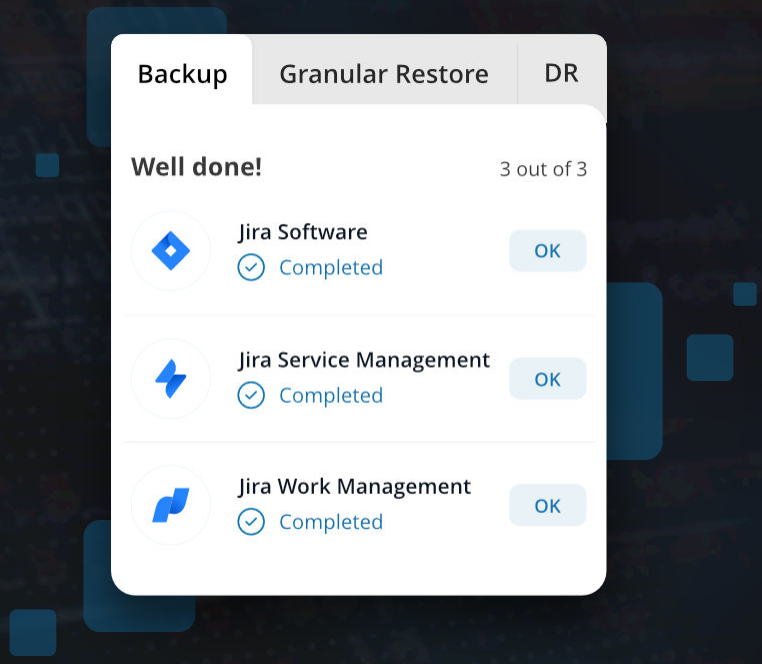
GitProtect.io
by Xopero ONE



ATLASSIAN DATA RESILIENCE GUIDE FOR JIRA ADMINS

Jira backup
Disaster Recovery
Jira migration
Data mobility
Data protection
Jira security

with 👍 &❤️ for all Jira Admins

Table of contents

PART 1

Jira Data Loss Risks - key reasons and factors

Jira data loss risks - what are key reasons and factors? This is a question that every DevOps, CTO, IT Manager or Security Leader should ask themselves when they start using any software that they will greatly rely on. Well, basically every team member should ask himself this question. If you need arguments to raise to decide whether your Jira environment needs professional backup software support, here they are...

Argument #1: Outages

SaaS or Cloud outages are nothing shocking – they happen to every cloud provider. While many reasons could contribute to such an unavailability, it does not necessarily mean that your data is gone. The question is what to do to keep your business up and running? How to minimize costs? Do you have a fail-over or Disaster Recovery plan for your SaaS application data?

Okay, but this guide is about Jira... We bet you heard about the biggest Jira failure of the last year. And if not, you should listen to this story. An all-time Jira outage affected 775 customers and lasted for almost two weeks. And this is how long it took the company to recover all customer data. What was the reason for this massive outage? No surprises this time – human error.

To make a long story short – the reason behind it was a maintenance script that accidentally wiped hundreds of customer sites due to communication issues between two Atlassian teams working on deactivating a legacy app. However, instead of being provided the ID required to disable the app, the deactivation team was sent the IDs for the cloud sites where the app was installed. Also, the script was launched using the wrong execution mode (permanent deletion instead of recovery failsafe deletion).

📌Want to learn more? Read the article: Was the Jira Outage the Last Atlassian Problem?

In our annual rankings of the loudest threats, we calculated 41 incidents in Bitbucket and 53 incidents in Jira mentioned in Atlassian Status. About 11 hours Atlassian Bitbucket users were out of the service or partially out, while Jira users experienced about a staggering 329 hours of outage.

📌Read more: 2022 In A Nutshell: Atlassian Outages And Vulnerabilities

Argument #2: Accidental deletions & human errors

Human mistake is probably one of the most common reasons for cybersecurity incidents and one of the most favorite attack vectors for criminals. Why not remember the almost forgotten “5 whys” method of Toyota founder, Sakichi Toyoda: ask the question “why?” up to 5 times and you will find the root of the problem. In most cases, the reason for the problem will be a human mistake in the end.

For example, the abovementioned Atlassian outage in April. If we ask why that Jira outage happened, the final reason will be human error – lack of communication between teams, and, as a result, an outage that influenced more than 700 customers. Ok, and from more “everyday” situations... Have any of you accidentally deleted an issue from Jira?

Unfortunately, most vendors, including Atlassian do not ensure you with granular, point-in-time restore in case of unintentional deletion and daily operations. Let us remind you – for example, that it is not possible to restore a single issue from Jira if it was accidentally deleted. You probably know how much information a single issue can contain – configuration, all comments, attachments, links, or sub-tasks. All this can disappear forever as a result of one mistaken click by your employee.

