Module

ECE Fundamentals

Topics

- Elastic Cloud Enterprise Architecture
- Elastic Cloud Enterprise Interfaces
- Elastic Cloud Enterprise Features
- Learn More

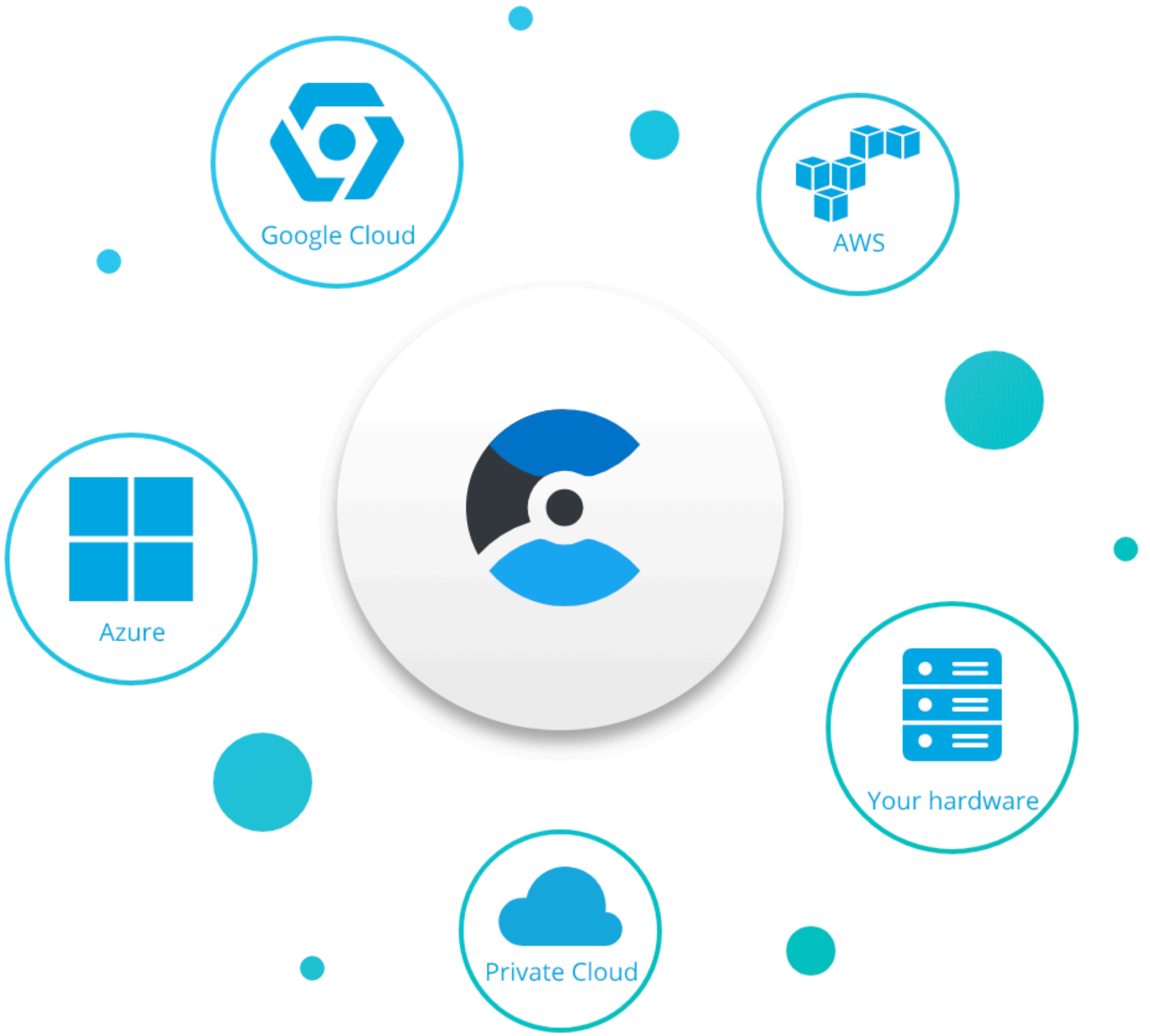
ECE Fundamentals

Lesson 1

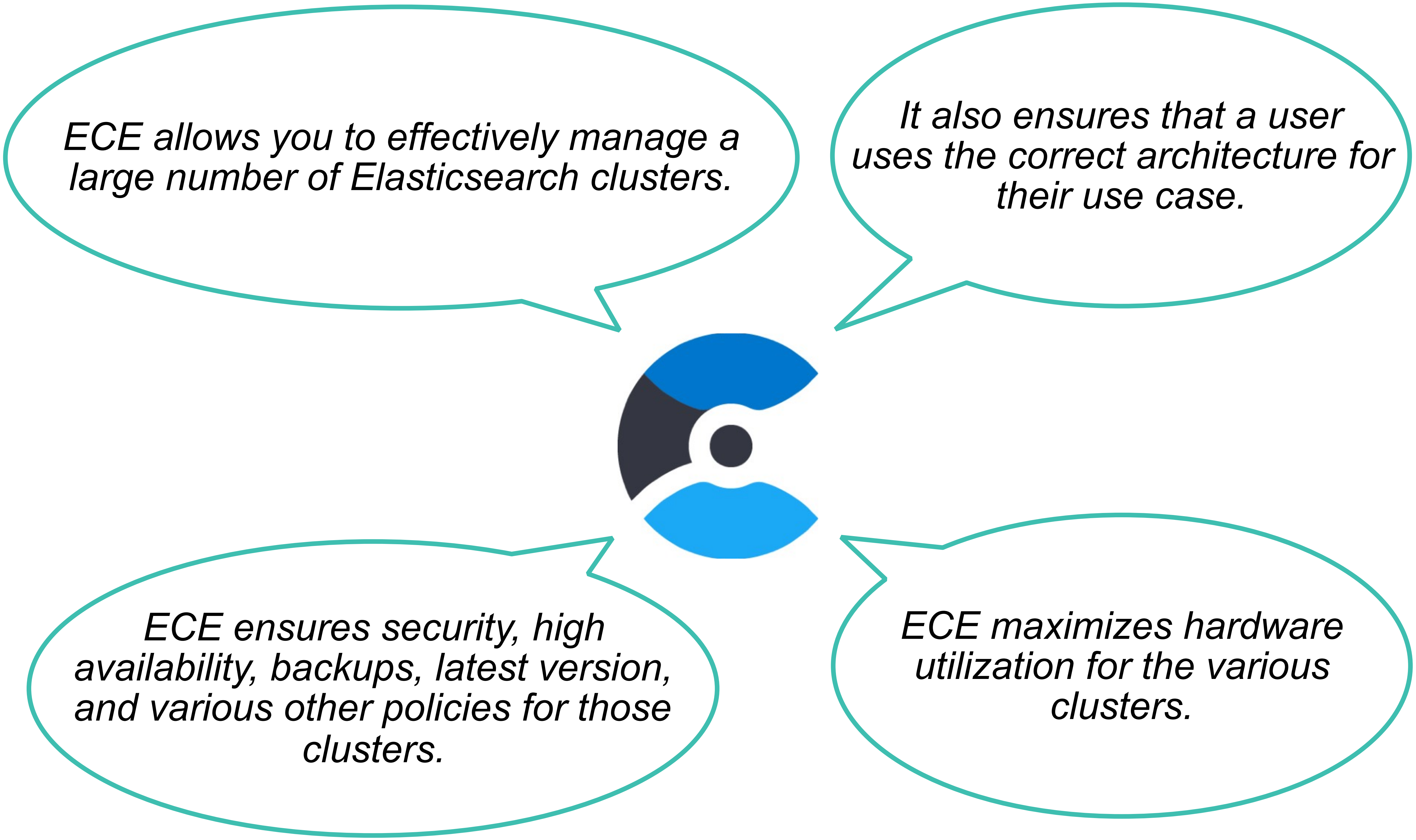
Elastic Cloud Enterprise Architecture

elastic

What is Elastic Cloud Enterprise?



Why Elastic Cloud Enterprise



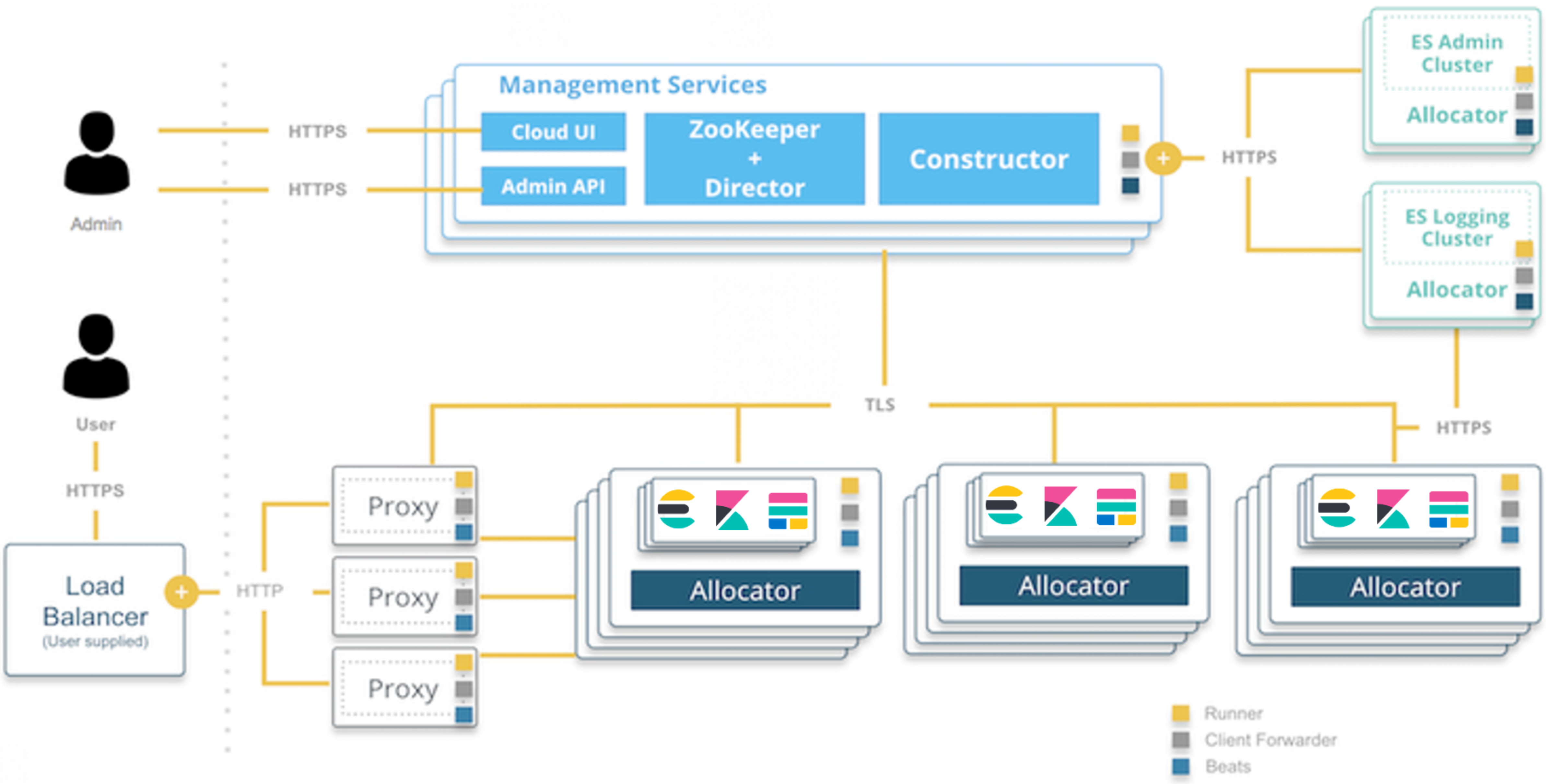
ECE allows you to effectively manage a large number of Elasticsearch clusters.

It also ensures that a user uses the correct architecture for their use case.

ECE ensures security, high availability, backups, latest version, and various other policies for those clusters.

ECE maximizes hardware utilization for the various clusters.

