8 Tips to Make Your Atlassian Instances More Secure and Reliable

How secure are your Jira, Confluence or Bitbucket? Is your software reliable enough? Let's see useful tips that can improve security and reliability of your Atlassian software instances.

Do you really need external access to your services?

Of course, you should keep in mind the best practices that protect your servers and network, such as password policies, firewalls and so on. But think twice before opening access to your services through the Internet. Do your users really need to access the data outside the network? If so, you can improve security using the suggestions below:

- Consider using VPN out of the office instead of opening access to your applications from the Internet directly.
- Use the encrypted connections to improve security.
- Secure your employees' devices that can access your network (such as laptops, tablets, smartphones and so on).
- Use antivirus software, strong passwords, biometric authentication, smart cards, tokens, and two-factor authentication to make sure that only authorized persons have access to applications.

Use HTTPS instead of HTTP

There is no reason to use unencrypted HTTP connections because browsers mark them as insecure (and that's true!). Even in case you are on a tight budget, you can afford SSL for your services. Use free certificates from Let's Encrypt to protect your services. On the opposite side, it's more convenient to use the single wildcard certificate from a reliable certificate authority for multiple web services. Always redirect HTTP connections to HTTPS ones to maintain compatibility and security.

Also, make sure that your SSL connections are properly configured and secure. You can perform a quick check with a free Qualys SSL test online tool. If your service got a grade lower than A or A+, it's recommended to review encryption settings. There are examples of A+ rate settings for different platforms here and here.

Take care of your database

This can sound obvious, but it's a common practice to install an application and its database on the single host. Sometimes this can look reasonable (especially during evaluation) but it's better to split the application and the database to different hosts for production instances.

It's also better to use the encrypted connections between the database and applications if possible. Finally, you should check if the database and Atlassian applications configure sufficient database connections. This doesn't affect security but can affect stability of your Jira, Confluence or Bitbucket instance, especially during peak load times.

Remember to update your database because it is essential to your data security.

Keep your systems up-to-date

It's extremely important to have the latest versions of operating systems and software to avoid known vulnerabilities. Have you heard about the Heartbleed vulnerability? A bug in the open-source library OpenSSL caused this vulnerability. The only way to fix it was updating the OpenSSL library that was used for encrypting purposes almost everywhere.

If you need to keep your HTTPS as much secure as possible, you need TLS1.3 cryptographic protocol that requires to upgrade OpenSSL once again. In some cases, you must update your operating system to upgrade OpenSSL. Security is a reason to keep your infrastructure always up-to-date.

Atlassian applications also need ongoing maintenance and updates in order to keep performing well. This can be a challenging task for large enterprises, but there are two approaches (they can be combined) to make your upgrade process less stressful:

- DataCenter versions of Atlassian applications that allow you to minimize downtimes during upgrades.
- Enterprise releases that allow you to get the latest security updates for your Atlassian software without migrating to next major releases that should be thoroughly tested.

Back up your data

There is an old joke about two kinds of admins: admins who make backups and admins who **started to back up**. Backups allow you to restore your application after any kind of failures like external attack, hardware failure or human error. Your strategy may depend on requirements of your business but main ideas are:

- Know your stack of technologies. You may run Jira, Confluence, and Bitbucket on Linux or Windows, using AWS or your own datacenter, using bare metal hardware, virtual machines or Docker environment. Each installation has different strategies of making backups.
- Feel free to use advantages provided by your environment (like LVM snapshots, VM snapshots and so on) to minimize the impact on the availability of services.
- Back up your database as well as the Atlassian application's home directory.
- Don't forget to add other important settings to your backup (reverse proxy settings, SSL certificate, firewall settings and so on).
- Check your backups and restore procedure on a regular basis to make sure they help you when a real issue happens.

Good backup allows you to restore your service literally in one click in a reasonable amount of time.

How to prevent DDoS and brute force attacks

You lose money when your service is down or you can lose your data (and even the whole business) when hackers break into your system. As Atlassian applications are extremely important for businesses, you need to make sure that they have adequate protection against DDoS and brute force attacks.

You can tune up your reverse proxy or choose a solution from your hosting provider to get rid of DDoS. Atlassian applications also have built-in protection against brute force attacks – feel free to activate captcha for failed logins. As an alternative, you can choose an app to implement two-factor authentication for Atlassian software.

Use your existing user directories and groups for managing users in Atlassian applications

Do you have LDAP directories (Active Directory, OpenLDAP, Microsoft Azure AD and so on)? Use them to authenticate your users in Jira, Confluence, and Bitbucket. This allows you to reduce the number of passwords for users and reduce the administrative burden as well.

Also, it's a good practice to use groups to give access to spaces in Confluence (or to projects in Jira and Bitbucket). This way you can simplify administration and reduce the number of errors. For example, disabling a user that leaves the company in the Active Directory will make it inactive in Jira, Confluence, and Bitbucket as well. However, you may forget to disable it somewhere if you need to disable the account in a few applications.

Perform security reviews and penetration tests on a regular basis

It's a good practice to make security reviews at least once a year. This can be a simple checklist or you can order a full review and penetration test from a consulting agency. The main points are:

- All the issues found during the review must be fixed.
- Make reviews on a regular basis.
- Maintain the documentation related to your services relevant. Update it after each review.
- It's a good practice to review your security and reliability after any failure.

An alternative way to improve security and reliability of Atlassian applications

Ask us! Tell us about your company. Show us how you use Atlassian applications for your business. Get personal recommendations and help with checking and implementing them.