AdOPT Platform Security Q&A

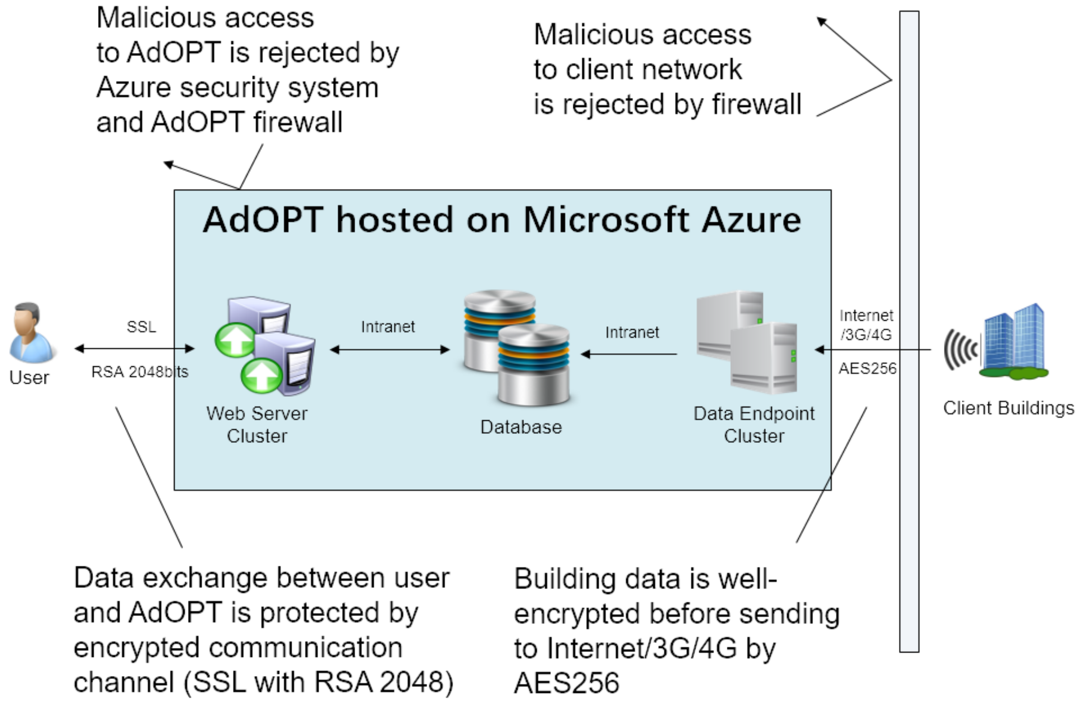
Where is AdOPT platform hosted?

AdOPT Platform is hosted on Microsoft Azure, the world’s top 2 public cloud service provider.

Where is data stored?

AdOPT Platform stores data in disks hosted on Microsoft Azure.

What does data flow look like? How is data safely transferred?



Malicious access to AdOPT is rejected by Azure security system and AdOPT firewall

Malicious access to client network is rejected by firewall

Data exchange between user and AdOPT is protected by encrypted communication channel (SSL with RSA 2048)

Building data is well-encrypted before sending to Internet/3G/4G by AES256

What kind of firewall is recommended for client?

Usually a software firewall (like Norton) is good enough. In case a hardware firewall is required, Cisco hardware firewall is recommended (e.g. Cisco ASA5506-K9).

What kind of controls are in place at Microsoft Azure?

Azure provides world-class security controls and operation auditing for our services, including but not limited to:

- Azure Application Gateway Web application firewall provides protection for common web vulnerabilities and attacks, including:
  - HTTP Protocol Violations
  - HTTP Protocol Anomalies
  - SQL Injection
  - Cross-site Scripting
- Azure provides key-vault service that uses FIPS 140-2 level 2 validated HSMs to protect encryption keys.

- Azure security scanning will inform us to install important security patches to keep the security protection up-to-date. For extremely important security vulnerabilities like the Heartbleed bug, Azure will have all machines patched forcibly.
- Azure built-in operation auditing system will log all operations performed on Azure virtual machines, databases and network from Azure management console.
- Azure supports integration with Jump-Server to audit all performed commands and command issuers on all virtual machines.

What type of data is collected and stored?

Various data that measures the basic state of building equipment and systems, like HVAC, plumbing and lighting system.

How is data protected after it is decrypted and saved to database?

User password is never decrypted and saved in salted hashes (check encryption policy for details). Other data is stored with 3-layer strict access control:

- The first layer is web-level control, which limits access to data at the time when AdOPT HTTP APIs are invoked (either by AdOPT web pages or other programming integration endpoints). Every invocation is validated in conjunction with Azure web app protection service (described in point c.) to ensure no malicious access will pass through.
- The second layer is database-level control. MongoDB built-in entitlement system leverages Salted Challenge Response Authentication Mechanism (SCRAM) based on IETF RFC 5802 standard authentication. Meanwhile, security policy is set to allow access only from Azure internal network to MongoDB.
- The third layer is machine-level control. Machines that host MongoDB can only be accessed over SSH by pre-registered private keys that generated by RSA 2048 algorithm from clients with pre-registered IP addresses. Private keys are forced to be updated every 90 days.

What is the encryption policy?

