CONTEGIX®

The Hero's Guide to Atlassian Management

A Practical Guide for the Busy Atlassian Manager

contegix.com 877.289.0395 sales@contegix.com

Table of Contents

Being your company's Atlassian Administrator is no easy task. Contegix understands. We know all the ins and outs, and we want to share them with you! This eBook will cover everything you need to know to be the company hero.

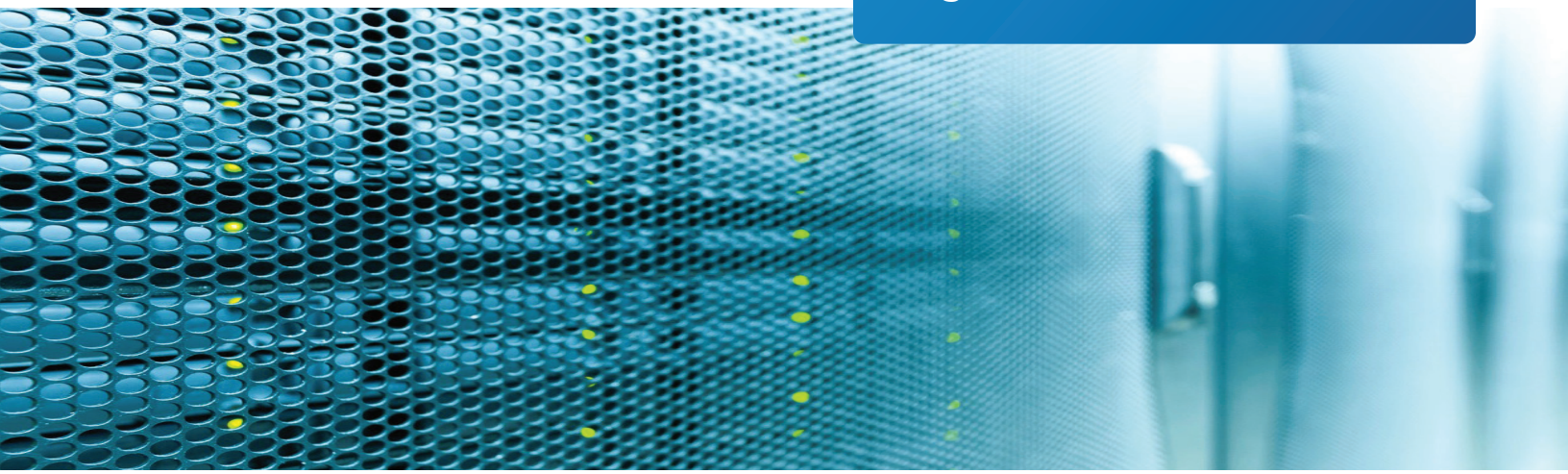
© 2020 Contegix, All rights reserved.

The Typical Atlassian Environment

Atlassian Cloud Version

Your environment is suitable for the Atlassian Cloud if your needs are simple and you have low user count. For instance, this option may suit your needs if your company doesn't have customization needs or compliance regulations.

Your user base and any security or data compliance needs you have are the most common factors that dictate which type of environment your organization needs.



Server and Data Center Versions

The server version of the Atlassian apps can be used a number of ways: on premise, on a public cloud (like AWS), or through a hosting provider like Contegix. This option gives you greater flexibility overall, and customizations and plugins cease to be an issue. It also allows you to increase your user count without fear of losing performance.

The data center version is largely similar to the server version. While the core functions are the same between the two, data center has more features around usage like built-in single sign on and easier archiving options for projects. The biggest advantage to the data center version is in the infrastructure set up. With data center, your applications are split between different nodes which allows for 100% uptime while updating/upgrading. If one thing goes wrong it doesn't take down your whole application.

The server and data center versions are required for those companies who have strict compliance needs. For instance, companies that must comply with HIPAA or FedRAMP regulations cannot meet increased security demands with the cloud version.

© 2020 Contegix, All rights reserved.

