Ocean Digital

Ocean WiFi

Security Overview

25.11.2017

Contents

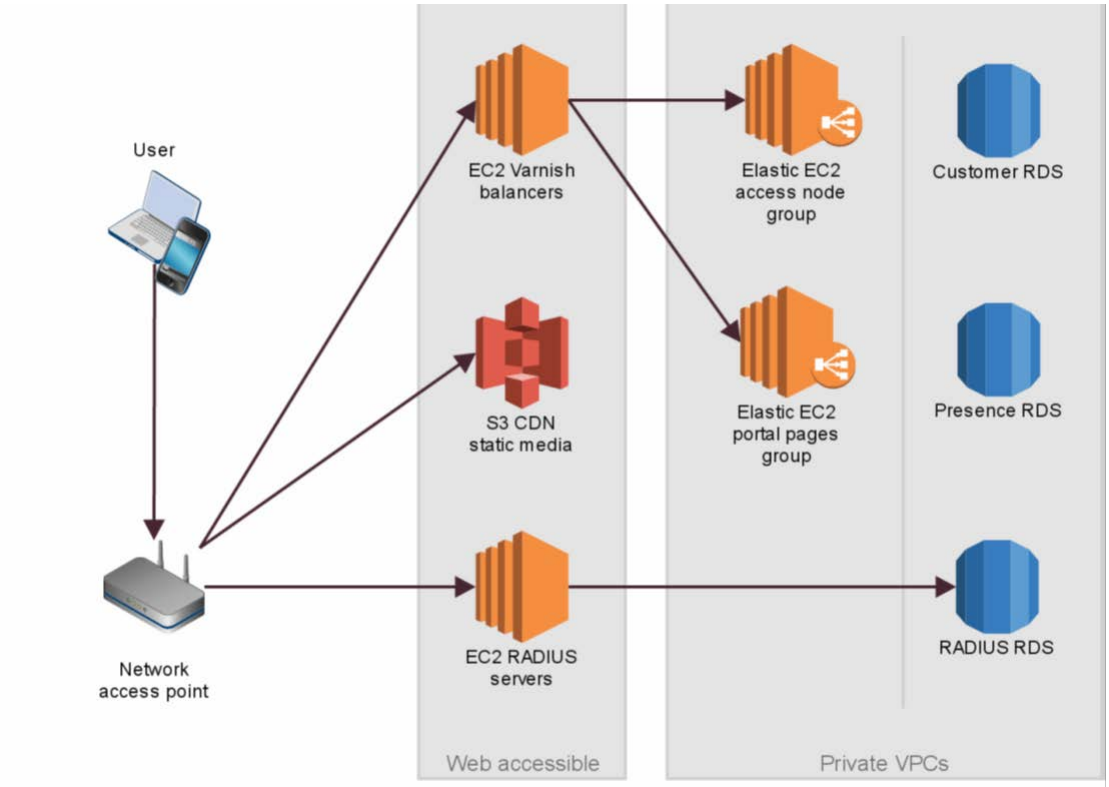
Commercial in Confidence

This document is Commercial in Confidence. The recipient of this document agrees to hold all information presented within as confidential and agree not to use or disclose, or allow to use or disclosure of the said information to unauthorised parties, directly or indirectly, irrespective of the acceptance or rejection of the document or at any time before, during or after an agreement has been reached, without prior written consent.

Security Overview

Ocean WiFi is hosted entirely on AWS, using the following services: EC2 for instances, VPC for network isolation, ELB for deployment and elastic scaling, S3 for static content storage and CDN, ElastiCache for application caching, SES for email delivery and SQS for message queueing.

Below is a basic web-facing infrastructure diagram:



The AWS security group default policy denies all access to any new server and access is opened strictly as required by port, source and destination.

Different elements of the platform (e.g. production vs development and test environments) are allocated to independent VPCs. Only systems that need to be web-facing are placed in an internet visible VPC and access is opened strictly as required by port, source and destination.

Ocean Digital utilises AWS IAM with granular permissions to ensure components have distinct security roles in line with least privilege principles. For example, SQS queues have different user roles for applications that write to the queues and retrieve from the queues.

User and application security roles are reviewed quarterly and on change. Any changes to security roles are requested by raising a ticket and are approved by the appropriate owners. Ocean Digital follows all AWS best practices for cloud security as documented by Amazon, where applicable for our solution and the services we use.