Elastic Cloud Enterprise Architecture

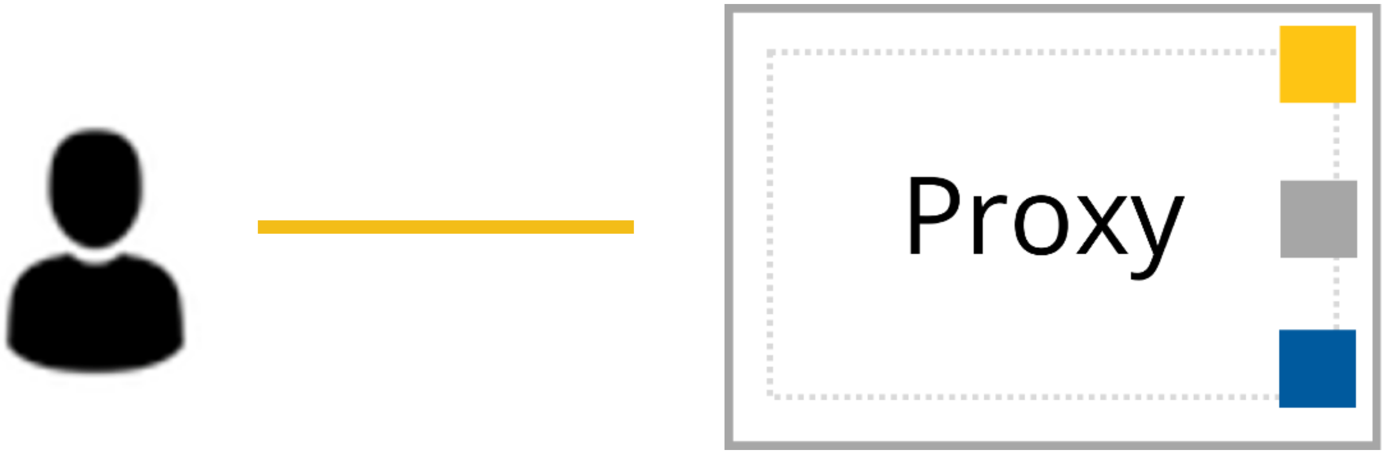


Roles and Runners

- Runners are "supervisors" on a single machine
- Runners are assigned one or more roles
- Roles map to one or more containers
- Runners ensure all containers for that role are online and healthy
- Now, let's look at each of these roles

Proxy Role

- Handle user requests
- Keep track of the state and availability of cloud assets
- Help with no-downtime scaling and upgrades



Proxy

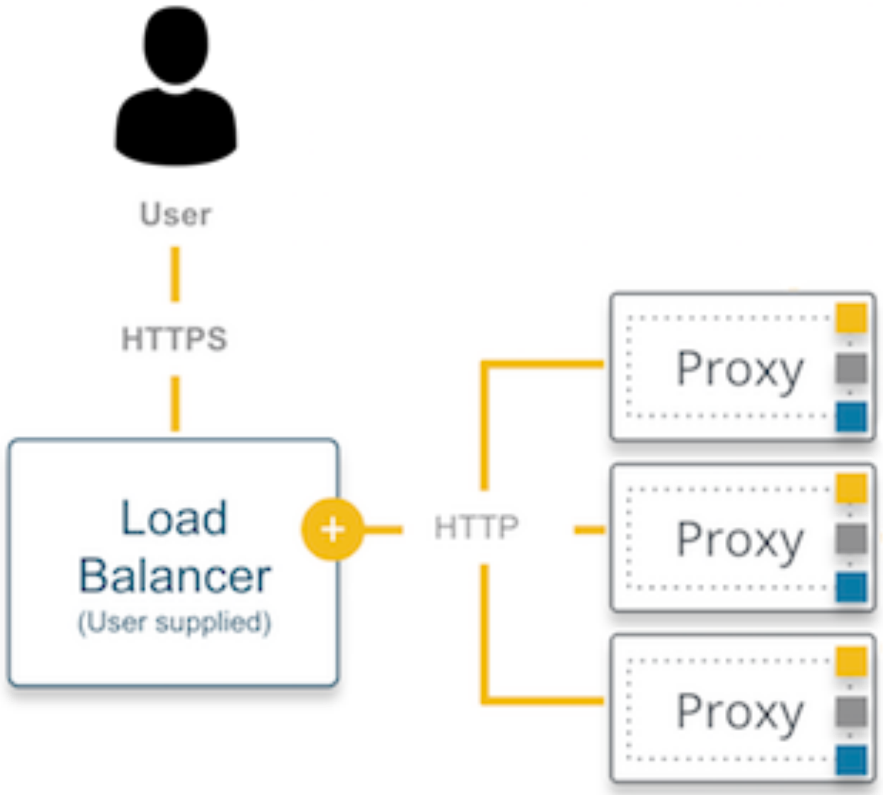
🟨 Runner

⬜ Client Forwarder

🟦 Beats

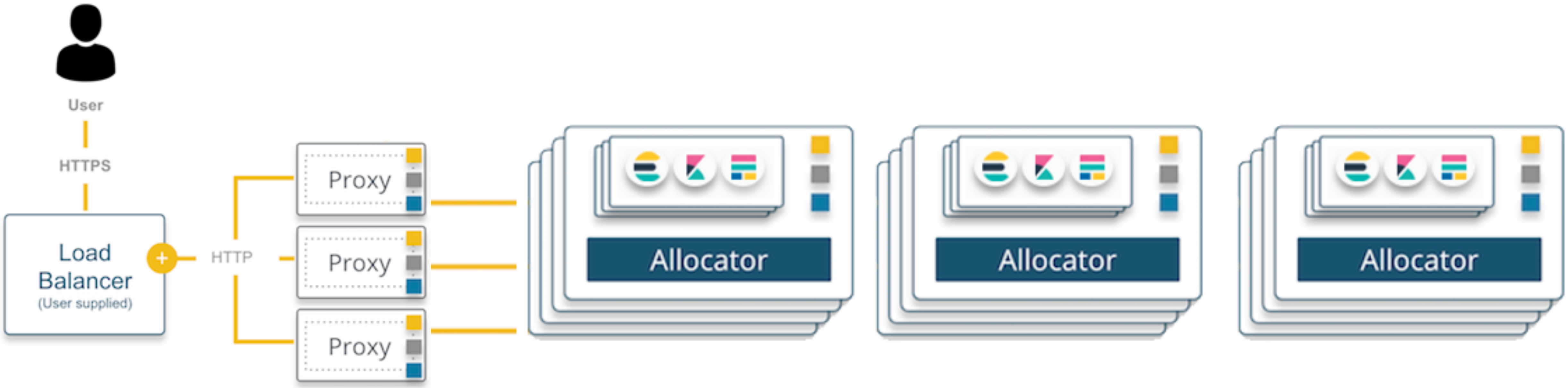
Load Balancer

- Typically, multiple proxies are put behind a load balancer
- This is not something that ECE offers out of the box
  - so you're going to be responsible for setting this up within your own infrastructure

