## Agenda for Second Meeting

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| **Skyward Federal**  **COPS Platform** | | **1/23/2019**  **1:00 PM to 1:45 PM**  **NCSU – EB2-2253** | | |
|  | | | | |
|  | | | | |
| Type of meeting: | Project Requirements and Design | Note Taker:  Facilitator: | Spencer Yoder  Jonathan Balliet | |
|  | | | | |
|  | | | | |
| Invitees: | Jonathan Balliet, Jeen Shaji, Daniel Mills, Caleb Boswell, Spencer Yoder, Erin Kotlyn, Danny Caudill, Ryan Carr | | | |
| Please read:  Meeting info: | Questions Below  [meet.google.com/jxn-hjjm-svb](https://meet.google.com/jxn-hjjm-svb) | | | |
| **Agenda** | | | | |
|  | | | | |
| Agenda Overview | | All | | 5 min |
| Discuss Questions | | All | | 25 min. |
| Present Requirements (if time) | | All | | 10 min. |
| Action Items & Next Meeting | | All | | 5 min. |
|  | | | | |
| **Additional Information** | | | | |
|  | | | | |
| Resource persons: | Dr. Jason King, Ms. Margaret Heil, Mr. Richard Kaufman, Erin Kotlyn, Danny Caudill, Ryan Carr | | | |

**COPS Platform Questions**

**Requirements Clarification**

<https://docs.google.com/document/d/1Ccvz7wOBsk3VC3LaWDXpd4Er7gSOqWrZgNiQ8tX9rDc/edit?usp=sharing>

1. What sort of reports are we writing to return to the client on the data? - Spencer

**Access**

1. When can we expect to have access to Jira and Confluence? - Jeen
2. When can we expect to have access to Skyward’s Gitlab? - Jonathan
3. How can we access the VPN so we can use the sandbox environment? - Daniel

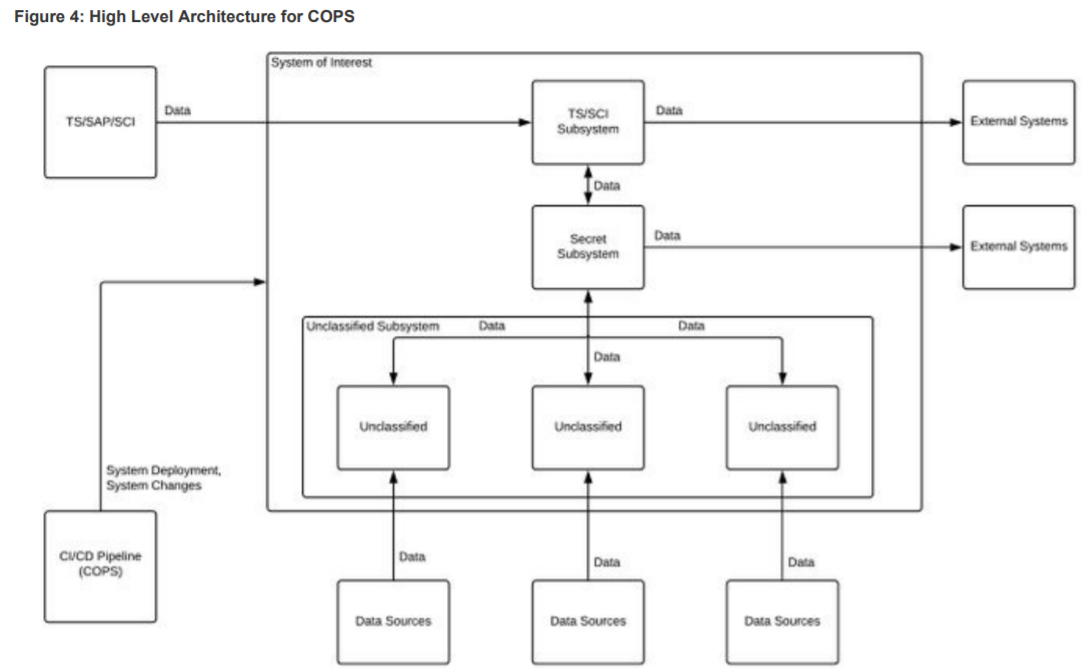
**Documentation**

1. We have a lot of information handed to us and we need to document this for our class. Is there a preference about how we format requirements & design? - Jeen

