



**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

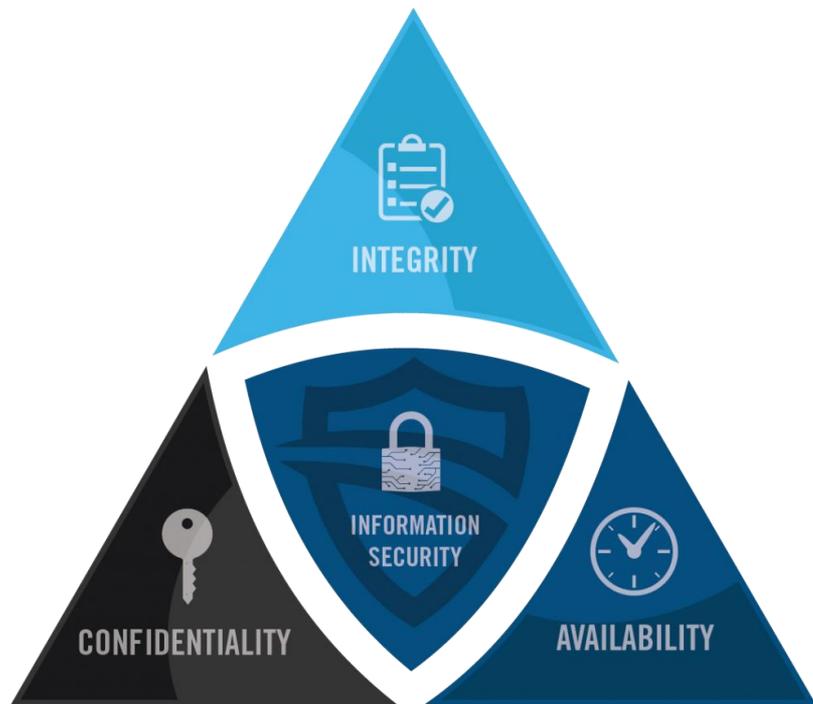


**Intégrité:** S'assurer que les données ne sont pas falsifiées ou altérées par des utilisateurs non autorisés



**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.

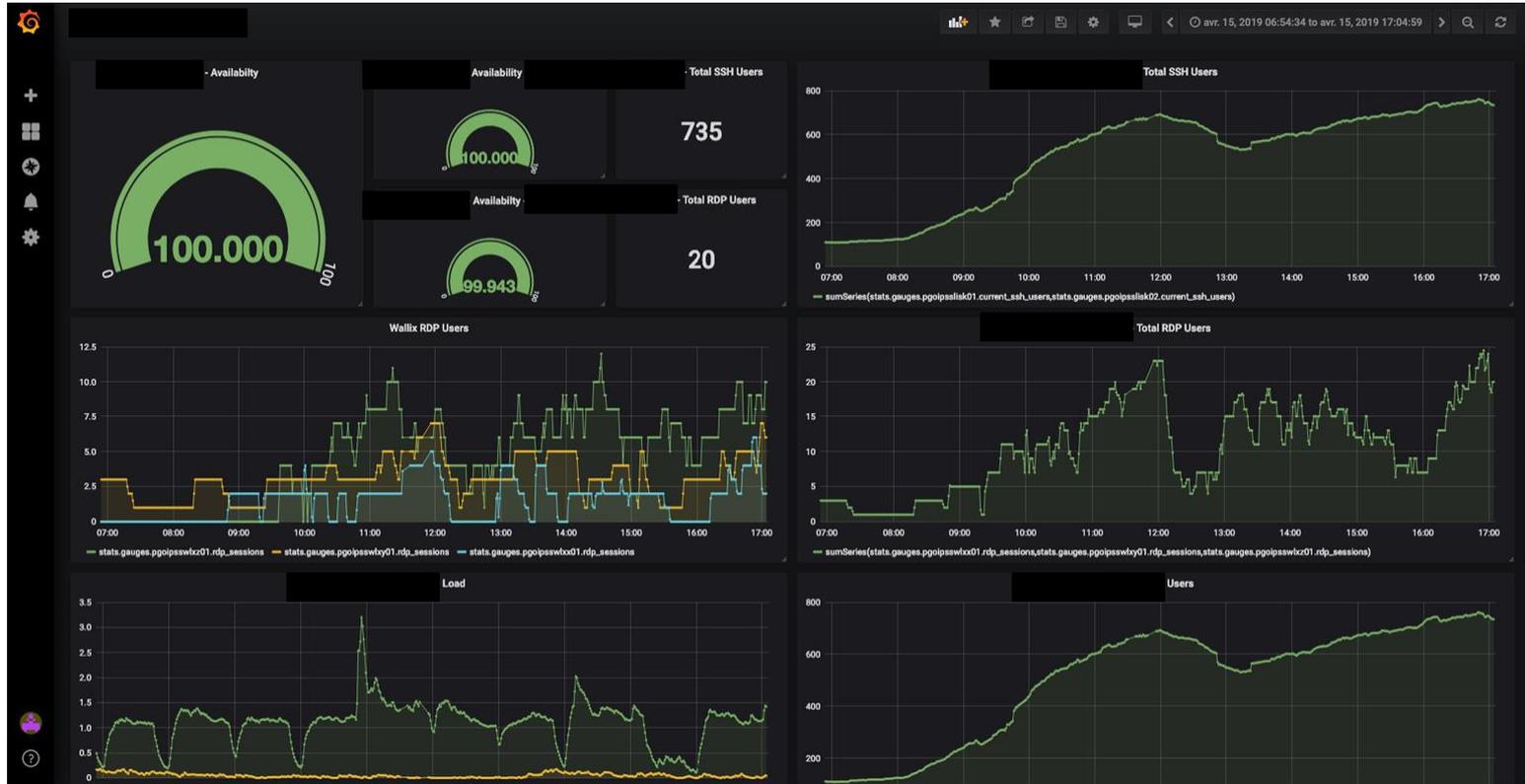


**Une démonstration avec une  
solution de monitoring ?**

## 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**

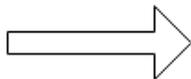
# Un aperçu de l'application



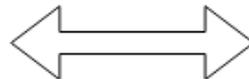
# Un aperçu de l'application

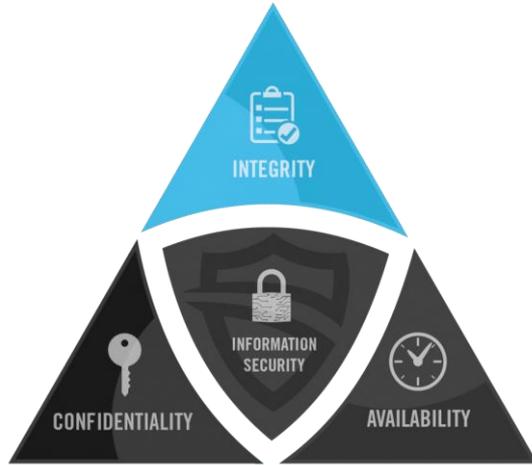


Comment cela fonctionne ?



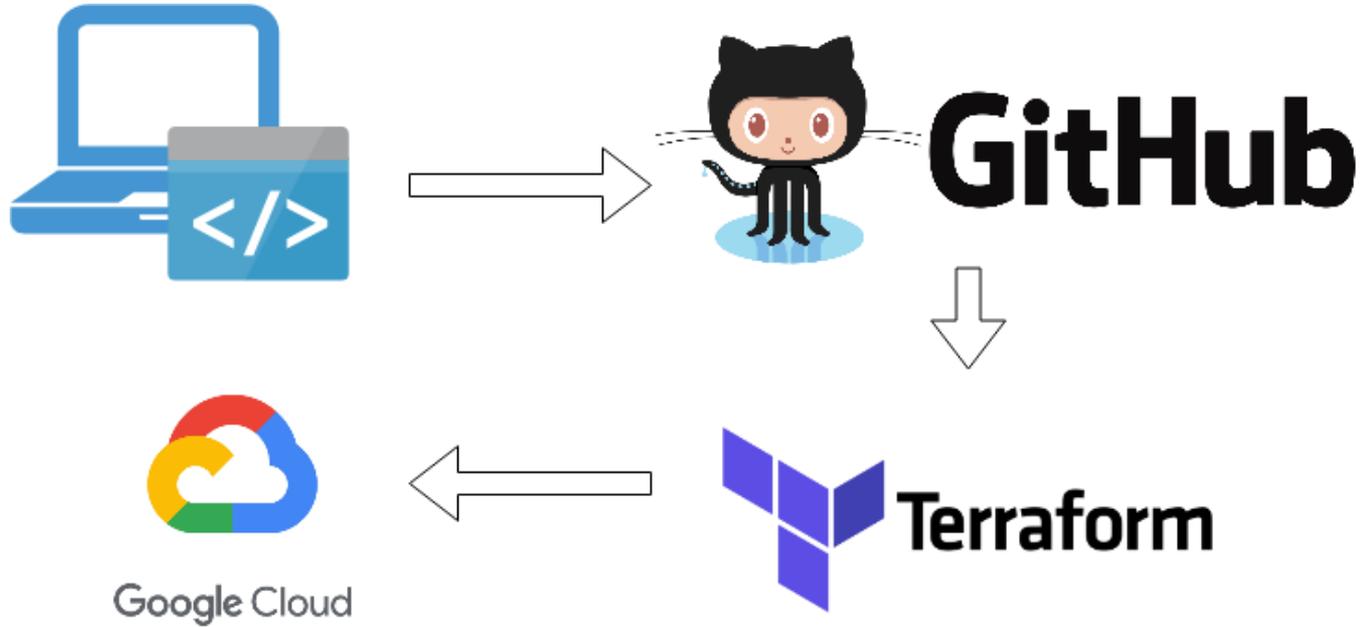
Google Cloud  
Public IAAS





## Un peu d'infrastructure as code

# Security by design - Intégrité



# Security by design - Intégrité

The screenshot shows a GitHub repository page for 'opsec-monitoring'. The browser address bar shows 'https://github.com/'. The repository is private and has 2 watchers, 0 stars, and 0 forks. The main content area displays the repository name, a description 'Dedicated monitoring for security team.', and statistics: 11 commits, 2 branches, 0 releases, and 1 contributor. Below this, there are buttons for 'Branch: master', 'New pull request', 'Create new file', 'Upload files', 'Find File', and 'Clone or download'. A list of files and folders is shown, including 'conf', 'scripts', 'stats', 'terraform', '.gitignore', and 'README.md', each with a description and a commit date.

