F69C-A3F6C387244D","hostname":"dc.windomain.l
ocal"},"columns":{"description":"Enables the detection, download, and installation of updates for Windows and other programs. If this service is disabled,
 users of this computer will not be able to use Windows Update or its automatic updating feature, and programs will not be able to use the Windows Update
Agent (WUA) API.","display_name":"Windows Update","module_path":"%systemroot%\\system32\\wuaueng.dll","name":"wuauserv","path":"C:\\Windows\\system32\\svc
host.exe -k netsvcs","start_type":"DISABLED","status":"STOPPED","user_account":"LocalSystem"},"action":"added"}
{"name":"pack/Workshop Lab/All Services","hostIdentifier":"399D4D56-E6F8-E906-F69C-A3F6C387244D","calendarTime":"Thu Jun 27 06:21:09 2019 UTC","unixTime":
1561616469,"epoch":0,"counter":0,"logNumericsAsNumbers":false,"decorations":{"host_uuid":"399D4D56-E6F8-E906-F69C-A3F6C387244D","hostname":"dc.windomain.l
ocal"},"columns":{"description":"Creates and manages user-mode driver processes. This service cannot be stopped.","display_name":"Windows Driver Foundatio
n - User-mode Driver Framework","module_path":"%SystemRoot%\\System32\\WUDFSvc.dll","name":"wudfsvc","path":"C:\\Windows\\system32\\svchost.exe -k LocalSy
stemNetworkRestricted","start_type":"DEMAND_START","status":"RUNNING","user_account":"LocalSystem"},"action":"added"}
{"name":"pack/Workshop Lab/All Services","hostIdentifier":"399D4D56-E6F8-E906-F69C-A3F6C387244D","calendarTime":"Thu Jun 27 06:21:09 2019 UTC","unixTime":
1561616469,"epoch":0,"counter":0,"logNumericsAsNumbers":false,"decorations":{"host_uuid":"399D4D56-E6F8-E906-F69C-A3F6C387244D","hostname":"dc.windomain.l
ocal"},"columns":{"description":"Provides authentication and authorization services for interacting with Xbox Live. If this service is stopped, some appli
cations may not operate correctly.","display_name":"Xbox Live Auth Manager","module_path":"%SystemRoot%\\System32\\XblAuthManager.dll","name":"XblAuthMana
ger","path":"C:\\Windows\\system32\\svchost.exe -k netsvcs","start_type":"DEMAND_START","status":"STOPPED","user_account":"LocalSystem"},"action":"added"}
{"name":"pack/Workshop Lab/All Services","hostIdentifier":"399D4D56-E6F8-E906-F69C-A3F6C387244D","calendarTime":"Thu Jun 27 06:21:09 2019 UTC","unixTime":
1561616469,"epoch":0,"counter":0,"logNumericsAsNumbers":false,"decorations":{"host_uuid":"399D4D56-E6F8-E906-F69C-A3F6C387244D","hostname":"dc.windomain.l
```

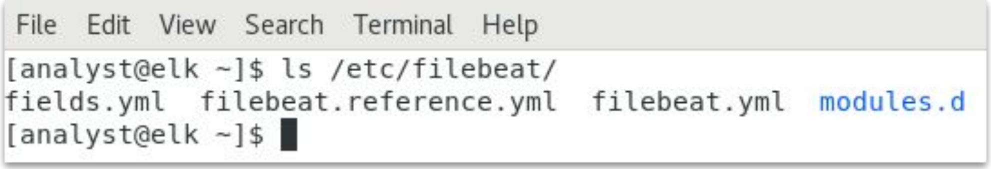
②



