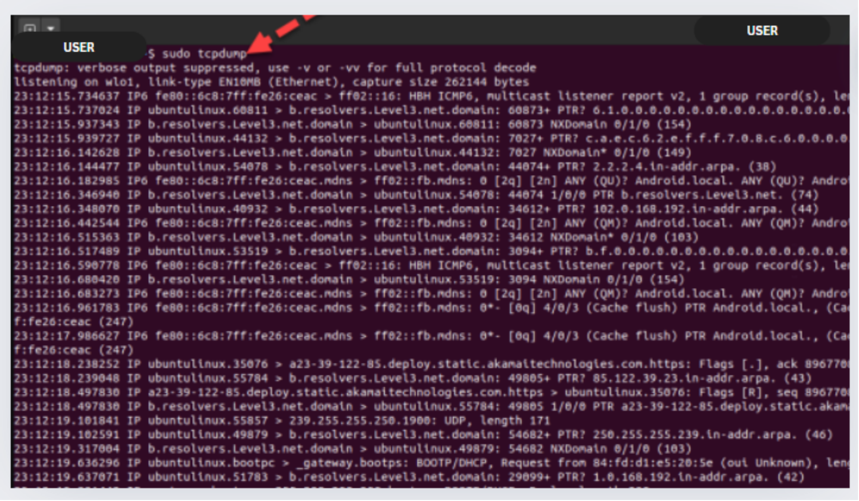
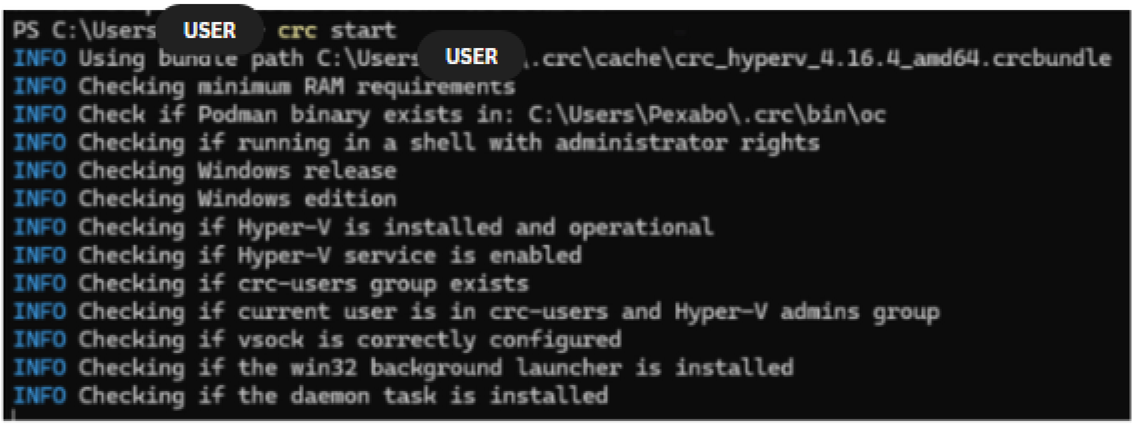
Workshop