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

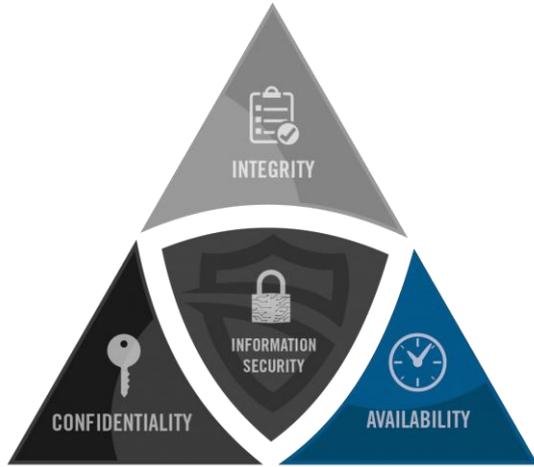
- VM instances
- Instance groups
- Instance templates
- Sole tenant nodes
- Disks
- Snapshots
- Images
- TPUs
- Committed use discounts
- Marketplace

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](#)

[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



**NGINX**



Google Cloud



- 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.

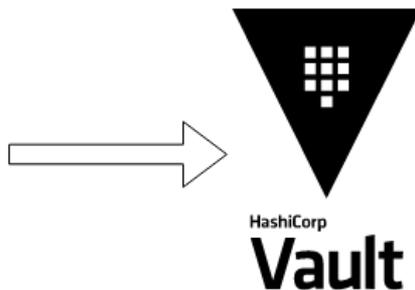
Si une nouvelle image est trouvée, le conteneur est mis à jour.

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. At the top, a browser address bar shows a secure connection (https://). The 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 is titled 'Vault Web UI' and contains a message: '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.' Below this message, there is a section 'Walk me through setting up:' with two options: 'Secrets' and 'Authentication', each with an unchecked checkbox and a dropdown arrow. The footer of the page includes the HashiCorp logo, copyright information for 2019 HashiCorp, Inc., the version 'Vault 1.1.0+pro', and a link to 'Documentation'.

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.

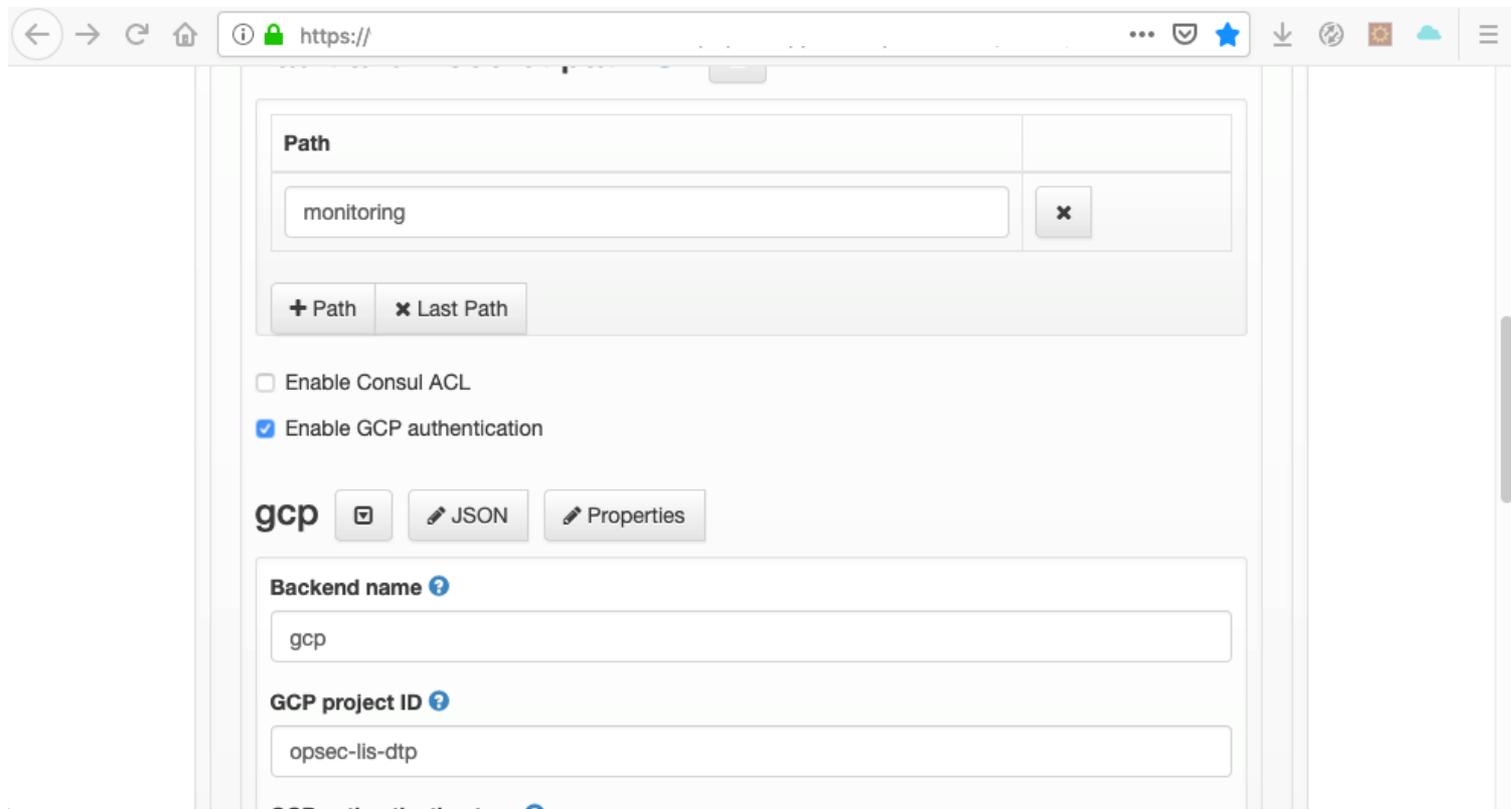
- ! Vault only shows links to pages that you have access to based on your policies. Contact your administrator if you need access changes.