**Platform Controller**

1. There are 2 parts: REST requests and Data API. Does this mean we check user authentication/ authorization twice? - Jeen
2. Can you elaborate on what “zuul” is and how do we incorporate this? - Jeen
3. Can you elaborate on the necessity to “mirror build dependencies locally”? - Jeen

**COPs Overview**:

1. Figure 4: Can you explain this diagram in more detail?
   1. 
2. What do we do with logs if they fail to forward? - Caleb
3. Can you explain what you mean by a “Service” in Figure 2 ( Flow through the COPS Platform Subsystem ). - Jonathan

**Container Runtime** ( Docker Container/Firecracker )

1. Are we correct in saying we’re responsible for creating a backend application that handles REST requests/responses inside the Container Runtime? - Jonathan
2. If so, are there are any restrictions on how this is handled? For example, what languages/technologies we can use for implementing this? - Jonathan
3. Are the REST requests sent directly from the “external consumer” to the Container Runtime once this consumer has been authenticated and given their level of authorization? Or, does the Platform Container act as a “middle-man” that forwards the requests and responses between the Container Runtime and this consumer? - Jonathan
4. Does the consumer ever need to re-authorize when requesting services? Or is only the initial authentication and authorization of this consumer required for a session? - Jonathan
5. It’s mentioned that both the Data Storage and Container Runtime will be on the same CentOs 7 host. Will we be using an EC2 instance for doing this on AWS? - Jonathan
6. Are we using both Docker Container and Firecracker? Do they work together? - Jonathan
7. What do you want to do with Firecracker? - Caleb

**IdAM (KeyCloak)**

1. How exactly will   
   the IdAM system  
   isolate data? - Spencer
2. Will users have associated SE Linux labels which signify what they can access? -Spencer
3. What is our level of responsibility for the log aggregator? - Spencer
4. What logs does the IdAM send out? - Spencer
5. Will install/config be automated from some script lying around? Or will it be done through another part of the system? - Spencer

**Data Storage (Postgres w/ SE Linux)**

1. Are the users the ones responsible for creating labels for the data? - Caleb
2. Would users only be allowed to classify labels up to their own clearance level? - Caleb
3. Should users with higher privilege be able to edit the labels made by users with lower classification. - Caleb
4. The documentation mentions that each service running inside the container runtime will have a different account. Will these accounts be generated every time a container is spun up? How will the username and password be determined, since PostgreSQL can’t interact with Keycloak?

**Second Sponsor Meeting Minutes**

**Team**: Skyward Federal – MLS API Part 1 **Date**: January 23, 2020

**Facilitator**: Jonathan Balliet **Recorder**: Spencer Yoder

**Attendance**:

* Spencer Yoder
* Jeen Shaji
* Jonathan Balliet
* Daniel Mills
* Caleb Boswell
* Dr. Jason King
* Ms. Margaret Heil
* Erin Kotlyn
* Danny Caudill
* Matthew Peters

**Minutes:**

**Requirements Clarification**

<https://docs.google.com/document/d/1Ccvz7wOBsk3VC3LaWDXpd4Er7gSOqWrZgNiQ8tX9rDc/edit?usp=sharing>

1. What sort of reports are we writing to return to the client on the data? - Spencer
   1. **That depends on what we decide to use this thing for (push to the backburner)**
   2. **We need to talk about the scope**
      1. **We can talk about are bare minimum and stretch goals**
   3. **We need to get through questions first before we can decide scope**

**Access**

1. When can we expect to have access to Jira and Confluence? - Jeen
   1. **An environment is being built but they need to set up a seperate one without sensitive information. This also limits the scope. This answer applies to the next question. This week maybe. Definitely by next Thursday.**
   2. **They’re setting up AWS**
   3. **We need to use MFA to use our AWS. They will send us a link for that.**
2. When can we expect to have access to Skyward’s Gitlab? - Jonathan
   1. **See previous answer**
3. How can we access the VPN so we can use the sandbox environment? - Daniel
   1. **It might be set up a little differently (through AWS). The AWS solution would limit a set of IPs instead of setting up a whole VPN**
   2. **This new solution isn’t that different from how it would have been done initially.**

