Evidian

# SafeKit Cluster in the Google GCP Marketplace

## Startup Guide

# Table of Contents

# 1. Overview

Evidian SafeKit provides a high availability cluster with synchronous real-time file replication, load balancing and automatic application failover. This clustering solution is recognized as the simplest to implement by our customers and partners. It is also a complete solution that solves hardware failures (20% of problems) including the complete failure of a computer room, software failures (40% of problems) including software error detection and automatic restart and human errors (40% of problems) thanks to its simplicity of administration.

Evidian is a Google partner and provides packaged solutions for SafeKit on Google Cloud Platform (GCP). These enable you to be up and running with SafeKit high availability clusters on GCP quickly and easily. 4 different solutions are offered:

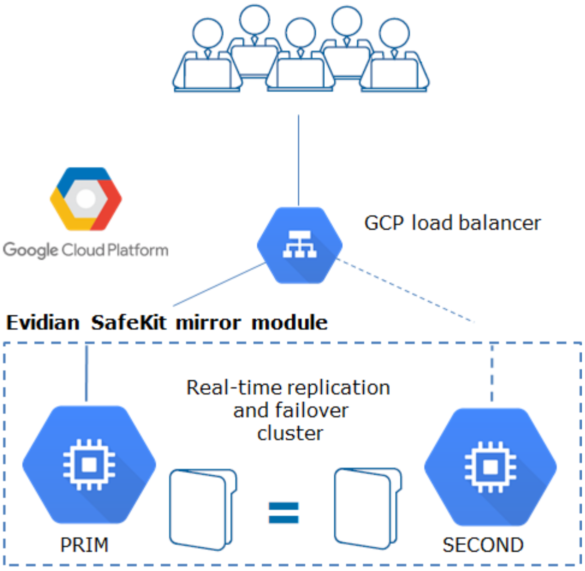
- SafeKit mirror cluster on Windows
- SafeKit mirror cluster on Linux
- SafeKit farm cluster on Windows
- SafeKit farm cluster on Linux

The mirror solutions deploy a high availability cluster with virtual IP, synchronous real-time file replication and automatic application failover, between 2 Windows or CentOS VM instances in different availability zones. For details, refer to SafeKit Mirror Cluster in Google GCP page 5.

The farm solutions deploy a high availability cluster with network load balancing on a virtual IP address and automatic application failover, between 2 Windows or CentOS VM instances in different availability zones. For details, refer to SafeKit Farm Cluster in Google GCP page 7.

For instructions to setup mirror and farm solutions into GCP, refer to Deploy a SafeKit Cluster Solution page 9.

# 2. SafeKit Mirror Cluster in Google GCP



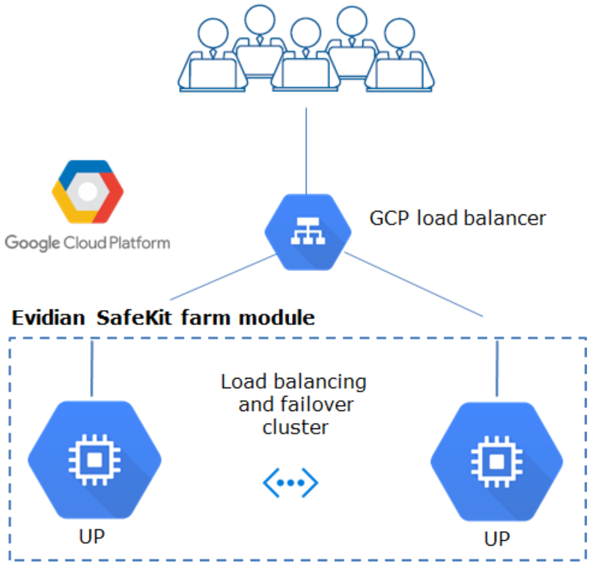
On the previous figure,

- the servers are running in different availability zones. The VM instances are based on Windows or CentOS depending on the deployed solution
- the critical application is running on the PRIM server
- users are connected to a primary/secondary virtual IP address which is configured in the Google GCP load balancer
- SafeKit provides a generic health check for the load balancer (URL managed by SafeKit and configured in the load balancer). On the PRIM server, the health check returns OK to the load balancer and NOK on the SECOND server.
- in each server, SafeKit monitors the critical application with process checkers and custom checkers
- SafeKit restarts automatically the critical application when there is a software failure or a hardware failure thanks to restart scripts
- SafeKit makes synchronous real-time replication of files containing critical data
- a connector for the SafeKit web console is installed in each server. Thus, the high availability cluster can be managed in a very simple way to avoid human errors

On the previous figure, the server 1/PRIM runs the critical application. Users are connected to the virtual IP address of the mirror cluster. SafeKit replicates files opened by the critical application in real time. Only changes in the files are replicated across the network, thus limiting traffic (byte-level file replication). Names of file directories containing critical data are simply configured in SafeKit. There are no pre-requisites on disk organization for the two servers. Directories to replicate may be located in the system disk. SafeKit implements synchronous replication with no data loss on failure contrary to asynchronous replication.

In case of server 1 failure, there is an automatic failover on server 2 with restart of the critical application. Then, when server 1 is restarted, SafeKit implements automatic failback with reintegration of data without stopping the critical application on server 2. Finally, the system returns to synchronous replication between server 2 and server 1. The administrator can decide to swap the role of primary and secondary and return to a server 1 running the critical application. The swap can also be done automatically by configuration.

# 3. SafeKit Farm Cluster in Google GCP


Google Cloud Platform
GCP load balancer
Evidian SafeKit farm module
Load balancing and failover cluster
UP
UP

On the previous figure,

- ➩ the servers are running in different availability zones. The VM instances are based on Windows or CentOS depending on the deployed solution.
- the critical application is running in all servers of the farm
- users are connected to a virtual IP address which is configured in the Google GCP load balancer
- SafeKit provides a generic health check for the load balancer (URL managed by SafeKit and configured in the load balancer). When the farm module is stopped in a server, the health check returns NOK to the load balancer which stops the load balancing of requests to the server. The same behavior happens when there is a hardware failure
- in each server, SafeKit monitors the critical application with process checkers and custom checkers
- SafeKit restarts automatically the critical application in a server when there is a software failure thanks to restart scripts
- a connector for the SafeKit web console is installed in each server. Thus, the load balancing cluster can be managed in a very simple way to avoid human errors

# 4. Deploy a SafeKit Cluster Solution

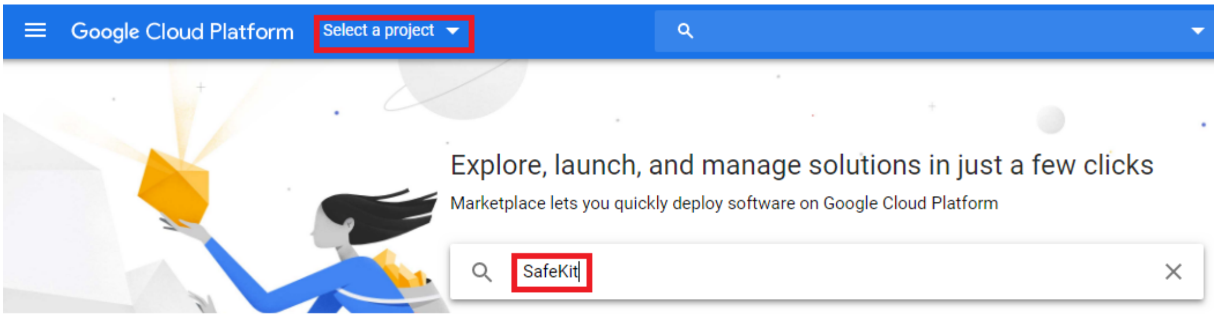
To quickly set up a SafeKit cluster on the Google Cloud Platform, perform the following steps. All the SafeKit solutions are based on the same procedure. In the following, we take the SafeKit mirror cluster on Windows sample.

## 4.1 Prerequisites

- you must be able to sign in to the Google Cloud Platform Console using a Google Account. Refer to Signing In to the Google Cloud Platform Console
- You must have Google project(s) and select one for deploying the solution. Refer to Creating and managing Google Cloud Platform projects
- You must have configured a VPC network for the selected project. It will be used to provide connectivity for the VM instances in your project. Refer to Using VPC networks
- The SafeKit solutions are BYOL (Bring Your Own License). The GCP Marketplace deploys the solution but you are responsible for getting the SafeKit license directly from Evidian. You can get here a free SafeKit one-month key.

