sysdig

CASE STUDY

COMPANY DETAILS:
The leading global provider of integrated travel, expense, and invoice management solutions for businesses and government agencies.

BUSINESS NEED:
- Deliver secure financial applications globally
- Ensure always on platform availability
- Deliver applications quickly and safely to stay competitive

CHALLENGES:
- Prometheus was an operational burden
- Manual scanning was labor intensive, slowing them down
- Lack of data for troubleshooting and compliance audits

BUSINESS IMPACT OF SYSDIG:
SAP Concur delivers a global, always on platform, that meets security and compliance requirements. New services are brought to market faster.

SYSDIG PLATFORM BENEFITS:
- Automation saves 10,000+ hours
- Secure DevOps approach, single agent is more cost effective
- Forensics, even when containers are gone
- Platform scales with K8s growth- 20x since inception
- Audit trails to ease the burden of audits

INFRASTRUCTURE:
Amazon Web Services (AWS) and on-prem

ORCHESTRATION:
Kubernetes

SAP Concur

SAP Concur Delivers Secure, Compliant Solutions to More than 50M End Users Globally

Overview

SAP Concur is a SaaS company that provides travel, expense, and invoice management services to businesses and government agencies. With a global customer reach that includes more than 25,000 SMBs in North America alone, SAP Concur is operating a massive infrastructure at scale. Rolling out new, reliable, and always on services as securely as possible is of the utmost importance to the business.

SAP Concur made the decision to move from a monolithic architecture to microservices for the flexibility in delivering applications faster. Four years after that journey began, SAP Concur now has a team of 20 that is responsible for a container ecosystem that consists of more than 2,000 nodes in production.

Challenge

Building microservices at SAP Concur started with a small tiger team. As Mike Luedke, Director Engineering at SAP Concur explained, “We started off as a grassroots effort. There were a few of us from different teams that got started originally building a cluster. Eventually, we then opened that up to some early adopters within Concur. After that, it gained traction pretty quickly. We went from an informal group managing this thing, to where it became clear that this was gonna have a definite future at Concur. At that point, we started to build a formalized team around it.”

Starting out the way that they did, everything in the SAP Concur stack was open source. As they grew, they engaged the security team and quickly identified security and visibility gaps, especially when comparing the security for the traditional infrastructure to the new container environment.

According to Tiziano Tarolla, Senior Development Manager, “We hit an inflection point around the time we hit 100 nodes with open source Prometheus, where we had to come up with a better scaling strategy. We were strapped for resources. We were so busy expanding and trying to meet the demand for our internal applications teams that we didn't really have a lot of spare cycles to figure out a scaling solution for Prometheus, so we started taking a look at commercial options. Since Sysdig Monitor's managed Prometheus service is based on open standards we didn't have to worry about re-tooling our monitoring environment."

Reasons SAP Concur selected Sysdig

Luedke explained that when looking for options, “Concur spent quite a bit of time thinking about the commercial solution we were going to bring into our stack because this was the only piece of our stack that was commercial. Everything else was free open source.”

After comparing the known commercial monitoring and security tools, SAP Concur selected Sysdig because:

- Kubernetes-first approach to security
- Open source roots
- Unique syscall implementation
- Unified security, compliance, and monitoring
- Support for PromQL
- Deep kernel-level metrics out-of-the-box that can be sliced any way

Saves thousands of hours, making daily releases possible

Before using Sysdig, SAP Concur was conducting manual reviews before pushing code to production. According to Luedke, “With Sysdig, we were able to automate many of the manual reviews. We’ve instrumented Sysdig into our pipelines where it is executing container vulnerability and compliance checks on containers as they're promoted into our production environment. Those automated checks allow us to move faster.”

