

STONE
DOOR 
GROUP



MIRANTIS

Docker Tips for Better Security

Amber Ernst + Bill Mills

About Stone Door Group

- Mirantis Solutions Integrator that helps companies implement DevOps best practices using Docker & Kubernetes
- Docker CE to EE Accelerator Engagement
 - Complete solution for migrating applications to a secure production environment
 - Includes software licensing and consulting services needed to get Docker EE implemented
 - Migrate application workloads and ensure security/regulatory compliance
- Free 5-day trial of Docker EE available on our website

<http://www.stonedoorgroup.com/docker-launcher-request>

Housekeeping

- Trouble with your connection?
 - You may dial in via phone - [1.888.788.0099](tel:18887880099) Webinar ID: [742 327 577](https://www.stonedoorgroup.com/webinars/742327577)
 - Email us at webinar@stonedoorgroup.com for assistance
- Q&A
 - Throughout the webinar participants may enter Questions into the Q&A panel, located at the bottom of your screen
 - Our instructors will address your questions following their presentation
- Webinar Recording & Follow Up
 - Following today's session, we will distribute a link to the webinar recording as well as a link to today's presentation

Connect with us at letsdothis@stonedoorgroup.com

Docker Enterprise Social Distance Learning Series

Register here > <https://www.stonedoor.io/docker-webinar>

Webinar	Title	Event Date/Time	Description
1	Get Docker Enterprise Edition Running in an Hour	April 16, 2020 9.00 - 10.00am PST	Quickly install or upgrade to Docker Enterprise Edition
2	Docker Tips for Better Productivity	April 23, 2020 9.00 - 10.00am PST	Gain an edge in Docker administration
3	Docker Tips for Better Security	May 7, 2020 9.00 - 10.00am PST	Leverage the features of Docker Enterprise Edition for corporate security and regulatory compliance
4	Kubernetes Tips for Better Productivity	May 14, 2020 9.00 - 10.00am PST	Gain an edge in Kubernetes implementation

STONE
DOOR 
GROUP



MIRANTIS

Docker Tips for Better Security

Amber Ernst + Bill Mills

About Stone Door Group

- Mirantis Solutions Integrator that helps companies implement DevOps best practices using Docker & Kubernetes
- Docker CE to EE Accelerator Engagement
 - Complete solution for migrating applications to a secure production environment
 - Includes software licensing and consulting services needed to get Docker EE implemented
 - Migrate application workloads and ensure security/regulatory compliance
- Free 5-day trial of Docker EE available on our website

<http://www.stonedoorgroup.com/docker-launcher-request>

Housekeeping

- Trouble with your connection?
 - You may dial in via phone - [1.888.788.0099](tel:18887880099) Webinar ID: [742 327 577](https://www.stonedoorgroup.com/webinars/742327577)
 - Email us at webinar@stonedoorgroup.com for assistance
- Q&A
 - Throughout the webinar participants may enter Questions into the Q&A panel, located at the bottom of your screen
 - Our instructors will address your questions following their presentation
- Webinar Recording & Follow Up
 - Following today's session, we will distribute a link to the webinar recording as well as a link to today's presentation

Connect with us at letsdothis@stonedoorgroup.com

Docker Enterprise Social Distance Learning Series

Register here > <https://www.stonedoor.io/docker-webinar>

Webinar	Title	Event Date/Time	Description
1	Get Docker Enterprise Edition Running in an Hour	April 16, 2020 9.00 - 10.00am PST	Quickly install or upgrade to Docker Enterprise Edition
2	Docker Tips for Better Productivity	April 23, 2020 9.00 - 10.00am PST	Gain an edge in Docker administration
3	Docker Tips for Better Security	May 7, 2020 9.00 - 10.00am PST	Leverage the features of Docker Enterprise Edition for corporate security and regulatory compliance
4	Kubernetes Tips for Better Productivity	May 14, 2020 9.00 - 10.00am PST	Gain an edge in Kubernetes implementation

STONE
DOOR 
GROUP



Docker Tips for Better Security

Amber Ernst + Bill Mills

About Stone Door Group

- Mirantis Solutions Integrator that helps companies implement DevOps best practices using Docker & Kubernetes
- Docker CE to EE Accelerator Engagement
 - Complete solution for migrating applications to a secure production environment
 - Includes software licensing and consulting services needed to get Docker EE implemented
 - Migrate application workloads and ensure security/regulatory compliance
- Free 5-day trial of Docker EE available on our website