TCPDUMP OUTPUT



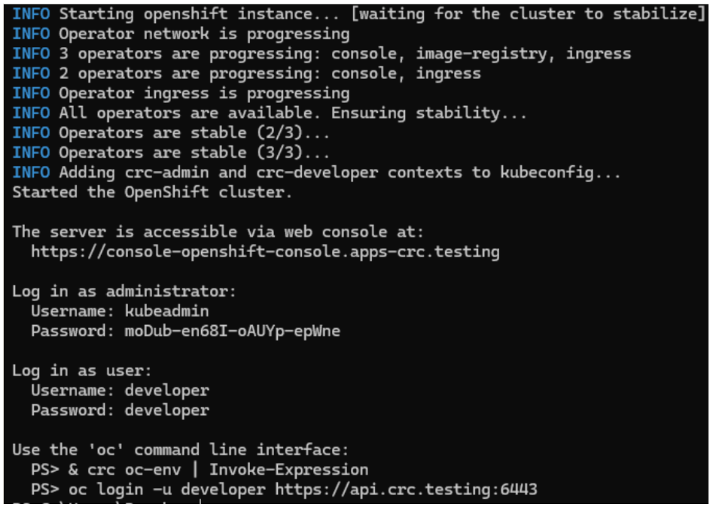
```
USER ~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
23:12:15.734637 IP6 fe80::6c8:7ff:fe26:ceac > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), le
23:12:15.737024 IP ubuntulinux.60811 > b.resolvers.Level3.net.domain: 60873+ PTR? 6.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
23:12:15.937343 IP b.resolvers.Level3.net.domain > ubuntulinux.60811: 60873 NXDomain 0/1/0 (154)
23:12:15.939727 IP ubuntulinux.44132 > b.resolvers.Level3.net.domain: 7027+ PTR? c.a.e.c.6.2.e.f.f.f.7.0.8.c.6.0.0.0.0.0
23:12:16.142628 IP b.resolvers.Level3.net.domain > ubuntulinux.44132: 7027 NXDomain* 0/1/0 (149)
23:12:16.144477 IP ubuntulinux.54078 > b.resolvers.Level3.net.domain: 44074+ PTR? 2.2.2.4.in-addr.arpa. (38)
23:12:16.182985 IP6 fe80::6c8:7ff:fe26:ceac.mdns > ff02::fb.mdns: 0 [2q] [2n] ANY (QU)? Android.local. ANY (QU)? Andro
23:12:16.346940 IP b.resolvers.Level3.net.domain > ubuntulinux.54078: 44074 1/0/0 PTR b.resolvers.Level3.net. (74)
23:12:16.348070 IP ubuntulinux.40932 > b.resolvers.Level3.net.domain: 34612+ PTR? 102.0.168.192.in-addr.arpa. (44)
23:12:16.442544 IP6 fe80::6c8:7ff:fe26:ceac.mdns > ff02::fb.mdns: 0 [2q] [2n] ANY (QM)? Android.local. ANY (QM)? Andro
23:12:16.515363 IP b.resolvers.Level3.net.domain > ubuntulinux.40932: 34612 NXDomain* 0/1/0 (103)
23:12:16.517489 IP ubuntulinux.53519 > b.resolvers.Level3.net.domain: 3094+ PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
23:12:16.590778 IP6 fe80::6c8:7ff:fe26:ceac > ff02::16: HBH ICMP6, multicast listener report v2, 1 group record(s), le
23:12:16.680420 IP b.resolvers.Level3.net.domain > ubuntulinux.53519: 3094 NXDomain 0/1/0 (154)
23:12:16.683273 IP6 fe80::6c8:7ff:fe26:ceac.mdns > ff02::fb.mdns: 0 [2q] [2n] ANY (QM)? Android.local. ANY (QM)? Andro
23:12:16.961783 IP6 fe80::6c8:7ff:fe26:ceac.mdns > ff02::fb.mdns: 0*- [0q] 4/0/3 (Cache flush) PTR Android.local., (Ca
f:fe26:ceac (247)
23:12:17.986627 IP6 fe80::6c8:7ff:fe26:ceac.mdns > ff02::fb.mdns: 0*- [0q] 4/0/3 (Cache flush) PTR Android.local., (Ca
f:fe26:ceac (247)
23:12:18.238252 IP ubuntulinux.35076 > a23-39-122-85.deploy.static.akamaitechnologies.com.https: Flags [.], ack 896770
23:12:18.239048 IP ubuntulinux.55784 > b.resolvers.Level3.net.domain: 49805+ PTR? 85.122.39.23.in-addr.arpa. (43)
23:12:18.497830 IP a23-39-122-85.deploy.static.akamaitechnologies.com.https > ubuntulinux.35076: Flags [R], seq 896770
23:12:18.497830 IP b.resolvers.Level3.net.domain > ubuntulinux.55784: 49805 1/0/0 PTR a23-39-122-85.deploy.static.akam
23:12:19.101841 IP ubuntulinux.55857 > 239.255.255.250.1900: UDP, length 171
23:12:19.102591 IP ubuntulinux.49879 > b.resolvers.Level3.net.domain: 54682+ PTR? 250.255.255.239.in-addr.arpa. (46)
23:12:19.317004 IP b.resolvers.Level3.net.domain > ubuntulinux.49879: 54682 NXDomain 0/1/0 (103)
23:12:19.636296 IP ubuntulinux.bootpc > _gateway.bootps: BOOTP/DHCP, Request from 84:fd:d1:e5:20:5e (oui Unknown), len
23:12:19.637071 IP ubuntulinux.51783 > b.resolvers.Level3.net.domain: 29099+ PTR? 1.0.168.192.in-addr.arpa. (42)
```

CRC ON LOCAL



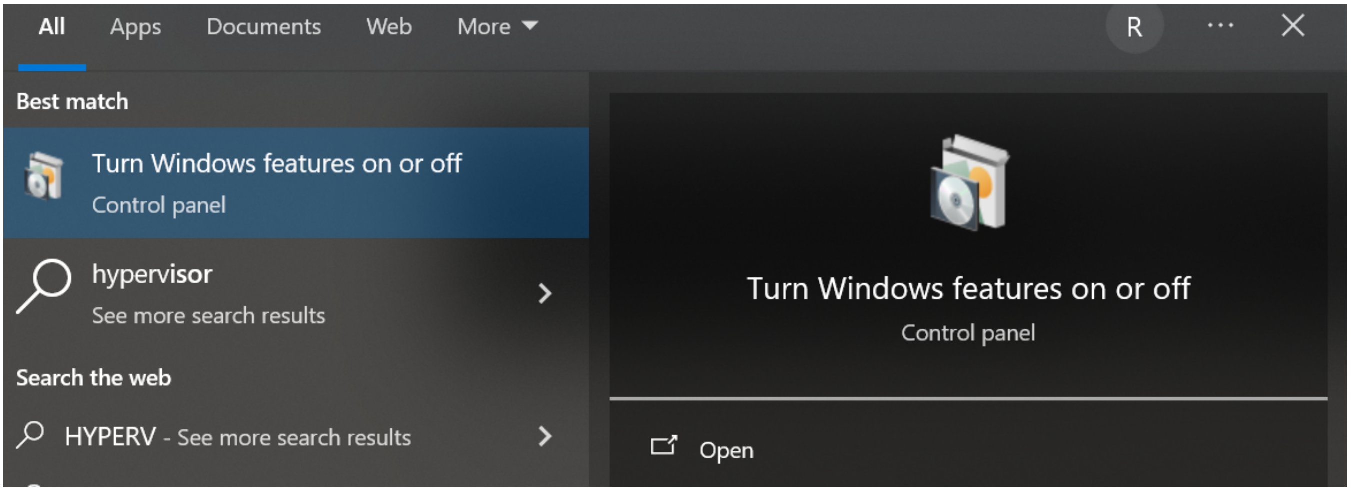
```
PS C:\Users USER crc start
INFO Using bundle path C:\Users USER .crc\cache\crc_hyperv_4.16.4_amd64.crcbundle
INFO Checking minimum RAM requirements
INFO Check if Podman binary exists in: C:\Users\Pexabo\.crc\bin\oc
INFO Checking if running in a shell with administrator rights
INFO Checking Windows release
INFO Checking Windows edition
INFO Checking if Hyper-V is installed and operational
INFO Checking if Hyper-V service is enabled
INFO Checking if crc-users group exists
INFO Checking if current user is in crc-users and Hyper-V admins group
INFO Checking if vsock is correctly configured
INFO Checking if the win32 background launcher is installed
INFO Checking if the daemon task is installed
```