```
[analyst@elk ~]$ tail /var/log/kolide/osquery_status.log
{"hostIdentifier":"399D4D56-E6F8-E906-F69C-A3F6C387244D","calendarTime":"Thu Jun 27 06:22:58 2019 UTC","unixTime":"1561616578","severity":"0","filename":"
scheduler.cpp","line":"105","message":"Executing scheduled query pack/Workshop Lab/All Services: SELECT name,display_name,status,start_type,path,module_pa
th,description,user_account FROM services;","version":"3.4.0","decorations":{"host_uuid":"399D4D56-E6F8-E906-F69C-A3F6C387244D","hostname":"dc.windomain.l
ocal"}}
{"hostIdentifier":"399D4D56-E6F8-E906-F69C-A3F6C387244D","calendarTime":"Thu Jun 27 06:23:25 2019 UTC","unixTime":"1561616605","severity":"0","filename":"
scheduler.cpp","line":"105","message":"Executing scheduled query pack/Workshop Lab/All Services: SELECT name,display_name,status,start_type,path,module_pa
th,description,user_account FROM services;","version":"3.4.0","decorations":{"host_uuid":"399D4D56-E6F8-E906-F69C-A3F6C387244D","hostname":"dc.windomain.l
ocal"}}
{"hostIdentifier":"399D4D56-E6F8-E906-F69C-A3F6C387244D","calendarTime":"Thu Jun 27 06:23:53 2019 UTC","unixTime":"1561616633","severity":"0","filename":"
scheduler.cpp","line":"105","message":"Executing scheduled query pack/Workshop Lab/All Services: SELECT name,display_name,status,start_type,path,module_pa
th,description,user_account FROM services;","version":"3.4.0","decorations":{"host_uuid":"399D4D56-E6F8-E906-F69C-A3F6C387244D","hostname":"dc.windomain.l
ocal"}}
```

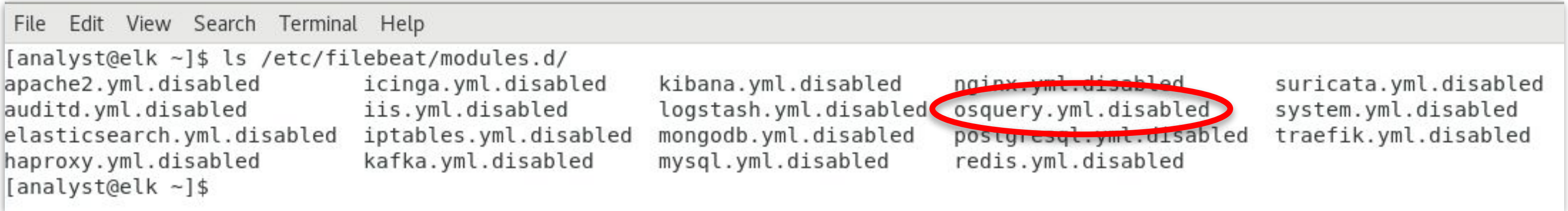
Fleet - Filebeat Config

①



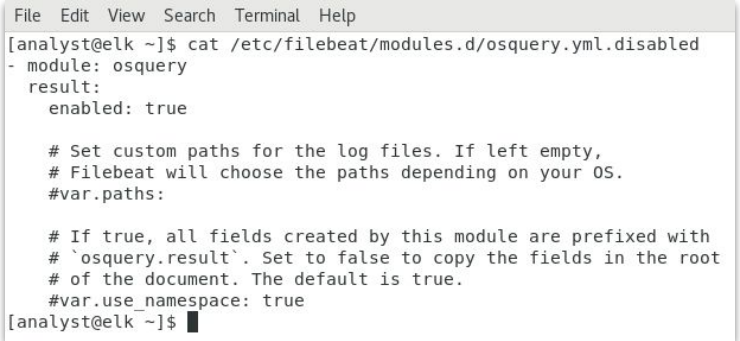
```
[analyst@elk ~]$ ls /etc/filebeat/
fields.yml  filebeat.reference.yml  filebeat.yml  modules.d
[analyst@elk ~]$ 
```

②