More SaaS providers enable you to restore data after deletion for

some given time. Once you discover such a period, you won't be able to restore this repo anymore. The so-called permanent/hard deletion occurred. All those rules are outlined in the Shared Responsibility Models and Terms of Service and this is another reason for a backup. We will devote the entire next chapter to this topic.

Argument # 3: Ransomware

One of the most expensive threats for any business is ransomware. Just imagine every 11 seconds some ransomware attack happens somewhere in the world.

After the attack, the only thing the user has is a notification that his data has been encrypted and now he needs to pay a ransom to get his data back... It's double financial loss – first, you need to pay the attacker, and is there any assurance that he will give the data back safe and sound? The attacker may either fail to return, or modify, or encrypt it.

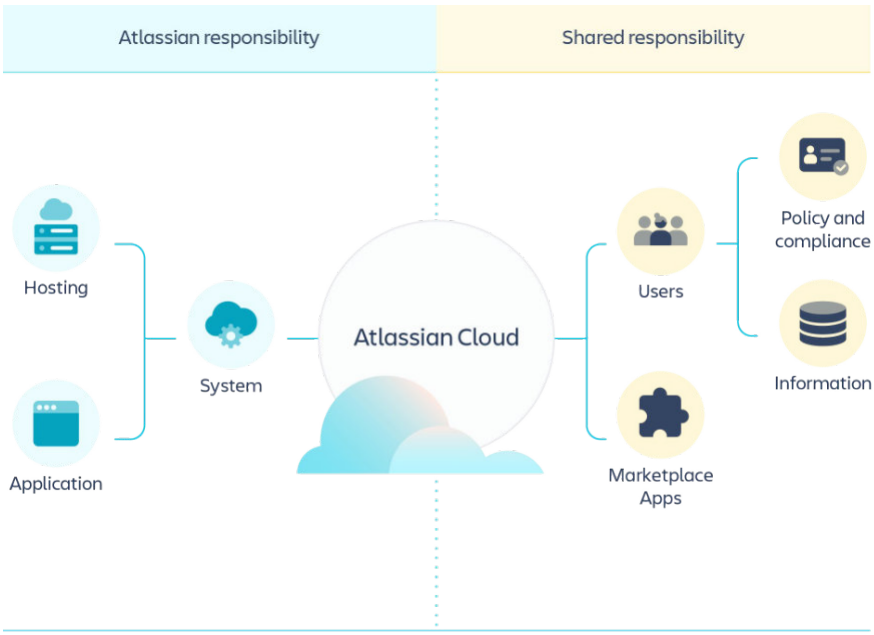
Second, business downtime, and who knows how much time the company will need to recover – usually it lasts for days. Then, add here weeks of restoring the system... Sounds scary. However, if you have a ransomware-proof DevOps backup in place, you can continue your work after running the backup copy from any point in time.

PART 2

Atlassian Cloud Shared Responsibility Model - know your duties

Introduction to the Atlassian Cloud Shared Responsibility Model

Atlassian, GitLab, GitHub, Microsoft, Google, and seriously – put any SaaS here – operate according to the so-called “Shared Responsibility Model”. This concept has evolved with the introduction of plenty of SaaS tools and has become a standard used in legal policies by almost all possible vendors now. It assumes that both provider and customer have their responsibilities resulting from the use of SaaS platforms. While the official names of such documented rules can differ, all of them are based on nearly the same rules – especially when it comes to data protection.



Source: Atlassian Cloud Security Shared Responsibilities

In short: service providers are responsible for their systems, hosting, and applications focusing on their own business and integrity at a macro level. Most of them provide 99.999% availability and uptime, preventing infrastructure from failures, errors, attacks, etc. However, when it comes to data protection at the account level, the user is responsible for data security and should be able to restore lost, stolen, deleted, or compromised data. Seems reasonable and obvious. After all, it's user data, right?

Know your responsibilities

- ☑ Data availability and security.
- ☑ Recovering from operational data loss, human error, or ransomware attack.
- ☑ Meeting compliance and long-term data retention.
- ☑ Following the 3-2-1 backup rule with multiple storages, and offsite copies in case of outages and downtime.
- ☑ Data encryption and integrity.

More about:

📌 Atlassian Cloud Shared Responsibility Model
📌 GitHub Shared Responsibility Model

Your Responsibilities in the Shared Model

Atlassian is a pro-user service, which is guided by the strong principles of fast support and security. Thus, their Cloud Security Model covers such areas as Policy and compliance, User accounts, Information, and Applications the customer uses.

Policy and compliance

Under this point, Atlassian, as a provider, has to value all the risks and vulnerabilities that happen to the platform and inform its customers about it. When it comes to data, Atlassian is only their processor, setting a clear boundary that it is not responsible for the data of the owners - users.

