Actian Avalanche Security

Security Architecture Overview

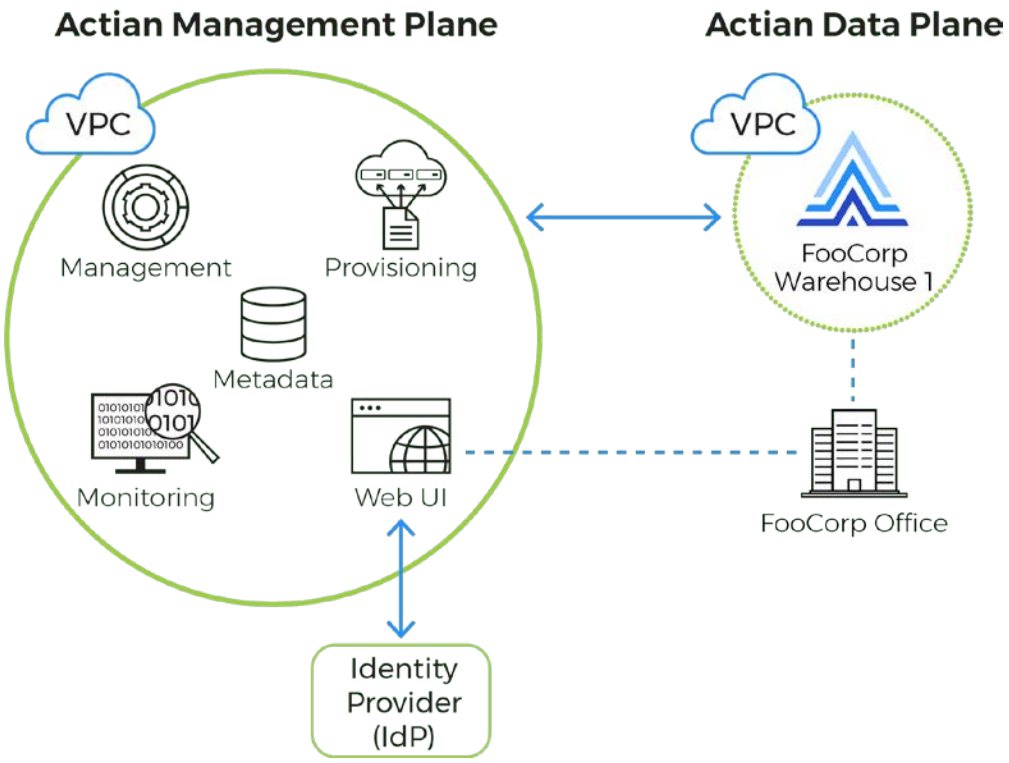
White Paper

Contents

Actian Avalanche is a single tenant, fully managed hybrid cloud data warehouse service that ensures the highest levels of security. Avalanche provides private network isolation, disk and columnar encryption, robust access control capabilities as well as 24x7 maintenance and monitoring. As part of the Cloud Security Alliance, Avalanche continuously adopts best practices to ensure secure cloud computing. A Soc 2 Type II attestation is available upon request under NDA.

VPC Isolation

The Avalanche management plane is isolated from the data warehouse level. The management plane is only able to access warehouse metadata as well as provisioning, management and monitoring information. Monitoring data relates to warehouse health and performance. Metadata includes warehouse name, creation time, size, region, etc. Metadata does not contain any customer data. Each data warehouse tenant is separate and isolated using the cloud service's VPC isolation. This separates the data plane from the management plane as well as isolating each warehouse. Warehouses are then isolated from the Internet and only accessible through limited port ranges and customer-specified IP addresses defined in the IP allow list. An advanced option is available in Avalanche to enable deployment of an advanced firewall to further isolate the instance and only allow private VPN tunneling to the customer site. Each warehouse can span multiple geographic regions or limit to a specific geographical region depending on requirements.