```
[analyst@elk ~]$ ls /etc/filebeat/modules.d/
apache2.yml.disabled        icinga.yml.disabled    kibana.yml.disabled    nginx.yml.disabled       suricata.yml.disabled
auditd.yml.disabled         iis.yml.disabled       logstash.yml.disabled  osquery.yml.disabled     system.yml.disabled
elasticsearch.yml.disabled  iptables.yml.disabled  mongodb.yml.disabled   postgresql.yml.disabled  traefik.yml.disabled
haproxy.yml.disabled        kafka.yml.disabled     mysql.yml.disabled     redis.yml.disabled
[analyst@elk ~]$
```

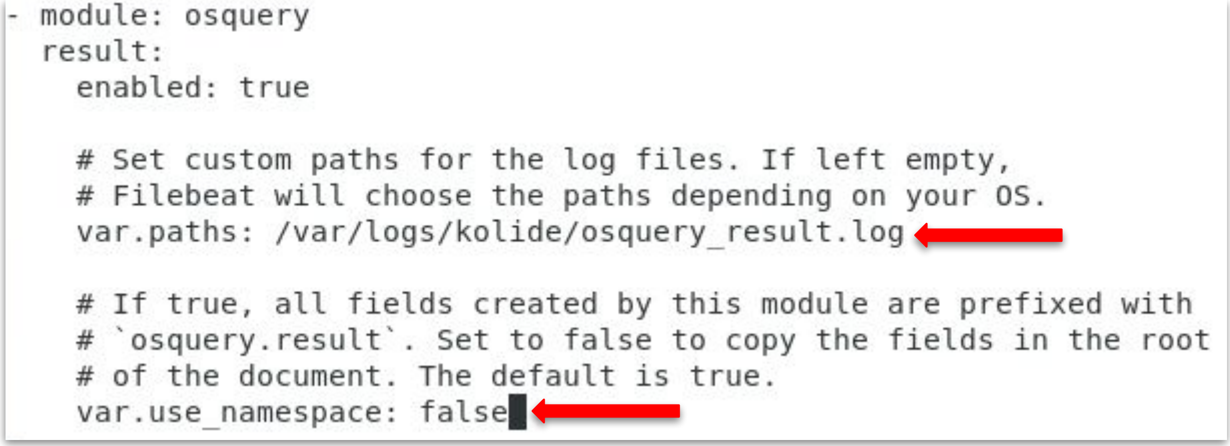
③



```
[analyst@elk ~]$ cat /etc/filebeat/modules.d/osquery.yml.disabled
- module: osquery
  result:
    enabled: true

    # Set custom paths for the log files. If left empty,
    # Filebeat will choose the paths depending on your OS.
    #var.paths:

    # If true, all fields created by this module are prefixed with
    # `osquery.result`. Set to false to copy the fields in the root
    # of the document. The default is true.
    #var.use_namespace: true
[analyst@elk ~]$ 
```

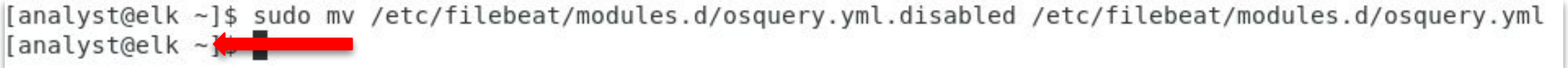
Fleet - Filebeat Config

①



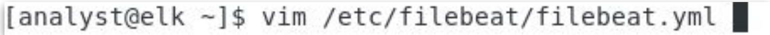
```
- module: osquery
  result:
    enabled: true

    # Set custom paths for the log files. If left empty,
    # Filebeat will choose the paths depending on your OS.
    var.paths: /var/logs/kolide/osquery_result.log

    # If true, all fields created by this module are prefixed with
    # `osquery.result`. Set to false to copy the fields in the root
    # of the document. The default is true.
    var.use_namespace: false
```

②



