Get the Most Value Out of Your Observability Investment

Observability offers visibility into the data being generated by your infrastructure devices, systems, and applications — but in reality, it offers the opportunity to see what's happening, There's no guarantee that you'll get what you want; you have to set things up in a way that makes it possible for you to get the insights you need.

It's kind of like going fishing for data — you'll need the right rod and lures to reel in the kind of fish you want, and you have to be fishing in the right spot. Similarly, you'll need the right observability infrastructure and tools in place to gather, route, and process the data so that you get the exact information you're looking for. Not only do you need the right agents and pipelines in place, but you also need the right event buses, logs, shippers, API collectors, and analytics systems. Your strategy is just as important as your tools.

Define the Problem Before Buying the Tools
You wouldn't take your fly fishing gear out into a lake if you were looking to catch a 500-pound tuna, so why choose your observability tooling before deciding on exactly what problems need to be solved and what type of data will solve them? A better approach would be to start from first principles and figure out your call to action. For instance, why do anything at all? What are you not able to accomplish with your data today that you want to be able to accomplish tomorrow?

Before trying to buy or build anything, consider what components of observability you already have – whether it's a syslog server or a collection of millions of dollars worth of software. You might not have all the features, capacity, licenses, or storage you want, but chances are you already have some of the pieces in place.

Take a Deep Dive into Your Current Observability Architecture
Start with your hardware and software systems. Do you have IaaS up in the cloud? Are you using SaaS? Do you already have observability systems? If you have systems on a freemium contract with restricted capabilities, you may want to upgrade licenses. There might be some open source projects that you decided to use to build things on your own, but they're still sitting on the shelf because you don't have the staffing or the expertise — or let's just be honest, the budget. Open source sounds like it's free, but once you actually have to do something with it, you could run into unexpected costs, which can start to add up.

What Sources and Destinations Are You Working With?
After you get an idea of what everyone needs, you want to talk about the sources you are currently capturing data from. You probably have a syslog server and a bunch of other agents like REST APIs that are generating data. Log shippers, applications, network devices, and customers' instrumentation that your software developers may have built will all collect and forward data at some level. Find out exactly what your stakeholders are missing — which events, metrics, or data do they need, and from which devices?

Then there's the other side of the data pipeline coin: destinations. Where does that data you collect actually go? These are your log servers, systems of analysis, and storage that can be either on-premises or in the cloud, databases, search engines, APM, systems API collector, or any custom systems that were developed. Decide what might be missing here as well, and then figure out if all the data you bring in is being processed correctly. What are you not doing that the stakeholders want you to do? Is anything missing or duplicated? Do you have sufficient licenses and capacities?

Optimize Your Observability Pipeline

Now that you know where data is coming from and how it's getting to its destination, it's time to optimize. You may have a simple setup with one set of agents connecting to a single analytics platform, essentially as a point-to-point connection, and that may be all you need. But if you have over 50 different destinations or a handful of agents sending data to 7 or 8 different systems of analysis, you want to stop and ask how it could be optimized. How much of that data is duplicated? And if those agents are doing totally different things, why change?

You might find it helpful to put something in the middle. An event bus, data bus — or pipeline, as we like to refer to it at Cribl — can take data from lots of different agents and sources and shape it while still in motion. That central location can serve as a manifold or distribution hub to send that data to different places, giving you the ability to replicate it identically if you need to. More importantly, you can shape it exactly the way the ITOps, DevOps, AIOps, or SecOps teams need it. If data is coming from the same source and one department wants all the information but another just wants a subset, you shouldn't have to manage a whole set of agents to do that. With Cribl's suite of products, you can filter data, forward it, or take a full-fidelity copy of an event and send it off to cold, inexpensive storage. That way if someone ever needs it again, which is bound to happen at some point, you can easily go back and retrieve it for additional processing.

Build Your Observability Solutions With the Future in Mind

Keep in mind that no matter how thought out and tested your observability solution is, it might need to be altered as your requirements change. There are always going to be new types of data and analytics systems, as well as departmental or legal requirements and budget changes to adjust to. Because of this, it's important to build an open observability solution that you can grow in scope, capacity, and capabilities as your enterprise grows.

Make sure to avoid vendor lock-in and proprietary tools that don't "play nice" with others. Detach the idea of vendor functionality and storage being tied together. Data wants to be in open formats in vendor-neutral storage. To achieve maximum flexibility, focus on building your solutions with a vendor-neutral observability pipeline.

We know there's a wealth of interest in observability right now — the technology, the vendors, the hype/marketing, and the promises– and it has driven confusion, not clarity, around observability and the benefits it can deliver.

Want to learn more? Get started with this **video** for more details on Cribl's Stream solution or visit us at **www.cribl.io**