Sponge.

Kaspersky Cloudshare / Spark integration PoC

Introduction

A short Proof of Concept (PoC) has been completed to evaluate the work required to integrate Spark and Cloudshare.

Cloudshare is a company that provides Virtual Machines (VMs) for learners. VMs can be configured and then provisioned for learners which they can use to complete courses.

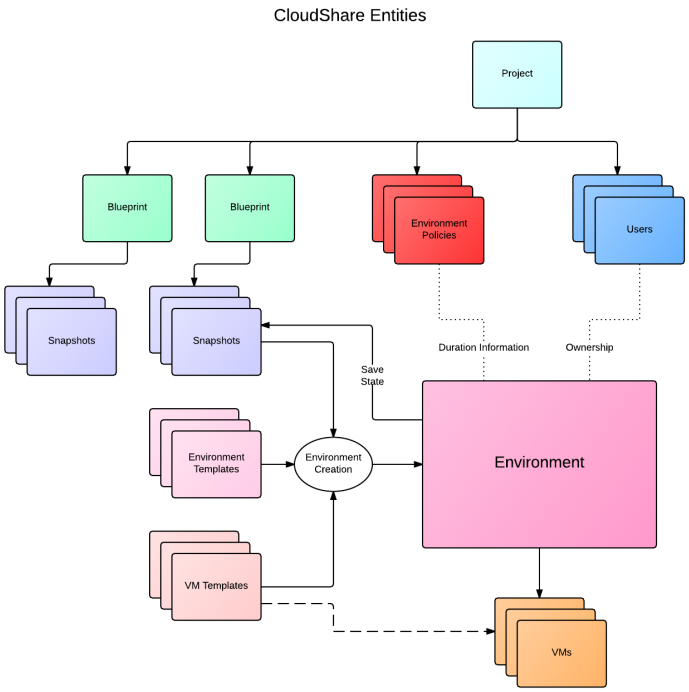
Kaspersky are delivering an eLearning module which will be hosted on the Spark platform to train learners in the analysis of malware. To do this the learner needs to have access to a virtual machine that has been pre-loaded with malware to analyse as well as the software to complete that analysis. This PoC does not cover the process of malware analysis or the software involved in that process.

Proof of Concept Work

Cloudshare provide an API which allows authenticated access to their system. The API can be used to register and provision VMs to users.

The VM itself, and the software that is needed for the course can be created and uploaded using the Cloudshare interface. The creation process would be completed manually. Although it could be automated the work required to automate the process is likely to be far more than using the existing Cloudshare interface.

Base 'blueprints' can be created from Cloudshares library, software can be uploaded to the VM and a 'snapshot' is taken. The snapshot is the base for the VM that learners create:



A class must be created on Cloudshare, this can be done programmatically using the API or manually using the interface. In conversation with Cloudshare the limit on 'Self Paced' classes is 500 students so managing students should not be necessary programmatically but has been demonstrated as part of the PoC work. It is proposed that creating a class is done using the Cloudshare interface.

The VM is created within the constraints of the Cloudshare platform. Policies can be attached in the interface that limit the users to the required 6 month access with 100 hours of run time. The time left is displayed on the user interface

The learner can reset the virtual machine using the button provided on the interface (see later) to its initial state should they make a mistake.

Network connections to the internet can be allowed or disabled, there is no provision in Cloudshare to restrict outbound connections to specific CIDR ranges unless using software running on the VM. Kaspersky require that all outbound connections are prohibited to ensure malware cannot spread.

Once a class has been created on Cloudshare, Spark would need to use credentials to call to the Cloudshare API, passing:

- Class ID (this will be the same for all students on the course, class ID is the same for all students)
- First name
- Last name
- Email address

(see appendix for API Sequence diagram)