#### Walk me through setting up:

- Secrets
- Authentication

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

# Security by design - Confidentialité



# Security by design - Confidentialité

The screenshot shows the Vault Web UI interface. At the top, there is a navigation bar with a dropdown menu set to 'opsec-lis-' and tabs for 'Secrets', 'Access', 'Policies', and 'Tools'. 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 copy icon, an eye icon, and a redacted value. To the right of the table is a sidebar with a 'Vault Web UI' header and a 'Choosing where to go' section. This section contains a message about access and a 'Walk me through setting up:' section with two dropdown menus: 'Secrets' and 'Authentication'.

opsec-lis- | Secrets | Access | Policies | Tools

## monitoring

[Delete secret](#)

JSON [Copy Secret](#) [Create new version](#) Version 7 > [History](#) >

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.

- i** 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

← → ↻ 🏠 ⓘ 🔒 https://console.cloud.google.com/compute/metadata/sshKeys?project=opsec-lis-dtp

☰ Google Cloud Platform opsec-lis-dtp 🔍

🔧 Compute Engine

- 📄 VM instances
- 🏠 Instance groups
- 📄 Instance templates
- 👤 Sole tenant nodes
- 📀 Disks
- 📷 Snapshots
- 🏠 Images
- 🔧 TPUs
- 🛒 Marketplace

Metadata SSH Keys

wallix

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACyM2AXy8mtz8mMJ5zRZ0uyeY+ePA2bnRdrxdAqin0xJa
Ir41qpBxFuQNJcsMwCvusw844RT1mmnJ27fz91yqDpEj8KdJ0K1n2xqjts0VegaYdBhEMh0I5wgvsevs
TQ1Z5U1YjTZyaz1jv5h2F1qrCZHELGbAE6Ak0NAQek05UfeHR+rSR2TDBsmr1ygf+YviT2m0J9w+zb1TTt
y261Ub3S0a02nZeZGvf1B+a1NSoNeEbjNBjIHfVsEjG85LrRW4AEbax2yf0Aa5XMMWf3d3CEoqeXC91dyIJ
pMYyxHK4GSi6AKVmBL41Mm688Cd+f9aLWkwbw1VB2D546PekUqIUGUx/q0AcVjMtQ4amtrWSer20E8xANi
87vWxaIF12r2gIDkFH04dk1B90peRh1kutnB0vGPREuZMSoAC64248j+XGhnJi0Htn689n6Cp6tKvu9GTx
vniIHY44e30h8uMechOKUn+OX1Wl07Vb4oYF0naE15eT1sCfzkbL/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.securit ██████████	local	wallix	SSH	AS_N3_SECUREITE	██████████
<input type="checkbox"/>	>_	🔒 terraform.monitori ██████████	local	wallix	SSH	AS_N3_SECUREITE	██████████

# Security by design

The screenshot displays a web application interface for managing sessions. The main page is titled "Sessions" and includes a search bar with the text "monitoring". A table lists resources, with columns for checkboxes, resource names, and bastion hosts. A modal dialog titled "Choose an SSH action" is open, showing a list of actions for the user "wallix@local@monitoring.security:" on the host "SSH:AS\_N3\_SECUREITE". The actions are: "Open an SSH shell session", "Open an SFTP session", "SCP Upload", "SCP Download", and "Remote Command". A "Close" button is located at the bottom right of the modal.

Choose an SSH action

wallix@local@monitoring.security: SSH:AS\_N3\_SECUREITE

- Open an SSH shell session
- Open an SFTP session
- SCP Upload
- SCP Download
- Remote Command