Data and Data Security

Captive Portal

When a user joins an Ocean WiFi SSID and reaches the splash page, their device MAC address and user agent are stored. When a user logs in via the WiFi, any user data they provide is also stored against their profile. The exact data collected varies according to the login method chosen and the configuration created by the customer, but can include PII data (see PII on page 6), as well as other potentially sensitive information (when combined with a user's PII) such as a zip/postal code or Facebook likes. This data is either user-submit via form, or transferred from their social media account if they grant access. Data in transit via the captive portal is secured via SSL.

If configured by the customer, Ocean WiFi may additionally collect domain lookup data via Cisco OpenDNS Umbrella service. Domain lookups are logged against the venue's web-facing IP and aren't traceable to an individual user.

Once a user is connected, RADIUS accounting data should be passed from the network controller to Ocean Digital's RADIUS servers, providing basic network usage metrics: the time the session started, ended, the reason for the session end and data upload and download.

This data is also stored in an RDS instance with daily snapshots.

SSL

All public facing portals and websites are encrypted with SSL (Secure Sockets Layer). SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

Location-based Services

This data is also stored in an RDS instance with daily snapshots. The method of gathering this data varies from vendor to vendor, and may be chosen where the vendor provides both methods (e.g. for Cisco MSE). This is either an SSL pull request initiated from Ocean WiFi to the client or an SSL push from the vendor hardware to the Ocean Digital servers.

Data collected depends on the vendor and the network setup, but can include the client MAC (which is stored hashed for anonymous non-associated devices), access point MAC, RSSI signal strength, X/Y coordinate, associated floorplan, seen time and network information such as internal IP and SSID where applicable for associated devices.

When a client MAC is recognised as having logged in via Ocean WiFi in the past, some demographic data may be associated with the LBS records (gender, age). Where a user has logged into this venue before and accepted the venue's T&Cs, a recognised device will be linked against the user record.

API

A RESTful API exists for extracting most end user data in raw format. Access to this service is via signed public/private keys, provided on request by the Ocean Digital support team once a customer's rights to the data have been verified. Access to Ocean WiFi APIs is encrypted using SSL. This can be used to get status information about a venue (e.g. users online now or in the past 24 hours) or extract most raw end user information.

Personally Identifiable Information (PII)

Depending on the customer's configuration of their captive portal and the access method chosen by the end user, Ocean WiFi may capture and store the following PII: first name, last name, date of birth, email address, mobile number and social user ID (e.g. Facebook ID).

PII data is stored in the main customer RDS instance in each region. RDS database storage is encrypted, which means they (and any snapshots) are encrypted on disk to prevent unauthenticated access to the underlying storage. Individual PII records are not themselves encrypted in the database. The data is encrypted while in transit, and all access to the data by customers is via SSL.

Device IDs / MAC Addresses

Device MAC addresses, IPs and user agents are stored in the same format as PII data for users who have connected to the WiFi and agreed to have their data stored on the platform. MAC addresses for anonymous devices (i.e. location data) are hashed using a SHA-256 algorithm with a unique salt per venue so MACs are still uniquely identifiable at the same venue (for identifying repeat visitors/devices), but not identifiable across venues or against other datasets.

Payments

Ocean Digital do not handle or store any user financial data. Should a transaction need to take place through the payment platform, the payment is taken via a direct communication between the end user and our payment gateway provider 'Stripe' (www.stripe.com). Stripe is fully PCI-DSS compliant.

ISO Compliance

The Ocean WiFi system is ISO 27001 compliant for data security and storage. This is addition to our own in house interim audits and management reviews.

AWS Certification / Attestations

Please see below some of the certifications that AWS has:

DoD SRG | FedRAMP | FIPS | IRAP | ISO 9001 | ISO 27001 | ISO 27017 | ISO 27018 | MLPS Level 3 | MTCS | PCI DSS Level 1 | SEC Rule 17-a-4(f) | SOC 1 | SOC 2 | SOC 3 | UK Cyber Essentials Plus

More information on this can be found at the following link:
https://aws.amazon.com/compliance/

Data Sovereignty

All data gathered in the UK and Europe by the Ocean WiFi platform resides in AWS hosting location in Dublin.

Ocean Digital is compliant with EU-EEA storage as defined in the UK's Data Protection Act.

Data Retention

All user data is anonymised after a period of 2 years of inactivity. This means Ocean Digital will store a user's personal data, in its full form, for 2 years, and after 2 years of inactivity (not logging back into the WiFi) we strip out anything which is deemed personally identifiable. This includes name, email, telephone number, etc. However, we do maintain non-identifiable information such as age group, gender and connection method used.

Ocean Digital may discard raw data sooner. For example individual XY records from location services are dropped after 24 hours, but an aggregated record of when the device was present on a floor plan and what zones were visited will be kept.