LOGIN TO LOCAL CLUSTER

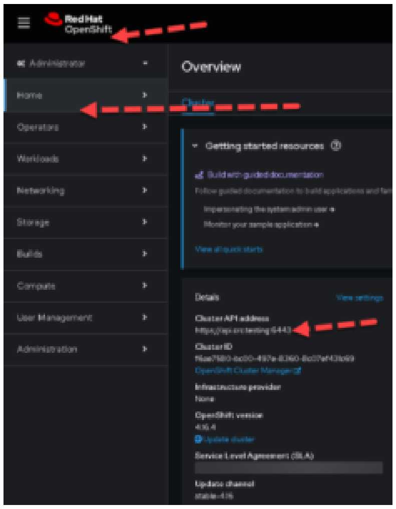


```
INFO Starting openshift instance... [waiting for the cluster to stabilize]
INFO Operator network is progressing
INFO 3 operators are progressing: console, image-registry, ingress
INFO 2 operators are progressing: console, ingress
INFO Operator ingress is progressing
INFO All operators are available. Ensuring stability...
INFO Operators are stable (2/3)...
INFO Operators are stable (3/3)...
INFO Adding crc-admin and crc-developer contexts to kubeconfig...
Started the OpenShift cluster.

The server is accessible via web console at:
  https://console-openshift-console.apps-crc.testing

Log in as administrator:
  Username: kubeadmin
  Password: moDub-en68I-oAUYp-epWne

Log in as user:
  Username: developer
  Password: developer

Use the 'oc' command line interface:
  PS> & crc oc-env | Invoke-Expression
  PS> oc login -u developer https://api.crc.testing:6443
```

LAPTOP NOT HAVING THE HYPERV



CRC WEB CONSOLE


Red Hat
OpenShift
Administrator
Home
Operators
Workloads
Networking
Storage
Builds
Compute
User Management
Administration
Overview
Cluster
Getting started resources
Build with guided documentation
Follow guided documentation to build applications and fam
Impersonating the system:admin user →
Monitor your sample application →
View all quick starts
Details
View settings
OpenShift Cluster Manager
Update cluster

Cluster API address
https://api.crc.testing:6443

Cluster ID
f6ae7580-bc00-497e-8360-8c07ef43b69

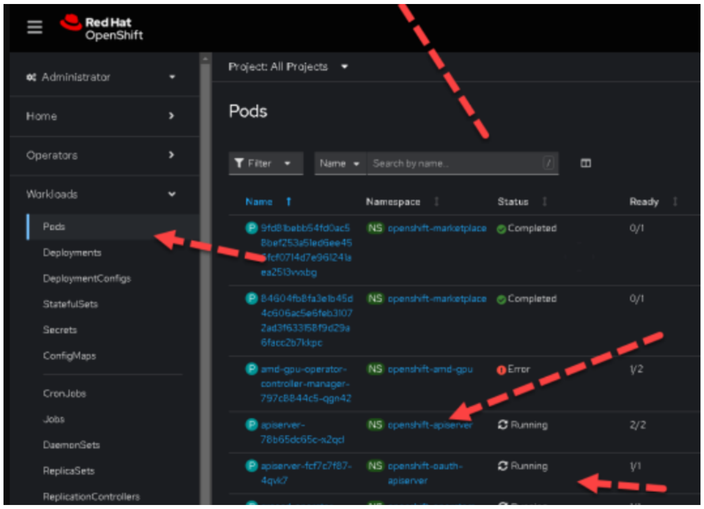
Infrastructure provider
None

OpenShift version
4.16.4

Service Level Agreement (SLA)

