Monitoring and reporting Confluence Data Center

Atlassian Resource

ATLASSIAN

Monitoring and reporting

How to drive enterprise efficiency with Confluence Data Center

ATLASSIAN

Monitoring and reporting

How to drive enterprise efficiency with
Confluence Data Center

Monitoring and reporting

When it comes to driving efficiency and effectiveness in your organization, monitoring and reporting capabilities are your best friends. These capabilities are what allow you to gain insight into how your teams are using their software.

Consider your current products and if they provide the right kind of data you need to answer questions, such as:

- Are my teams following the organization's established best practices?
- What does my product's performance look like?
- Can I report back to the executive team on our security and compliance position?

If the software that your organization relies on can't help you answer questions like these, then they aren't contributing to efficiency and effectiveness in your enterprise.

Being an admin of a self-managed environment means that you are responsible for the management of your entire instance. This includes data retention, scale, performance, and end-user activity just to name a few things. On top of this, you also have to deliver on aggressive business objects, break down organizational silos, and establish consistent ways of working across the enterprise, that's a whole lot to manage when you can't understand what's actually happening in your instance. That's why having the right software that enables you to take action is so important.

Gain insight with Data Center

Data Center, Atlassian's self-managed enterprise edition, has advanced auditing capabilities, which allow you to create a digital record of what's happening in your instance.

You can choose one of four different coverage levels (off, base, full, advanced) to log different types of events, depending on the unique needs and insight that your organization requires.

Advanced auditing is built with file externalization capabilities, which means that you can integrate your Data Center products with third-party monitoring tools, such as Splunk, Elastic Stack, Sumo Logic, or CloudWatch. By leveraging file externalization, you can even use key features provided by your monitoring tools to gain even more insight into your events.

5 ways to become more efficient with advanced auditing

- Be proactive rather than reactive
- Keep good instance hygiene
- Maintain security and compliance
- Boost performance and capacity
- Focus on your business objectives

Be proactive rather than reactive

Up until recently, the IT strategy for most large organizations looked something like this: One of your teammates is having trouble with their software. They submit a ticket to IT to get help with their problem. At which point, the ticket gets added to a queue until it's assigned to someone on the team. Once the ticket is assigned, someone on your IT team works on troubleshooting and identifying the problem. After they've finally identified the problem and resolved it, the issue is marked as done, but it took quite a bit of time to fix the problem; this is an example of a reactive IT strategy.

A **reactive strategy** is when you're only reacting to a problem and relying on your teams to report an issue while it happens. This means that your teams have already experienced the problem and aren't able to deliver on their objectives until the issue is resolved.

VS

A **proactive strategy** is a more efficient approach where advanced auditing can help you change your strategy. Because advanced auditing tracks all the events that occur in your instance, if you start to notice too many events being logged or events that are different than your normal ones, you can act quickly. Since events are logged in real-time, you can identify the issue and potentially avoid any interruptions or problems with your products.

Keep good instance hygiene

You may have already undergone a cleanup initiative within your organization, but that's only half the battle. While it's important to look critically at your instance and clean up any old data or suboptimal configurations, if you don't have the monitoring or reporting capabilities to ensure that your teams are using the products correctly, you'll likely end up where you started. By looking into your instance on a regular basis, you can maintain good instance hygiene.

You might be asking yourself what good instance hygiene is. It means you are maintaining your cleanup efforts and upholding the practices that you've put in place. However, old habits are hard to break and it can be challenging for teams to change the way they work.

EXAMPLE

When teams operated in silos, they would often request custom fields that they felt were required to carry out their department or team's goals. To help reduce the amount of data and to make it easier for teams to use their products, cleaning up unused or duplicated custom fields is one of the first cleanup initiatives an admin tackles. The problem is that after you've done this cleanup, your teams may still continue to create custom fields, which can lead you back to managing a suboptimal instance (and that's quite inefficient).

Advanced auditing can help you stop that from happening. By setting your global configuration and administration coverage levels to advanced, you can easily track when someone has created a new field. This allows you to address the issue before it becomes a problem later on.

Maintain security and compliance

Security and compliance is a top priority for any enterprise or government agency. Constantly changing external conditions like evolving regulations, the rise of remote work, and globally distributed teams makes the security and compliance of your instance an increasingly important initiative

According to most compliance guidelines, you should be actively monitoring changes in your system's behavior and data flow, which requires that you have products with 24/7 monitoring capabilities.

Depending on the coverage level that you specify, advanced auditing will log security relevant events, such as all failed login attempts. If you're leveraging a third-party monitoring tool, you can set up anomaly detection to notify you when there are changes to your security events or if a security event is logged too many times in a row. You can rest assured that your instance will remain secure and you can return it back to compliance.

Boost performance and capacity

The performance of your products is always a big concern, especially when you have a globally distributed team. To get ahead of performance issues, you need to track your product's performance to understand how many people are using your products and what they're doing.

LET'S THINK ABOUT IT

Before enterprise-grade products, you used to have to run stress tests to identify performance issues.

Now, modern products, like Data Center, provide monitoring and reporting capabilities that can give you insight in a fraction of the time you would have spent running tests.