User accounts

According to its Shared Responsibility Model, Atlassian is responsible for testing its entire platform for bad or malicious use. It means that if they notice some malware activity on the entire platform, they will inform their customers about it. Moreover, they are always developing their security controls, so that their customers can manage their users, tasks, and projects more efficiently. On the other hand, it is the user's responsibility to take care of his passwords and access, which is obvious, and, most importantly, monitor his company user accounts for malware activity. Thus, if something happens to the customer's data, it is an absolute user's duty to take care of it.

Applications

Following the Atlassian Cloud Shared Responsibility Model, the Atlassian Marketplace vendor should receive and manage all vulnerability reports that are related to its applications. But just like with all data, when installing add-ons to their Jira and Bitbucket accounts, the user should be aware that he is responsible for the data processed within these applications.

Data Protection, Backup and Recovery

We have already mentioned that due to the Shared Responsibility Model, service providers are responsible for their systems, hosting, and applications focusing on a macro level. However, when it comes to data protection at the account level, the user is responsible for data security and should be able to restore lost, stolen, deleted, or compromised data. In order not to be unfounded, let us quote fragments of such regulations:

Atlassian Cloud Terms of Service Check source

18 Warranties and Disclaimer.

18.4. WARRANTY DISCLAIMER. EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION 18, ALL CLOUD PRODUCTS, SUPPORT AND ADDITIONAL SERVICES ARE PROVIDED "AS IS," AND WE AND OUR SUPPLIERS EXPRESSLY DISCLAIM ANY AND ALL WARRANTIES AND REPRESENTATIONS OF ANY KIND, INCLUDING ANY WARRANTY OF NON-INFRINGEMENT, TITLE, FITNESS FOR A PARTICULAR PURPOSE, FUNCTIONALITY OR MERCHANTABILITY, WHETHER EXPRESS, IMPLIED OR STATUTORY. WITHOUT LIMITING OUR EXPRESS OBLIGATIONS IN THESE TERMS, **WE DO NOT WARRANT THAT YOUR USE OF THE CLOUD PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, THAT WE WILL REVIEW YOUR DATA FOR ACCURACY OR THAT WE WILL PRESERVE OR MAINTAIN YOUR DATA WITHOUT LOSS**. YOU UNDERSTAND THAT USE OF THE CLOUD PRODUCTS NECESSARILY INVOLVES TRANSMISSION OF YOUR DATA OVER NETWORKS THAT WE DO NOT OWN, OPERATE OR CONTROL, AND **WE ARE NOT RESPONSIBLE FOR ANY OF YOUR DATA LOST, ALTERED, INTERCEPTED OR STORED ACROSS SUCH NETWORKS. WE CANNOT GUARANTEE THAT OUR SECURITY PROCEDURES WILL BE ERROR-FREE, THAT TRANSMISSIONS OF YOUR DATA WILL ALWAYS BE SECURE** OR THAT UNAUTHORIZED THIRD PARTIES WILL NEVER BE ABLE TO DEFEAT OUR SECURITY MEASURES OR THOSE OF OUR THIRD PARTY SERVICE PROVIDERS. WE WILL NOT BE LIABLE FOR DELAYS, INTERRUPTIONS, SERVICE FAILURES OR OTHER PROBLEMS INHERENT IN USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS OR OTHER SYSTEMS OUTSIDE OUR REASONABLE CONTROL. YOU MAY HAVE OTHER STATUTORY RIGHTS, BUT THE DURATION OF STATUTORILY REQUIRED WARRANTIES, IF ANY, WILL BE LIMITED TO THE SHORTEST PERIOD PERMITTED BY LAW.

Atlassian, GitHub, or GitLab (and any SaaS) claims to perform system-level backups and disaster recovery operations in case of infrastructure failure, attack, etc. to ensure uptime and accessibility. But let's be clear – it's impossible for them to perform restores of each of their tenants' account data. Account-level recovery is non-trivial to develop and typically lies outside their responsibilities. That's why they require each tenant to protect their own data and

to avoid such expectations, most of them, including Atlassian, plainly state: “To avoid data loss, we recommend making regular backups.”

Checkmate.

PART 3

PRO Security tips for Jira Admins

Let's take a look at some interesting data from the *2021: State of the Atlassian Ecosystem Report*:

- Atlassian extends beyond IT teams – compared to 2020, there is a significant increase in tool adoption among non-technical teams, for example, operations (7%) or customer service (15%),
- 82% of respondents have embraced agile ways of working,
- 54% of organizations have implemented a DevOps strategy – up from 48% in 2020,
- 87% of respondents customizing their Atlassian tools.