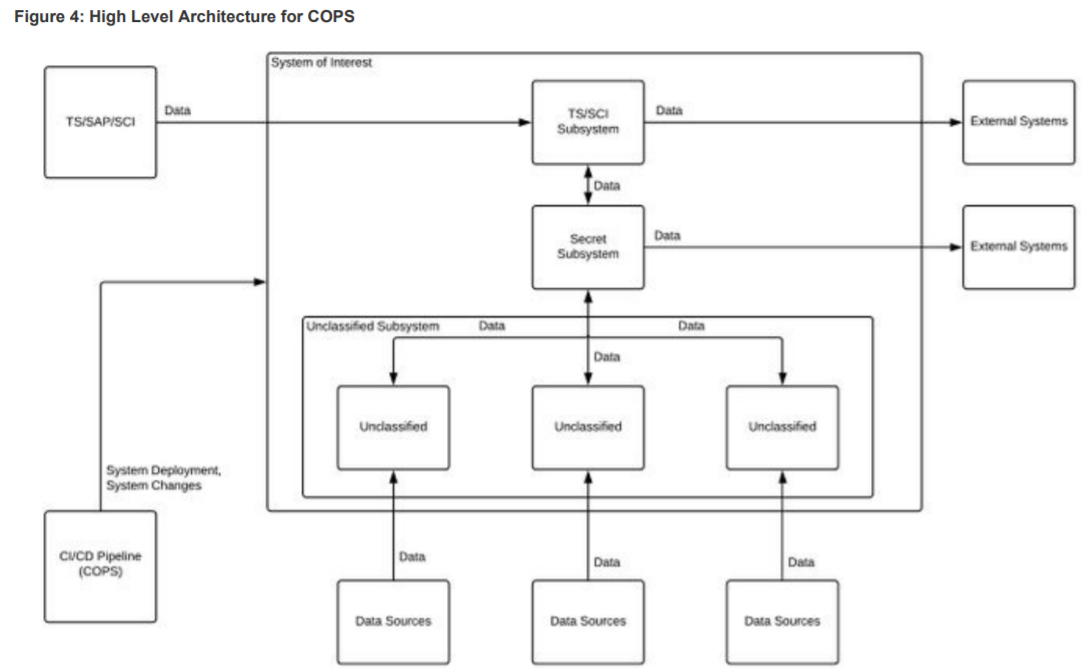
**Documentation**

1. We have a lot of information handed to us and we need to document this for our class. Is there a preference about how we format requirements & design? - Jeen
   1. **Not really. The formats we use for class will be find. Skyward doesn’t have standard documentation yet.**
   2. **Shall statements.**

**Platform Controller**

1. There are 2 parts: REST requests and Data API. Does this mean we check user authentication/ authorization twice? - Jeen
2. Can you elaborate on what “zuul” is and how do we incorporate this? - Jeen
   1. **Java library created by Netflix to serve as a flexible API gateway**
   2. **External device connects to the gateway, the gateway validates it and connects it to a backend server. Maintains connections even if backend containers aren’t running. It’s our container manager.**
   3. **We still have to implement inbound and outbound filters. It’s just a library.**
   4. **Doing everything except for this gateway could be an initial goal. This would be a stretch goal.**
   5. **IdAM is also a potential stretch goal. We can just set up the containers and some users.**
3. Can you elaborate on the necessity to “mirror build dependencies locally”? - Jeen
   1. **Build tools are given a config file which allow them to download dependencies.**
   2. **So we can have an artifact repository along with our source code repo. The jar files and stuff can live there. Another solution (if small dependencies) is to push these jar files into the source code repo.**