Close

Sessions

Explorer

monitoring

Q Search

1 - 2 of 2

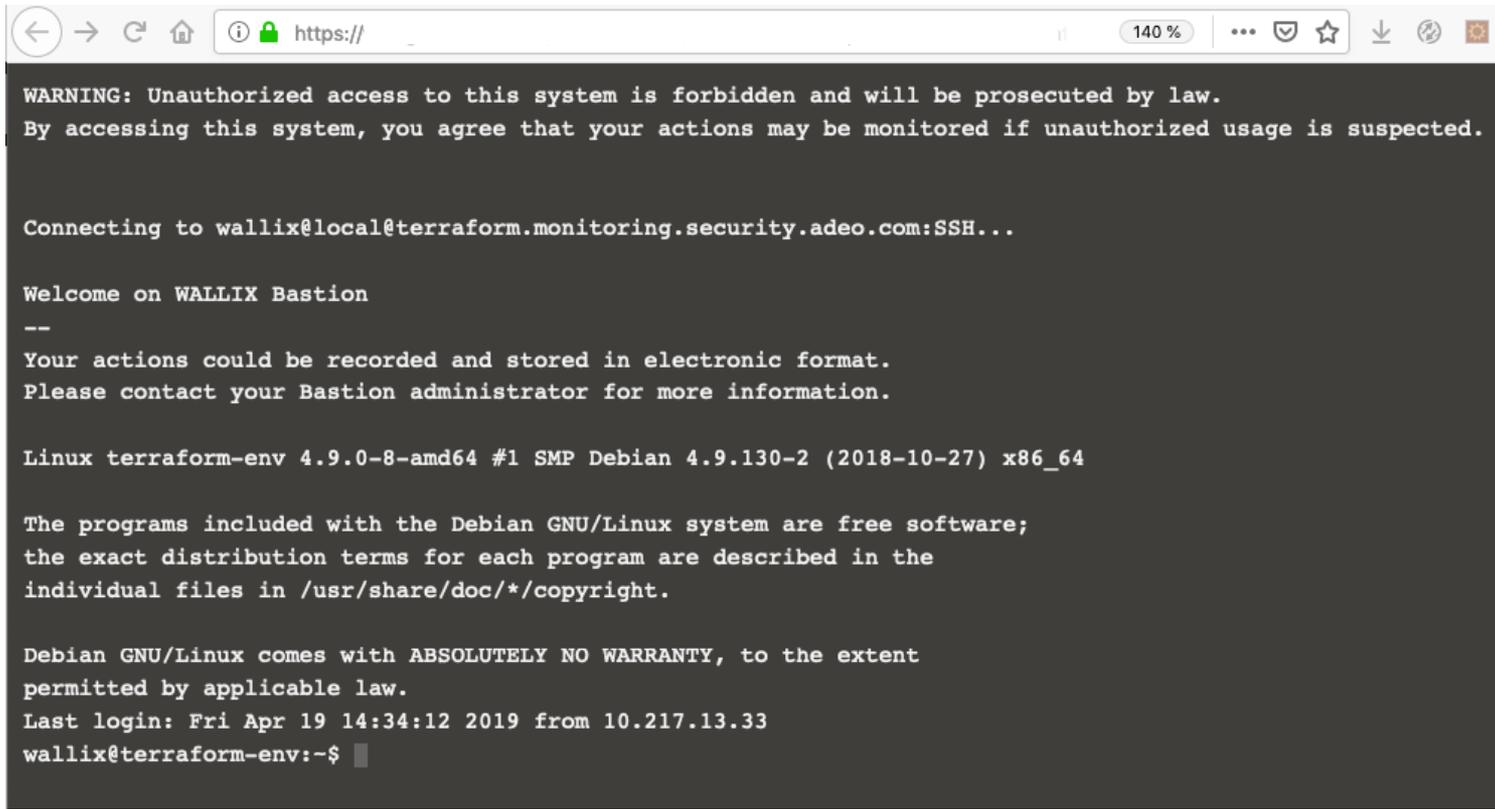
Bastion

BASTIONS

BASTIONS\_

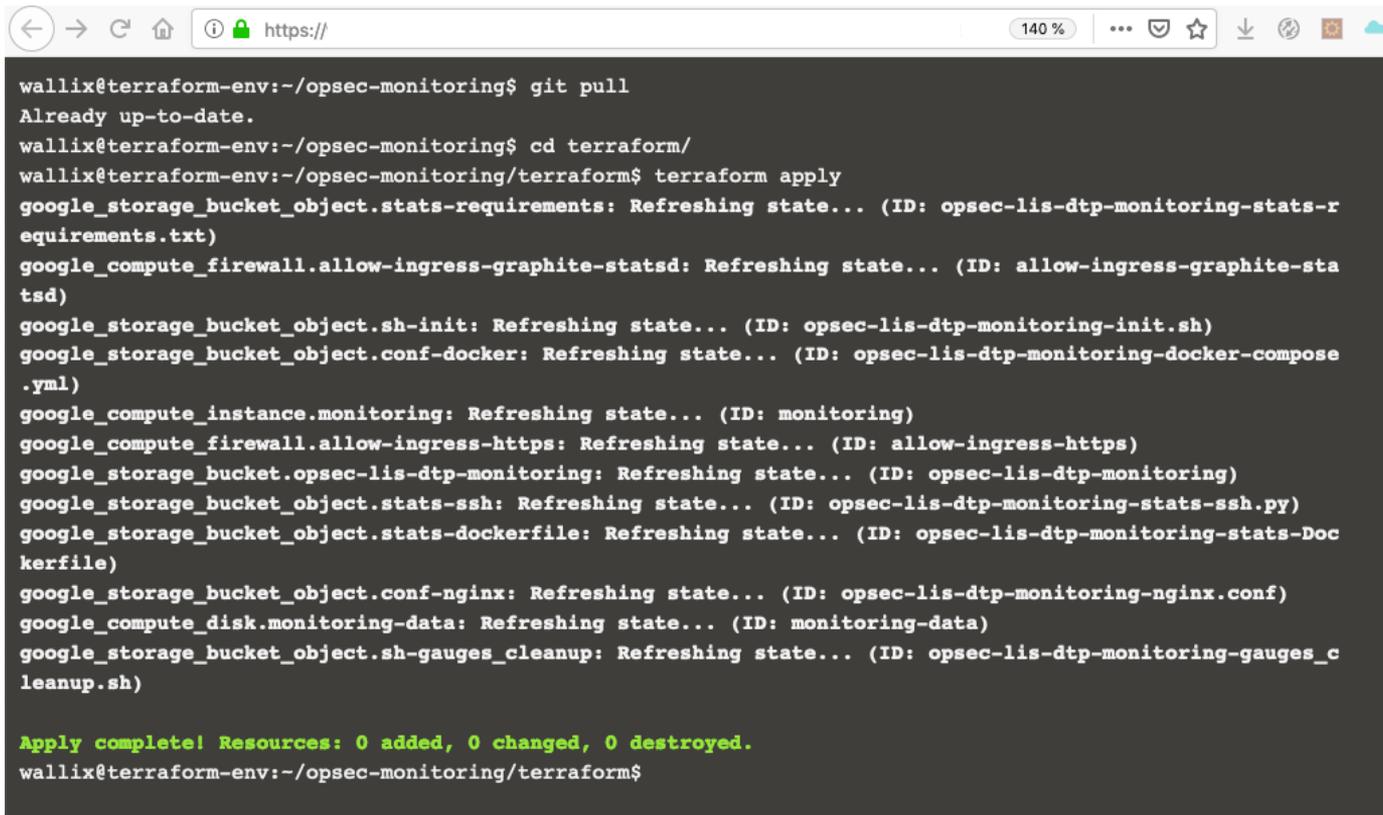
<input type="checkbox"/>	Resource
<input type="checkbox"/>	>_ monitoring.s
<input type="checkbox"/>	>_ terraform.m