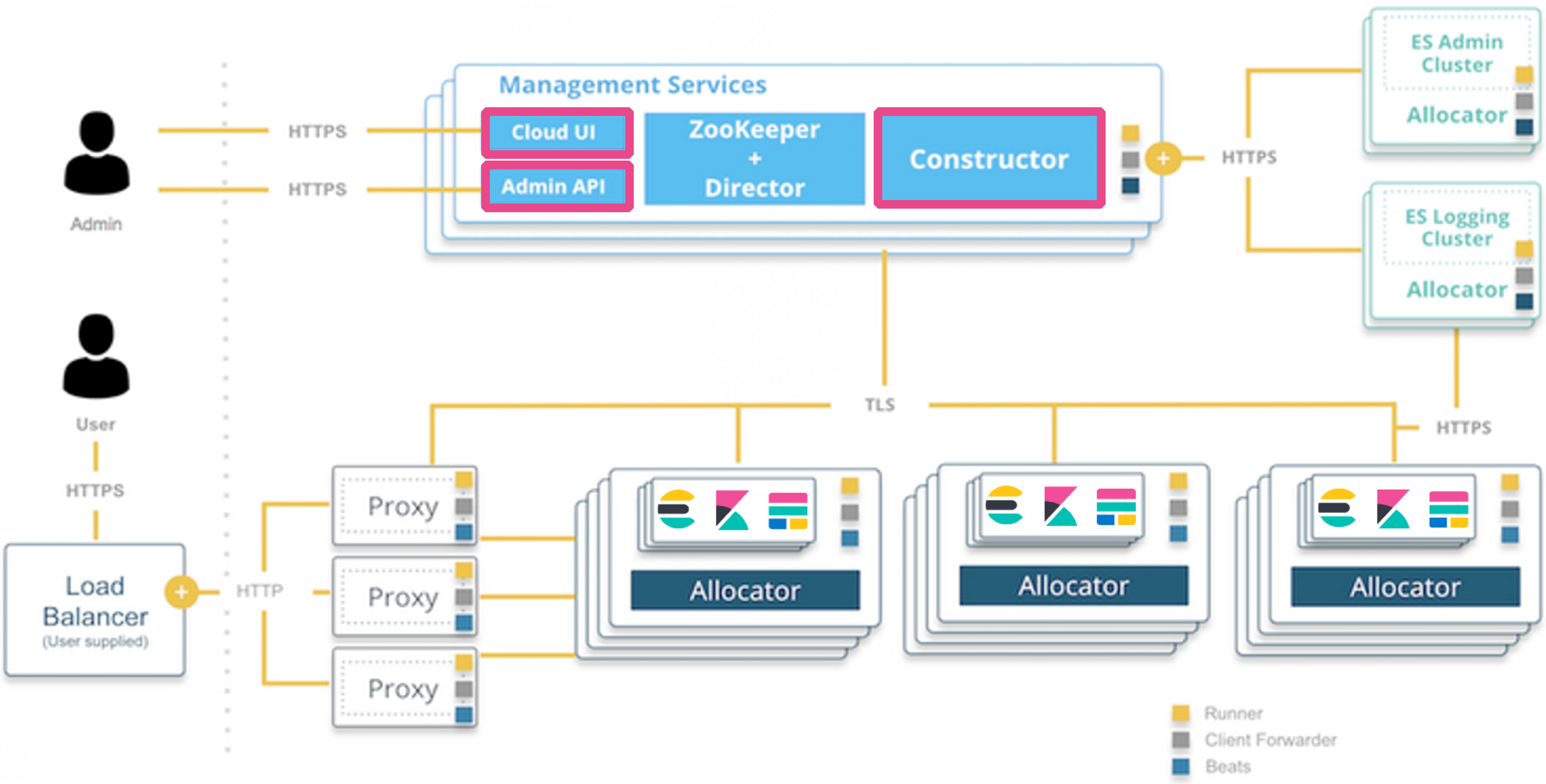


Allocator Role

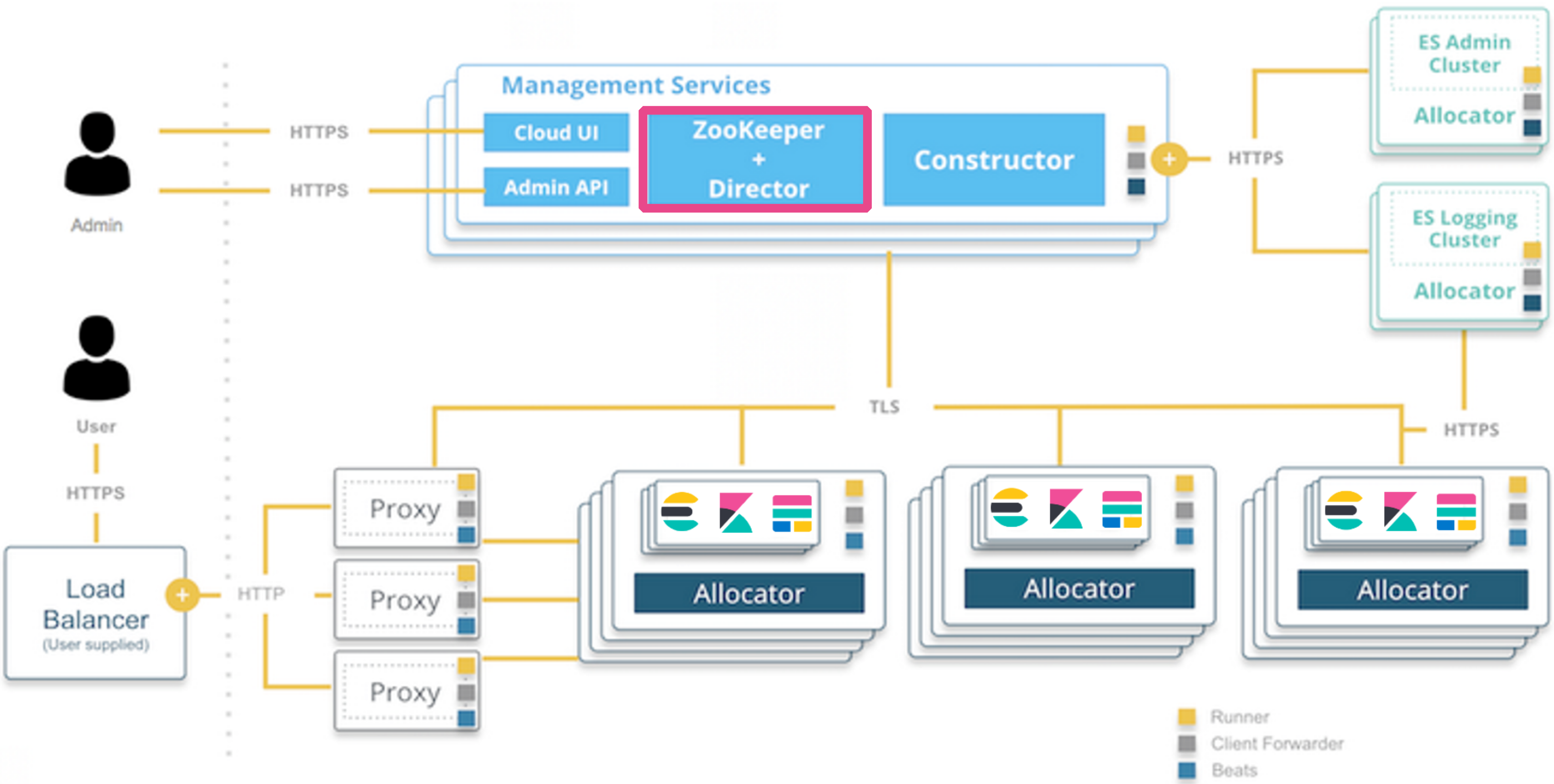
- Run all the instances that you want to host Elasticsearch and Kibana nodes on
- Create new containers and start Elasticsearch and Kibana nodes when requested



Coordinator Role



Director Role



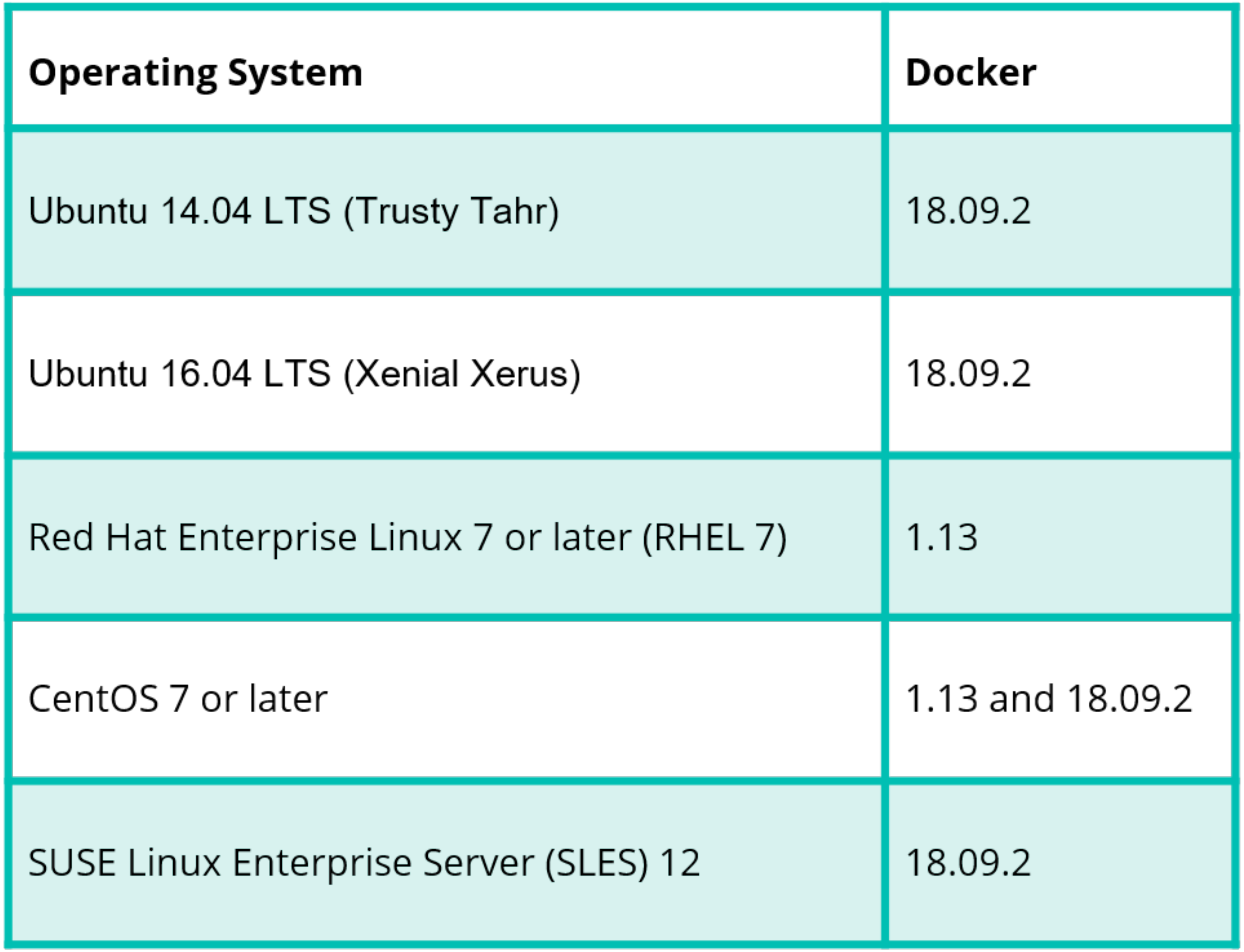
Prerequisites

- Before installing ECE you need to check whether your environment meets the installation prerequisites
- They are broken down into the following five categories
  1. Hardware
  2. Software
  3. Users
  4. Networking
  5. JVM heap sizes
- If you use AWS you can use one of the Elastic AMIs
  - https://www.elastic.co/guide/en/cloud-enterprise/current/ece-configure-ami.html

Hardware

- Memory
  - at least 8 GB RAM
  - but 128 GB RAM to 256 GB RAM is recommended for allocators
  - and 64 GB RAM for other hosts
- Storage
  - at least 10 GB
  - allocators in particular require enough storage to support your RAM-to-storage ratio
- RAM-to-storage ratio example
  - if you have a host with 16 GB RAM and the default ratio of 1:32
  - then you should provide 512 GB of disk space

Software



Operating System	Docker
Ubuntu 14.04 LTS (Trusty Tahr)	18.09.2
Ubuntu 16.04 LTS (Xenial Xerus)	18.09.2
Red Hat Enterprise Linux 7 or later (RHEL 7)	1.13
CentOS 7 or later	1.13 and 18.09.2
SUSE Linux Enterprise Server (SLES) 12	18.09.2

Users

- To prepare the environment
  - a user with **sudo** permissions
  - to install docker, XFS, etc
  - not required if using prepared AMI
- To install ECE
  - a user with UID and GID greater than or equal to 1000
  - who is part of the **docker** group
  - note that you must not install ECE as the **root** user

Networking

- Decide between internet vs. offline install
- Open the following ports to allow access to ECE and between ECE hosts

Operating System	Docker	Role
80	outbound HTTP	all
443	outbound HTTPS	all
22	outbound HTTPS	all
12300/12343	inbound	coordinator
12400/12443	Inbound HTTP/HTTPS	coordinator
9200/9243	Inbound HTTP/HTTPS	proxy
9300/9343	Inbound HTTP/HTTPS	proxy

JVM Heap Sizes

Service	JVM Heap Size (Xms and Xmx)
runner	1 GB
allocator	4 GB
proxy	8 GB
zookeeper	4 GB
director	1 GB
constructor	4 GB
Admin-console	4 GB

Elasticsearch Clusters and JVM Heap Size

- For Elasticsearch clusters, ECE gives 50% of available memory to the JVM heap used by Elasticsearch
- While leaving the other 50% for the operating system
- The ideal heap size is somewhere below 32 GB
  - as heap sizes above 32 GB become less efficient
- Example
  - on a 64 GB cluster you dedicate 32 GB to ES and 32 GB to OS
  - what if you provision a 128 GB cluster?
  - in this case ECE creates two 64 GB nodes
  - each node with 32 GB for ES and 32 GB for OS

Lesson 1

Review - Elastic Cloud Enterprise Architecture

Summary

- You can install ECE on your own infrastructure
- You can use ECE to manage a large number of Elasticsearch clusters, making sure that security, high availability, backups, latest version and various other policies apply for those clusters
- The ECE architecture is composed by load balancers, proxies, allocators, zookeeper and directors, constructors as well as the cloud UI and admin API
- Each service is deployed independently in its own Docker container
- You must meet the prerequisites before installing ECE

Quiz

1. **True** or **False**: ECE might be a preferred choice if your enterprise data cannot be hosted on a public cloud, for example, where regulated or sensitive data cannot leave your internal network.
2. What is the primary purpose of a runner?
3. **True** or **False**: Elastic Cloud Enterprise can run on hosts with 4GB memory.

ECE Fundamentals

Lesson 1

Lab - Elastic Cloud Enterprise Architecture

Lesson 2

Elastic Cloud Enterprise Interfaces

elastic

Install Elastic Cloud Enterprise

- Once you have met all the prerequisites
  - you can install ECE on your first host

```
bash \
<(curl -fsSL https://download.elastic.co/cloud/elastic-cloud-enterprise.sh) \
install
```

- The command above will install the latest version of ECE
  - but you can specify which version you want to install