<http://www.stonedoorgroup.com/docker-launcher-request>

Housekeeping

- Trouble with your connection?
 - You may dial in via phone - **1.888.788.0099** Webinar ID: **742 327 577**
 - Email us at webinar@stonedoorgroup.com for assistance
- Q&A
 - Throughout the webinar participants may enter Questions into the Q&A panel, located at the bottom of your screen
 - Our instructors will address your questions following their presentation
- Webinar Recording & Follow Up
 - Following today's session, we will distribute a link to the webinar recording as well as a link to today's presentation

Connect with us at letsdothis@stonedoorgroup.com

Docker Enterprise Social Distance Learning Series

Register here > <https://www.stonedoor.io/docker-webinar>

Webinar	Title	Event Date/Time	Description
1	Get Docker Enterprise Edition Running in an Hour	April 16, 2020 9.00 - 10.00am PST	Quickly install or upgrade to Docker Enterprise Edition
2	Docker Tips for Better Productivity	April 23, 2020 9.00 - 10.00am PST	Gain an edge in Docker administration
3	Docker Tips for Better Security	May 7, 2020 9.00 - 10.00am PST	Leverage the features of Docker Enterprise Edition for corporate security and regulatory compliance
4	Kubernetes Tips for Better Productivity	May 14, 2020 9.00 - 10.00am PST	Gain an edge in Kubernetes implementation

Week #2 - Prize Winners

US Winners

Ranthy R.	TX	Jeff H.	TN
Gary Lon B.	OK	Alan H.	VA
Michael P.	OH	Glenn Z.	MD
Nagendran J.	CA	Ryan J.	MD
Paul S.	OH	Greg B.	VA
David A.	WY	Bernard N.	TX
Zai F.	NY	Jose B.	VA
Mohammed P.	IL	Joe C.	NJ
Prakash N.	CA	Quang L.	MD
Ed B.	NY	Ashok S.	NY

International Winners

Bruce C.	UK
Vokan G.	Turkey
Enrico P.	Canada
Mateusz P.	Italy
Subhranshu D.	Germany

Congratulations to our prize winners from our previous event!

Introduction



Head of Curriculum
Development, Mirantis

Bill currently teaches,
develops and maintains
the Docker Enterprise
training stack, and is
based in Brooklyn, NY.

Bill Mills



Docker Accredited
Instructor and Certified
Associate, Stone Door
Group

Amber Ernst is a Docker
Certified Associate and
Docker Accredited
Instructor for Stone Door
Group.

Amber Ernst

A Refresher on Docker

- Scalable
- Easy to maintain
- Easier to get set up



Community vs Enterprise Edition

Docker Enterprise

- Paid Mirantis subscription
- Includes support from Mirantis
- Predictable bi-annual releases
- Certified partner ecosystem
- Enterprise-grade features (security, management, automation)



Recommended for production use

Community Edition

- Free “do it yourself” dev & ops
- Does not include support
- Quarterly stable release for ops

Managing Access

Managing Access- Engine and Node Security

To take advantage of the built-in security configurations and policies, make sure they run the latest version on Docker Enterprise.

- FIPS
 - Supports Cryptographic security functions
- Seccomp
 - used to restrict the syscalls available to a given process
- AppArmor/SELinux
 - security modules similar to Seccomp in their use of profiles

Demo: Seccomp

```
$ grep CONFIG_SECCOMP= /boot/config-$(uname -r)
```

Demo: AppArmor & SELinux

	App Armor	SELinux
Type of Security	<ul style="list-style-type: none">● Pathname based system● Labeling/ re-labeling fs not required	<ul style="list-style-type: none">● Label based, associate to inode● Attaches labels to all files, processes
Features	<ul style="list-style-type: none">● Based on principle of least privilege● Pathnames-easy to understand/audit	<ul style="list-style-type: none">● Based on the default deny principle● Not all applications preserve labels
Ease of use	<ul style="list-style-type: none">● Auditable policies● New/advanced users	<ul style="list-style-type: none">● Complex policy language● Advanced users

Docker Enterprise Access Control

DE enhances Role-based Access Control (RBAC) policies. These enhancements allow organizations to have more granular controls and also flexible policy modeling.