Configuration possibilities within Jira

The above numbers should come as no surprise. Jira is a very flexible tool that has great configuration options. Agile boards, swimlines, specific workflows. We could talk about it for hours and discuss the best practices that can be implemented here. This is a good feature because, with the right motivation and knowledge, we can perfectly match the tool to the needs of our specific process. Here are some examples of things that we can build or define depending on our needs:

- JQL queries to filter issues for specific criteria,
- specific ticket statuses can be assigned to particular, columns,
- plugins and add-ons from Atlassian Marketplace,
- integration with external tools, for example, GitHub,

Confluence, Zendesk or Slack,

- proper access rights and assignments,
- customizable dashboards

With such a great number of configurations, transitions, boards, etc. comes the question of permissions and their control. After all, we don't want everyone to be able to freely change our process. First, we need to control who has access to our Jira account at all. And secondly, what privileges everybody has. Another thing that is important to mention is the fact that you can also use the mobile application, which on the one hand is convenient, but on the other hand, exposes us to additional risk.

Jira administrator responsibilities and duties

So, here comes a very responsible position called Jira Administrator. This software offers nice tools for managing user roles and restrictions to keep your process in shape. Let's start with groups and permissions. There are many default groups that we can use, but of course, we can create our own and assign appropriate permissions to them. Thanks to this, we can easily manage user access by assigning it to individual groups. There is also the project roles mechanism. It allows you to give users or entire groups appropriate roles that can also be used to control access and permissions.

Jira Administrator must properly broadcast and control what I described above. An important aspect, from the perspective of the security of our system, is also the control over inactive users and the removal of permissions (or users) in the event of, for example, a change in project, position, or departure of an employee from the company. Jira allows you to monitor user activity, and thanks to this, we can, for example, delete inactive accounts after a specified period of time. On the topic of permissions, I pay attention to some known issues that may cause an unexpected change in the visibility of a given project:

Source: Atlassian

Best practices for Jira Admins

Keep the standards

Define some standards and good practices and keep them alive. For example in workflows, there are statuses, transitions, and resolutions – keep them clearly defined and simple to avoid chaos and misuse.

Clean and tidy

Jira Admins should keep their instances simple and clean. To achieve that it is good to have a regular time-slot for maintenance activities such as:

- removing unnecessary items (like fields, transitions, statuses, etc.)
- cleaning up duplicate tickets
- checking consistency

Training

Jira is constantly being updated or some standards or good practices may evolve. Therefore Jira Administrator (and all the users) should know all the newest updates. Regular and short training sessions could be very beneficial in this case.

Cloud migration

As Jira is migrating to Cloud we should be prepared for that. It may cause some issues, like some add-ons compatibility/support, etc.

Appropriate preparation and support may be necessary. This is worth taking into account, especially about the previous point.

Automation

We all like automation. Jira Administrator is a position that requires it. Anyway, most admins already use a few add-ons to improve their work. One of the top-selling Jira apps in Atlassian Marketplace is ScriptRunner, which allows us to automate or customize our Jira. So let’s use such tools to boost our automation capabilities.

Minimalize downtime with backup and DR

The biggest so far 2022' Jira outage has affected hundreds of Atlassian’s customers and thousands of developers around the world. It may sound too obvious, but as a Jira Administrator, you need to take into consideration such a scenario and prepare your organization against alike incidents. The most logical action will be to implement a professional DevOps backup solution. Backup play a very important part, but don’t overlook the restore process – frequently test your Jira backups to be sure that the critical data is easily recoverable at any given time. GitProtect backup for Jira fully covers all your data protection needs and offers many restore options – instant restore, bulk restore, and point-in-time restore.

PART 4

Jira Backup Best Practices

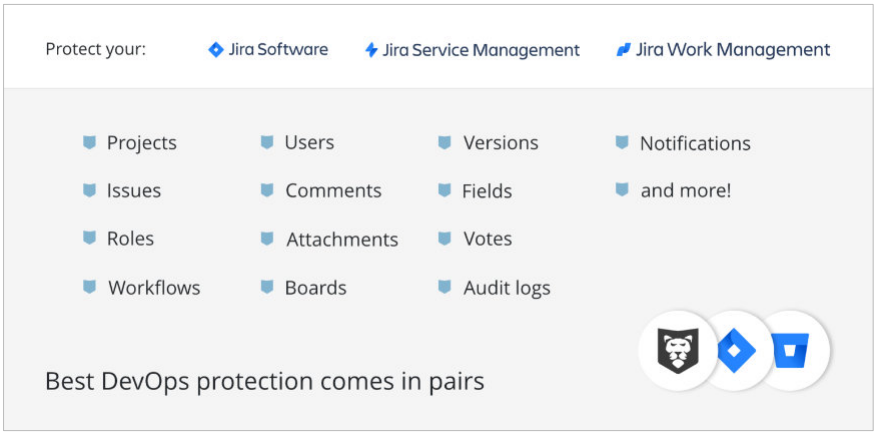
Jira data backup software allows you not only to eliminate or reduce the effects of data loss and cyber risks, but also, it relieves you of the burden of responsibility resulting from the shared responsibility model.

