



Security by design

**Comment construire un
produit SECURE BY DESIGN?**

Security by design

- Thème centraux de la sécurité de l'information



Confidentialité: Ne permettre que l'accès aux données pour lesquelles l'utilisateur est autorisé



Intégrité: S'assurer que les données ne sont pas falsifiées ou altérées par des utilisateurs non autorisés



Disponibilité: S'assurer que les systèmes et les données sont disponibles pour les utilisateurs autorisés quand ils en ont besoin

Security by design



Comment mettre en oeuvre ?

- ☐ Minimiser la surface d'attaque
- ☐ Établir des valeurs par défaut sécurisées
- ☐ Principe du moindre privilège
- ☐ Principe de défense en profondeur
- ☐ Échouer en toute sécurité
- ☐ Ne faites pas confiance aux services
- ☐ Séparation des tâches
- ☐ Évitez la sécurité par l'obscurité
- ☐ Gardez la sécurité simple
- ☐ Résoudre les problèmes de sécurité correctement

Security by design

Et concrètement, lorsque l'application est en production:

- ☐ Utilisez un gestionnaire de mot de passe comme Vault. Il sera utile d'avoir des mots de passe de bonne qualité.
- ☐ Mettez à jour votre système d'exploitation et tous les logiciels utilisés.
- ☐ Implémentez des sauvegardes et testez-les.
- ☐ Testez votre DRP périodiquement.
- ☐ Séparez les différents comptes pour chaque utilisation.
- ☐ Utilisez un bastion pour accéder au compte administrateur.
- ☐ Faites attention aux différents composants que vous trouvez sur internet.

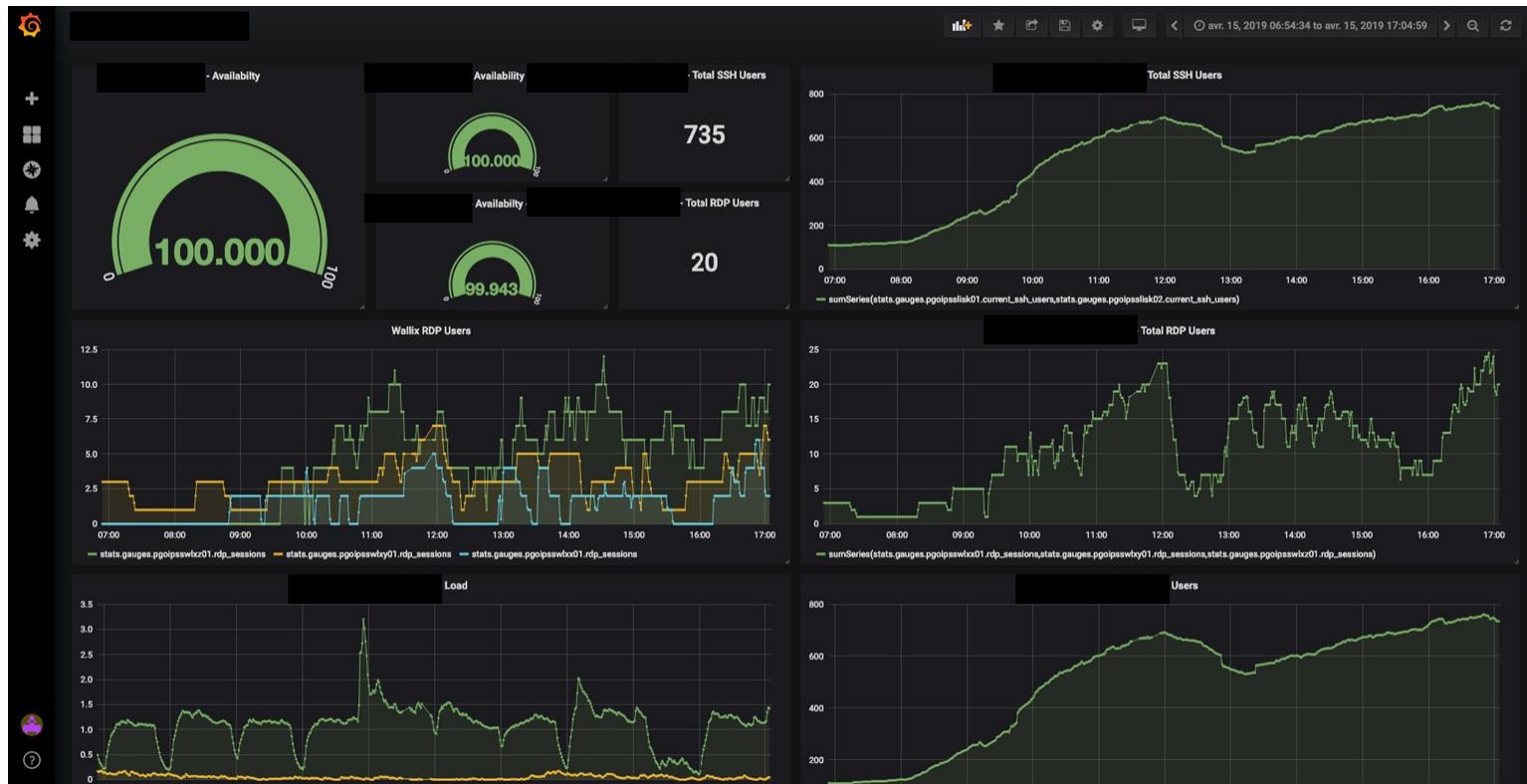


**Une démonstration avec une
solution de monitoring ?**

Security by design - Cas d'usage

- **Notre client avait besoin d'une solution rapide et sécurisée pour surveiller les produits de sécurité.**
- **Capable de superviser des solutions propriétaires implémentées chez le client**
- **Flexible sur les méthodes d'authentification (Contrôles authentifiés RDP et SSH...)**
- **Infrastructure as code pour faciliter la maintenance**
- **Qui fonctionne avec l'infrastructure existante du client**

Un aperçu de l'application

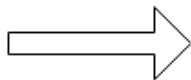


Un aperçu de l'application

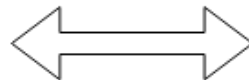


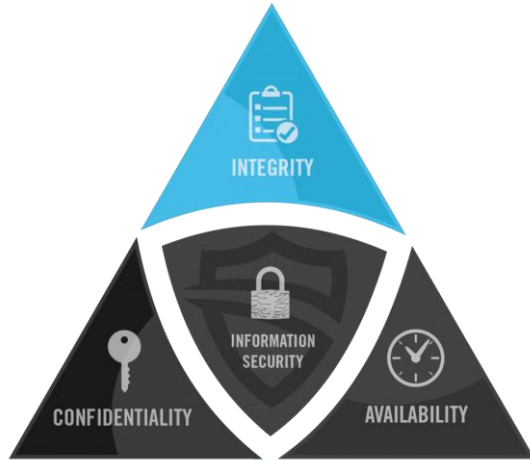
L'architecture

Comment cela fonctionne ?



