hystax

Technical Due Diligence and Audit Report

Company: Sunflower Inc (www.sunflower.com)

Generated by Hystax OptScale (my.optscale.com)
Date: 11/23/2021

Technical Due Diligence Report: Private Part

(shared with the report requestor only. Not available for the company under due diligence)

Overall score	Red flags	Overall feedback
67 / 100 **(average score is between 70 and 85%)**	**4**	**Moderate Negative**
Inconsistencies in survey responses: **3**		

Scores by category

Architecture: **40 / 100**	Source code quality: **80 / 100**
IT Infrastructure: **24 / 100**	QA & Dev techniques: **70 / 100**
CI/CD process: **90 / 100**	Team: **90 / 100**
IT security: **100/100**	

Identified Red Flags

1. **The IT infrastructure score is below 30%.** The company uses VMware and IBM Cloud which is not typical for early-stage startups as the cloud platforms are dedicated to enterprise customers. The company doesn't have any credits from cloud providers and is not a participant in any cloud startup program.

   Usually, it means that CTO does not have enough experience with cloud platforms, there can be potential scalability and CAPeX issues concerning the private cloud.

   Recommendations: interview CTO, migrate workloads to AWS, validate the necessity of using the private cloud, apply for AWS startup programs. (https://aws.amazon.com/startups/startup-programs/).

2. **Architecture: no container usage.** The company uses monolithic architecture which can potentially lead to scalability and high-availability issues.

   Recommendations: interview CTO and validate previous experience in building high-load applications with a monolithic architecture.

3. **Perl is one of the source code programming languages used by the company.** Just 3.1% of developers used it in 2020 which makes the process of finding the right talent complex. (https://bootcamp.berkeley.edu/blog/most-in-demand-programming-languages/)

   Recommendations: figure out the state of product readiness and the possibility to switch to a modern programming language, at least, for new libraries and capabilities.

4. **There are two inconsistencies in CTO's replies to the survey and what OptScale detected.**

Question	CTO's reply	Automated audit results
Infrastructure: What PaaS services do you use in the public cloud?	None	Detected DBaaS, CDN and Big Data services usage
Development: What methodology do you use in development?	Scrum	No regular sprints in Jira detected
Development: What programming languages do you use in your product?	Perl, Python	Perl, Python, **JavaScript**

Release frequency

OptScale has detected **one release per month** to the production environment and **weekly** deployments to the staging environment.

Conclusion

Based on the analysis there are significant issues with infrastructure decisions as they can potentially lead to issues with the product scalability and R&D team growth pace. CTO’s expertise is under question and must be validated during an interview with a technical expert.

Technical Due Diligence Report

(shared with the company and the report requestor)

Overview

Areas with no issues	Recommendations	Potential issues
3 / 7	**11**	**6**

You are doing a great job in CI/CD process, IT security and R&D team expertise. However, there are a few items requiring your attention.

Areas for analysis: IT infrastructure, product architecture, CI/CD process, source code state, QA & Development techniques, IT security, R&D team.

IT infrastructure

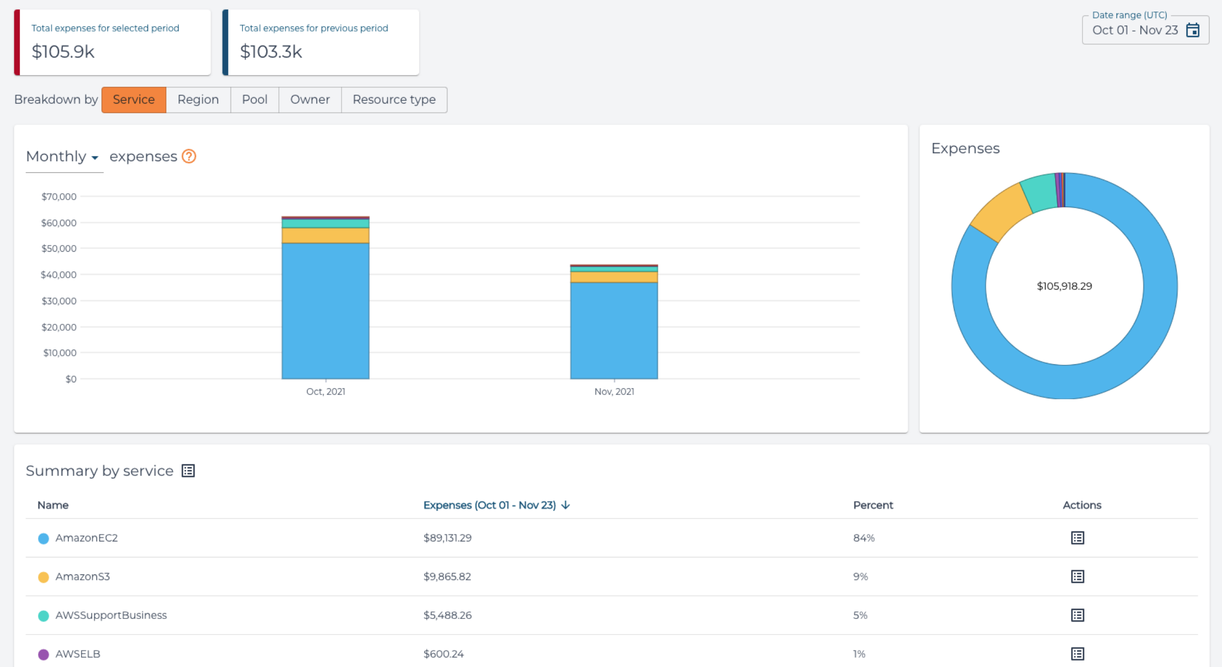
Audit data sources: OptScale with connected cloud accounts and IT environments, survey.