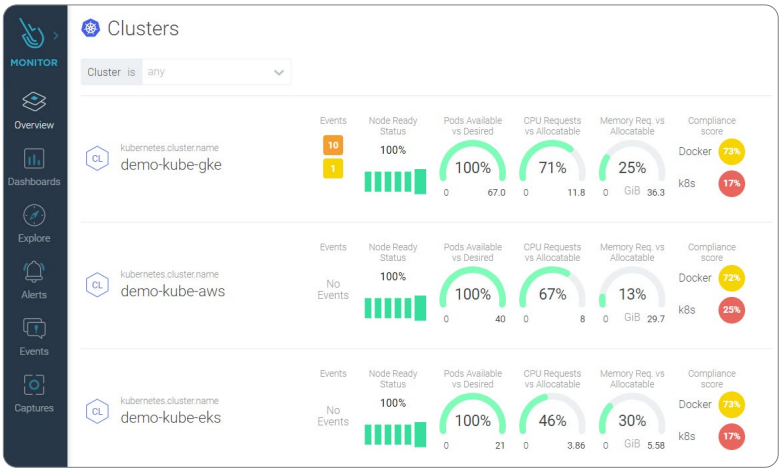
Further explaining the review process and what it would be like without Sysdig at the current scale, Luedke said, "A manual review for those vulnerabilities or a manual scan could take 10 minutes per check in. Our previous vulnerability scan option was using open source Clair, so my team would have to go and check the results in another interface, which took time. With Sysdig, all of that just becomes automatic as part of the pipelines as the team is doing their deployments. Today, we handle thousands of merges per day. If you consider each could take 10 minutes on average and multiply that by thousands a day, we wouldn’t be able to operate close to the same speed without Sysdig.”

Removes security and visibility gaps

As the only unified security, compliance, and monitoring platform, Sysdig provides a single source of truth to eliminate silos of information between development, DevOps, and security teams. With this approach, organizations can resolve issues quicker by analyzing granular system data automatically correlated to cloud and Kubernetes context. It also empowers DevOps teams to take on security responsibilities.

Sysdig is used by many teams at SAP Concur, including application, operations, infrastructure, DevOps, and the security teams. Having a single tool for multiple use cases has enabled everyone to take responsibility for security and embrace secure DevOps. As Luedke explained, “With Sysdig, our application developers have direct insight into what is going on. They have access to look at things like performance metrics and they can use Sysdig as a troubleshooting tool. This empowers them to do their own DevOps on their applications. They can just go to Sysdig and see what's going on without having to contact the operations team or the infrastructure team.”

> **"A manual review for those vulnerabilities or a manual scan could take 10 minutes per check in. [...] With Sysdig, all of that just becomes automatic as part of the pipelines as the team is doing their deployments. Today, we handle thousands of merges per day. [...] we wouldn’t be able to operate close to the same speed without Sysdig.”**



Luedke went on to explain, “Sysdig saves everybody time, application developers, as well as the infrastructure team. And because it saves time, it allows people to ask a lot of questions because they are more frequently looking at this data. This lowers the bar by being able to have that visibility. There is no extra overhead when they want to look at something, they can just go do it. I think it makes us more aware of what's going on in our infrastructure.”

Luedke also explained that the unified platform not only makes them more secure, but it saves resources and money. “There is a simplicity of having a single solution to go to that looks at monitoring holistically. By that, I mean, it provides infrastructure operational monitoring, as well as security monitoring. There is a lot of value in that! From a more tactical standpoint, having one agent report all that stuff up saves us a ton of money because each agent takes processing power, and so being able to do it with a single agent is very nice. To get what we get with Sysdig means we would need two tools, which is double the number of agents.”

Prometheus metrics at enterprise scale

Before SAP Concur selected Sysdig, the team was using Prometheus for monitoring. According to Luedke, “On the metrics side, we were doing okay because we had Prometheus. However, the issues that we were running into were around scalability. As we grew, we were losing our Prometheus database regularly because of the scaling issues. We would only be able to store an hour’s worth of data at a certain point. If something happened more than an hour prior, we were kind of hosed just because of the amount of data we were collecting. Sometimes we would just lose the database entirely and it would crash. We wouldn't have the data at all. We were flying blind.”