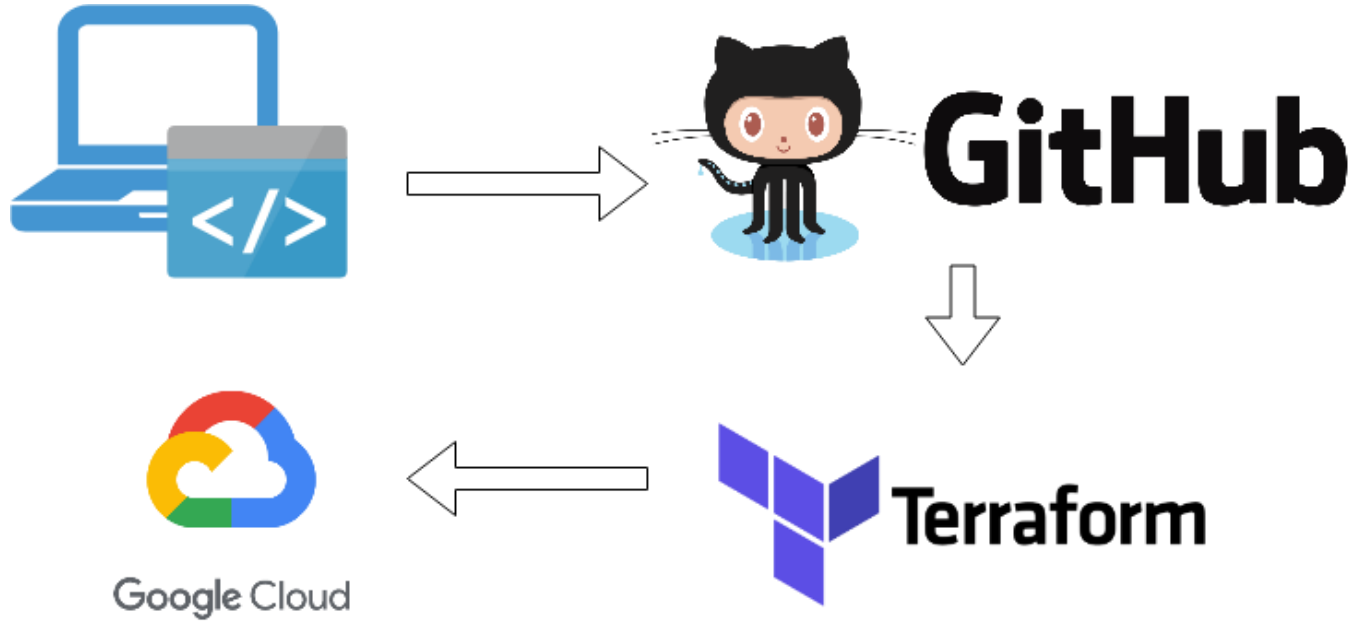
Google Cloud
Public IAAS





Un peu d'infrastructure as code

Security by design - Intégrité



Security by design - Intégrité

The screenshot shows the GitHub interface for a repository named 'opsec-monitoring'. The repository is private and has 2 watchers, 0 stars, and 0 forks. The main content area displays the repository's description, 'Dedicated monitoring for security team.', and a list of files and folders. The files include 'conf', 'scripts', 'stats', 'terraform', '.gitignore', and 'README.md'. The 'README.md' file is currently selected and its content is visible at the bottom of the page.

GitHub, Inc. (US) | https://github.com/

Search or jump to... Pull requests Issues Marketplace Explore

/ opsec-monitoring Private

Watch 2 Star 0 Fork 0

Code Issues 0 Pull requests 0 Actions Projects 0 Wiki Insights Settings

Dedicated monitoring for security team. Edit

Manage topics

11 commits 2 branches 0 releases 1 contributor

Branch: master New pull request Create new file Upload files Find File Clone or download

Fix debian frontend errors Latest commit 60662fb 4 days ago

conf	Fix debian frontend errors	4 days ago
scripts	Fix debian frontend errors	4 days ago
stats	Use Vault for ssh.py in Stats container	4 days ago
terraform	Add "stats" container for ssh supervision.	8 days ago
.gitignore	Fix stats container class error	8 days ago
README.md	Initial commit	15 days ago

README.md

Security by design - Intégrité

Google Cloud Platform

opsec-lis-dtp

Compute Engine

VM instances

Instance groups

Instance templates

Sole tenant nodes

Disks

Snapshots

Images

TPUs

Committed use discounts

Marketplace

<|

VM instances

CREATE INSTANCE

SHOW INFO PANEL

LEARN

Instance "monitoring" is overutilized. Consider switching to the machine type: g1-small (1 vCPU, 1.7 GB memory). [Learn more](#)

Dismiss

Filter VM instances

Columns

<input type="checkbox"/> Name ^	Zone	Recommendation	In use by	Internal IP	External IP	Connect
<input type="checkbox"/> dns-forwarder-europe-west3-2x1x	europe-west3-a		dns-instance-group-europe-west3	10.205.138.195 (nic0)	None	SSH ▾ ⋮
<input type="checkbox"/> dns-forwarder-europe-west4-12mn	europe-west4-c		dns-instance-group-europe-west4	10.205.10.196 (nic0)	None	SSH ▾ ⋮
<input type="checkbox"/> monitoring	europe-west4-a	Increase perf.		10.205.10.198 (nic0)	None	SSH ▾ ⋮
<input type="checkbox"/> terraform-env	europe-west4-b			10.205.10.194 (nic0)	None	SSH ▾ ⋮



Un peu de Docker

Security by design - Disponibilité



- Base de données Time-series
- Conteneur de contrôle actif SSH
- Https proxy pour Graphite DB



Nous utilisons WatchTower

```
watchtower:  
  image: containrrr/watchtower  
  volumes:  
  - /var/run/docker.sock:/var/run/docker.sock  
  command: --interval 30 --cleanup
```

WatchTower vérifie régulièrement s'il existe une nouvelle image de chaque conteneur.

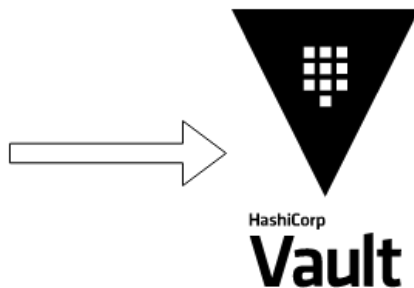
Si une nouvelle image est trouvée, le conteneur est mis à jour.

Ainsi, une vulnérabilité de sécurité est corrigée 30 secondes après la publication du correctif.



Un peu de Vault

Security by design - Confidentialité



- Récupérer le certificat SSL, les clés SSH et l'URL de l'API dans le coffre fort
- Authentification à l'aide du jeton JWT à partir des métadonnées internes de Google

Security by design - Confidentialité

The screenshot displays the Vault Web UI interface. The top navigation bar includes a dropdown menu for 'opsec-lis' and tabs for 'Secrets', 'Access', 'Policies', and 'Tools'. The main content area is titled 'Secrets Engines' and lists three engines: 'cubbyhole/' (ns_cubbyhole_04c90e55), 'secret/' (v2 kv_6e959b32), and 'transit/' (transit_c1421170). A sidebar on the right contains a 'Vault Web UI' section with a 'Choosing where to go' message and a 'Walk me through setting up:' section with checkboxes for 'Secrets' and 'Authentication'. The footer shows the HashiCorp logo, copyright information for 2019, and the version 'Vault 1.1.0+pro'.

opsec-lis · Secrets Access Policies Tools

Secrets Engines [Enable new engine >](#)

cubbyhole/ ns_cubbyhole_04c90e55	...
secret/ v2 kv_6e959b32	...
transit/ transit_c1421170	...

Vault Web UI ...

Choosing where to go

You did it! You now have access to your Vault and can start entering your data. We can help you get started with any of the options below.

- Vault only shows links to pages that you have access to based on your policies. Contact your administrator if you need access changes.

Walk me through setting up:

- ☐ Secrets
- ☐ Authentication

© 2019 HashiCorp, Inc. Vault 1.1.0+pro [Documentation](#)

Security by design - Confidentialité

The screenshot shows the Consul web interface in a browser. The address bar displays "https://". The main content area is titled "Path" and contains a text input field with the value "monitoring". Below this field are two buttons: "+ Path" and "x Last Path". Further down, there are two checkboxes: "Enable Consul ACL" (unchecked) and "Enable GCP authentication" (checked). Below the checkboxes, there is a section for the "gcp" backend, which includes three tabs: "gcp", "JSON", and "Properties". The "gcp" tab is active, showing two text input fields: "Backend name" with the value "gcp" and "GCP project ID" with the value "opsec-lis-dtp".

Path

monitoring

+ Path x Last Path

☐ Enable Consul ACL

☒ Enable GCP authentication

gcp JSON Properties

Backend name ?

gcp

GCP project ID ?

opsec-lis-dtp

Security by design - Confidentialité

The screenshot shows the Vault Web UI interface. The top navigation bar includes a dropdown menu for 'opsec-lis', tabs for 'Secrets', 'Access', 'Policies', and 'Tools', and user profile icons. The main content area is titled 'monitoring' and features a 'Delete secret' link. Below the title is a table with columns 'KEY' and 'VALUE'. The table lists several secrets, each with a 'JSON' toggle, a 'Copy Secret' link, a 'Create new version' link, and a 'Version 7' link. The 'VALUE' column displays redacted content (dots). A sidebar on the right contains a 'Vault Web UI' section with a 'Choosing where to go' message and two options: 'Secrets' and 'Authentication', both with checkboxes and dropdown arrows.

KEY	VALUE
certificate_p12	[Redacted]
certificate_password	[Redacted]
graphite_host	[Redacted]
graphite_port	[Redacted]
ssh_bastion_hosts	[Redacted]
ssh_private_key	[Redacted]
ssh_private_key_ascii	[Redacted]
ssh_user	[Redacted]

Vault Web UI

Choosing where to go

You did it! You now have access to your Vault and can start entering your data. We can help you get started with any of the options below.