Data Storage and Back up

All of our databases are replicated to a secondary instance in a different Availability Zone (AZ). The replication is real time. In the event of planned database maintenance, DB instance failure, or an Availability Zone failure, Amazon RDS will automatically failover to the standby. This means that we do not have a single point of failure.

Ocean Digital runs daily snapshots on all databases, which means we have the ability to restore our database within minutes should the need arise, without losing more than 24 hours of data.

Data Ownership

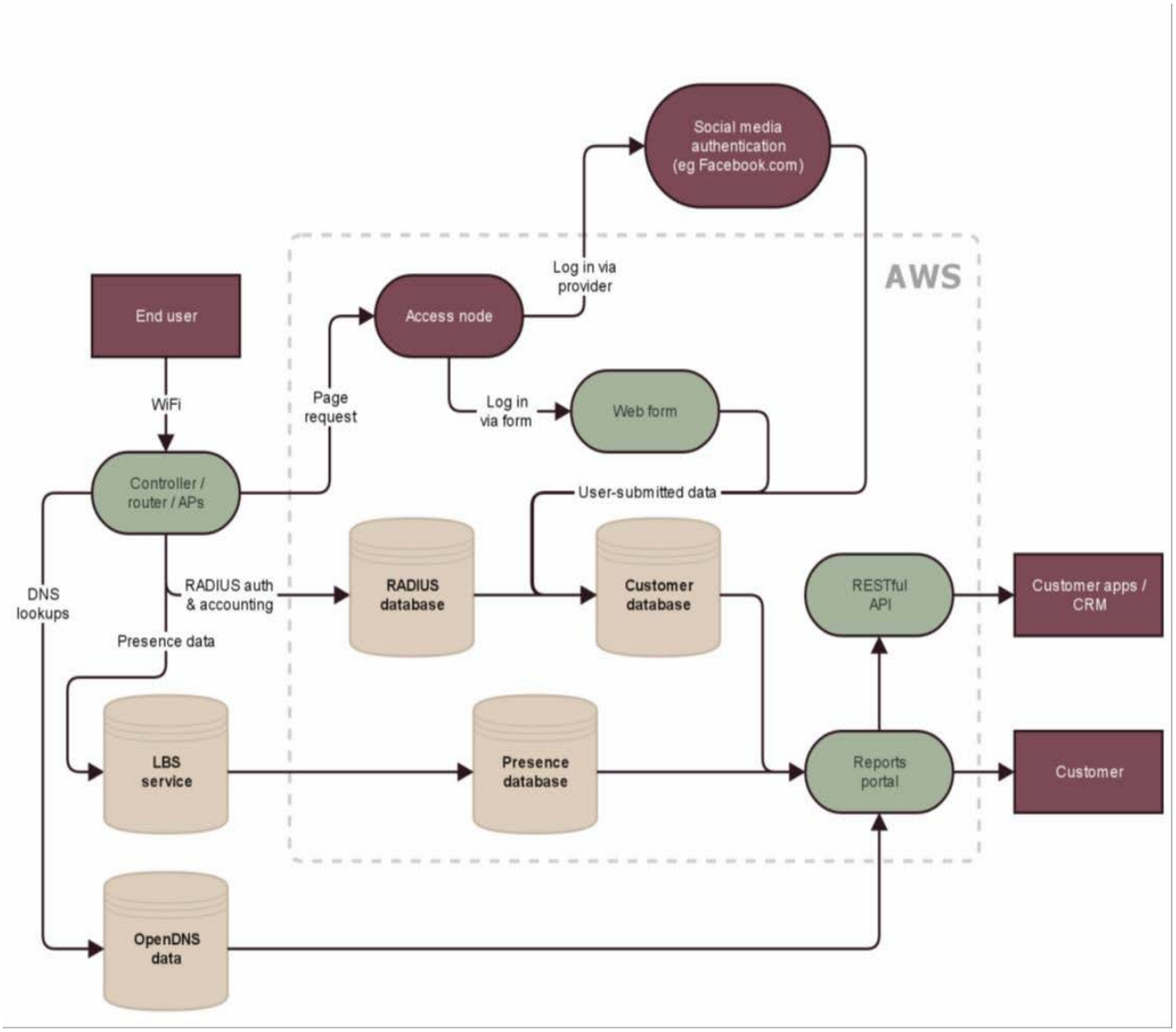
In order to comply with the Data Retention Regulations 2009 (EC Directive), which assists in the prevention and detection of organised crime and terrorism, certain communication data must be retained by service providers. Ocean Digital stores data in line with the requirements of the regulation on secure third party Amazon Web Servers.