## 4.2 Select the SafeKit Solution in Google Marketplace

- Sign in to the Google Cloud Platform Console and navigate to the Google Marketplace page

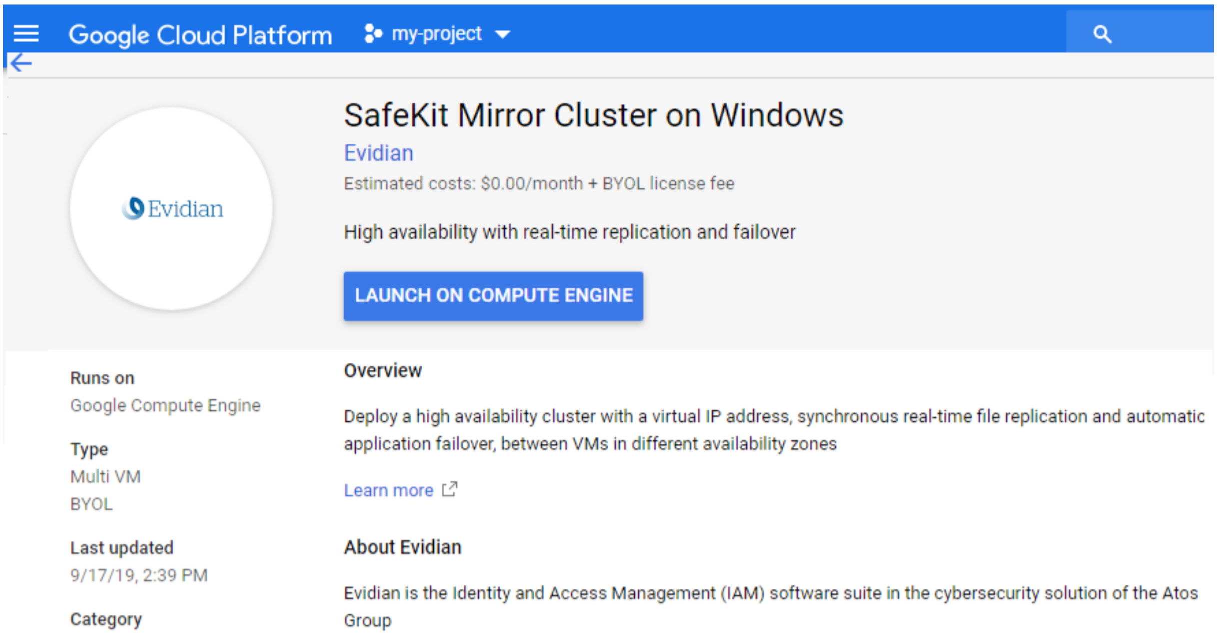


Explore, launch, and manage solutions in just a few clicks

Marketplace lets you quickly deploy software on Google Cloud Platform

SafeKit

- Select the project that will contain the deployment
- Search for SafeKit solutions
- According your needs, select either: SafeKit Mirror Cluster on Windows, SafeKit Farm Cluster on Windows, SafeKit Mirror Cluster on Linux, SafeKit Farm Cluster on Linux. For instance, for SafeKit mirror cluster on Windows, it opens the window:



SafeKit Mirror Cluster on Windows

Evidian

Estimated costs: $0.00/month + BYOL license fee

High availability with real-time replication and failover

LAUNCH ON COMPUTE ENGINE

Runs on
Google Compute Engine

Type
Multi VM
BYOL

Last updated
9/17/19, 2:39 PM

Category

Overview

Deploy a high availability cluster with a virtual IP address, synchronous real-time file replication and automatic application failover, between VMs in different availability zones

Learn more

About Evidian

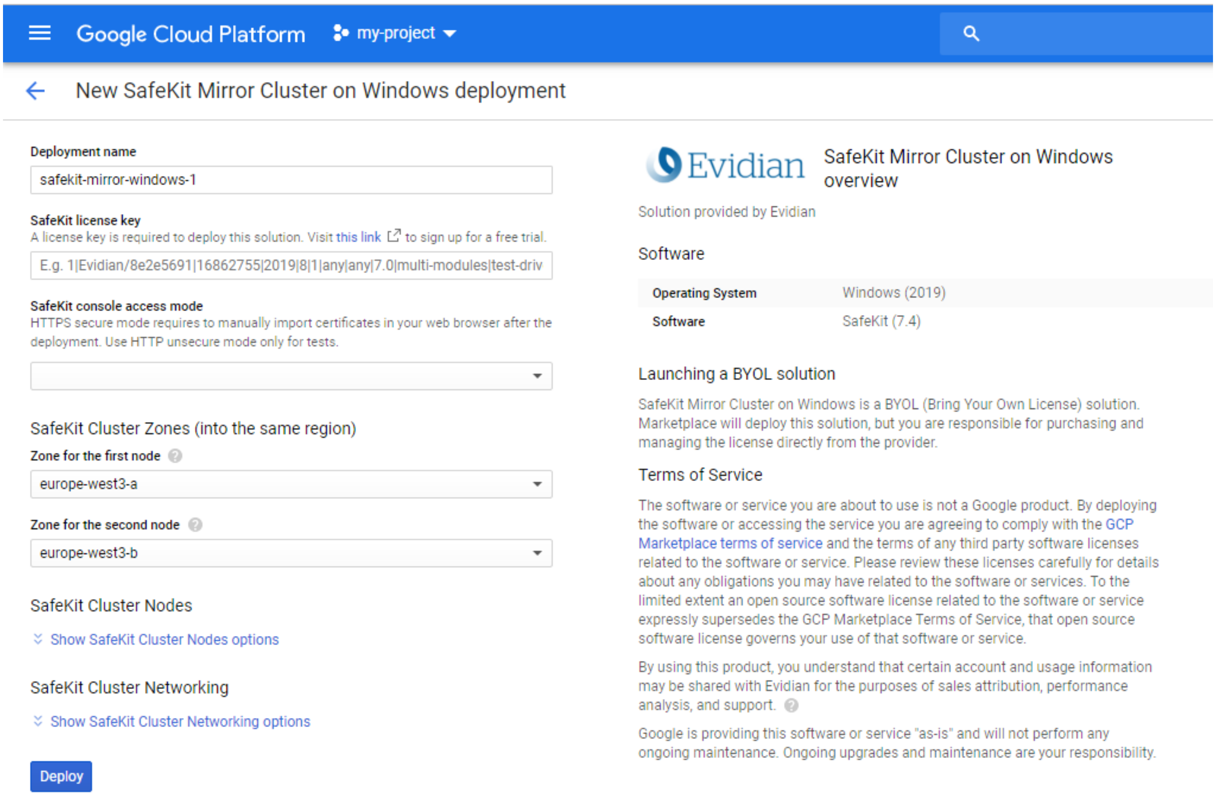
Evidian is the Identity and Access Management (IAM) software suite in the cybersecurity solution of the Atos Group

⇨ Click the **LAUNCH ON COMPUTE ENGINE** button

LAUNCH ON COMPUTE ENGINE

## 4.3 Parameterize the Solution

In the Configure & Deploy window:



New SafeKit Mirror Cluster on Windows deployment

Deployment name
safekit-mirror-windows-1

SafeKit license key
A license key is required to deploy this solution. Visit this link to sign up for a free trial.
E.g. 1|Evidian/8e2e5691|16862755|2019|8|1|any|any|7.0|multi-modules|test-driv

SafeKit console access mode
HTTPS secure mode requires to manually import certificates in your web browser after the deployment. Use HTTP unsecure mode only for tests.

SafeKit Cluster Zones (into the same region)

Zone for the first node
europe-west3-a

Zone for the second node
europe-west3-b

SafeKit Cluster Nodes
Show SafeKit Cluster Nodes options

SafeKit Cluster Networking
Show SafeKit Cluster Networking options

Deploy

SafeKit Mirror Cluster on Windows overview

Solution provided by Evidian

Software

| | |
|---|---|
| Operating System | Windows (2019) |
| Software | SafeKit (7.4) |

Launching a BYOL solution

SafeKit Mirror Cluster on Windows is a BYOL (Bring Your Own License) solution. Marketplace will deploy this solution, but you are responsible for purchasing and managing the license directly from the provider.