- Vault only shows links to pages that you have access to based on your policies. Contact your administrator if you need access changes.

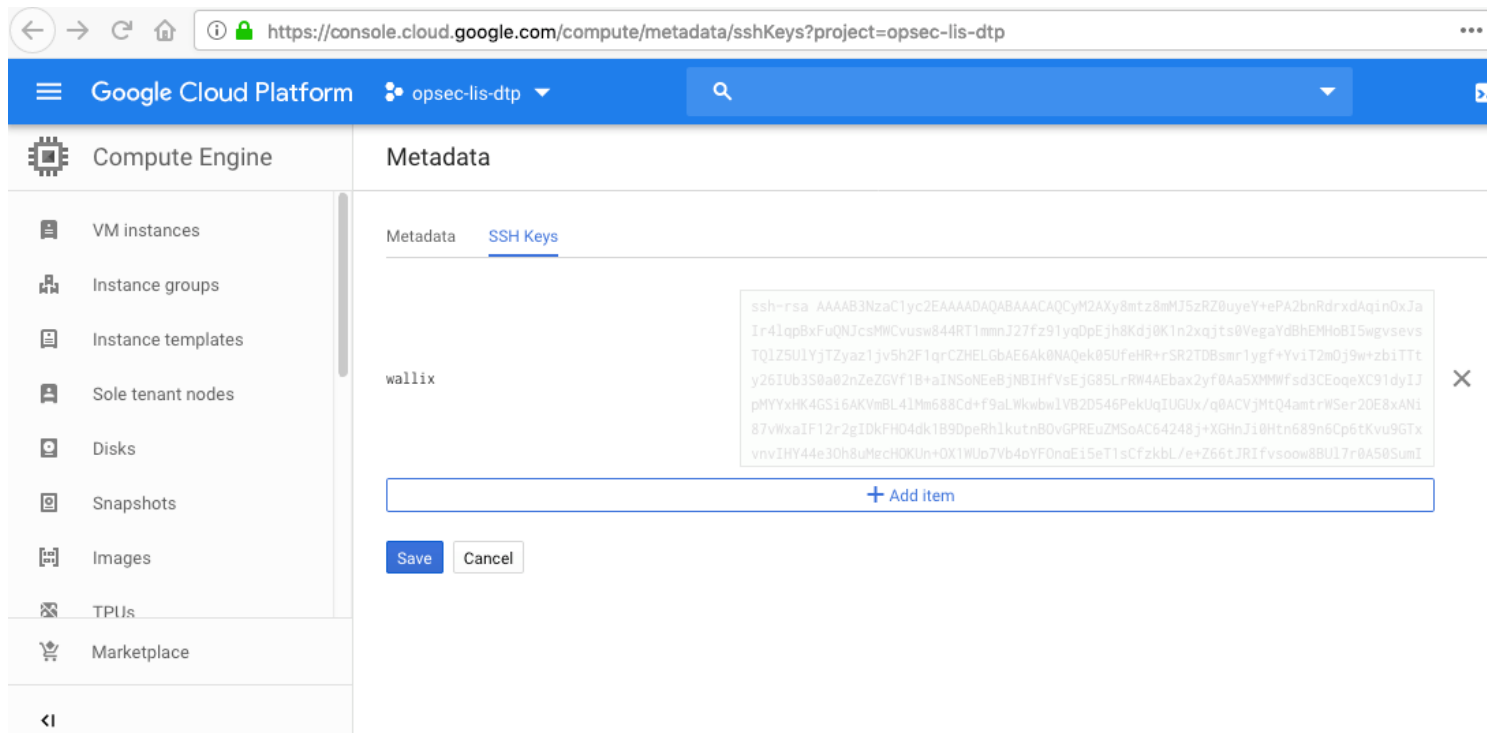
Walk me through setting up:

- ☐ Secrets
- ☐ Authentication



Un peu de bastion

Security by design



The screenshot shows the Google Cloud Platform console interface. The top navigation bar includes the Google Cloud Platform logo, the project name 'opsec-lis-dtp', and a search bar. The left sidebar contains a list of navigation items: Compute Engine, VM instances, Instance groups, Instance templates, Sole tenant nodes, Disks, Snapshots, Images, TPU's, and Marketplace. The main content area is titled 'Metadata' and shows the 'SSH Keys' tab for the 'wallix' instance. A text box contains a long SSH key string. Below the text box is a '+ Add item' button. At the bottom of the page are 'Save' and 'Cancel' buttons.