Now, let's take a look at the Jira backup best practices that will help you make even every issue easily accessible and quickly recoverable, so your team can work uninterruptedly in any event of failure and your organization saves hours of work, reputation, and customer trust.

Jira Backup Performance

Backup Jira data with full data coverage

When it comes to automated backup, you need to make sure that your Jira backup and restore software ensures you with full data coverage for all Jira Software, Jira Service Management, and Jira Work Management in any deployment model (SaaS or self-hosted).



It is always essential that your backup software gives you the possibility to set many customs and scheduled backup plans in only a few clicks, so that your data protection policy meets your organization's needs, structure, and workflow.

One of the best practices when it comes to Jira backup and data protection is the possibility to set a backup plan for some critical, current data that changes on daily basis (or even more often) and another one for some finished projects that basically don't change and need to be backed up only for the future reference or due to some policies. Sometimes to meet legal or internal requirements you need to keep all the data for 3, 5, or even n-years... your backup software should enable you to keep your copies longer than usual 365 days, even infinitely.

Storage optimization technology

In most situations, you need to back up only changed blocks of data since the last copy in a form of automated daily backups instead of making a full backup each time and burdening storage and bandwidth. For better backup efficiency you should have the possibility to create incremental and differential copies of your Jira data. Also, it is essential that you have the possibility to define different retention and performance schemes for each type of copy, among full, incremental, or differential opportunities.

Deployment of your choice: SaaS and On-Premise one

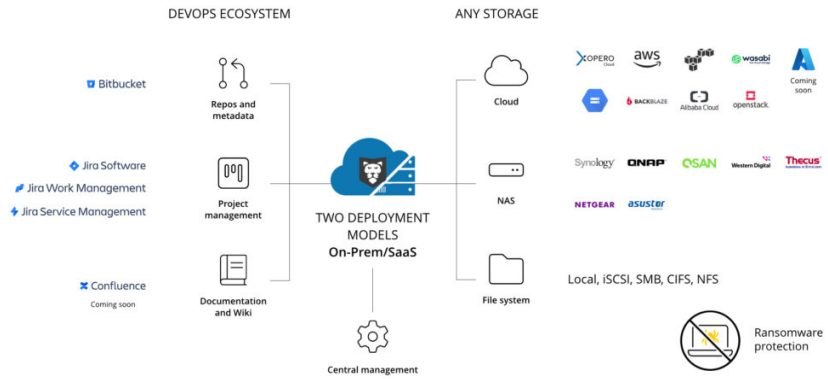
Just like most kinds of software, including the Jira instance itself, you should have the possibility to run your backup software as a SaaS service or install it on-premise, on your own infrastructure. The main difference here is the place where the backup service will be installed and running.

SaaS deployment means that the service is up and running in the provider's cloud infrastructure Thus, it is a backup service provider who is responsible for infrastructure, administration, maintenance, and the continuity of operation.

If you decide to choose on-premise deployment, you will need to

install the software on a machine you provision and control. You should have the possibility to install it on any computer (Windows, Linux, or macOS), and even on NAS devices. With this kind of deployment, you can reduce any network connectivity issues, and using the local network will make the backup more efficient and faster.

Please take note to not confuse the deployment model with storage capabilities. Regardless of the SaaS or On-Premise deployment you can assign as many storages as you want – cloud or local. GitProtect.io supports AWS S3, Backblaze B2, Azure Blob Storage, Wasabi Cloud, Google Cloud Storage, and any public cloud compatible with S3, on-premise storage (NFS, CIFS, SMB network shares, local disk resources), as well as, hybrid and multi-cloud environments. Additionally, together with a license, you get free unlimited GitProtect Cloud Storage as your primary or additional datastore for replication purposes.



Multiple storage instances and the 3-2-1 backup rule

With your Jira backup software, you should have the possibility to add an unlimited number of storage instances, preferably both cloud and on-premise. Why? First of all, to replicate backups between storages and have independent copies on at least two different data stores. It can help eliminate any outage or disaster risks and meet the 3-2-1 backup rule, according to which you should have at least 3 copies on 2 different data stores, one of which is in the cloud.

Due to the fact that GitProtect.io is a multi-storage system, you can add the following storages:

- Cloud: GitProtect Cloud Storage, AWS S3, Azure Blob Storage, Backblaze B2, Wasabi Cloud, Google Cloud Storage, or any other public cloud compatible with S3,
- on-premise: NFS, CIFS, SMB network shares, local disk resources,
- in a multi-cloud / hybrid environment.

