Unit 5/9 Stockwell place
Archerfield QLD 4108
P +61 7 3276 7977

Version 2.0
28/06/2021

zencontrol

Application note: Cloud system architecture

Cloud system architecture.

The zencontrol cloud system consists of a suite of flexible, and scalable service containers running on EC2 elastic compute cloud virtualised hardware by Amazon AWS. The number and type of services are dynamically created and destroyed, dependant on the current demand and active connections. At time of writing there are more than 230 active services across 10 EC2 nodes, servicing 20,000 cloud connected control systems.

The function of each service is broken down into general categories depending on the function of that service. Services communicate with others via remote procedure calls, allowing the interoperability between independent name spaces and physical machine locations. The general categories and inter-process communication paths are shown in Figure 1.

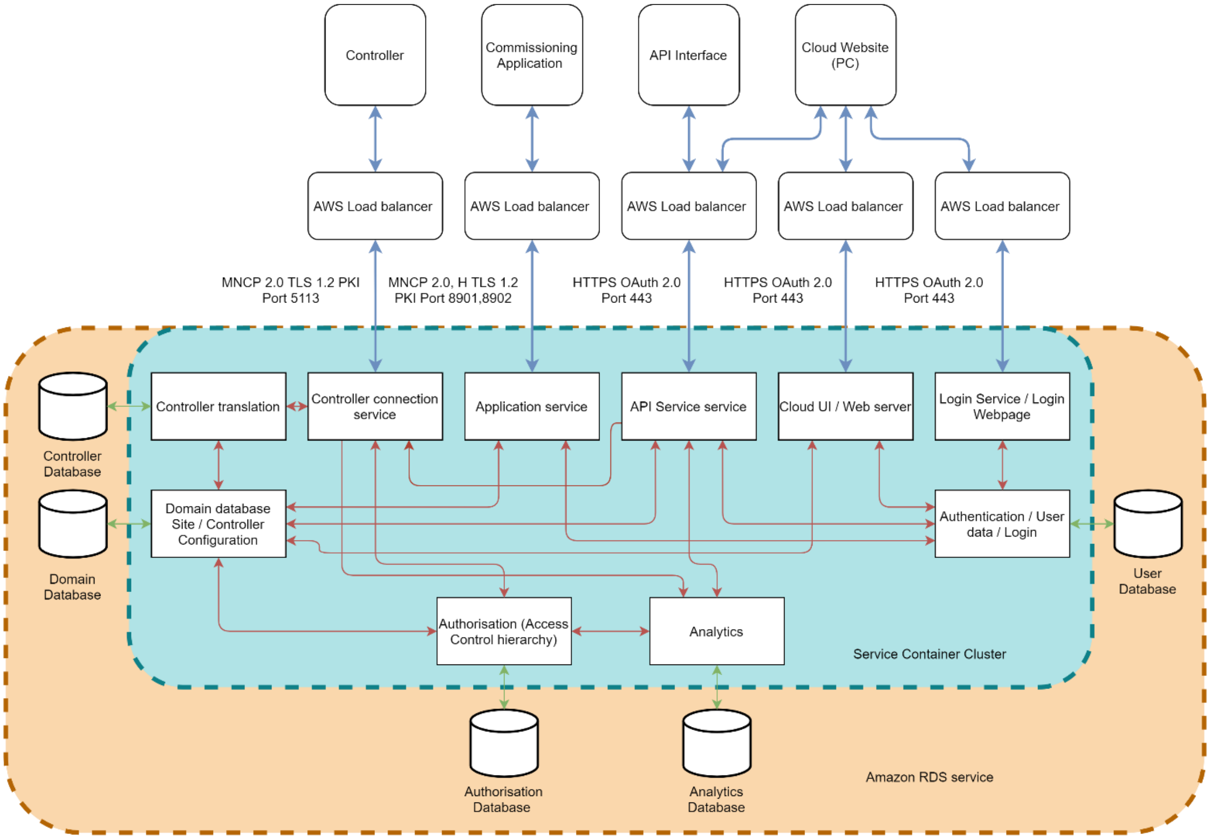

Figure 1 Cloud System Architecture

Amazon managed security groups ensure that database storage is accessible only via the service dedicated to managing that database. Security policies ensure that databases cannot be directly accessed and access to the services is only via secured, encrypted, and authenticated connections.