Google Cloud Platform opsec-lis-dtp

Compute Engine

VM instances

Instance groups

Instance templates

Sole tenant nodes

Disks

Snapshots

Images

TPU's

Marketplace

Metadata

SSH Keys

wallix

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACyM2AXy8mtz8mMJ5zRZ0uyeY+ePA2bnRdrxdAqinOxJa
Ir4lqp8xFuQNJcsMwCvusw844RT1mmnJ27fz91yqDpEjh8Kdj0K1n2xqjts0VegaYd8hEMHoB15wgvs
TQ1Z5U1YjTZyaz1jv5h2F1qrCZHELGbAE6Ak0NAQek05UfeHR+rSR2TDBsmrlygf+YviT2m0j9w+zb1TTt
y26IUb3S0a02nZeZGVf1B+aINSoNEeBjNBjHfVsEjG85LrRW4AEbax2yf0Aa5XMMWfsd3CEoqXC91dyIJ
pMYyxHk4GSi6AKVmBL41Mm688Cd+f9aLWkwblVB2D546PekUqIUGUx/q0ACVjMtQ4amtrW5er20E8xANi
87vWxaIF12r2gIDkFH04dk1B90peRh1kutnB0vGPReuZM5oAC64248j+XGhnJi0Htn689n6Cp6tKvu9GTx
vnnvIHY44e30h8uMechOKUn+OX1WJo7Vb4eYF0naEi5eT1sCfzkbL/e+Z66tJRIfvsoow8BU17r0A50SumI
```

+ Add item

Save Cancel

Security by design

← → ↻ 🏠 ⓘ <https://> ... 🛡️ ☆ ⬇️ 🔄 📦 ☁️ ☰

🔍 Authorizations 👤 Sign Out

➡ Sessions

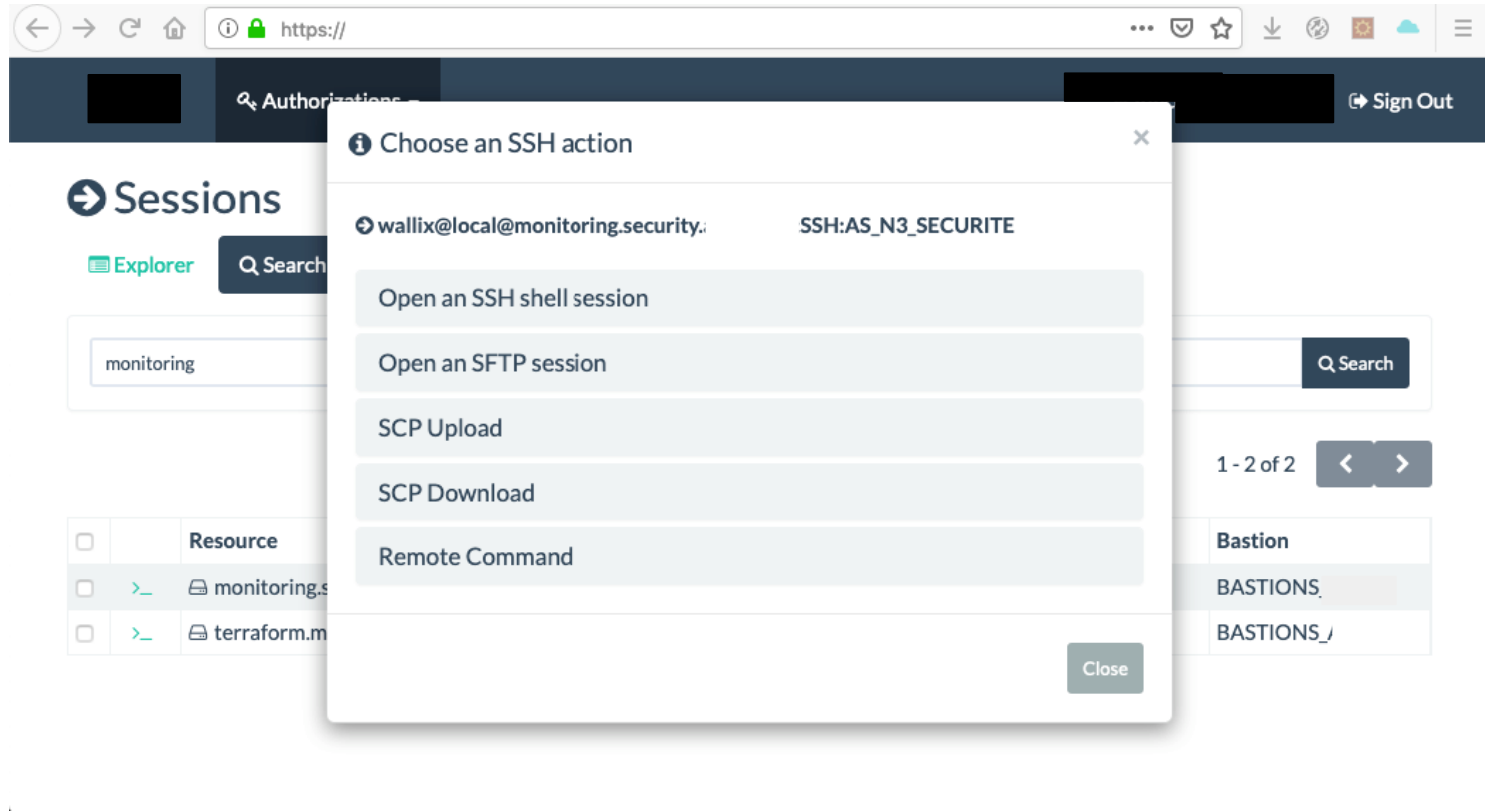
📖 Explorer 🔍 Search

monitoring 🔍 Search

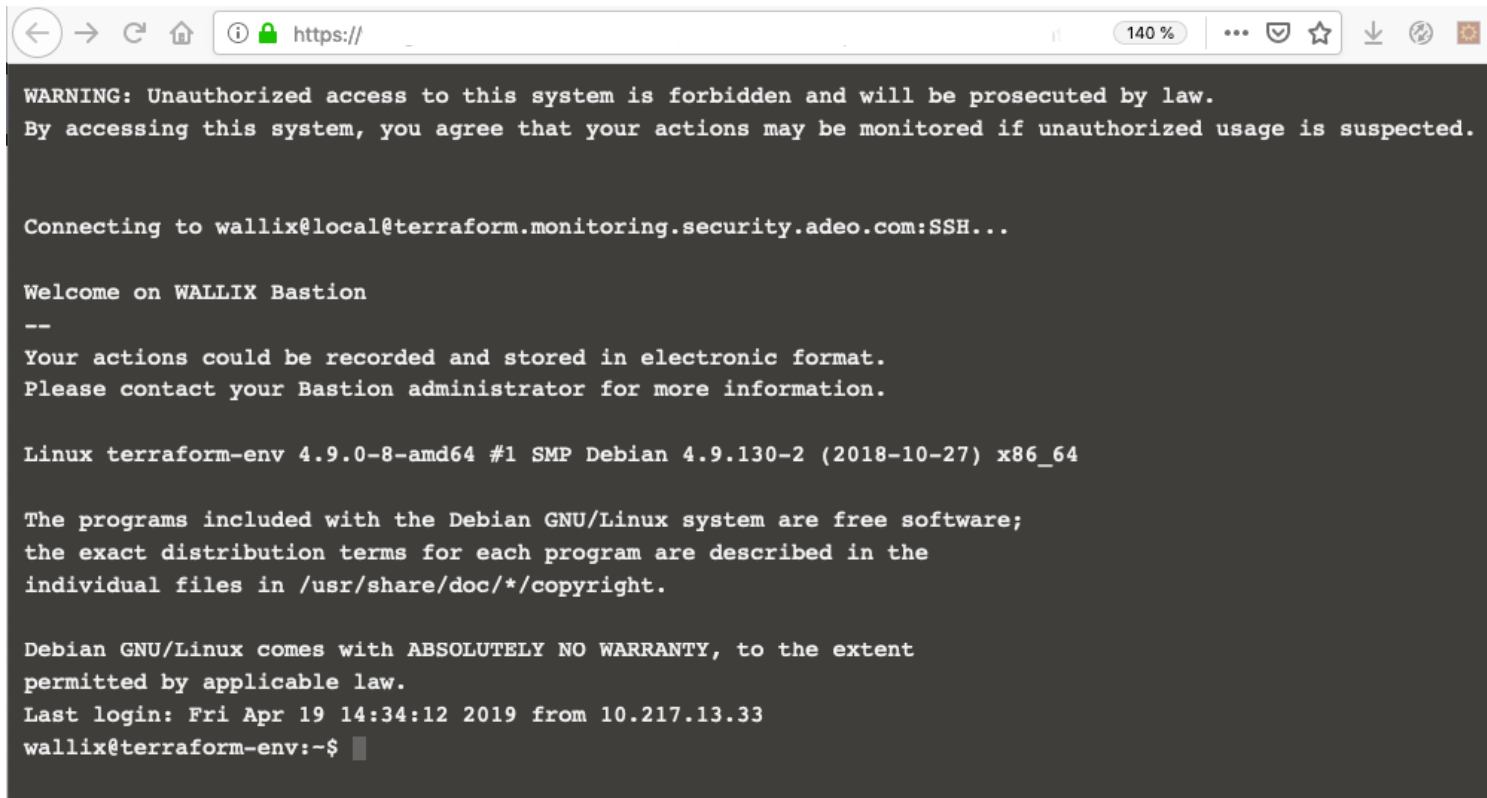
1 - 2 of 2 < >

<input type="checkbox"/>		Resource	Domain	Account	Service	Name/Groups	Bastion
<input type="checkbox"/>	>_	🔒 monitoring.securite	local	wallix	SSH	AS_N3_SECURITE	
<input type="checkbox"/>	>_	🔒 terraform.monitori	local	wallix	SSH	AS_N3_SECURITE	

Security by design



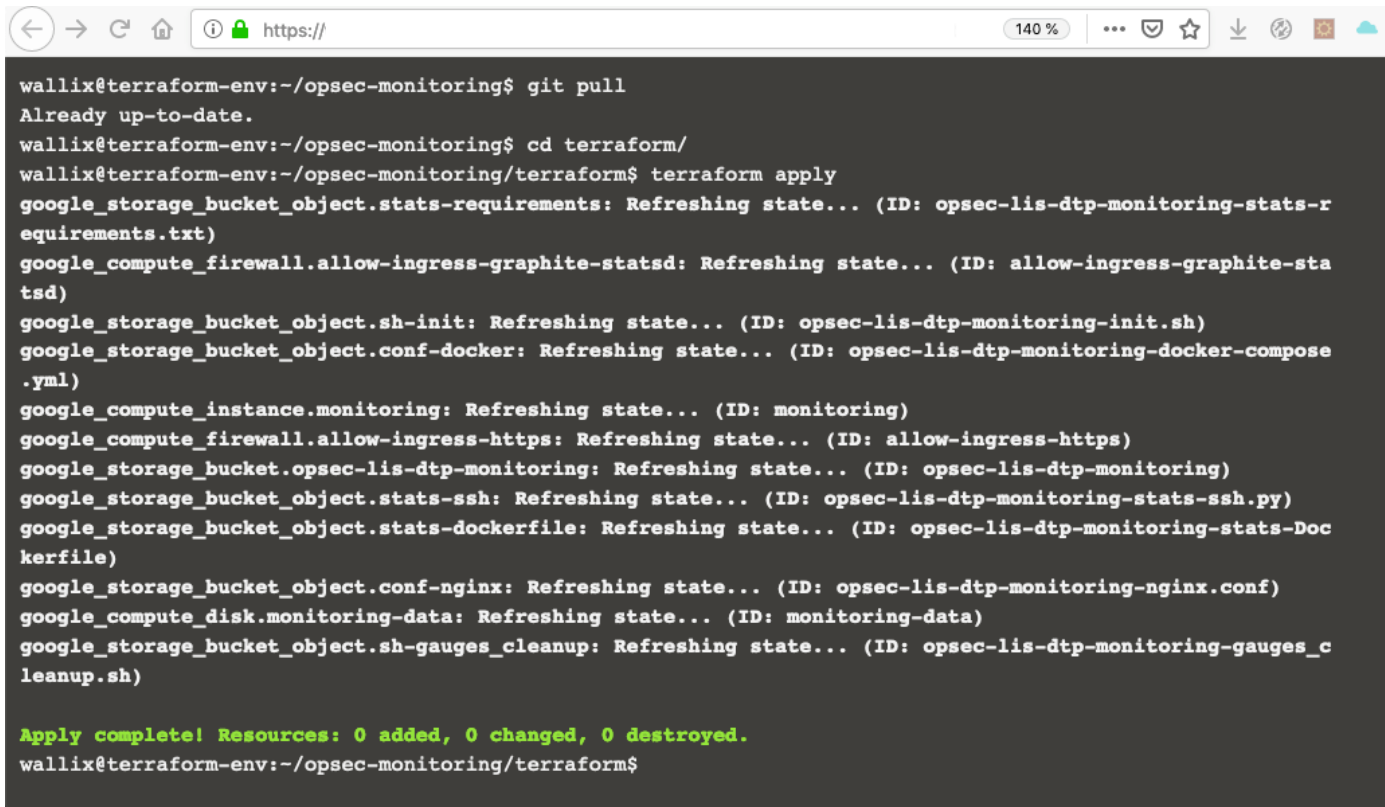
Security by design



A screenshot of a web browser window. The address bar shows a URL starting with 'https://'. The page content is a terminal window with a dark background and light-colored text. The text includes a warning about unauthorized access, a connection message to 'wallix@local@terraform.monitoring.security.adeo.com:SSH...', a welcome message for 'WALLIX Bastion', and system information for a Debian GNU/Linux system. The terminal prompt is 'wallix@terraform-env:~\$'.