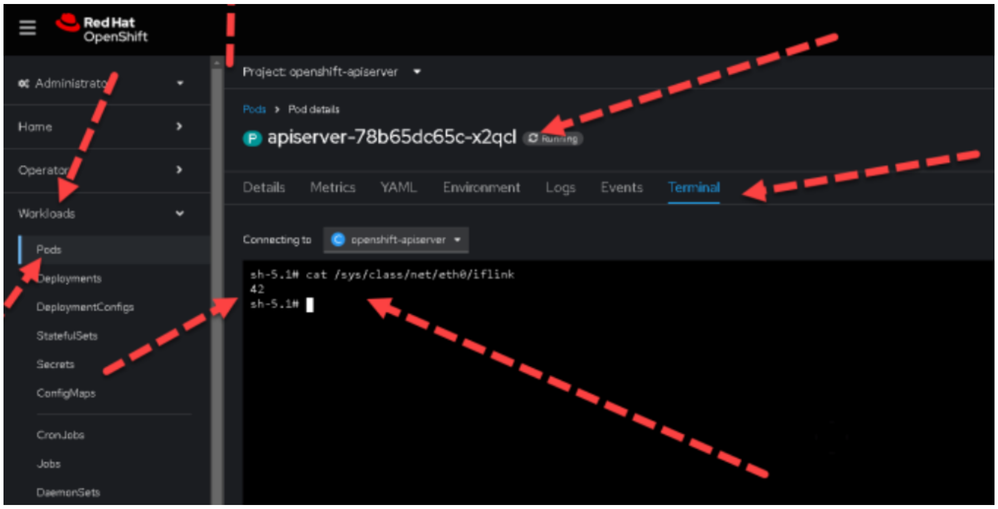
Update channel
stable-4.16

NODES SELECTION



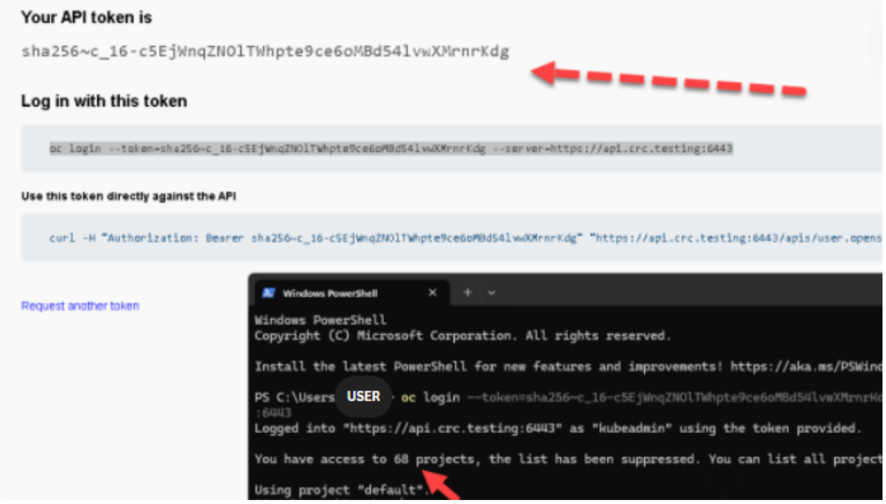
Name	Namespace	Status	Ready
P 9fd81bebb54fd0ac58bef253a51ed6ee456fcf0714d7e961241aea2513vvxbg	NS openshift-marketplace	Completed	0/1
P 84604fb8fa3e1b45d4c606ac5e6feb31072ad3f633158f9d29a6facc2b7kkpc	NS openshift-marketplace	Completed	0/1
P amd-gpu-operator-controller-manager-797c8844c5-qgn42	NS openshift-amd-gpu	Error	1/2
P apiserver-78b65dc65c-x2qd	NS openshift-apiserver	Running	2/2
P apiserver-fcf7c7f87-4qvk7	NS openshift-oauth-apiserver	Running	1/1

TERMINAL FOR THE POD



```
sh-5.1# cat /sys/class/net/eth0/iflink
42
sh-5.1# █
```

LOGIN TO THE CONSOLE



Your API token is

sha256~c_16-c5EjWnqZNOlTWhpte9ce6oMBd54lvwXMrnrKdg

Log in with this token

```
oc login --token=sha256~c_16-c5EjWnqZNOlTWhpte9ce6oMBd54lvwXMrnrKdg --server=https://api.crc.testing:6443
```

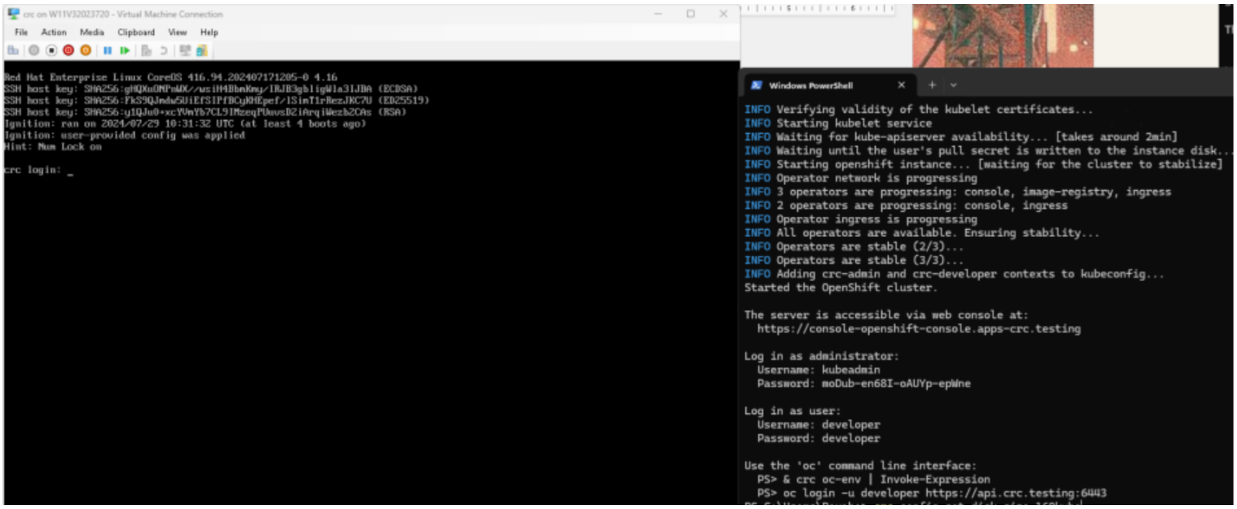
Use this token directly against the API

```
curl -H "Authorization: Bearer sha256~c_16-c5EjWnqZNOlTWhpte9ce6oMBd54lvwXMrnrKdg" "https://api.crc.testing:6443/apis/user.opens
```

Request another token

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWind

PS C:\Users USER > oc login --token=sha256~c_16-c5EjWnqZNOlTWhpte9ce6oMBd54lvwXMrnrKd
:6443
Logged into "https://api.crc.testing:6443" as "kubeadmin" using the token provided.