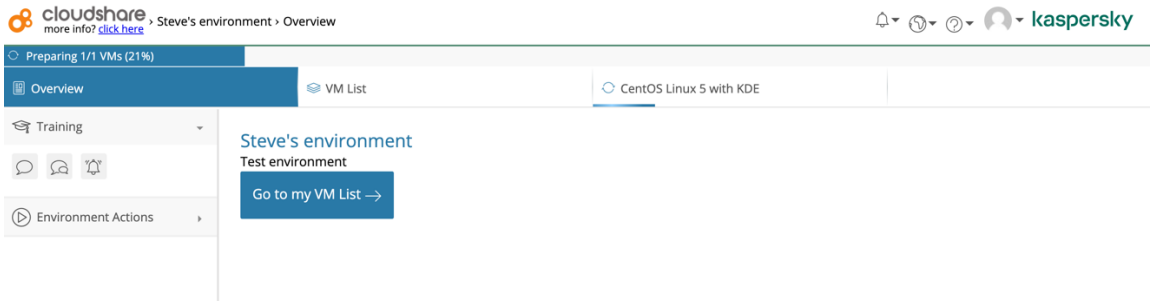
This returns a link that should be displayed to the user on the spark interface (to be determined where) so that they can click through into Cloudshare.

Users do not need to be added to the class in advance, a 'sponsored link' can be generated. This avoids a student needing a username and password. The user than can interact with their VM using the Cloudshare web interface.

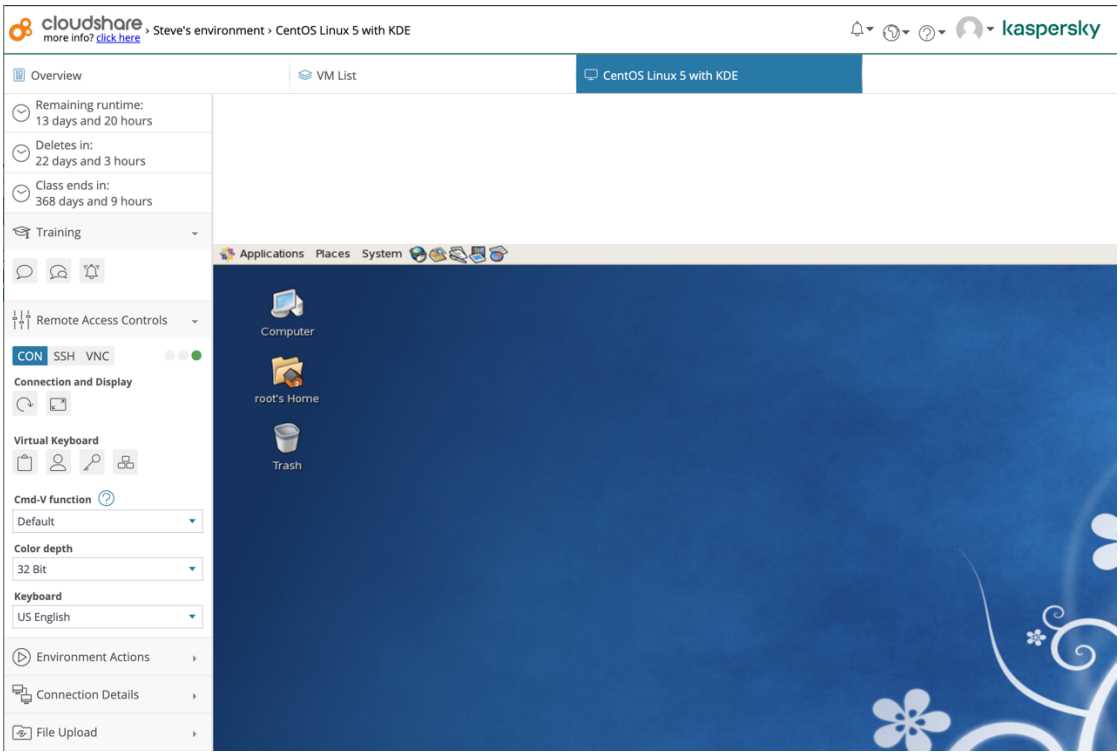
Proposed Solution

Based on the results of the PoC a URL could be provided to the user through the Spark interface.

1. The user clicks the link, launching a browser tab that would take them to the Cloudshare interface:



2. The learner clicks the blue button, opening their VM (image does not show the VM that would be used in production):



3. The learner is now logged into their VM where they can follow the instructions provided in the eLearning module.

On the left of the screen is a side bar menu provided by the Cloudshare interface, features pertinent to the solution are highlighted in the appendix.

Scope of integration

It is understood that the underlying operating system is managed by Cloudshare and updates are applied as per Cloudshare's existing practice.

IDA Pro has licensing requirements, these have not been investigated as part of the PoC, Cloudshare have experience of the licensing software used by IDA Pro and believe that they have a solution.