Common questions:

- How do I prevent different teams from viewing or interacting with each other's applications in our infrastructure?
- How can I enforce scheduling on certain nodes in my cluster?
- How can I manage my access policies in a clear and understandable manner?

Docker Enterprise Access Control

Docker EE Access Control is a policy-based model, using access control lists referred to as **grants** that dictate access between users and cluster resources.

A grant is a rule that states **who** can do **what actions**, against **which resource**.

- Roles (what operations can be performed by whom)
- Collections (Cluster resources)
- Subjects (a user, team, org, or service account)

Demo:

Docker Enterprise
Universal Control Plane
v3.2.5

6 Users

admin

Dashboard

Access Control

- Orgs & Teams
- Users**
- Roles
- Grants

Shared Resources

Kubernetes

Swarm

STATUS

USER NAME

FULL NAME

Active

admin

Active

barry

barry

Active

chloe

chloe

Active

joey

joey

Active

kelly

kelly

Active

shawn

shawn

Actions

Create

Content Control

Docker Trusted Registry

Docker Trusted Registry enforces the "Secure by Default" theme with two features:

- Image Signing (Notary project)
- Image Scanning

DTR shares authentication with UCP, simplifying setup and providing a well-built RBAC without any added effort

Docker Trusted Registry stores metadata and layer data in two separate locations:

- metadata- locally in a database that is shared between replicas
- layer data- in a configurable location

Demo: DTR

```
[centos@manager-0 ~]$ docker run -it --rm docker/dtr install \  
> --ucp-node node-1 \  
> --ucp-username admin \  
> --ucp-url https:///<your.manager0.ip.address> \  
> --dtr-external-url https://<your.node-3.ip.address> \  
> --ucp-insecure-tls
```

Security Scanning in DTR

To enable security scanning in DTR:

- Log in to your DTR instance with an administrator account
- Click **Settings** in the left navigation >Click **Security** tab
- Click the **Enable scanning** toggle
- provide a security database for the scanner*

Set repository scanning mode:

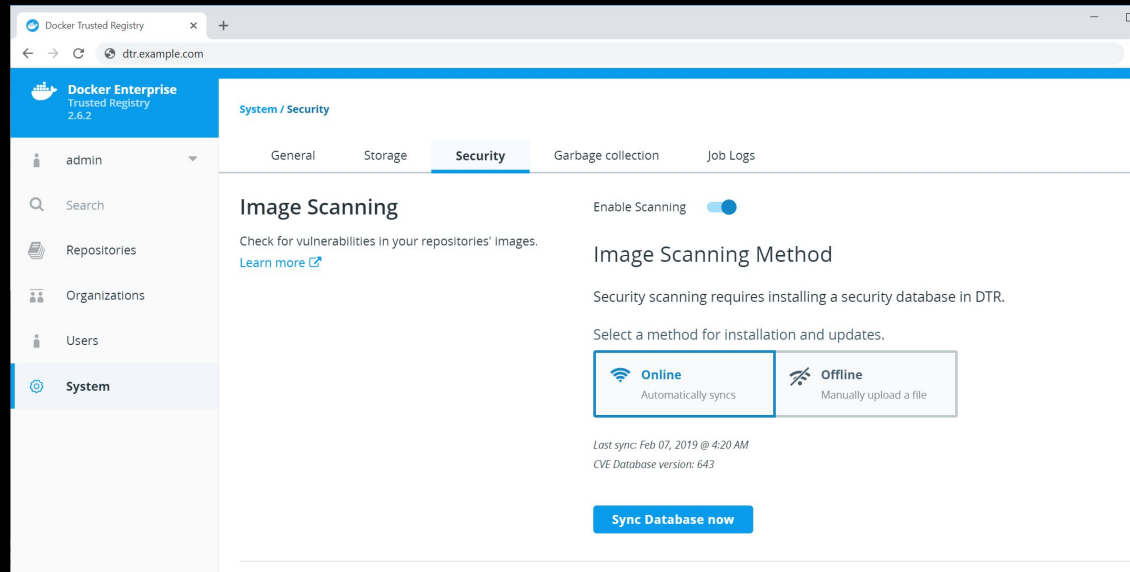
- Scan on push
- Scan manually

* Security scanning will not function until DTR has a security database to use

Demo: Security Scanning in DTR

Docker Trusted Registry (DTR)- image storage solution

- Securely store and manage the Docker images you use in your applications
 - Built-in security scanner discovers vulnerabilities in the images