It doesn't matter what type of license you have chosen, GitProtect Unlimited Cloud Storage is always included in a package for free, hence you may start protecting your data immediately.

Backup replication

Make sure to take backup replication criterium as one of the most important when deciding on backup and restore software for your Jira. Why? Because it let you have consistent copies in multiple locations and easily follow the 3-2-1 backup rule, ensuring better business continuity and uptime. Thus, it is vital to have the possibility to replicate from any to any datastore – cloud to cloud, cloud to local, local to cloud, or locally with no limitations.

Examples? Let's take a look at GitProtect. You can easily find and set a replication plan in the menu of the central management console. You just need to indicate the source and target storage, the agent if needed, a simple schedule, and that's it... your replication plan is ready!

Unlimited and flexible retention

Atlassian Shared Responsibility Model states very clearly that this is the user who is responsible for data protection of Jira data. And the concept of retention is inextricably linked to data protection. But you might need longer retention for your copies also due to other legal, compliance, and industry requirements. As we have already mentioned there are organizations that need to keep some crucial data for years. Nowadays Jira permits retention of only 3 years, but

depending on the data, sometimes you should store it much longer. What if you will need it for future references in your projects? Or when you consider your backup software for archiving old, unused data or meeting your compliance?

Thus, it is always great when you have the possibility to set different retention schemes for every backup plan by:

- indicating the number of copies you want to keep,
- indicating the tie of each copy to be kept in the storage (such parameters it's worth setting separately for the full, differential, and incremental backup),
- disabling rules, and keeping copies infinitely.

Monitoring center – email and Slack notifications, tasks, advanced audit logs

Maybe you are not the exact person who is responsible for managing backup software, but there is no doubt, you want to have a complex, customized monitoring center, so that you can monitor your backup performance, check on statuses, and if there is a need, to check on who is responsible for a definite change in the settings to control your team. Forget long-term managing backup scripts, DIY apps, manual backup, manual exports, and import.

Custom email notifications are one of the easiest ways to stay up to date. What is more, you don't even need to log in. All you need to do is to configure such settings:

- recipients (there is no need for you to have an account in the backup software to stay informed about backup statuses),
- backup plan summary details such as successfully finished tasks, tasks finished with warnings, failed tasks, canceled tasks, and tasks not started,
- a possibility to choose a language.

In an ideal world, it is great to get notifications directly in your software which you and your team use as a daily routine, right? So

let us introduce to you: Slack notifications. In this case, you have a guarantee that you won't miss any important information.

Ongoing tasks and historical events are other things you should be able to check. Thus, you can always turn to the tasks section, which will provide you with a clear view of actions in progress with detailed information. Thus, you will need just a second to check on running operations.

Advanced audit logs are another feature your Jira backup should provide you with. Such logs give you all the information about the work of applications, services, made regular backups, and restored data. What is more, it permits you to see which actions are performed by each member of the team and can prevent any intentional malicious activity.

If you want to make monitoring easier and non-engaging, it should be possible to attach those audit logs to your external monitoring systems and remote management software with the help of webhooks and API.

All the mentioned features should be accessible through one central management console which permits you to manage regular backup, restore data, monitoring, and all the system settings. With powerful visual statistics, data-driven dashboards, and real-time actions you will be able to greatly save your time. Can you imagine this with backup scripts? No!

Jira Backup Security

Jira backup software for SOC 2, ISO 27001 certification

The sharpest issue that worries the majority of companies nowadays is security. Now, let's think about your Jira – all information on projects, tasks, user notes, and more... – can you imagine losing access to this data and starting from scratch? That is the reason why your Jira backup should provide you with different security features that significantly ensure that your data is accessible and recoverable. Thus, it will permit your team to stay at the top of regulatory standards.

What security features should you pay attention to?

- AES encryption with your own encryption key,
- In-flight or at-rest encryption,
- Long-term, unlimited, flexible retention,
- SAML and SSO integration - compatibility with your IdP
- Easy monitoring center,
- Multi-tenancy, the possibility to add additional admins and assign privileges,
- Data Center strict security measures (more),
- Ransomware Protection,
- Disaster Recovery technologies.

User AES encryption in-flight and at rest

Proper and reliable encryption is essential when we speak about data protection. Thus, it is crucial for your data to be encrypted at every stage, in-flight, and at rest. In-flight encryption means that your data is encrypted on your device before it leaves your machine. Then it's encrypted during transfer and at rest, at a repository. These encryption levels give you a full guarantee that even if your data is intercepted, nobody can decrypt it.