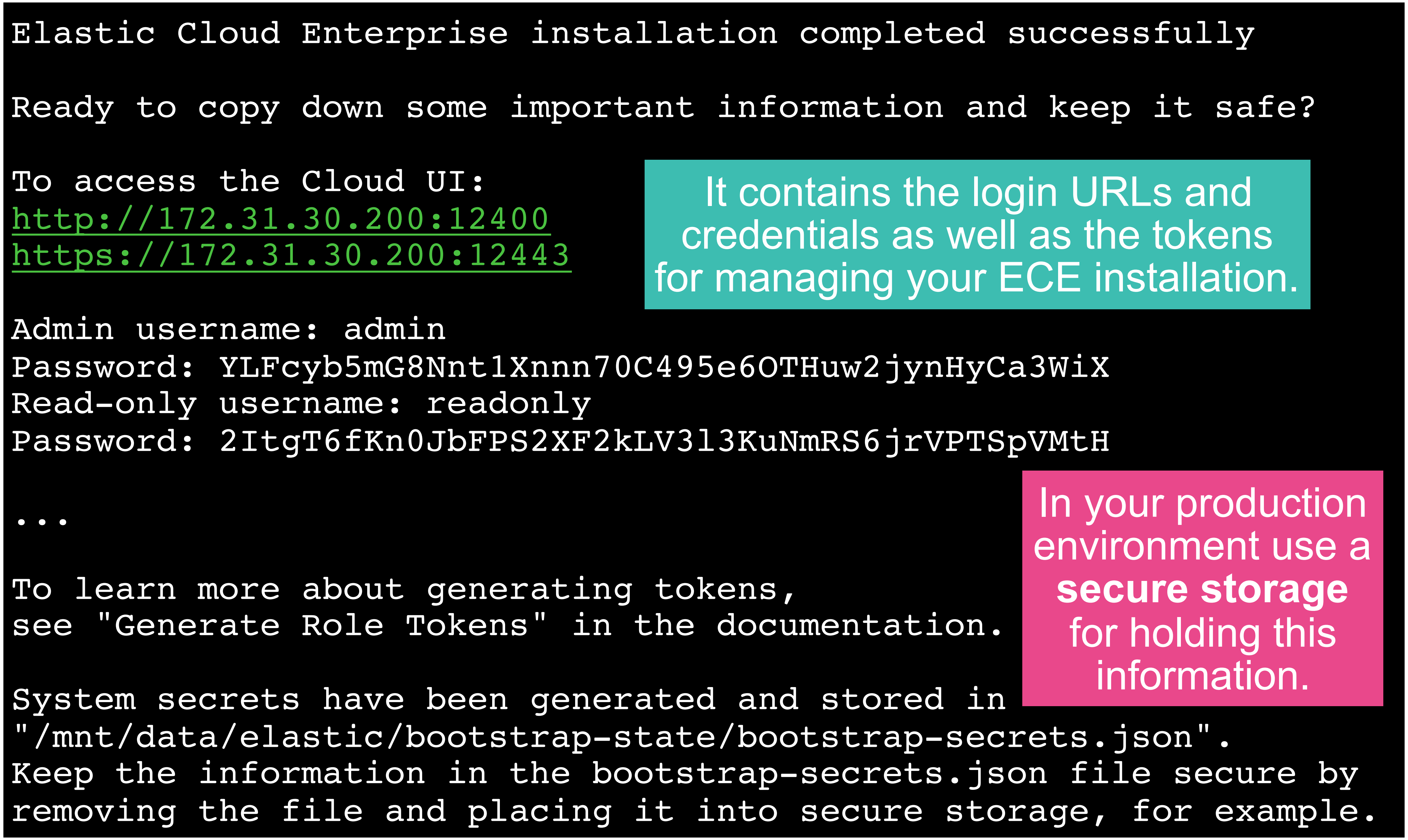
```
bash \
<(curl -fsSL https://download.elastic.co/cloud/elastic-cloud-enterprise.sh) \
install --cloud-enterprise-version 2.1.0
```

The Installation Script

- The installation script will download all the necessary Docker images to install ECE
- If you want to install ECE on hosts without internet access
  - you will need to use the offline installation
  - https://www.elastic.co/guide/en/cloud-enterprise/current/ece-installing-offline.html
- The installation script can also perform other operations
  - upgrade your existing ECE installation
  - add a new Elastic Stack version
  - https://www.elastic.co/guide/en/cloud-enterprise/current/ece-script-reference.html

Installation Script Output

- Save the installation output



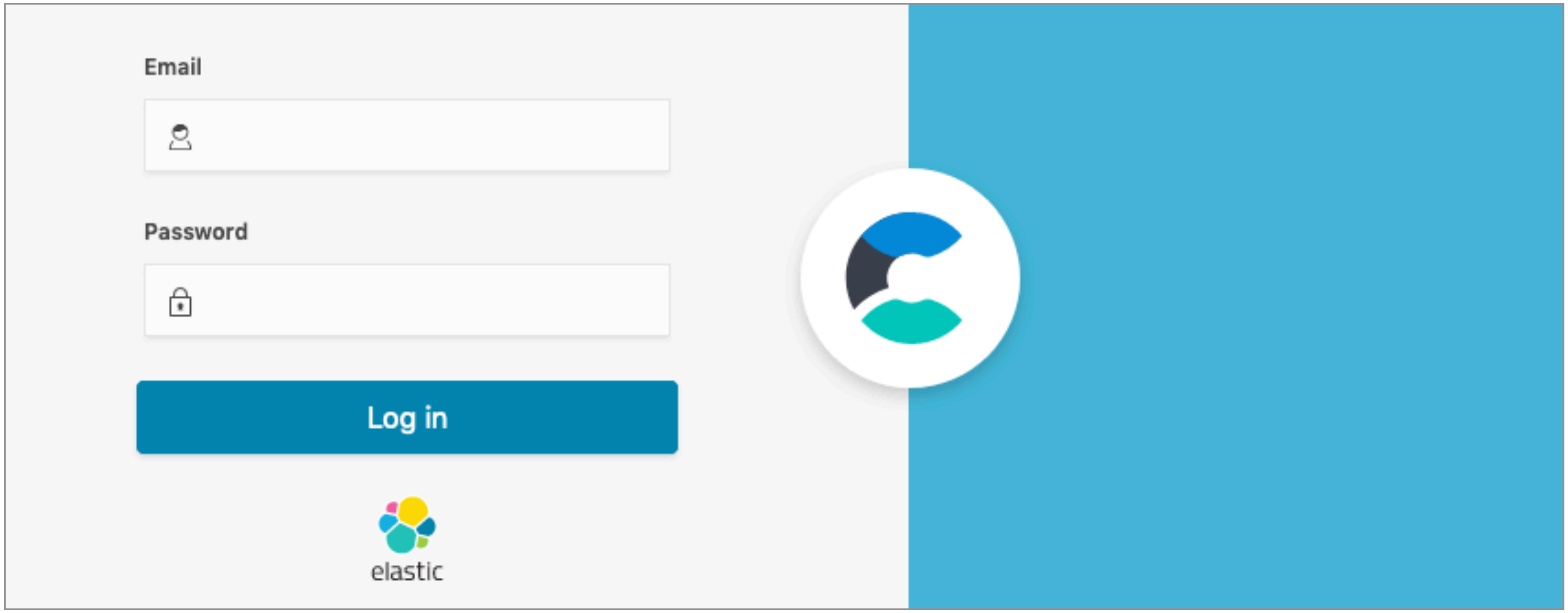
```
Elastic Cloud Enterprise installation completed successfully

Ready to copy down some important information and keep it safe?

To access the Cloud UI:
http://172.31.30.200:12400
https://172.31.30.200:12443

Admin username: admin
Password: YLFcyb5mG8Nnt1Xnnn70C495e6OTHuw2jynHyCa3WiX
Read-only username: readonly
Password: 2ItgT6fKn0JbFPS2XF2kLV3l3KuNmRS6jrVPTSpVMtH

...

To learn more about generating tokens,
see "Generate Role Tokens" in the documentation.

System secrets have been generated and stored in
"/mnt/data/elastic/bootstrap-state/bootstrap-secrets.json".
Keep the information in the bootstrap-secrets.json file secure by
removing the file and placing it into secure storage, for example.
```

It contains the login URLs and credentials as well as the tokens for managing your ECE installation.

In your production environment use a **secure storage** for holding this information.

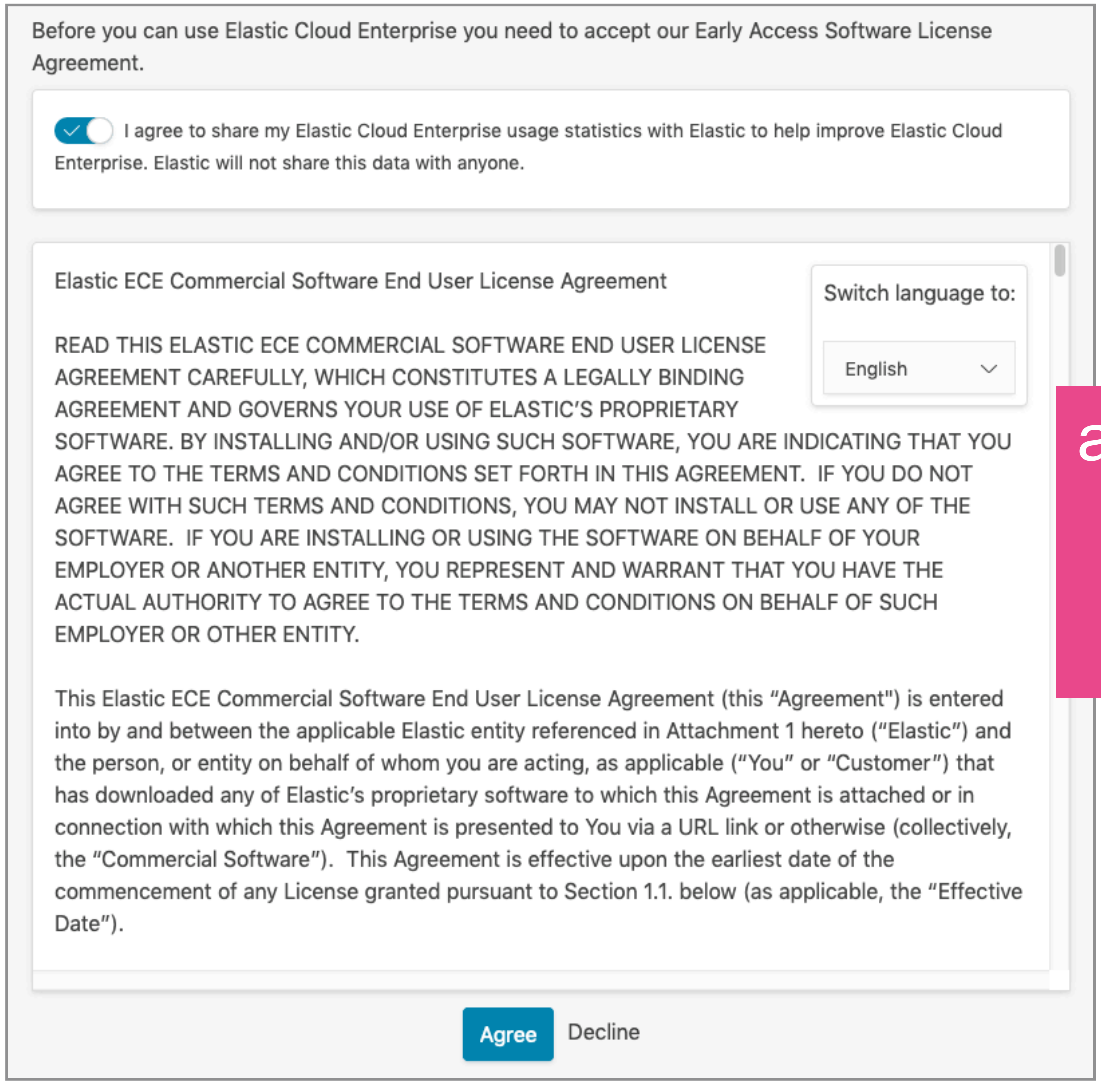
Cloud UI

- You can use the Cloud UI URL from the installer output to access the Elastic Cloud Enterprise UI
  - login as either **admin** or **readonly** user
  - only the admin user has the required privileges to make changes



Logging into the Cloud UI for the First Time

- If you are logging for the first time use the **admin** user



Before you can use Elastic Cloud Enterprise you need to accept our Early Access Software License Agreement.

☑ I agree to share my Elastic Cloud Enterprise usage statistics with Elastic to help improve Elastic Cloud Enterprise. Elastic will not share this data with anyone.

Elastic ECE Commercial Software End User License Agreement

Switch language to: English

READ THIS ELASTIC ECE COMMERCIAL SOFTWARE END USER LICENSE AGREEMENT CAREFULLY, WHICH CONSTITUTES A LEGALLY BINDING AGREEMENT AND GOVERNS YOUR USE OF ELASTIC'S PROPRIETARY SOFTWARE. BY INSTALLING AND/OR USING SUCH SOFTWARE, YOU ARE INDICATING THAT YOU AGREE TO THE TERMS AND CONDITIONS SET FORTH IN THIS AGREEMENT. IF YOU DO NOT AGREE WITH SUCH TERMS AND CONDITIONS, YOU MAY NOT INSTALL OR USE ANY OF THE SOFTWARE. IF YOU ARE INSTALLING OR USING THE SOFTWARE ON BEHALF OF YOUR EMPLOYER OR ANOTHER ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE THE ACTUAL AUTHORITY TO AGREE TO THE TERMS AND CONDITIONS ON BEHALF OF SUCH EMPLOYER OR OTHER ENTITY.