Terms of Service

The software or service you are about to use is not a Google product. By deploying the software or accessing the service you are agreeing to comply with the GCP Marketplace terms of service and the terms of any third party software licenses related to the software or service. Please review these licenses carefully for details about any obligations you may have related to the software or services. To the limited extent an open source software license related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software license governs your use of that software or service.

By using this product, you understand that certain account and usage information may be shared with Evidian for the purposes of sales attribution, performance analysis, and support.

Google is providing this software or service "as-is" and will not perform any ongoing maintenance. Ongoing upgrades and maintenance are your responsibility.

- enter or select appropriate values:
  - ✓ get here a free SafeKit one-month key. You will receive a mail containing a license.txt file that looks like:

```
# Before License Key installation, pay attention to any product-specific
instructions.

# ONLY USE A TEXT EDITOR to edit the specified files. DO NOT USE word processors.

#

# SafeKit

# Please copy or append the License Keys to the safekit/conf/license.txt file.

# Hostname: any

# multi-modules Version 7 license key for machine any OS any available up to
2019/10

1|Evidian/99f05635|16862755|2019|10|1|any|any|7.0|multi-modules|test-
drive|553af1484c6e7887517d3466ec96fae4
```

Copy only the last line into the license key field

  - ✓ select HTTP or HTTPS for the SafeKit console access mode; HTTPS requires to manually import certificates into your web browser before starting the SafeKit web console. It is described in Import Certificates in your Web Browser page 14

  - ✓ select 2 different zones, located into the same region, for running the 2 VM instances of the SafeKit cluster

- Click the **Deploy** button

Deployment begins, and you will be redirected to the Deployment Manager where the deployment status is displayed.

### *Notes*

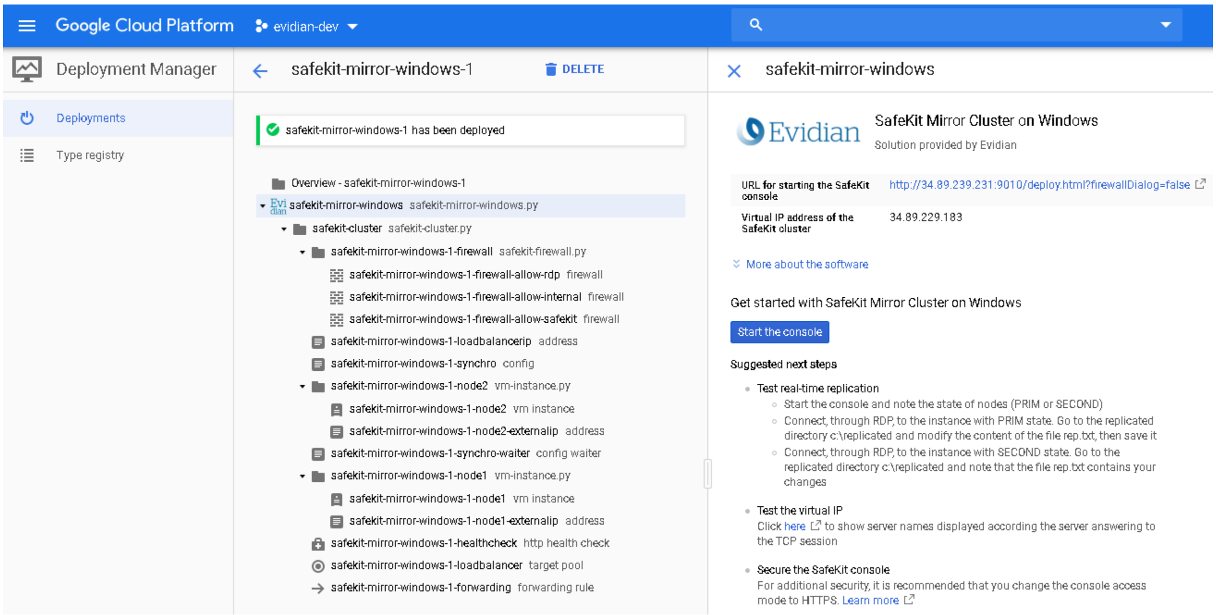
External IP address is attached to each VM instance to enable external internet access for the SafeKit cluster administration. External IP addresses are stored into the SafeKit cluster configuration and HTTPS configuration when it is selected. By default, the deployment sets static external IP addresses. If you prefer, you can select ephemeral external IP into the SafeKit Cluster Networking options panel. In that case, you will have to change the configuration for the remote administration, when the external IP address value will change on VM instances reboot.

## 4.4 Check the Deployment

The deployment may take several minutes, the time to create all the GCP resources and customize the SafeKit cluster. It appears as pending. Firewall configuration, load balancer for a virtual IP, 2 VMs, installation and configuration of SafeKit are deployed automatically. For details on deployed GCP resources and SafeKit cluster configuration, see SafeKit Mirror Cluster in Google GCP page 5 and SafeKit Farm Cluster in Google GCP page 7.

➩ A green check mark is displayed one deployment completes successfully.

The image below is the output of the deployment when selecting HTTP for the SafeKit console access mode.



✓ safekit-mirror-windows-1 has been deployed

```
Overview - safekit-mirror-windows-1
▾ safekit-mirror-windows  safekit-mirror-windows.py
    ▾ safekit-cluster  safekit-cluster.py
        ▾ safekit-mirror-windows-1-firewall  safekit-firewall.py
              safekit-mirror-windows-1-firewall-allow-rdp  firewall
              safekit-mirror-windows-1-firewall-allow-internal  firewall
              safekit-mirror-windows-1-firewall-allow-safekit  firewall
          safekit-mirror-windows-1-loadbalancerip  address
          safekit-mirror-windows-1-synchro  config
        ▾ safekit-mirror-windows-1-node2  vm-instance.py
              safekit-mirror-windows-1-node2  vm instance
              safekit-mirror-windows-1-node2-externalip  address
          safekit-mirror-windows-1-synchro-waiter  config waiter
        ▾ safekit-mirror-windows-1-node1  vm-instance.py
              safekit-mirror-windows-1-node1  vm instance
              safekit-mirror-windows-1-node1-externalip  address
          safekit-mirror-windows-1-healthcheck  http health check
          safekit-mirror-windows-1-loadbalancer  target pool
          safekit-mirror-windows-1-forwarding  forwarding rule
```

SafeKit Mirror Cluster on Windows

Solution provided by Evidian

| | |
|---|---|
| URL for starting the SafeKit console | http://34.89.239.231:9010/deploy.html?firewallDialog=false |
| Virtual IP address of the SafeKit cluster | 34.89.229.183 |