```
[analyst@elk ~]$ sudo mv /etc/filebeat/modules.d/osquery.yml.disabled /etc/filebeat/modules.d/osquery.yml
[analyst@elk ~]$
```

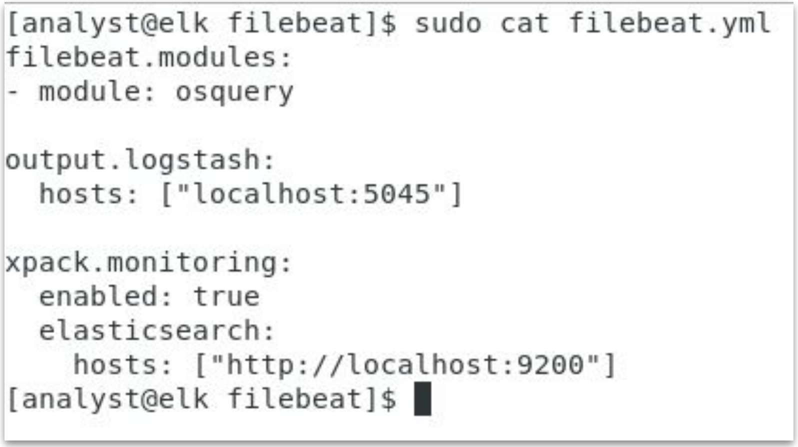
③



```
[analyst@elk ~]$ vim /etc/filebeat/filebeat.yml
```

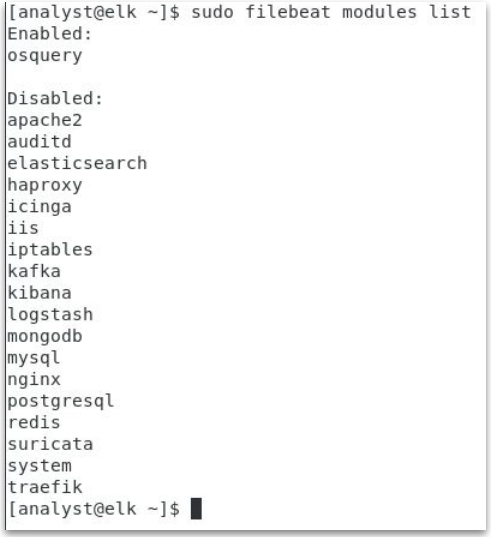
Fleet - Filebeat Config

①



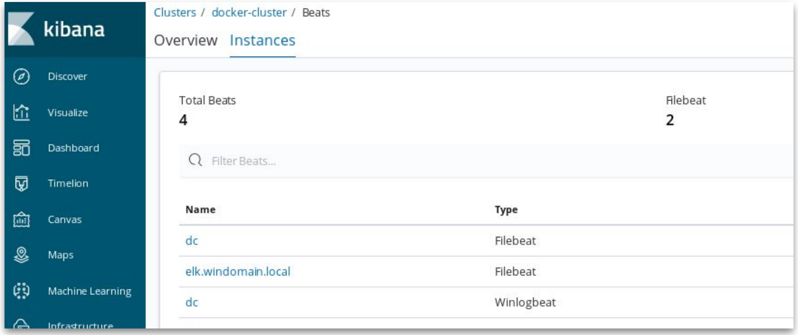
```
[analyst@elk filebeat]$ sudo cat filebeat.yml
filebeat.modules:
- module: osquery

output.logstash:
  hosts: ["localhost:5045"]

xpack.monitoring:
  enabled: true
  elasticsearch:
    hosts: ["http://localhost:9200"]
[analyst@elk filebeat]$ 
```

②