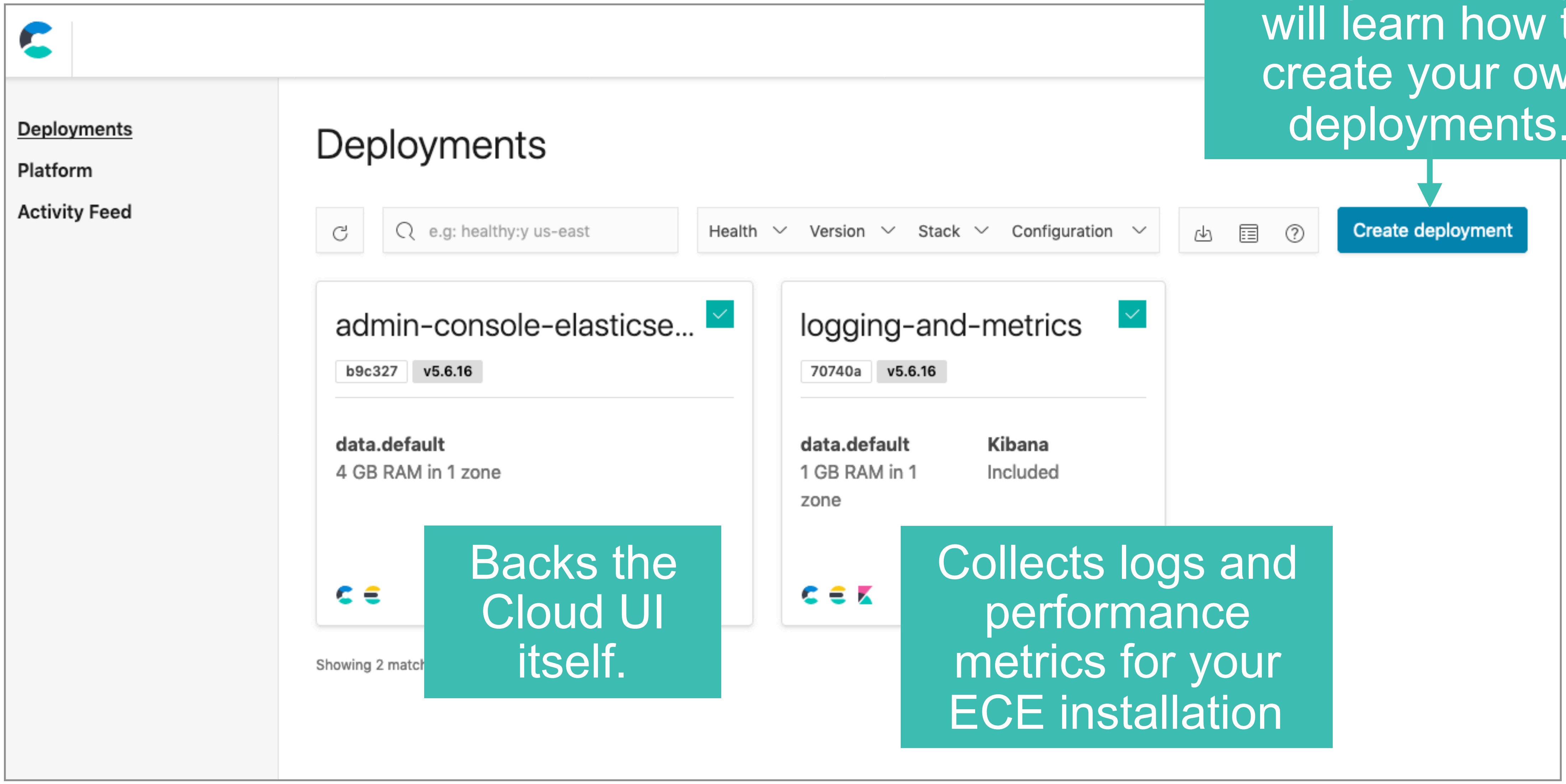
This Elastic ECE Commercial Software End User License Agreement (this "Agreement") is entered into by and between the applicable Elastic entity referenced in Attachment 1 hereto ("Elastic") and the person, or entity on behalf of whom you are acting, as applicable ("You" or "Customer") that has downloaded any of Elastic's proprietary software to which this Agreement is attached or in connection with which this Agreement is presented to You via a URL link or otherwise (collectively, the "Commercial Software"). This Agreement is effective upon the earliest date of the commencement of any License granted pursuant to Section 1.1. below (as applicable, the "Effective Date").

and then read and accept the terms of service after logging in.

- If you lose the password of your administration user
  - you can use the option **reset-adminconsole-password** from the installation script to reset the password

Deployments

- When you log into the Cloud UI you will land at the **Deployments** page
- Every ECE installation always include two deployments by default



Deployments

Platform

Activity Feed

Deployments

e.g: healthy:y us-east

admin-console-elasticse... ✓

b9c327 v5.6.16

data.default
4 GB RAM in 1 zone

logging-and-metrics ✓

70740a v5.6.16

data.default
1 GB RAM in 1 zone

Kibana
Included

Showing 2 match

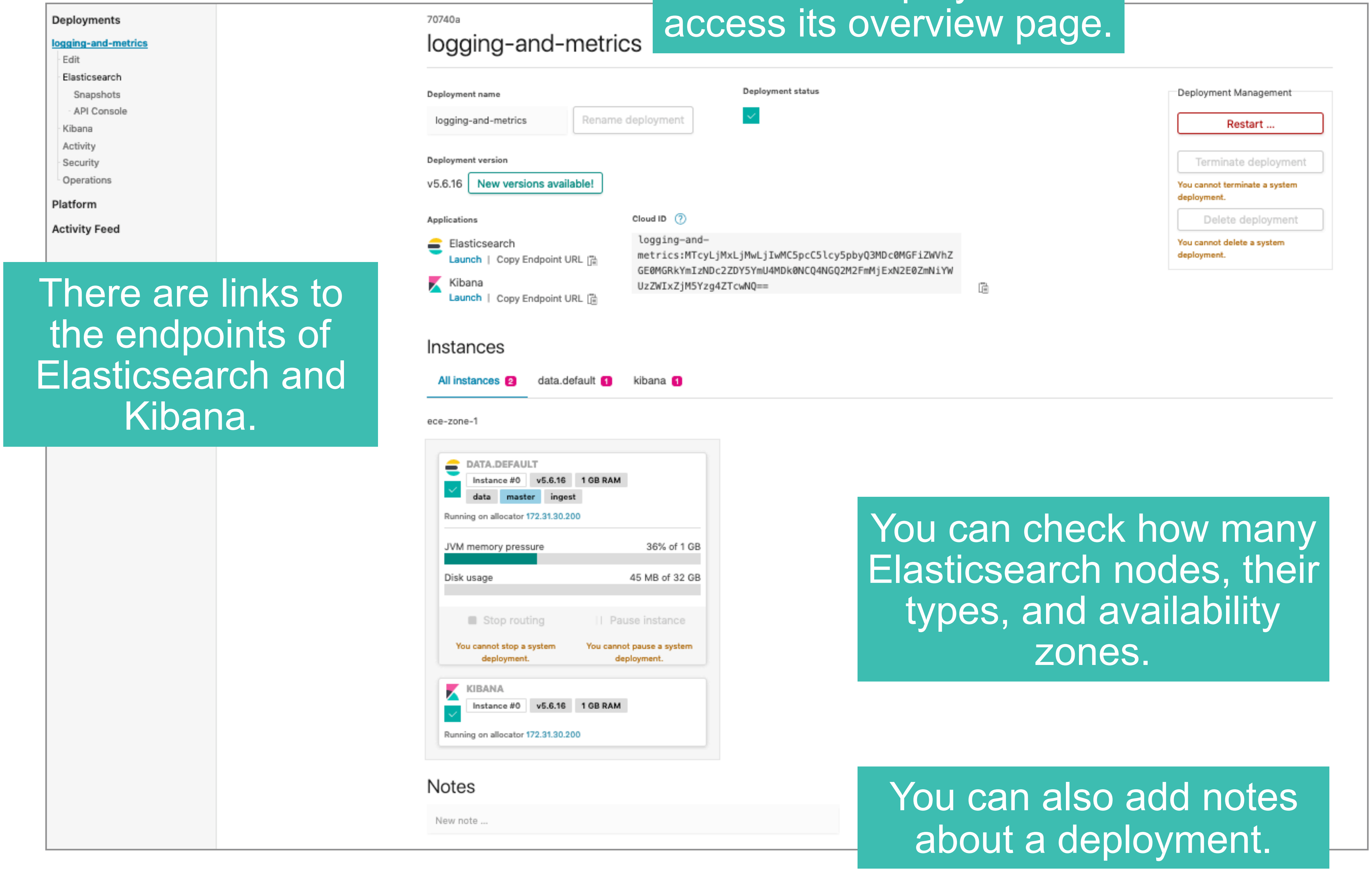
During the labs you will learn how to create your own deployments.

Backs the Cloud UI itself.

Collects logs and performance metrics for your ECE installation

Deployment Overview

Click on a deployment to access its overview page.



70740a

logging-and-metrics

Deployment name: logging-and-metrics

Deployment status: ✓

Deployment version: v5.6.16

Applications

Elasticsearch — Launch | Copy Endpoint URL

Kibana — Launch | Copy Endpoint URL

Cloud ID

```
logging-and-
metrics:MTcyLjMxLjMwLjIwMC5pcC5lcy5pbyQ3MDc0MGFiZWVhZ
GE0MGRkYmIzNDc2ZDY5YmU4MDk0NCQ4NGQ2M2FmMjExN2E0ZmNiYW
UzZWIxZjM5Yzg4ZTcwNQ==
```

Deployment Management

You cannot terminate a system deployment.

You cannot delete a system deployment.

Instances

ece-zone-1

DATA.DEFAULT ✓ Instance #0 | v5.6.16 | 1 GB RAM | data | master | ingest

Running on allocator 172.31.30.200

JVM memory pressure: 36% of 1 GB

Disk usage: 45 MB of 32 GB

You cannot stop a system deployment.

You cannot pause a system deployment.

KIBANA ✓ Instance #0 | v5.6.16 | 1 GB RAM

Running on allocator 172.31.30.200

Notes

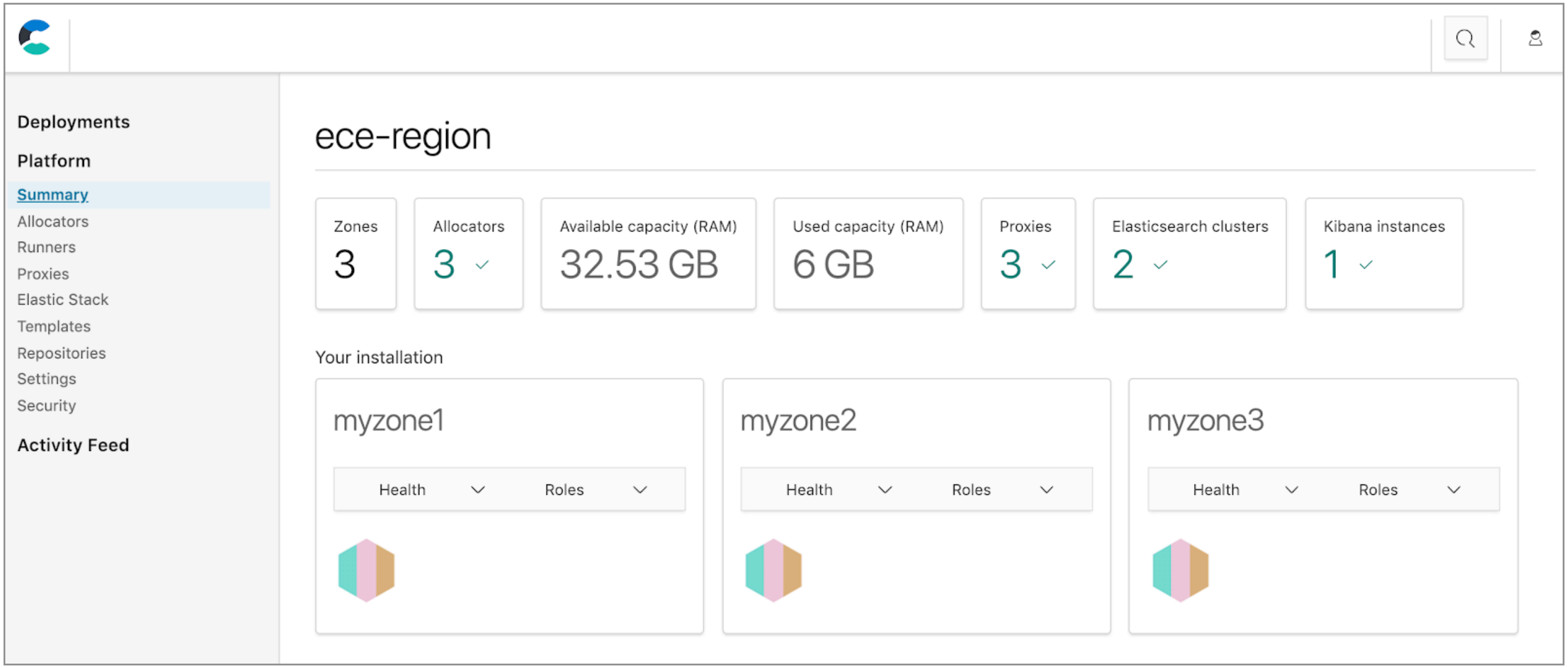
There are links to the endpoints of Elasticsearch and Kibana.