# Security by design



```
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

A screenshot of a web browser window displaying a terminal session. The browser's address bar shows a secure connection (https://) and a zoom level of 140%. The terminal output shows a user named 'wallix' running 'git pull' in a directory named 'terraform-env', which reports 'Already up-to-date.'. The user then runs 'cd terraform/' and 'terraform apply'. The apply process refreshes the state for several resources, including Google Storage buckets for stats requirements, firewall rules for graphite-statsd and https, monitoring configurations, and disk data. The final output is 'Apply complete! Resources: 0 added, 0 changed, 0 destroyed.' followed by the prompt 'wallix@terraform-env:~/opsec-monitoring/terraform\$'.

```
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$
```

- 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 LL

Audit Historique des sessions	
Mes préférences	
Mes autorisations	
Audit	
Sessions courantes	
<b>Historique des sessions</b>	
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: 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

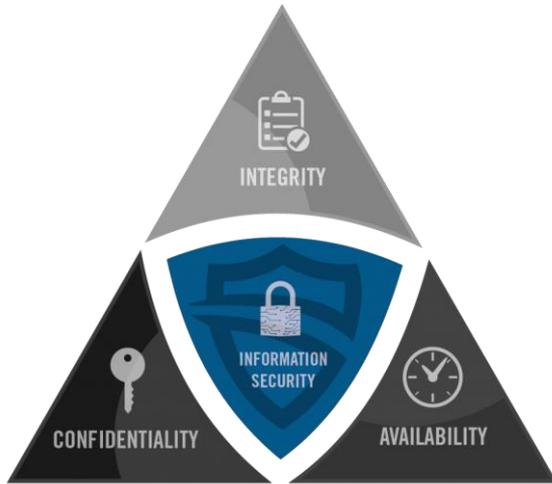


## Transcription

```
google_storage_bucket.opsec-lis-dtp-monitoring-states-ssh: Refreshing state... (ID: opsec-lis-dtp-monitoring-states-ssh.py)
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.stats-requirements: Refreshing state... (ID: opsec-lis-dtp-monitoring-states-requirements.txt)
google_storage_bucket_object.stats-ssh: Refreshing state... (ID: opsec-lis-dtp-monitoring-states-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

The screenshot shows the Google Cloud Platform Logging interface. The left sidebar contains navigation options: Stackdriver Logging, Logs, Logs-based metrics, Exports, and Logs ingestion. The main content area displays a list of logs for a GCE VM Instance, filtered by the 'auth' label and 'Any log level' over the last 7 days. The logs show various SSH and PAM events, including session openings and disconnections for user 'wallix'.

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)

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

Logs d'authentification

# Security by design - Intégrité

## Logs Docker

The screenshot displays the Google Cloud Platform Logging console. The left sidebar shows navigation options: Stackdriver Logging, Logs, Logs-based metrics, Exports, and Logs ingestion. The main content area shows a log entry for a Docker container. The log entry is expanded, revealing a JSON payload. Two red boxes highlight specific parts of the log: the container details and the log message.