Sysdig is the only fully compatible Prometheus solution. This includes support for the Prometheus Query Language (PromQL) to perform advanced metric queries, build dashboards, and create alerts. Sysdig addresses the issues that hold teams back from organization-wide adoption of Prometheus monitoring: scale, data retention, and enterprise access controls.

Shifting security left with image scanning

Organizations can manage security risk by finding and fixing vulnerabilities and misconfigurations early in the DevOps process through image scanning. SAP Concur uses Sysdig to continuously scan images within registries and CI/CD pipelines, as well as during production. This saves time by uniquely mapping vulnerabilities to Kubernetes-based applications.

According to Luedke, “We depend on Sysdig to do vulnerability scanning and intrusion detection for our containers. Before Sysdig, we had host-based intrusion detection running on our nodes, but there wasn’t any context. It would maybe tell us what process was impacted, which looked like just the Docker ID. In a large multi-tenant environment, we had no idea what that container belonged to without mixing it with some Kubernetes metadata. It’s not that we couldn't get that information, it was really painstakingly difficult to do that on a regular basis. Sysdig gave us a really quick way to view security events and other low-level information in the context.”

“Over time, the usage of Sysdig and how we secure the environment continues to grow as the company has evolved. We used to focus quite a bit on commercial customers and lately, we’ve really grown our public sector business. With this has come new compliance obligations. We've been able to leverage Sysdig to check the boxes on some of these compliance items as well. When we first started, we would have to do these manual investigations once or twice a week, taking a few hours of time; however, as our compliance requirements grew along with our Kubernetes environment, we wouldn’t be able to do that manually anymore. At the scale we are at now, we couldn't operate without Sysdig. We just simply couldn't use Kubernetes if we didn't have a solution like this.”

> **“We’ve instrumented Sysdig into our pipelines where it is executing container vulnerability and compliance checks on containers as they're promoted into our production environment. Those automated checks allow us to move faster."**

Simplified compliance reporting

With Activity Audit, Sysdig captures container activity and correlates the information with application context, as well as users or services from Kubernetes. This feature has come in handy hundreds of times for SAP Concur, including during audits.

Luedke explained, "Having the audit trails has helped us in many situations. One time we had auditors that wanted to make sure we were running the environment as we said we were. They asked for process information from a particular container that was running an infrastructure, but that container was running distrolesss, so there's no shell on it. It's very secure because it's locked down to just what needs to be running, but that also means you can't do things like get process information by executing into it. We were able to use Sysdig to get visibility into that container to provide the auditors evidence."

Going into further detail, Luedke said, "I just looked at the dashboards at the top processes metrics view for that instance and provided what they needed. They also had follow-up questions about making sure that our containers were immutable because we told them that we were meeting this obligation. With Sysdig, we were able to prove that our running containers had not been modified since they were launched. We just used the audit events in Sysdig to show file system and shell activity on the containers to prove it."

Forensics even when containers are gone

The same activity audit trails that are useful in compliance audits are invaluable in the event of anomalous behavior. With Sysdig, enterprises have the ability to capture all activity information into a capture file for forensics, even if the container no longer exists.

For SAP Concur, Luedke explained that, "Many times Sysdig has given us insight into troubleshooting. We use it as a troubleshooting tool all the time when there are service degradations. Sysdig helps us to pinpoint where the problems are. This is one of the most valuable features we use in Sysdig."

According to Luedke, beyond the captures, "Being able to slice-and-dice metrics by various attributes is incredibly useful. We often run into unique problems and when there isn't a canned view that shows the problem the way we need to see it, we can quickly build that view. I cannot begin to explain to you how valuable this is when something isn't going as planned."