The screenshot shows the Docker Trusted Registry (DTR) web interface. The browser address bar displays 'dtr.example.com'. The page title is 'Docker Enterprise Trusted Registry 2.6.2'. The left sidebar contains navigation options: 'admin', 'Search', 'Repositories', 'Organizations', 'Users', and 'System' (which is selected). The main content area is titled 'System / Security' and has tabs for 'General', 'Storage', 'Security' (selected), 'Garbage collection', and 'Job Logs'. Under the 'Security' tab, the 'Image Scanning' section is visible. It includes a toggle for 'Enable Scanning' which is turned on. Below this, there is a section for 'Image Scanning Method' with the text: 'Security scanning requires installing a security database in DTR. Select a method for installation and updates.' Two options are presented: 'Online' (Automatically syncs) and 'Offline' (Manually upload a file). The 'Online' option is selected. At the bottom, it shows 'Last sync: Feb 07, 2019 @ 4:20 AM' and 'CVE Database version: 643'. A blue button labeled 'Sync Database now' is located at the bottom of the section.

Image safety

- Use trustworthy images
- Require signed images
- Signing images with Docker Content Trust

Using Trustworthy Images

The best practice is to use Docker Official Images

- curated set of Docker repositories
- hosted on Docker Hub

Some examples:

alpine, ubuntu, python, Golang, Redis, Postgres, etc.

Each has over 10M downloads and has a dedicated team that reviews and publishes them.

Require Signed Images

You can ensure that images are signed by using Docker Content Trust.

Docker Content Trust (DCT) gives you the ability to use digital signatures for data sent to and received from remote Docker registries.

- Prevents users from working with tagged images unless they contain a signature

*Content Trust is disabled by default

Demo: Enabling Content Trust

```
Export DOCKER_CONTENT_TRUST=1
```


Signing Images With Content Trust

Within the Docker CLI we have the ability to sign and push a container image with `$ docker trust` commands.

To sign a Docker Image, you first need a delegation key pair.

This can be generated locally with:

```
$ docker trust key generate
```

With DE, the Universal Control Plane (UCP) provides adequate keys in the user's Client Bundle.

Signing Images With Content Trust

First, add the delegation private key to the local DTR (you can find this stored in `~/.docker/trust`)

- When generating the delegation keys with `$ docker trust key generate`, they will automatically add the key to the local trust store.
- If you are importing one from a UCP Client Bundle, you use the command:
`$ docker trust key load`

Next, add the delegation public key to the Notary server

Finally, use the delegation private key to sign our tag and push it to the registry

Demo: Signing Images With Content Trust

To generate a key:

```
$ docker trust key generate moby
Generating key for moby...
Enter passphrase for new moby key with ID 9deed28:
Repeat passphrase for new moby key with ID 9deed28:
Successfully generated and loaded private key.
```

Managing Sensitive Information

Managing Secrets

Two rules when it comes to managing sensitive information:

1. Don't bake it into your image.
2. Don't use environment variables for your sensitive information.
 - Anyone who can run the command `docker inspect` or `exec` into your container can find your secret.
 - The same goes for any user running as `root`.

Docker Volumes

The recommended way to access your sensitive info in the Docker docs

- You can use a volume as a tmpfs held in memory
- Volumes remove the `docker inspect` and the logging risk

However, root users could still see the secret, as well as anyone who can `exec` into the container.

Docker Secrets- An Even Better Option

Encrypted

If you need your secret in your running container, and not just when building your image, use:

- Docker Compose
- Kubernetes

With Docker Compose, add the secrets key-value pair to a service and specify the secret file.

Demo: Docker Secrets

```
version: "3.8"

services:
  my_service:
    image: centos:7
    entrypoint: "cat /run/secrets/my_secret"
    secrets:
      - my_secret

secrets:
  my_secret:
    file: ./my_secret_file.txt
```


Next Steps - Try Docker Enterprise for Free

If you are new to Docker or you have setup a successful proof of concept and need some direction, Stone Door Group offers our Docker Accelerator. This comprehensive services offering enables you to transition a Docker pet project into a secure production Docker enterprise environment.