```
[analyst@elk ~]$ sudo filebeat modules list
Enabled:
osquery

Disabled:
apache2
auditd
elasticsearch
haproxy
icinga
iis
iptables
kafka
kibana
logstash
mongodb
mysql
nginx
postgresql
redis
suricata
system
traefik
[analyst@elk ~]$ 
```

③



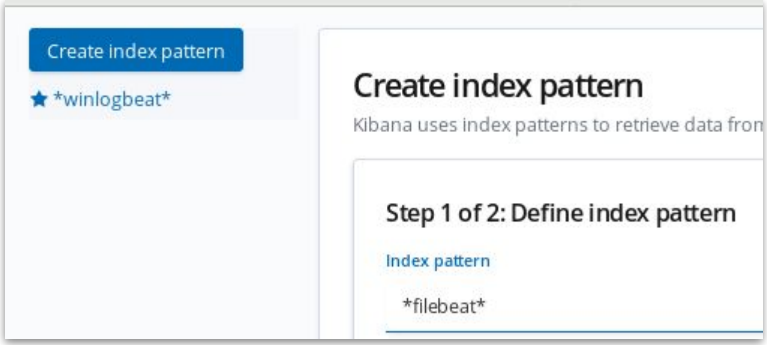
Total Beats 4

Filebeat 2

Name	Type
dc	Filebeat
elk.windomain.local	Filebeat
dc	Winlogbeat

Fleet - Filebeat Config

①



Create index pattern

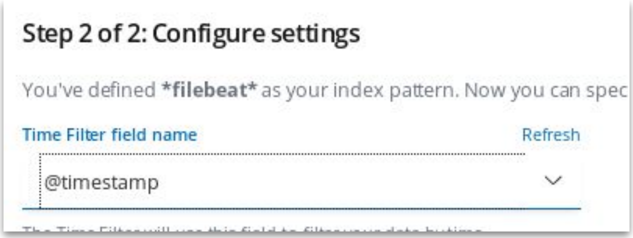
Kibana uses index patterns to retrieve data fron

Step 1 of 2: Define index pattern

Index pattern

filebeat

②



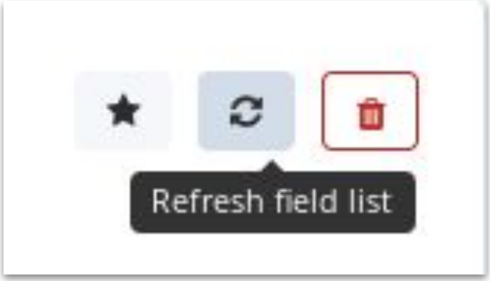
Step 2 of 2: Configure settings

You've defined ***filebeat*** as your index pattern. Now you can spec

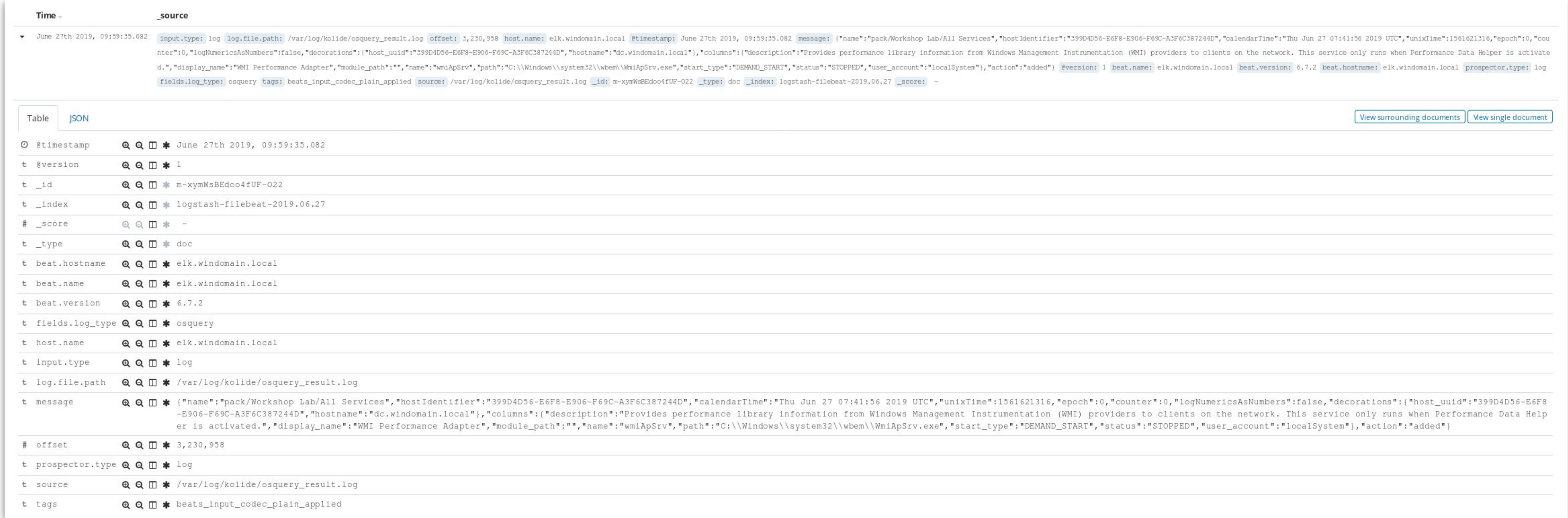
Time Filter field name

@timestamp

③



Fleet - Filebeat Config



Time	_source
June 27th 2019, 09:59:35.082	input.type: log log.file.path: /var/log/kolide/osquery_result.log offset: 3,230,958 host.name: elk.windomain.local @timestamp: June 27th 2019, 09:59:35.082 message: {"name":"pack/Workshop Lab/All Services","hostIdentifier":"399D4D56-E6F8-E906-F69C-A3F6C387244D","calendarTime":"Thu Jun 27 07:41:56 2019 UTC","unixTime":1561621316,"epoch":0,"counter":0,"logNumericsAsNumbers":false,"decorations":{"host_uuid":"399D4D56-E6F8-E906-F69C-A3F6C387244D","hostname":"dc.windomain.local"},"columns":{"description":"Provides performance library information from Windows Management Instrumentation (WMI) providers to clients on the network. This service only runs when Performance Data Helper is activated.","display_name":"WMI Performance