You have access to 68 projects, the list has been suppressed. You can list all project

Using project "default".
```

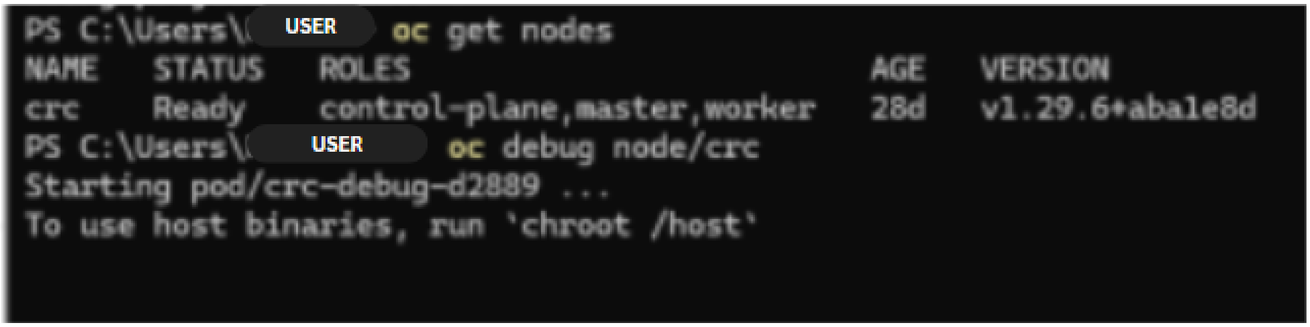
VIRTUAL MACHINE FOR CRC



```
Red Hat Enterprise Linux CoreOS 416.94.202407171205-0 4.16
SSH host key: SHA256:gHQXuONPnWX//usiH4BbmKmy/IRJB3gbligWla3lJBA (ECDSA)
SSH host key: SHA256:FkS9QJmdw5UiEfSIPfBCyKHEpef/lSimT1rRezJKC7U (ED25519)
SSH host key: SHA256:y1QJu0+xcYVmYb7CL9IMzeqPUwvsDZiArqiWezb2CAs (RSA)
Ignition: ran on 2024/07/29 10:31:32 UTC (at least 4 boots ago)
Ignition: user-provided config was applied
Hint: Num Lock on

crc login: _
```

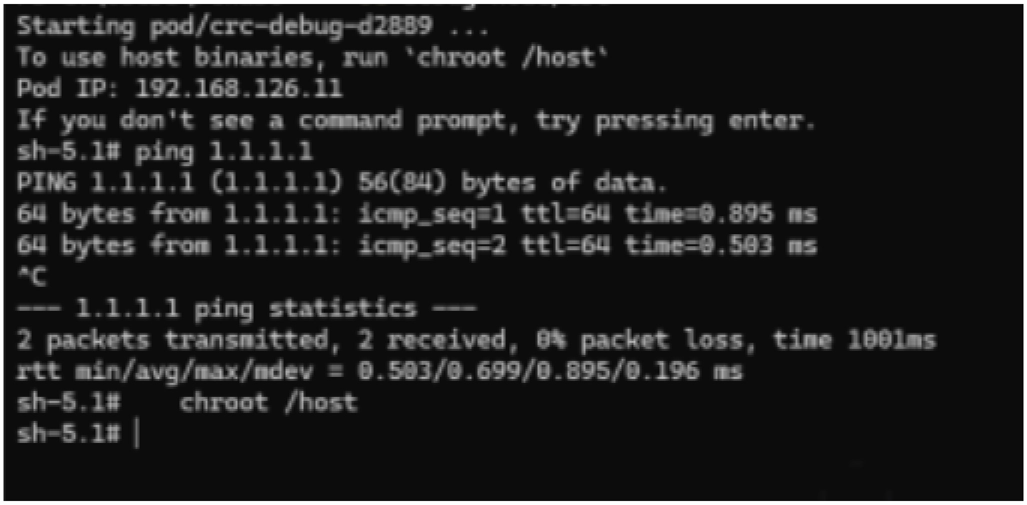
```
INFO Verifying validity of the kubelet certificates...
INFO Starting kubelet service
INFO Waiting for kube-apiserver availability... [takes around 2min]
INFO Waiting until the user's pull secret is written to the instance disk...
INFO Starting openshift instance... [waiting for the cluster to stabilize]
INFO Operator network is progressing
INFO 3 operators are progressing: console, image-registry, ingress
INFO 2 operators are progressing: console, ingress
INFO Operator ingress is progressing
INFO All operators are available. Ensuring stability...
INFO Operators are stable (2/3)...
INFO Operators are stable (3/3)...
INFO Adding crc-admin and crc-developer contexts to kubeconfig...
Started the OpenShift cluster.