Using Monitors to Optimize Your Instance

Monitors are the first way to make yourself the company hero. If you monitor your suite correctly, you can guarantee optimum performance for your users. Here's a few of the key things you can monitor:

Availability

Simply put, is the app running or not? It seems like a no-brainer, but you don't want to be notified of an outage by a user. It's a lot better for you to notify them and let them know you are already aware of a problem and working on a solution.

Performance

You should always be aware of operational health. Noticing drops in performance will allow you to identify the cause of the drop and quickly resume normal working order before it crashes (avoiding bigger problems).

Random Access Memory (RAM)

You will want to monitor your RAM to ensure it's not at a dangerously low level. If it is, you can identify the culprit and preemptively make adjustments. If a plugin is consuming your RAM, it can cause crashes during spike usage. Bad plugins or poorly integrated customizations can also leak memory that can cause runaway processes and application instability.

Central Processing Unit (CPU)

Monitor your CPU. If you have sustained high CPU utilization periods or unexpected spikes, it can cause your apps to crash.

Java Virtual Memory (JVM) /Heap

We highly suggest A/B testing. Monitoring these closely will give you the insight you need to optimize these attributes to maximize performance and stability. You can raise or lower it to see what works best with your environment.

© 2020 Contegix, All rights reserved.

Determining The Best Back Up & Recovery Approach

RTOs & RPOs

Unless you have compliance requirements, begin by defining your Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). What is your tolerance for loss of data and loss of service? Once you have defined these, you can determine which method of backups will work best for your needs. Particular compliance requirements will likely dictate your RTOs and RPOs, and thus, your back up and recovery approach.

Resources

Next, ask yourself if you have the right resources to restore from a backup. Some people think backups are enough, but if you do not have a clear-cut process and tools to restore those backups, what's the point? You will never meet those RTOs and RPOs.

Diversity

A disaster is pretty much anything affecting your production environment, outside of planned maintenance. Therefore, your recovery approach must be diverse. Plan for a variety of different scenarios. Will it work in the event of a fire, power outage, tornado, etc.?

© 2020 Contegix, All rights reserved.

Disaster Recovery for Worst Case Scenerios

DR Runbooks

A DR Runbook is your playbook on how to declare a disaster and the steps that follow declaration. Again, it's important to remember each disaster will require a different approach to restore critical business systems. Nevertheless, the primary goal must be restoring your company's ability to serve customers and generate revenue. In some situations, it may be a better decision to focus on restoring the production environment vs. bringing the disaster recovery location online. However, the best approach is always a parallel resolution path if you have the available staffing.

> Our best advice to plan for worst case scenarios is enhancing the previously mentioned back up and disaster recovery plan. Develop runbooks and TEST to be prepared!

Test! Test! Test!

Never assume that your plan is perfect. Test thoroughly and regularly. Your data changes and so does the technology used for backups and recovery. This can change your process drastically, and you do not want to wait until a disaster to discover this. You can also start to think about what steps, if any, you can automate. Either way, remember that you must keep any scripts and documentation current as the environment changes.

© 2020 Contegix, All rights reserved.

User Control

User control is very important, and is an often-overlooked task when a company decides to take on the Atlassian suite. These apps are diverse and offer a wide range of permissions at many levels. There are a number of things to consider, but start with these three:

Managing Users

How are you determining user permission levels? It's important to limit the number of Global and Project Admins. Not many people should fit the criteria you choose for these rules. Limit who can make sweeping changes to your apps, projects, underlying infrastructure, and support services. Your hosting provider can't tell you who your admins should be, but they can work with them to ensure those that you assign Admin access can make proper requests to our support team with authority.

Permissions

Confluence, for instance, has many different levels of permissions. You can limit access to spaces to include only certain people. Then, you can further restrict individual pages. Be sure to identify these appropriately and assign admins for those areas to control users.