The customer will have access to the end-user data and share ownership of this data with Ocean Digital as a third party, in order to provide the solution. In this scenario you are also considered a joint Controller of this data and are required to treat this data in accordance with the same regulations as Ocean Digital and any local legislation concerning the safe storage of data. At present the solution is centrally hosted.

Application Components

Data Flow

Below is a high level overview of the data collection process within Ocean WiFi.



Captive Portal

When a user connects to a SSID, they will be redirected to a captive portal splash page hosted by Ocean Digital. This splash page is configurable by Ocean Digital customers, and will present the user with one or more access methods (e.g. a registration form or social media login such as Facebook).

Upon choosing an access method, the user will be presented with a T&Cs popup which they must accept to continue. This pop up contains links to Ocean WiFi's terms of use, privacy policy and any user-defined terms.

By declining the terms, the user will be returned to the splash page. Upon accepting the terms, the user will either fill in the form or grant Ocean WiFi authorised access via a social media platform.

Ocean WiFi will then authorise the user on our RADIUS server and redirect the user back to the network controller which will release the user from the captive portal so they can access the wider Internet.

Captive portal splash pages are hosted on access nodes which is an elastically scaling PHP application backed by a scaling NoSQL database. Static content is served from Amazon's Cloudfront.

Our RADIUS servers are FreeRADIUS servers that store data on an RDS MySQL database.

Location / Presence Data Collection

Location-based services such as Cisco MSE, Ruckus SPOT or Meraki Cloud can be used with the product. These collect the MAC addresses of WiFi-enabled devices within range of the network APs and either provide basic RSSI information (which can be used to estimate distance from the AP to derive footfall, dwell time, conversion and bounce rate stats) or estimated X/Y coordinates that can be used to place a user on a map and track paths a user takes around a venue. Location data can be linked to known WiFi users via MAC address.

Customer Portal

The portal is the application where resellers and customers manage their licenses, infrastructure and view reports. Access to this application is controlled by username and password. User accounts can be given granular rights (read or write access to many individual sections of the portal) and are assigned hierarchically (e.g. with rights to a single venue, a group of venues, a whole company or a whole reseller, etc.). Platform rights are granted by individual users, and a user cannot grant or revoke rights beyond their own scope.

When a new portal user is created, they are sent a username (email) and a randomly generated password in email format. Upon first login, they are asked to change this password to one of their choice, which must be greater than 8 characters and contain both numbers and capital letters. The user must change their password every 90 days and they are not allowed to reuse any password from the past 12 months.

Radius

All traffic to our Radius server has to be authenticated with a called station ID and password. Without this traffic is denied access. For additional security a one-time password is also created and once used is discarded and cannot be used again.

Personnel Management, Procedures and Policies

Staff Access

Access to Ocean Digital's system within AWS is strictly limited to key members of staff, which is reviewed on a regular basis to ensure only appropriate staff have accounts.

Contractors and outsource companies are occasionally retained to do Greenfield development work. Access to live data, servers or services and existing code is strictly prohibited.

Staff access roles are clearly defined and reviewed quarterly and on contract change. Access to data and applications is established on a least privilege basis, with users only being granted access to what they need to fulfil their role for as long as they need it. Staff have minimal access rights while on their three month probation period, and non-employees (e.g. contractors) have no access to any customer data, live services or code repositories.

Development and testing procedures are clearly defined in our secure development policy. All code is submitted via pull request and peer-reviewed by the team and at least two senior developers prior to merge. It then goes through regression testing processing with our QA team who create and maintain standardised test sheets. Unit testing is used throughout the code base, and test-driven development encouraged. UAT may be carried out with selected partners prior to the release of large new features in the form of betas/trials.

Releases

Deployments occur at least weekly for general maintenance and bug fixes are deployed as required. Large releases follow a quarterly deployment schedule. All deployments go via Ocean Digital's test platform for final sign-off by our Development QA team.

Vulnerability / Threat Management

Ocean Digital carries out monthly automated vulnerability/threat analysis tests of all of our applications and infrastructure, and on every significant change (large code releases, infrastructure/architecture changes or after software upgrades). Software patches are applied at least weekly. Should a vulnerability be found during these tests, the threat will be assessed for level of impact and patched immediately should it be deemed necessary or have the fix rolled into the next release.

Incident Response

As part of the ISO 27001 certification, we implement a Security Incident Reporting Policy that gives development staff clear guidelines to protect the integrity of data collected by Ocean Digital. This ensures that security incidents, or potential incidents, are identified, brought to the attention of the Information Security Manager and dealt with in a manner appropriate to the urgency and impact of the breach.

Staff Termination

Ocean Digital has a clear procedure for staff termination. Requests to remove access to systems and recall hardware are logged as change requests on the in-house service desk.