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

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

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

{
  insertId: "ophdmqg24jrreg"
  jsonPayload: {
    container: {
      created: "2019-04-19T07:17:57.501940421Z"
      id: "84f7b83c22fa38a6888093d8b802dc75096724c9c1645df2c624d7e5af7d2d40"
      imageId: "sha256:1d7b81067e37934de60c2988ed68e6b749cc5e1c9c22072803f813a6cef90411"
      imageName: "graphiteapp/graphite-stats:latest"
      name: "/scripts_graphite_1_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"
```

The screenshot shows the Google Cloud Platform logs viewer interface. The browser address bar displays the URL: `https://console.cloud.google.com/logs/viewer?orgonly=true&project=opsec-lis-dtp&minLogLevel=0&expandAll=false&timestamp=2`. The page header includes the Google Cloud Platform logo, the project name 'opsec-lis-dtp', and a search bar. Below the header, there are buttons for 'CREATE METRIC', 'CREATE EXPORT', and a refresh icon. The main content area shows a filter bar with 'GCE VM Instance' selected, 'auth' as the log source, and 'Any log level' as the filter. The logs are filtered to the last hour, ending at 5:36 PM (CEST). The log entries show a sequence of events for a sudo session:

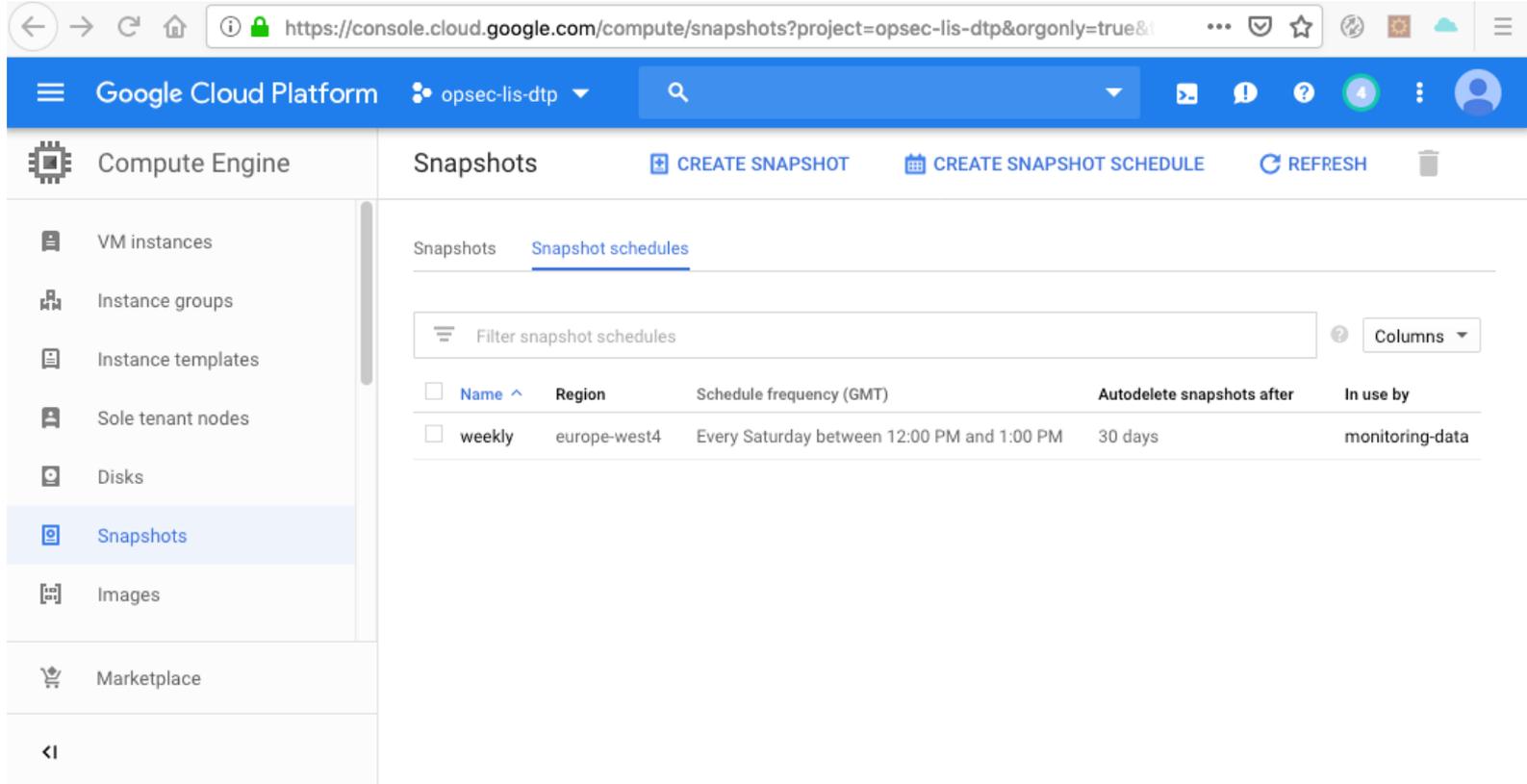
- 2019-04-23 17:27:16.000 CEST Apr 23 15:27:16 monitoring sudo: wallix : TTY=pts/0 ; PWD=/home/wallix ; USER=root ; COMMAND=/bin/cat /etc/sudoers
- 2019-04-23 17:27:16.000 CEST Apr 23 15:27:16 monitoring sudo: pam\_unix(sudo:session): session opened for user root by wallix(uid=0)
- 2019-04-23 17:27:16.000 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

The log entry for the command `COMMAND=/bin/cat /var/log/auth.log` is highlighted with a red box.



## Un peu de sauvegarde

# Security by design - Intégrité



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 navigation menu with options: 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 this, there are tabs for 'Snapshots' and 'Snapshot schedules'. A search box labeled 'Filter snapshot schedules' and a 'Columns' dropdown are present. A table displays the following data:

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

# Security by design - Intégrité

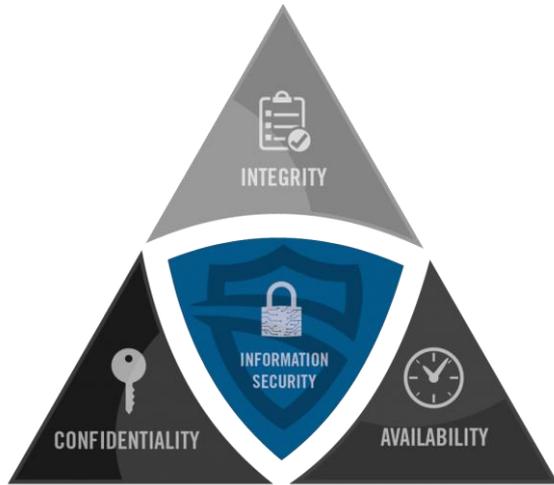
The screenshot shows the Google Cloud Platform console interface. The top navigation bar includes the Google Cloud Platform logo, the project name 'opsec-lis-dtp', a search bar, and various utility icons. The left sidebar lists navigation options: Compute Engine, VM instances, Instance groups, Instance templates, Sole tenant nodes, Disks, Snapshots (highlighted), Images, and Marketplace. The main content area is titled 'Snapshots' and includes a 'CREATE SNAPSHOT' button, a calendar icon, a refresh icon, a trash icon, and a 'SHOW INFO PANEL' link. Below the title, there are tabs for 'Snapshots' and 'Snapshot schedules'. A search bar labeled 'Filter snapshots' and a 'Columns' dropdown menu are present. A table lists the snapshots with the following data:

<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:
      - [REDACTED]
      - '/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://[REDACTED]
      VAULT_AUDIENCE_URL : [REDACTED]
      VAULT_AUTH_URL : https://[REDACTED]
      VAULT_NAMESPACE : [REDACTED]
      VAULT_ROLE : monitoring
```