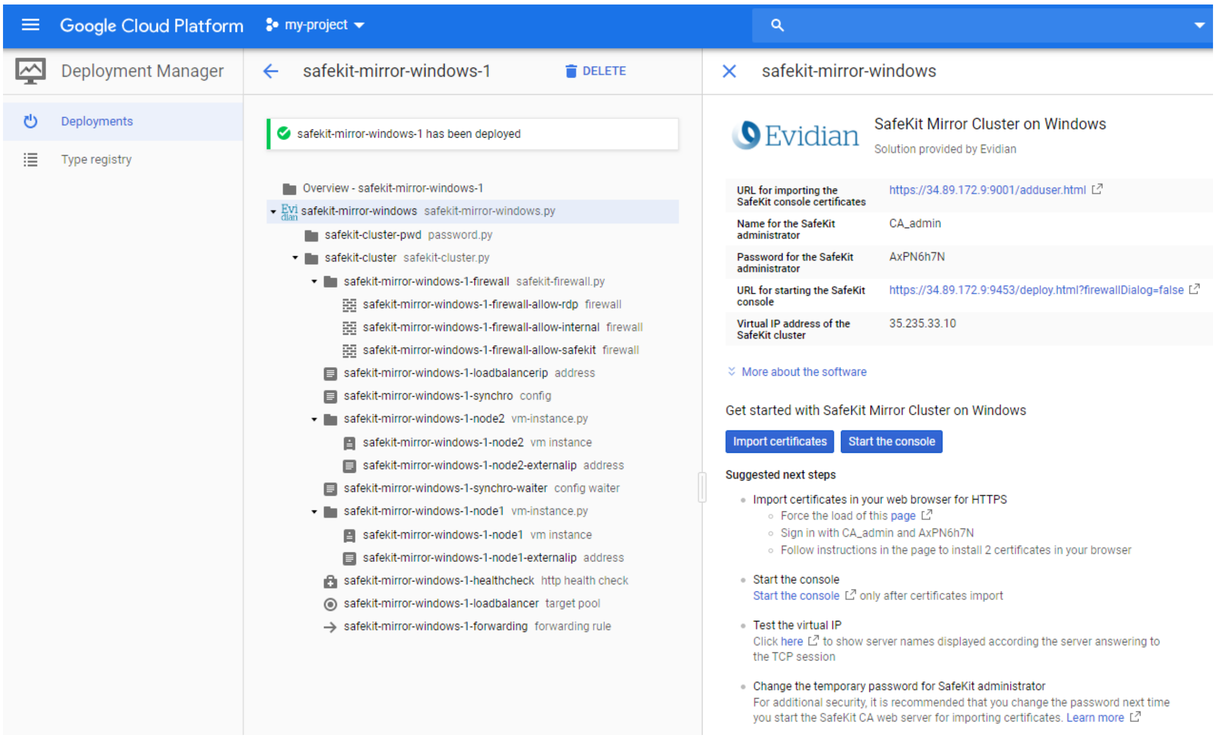
More about the software

Get started with SafeKit Mirror Cluster on Windows

Suggested next steps

- Test real-time replication
  - Start the console and note the state of nodes (PRIM or SECOND)
  - Connect, through RDP, to the instance with PRIM state. Go to the replicated directory c:\replicated and modify the content of the file rep.txt, then save it
  - Connect, through RDP, to the instance with SECOND state. Go to the replicated directory c:\replicated and note that the file rep.txt contains your changes
- Test the virtual IP
  Click here to show server names displayed according the server answering to the TCP session
- Secure the SafeKit console
  For additional security, it is recommended that you change the console access mode to HTTPS. Learn more

The image below is the output of the deployment when selecting HTTPS for the SafeKit console access mode.



safekit-mirror-windows-1 has been deployed

```
Overview - safekit-mirror-windows-1
safekit-mirror-windows  safekit-mirror-windows.py
    safekit-cluster-pwd  password.py
    safekit-cluster  safekit-cluster.py
        safekit-mirror-windows-1-firewall  safekit-firewall.py
            safekit-mirror-windows-1-firewall-allow-rdp  firewall
            safekit-mirror-windows-1-firewall-allow-internal  firewall
            safekit-mirror-windows-1-firewall-allow-safekit  firewall
        safekit-mirror-windows-1-loadbalancerip  address
        safekit-mirror-windows-1-synchro  config
        safekit-mirror-windows-1-node2  vm-instance.py
            safekit-mirror-windows-1-node2  vm instance
            safekit-mirror-windows-1-node2-externalip  address
        safekit-mirror-windows-1-synchro-waiter  config waiter
        safekit-mirror-windows-1-node1  vm-instance.py
            safekit-mirror-windows-1-node1  vm instance
            safekit-mirror-windows-1-node1-externalip  address
        safekit-mirror-windows-1-healthcheck  http health check
        safekit-mirror-windows-1-loadbalancer  target pool
        safekit-mirror-windows-1-forwarding  forwarding rule
```

SafeKit Mirror Cluster on Windows

Solution provided by Evidian

| | |
|---|---|
| URL for importing the SafeKit console certificates | https://34.89.172.9:9001/adduser.html |
| Name for the SafeKit administrator | CA_admin |
| Password for the SafeKit administrator | AxPN6h7N |
| URL for starting the SafeKit console | https://34.89.172.9:9453/deploy.html?firewallDialog=false |
| Virtual IP address of the SafeKit cluster | 35.235.33.10 |

More about the software

Get started with SafeKit Mirror Cluster on Windows

Suggested next steps

- Import certificates in your web browser for HTTPS
  - Force the load of this page
  - Sign in with CA_admin and AxPN6h7N
  - Follow instructions in the page to install 2 certificates in your browser
- Start the console
  Start the console only after certificates import
- Test the virtual IP
  Click here to show server names displayed according the server answering to the TCP session
- Change the temporary password for SafeKit administrator
  For additional security, it is recommended that you change the password next time you start the SafeKit CA web server for importing certificates. Learn more

At this point, the SafeKit cluster is ready to use and running.

If you have selected the HTTP mode for the console, you can start directly the SafeKit administration console as described in Start the Console page 19. With the console, you can configure, control and monitor the cluster.

In the HTTPS case, before starting the SafeKit console, you must first import certificates as described in Import Certificates in your Web Browser for HTTPS page 14. The SafeKit administrator name and password, required by this procedure, are displayed on this output page.

## 4.5 Import Certificates in your Web Browser for HTTPS

The SafeKit web console for administering the SafeKit cluster is secured with HTTPS and client certificates. You must import certificates in your web browser before starting the SafeKit web console as described below.

### 4.5.1 Load the Import Certificates Page

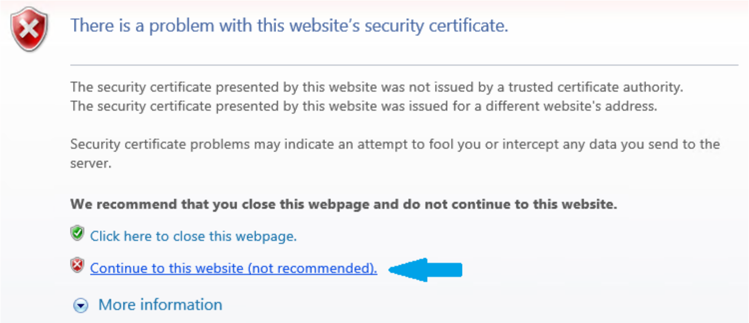
➩ Click on **Import certificates** button

Import certificates

Or

○ Force the load of this page

➩ When loading the page, the browser will display a security warning saying the certificate is invalid. This is expected, and you must click through the warning to continue.


There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

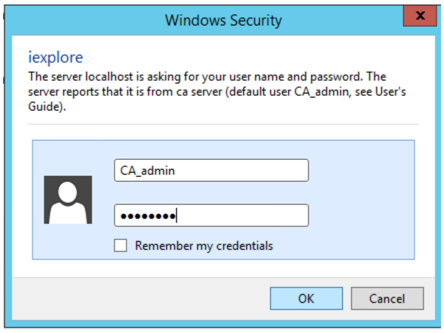
**We recommend that you close this webpage and do not continue to this website.**

Click here to close this webpage.

Continue to this website (not recommended).

More information

➩ At the login prompt, enter name and password for the SafeKit administrator


Windows Security

iexplore

The server localhost is asking for your user name and password. The server reports that it is from ca server (default user CA_admin, see User's Guide).

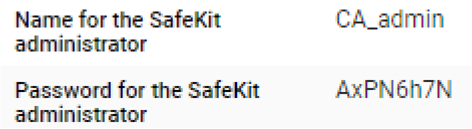
CA_admin

••••••••

□ Remember my credentials

OK Cancel

These values are displayed into the deployment output page. For instance:

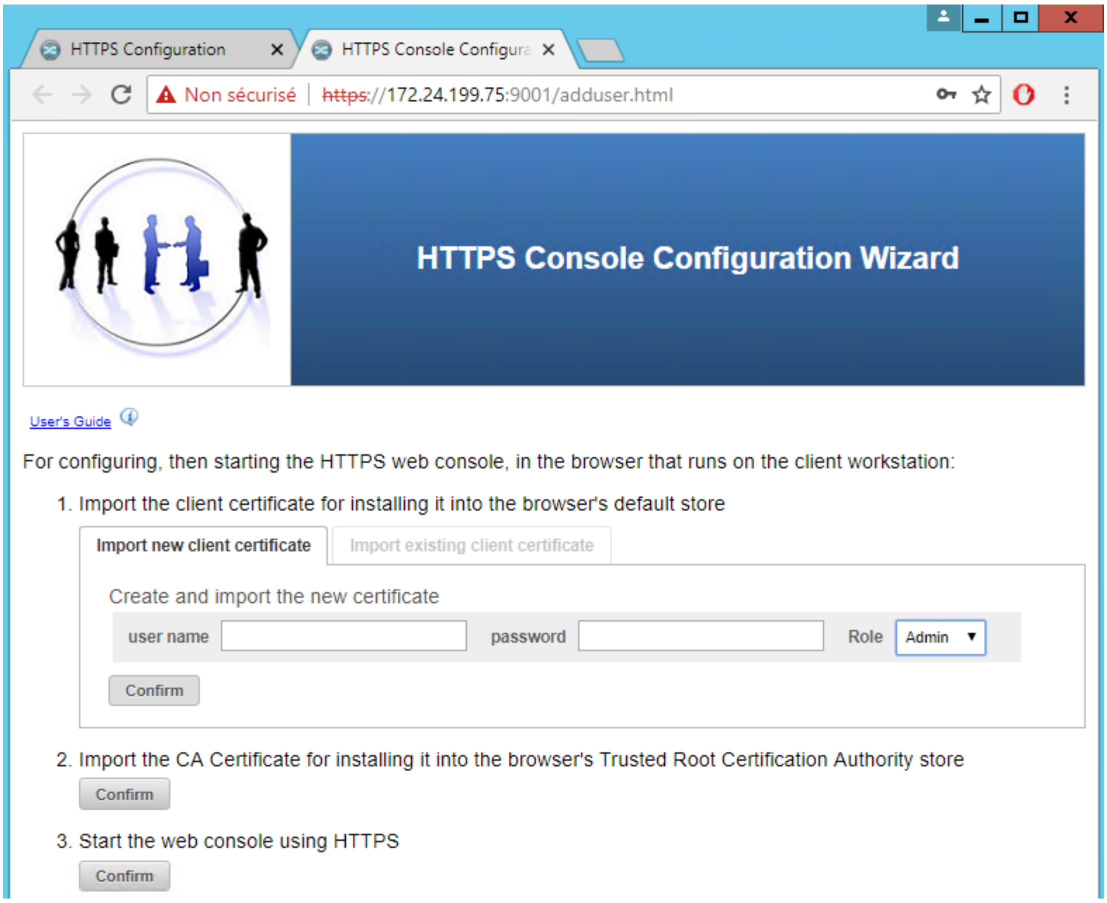


| | |
|---|---|
| Name for the SafeKit administrator | CA_admin |
| Password for the SafeKit administrator | AxPN6h7N |

Or

○ Sign in with CA_admin and AxPN6h7N

➩ It opens the following page



HTTPS Configuration
HTTPS Console Configura
Non sécurisé
https://172.24.199.75:9001/adduser.html
HTTPS Console Configuration Wizard
User's Guide

For configuring, then starting the HTTPS web console, in the browser that runs on the client workstation:

1. Import the client certificate for installing it into the browser's default store

   Import new client certificate | Import existing client certificate

   Create and import the new certificate

   user name | password | Role Admin

   Confirm

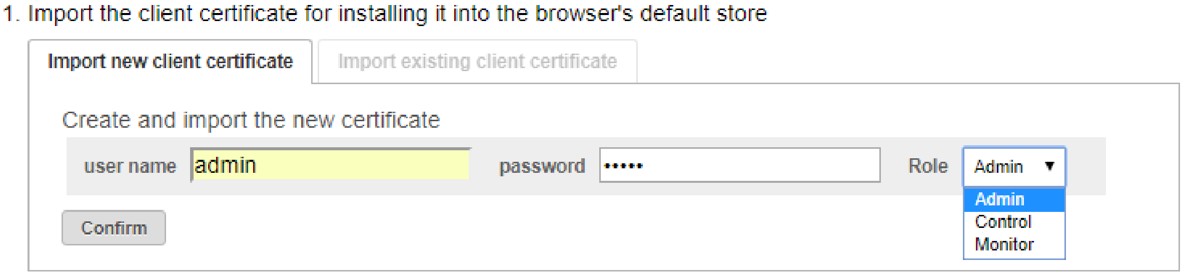
2. Import the CA Certificate for installing it into the browser's Trusted Root Certification Authority store

   Confirm

3. Start the web console using HTTPS

   Confirm

### 4.5.2 Create a New Client Certificate



1. Import the client certificate for installing it into the browser's default store

   Import new client certificate | Import existing client certificate

   Create and import the new certificate

   user name: admin | password: ••••• | Role: Admin

➩ Fill in the "user name", "password". Please note that the user name must be unique. Select the Admin role for granting all administration privileges.

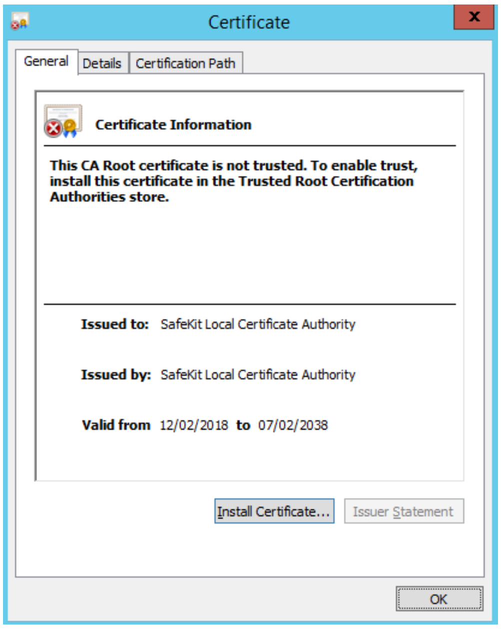
➩ Click on "Confirm"

➩ After the form is processed, the resulting client certificate (the `user_Admin_administrator.p12` file) is downloaded

### 4.5.3 Import the Client Certificate

The procedure depends on the browser and the operating system used. The following describes the installation in Windows with Internet Explorer.

- ➾ Click on the downloaded `.p12` file (for instance `user_Admin_administrator.p12)` for opening the certificate window. Then click on "Install Certificate" button.



Certificate

General | Details | Certification Path

Certificate Information

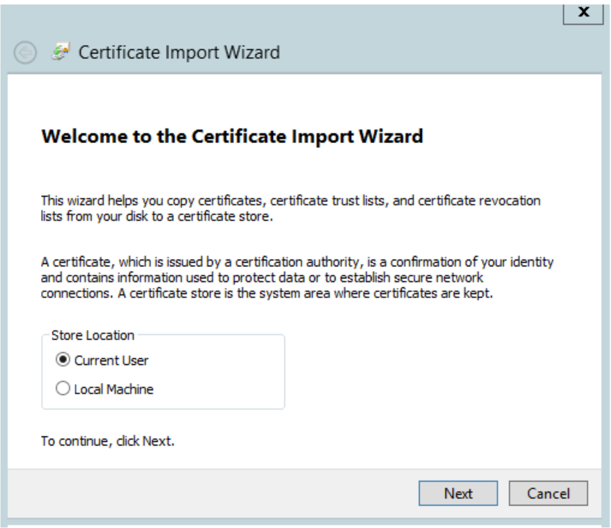
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: SafeKit Local Certificate Authority

Issued by: SafeKit Local Certificate Authority

Valid from 12/02/2018 to 07/02/2038

- ➾ It opens the Certificate Import Wizard. Select "Current User" and click on the "Next" button. Go on until the wizard requires the password that protects the certificate.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

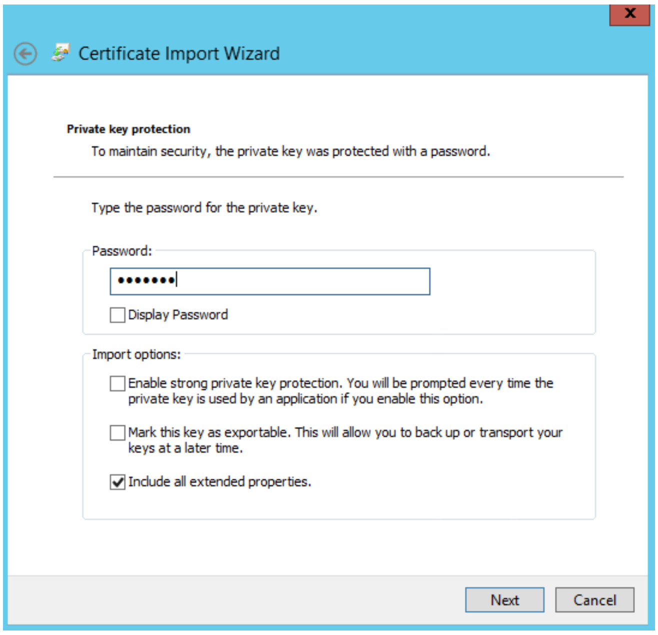
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
● Current User
○ Local Machine

To continue, click Next.