You can check how many Elasticsearch nodes, their types, and availability zones.

You can also add notes about a deployment.

Platform

- Besides checking the details about an individual deployment
- You can use the **Platform** page to check the overall details about your infrastructure



Deployments

Platform

Summary

Allocators

Runners

Proxies

Elastic Stack

Templates

Repositories

Settings

Security

Activity Feed

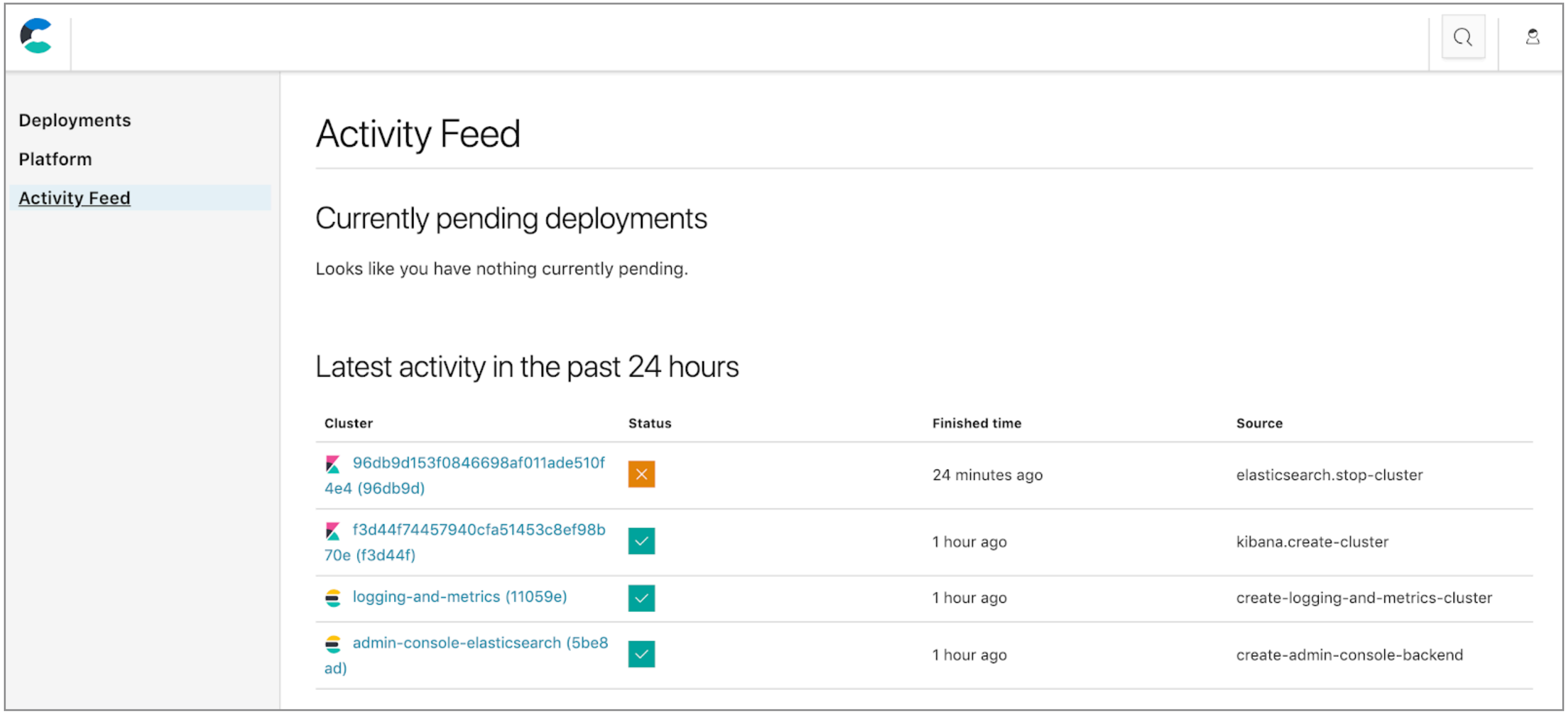
ece-region

Zones	Allocators	Available capacity (RAM)	Used capacity (RAM)	Proxies	Elasticsearch clusters	Kibana instances
3	3 ✓	32.53 GB	6 GB	3 ✓	2 ✓	1 ✓

Your installation

Activity Feed

- The **Activity Feed** page shows recent activity on your infrastructure
- It also shows activities that happened on your clusters in the last 24 hours.



Activity Feed

Currently pending deployments

Looks like you have nothing currently pending.

Latest activity in the past 24 hours

Cluster	Status	Finished time	Source
96db9d153f0846698af011ade510f4e4 (96db9d)	✗	24 minutes ago	elasticsearch.stop-cluster
f3d44f74457940cfa51453c8ef98b70e (f3d44f)	✓	1 hour ago	kibana.create-cluster
logging-and-metrics (11059e)	✓	1 hour ago	create-logging-and-metrics-cluster
admin-console-elasticsearch (5be8ad)	✓	1 hour ago	create-admin-console-backend

Lesson 2

Review - Elastic Cloud Enterprise Interfaces

Summary

- You can use the installation script not just for installing ECE, but also for upgrading your existing ECE installation, resetting the user passwords, adding new Elastic Stack versions and setting the retention period for the logging and metrics indices
- You need to back up the output of the installation script because it contains important information for administering your ECE installation
- The **Deployments** page of the Cloud UI shows all the deployments, and you can explore the overall health of each specific deployment you have
- The **Platforms** page of the Cloud UI shows the overall health of your infrastructure
- The **Activity Feed** page shows recent activity on your infrastructure

Quiz

1. **True** or **False**: There is no way to choose what ECE version the installation script is going to install.
2. Which Cloud UI page can be used to create new Elasticsearch clusters?
3. **True** or **False**: The Platforms page is a good place to check the overall health of your ECE installation.

ECE Fundamentals

Lesson 2

Lab - Elastic Cloud Enterprise Interfaces

elastic

Lesson 3

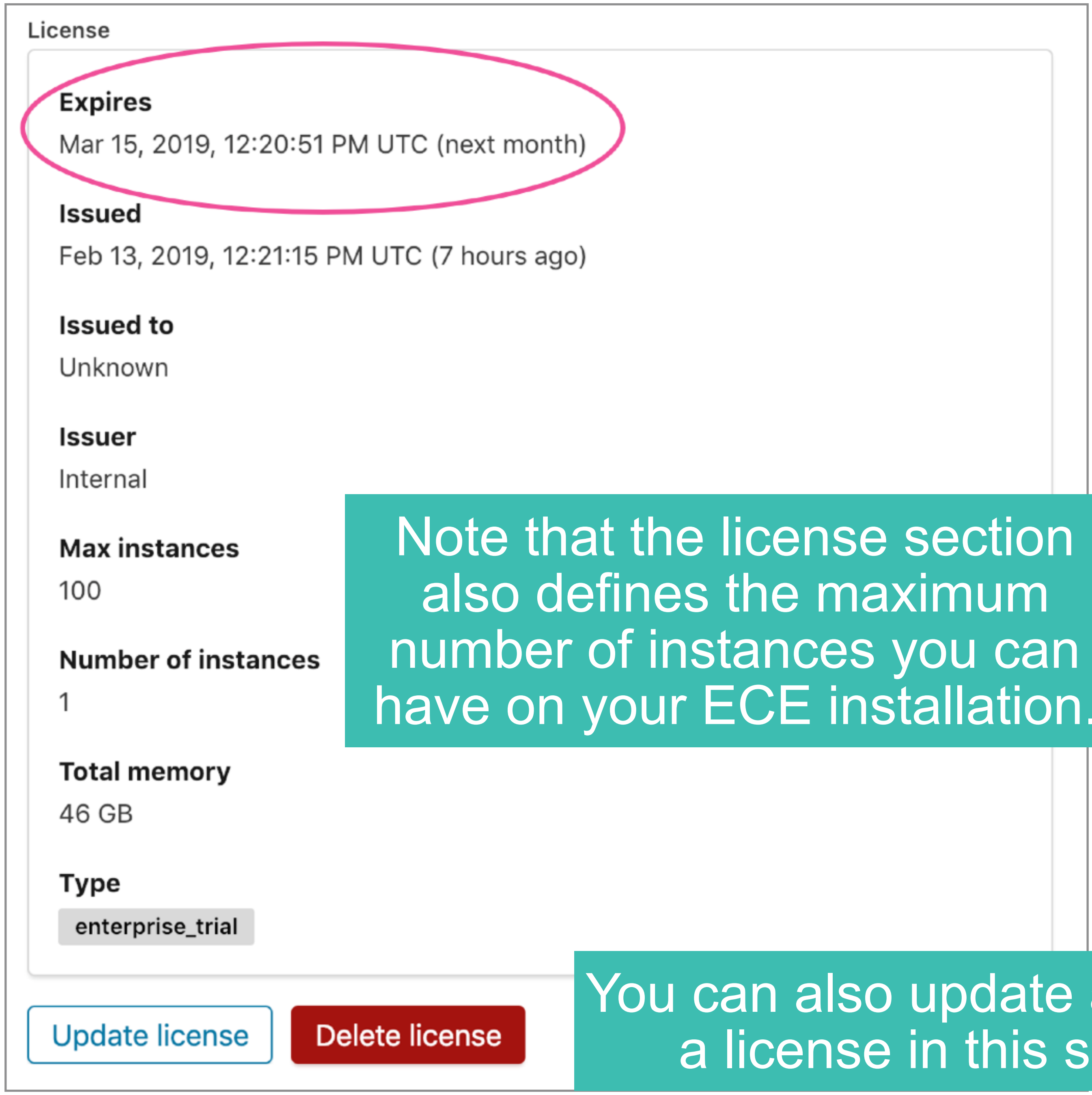
Elastic Cloud Enterprise Features

License

- The use of Elastic Cloud Enterprise requires a valid license
  - which you can obtain from Elastic and add to your installation
- These steps are not required initially
  - because ECE is installed with a trial license
  - which is valid for 30 days
- This means that ECE includes Elastic Stack features
  - such as security, alerting, monitoring, reporting, and canvas
- Full ECE licenses that you obtain from Elastic enable the same products, features, and support that are available to Platinum subscriptions on Elastic Cloud

Check When Your License Will Expire

- Click on the **Platform** page and then on the **Settings** tab



License

Expires
Mar 15, 2019, 12:20:51 PM UTC (next month)

Issued
Feb 13, 2019, 12:21:15 PM UTC (7 hours ago)