<http://www.stonedoorgroup.com/docker-ce-to-ee>

```
docker container run --rm -it sdgdockerlabs/coffee
```

Or reach us at: letsdothis@stonedoorgroup.com to have a chat about our experiences with migrations.

Q & A

Download slides: bit.ly/mirantis-stone-door-webinar3



Why Mirantis Training

- **Preparation for the real world**
 - Based on years of **production experience** at scale
 - Extensive **hands on labs** to put what you learn into practice
 - Industry standard certifications
- **Where and when you want it**
 - Choice of instructor led classroom or instructor led live online
 - Robust public class schedule from global partners

Mirantis Training: Docker Enterprise

Get 25% off public classes offered by Global Knowledge and ExitCertified,
promo codes will be emailed



Docker Fundamentals	Learn the best practices of running containers, creating images, and orchestrating applications in Swarm and Kubernetes	2 days
Docker for Enterprise Operations	Take an extended deep dive into all the features of the Docker Enterprise platform, covering all core operational responsibilities.	3 days
Docker for Enterprise Developers	Explore techniques in software development and continuous integration for container-native applications.	2 days
Docker Troubleshooting & Support	Learn how to troubleshoot and maintain the Docker Enterprise platform in a wide range of day-2 operations scenarios.	2 days

training.mirantis.com

Mirantis Training: Kubernetes



Get 25% off any public class offered by Mirantis,
promo code **SOCIAL25**



Kubernetes & Docker Bootcamp I (KD100)	Learn Docker and Kubernetes to deploy, run, and manage containerized applications	2 days
Kubernetes & Docker Bootcamp II (KD200)	Comprehensive Administration training, preps for the CKA exam	3 days
Accelerated Kubernetes & Docker Bootcamp (KD250)	Most popular course! A combination of KD100 & KD200 at an accelerated pace, preps for the CKA exam	4 days
Advanced Kubernetes Operations (CN320)	NEW! Advanced training focused on production grade architecture, operational best practices, and cluster management.	2 days

training.mirantis.com

STONE
DOOR
GROUP

Source Attribution

<https://docs.docker.com/engine/security/apparmor/>

<https://success.docker.com/article/how-to-set-selinux-file-contexts-when-using-a-custom-docker-data-root>

<https://docs.docker.com/storage/bind-mounts/#configure-the-selinux-label>

<https://docs.docker.com/ee/ucp/authorization/ee-advanced/>

<https://docs.docker.com/ee/dtr/>

<https://docs.docker.com/ee/dtr/user/access-dtr/>

https://docs.docker.com/engine/security/trust/content_trust/

Week #2 - Prize Winners

US Winners

Ranthy R.	TX	Jeff H.	TN
Gary Lon B.	OK	Alan H.	VA
Michael P.	OH	Glenn Z.	MD
Nagendran J.	CA	Ryan J.	MD
Paul S.	OH	Greg B.	VA
David A.	WY	Bernard N.	TX
Zai F.	NY	Jose B.	VA
Mohammed P.	IL	Joe C.	NJ
Prakash N.	CA	Quang L.	MD
Ed B.	NY	Ashok S.	NY

International Winners

Bruce C.	UK
Vokan G.	Turkey
Enrico P.	Canada
Mateusz P.	Italy
Subhranshu D.	Germany

Congratulations to our prize winners from our previous event!

Thank You for Joining Us Today

Docker Enterprise Social Distance Learning Series

Webinar	Title	Event Date/Time	Description
1	Get Docker Enterprise Edition Running in an Hour	April 16, 2020 9.00 - 10.00am PST	Quickly install or upgrade to Docker Enterprise Edition
2	Docker Tips for Better Productivity	April 23, 2020 9.00 - 10.00am PST	Gain an edge in Docker administration
3	Docker Tips for Better Security	May 7, 2020 9.00 - 10.00am PST	Leverage the features of Docker Enterprise Edition for corporate security and regulatory compliance
4	Kubernetes Tips for Better Productivity	May 14, 2020 9.00 - 10.00am PST	Gain an edge in Kubernetes implementation

Register here > <https://www.stonedoor.io/docker-webinar>

Questions? Email us at letsdothis@stonedoorgroup.com