- ➩ Enter the password when required. The password to use is the one set during client certificate creation



Certificate Import Wizard

**Private key protection**

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password: •••••••

□ Display Password

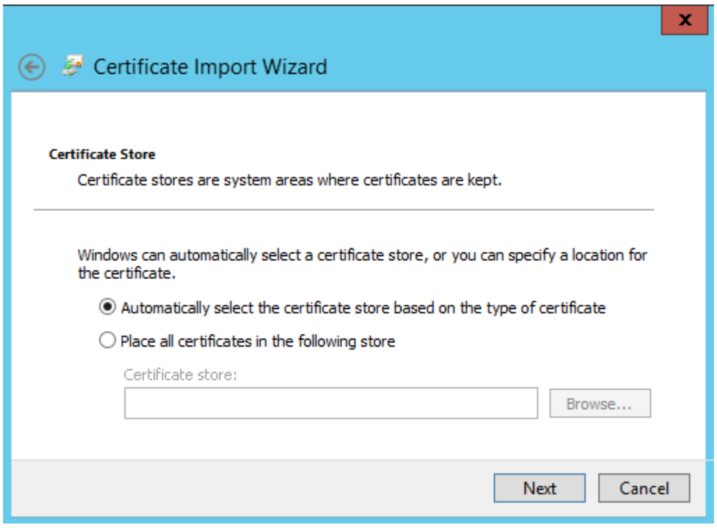
Import options:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

- ➩ Let the wizard automatically select the certificate store that is the Personal store.



Certificate Import Wizard

**Certificate Store**

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

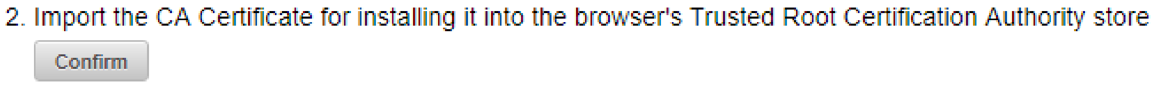
Certificate store:

- ➩ Then complete the certificate import.

### 4.5.4 Import the CA Certificate as Trusted Root Certification Authority

Note

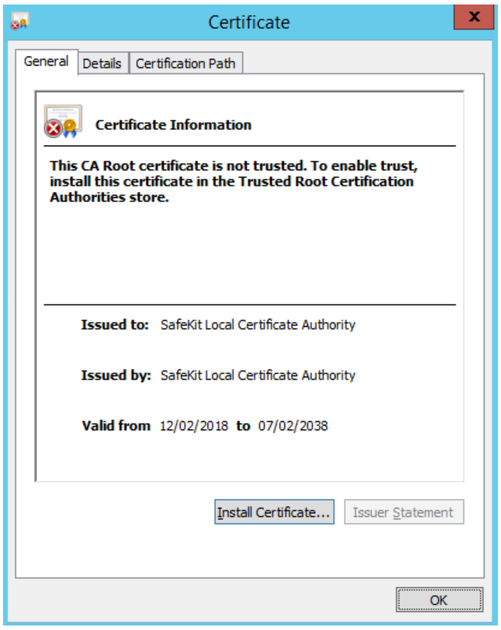
The browser will issue security warnings when you connect to the SafeKit web console unless you install this certificate.



2. Import the CA Certificate for installing it into the browser's Trusted Root Certification Authority store

The procedure depends on the browser and the operating system used. The following describes the installation in Windows with Internet Explorer.

- Click on the downloaded `cacert.crt` file for opening the certificate window. Then click on "Install Certificate" button



Certificate

Certificate Information

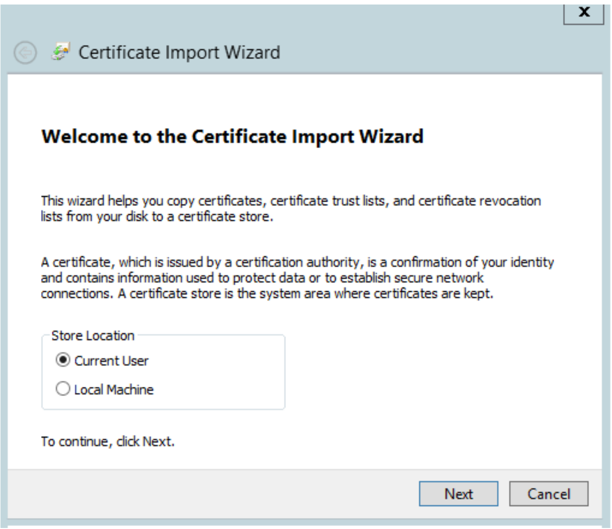
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: SafeKit Local Certificate Authority

Issued by: SafeKit Local Certificate Authority

Valid from 12/02/2018 to 07/02/2038

- It opens the Certificate Import Wizard. Select "Current User" and click on the "Next" button



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

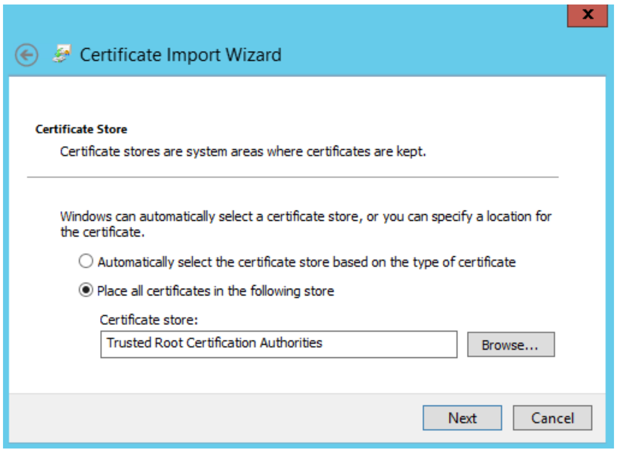
Store Location

● Current User

○ Local Machine

To continue, click Next.

- ➩ Browse stores to select the "Trusted Root Certification Authorities" store. Then click on "Next" button



Certificate Import Wizard

**Certificate Store**

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

- ➩ Then complete the certificate import.

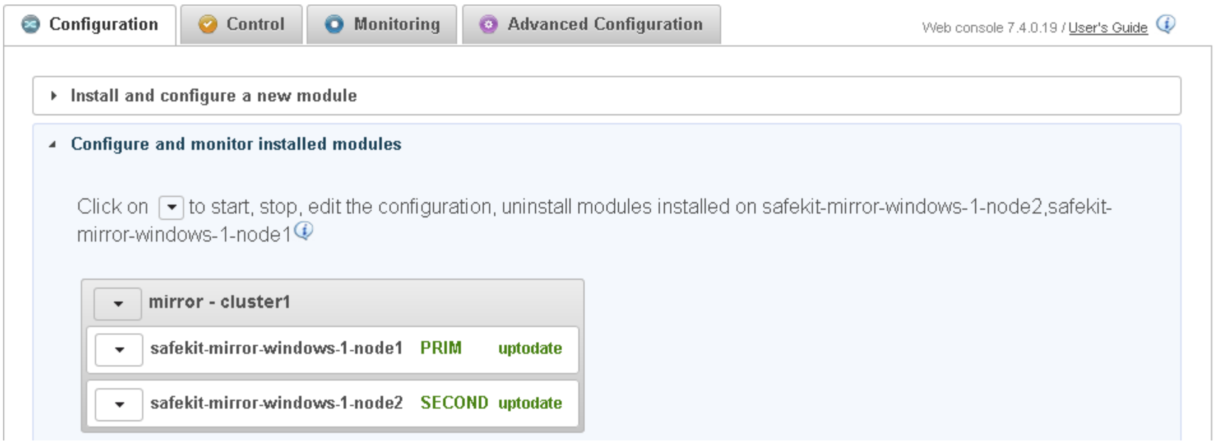
## 4.6 Start the Console

- ➩ Click on

Or

- Start the console
  Start the console only after certificates import

- ➩ It shows the SafeKit cluster state. Green states show that the SafeKit cluster is operational.


Configuration
Control
Monitoring
Advanced Configuration
Web console 7.4.0.19 / User's Guide
Install and configure a new module
Configure and monitor installed modules

Click on ▾ to start, stop, edit the configuration, uninstall modules installed on safekit-mirror-windows-1-node2,safekit-mirror-windows-1-node1

| mirror - cluster1 | | |
|---|---|---|
| safekit-mirror-windows-1-node1 | PRIM | uptodate |
| safekit-mirror-windows-1-node2 | SECOND | uptodate |

With the SafeKit web console, you can configure, control and monitor the SafeKit cluster. See the SafeKit User's Guide for details.