```
WARNING: Unauthorized access to this system is forbidden and will be prosecuted by law.  
By accessing this system, you agree that your actions may be monitored if unauthorized usage is suspected.  
  
Connecting to wallix@local@terraform.monitoring.security.adeo.com:SSH...  
  
Welcome on WALLIX Bastion  
--  
Your actions could be recorded and stored in electronic format.  
Please contact your Bastion administrator for more information.  
  
Linux terraform-env 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Fri Apr 19 14:34:12 2019 from 10.217.13.33  
wallix@terraform-env:~$
```

Security by design



The image shows a terminal window with a dark background and light-colored text. The terminal output shows a series of Terraform commands being executed in a directory named /opsec-monitoring. The commands are: git pull, cd terraform/, and terraform apply. The output of terraform apply shows the state of various resources being refreshed, including google_storage_bucket_object, google_compute_firewall, google_compute_instance, and google_compute_disk. The final output indicates that the apply was successful, with 0 resources added, 0 changed, and 0 destroyed.

```
wallix@terraform-env:~/opsec-monitoring$ git pull
Already up-to-date.
wallix@terraform-env:~/opsec-monitoring$ cd terraform/
wallix@terraform-env:~/opsec-monitoring/terraform$ terraform apply
google_storage_bucket_object.stats-requirements: Refreshing state... (ID: opsec-lis-dtp-monitoring-stats-r
equirements.txt)
google_compute_firewall.allow-ingress-graphite-statsd: Refreshing state... (ID: allow-ingress-graphite-sta
tsd)
google_storage_bucket_object.sh-init: Refreshing state... (ID: opsec-lis-dtp-monitoring-init.sh)
google_storage_bucket_object.conf-docker: Refreshing state... (ID: opsec-lis-dtp-monitoring-docker-compose
.yml)
google_compute_instance.monitoring: Refreshing state... (ID: monitoring)
google_compute_firewall.allow-ingress-https: Refreshing state... (ID: allow-ingress-https)
google_storage_bucket.opsec-lis-dtp-monitoring: Refreshing state... (ID: opsec-lis-dtp-monitoring)
google_storage_bucket_object.stats-ssh: Refreshing state... (ID: opsec-lis-dtp-monitoring-stats-ssh.py)
google_storage_bucket_object.stats-dockerfile: Refreshing state... (ID: opsec-lis-dtp-monitoring-stats-Doc
kerfile)
google_storage_bucket_object.conf-nginx: Refreshing state... (ID: opsec-lis-dtp-monitoring-nginx.conf)
google_compute_disk.monitoring-data: Refreshing state... (ID: monitoring-data)
google_storage_bucket_object.sh-gauges_cleanup: Refreshing state... (ID: opsec-lis-dtp-monitoring-gauges_c
leanup.sh)

Apply complete! Resources: 0 added, 0 changed, 0 destroyed.
wallix@terraform-env:~/opsec-monitoring/terraform$
```

Security by design

- Nous utilisons un bastion et le fichier sudoers

```
wallix@monitoring:~$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
wallix@monitoring:~$ sudo cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
```

- Toutes les actions sont tracées dans le fichier `/var/log/auth.log`

```
Apr 23 15:27:16 monitoring sudo: pam_unix(sudo:session): session closed for user root
Apr 23 15:31:56 monitoring sudo: wallix : TTY=pts/0 ; PWD=/home/wallix ; USER=root ; COMMAND=/bin/cat /etc/sudoers
Apr 23 15:31:56 monitoring sudo: pam_unix(sudo:session): session opened for user root by wallix(uid=0)
```

Security by design

WALLIX Bastion 2.2

Audit Historique des sessions

Mes préférences

Mes autorisations

Audit

Sessions courantes

Historique des sessions

Historique des comptes

Historique des approbations

Historique des authentifications

Statistiques sur les connexions

Utilisateurs

Ressources

Gestion des mots de passe

Gestion des sessions

Autorisations

Configuration

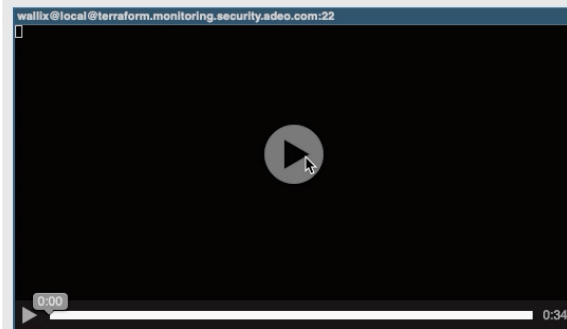
Système

Import/Export

Informations de la session

Identifiant : 20009060a@corp. @10.12.12.130
Cible : wallix@local@terraform.monitoring.security.i 22
Hôte/IP cible : 10.205.10.194
Protocole SRC/DST : SSH/SSH_SHELL_SESSION
Heure de début : 2019-04-25 11:32:58
Heure de fin : 2019-04-25 11:33:33
Durée : 0:00:35
Résultat : Success
Description : --

Visualiseur SSH

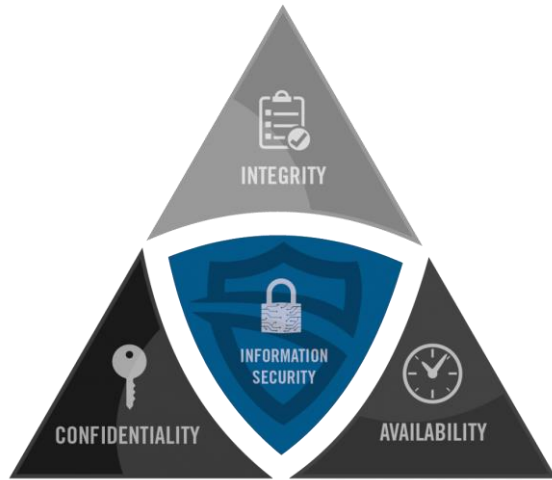


Transcription

```
google_storage_bucket.opsec-lis-dtp-monitoring-state... (ID: opsec-lis-dtp-monitoring-state-requirements.txt)
google_compute_firewall.allow-ingress-graphite-stats: Refreshing state... (ID: allow-ingress-graphite-stats)
google_compute_firewall.allow-ingress-https: Refreshing state... (ID: allow-ingress-https)
google_compute_instance.monitoring: Refreshing state... (ID: monitoring)
google_storage_bucket.opsec-lis-dtp-monitoring: Refreshing state... (ID: opsec-lis-dtp-monitoring)
google_storage_bucket_object.state-requirements: Refreshing state... (ID: opsec-lis-dtp-monitoring-state-requirements.txt)
google_storage_bucket_object.state-ssh: Refreshing state... (ID: opsec-lis-dtp-monitoring-state-ssh.py)
```

An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
- update in-place

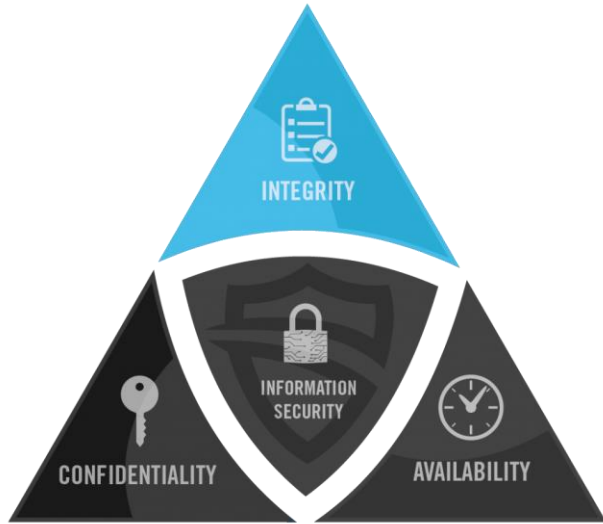
Visualization of logs
on Wallix



Un peu de patch management

Le redéploiement de l'instance pour mettre à jour tous les composants en une ligne de commande!