**COPs Overview**:

1. Figure 4: Can you explain this diagram in more detail?
   1. 
2. What do we do with logs if they fail to forward? - Caleb
   1. **They would be stored locally. We would have to define a retention policy. We need to develop the answer to this question together.**
   2. **Another issue is how to alert people if the network is down.**
   3. **Would the alert be an email?**
      1. **It could be an instant response process. It depends in the tools you’re using.**
3. Can you explain what you mean by a “Service” in Figure 2 ( Flow through the COPS Platform Subsystem ). - Jonathan
   1. **Jonathan understands.**
   2. **A service is a way to create value between a consumer and a producer**

**Container Runtime** ( Docker Container/Firecracker )

1. Are we correct in saying we’re responsible for creating a backend application that handles REST requests/responses inside the Container Runtime? - Jonathan
   1. **Some web service would do it for us. We would find one that could talk to Postgres. Also answers the next question.**
   2. **Once the consumer is authorized, the container is created based on their access list. Does the REST request get sent directly to the container or is it handled by the platform controller?**
      1. **The answer is it depends. In Zuul, clients connect to the gateway even if the backend isn’t running and traffic flows through the gateway. The backend can crash while the gateway is still runnning**
2. If so, are there are any restrictions on how this is handled? For example, what languages/technologies we can use for implementing this? - Jonathan
3. Are the REST requests sent directly from the “external consumer” to the Container Runtime once this consumer has been authenticated and given their level of authorization? Or, does the Platform Container act as a “middle-man” that forwards the requests and responses between the Container Runtime and this consumer? - Jonathan
4. Does the consumer ever need to re-authorize when requesting services? Or is only the initial authentication and authorization of this consumer required for a session? - Jonathan
5. It’s mentioned that both the Data Storage and Container Runtime will be on the same CentOs 7 host. Will we be using an EC2 instance for doing this on AWS? - Jonathan
6. Are we using both Docker Container and Firecracker? Do they work together? - Jonathan
   1. **We should just focus on Docker. Firecracker would run independently, but we won’t be using them.**
7. What do you want to do with Firecracker? - Caleb

**IdAM (KeyCloak)**

1. How exactly will   
   the IdAM system  
   isolate data? - Spencer
   1. **When a user makes a web request, the API gateway has no connection. “I am” gets the credentials through an encrypted channel.**
   2. **Attributes and groups are used to query databases all over industry.**
2. Will users have associated SE Linux labels which signify what they can access? -Spencer
   1. **This depends on our implementation. It depends on how we decide to label users.**
   2. **Danny will send a link. The page is called MLS statements. It deals with security levels and categories.**
   3. **In our requirements, we should talk about security levels and categories and not “clearance levels”**
   4. **SE Linux has 16 levels. What about arbitrary numbers?**
      1. **Categories expand the levels into bigger numbers.**
3. What is our level of responsibility for the log aggregator? - Spencer
   1. **It would be nice if we tried setting one up just to show that logs are getting sent and stuff.**
   2. **In deployment, it will be external. In other systems (which will be offline), the log aggregator is a one-way link**
4. What logs does the IdAM send out? - Spencer
5. Will install/config be automated from some script lying around? Or will it be done through another part of the system? - Spencer

**Data Storage (Postgres w/ SE Linux)**

1. Are the users the ones responsible for creating labels for the data? - Caleb
   1. **There is a proof of concept but we are not responsible for solving it.**
   2. **Sys admins will create the data labels.**
2. Would users only be allowed to classify labels up to their own clearance level? - Caleb
3. Should users with higher privilege be able to edit the labels made by users with lower classification. - Caleb
4. The documentation mentions that each service running inside the container runtime will have a different account. Will these accounts be generated every time a container is spun up? How will the username and password be determined, since PostgreSQL can’t interact with Keycloak?
   1. **Haven’t quite solved this one yet. Danny’s solution would be that each service has a service account. Each service has a unique user regardless of the container its run from.**
   2. **Each container has its own credentials**
   3. **But in SE Linux, each container has its own labels. This is how we would deny access to certain users.**

|  |  |  |
| --- | --- | --- |
| **Action Item** | **Person Responsible** | **Due Date** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Meeting Evaluation:**

* **Positive -**
* **Negative -**

**Next Meeting:**