- Sensitive data must be encrypted before transferring.
- Highly sensitive data (like password, credit card number) shall never be stored in plain text. No highly sensitive data shall be logged anywhere.
- Use of known insecure encryption algorithm is forbidden, including but not limited to DES/3DES/SKIPJACK/RC2/RSA 1024 or below/MD2/MD4/MD5.
- Recommended encryption algorithm: AES 128 bits or above/RS 2048 bits or above/SHA2 256 bits or above/DH 2048 bits or above/HMAC-SHA2
- Insecure data transfer protocol is not recommended, including FTP, Telnet, SSHv1.x (exceptional case must be approved by IT director or above)
- Recommended data transfer protocols: SSHv2/TLS1.1/IPSec/SFTP/SNMPv3

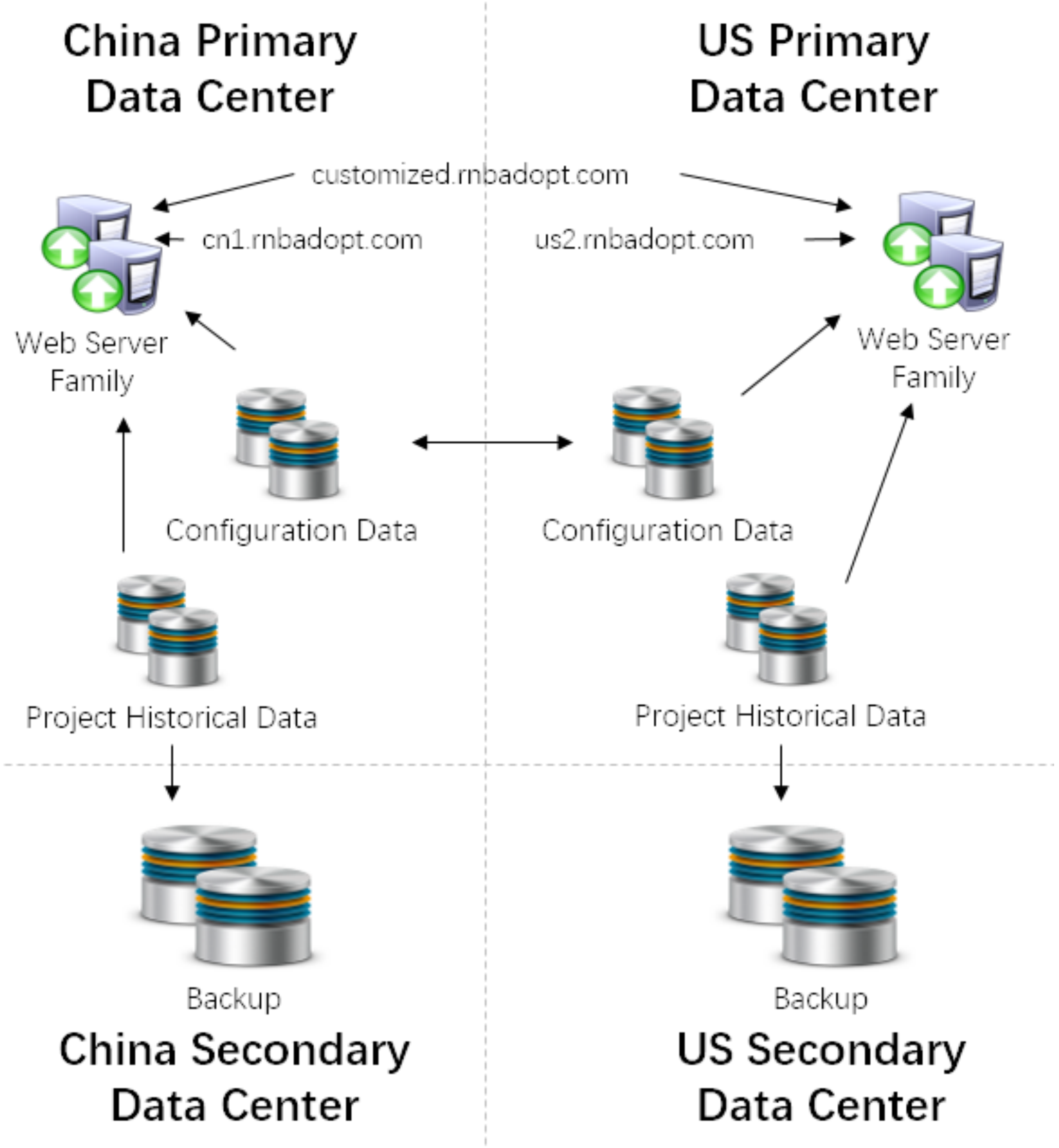
What is the password policy?

- Password should be longer than 8 characters
- Password should contain letters in lowercase and uppercase, number and special characters.
- Password should be updated every 180 days unless client requires to make it unchanged.
- If constant login failures are detected from specific clients within a very short period of time, subsequent logins from that client will be rejected for a certain period of time.

What type of security controls are implemented to ensure data from a client is isolated from other clients?

The data of different customers is stored in separated database tables. It is also possible to store data on an isolated database server for specific users, though it might involve additional costs.

What is the data backup strategy?



How is data deleted?

In normal cases, AdOPT never deletes any data. However, clients can explicitly request data deletion by contacting technical support.