Issued to
Unknown

Issuer
Internal

Max instances
100

Number of instances
1

Total memory
46 GB

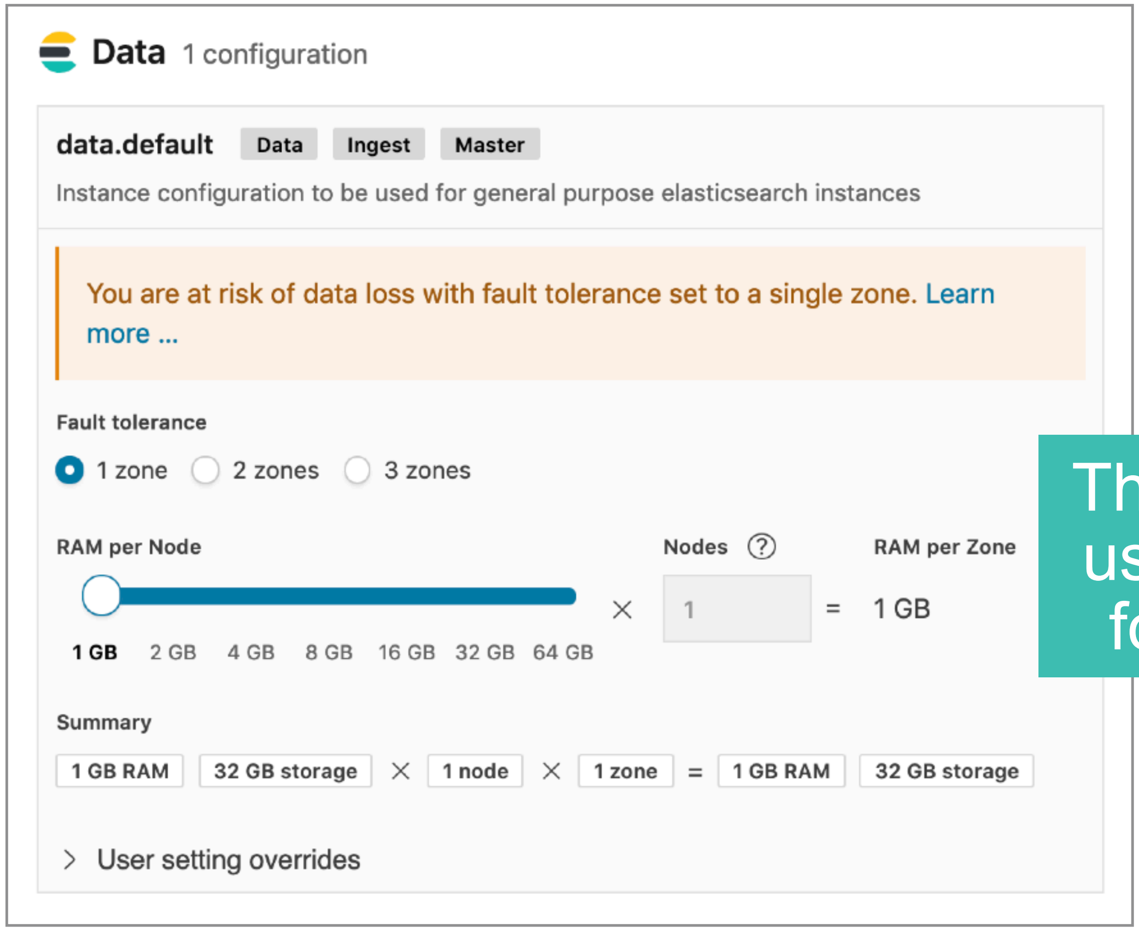
Type
enterprise_trial

Note that the license section also defines the maximum number of instances you can have on your ECE installation.

You can also update and delete a license in this section.

Storage Ratios

- Allows administrators to set the ratio of RAM to disk
  - multiply the amount of RAM by this ratio
  - to determine the amount of disk space
- The default ratio is 1:32



Data 1 configuration

data.default Data Ingest Master

Instance configuration to be used for general purpose elasticsearch instances

You are at risk of data loss with fault tolerance set to a single zone. Learn more ...

Fault tolerance

● 1 zone ○ 2 zones ○ 3 zones

RAM per Node: **1 GB** (2 GB, 4 GB, 8 GB, 16 GB, 32 GB, 64 GB) × Nodes: 1 = RAM per Zone: 1 GB

Summary

1 GB RAM | 32 GB storage × 1 node × 1 zone = 1 GB RAM | 32 GB storage

> User setting overrides

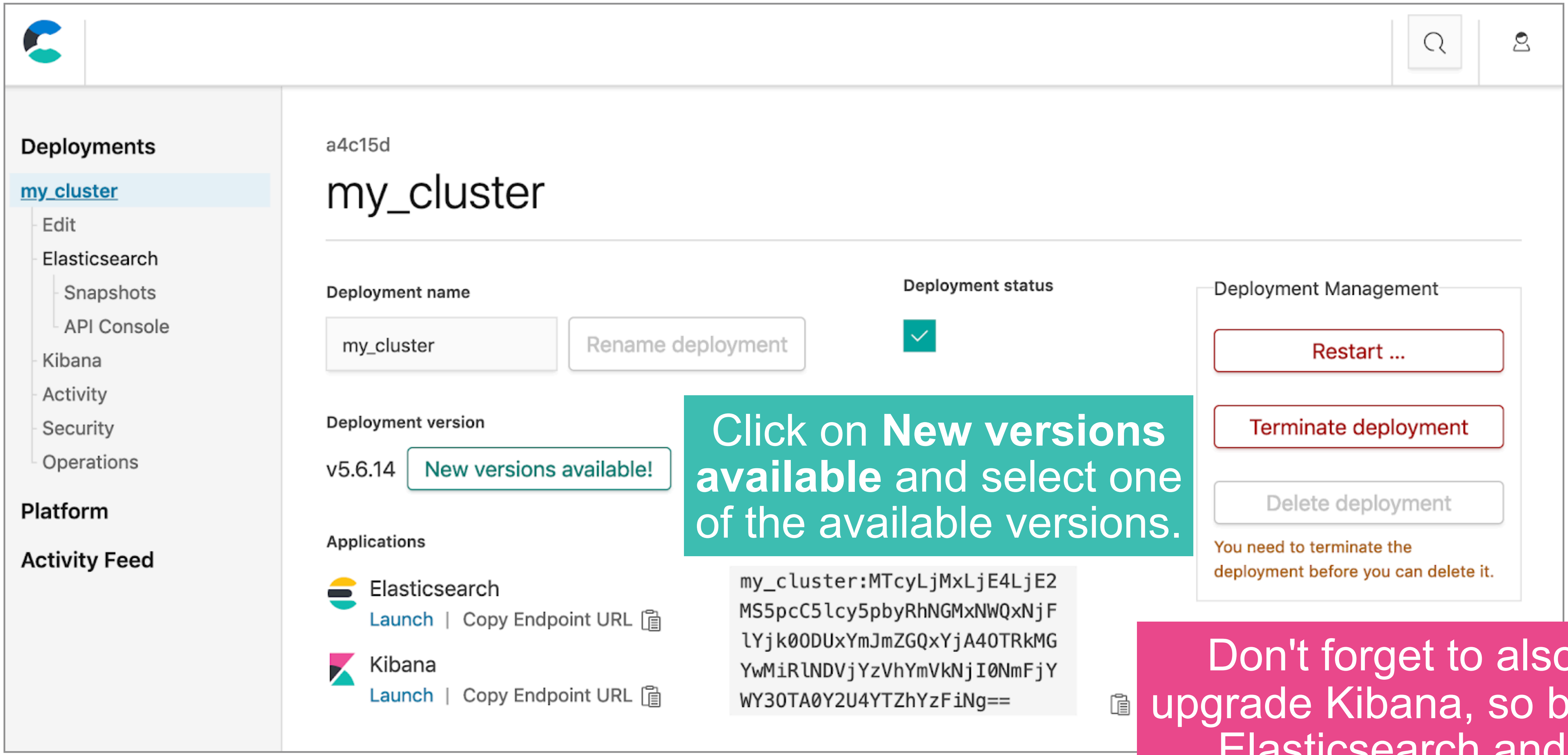
This means that ECE will use 32 GB of disk space for each 1 GB of RAM.

Custom Storage Ratios

- The default storage ratio does not address all use cases
- For memory-intensive workloads
  - more RAM can improve performance
  - use high-performance SSDs and 1:16 ratio (or even 1:8)
- For logging workloads
  - more storage space can be more cost-effective
  - use a ratio from 1:48 to 1:96
  - as data sizes are typically much larger
  - when compared to the RAM needed for logging
  - you can also step down from SSDs to spinning media for costs

Upgrading a Cluster

- Upgrading a deployment is easy
  - and you can accomplish that with just a few clicks



a4c15d

my_cluster

Deployment name: my_cluster

Deployment status: ✓

Deployment version: v5.6.14

Applications

Elasticsearch
Launch | Copy Endpoint URL

Kibana
Launch | Copy Endpoint URL

```
my_cluster:MTcyLjMxLjE4LjE2
MS5pcC5lcy5pbyRhNGMxNWQxNjF
lYjk0ODUxYmJmZGQxYjA4OTRkMG
YwMiRlNDVjYzVhYmVkNjI0NmFjY
WY3OTA0Y2U4YTZhYzFiNg==
```

Deployment Management

You need to terminate the deployment before you can delete it.

Click on **New versions available** and select one of the available versions.

Don't forget to also upgrade Kibana, so both Elasticsearch and Kibana versions match.

Prepare Before Upgrade

- When upgrading from one recent major version to the next
  - it is recommended that you prepare ahead of time
- This will make the process go smoothly
  - because these upgrades require a full cluster restart
  - which means you will have some downtime during the upgrade
- Thus, it is a good idea to create a new deployment
  - with the latest major version you want to upgrade to
  - reindex everything and make sure index requests are temporarily sent to both clusters
- With the new cluster ready, tested, and working
  - you can then remove the old deployment

Elastic Stack Versions

- ECE ships with a number of different versions of the Stack
  - Elasticsearch and Kibana 5.6.x
  - Elasticsearch and Kibana 6.6.x
- You might want to add new Elastic Stack versions as soon as they become available
- You might want to add the Elastic Stack versions that shipped with a version of ECE that you upgraded to
- New or updated versions are prepared to work with ECE
  - and provided as packs that you can add to your ECE installation
- During the labs you are going to learn how to add new Elastic Stack packs to your ECE installation