```
terraform destroy -target google_compute_instance.monitoring -auto-approve \  
&& terraform apply -auto-approve
```

Et les logs?

Nous utilisons  Stackdriver

```
curl -sSO https://dl.google.com/cloudagents/install-logging-agent.sh  
sudo bash install-logging-agent.sh
```

Security by design - Intégrité

← → ↺ 🏠 ⓘ <https://console.cloud.google.com/logs/viewer?project=opsec-lis-dtp&minLogLevel=0&expandAll=false×tamp=2019-04-23T09:19:56> ... 🛡️ ⭐ 🌐 📄 🌱 ☁️ ☰

☰ Google Cloud Platform opsec-lis-dtp 🔍

Stackdriver Logging

☰ Logs

📊 Logs-based metrics

📄 Exports

📄 Logs ingestion

📊 CREATE METRIC 📄 CREATE EXPORT ↺ ▶

Filter by label or text search

GCE VM Instance auth Any log level ⌚ Last 7 days 📅 Jump to now

Showing logs from the last 7 days ending at 11:19 AM (CEST) Download logs View Options

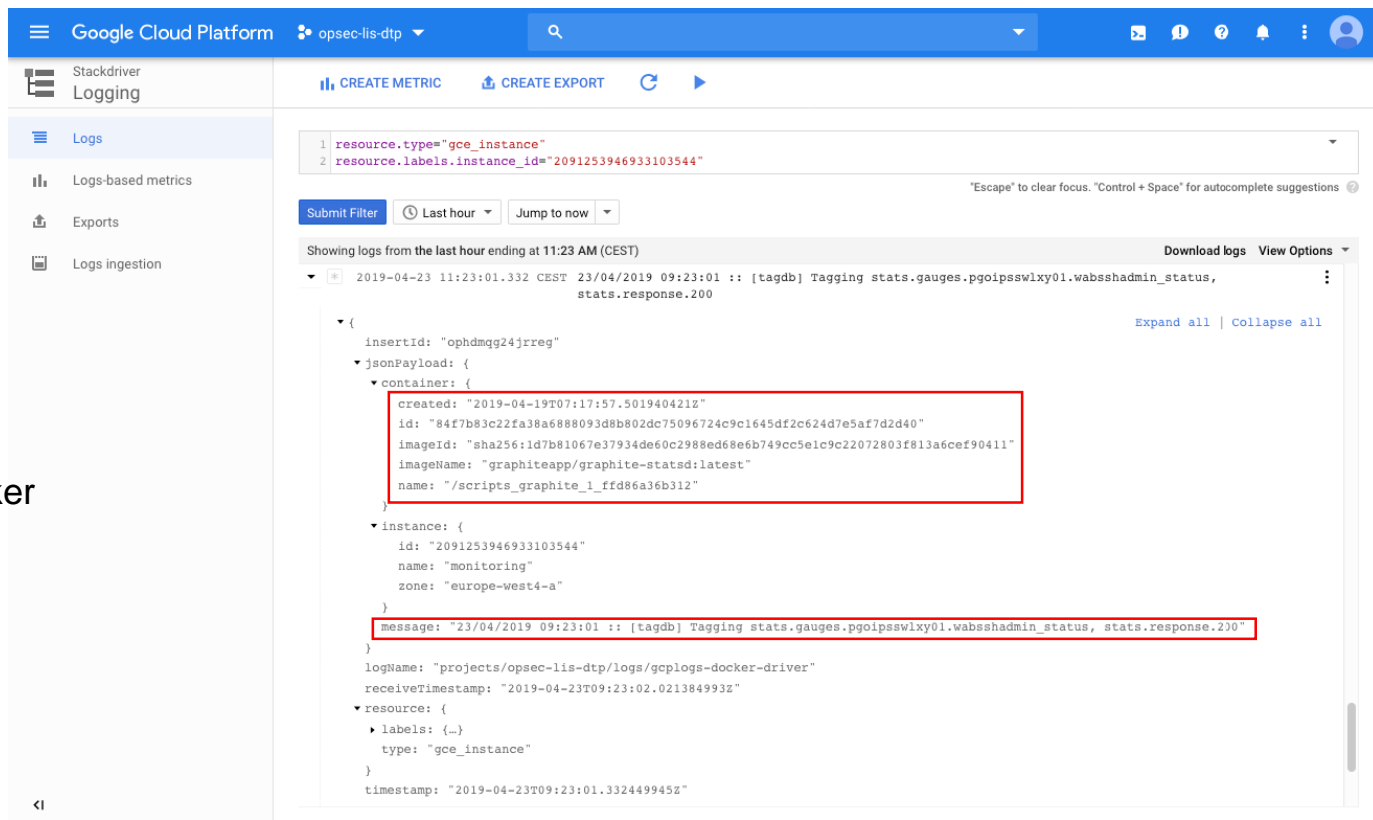
▶	2019-04-19 16:17:01.000 CEST	Apr 19 14:17:01 monitoring cron[390]: pam_unix(cron:session): session closed for user root	⋮
▶	2019-04-19 16:33:19.000 CEST	Apr 19 14:33:19 monitoring sshd[3743]: Accepted publickey for wallix from 10.212.13.35 port 59960...	⋮
▶	2019-04-19 16:33:19.000 CEST	Apr 19 14:33:19 monitoring sshd[3743]: pam_unix(sshd:session): session opened for user wallix by ...	⋮
▶	2019-04-19 16:38:25.000 CEST	Apr 19 14:38:25 monitoring sshd[3752]: Received disconnect from 10.212.13.35 port 59960:11: Disco...	⋮
▶	2019-04-19 16:38:25.000 CEST	Apr 19 14:38:25 monitoring sshd[3752]: Disconnected from 10.212.13.35 port 59960	⋮
▶	2019-04-19 16:38:25.000 CEST	Apr 19 14:38:25 monitoring sshd[3743]: pam_unix(sshd:session): session closed for user wallix	⋮
▶	2019-04-19 16:38:43.000 CEST	Apr 19 14:38:43 monitoring sshd[4882]: Accepted publickey for wallix from 10.212.13.35 port 60184...	⋮
▶	2019-04-19 16:38:43.000 CEST	Apr 19 14:38:43 monitoring sshd[4882]: pam_unix(sshd:session): session opened for user wallix by ...	⋮
▶	2019-04-19 16:39:47.000 CEST	Apr 19 14:39:47 monitoring sshd[4891]: Received disconnect from 10.212.13.35 port 60184:11: Disco...	⋮
▶	2019-04-19 16:39:47.000 CEST	Apr 19 14:39:47 monitoring sshd[4891]: Disconnected from 10.212.13.35 port 60184	⋮
▶	2019-04-19 16:39:47.000 CEST	Apr 19 14:39:47 monitoring sshd[4882]: pam_unix(sshd:session): session closed for user wallix	⋮
▶	2019-04-19 16:39:58.000 CEST	Apr 19 14:39:58 monitoring sshd[5154]: Accepted publickey for wallix from 10.217.13.33 port 43752...	⋮
▶	2019-04-19 16:39:58.000 CEST	Apr 19 14:39:58 monitoring sshd[5154]: pam_unix(sshd:session): session opened for user wallix by ...	⋮
▶	2019-04-19 16:41:43.000 CEST	Apr 19 14:41:43 monitoring sshd[5163]: Received disconnect from 10.217.13.33 port 43752:11: Disco...	⋮

<1

Logs d'authentification

Security by design - Intégrité

Logs Docker



The screenshot displays the Google Cloud Platform Logging interface. The left sidebar shows the navigation menu with 'Stackdriver Logging' selected. The main panel shows a log entry for a Docker container. The log entry is expanded, revealing a JSON payload. A red box highlights the 'container' section, which contains details about a Docker container named 'stats.gauges.pgoipsswly01.wabsshadmin_status'. Another red box highlights the 'message' field, which contains the log message: '23/04/2019 09:23:01 :: [tagdb] Tagging stats.gauges.pgoipsswly01.wabsshadmin_status, stats.response.200'.

Google Cloud Platform opsec-lis-dtp

Stackdriver Logging

CREATE METRIC CREATE EXPORT

1 resource.type="gce_instance"
2 resource.labels.instance_id="2091253946933103544"

Submit Filter Last hour Jump to now

Showing logs from the last hour ending at 11:23 AM (CEST) Download logs View Options

2019-04-23 11:23:01.332 CEST 23/04/2019 09:23:01 :: [tagdb] Tagging stats.gauges.pgoipsswly01.wabsshadmin_status, stats.response.200

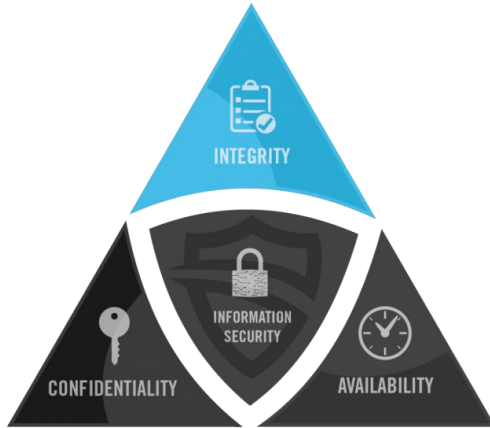
Expand all | Collapse all

