Route Manager by WORKWAVE

Route Manager Data Security FAQ

SOLUTION ARCHITECTURE

1 Do you host the solution in-house or contract out for hosting?

Our solution is managed by WorkWave employees, leveraging the hosting infrastructure and services of Amazon Web Services.

2 Does the primary datacenter use an N+1 configuration for high availability/redundancy? What about the redundant data centers?

Our servers are located in two different availability zones in the same AWS data center, and data between databases is constantly synced. In the event of a server failure (up to a full data center outage), traffic is automatically re-routed to the other AZ. We are currently in the discovery phase to improve this configuration to add more servers in different, geographically distributed data centers.

3 How does the solution scale as workloads grow or shrink?

We have metrics to automatically check the servers' load and usage; if those metrics indicate a decreased availability of resources, we implement the servers' capacity accordingly in order for our systems to be functional and available to all our customers.

4 Is the process of growing and shrinking automatic?

Not yet, but we are working on a solution that automatically spins new servers (and shuts them off) based on the current workload.

5 Is the solution Multi-tenant?

Yes.

6 What is your disaster recovery plan?

High-availability load balancers redirect traffic to operating servers within the same data center. In the case that an entire data center becomes unavailable, DNS fallback redirects traffic to data centers in different geographical regions. Data is protected via AWS RDS Multi-AZ high availability (https://aws.amazon.com/rds/details/multi-az/). WorkWave also leverages automatic RDS backups to further protect against data loss.

7 What is your Recovery Time Objective (RTO)?

- Total failure of one availability zone in the AWS region: 2 minutes (standby automatically promoted to primary in a different availability zone).
- Whole region failure: up to 6 hours.

8 What is your Recovery Point Objective (RPO)?

- Total failure of one availability zone in the AWS region: 2 minutes (standby automatically promoted to primary in a different availability zone).
- Whole region failure: up to 24 hours (daily backup).

9 How do you backup customers' data?

- Backups occur every 24 hours.
- Backups are encrypted on each host using asymmetric cryptography.
- The private key is not stored on the hosts.
- After encryption, backups are archived on a secure, durable, redundant and geographically distributed storage system and deleted from the host server.

10 Are the backups stored off-site?

Yes, multiple sites (automatic redundancy provided by the cloud storage provider).

11 If the backups are stored off-site, where are they stored and how are they transported?

Amazon, transported internally within the cloud storage provider (Proofs of Delivery and customer-uploaded data) Amazon S3, through encrypted AWS sync.

12 Are backups encrypted?

Yes.

13 How often do you audit your off-site backup solution?

Monthly.

14 Do you test that the backups you take are actually reliable and can be used to restore the system in the event it becomes necessary to do so?

Yes.

15 If we decided to terminate the contract, how will we be able to get our data back?

You may request an export of your data, that will be provided as a JSON file + ZIP files of your Proof of Deliveries (if any).

16 What happens to all of the customer data that has been backed up when the contract is terminated?

Deleted after 35 days; it can be deleted immediately if requested.

17 What are the different methods that can be used to integrate your solution with other external solutions?

REST API.

18 What programming language(s) are used by your developers to build your solution?

C, C++, Java, Groovy, Javascript, TypeScript.

Please note that our solution is cloud-based and as such the programming languages could change at any time, and do so without any discernible impact on customers.

19 Can we customize the application to suit our needs? If so, how?

- Our UI and our mobile app are not open to customizations, but completely custom UI and mobile apps can be built on top of the exposed REST API.
- We do take requests from our customers on features and evaluate them seriously.

SYSTEM MAINTENANCE/ADMINISTRATION

20 How is the back-end of the solution managed and who is involved in the administration process?

- Account passwords are stored as a one-way salted hash (NOTE: Does not currently apply to drivers' mobile app passwords).
- Best practices for server lockdown are followed (principle of Minimum Access).
- IT/Ops department has Server Access to apply security patches for the OS and technology stack components (front-end server, database, JVM, etc.).
- Support team members can access the user's data only if users grant permission by opening a support ticket. Support team members can access the backend Control Panel where they can see: contact details, last login, and account licensing parameters.
- The Accounting department can access the backend Control Panel only to activate, deactivate, or suspend Accounts; they can see: contact details, last login, and account licensing parameters.