Secure Authentication & Single Sign On

Since many Atlassian users utilize multiple tools, it's common to see a Single Sign On (SSO) tool with Secure Authentication. In fact, Atlassian offers Crowd for this. Some other options are Lightweight Directory Access Protocol (LDAP) tools and Active Directory (AD). Third party Security Assertion Markup Language (SAML), Two-Factor Authentication (2FA), and federated authentication sources can also be integrated, depending on your needs and requirements.

© 2020 Contegix, All rights reserved.

General Security

Today, security is probably the most important part of setting up your applications. A breach or hack can ruin your reputation, slow productivity to a halt, and cost your business big. Security, like DR, is not a checkbox. It is complex, and evolves with your business needs. Here are three inportant topics to make sure you have covered for your apps.

How much security do you need?

Start out by asking yourself how much security you need. Compliance requirements will dictate specific needs, and you should always start there. However, if your compliance needs are not spelled out, start with your basic security needs. If you are only running a JIRA instance to plan each meeting of the Contegix Fan Club, your security needs are not going to be as extensive as a Fortune 500 company.

What is the cost of a data breach?

Similar to security, the answer to this question is different for everyone. If you are only working on test and dev, then a breach may not cost you any more than a little aggravation. On the other hand, if someone hacks the wiki that holds your customer, employee, and other private data, it could be devastating to your company.

Effective and timely off-boarding

When an employee goes rogue or leaves the company, effective and timely off-boarding is a must. Assume that every minute this individual has access to your apps is equivalent to a stranger who has breached your system. The best way to guarantee access is revoked as soon as possible is to have a thorough procedure and reliable staff you can delegate this task to, at any time.

FedRAMP

Did you know Contegix is Atlassian's only FedRAMP-authorized provider?

Our FedRAMP authorization means improved trustworthiness, reliability, consistency, and quality for your Atlassian stack.

© 2020 Contegix, All rights reserved.

Atlassian Version/Plugin Upgrades

These are some of the biggest pain points for any Atlassian Administrator. It's not uncommon for an organization to be 4 versions behind because upgrading can be so problematic. Here are our top 4 tips to make upgrades less intimidating:

Don't "Do it Live!"

This may be common sense, but many organizations are operating without a testing environment for upgrades. Upgrades can adversely affect an app in many ways, especially those with plugins. If you don't already have a test and dev environment, create one. NEVER DO IT LIVE!

Bleeding Edge versus Seriously Stable

When it comes to application versioning, you'll have a decision to make. Do you want to be on the latest and greatest version? Smaller, fast-paced teams often go this route. More conservative teams may upgrade versions only once a year (or even less). Our recommendation is to remain a couple point revisions back to avoid being affected by new release bugs or zero-day exploits.

On the other hand, infrequent updates can also lead to apps that become "end of support." Some hosting platforms automatically upgrade you to the latest version, whether you want to or not. Most do not let you choose when the updates happen either. This could be risky and invasive for your team. Ultimately, corporate policy and your comfort level as an administrator will help you choose the right mix.

How to Test Upgrades

After the upgrade is complete, you're now tasked with the rigorous review process. You must thoroughly test EVERYTHING. You should be looking for any obvious program errors, corrupted/missing data, or any other oddities that come up. Once you're satisfied with the results of the test migration, you can schedule the final cutover. Retrieve fresh backups of your instance and make the final cutover. Now you must examine the instance again, making sure everything looks as expected and meets your needs and expectations. Troubleshoot any problems you find.

Successful Regression Strategies

Backups are key here. Be sure that you make a fresh backup before you begin your upgrade, and another before you push your update live. The unexpected does occasionally happen, and a modest amount of caution and best practice planning can go a long way to preventing outages, downtime, and potentially data loss.

© 2020 Contegix, All rights reserved.

About Contegix

Our Story

Your digital applications power your business. Customers and employees expect you to deliver user-friendly, fast, and delightful digital experiences. At Contegix, we understand how critical these apps and the underlying cloud infrastructure are to your success. You need to move quickly, and you can't afford to worry about maintenance, upgrades, downtime, and other system issues. That's why we built our business.