Advanced Encryption Standard (AES) is another aspect your software should have. AES is a symmetric-key algorithm according to which you need to use the same key for both encrypting and decrypting the data. Due to the fact that AES is considered unbreakable, it is widely used by governments and organizations.

It's ideal when you can choose the strength and level of encryption. This process can be:

- Low, as it forces the AES algorithm to work in OFB (OUTPUFEEDBACK) mode. The encryption key here is 128 bits.
- Medium – the AES algorithm is run in OFB mode,

though the key is twice longer as it consists of 256 bits.

- High, which makes the AES algorithm work in CBC (CYBER-BLOCK CHAINING) mode with an encryption key of 256 bits long.

But note, despite the fact that all these AWS levels are considered unbreakable, depending on the chosen encryption method, the backup time can vary. Moreover, thus you can limit the selected functionalities and the load on the end device.

When you configure your encryption level, you should produce a string of characters, on their basis, your encryption key will be built. You should be the only person who knows the string and it's a good idea to save it in the password manager.

But what really makes your encryption strong is your own encryption key. Unlike other backup and restore providers, who set your encryption key, GitProtect.io enables you to create custom encryption keys to strengthen your data security.

Among other bonuses, you can use your own Vault. What does it mean? You will provide us with your key only when a backup is performed and you have a definite assurance that your control over access and credentials is stronger than ever.

Zero-knowledge encryption

Zero-knowledge encryption is an approach when neither your device nor your provider knows the encryption key, the only person who possesses this information is you by default. Thus, you, as a key owner, are able to decrypt it. So, if you are looking for really reliable backup software, make sure that it has all AES data encryption (and you can use your own encryption key) and zero-knowledge infrastructure.

Data Center (DC) region of choice

When you build your business as a security-oriented one, you should definitely know how your data is stored and managed. Your

backup software provider as well as the DC should meet your requirements, and location preferences. It can influence coverage, application availability, and uptime. That's why it is important to have a choice since you sign up. It's up to you to decide where to store your management service – in the US, EU or Australia.

Though, the main requirement should be compliance with strict security guidelines, standards, and certifications, including ISO 27001, EN 50600, EN 1047-2 standard, SOC 2 Type II, SOC 3, FISMA, DOD, DCID, HIPAA, PCI-DSS Level 1 and PCI DSS, ISO 50001, LEED Gold Certified, SSAE 16.

What other requirements should your DC have? Among them, there should definitely be mentioned physical security, fire protection and suppression, regular audits, and constant technical and network support.

SSO and SAML

To secure the authorization, authentication and access process in the highest possible way, your backup vendor should enable you to control authentication and authorization processes due to the integration with external identity providers - Auth0, Azure AD, Okta, CyberArk, or Google, using SAML (Security Assertion Markup Language) standard.

Sharing the responsibility for managing the backup system

Sharing responsibility among employees not only allows you to perform faster, but also increases your team morale and enables you to focus on a wider picture, and it doesn't matter what kind of business we take into consideration. What should your Jira backup and restore software let you do? You should be able not only to add new accounts, set roles, and privileges to delegate responsibilities to your team and administrators but also have more control over access and data protection.

All of that you can gain only if you have a central management console and can easily monitor and track the activities. You should know which actions were performed in the system and track who

made each of those changes. Hence, you can see the whole picture with the help of access to insightful and advanced audit logs.

Ransomware protection

Backup should be ransomware-proof, as it is the last resort in defense against ransomware. Why? Let's figure it out. Here you should remember how backup vendors process your data. GitProtect.io encrypts and compresses your data, and keeps non-executable copies on the storage. Thus, your data can't be executed and spread on the storage, even if some ransomware hits your backed-up data.

Also, it is worth mentioning that immutable, WORM-compliant storage technology which writes each file just once and reads it multiple times, prevents data from being erased or modified, thus it becomes ransomware-proof.

Usually, your authorization data for storage and Jira are stored in Secure Password Manager and, thus, the agent receives them only during backup if we mean on-premise instances. In this situation, if ransomware hits the machine our agent is on, there would be no access to authorization data and storage.

PART 5

Disaster Recovery and planning for business continuity

The moment when you need to choose the right backup and recovery solution for your Jira production environment, you need to check its Disaster Recovery technology. Why? Because it should respond to every possible data loss scenario. There are a lot of dangerous situations but, unfortunately, the majority of vendors provide you with recoverability only in case Jira is down. Here, are just a few words about the data restore options GitProtect.io offers you:

- point-in-time restore,
- granular restore,
- restore to the same or a new account,
- Cloud-to-cloud / Cloud-to-local restore
- restore to a free Jira account with a no-user recovery option
- restore to your local device.

Before we check on how GitProtect.io prepares you for every possible scenario, it's worth mentioning that with GitProtect.io you don't need any additional app, as it is a complete backup & recovery software for your DevOps ecosystem managed with a single central console.

