Unboxing Cloud

How we organize continuity and security in the BlueSpice Cloud

Markus Glaser, Hallo Welt! GmbH

www.bluespice.com
Agenda

• Backup
• Security
• Continuity
• Disaster Recovery
Backup - Purpose

• Ensure general operability
• Protect against data loss in disaster scenarios
  • Data center outages
  • Service outages
  • Spam and hacker attacks
• Meant to recover whole instances, not individual files
• Only for use by Hallo Welt!
Backup - Schedule

• All data (database, files, configuration) is backed up hourly
• All running data of the infrastructure is backed up hourly
• We keep
  • Last 4 hours
  • Last 7 days
  • Last 3 months
• All backups are created automatically
Backup - Safety

• Stored in two physical locations, both located in Bavaria
• Sync to second location is done daily
• Backups are stored encrypted
• We use a backup manager for this
Backup - Restore

• Backups can be restored on demand
• Restoration is semi-scripted
  • Depending on the root cause of the restore request, there may be different tasks to be done
• Restoration takes about 15 minutes
  • Secondary data has to be rebuilt
Customer accessible backup

- On request, we can provide a daily backup file
- You will get access to a NextCloud file store
- Backup is delivered on a daily basis and can be downloaded from there
Data retention on contract termination

- Instances cannot be deleted directly
- First step: archive
  - Instance is taken offline
  - Data is put to an archive
- Second step: deletion
  - Archived data is deleted after 4 weeks or earlier upon request
- For evaluation wikis, retention period is 1 week
Security
Security – Access control

• Access to infrastructure means access to all data
  • Managed centrally
  • Access is only granted to very few admins after management confirmation

• Access to individual instances
  • Hallo Welt! does not have access to your instance by default
Security - Encryption

- Data at rest
  Stored on an encrypted block storage
- Data in transit
  All traffic is secured
- Data in action
  No encryption possible
Security - Operational

- All external traffic is terminated in a loadbalancer
- Access is regulated by firewalls
- Various networks for different purposes
Security - Logging

• All operations on instances are logged
Security – Development

- Trivy security checker for docker images
- Security checks on BlueSpice code
  - Check 3rd party libraries on a daily basis
- Strict code review
Excursus: Handling BlueSpice vulnerabilities

- Hallo Welt! participates in the CVE program
- We are a CNA for BlueSpice
- Disclosure policy: https://bluespice.com/filebase/vulnerability-disclosure-policy/

<table>
<thead>
<tr>
<th>Release name</th>
<th>Release date</th>
<th>Title</th>
<th>References</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSA-2022-01</td>
<td>2022-01-31</td>
<td>XSS attack vector in Search Center</td>
<td>CVE-2022-25096</td>
<td>JavaScript in search field is reflected back to the browser.</td>
</tr>
<tr>
<td>BSSA-2022-02</td>
<td>2022-11-13</td>
<td>XSS attack vector on regular pages</td>
<td>CVE-2022-25118</td>
<td>Arbitrary HTML injection through the 'title' parameter</td>
</tr>
</tbody>
</table>
Excursus: GDPR

- Due diligence process when choosing service providers
  - Selection process and GDPR compliance is assessed and documented
- Focus on European based providers
  - BlueSpice Cloud is hosted in Germany at Hetzner
  - Mail service is provided by MailJet
Continuity
Continuity - Monitoring

- Basic server params like CPU, memory, network, disk space (Zabbix)
- Performance of one reference system (Zabbix)
- Automated tests in one reference system (Selenium)
- Current service status can be seen on [https://status.bluespice.com](https://status.bluespice.com)
Continuity – QA system

- Cloud has 3 almost identical systems
  - DEV for development
  - QA for pre-testing
  - PROD for production
- All changes must be deployed to QA before they go to PROD
  - This includes infrastructure as well as product
Continuity – Technical measures

• Self-healing setup
  • Docker swarm is set up to restart services if they are stale

• Redundancy
  • The swarm consists of several machines
  • Fail-over mechanisms ensure a service is moved if one machine goes down
  • This also allows for planned maintenance of the servers
Continuity – heavy standardisation

- All cloud instances are set up the same
- All operations on instances are scripted and reproducible
- We do have an API for allowed operations
- Standard operations are only done through management interface
Continuity – Knowledge transfer

• All personal skills are held redundantly
• All changes to the cloud are peer reviewed
• Critical operations are done in team sessions
• We will increase our team by July
Continuity – Cloud operations handbook

• We are a wiki company!
• All operations are documented
• Architecture is documented
• Troubleshooting is documented
Disaster recovery
Desaster recovery – Restoration plan

- Documentation in our Cloud operations handbook
- Continuously updated
Disaster recovery – Test recoveries

• Various outages and their effects were tested in DEV and QA
• Re-creation of the whole swarm was proven to be possible
Get in touch

Your contact: Markus Glaser
Hallo Welt! GmbH • Postfach 11 02 19 • 93015 Regensburg

Email: markus.glaser@bluespice.com
Phone: +49 (0)941 660 80 0

www.bluespice.com
www.hallowelt.com
Image credits

- [https://freesvg.org/prague-astronomical-clock](https://freesvg.org/prague-astronomical-clock), CC-0
- [https://freesvg.org/encryption](https://freesvg.org/encryption), CC-0
- [https://pixabay.com/de/photos/access-control-chip-125khts-1901327/](https://pixabay.com/de/photos/access-control-chip-125khts-1901327/)
- [https://de.m.wikipedia.org/wiki/Datei:Enigma_%28crittografia%29_-_Museo_scienza_e_tecnologia_Milano.jpg](https://de.m.wikipedia.org/wiki/Datei:Enigma_%28crittografia%29_-_Museo_scienza_e_tecnologia_Milano.jpg), CC-BY-SA 4.0
- [https://commons.wikimedia.org/wiki/File:Rockefeller_University_Disaster_Plan.jpg](https://commons.wikimedia.org/wiki/File:Rockefeller_University_Disaster_Plan.jpg), CC-BY-SA 4.0