```
{
  insertId: "ophdmqg24jrreg"
  jsonPayload: {
    container: {
      created: "2019-04-19T07:17:57.501940421Z"
      id: "84f7b83c22fa38a6888093d8b802dc75096724c9c1645df2c624d7e5af7d2d40"
      imageId: "sha256:1d7b81067e37934de60c2988ed68e6b749cc5e1c9c22072803f813a6cef90411"
      imageName: "graphiteapp/graphite-statsd:latest"
      name: "/scripts_graphite_i_ffd86a36b312"
    }
    instance: {
      id: "2091253946933103544"
      name: "monitoring"
      zone: "europe-west4-a"
    }
    message: "23/04/2019 09:23:01 :: [tagdb] Tagging stats.gauges.pgoipsswly01.wabsshadmin_status, stats.response.200"
  }
  logName: "projects/opsec-lis-dtp/logs/gcplogs-docker-driver"
  receiveTimestamp: "2019-04-23T09:23:02.021384993Z"
  resource: {
    labels: {...}
    type: "gce_instance"
  }
  timestamp: "2019-04-23T09:23:01.332449945Z"
```

Google Cloud Platform console showing logs for the project `opsec-lis-dtp`. The logs are filtered by label `auth` and show the last hour of activity.

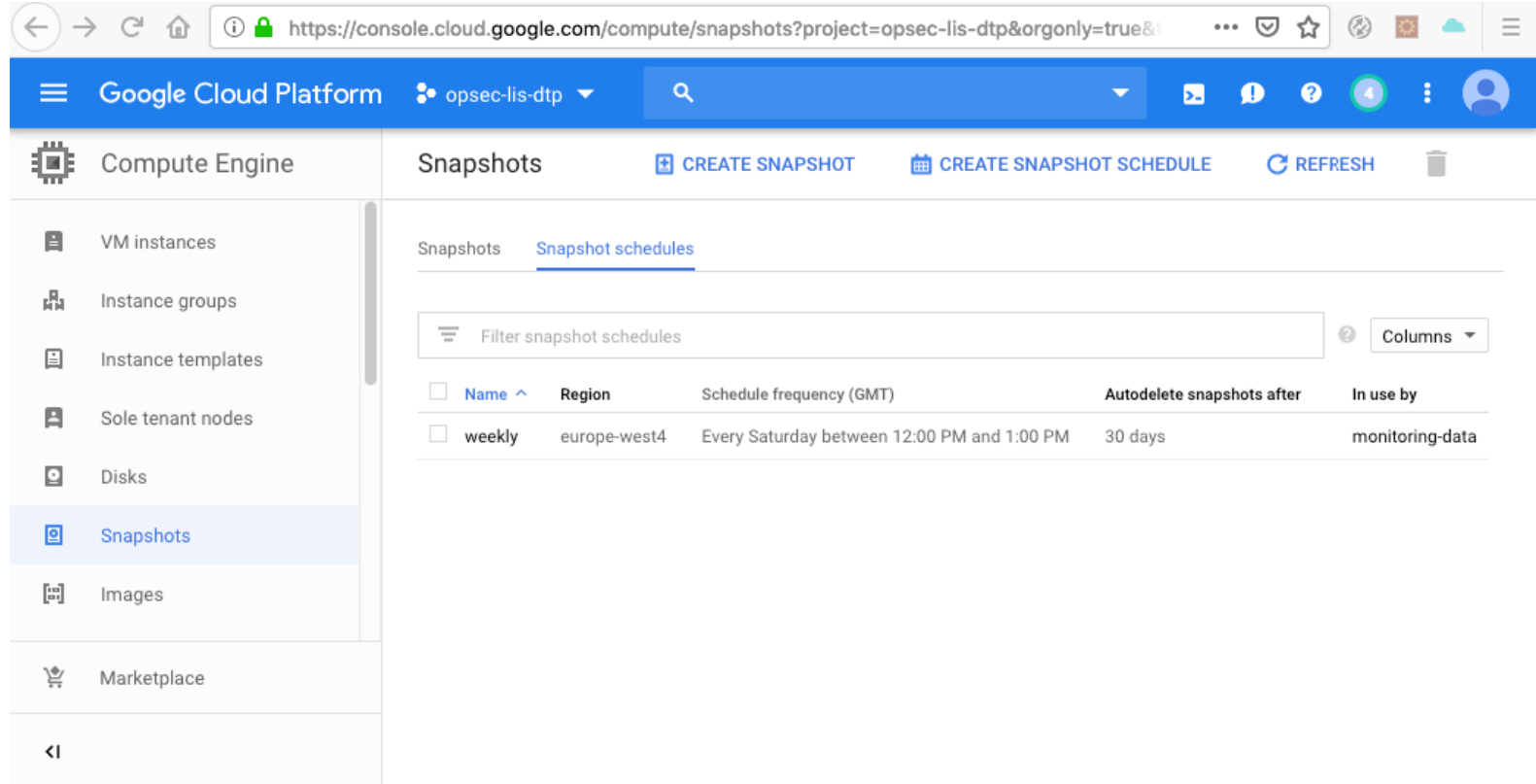
Showing logs from the last hour ending at 5:36 PM (CEST)

Timestamp	Log Message
2019-04-23 17:27:16.000 CEST Apr 23 15:27:16	monitoring sudo: wallix : TTY=pts/0 ; PWD=/home/wallix ; USER=root ; COMMAND=/bin/cat /etc/sudoers
2019-04-23 17:27:16.000 CEST Apr 23 15:27:16	monitoring sudo: pam_unix(sudo:session): session opened for user root by wallix(uid=0)
2019-04-23 17:27:16.000 CEST Apr 23 15:27:16	monitoring sudo: pam_unix(sudo:session): session closed for user root
2019-04-23 17:31:56.000 CEST Apr 23 15:31:56	monitoring sudo: wallix : TTY=pts/0 ; PWD=/home/wallix ; USER=root ; COMMAND=/bin/cat /etc/sudoers
2019-04-23 17:31:56.000 CEST Apr 23 15:31:56	monitoring sudo: pam_unix(sudo:session): session opened for user root by wallix(uid=0)
2019-04-23 17:31:56.000 CEST Apr 23 15:31:56	monitoring sudo: pam_unix(sudo:session): session closed for user root
2019-04-23 17:33:11.000 CEST Apr 23 15:33:11	monitoring sudo: wallix : TTY=pts/0 ; PWD=/home/wallix ; USER=root ; COMMAND=/bin/cat /var/log/auth.log
2019-04-23 17:33:11.000 CEST Apr 23 15:33:11	monitoring sudo: pam_unix(sudo:session): session opened for user root by wallix(uid=0)
2019-04-23 17:33:11.000 CEST Apr 23 15:33:11	monitoring sudo: pam_unix(sudo:session): session closed for user root
2019-04-23 17:33:23.000 CEST Apr 23 15:33:23	monitoring sudo: wallix : TTY=pts/0 ; PWD=/home/wallix ; USER=root ; COMMAND=/bin/cat /var/log/auth.log



Un peu de sauvegarde

Security by design - Intégrité



The screenshot shows the Google Cloud Platform console interface. The left sidebar contains a navigation menu with the following items: Compute Engine, VM instances, Instance groups, Instance templates, Sole tenant nodes, Disks, Snapshots (highlighted), Images, and Marketplace. The main content area is titled 'Snapshots' and includes buttons for 'CREATE SNAPSHOT', 'CREATE SNAPSHOT SCHEDULE', and 'REFRESH'. Below the title bar, there are tabs for 'Snapshots' and 'Snapshot schedules', with the latter being the active tab. A search bar and a 'Columns' dropdown are present above a table. The table lists snapshot schedules with the following data:

<input type="checkbox"/> Name ^	Region	Schedule frequency (GMT)	Autodelete snapshots after	In use by
<input type="checkbox"/> weekly	europe-west4	Every Saturday between 12:00 PM and 1:00 PM	30 days	monitoring-data

Security by design - Intégrité

← → ↺ 🏠 ⓘ 🔒 https://console.cloud.google.com/compute/snapshots?project=opsec-lis-dtp&orgonly=true&... ☆ 🌐 🇪🇺 ☁️ ☰

☰ Google Cloud Platform opsec-lis-dtp 🔍

🔧 Compute Engine

- 📄 VM instances
- 🏢 Instance groups
- 📄 Instance templates
- 👤 Sole tenant nodes
- 💾 Disks
- 📷 **Snapshots**
- 🖼️ Images
- 🛒 Marketplace
- <|

Snapshots [CREATE SNAPSHOT](#) 📅 ↺ 🗑️ [SHOW INFO PANEL](#)

[Snapshots](#) Snapshot schedules

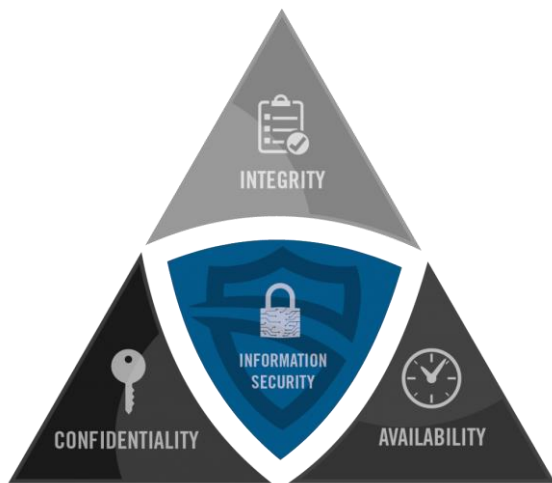
☰ Filter snapshots ⓘ Columns ▾

<input type="checkbox"/> Name ^	Location	Snapshot size	Creation time	Creation type	Source disk	Disk size
<input type="checkbox"/> ✓ weekly-1	eu	35.17 MB	Apr 23, 2019, 5:10:37 PM	Manual	monitoring-data	30 GB

Security by design - Intégrité

Nous utilisons simplement docker-compose pour définir la configuration de nos conteneurs