Adapter","module_path":"","name":"wmiApSrv","path":"C:\\\\Windows\\\\system32\\\\wbem\\\\WmiApSrv.exe","start_type":"DEMAND_START","status":"STOPPED","user_account":"localSystem"},"action":"added"} @version: 1 beat.name: elk.windomain.local beat.version: 6.7.2 beat.hostname: elk.windomain.local prospector.type: log fields.log_type: osquery tags: beats_input_codec_plain_applied source: /var/log/kolide/osquery_result.log _id: m-xymWsBEdoo4fUF-O22 _type: doc _index: logstash-filebeat-2019.06.27 _score: -

⏲	@timestamp	June 27th 2019, 09:59:35.082
t	@version	1
t	_id	m-xymWsBEdoo4fUF-O22
t	_index	logstash-filebeat-2019.06.27
#	_score	-
t	_type	doc
t	beat.hostname	elk.windomain.local
t	beat.name	elk.windomain.local
t	beat.version	6.7.2
t	fields.log_type	osquery
t	host.name	elk.windomain.local
t	input.type	log
t	log.file.path	/var/log/kolide/osquery_result.log
t	message	{"name":"pack/Workshop Lab/All Services","hostIdentifier":"399D4D56-E6F8-E906-F69C-A3F6C387244D","calendarTime":"Thu Jun 27 07:41:56 2019 UTC","unixTime":1561621316,"epoch":0,"counter":0,"logNumericsAsNumbers":false,"decorations":{"host_uuid":"399D4D56-E6F8-E906-F69C-A3F6C387244D","hostname":"dc.windomain.local"},"columns":{"description":"Provides performance library information from Windows Management Instrumentation (WMI) providers to clients on the network. This service only runs when Performance Data Helper is activated.","display_name":"WMI Performance Adapter","module_path":"","name":"wmiApSrv","path":"C:\\\\Windows\\\\system32\\\\wbem\\\\WmiApSrv.exe","start_type":"DEMAND_START","status":"STOPPED","user_account":"localSystem"},"action":"added"}
#	offset	3,230,958
t	prospector.type	log
t	source	/var/log/kolide/osquery_result.log
t	tags	beats_input_codec_plain_applied