According to the audit, your company uses the following cloud platforms: AWS, Kyndryl (IBM Cloud), VMware.

Cloud accounts

Data source	Cloud platform	Connected to OptScale	Monthly cloud bill	Notes
Sunflower AWS	AWS	Yes	$88,377 (16% more than the previous month)	
VMware cloud	VMware	No (not supported)	N/A	3 ESXi servers with 40 VMs
IBM Cloud	Kyndryl / IBM Cloud	No (not supported)	$34,000	

Usage distributed by service



Summary by service

Name	Expenses (Oct 01 - Nov 23) ↓	Percent	Actions
● AmazonEC2	$89,131.29	84%	▤
● AmazonS3	$9,865.82	9%	▤
● AWSSupportBusiness	$5,488.26	5%	▤
● AWSELB	$600.24	1%	▤

PaaS services: AWS RDS, CloudFront and Sagemaker

Issues

1. VMware and IBM Cloud usage are not typical for early-stage startups as the cloud platforms are dedicated to enterprise customers.
2. Cloud bill is 16% more than the previous month which can lead to a more than a doubled annual cloud bill if the tendency stays the same.
3. Low ratio of tagged resources. Only 8% of resources have tags. Tags can help you properly allocate costs, remove unused resources and figure out resource purposes and creators.
4. Identified security issues. There are insecure security groups and 16 unused IAM users who still have access to your cloud accounts.

Recommendations

1. Migrate workloads to AWS and consider getting rid of the private cloud and CAPeX associated with it.
2. Implement Recommendations listed in OptScale to save up to $49,892 (56% of a monthly cloud bill) and allocate costs by setting budget limits.

The recommendations include removing unused resources and rightsizing virtual machines.

3. Define tag policy.
4. Create a clean-up script to remove unused resources.
5. Create resource auto-assignment rules in OptScale to monitor how your team consumes cloud resources.
6. Apply for cloud startup programs to get cloud credits: (https://aws.amazon.com/startups/startup-programs/)

Product architecture

Audit data sources: OptScale with connected cloud accounts and IT environments, survey.