Contegix was founded in 2002 as Atlassian's primary hosting partner and added consulting services to help Atlassian customers customize their toolsets. From there, we expanded our capabilities to support content management systems (CMS), and through our BlackMesh heritage, we have been managing a multitude of mission critical and highly trafficked websites in the world for the last 16 years. We also added extensive Service Desk capabilities, extending support to your end users, ensuring a great experience.

You're Unique. We Get it.

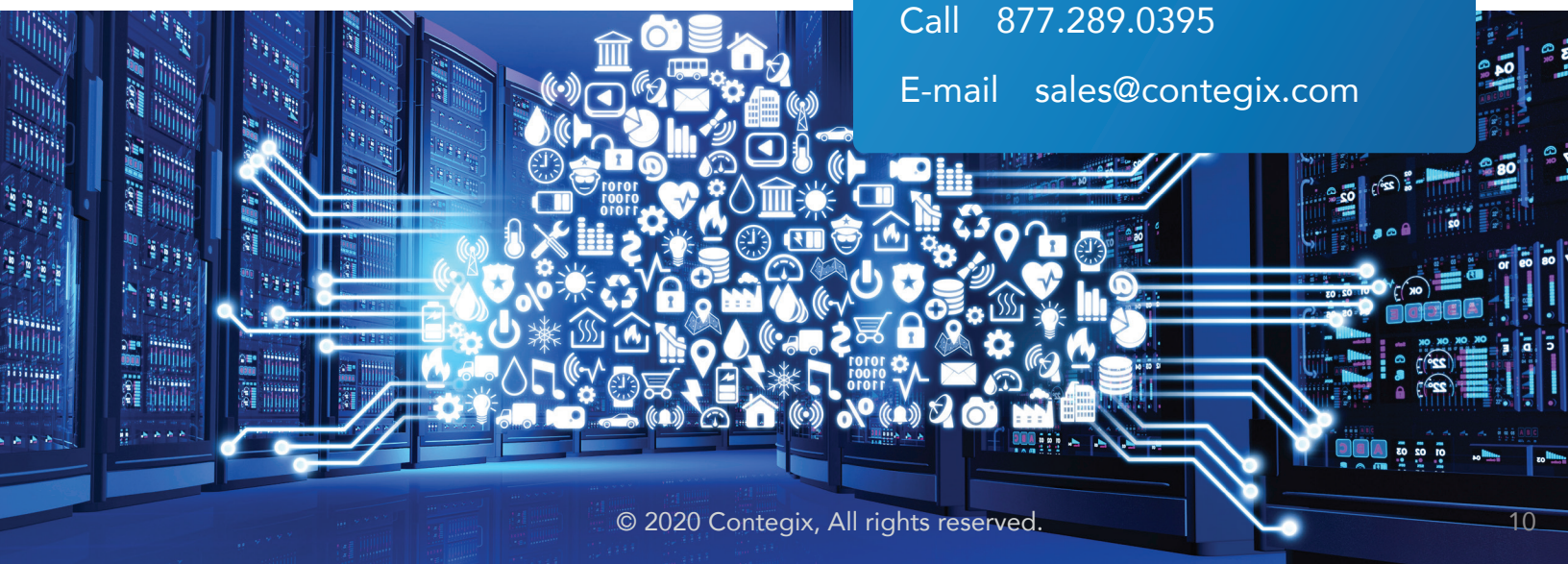
We understand the complexity of your unique applications, and that's why the industry's most sophisticated Drupal, WordPress, and Atlassian users work with us. We start by offering "concierge-level" application hosting with proactive, personalized support you won't find elsewhere. Then, we partner with you to advance and future-proof your apps, integrating into your team and advising you on best practices.

Our depth of expertise in CMS platforms and the Atlassian toolset paired with our FedRAMP authorization allows us to support and optimize the most complex and secure environments.

Visit contegix.com

Call 877.289.0395

E-mail sales@contegix.com



© 2020 Contegix, All rights reserved.