1. What if Atlassian is down?

Loud Jira outages showed us that even in companies like Atlassian, outages happen. In such a situation, you need to urgently recover your data and ensure

What can it lead to? Hours when your team is out of work and,

consequently, a great loss of money. Thus, the situation when there is a Jira outage definitely needs urgent recovery. With GitProtect.io you can instantly restore your Jira production environment from the latest copy or a chosen point in time to your local machine, the same, or another free Jira instance.

2. What if your infrastructure is down?

In the situation when your infrastructure is down, for sure the best backup practice is the 3-2-1 backup rule. Under this rule, you should have 3 or more copies of your data on 2 different storage instances, one of which is in the cloud – that has already become a golden standard in data protection. GitProtect.io, being a multi-storage system, allows you to add an unlimited number of storage instances, including on-premise, cloud, hybrid, or multi-cloud. Moreover, the solution permits you to make backup replication between the storages. Another advantage is that you get free cloud storage when you need a reliable, second backup instance. Thus, even if your backup storage is down, you can be sure that it is possible to restore everything or just the chosen data from any point in time from your second storage.

3. What if GitProtect's infrastructure is down?

Data protection has become our normal data routine. Thus, we are always ready for any potential outage scenario, especially if it can harm our environment. In case our infrastructure is down, the installer of your on-premise application will be given to you. With it, you can simply log in, assign your storage (where you keep your copies), and get access to all your backed up data. Finally, you can use all data restore and Disaster Recovery options, which are officially supported and mentioned above.

Restore multiple projects at a time

There are so many situations when you need to restore your Jira. Which exactly? Downtime, service outage, bad actor's activity, and the list can be easily continued. Thus, Restore and Disaster

Recovery technologies take a crucial place in backup planning. Well, if you have a backup, you can restore your data without effort.

One of the easiest ways to do so is the possibility to restore multiple Jira projects at a time. Just pick up projects you want to restore, look for the latest copies and assign them... now you are ready to restore them to your local machine or another Jira account. So, your Disaster Recovery plan is easy, fast, and efficient.

No-user recovery option

Jira's billing model assumes that you pay for each user who uses the application. So you will probably look for a problem in the possibility of restoring users. In theory, restoring your entire environment could cost you twice what you currently pay – you need to have 2x more users, after all. Nothing of that. With the no-user recovery option, you have the possibility to restore all your Jira data except users to not overcome your current Jira pricing plan. Moreover, with this feature in place, you can restore your data to a free Jira account.

Point-in-time restore gives no limits

What is the most common reason for cybersecurity risks and data losses? Of course, it is a human error. It is difficult to predict where the risk is hidden – it can be intentional or unintentional deletion, all you should worry about is the result and consequences you get. As soon as you know the exact state and date you want to roll out, you will be eager to restore your data as fast as possible from a very specific and defined moment in time. Here it is worth mentioning that most backup vendors offer you to restore only the most recent copy, or the copy from up to 30 days prior.

Granular restore of only selected Jira objects

The bigger a supporter of Jira you are, the more you know that Jira does not ensure you with granular, point-in-time restore in case of unintentional deletion, human errors, and daily operations. So

that’s another reason why you need a third-party Jira backup software empowered with Granular Restore possibility.

Granular restore allows you to select the data you need to recover: any projects, issues, attachments, and workflows with their dependent elements. Regardless of the selected resources for restoration, your backup vendor should permit you to recover your Jira data to either the same or a new Jira account, or to your local device. Thus, you can instantly restore your lost Jira data in the blink of an eye without interrupting your workflow and with no need to restore your entire Jira ecosystem in one go.

Restore directly to your local machine

There is no doubt that you may prefer working on your Jira in SaaS, but you may want to restore copies to your local machine as well. All of that is due to cloud infrastructure downtime, service outage, or weak Internet connection. Thus, another Jira backup software should provide you with the option to recover your Jira account and all the related tools to your local machine.

C2C, C2P, P2C restore

The main motivation for running any backups is security. But backup is also a must if you plan to upgrade your system or

migrate from Jira Server to Jira Cloud (or conversely). Not only a must – it brings huge facilitation to this process. But whether you need it as a one-time activity (application migration) or you would rather generate a new Jira backup at regular intervals (daily, for example) and restore in case of a Jira outage, you should have the possibility to simply restore Jira data from Jira Cloud to Jira Server account or conversely.

Together with your project's growth, more and more important data and issues are added to your Jira boards or moved between them. As a result, your Jira account stores an increasing amount of critical data that needs to be reliably protected. Even Atlassian itself, in its Shared Responsibility Model rules, recommends having backup software in place when it comes to its products. What to wait for? Make sure to follow best practices.

GitProtect.io

by Xopero ONE