With Data Center's advanced auditing, you can review trends in your data, such as when your products experience higher user traffic or when the number of new tickets or pages created increases. After you enable advanced auditing, your last 10 million records are stored, which gives you a chance to review your existing events and create a baseline. Then, you can integrate your monitoring tools with your Data Center products to continue tracking your team's activity over time.

With this data now being tracked, your IT team can start to build out a plan for better performance, which means that your teams will have their mission-critical products available when they need them.

Focus on your business objectives

One of the most important reasons why monitoring and reporting are so crucial to the admin of a self-managed environment is that it can help streamline some of your day-to-day tasks. Modernizing your infrastructure and finding ways to leverage newer technologies is often one of your business objectives, but it's impossible to really focus on modernizing your infrastructure if you're focused on manually monitoring events in your instance to stop problems from impacting your teams.

Advanced auditing tracks your instance events in real-time. If you've integrated with your monitoring tools, you can set triggers to notify you anytime there is a change in your events.

By looking at your team's activity, you can also get a better understanding of how your teams are using their products and what changes you can make to support them. If you've identified that you have a lot of user login events at a particular time of day, you can start to find a modern solution that will allow you to scale the infrastructure of your products.

Now that you've learned about five key areas where advanced auditing can help you drive enterprise efficiency, let's explore how advanced auditing will help solve for common problems in Confluence.

TOOL TIP

Advanced auditing also offers file externalization capabilities that allow you to work with third-party monitoring tools such as Splunk, Elastic Stack, Sumo Logic, or CloudWatch to automatically notify you every time there's an anomaly.

USE CASE

Confluence

Some of the largest organizations in the world standardize on Confluence Data Center to enable collaboration and content sharing across their businesses.

As enterprises host more of their work on Confluence, establishing the right permissions and maintaining visibility over your growing number of spaces and pages helps ensure your proprietary information is staying secure and compliant; so your teams can focus on being effective.

When you don't have the information you need, work slows down

More and more enterprises are turning to Confluence as a space for teams to document, share, and collaborate on work, but when usage spans the entire organization, it can be difficult to stay on top of every event taking place. Pages are deleted or moved, spaces are re-named, permissions change daily; while these actions seem easy enough to track on their own, when you consider the frequency of requests to resolve issues like this at enterprise scale, it's suddenly not so palatable.

Whether you're an admin or a space admin, requests like these inevitably pile up and can be a hindrance on efficiency; not just for you, but for the teams you're supporting. When a team comes to you having trouble accessing pages they need permission to, you need to understand who owns the page and can grant them the permission they need, as well as who (and when) these permissions were last changed, to make sure there wasn't a specific reason the page required restrictions.

> Global admin have the ability to view any and all spaces to resolve this problem, but as an admin or space admin, you may be restricted to a single space, making it even more difficult to provide this team the information and resolution they need to get back to work.

Without a convenient way to access information like who edited permissions and who has the ability to change them back, you're inadvertently causing teams to slow down. When work lives and flows through Confluence, a misplaced page or permission restrictions can create an unnecessary bottleneck, and the onus is on you to free it up.

Unblocking your teams' ability to work efficiently

With advanced auditing capabilities in Confluence Data Center, you can get the information you need quickly by leveraging the comprehensive audit log and permissions event coverage. With the ability to track events at the team level, you can quickly identify who changed what and when, and resolve the issues that block teams from getting work done. You can even revert to native audit logs within Confluence rather than filtering through a log file on a disk, making the user's access activity as easy to find as populating a search box.

> An added benefit of of the extended audit coverage provided by advanced auditing is the ability to identify holes in your user management process that may have led to these permissions problems in the first place. So not only are you able to perform ad hoc audits to resolve issues quicker, but you're able to perform a broader user management audit so your organization can take action and make sure it doesn't happen again. Understanding these discrepancies can help inform your user management processes in the future to enable a more streamlined flow of work, uninterrupted by process oversight.
>
> Last but not least, advanced auditing provides a delegated view, so that you can now see all of the audit events within your organization's spaces - meaning if you're a space admin, you no longer have to get in touch with the global admin to check on who did what outside of your space.

Permissions are an important element of any product being deployed across an enterprise, however when work exists and flows through Confluence the way it does - with so many team members involved and contributing - the need for a detailed, digital-record that examines all permissions and supporting actions should be high on your list.

Interested in driving enterprise-level efficiency with your teams?

Contact your local Atlassian Solution Partner to learn more about Confluence Data Center.

ATLASSIAN

ATLASSIAN

Thank you for downloading this Atlassian resource! Carahsoft is pleased to serve as Atlassian's public sector aggregator, working with an extensive ecosystem of resellers, system integrators, and solution partners who are committed to helping government agencies select and implement the best solution at the best possible value.

To learn how to take the next step toward acquiring Atlassian's solutions, please check out the following resources and information:

For additional resources:
carah.io/AtlassianResources

For additional Atlassian solutions:
carah.io/AtlassianPortfolio

To set up a meeting:
atlassian@carahsoft.com
833-JIRA-GOV

For upcoming events:
carah.io/AtlassianEvents

For additional DevSecOps solutions:
carah.io/DevSecOpsSolutions

To purchase, check out the contract vehicles available for procurement:
carah.io/AtlassianContracts

carahsoft.

For more information, contact Carahsoft or our reseller partners:
atlassian@carahsoft.com | 833-JIRA-GOV