21 What is your policy on applying software patches to all levels of the software and operating system stack?

Upgrades and patches are applied internally as needed with no planned downtime at least once a week, or immediately in case of important security patches. Updates and patches are applied to and verified on the internal test environment. Proactive monitoring and smoke testing are in place to ensure upgrade success.

22 How often are new versions released?

We rely on a continuous delivery process. Fixes and new features are made available after passing the testing process.

23 How and when do you perform the upgrades?

We rely on a continuous delivery process. Fixes and new features are made available after passing the testing process.

24 Can you provide the customer with a product roadmap?

Yes.

SYSTEM SECURITY

25 Does your company certify its security environment against an industry security standard (ISO 27001/2, NIST SP800, COBIT, etc.)?

- At Application, Administration, and Operations level WorkWave follows ISO27001 best practices, but has not pursued formal certification.
- Cloud infrastructure: WorkWave relies on Amazon's certifications of physical security and access to underlying hardware that hosts our VMs.

26 Does the application use 128 bit encryption or greater?

Yes.

27 Please describe the physical security of your primary and redundant data centers.

Handled by Amazon: https://aws.amazon.com/compliance/data-center/controls/

28 Has your system ever suffered a security breach? If so, please provide details of the occurrence.

No.

29 Is remote server and network administration controlled through two-factor authentication?

Network and physical servers administration is controlled through two-factor authentication, remote server access is handled via private key only.

30 Who has physical access to the servers?

Please refer to this document: https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

31 Is system security monitored by your company, or the hosting company if used or by a third-party?

WorkWave is primarily responsible for security monitoring. Amazon continuously monitors network traffic for evidence of possible security breaches. WorkWave responds to all incident notifications, whether internally or externally generated.

32 What security systems are monitored?

WorkWave leverages the AWS GuardDuty IDS system for monitoring and protection against security incidents. All cloud operations activities are logged via AWS CloudTrail. Additionally, log data is centrally stored in an ElasticSearch/Kibana system for review and auditing.

33 What is the response procedure in the event of an identified attack or compromise?

WorkWave maintains an active Security Committee which defines security incident response procedures. In the event of a breach, the high-level procedures are to analyze the incident to understand the nature of the breach, isolate any resources suspected of compromise, preserve and collect data from suspect systems, contain the breach, eradicate the root of the incident, recover systems and follow-up to review the response and performance of the incident response team. WorkWave Legal evaluates all suspected security incidents to assist with customer and legal notifications.

DATA SECURITY

34 Do you store data? What information is being stored?

- We keep order information in our AWS servers and work within the AWS environment.
- All data around orders, such as Customer Name, Address, Phone Number, Email Address. The information is stored on our AWS servers for 13 months.
- Separately, this data is fully encrypted before it is sent to our servers.

35 What data security measures do you take around customer data?

- The WorkWave Route Manager product works within the AWS environment.
- All connections between the client application and WorkWave Route Manager API's are managed by the load balancers in AWS.
- All connections between clients and load balancers, load balancers and servers, and servers and databases are encrypted.
- We use authentication based on API keys, which are encrypted within the Payload of communication between clients and the WorkWave Route Manager servers.
- The security policy we use is called "ELBSecurityPolicy-2016-08" and more information can be found: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html

36 Is the customer data accessible by third-parties either on-site or at a third-party's site?

No.

37 If the customer data is found possibly compromised, what are the procedures that are followed, including the customer notification?

- Emergency lockdown is handled by our Support team and can be initiated either internally if a breach is discovered by either automated tools or periodic data/log reviews, or as a result of a customer request.
- Extent of the lockdown varies based on the severity and nature of the breach from single-account lock-down to full-service lock-down.