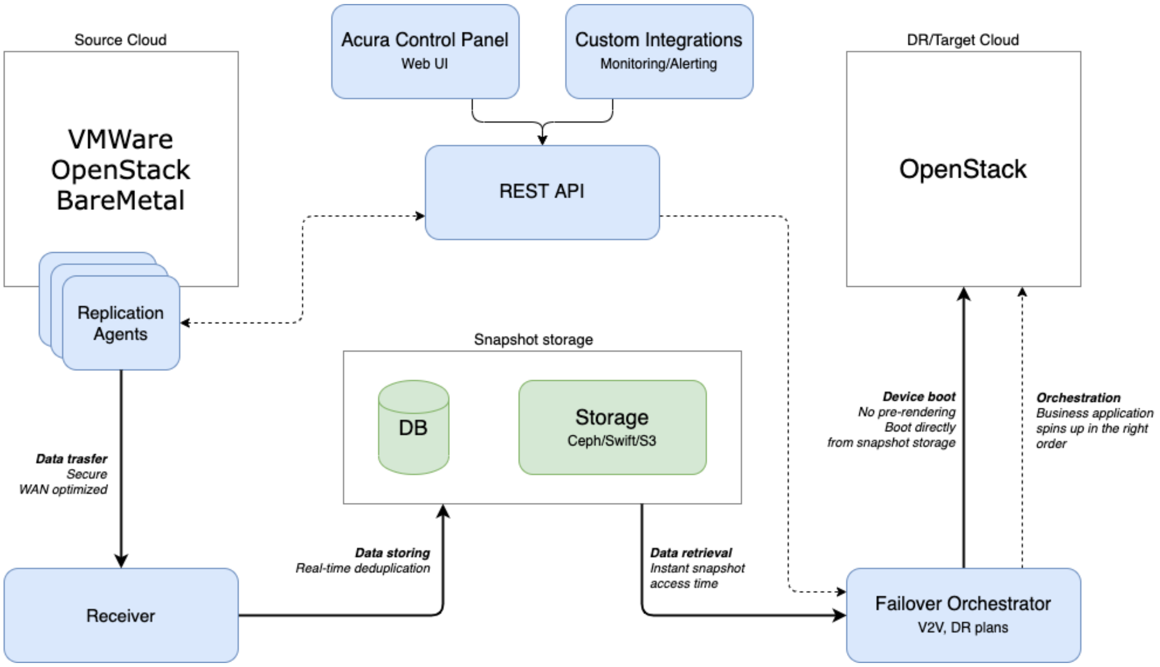
Product description: flowers online retailer

Product slides: <link>

Product demo link: <link>

Product documentation: <link>

Product architecture



Internal databases: MongoDB, ClickHouse.

Message brokers: RabbitMQ

Workloads platform: **VMs, no containers**

Machine learning: No

Issues

1. No container usage, monolithic architecture only. You may have scalability and high-availability issues at some point if you don’t use containerized product architecture. It will also require more DevOps and Operations efforts to update and maintain the architecture.

Recommendations

1. Consider using containerized architecture, at least, for new capabilities and releases. You may use a hybrid model and plan how to re-platform all the existing code.

QA & Development techniques, CI/CD process

Audit data sources: OptScale with connected cloud accounts and IT environments, survey, Jira.

Bugtracker: Jira

Communication tool: Slack

CI/CD tool: Jenkins

Programming languages: Perl, PHP, Javascript

Unit tests coverage: Full

Code review: for every commit

QA Automation: Yes, written in Python

Test coverage tracking: **No**

Nightly tests: **No**

Connected IT environments

Environment	Type	CI/CD integration	Deploy frequency
prod-env	production	Yes	Once a month
staging	staging	Yes	Weekly
dev-1	dev env	No	N/A

Issues

1. Perl is one of the source code programming languages used by your company. Just 3.1% of developers used it in 2020 which makes the process of finding the right talent complex. (https://bootcamp.berkeley.edu/blog/most-in-demand-programming-languages/)

Recommendations

1. Consider using one of the top 10 programming languages instead of Perl to avoid R&D team scalability issues.

2. Test coverage indicates software testing quality and effectiveness and helps to identify bottlenecks and defects at early stages.
3. Nightly test runs significantly improve product quality and allow QA team to be more effective: during nights environment usage is decreased, no new changes appear in the product, thus in the morning the whole team is aware of the current product state and possible issues.

Source code state

Audit data sources: open-source source code analyzing tools.

Semrep analysis result: No critical security issues; No major security issues; minor security issues: usage of outdated hash algorithms.

No issues or recommendations were identified.

IT Security

Audit data sources: survey.

Password rotation frequency: every 3 months

VPN access to internal workloads: Yes

SSO / SAML solution: Active Directory, Google

Internal workload integration with SAML: Yes

Frequency of expired credentials removal: N/A

Recommendations

1. Set policy or use OptScale to identify and remove unused/expired credentials from cloud accounts and R&D tools.

Team

CTO’s LinkedIn profile: <link>

LinkedIn profiles of top engineers: <link>, <link>, <link>

CTO and top engineers work together for 2 years

Number of developers: 12

Number of QA engineers 4

Number of DevOps engineers: 1

Number of out-staff engineers: 3

Out-staff engineers are located: Germany, Mexico

No issues or recommendations were identified.