```
wallix@monitoring:~$ sudo cat /mnt/scripts/docker-compose.yml
version: '3.3'
services:
  graphite:
    image: 'graphiteapp/graphite-statsd:latest'
    volumes:
      - '/mnt/data/opt/graphite/conf:/opt/graphite/conf'
      - '/mnt/data/opt/graphite/storage:/opt/graphite/storage'
      - '/mnt/data/opt/statsd/config:/opt/statsd/config'
    restart: always
    ports:
      - '2003-2004:2003-2004'
      - '2023-2024:2023-2024'
      - '8125:8125/udp'
      - '8126:8126'
  nginx:
    image: 'nginx:latest'
    volumes:
      - 
      - '/mnt/data/etc/nginx/nginx.conf:/etc/nginx/nginx.conf'
    restart: always
    ports:
      - '443:443'
  stats:
    image: 'python:latest'
    restart: always
    build:
      context: /tmp
      dockerfile: stats-Dockerfile
    environment:
      VAULT_URL : https://
      VAULT_AUDIENCE_URL : 
      VAULT_AUTH_URL : h
      VAULT_NAMESPACE : 
      VAULT_ROLE : monitoring
```

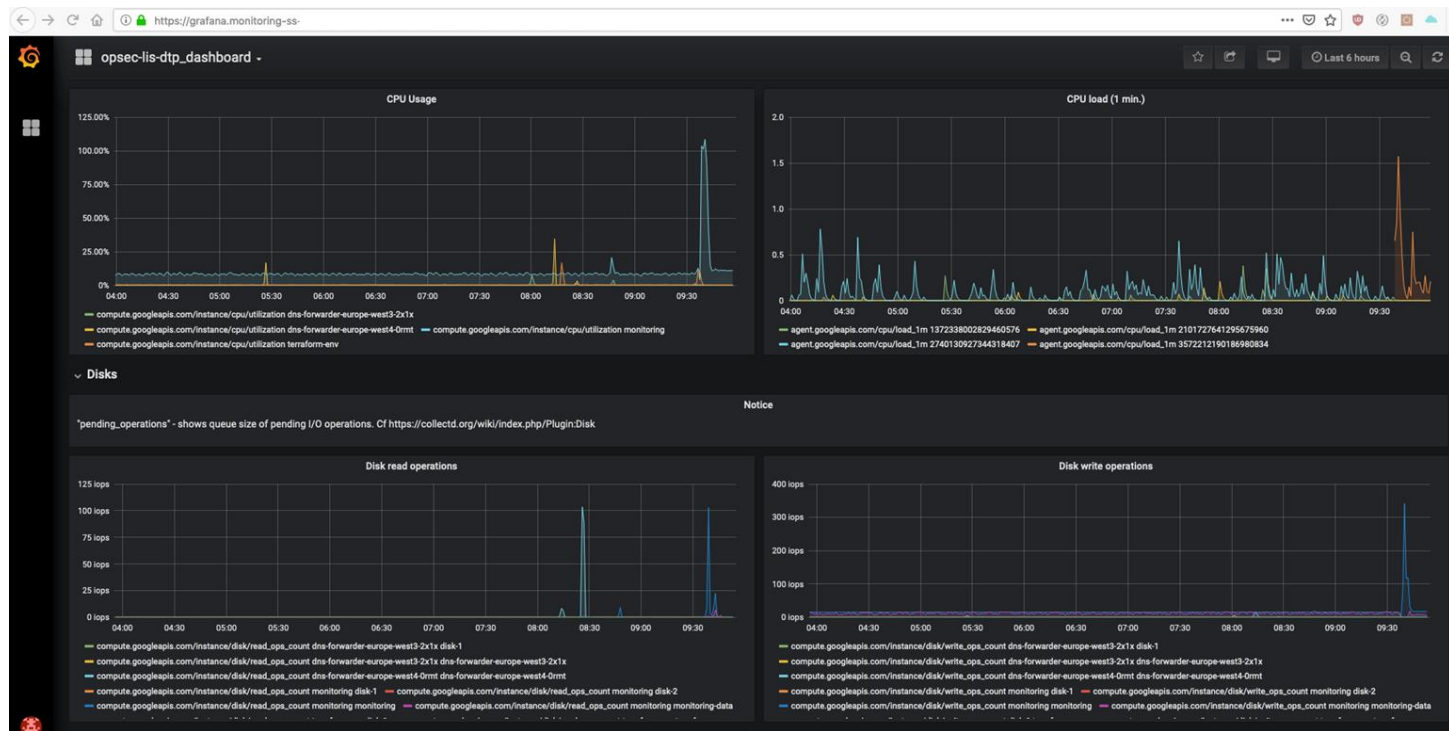


Et nous bénéficions de tous les avantages de la landing zone

Security by design

Le laas nous fournit
des statistiques

comme la CPU,
Disk ...



Security by design

réseau, Firewall

...