Each user of the zencontrol cloud system is granted a universally unique identifier created upon initial sign up. The combination of the user identifier and OAuth 2 uniquely and securely validates each user. An access control hierarchy dictates the asset and resource accessibility of each user id. So, whether accessing the cloud service through API, mobile application, or web browser, the cloud system will only ever respond to requests for information or changes for the predetermined access of the user identifier.

In practical terms this means that site data, controller configuration, and lighting control is available only on those sites and controllers a user has been assigned to.

Services interface on dedicated ports and minimal defined protocols. Unused ports and protocols are not implemented to reduce penetration surface area.

All connections are encrypted, and support industry proven and backed TLS1.2 Transport layer security. TLS 1.2 is not just encryption but as a complete security suite with technologies including SHA-2 and AES with a 4096-bit key length for controller to cloud communication and 2048 bits for API and web applications.

Device security

All cloud connected endpoints such as controllers and emergency test and monitoring systems, implement enterprise grade encryption.

Devices are upgradeable ensuring newly developed exploits will be patched and protected against. Firmware updates are cryptographically signed to prevent unauthorised or unintended firmware changes.

Every individual device is factory programmed with a unique and strong 16-byte encryption key. Factory protection mechanisms to ensure each controller is unique, and with a key uniquely tied to the device's serial number.

Controller to controller TCP connections are secured by TLS 1.2 PSK. Controller to cloud communications use TLS 1.2 PKI with a 4096-bit RSA encryption.

The TLS stack used on zencontrol controllers is developed and backed by ARM to ensure the highest level of vulnerability testing.

Communication security

In addition to cloud to controller encryption, all other cloud interfaces are secure and utilise industry proven encryption.

Web portal, API and mobile application access is secured via HTTPS signed with Sha256RSA and a 2048bit public private key infrastructure. User authentication utilises anonymous IDs and OAuth 2 access tokens. zencontrol supports OAuth 2 access tokens generated by zencontrol, Apple, Google, and Amazon.

API access identifies clients via unique client IDs and client secret for which a user access token must be unique. This ensures individual applications can be revoked and that user access tokens generated for one client, cannot be used on another. More information on API can be found at https://developer.zencontrol.com/ In a similar manner, access tokens generated and used on the web portal cannot be used to gain access to API, commissioning application or controllers.

Cloud security

zencontrol compute clusters run on dynamically scaled virtualised hardware from Amazon AWS. There is no physical access to the hardware running the platform. Services running in the production environment do not support any remote connection request other than those described in this environment for strictly necessary operation. Production environment access for zencontrol staff to update, maintain and manage running services is provided by reverse proxy connection to a protected connection at zencontrol head office in Brisbane. Credentials and certificates required to authenticate and establish connection are strictly limited to those authorised employees directly involved in each deployment.

Data security

Unlike traditional systems that are vulnerable to physical access and equipment, zencontrol data is stored on the cloud and follows standard best practice procedures. The amazon RDS system makes continuous incremental backups with a full roll back retention of 14 days. Additionally, periodic snapshots capture the full operation environment.

All cloud data is stored with encrypted access Amazon RDS service. This means that the data is protected from both physical and digital access. The managed storage provided by Amazon is 99.999999999999% (12 nines) fault tolerant, with multiple storage locations across physical hardware, across a minimum of 3 locations within a service availability region.

Within the user environment building managers can grant and revoke access to building areas and privileges. Changes and users are logged and auditable ▪ Incorrect or malicious changes can be identified and rolled back.

Cloud based data storage means there is no need for local storage on PCs. Lack of head end PC eliminates the risk of physical theft.

With a common service environment, zencontrol's system security is continuously providing the capability to protect all connected systems against future exploits via a common update process.

Data sovereignty

zencontrol hosts cloud services on Amazon AWS, local users will access nodes running on the deployed availability region closest to their physical location.

In Australia and New Zealand all data is stored in Amazon managed RDS systems in the Sydney availability region.

In Europe services are hosted in the London availability region. Other areas will use the closest available availability region.