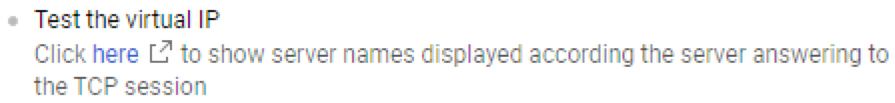
## 4.7 Test the Virtual IP

The SafeKit solution configures an external IP address with GCP load-balancer for providing a virtual IP address to access the SafeKit cluster.

In a SafeKit mirror solution, the virtual IP permits to connect users only to the primary node. In a SafeKit farm solution, the virtual IP permits to load balance TCP sessions between the 2 nodes.

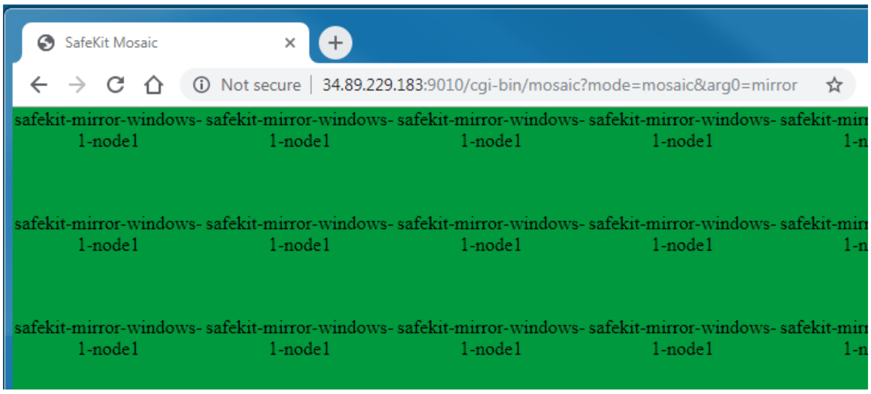
By default, the virtual IP forwarding rules are set according SafeKit console access mode: port TCP/9010 (when HTTP) or TCP/9453 (when HTTPS). This permits to test the virtual IP by loading a web page. You can change forwarding rules according your needs.

➩ Click on the link, displayed into the deployment output page, for testing the virtual IP



- Test the virtual IP
  Click here to show server names displayed according the server answering to the TCP session

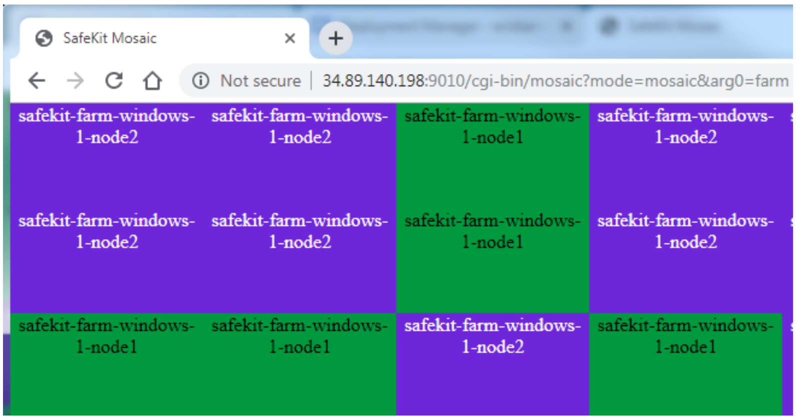
In a SafeKit mirror solution, the link displays a page where all connections go to the primary node:



Not secure | 34.89.229.183:9010/cgi-bin/mosaic?mode=mosaic&arg0=mirror

| | | | | |
|---|---|---|---|---|
| safekit-mirror-windows-1-node1 | safekit-mirror-windows-1-node1 | safekit-mirror-windows-1-node1 | safekit-mirror-windows-1-node1 | safekit-mirr 1-n |
| safekit-mirror-windows-1-node1 | safekit-mirror-windows-1-node1 | safekit-mirror-windows-1-node1 | safekit-mirror-windows-1-node1 | safekit-mirr 1-n |
| safekit-mirror-windows-1-node1 | safekit-mirror-windows-1-node1 | safekit-mirror-windows-1-node1 | safekit-mirror-windows-1-node1 | safekit-mirr 1-n |

In a SafeKit farm solution, the link displays a page where connections are load-balanced between the 2 nodes:



Not secure | 34.89.140.198:9010/cgi-bin/mosaic?mode=mosaic&arg0=farm

| | | | | |
|---|---|---|---|---|
| safekit-farm-windows-1-node2 | safekit-farm-windows-1-node2 | safekit-farm-windows-1-node1 | safekit-farm-windows-1-node2 | s |
| safekit-farm-windows-1-node2 | safekit-farm-windows-1-node2 | safekit-farm-windows-1-node1 | safekit-farm-windows-1-node2 | s |
| safekit-farm-windows-1-node1 | safekit-farm-windows-1-node1 | safekit-farm-windows-1-node2 | safekit-farm-windows-1-node1 | s |

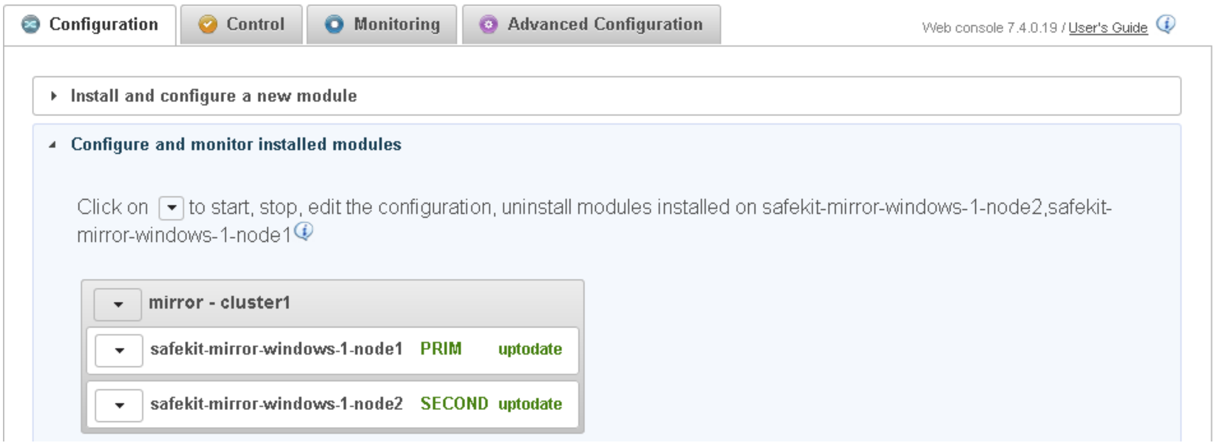
## 4.8 Test the Real-Time Replication in a Mirror Cluster

In SafeKit mirror solutions, the real-time file replication is automatically configured for replicating the directory:

- In Windows, c:\replicated
- In Linux, /var/replicated

This permits to test the real-time replication:

- Start the SafeKit console as described in Start the Console page 19



Install and configure a new module

Configure and monitor installed modules

Click on ▾ to start, stop, edit the configuration, uninstall modules installed on safekit-mirror-windows-1-node2,safekit-mirror-windows-1-node1

mirror - cluster1

| | | |
|---|---|---|
| safekit-mirror-windows-1-node1 | PRIM | uptodate |
| safekit-mirror-windows-1-node2 | SECOND | uptodate |

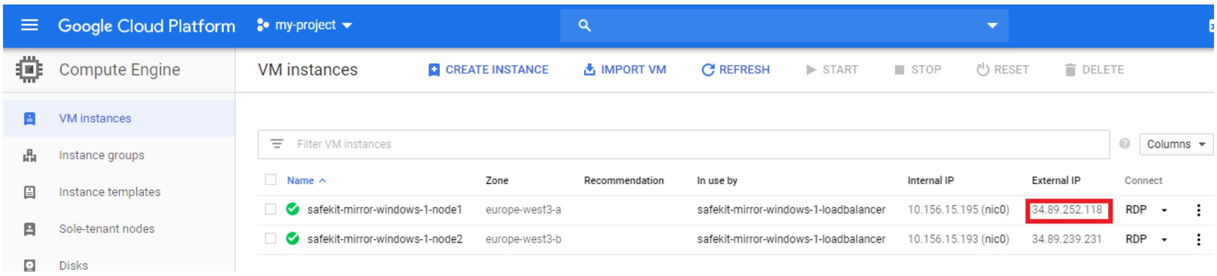
- Connect to the 2 SafeKit instances as described in Connect through RDP or SSH to the SafeKit Cluster Nodes page 22
- On the instance with PRIM state, go to the replicated directory and modify the content of the file rep.txt; then save it
- On the instance with SECOND state, go to the replicated directory and note that the file rep.txt contains your changes

## 4.9 Connect through RDP or SSH to the SafeKit Cluster Nodes

The SafeKit solution creates 2 VMs instances that run Windows or CentOS. Instances have public external IP addresses and firewall rules has been configured to allow TCP traffic to Remote Desktop port 3389 for Windows or SSH port 22 for Linux. This permits to use the standard GCP procedures for connecting to the SafeKit instances.