Snapshotting

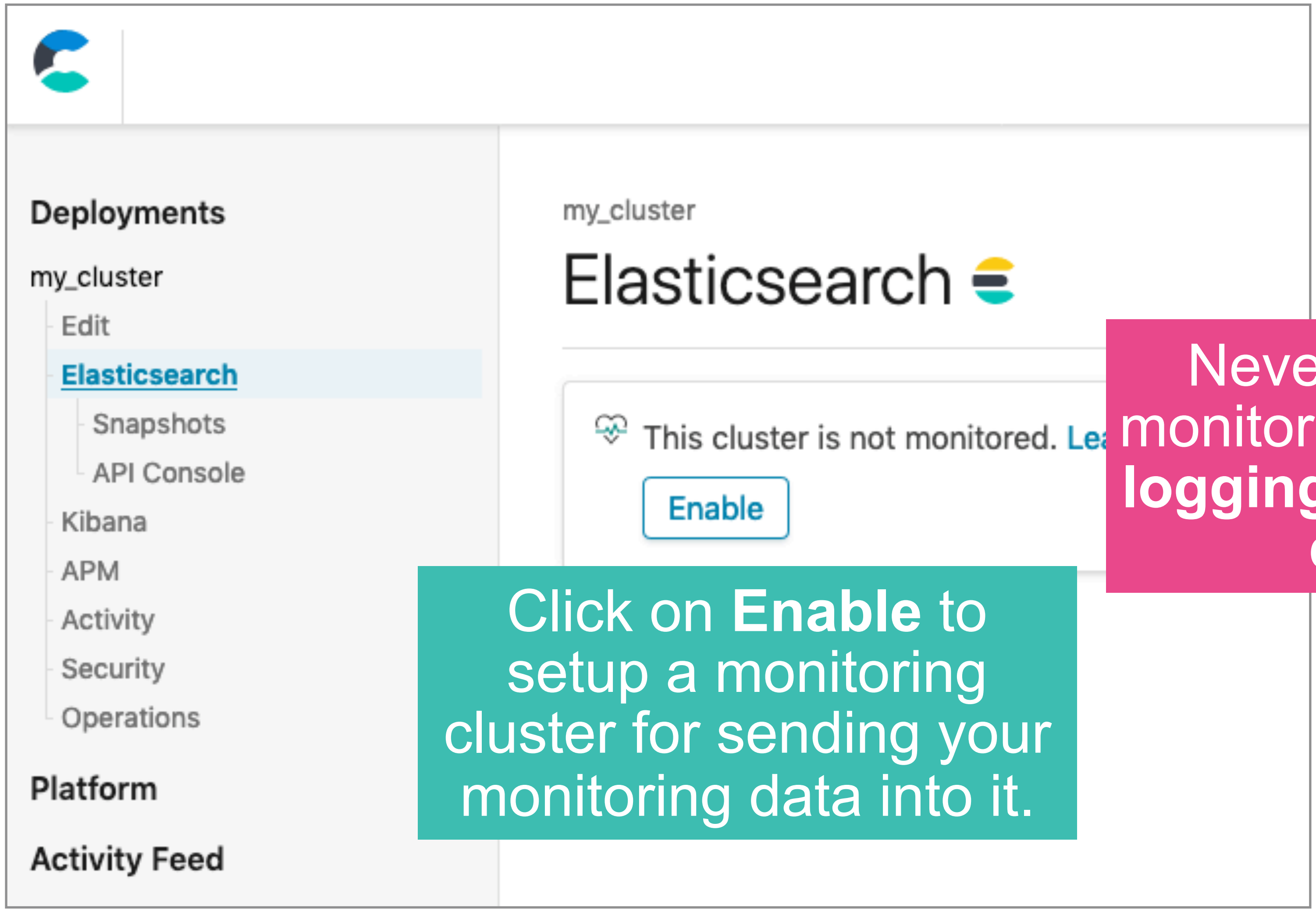
- Snapshot repositories and managed for your entire ECE installation
  - and can be specified for an Elasticsearch cluster
  - when you create or manage it
- After you have configured a snapshot repository
  - a snapshot is taken every 30 minutes
  - or at the interval you want
- Currently, ECE supports the following repositories
  - Amazon S3
  - Microsoft Azure
  - Google Cloud Storage

Monitoring Your ECE Installation

- ECE by default collects monitoring data for your installation
- Filebeat and Metricbeat ship the data
- Data is collected on every runner
- Data gets sent to monitoring indices
    - which live in a dedicated **logging-and-metrics** cluster

Monitoring Your Deployments

- The **logging-and-metrics** deployment monitors your ECE installation only
- But you can also monitor your deployments through Kibana
  - with the monitoring feature that comes in ECE



This cluster is not monitored. Lea

Never send your monitoring data to the **logging-and-metrics** cluster.

Click on **Enable** to setup a monitoring cluster for sending your monitoring data into it.

Security

- ECE has some built-in security features
  - such as IP filtering
  - identity authorization services for SAML or LDPA
  - Elasticsearch Keystore
- ECE also supports most of the Elastic Stack security features
  - prevent unauthorized to deployments with password protection
  - and role-based access control
  - preserve the integrity of your data with message authentication
  - and SSL/TLS encryption

What is Encrypted? And What is Not?

- ECE does not implement encryption at rest out of the box
  - hosts running ECE must be configured with disk-level encryption
  - such as **dm-crypt**
  - snapshot targets must ensure that data is encrypted at rest
- ECE provides full encryption of all network traffic
  - when using Elasticsearch 6.0 or higher
- TLS is supported when interacting with the RESTful API
  - and for the proxy layer that routes requests to clusters
  - internally, administrative services also ensure TLS
- Traffic between nodes in a cluster, and between proxies and clusters, is currently **not** encrypted
  - in Elasticsearch versions lower than 6.0

Lesson 3

Review - Elastic Cloud Enterprise Features

Summary

- The use of ECE requires a valid license, though it comes with a trial license by default to make it easier to get started
- By default, ECE provisions clusters at a 1:32 ratio, which means that you need 32GB of storage for each 1GB RAM
- You cannot downgrade after upgrading, so plan ahead to make sure that your applications still work after upgrading
- Snapshots come out-of-the box and you just need to configure the repositories, so ECE can take snapshots every 30 minutes or at the interval you specify
- You should send metrics for production clusters to a dedicated monitoring cluster, but never to the **logging-and-metrics** cluster that is used by ECE
- For data at rest, ECE does not implement encryption out of the box

Quiz

1. **True** or **False**: You can use the system deployment **logging-and-metrics** to send the monitoring data of your deployments.
2. Which security feature ECE does not implement out of the box?
3. **True** or **False**: The ability to backup your Elasticsearch data comes out-of-the-box.

Lesson 3

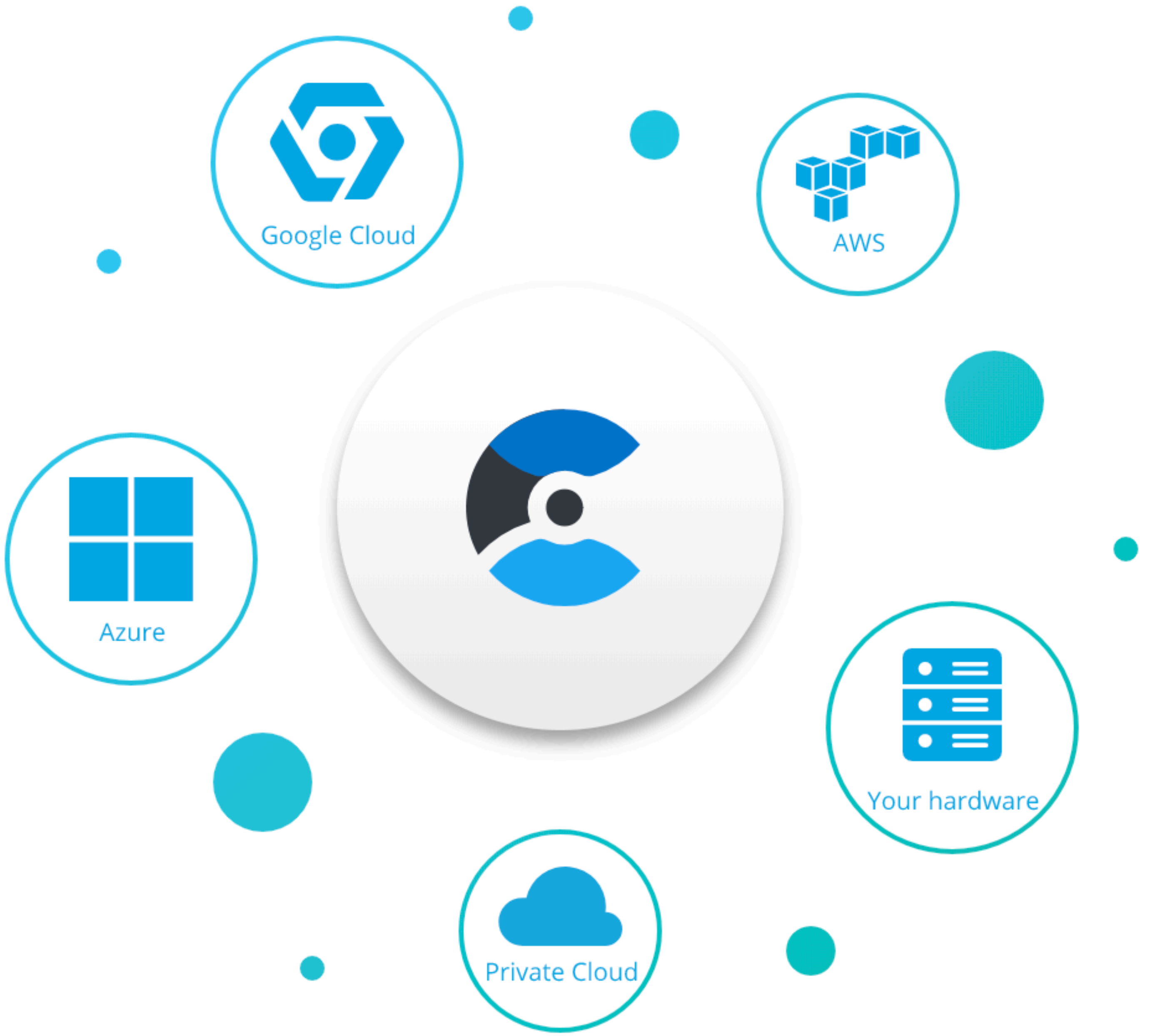
Lab - Elastic Cloud Enterprise Features

Lesson 4

Learn More

elastic

ECE Fundamentals



Next Steps

- This is an introductory course to ECE
- Next, deploy a development/test environment in your own infrastructure and try
  - create a test deployment and migrate your current indices to it
  - add more hosts and availability zones to your ECE infrastructure
  - add your own load balancer and a snapshot repository
  - configure ECE for deployment templates
  - install your security certificates and try ip filtering
  - add some capacity to your ECE installation
  - learn how to work around host maintenance or failure
  - if you received a license from Elastic, manage your licenses

References

- https://www.elastic.co/products/ece
- https://www.elastic.co/guide/en/cloud-enterprise/current/ece-quick-start.html
- https://www.elastic.co/guide/en/cloud-enterprise/current/ece-playbook.html

Other ECE Courses

- Join us on other trainings and deep dive into ECE according to your needs
- Installing and Scaling ECE
  - add more instances and availability zones to your infrastructure
  - explore deployment templates to accommodate different hardware settings
  - learn how to identify if a problem is caused by the ECE infrastructure or if it is an instance issue

ECE Fundamentals

Lesson 4

Review - Learn More

elastic

Summary

- ECE can be deployed anywhere - on public or private clouds, virtual machines, or even on bare metal hardware
- The Cloud UI provides web-based access for administrators to manage and monitor their ECE installation
- ECE was built on exactly the same code base that the Elasticsearch service runs, so you can enjoy the same battle tested software with the same set of features used to manage thousands of clusters across multiple cloud providers

Quiz

1. **True** or **False**: You cannot deploy Elastic Cloud Enterprise on public clouds, but only on your private infrastructure.
2. **True** or **False**: The Cloud UI makes it easier to manage and deploy your Elasticsearch clusters.
3. **True** or **False**: Elastic Cloud Enterprise uses the same software that is used to run the Elasticsearch service, so when you use ECE, you benefit from all the know-how behind it.

Quiz Answers

Elastic Cloud Enterprise Architecture

1. True. You can choose where you run Elasticsearch and Kibana: physical hardware, virtual environment, private cloud, private zone in a public cloud, or just plain cloud.
2. Ensures all containers needed to run a single ECE instance roles are online and healthy.
3. False. You need at least 8GB of free memory to run ECE.

Elastic Cloud Enterprise Interfaces

1. False. You can always use the --cloud-enterprise-version parameter of the install option to choose what ECE version you want to install.
2. The correct answer is the Deployments page. Use the Create Deployment button to create new Elasticsearch clusters.The Platforms page is used to check the overall health of your infrastructure, while the Activity Feed is used to check recent activity in your infrastructure.
3. True. You can use the Platforms page to check the overall health of your infrastructure.

Elastic Cloud Enterprise Features

1. False. You should never send metrics of your production deployments to the logging-and-metrics cluster, but rather to a dedicated monitoring cluster instead.
2. Encrypted data at rest is not implemented by ECE. To ensure encryption at rest for all data managed by ECE, you must use disk-level encryption.
3. True. You can use snapshots to backup your Elasticsearch indices and recover from a failure.

Learn More

1. False. ECE can be deployed anywhere - on public or private clouds, virtual machines, or even on bare metal hardware.
2. True. The Cloud UI provides web-based access that makes it easier for administrators to manage and monitor their ECE installation.
3. True. ECE was built on exactly the same code base that the Elasticsearch service runs, so when you use ECE, you benefit from all the know-how behind it.