The server is accessible via web console at:
  https://console-openshift-console.apps-crc.testing

Log in as administrator:
  Username: kubeadmin
  Password: moDub-en68I-oAUYp-epWne

Log in as user:
  Username: developer
  Password: developer

Use the 'oc' command line interface:
  PS> & crc oc-env | Invoke-Expression
  PS> oc login -u developer https://api.crc.testing:6443
```

CRC HOST / WORKER NODE DEBUG



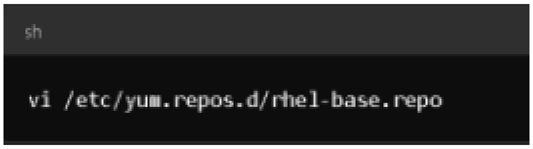
```
PS C:\Users\USER oc get nodes
NAME   STATUS   ROLES                         AGE   VERSION
crc    Ready    control-plane,master,worker   28d   v1.29.6+abale8d
PS C:\Users\USER oc debug node/crc
Starting pod/crc-debug-d2889 ...
To use host binaries, run `chroot /host`
```

GET PRIVILEGED ACCESS

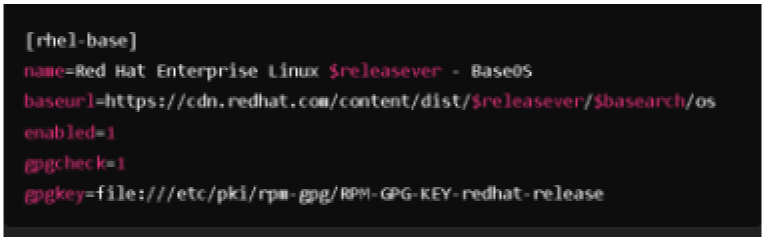


```
Starting pod/crc-debug-d2889 ...
To use host binaries, run `chroot /host`
Pod IP: 192.168.126.11
If you don't see a command prompt, try pressing enter.
sh-5.1# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=64 time=0.895 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=64 time=0.503 ms
^C
--- 1.1.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.503/0.699/0.895/0.196 ms
sh-5.1#    chroot /host
sh-5.1# |
```

REPO ON THE VM

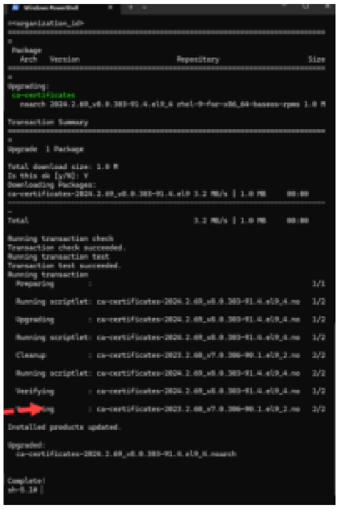


```sh
vi /etc/yum.repos.d/rhel-base.repo
```



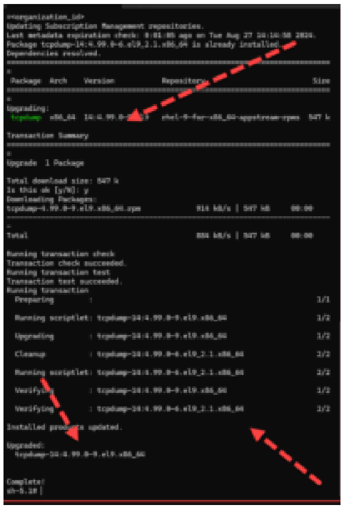
```
[rhel-base]
name=Red Hat Enterprise Linux $releasever - BaseOS
baseurl=https://cdn.redhat.com/content/dist/$releasever/$basearch/os
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

DNF UPDATE CA CERTIFICATES



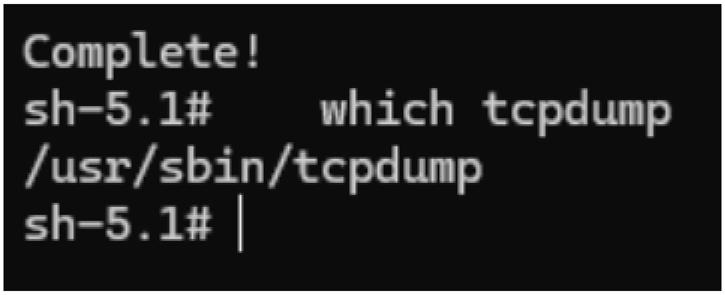
```
<<organization_id>
================================================================================
=
 Package
   Arch    Version                          Repository                     Size
================================================================================
=
Upgrading:
 ca-certificates
   noarch 2024.2.69_v8.0.303-91.4.el9_4 rhel-9-for-x86_64-baseos-rpms 1.0 M

Transaction Summary
================================================================================
=
Upgrade  1 Package

Total download size: 1.0 M
Is this ok [y/N]: Y
Downloading Packages:
ca-certificates-2024.2.69_v8.0.303-91.4.el9 3.2 MB/s | 1.0 MB     00:00
--------------------------------------------------------------------------------
-
Total                                       3.2 MB/s | 1.0 MB     00:00

Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1

  Running scriptlet: ca-certificates-2024.2.69_v8.0.303-91.4.el9_4.no   1/2

  Upgrading        : ca-certificates-2024.2.69_v8.0.303-91.4.el9_4.no   1/2

  Running scriptlet: ca-certificates-2024.2.69_v8.0.303-91.4.el9_4.no   1/2

  Cleanup          : ca-certificates-2023.2.60_v7.0.306-90.1.el9_2.no   2/2

  Running scriptlet: ca-certificates-2024.2.69_v8.0.303-91.4.el9_4.no   2/2

  Verifying        : ca-certificates-2024.2.69_v8.0.303-91.4.el9_4.no   1/2

  Verifying        : ca-certificates-2023.2.60_v7.0.306-90.1.el9_2.no   2/2

Installed products updated.

Upgraded:
  ca-certificates-2024.2.69_v8.0.303-91.4.el9_4.noarch


Complete!
sh-5.1#
```