Technical Due Diligence Methodology

Areas for analysis: IT infrastructure, product architecture, CI/CD process, source code state, QA & Development techniques, IT security, R&D team.

Data sources for analysis: OptScale with connected cloud accounts and IT environments, survey, Jira, open-source source code analyzing tools, materials uploaded by CTO, interview (optional).

Area	Subject of due diligence and methodology
IT infrastructure	**Method**: OptScale, survey **Subject**: review IT infrastructure, cloud accounts to identify potential scalability issues, security problems and possible IT infrastructure cost optimization scenarios
Product architecture	**Method**: OptScale, survey **Subject**: review product architecture, libraries, technologies, scalability & HA potential and Machine Learning data sources to identify inconsistencies with modern CI/CD strategies
CI/CD process	**Method**: OptScale, survey, CI/CD tools **Subject**: review CI/CD tools, list of IT environments and deployment frequency to identify inconsistencies with modern CI/CD strategies
Source code state	**Method**: open-source source code analyzing tools, survey **Subject**: identify programming languages, code base size,

	analyze code quality, security issues
QA & Development techniques	**Method**: OptScale, survey, Jira, CI/CD tools **Subject**: review development methodology, Dev&QA tools and programming languages to identify inconsistencies with modern R&D strategies
IT security	**Method**: survey **Subject**: review if there are potential security gaps that can lead to cyberattacks or data leakage
R&D team	**Method**: survey **Subject**: review profiles to identify CTO's and core team experience, how many years they work together (risk of losing top engineers). Identify the ratio of developers/QA engineers/DevOps engineers. Figure out if there are any out-staff engineers and if they are located in risky geographies

Survey Responses

Question	Response
General	
Company website link	sunflower.com
Product description	flowers online retailer
Product slides	sunflower.com/slides/
Product demo link	sunflower.com/live-demo/
Product documentation link	sunflower.com/docs/
IT infrastructure	
Do you use containers in your applications?	No
What cloud platforms do you use?	AWS IBM Cloud Other (Please specify) - VMware
Do you participate in any startup program from public clouds?	No
What PaaS services do you use in the public	None

cloud?	
Do you use multiple cloud regions?	Unsure
Do you have any on-premise R&D or production resources?	Yes
What platforms do you use on-premise?	VMware
What edition/version/server specification of VMware do you use?	ESXi 6.7
How many servers do you have on-premise?	3 ESXi servers with 40 VMs
Where do you host on-premise resources?	Yes
Describe why you decided to use on-premise resources instead of going cloud-only.	Previous experience with VMware clouds
Product architecture	
Where do your production workloads primarily run?	Containers managed by cloud
What databases do you use in your solution?	MongoDB
Do you use a message broker in your product?	No
Do you use ML in your application?	No
Development and QA	
What methodology do you use in development?	Scrum
What programming languages do you use in your product?	Python JavaScript Other (Please specify) - Perl
Why did you choose those languages?	Previous experience with the languages
Is your code covered with unit tests?	Yes
What source code versioning tool do you use?	GitLab

Do you run code reviews?	For every commit
Do you have any QA automation?	Yes
What language do you use?	Python
What Frameworks do you use for automation?	No
What automation tools do you use?	No
Do you track test coverage?	No
How often do you run existing test automation?	Every few days
Do you use CI/CD tools?	Jenkins
How do you deploy to production?	CI/CD flow
Do you run nightly tests?	No (Please specify) - N/A
How frequently do you deploy to production?	once a sprint (two weeks)
IT Security	
How frequently do you rotate passwords for all the internal workloads, R&D tools and engineering laptops?	90 days
Is access to your internal workloads organized via VPN?	Yes
Do you use any SSO / SAML to organize access to internal resources and tools?	Active Directory Google
Does your team access internal workloads via a single standard password?	No, everybody has access via SAML tool
Do you remove public keys from workloads when access is not needed?	We do not access workloads via public keys
How frequently do you remove unused credentials from cloud accounts, R&D workloads and internal systems?	N/A
Team	
How many developers do you have?	12
How many QA engineers do you have?	4

Please provide us with a link to your LinkedIn profile.	<link>
Please provide us with links to LinkedIn profiles of top engineers in your company.	<link>
How many years have you been working with your top engineers?	2
Do you have out-staff engineers (freelancers/contractors) in your team?	Yes
How many contractors do you have in Engineering?	3
Where geographically are those freelancers located?	Germany, Mexico