Deep kernel data provides unmatched visibility

Sysdig uses system calls to report what is happening inside a container. As the primary mechanism of user-to-kernel interaction, syscalls offer great insight into what a program is doing, and can be invaluable for troubleshooting, monitoring, and bottleneck identification.

According to Luedke, "We liked the Sysdig approach. We liked how they are instrumented and how they actually collect data was a superior security monitoring solution compared to the other options. The other security tools do a lot of residual extending of Kubernetes functions. They are kind of filling the gaps with Kubernetes, but as Kubernetes matures as well, those gaps are already included or dealt with upstream. We strongly believe in getting metrics out of the kernel. It's a very solid strategy. I have always been impressed by the out-of-the-box metrics that we get from Sysdig. It is this very low-level data and is very extensive compared to other solutions, so we're able to see deep, deep into the problems that are going on."

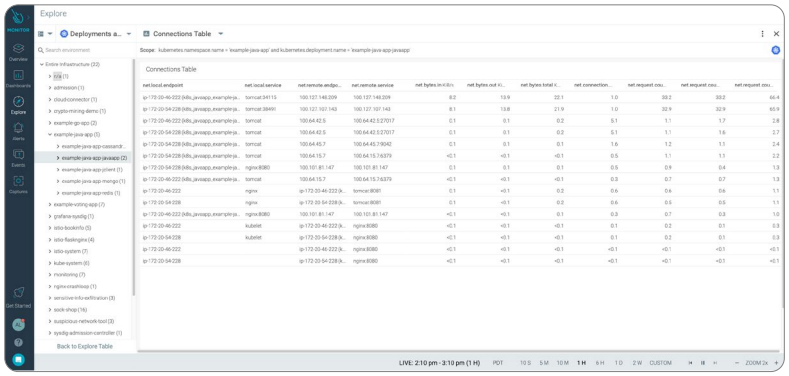
Maximize availability across hybrid cloud infrastructure

The SAP Concur environment spans AWS Cloud and on-premises infrastructure. With Sysdig, SAP Concur has the same viewing experience across all of its infrastructure, which makes it easier to anticipate issues with microservices that have cross-platform dependencies. In the event of an issue, having system-wide visibility can facilitate quicker resolutions.

As Luedke put it, “We can scope and look for issues across both AWS and on-prem in one view in Sysdig. The way the interface is set up allows us to understand if anomalies are happening in one versus the other pretty quickly. The smart groupings in the dashboards allow us to group different attributes of the metrics in a way that makes sense in the context that we need. Being able to scope and then slice-and-dice data, to get the view that I want — Kubernetes or a namespace view, or a more physical view, or maybe I want to see my cluster — and then being able to boil that up with context from Sysdig enables us to really understand with is going on across the entire infrastructure.”

Open, community-focused company

When SAP Concur was still in the selection stage, the team was drawn to Sysdig because it is built on an open source foundation. According to Luedke, “We liked how Sysdig embraced and also contributed to open source. That was important to us.”



Today, open source is driving the cloud. Being built on open source tools like Sysdig Inspect, Falco, and Prometheus enables Sysdig to move faster, while also providing more secure software.

For Luedke, since Sysdig embraces open source, it is easier when they need to add new capabilities. As he put it, “Being able to quickly and easily use open standards like Prometheus has been helpful. For example, in the few events when there hasn’t been an out-of-the-box integration, we’re able to build what we want with Prometheus endpoints. It's easy and quick, which is really nice.”

Being an open source-based company also means Sysdig believes in collaboration. Since Sysdig launched, the product team has spent hours listening to customers and letting their needs direct the roadmap. As long-time users, this level of service has been really important to Luedke “Sysdig has been a good partner for us. They have always been very receptive to our evolving needs and helping to find a solution for us, big or small. They are in the trenches with us.”

To learn more about Sysdig, visit www.sysdig.com or to try a free trial, visit www.sysdig.com/trial.

CS-SAPCONCUR Rev.C 7/22