DNF TCPDUMP INSTALL



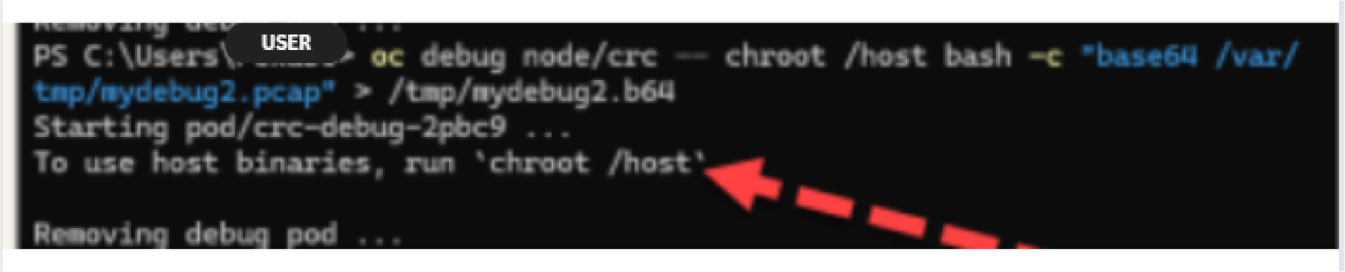
```
<<organization_id>
Updating Subscription Management repositories.
Last metadata expiration check: 0:01:05 ago on Tue Aug 27 16:16:58 2024.
Package tcpdump-14:4.99.0-6.el9_2.1.x86_64 is already installed.
Dependencies resolved.
================================================================================
=
 Package  Arch    Version          Repository                             Size
================================================================================
=
Upgrading:
 tcpdump  x86_64  14:4.99.0-9.el9  rhel-9-for-x86_64-appstream-rpms      547 k

Transaction Summary
================================================================================
=
Upgrade  1 Package

Total download size: 547 k
Is this ok [y/N]: y
Downloading Packages:
tcpdump-4.99.0-9.el9.x86_64.rpm                914 kB/s | 547 kB     00:00
--------------------------------------------------------------------------------
-
Total                                          884 kB/s | 547 kB     00:00

Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1

  Running scriptlet: tcpdump-14:4.99.0-9.el9.x86_64                         1/2

  Upgrading        : tcpdump-14:4.99.0-9.el9.x86_64                         1/2

  Cleanup          : tcpdump-14:4.99.0-6.el9_2.1.x86_64                     2/2

  Running scriptlet: tcpdump-14:4.99.0-6.el9_2.1.x86_64                     2/2

  Verifying        : tcpdump-14:4.99.0-9.el9.x86_64                         1/2

  Verifying        : tcpdump-14:4.99.0-6.el9_2.1.x86_64                     2/2

Installed products updated.

Upgraded:
  tcpdump-14:4.99.0-9.el9.x86_64


Complete!
sh-5.1#
```

LOCATE TCPDUMP



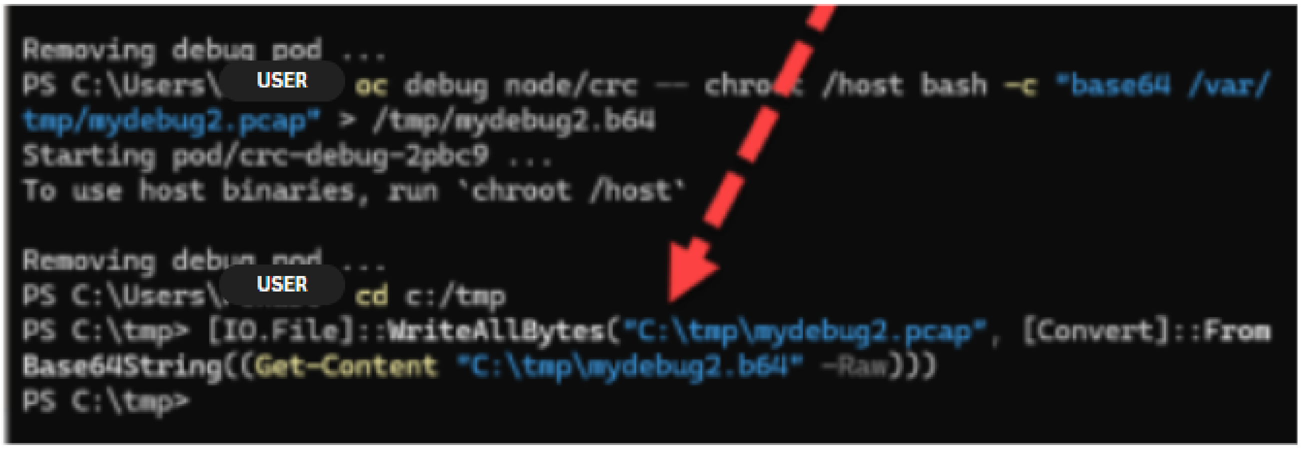
```
Complete!
sh-5.1#    which tcpdump
/usr/sbin/tcpdump
sh-5.1#
```