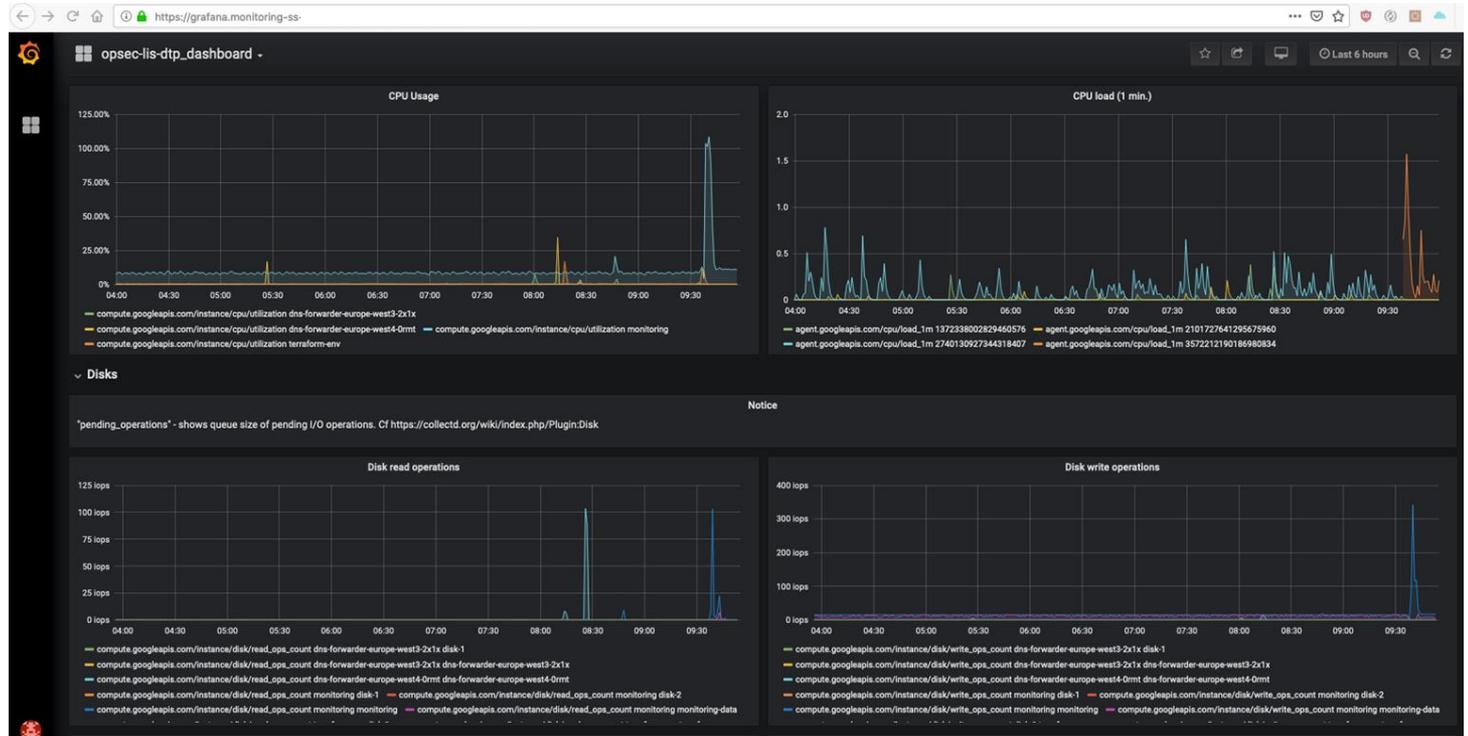


**Et nous bénéficions de tous les avantages de la landing zone**

# Security by design

Le Iaas nous fournit  
des statistiques

comme la CPU,  
Disk ...



# Security by design

réseau, Firewall

...