### 4.9.1 Connecting to Windows Instance

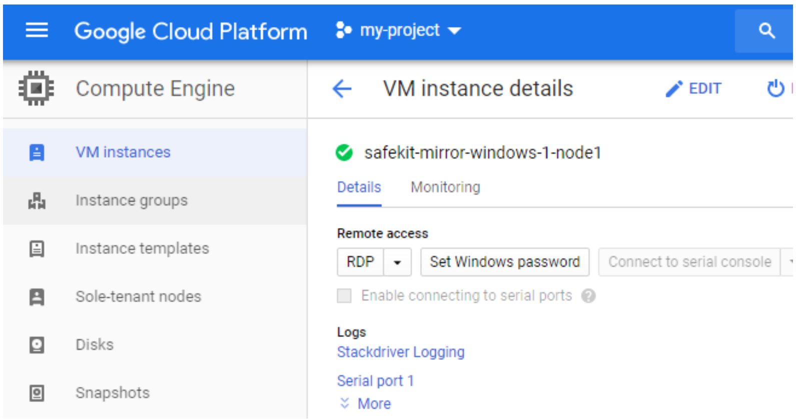
➩ Go to the VM instances page



| Name | Zone | Recommendation | In use by | Internal IP | External IP | Connect |
|---|---|---|---|---|---|---|
| safekit-mirror-windows-1-node1 | europe-west3-a | | safekit-mirror-windows-1-loadbalancer | 10.156.15.195 (nic0) | 34.89.252.118 | RDP |
| safekit-mirror-windows-1-node2 | europe-west3-b | | safekit-mirror-windows-1-loadbalancer | 10.156.15.193 (nic0) | 34.89.239.231 | RDP |

➩ Note the instance external IP address

➩ Click on the instance



safekit-mirror-windows-1-node1

Remote access

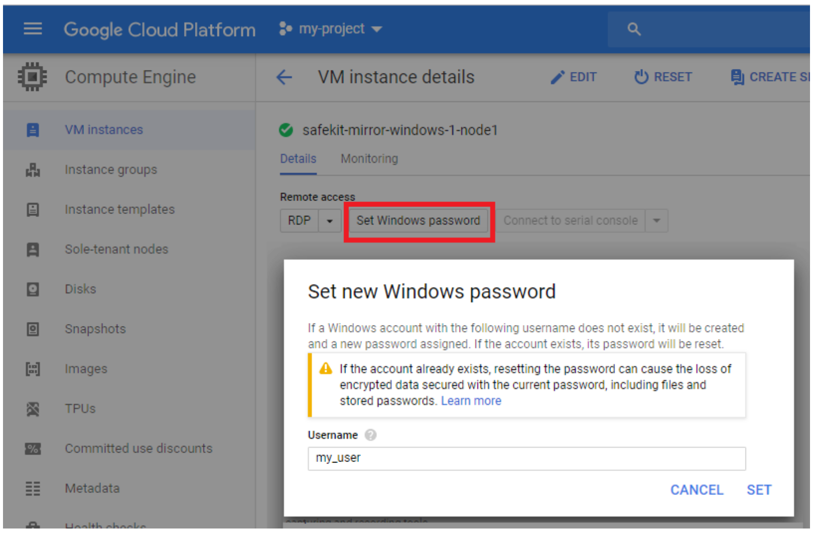
□ Enable connecting to serial ports

Logs

Stackdriver Logging

Serial port 1

➩ The connection mode is via Remote Desktop. Before you connect, you must create a Windows instance password by clicking on **Set Windows password** button and setting the user name.



Set new Windows password

If a Windows account with the following username does not exist, it will be created and a new password assigned. If the account exists, its password will be reset.

If the account already exists, resetting the password can cause the loss of encrypted data secured with the current password, including files and stored passwords. Learn more

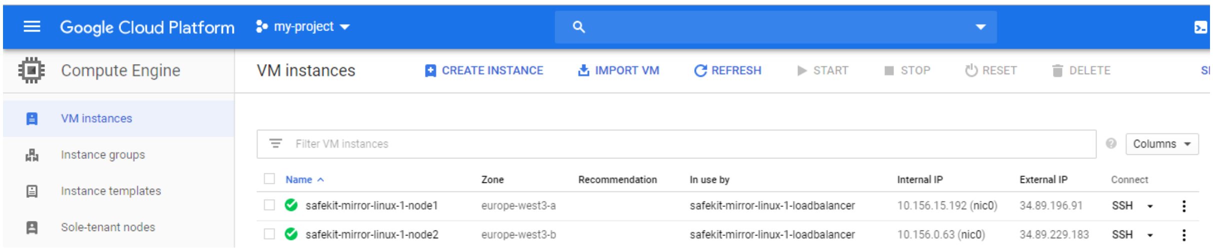
Username: my_user

It returns the password value that must be used for connecting with the remote desktop.

Refer to Connecting to Windows instances for more details.

### 4.9.2 Connecting to Linux Instance

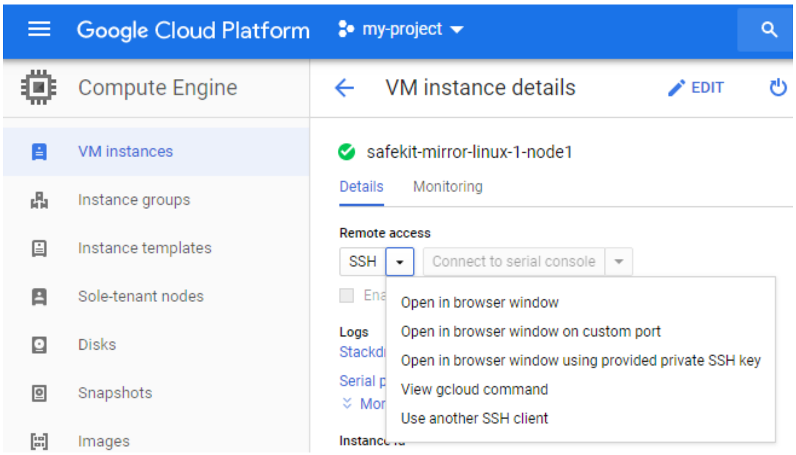
➾ Go to the VM instances page



| Name | Zone | Recommendation | In use by | Internal IP | External IP | Connect |
|---|---|---|---|---|---|---|
| safekit-mirror-linux-1-node1 | europe-west3-a | | safekit-mirror-linux-1-loadbalancer | 10.156.15.192 (nic0) | 34.89.196.91 | SSH |
| safekit-mirror-linux-1-node2 | europe-west3-b | | safekit-mirror-linux-1-loadbalancer | 10.156.0.63 (nic0) | 34.89.229.183 | SSH |

➾ Click on the instance you want to connect to

➾ Select the ssh connection mode

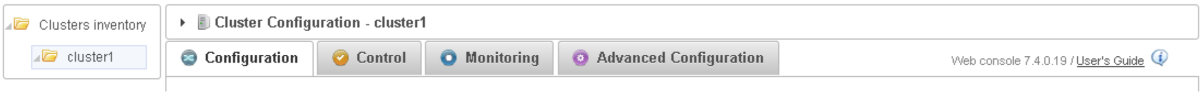


Refer to Connecting to Linux instances for more details

## 4.10 Access the Open Source Licenses for SafeKit

SafeKit includes open source software. The text of the open source licenses is provided in Third-Party Software section of the SafeKit User's Guide. To access this guide included with the SafeKit VM instance:

- ➩ either, start the SafeKit console, as described in in Start the Console page 19, then click on the User's Guide link to open the SafeKit User's Guide and read the section on third party software



- ➩ or connect to the instance, as described in Connect through RDP or SSH to the SafeKit Cluster Nodes page 22, and read license files:
  - in Windows, license files are in c:\safekit\licenses
  - in Linux, license files are in /opt/safekit/licenses