BASE64 DEBUG POD MOVE THE DATA



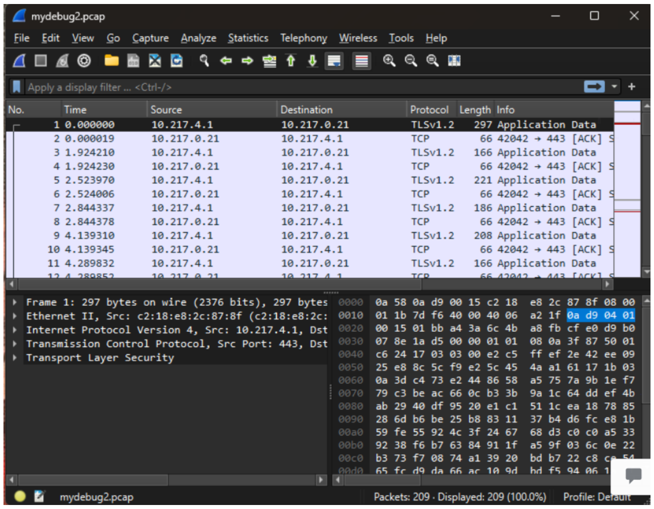
```
Removing debug pod ...
PS C:\Users\ USER > oc debug node/crc -- chroot /host bash -c "base64 /var/tmp/mydebug2.pcap" > /tmp/mydebug2.b64
Starting pod/crc-debug-2pbc9 ...
To use host binaries, run `chroot /host`

Removing debug pod ...
```

DECODE THE BASE64



```
Removing debug pod ...
PS C:\Users\USER oc debug node/crc -- chroot /host bash -c "base64 /var/tmp/mydebug2.pcap" > /tmp/mydebug2.b64
Starting pod/crc-debug-2pbc9 ...
To use host binaries, run `chroot /host`

Removing debug pod ...
PS C:\Users\USER cd c:/tmp
PS C:\tmp> [IO.File]::WriteAllBytes("C:\tmp\mydebug2.pcap", [Convert]::FromBase64String((Get-Content "C:\tmp\mydebug2.b64" -Raw)))
PS C:\tmp>
```

WIRESHARK



mydebug2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source       Destination  Protocol Length Info
   1 0.000000  10.217.4.1   10.217.0.21  TLSv1.2   297 Application Data
   2 0.000019  10.217.0.21  10.217.4.1   TCP        66 42042 → 443 [ACK] S
   3 1.924210  10.217.4.1   10.217.0.21  TLSv1.2   166 Application Data
   4 1.924230  10.217.0.21  10.217.4.1   TCP        66 42042 → 443 [ACK] S
   5 2.523970  10.217.4.1   10.217.0.21  TLSv1.2   221 Application Data
   6 2.524006  10.217.0.21  10.217.4.1   TCP        66 42042 → 443 [ACK] S
   7 2.844337  10.217.4.1   10.217.0.21  TLSv1.2   186 Application Data
   8 2.844378  10.217.0.21  10.217.4.1   TCP        66 42042 → 443 [ACK] S
   9 4.139310  10.217.4.1   10.217.0.21  TLSv1.2   208 Application Data
  10 4.139345  10.217.0.21  10.217.4.1   TCP        66 42042 → 443 [ACK] S
  11 4.289832  10.217.4.1   10.217.0.21  TLSv1.2   166 Application Data
  12 4.289852  10.217.0.21  10.217.4.1   TCP        66 42042 → 443 [ACK] S
```

```
› Frame 1: 297 bytes on wire (2376 bits), 297 bytes
› Ethernet II, Src: c2:18:e8:2c:87:8f (c2:18:e8:2c:
› Internet Protocol Version 4, Src: 10.217.4.1, Dst
› Transmission Control Protocol, Src Port: 443, Dst
› Transport Layer Security
```

```
0000  0a 58 0a d9 00 15 c2 18  e8 2c 87 8f 08 00
0010  01 1b 7d f6 40 00 40 06  a2 1f 0a d9 04 01
0020  00 15 01 bb a4 3a 6c 4b  a8 fb cf e0 d9 b0
0030  07 8e 1a d5 00 00 01 01  08 0a 3f 87 50 01
0040  c6 24 17 03 03 00 e2 c5  ff ef 2e 42 ee 09
0050  25 e8 8c 5c f9 e2 5c 45  4a a1 61 17 1b 03
0060  0a 3d c4 73 e2 44 86 58  a5 75 7a 9b 1e f7
0070  79 c3 be ac 66 0c b3 3b  9a 1c 64 dd ef 4b
0080  ab 29 40 df 95 20 e1 c1  51 1c ea 18 78 85
0090  28 6d b6 be 25 b8 83 11  37 b4 d6 fc e8 1b
00a0  59 fe 55 92 4c 3f 24 67  68 d3 c0 c0 a5 33
00b0  92 38 f6 b7 63 84 91 1f  a5 9f 03 6c 0e 22
00c0  b3 73 f7 08 74 a1 39 20  bd b7 22 c8 ce 54
00d0  65 fc d9 da 66 ac 10 9d  bd f5 94 06 1
```

```
mydebug2.pcap    Packets: 209 · Displayed: 209 (100.0%)    Profile: Default
```