As discussed with Cloudshare and Kaspersky we may with the 'help' link to be hidden on the Cloudshare interface or for clear instructions in the eLearning module for how learners should ask for help.

Unlike phase 1 the connection to the VM is made through a web interface and not through an RDP client.

The integration is limited to the generation of a sponsored link per student and the display of that link through the Spark interface.

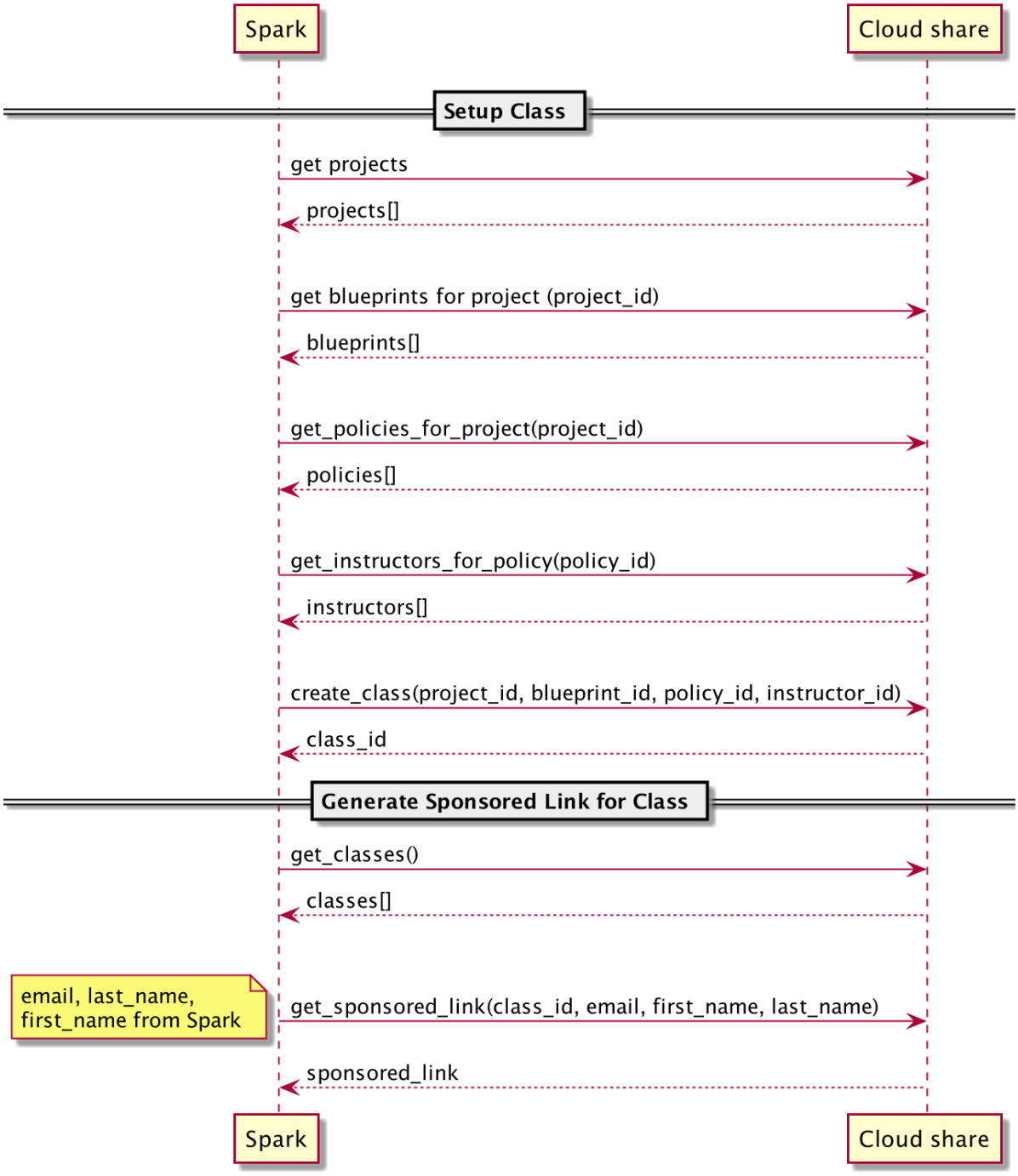
Integration Cost

To follow

Sponge.

Appendix

API Sequence diagram



Sponge.

Cloudshare user interface side bar