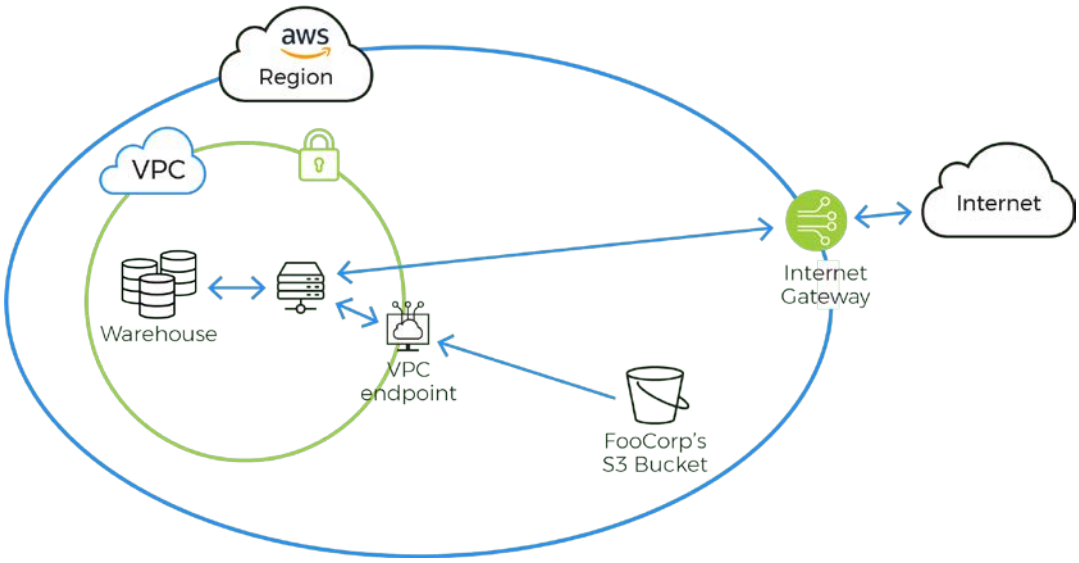


Avalanche Management Plane

Storage and encryption

Avalanche provides industrial grade encryption, including both disk level data-at-rest encryption, columnar encryption, and encryption in transit. Each warehouse is separated at the VPC level and has no communication with each other. Internal warehouse traffic does not traverse the internet.

Data is loaded into the customer warehouse over a secure channel (HTTPS/TLS) from the customer's object storage, e.g. S3 or Azure blob storage. If the cloud object storage and the warehouse are established within the same region, all data transmission is over the cloud as a private channel transfer (currently private channel transfer is AWS only). This data is stored in an optimized format in block storage on the cloud provider. All data is encrypted in transit during loading and encrypted at rest in the cloud providers' filesystem at the disk level. Data transmitted to the client from the warehouse is also encrypted. The data warehouse only accepts encrypted connections by default.



AWS private channel transfer

All data is encrypted at the disk level as it is stored. If further encryption is required for more sensitive information, columnar encryption can be enabled. Database / columnar encryption encrypts the values in columns in tables of the database, including temporary tables. AES encryption is utilized for all database encryption operations within the database, whether on the DBMS level or user specified. All encryption functions utilize randomness as a key component to ensure strong protection of data within the database. Database encryption is transparent and done at the DBMS Server level. Users can also encrypt columns with their own user-specified passphrase. The key length can be specified from 128 to 256 bits. Without the passphrase, a user cannot retrieve the underlying encrypted data. The passphrase can be changed to re-encrypt the key. Columns can also be masked based on access level or hidden from views.

Access to the Web UI is encrypted with TLS and authenticated against an enterprise identity provider. The Web UI is used to create and delete warehouses and has limited warehouse capabilities. The Web UI cannot access warehouse data.

Access and Authentication

Direct access to the data warehouse requires an IP allow list as well as database authentication. The data warehouse is not open to the internet but only available to users connecting from the specified allow list IPs. If the cluster is utilizing an advanced Avalanche configuration using a firewall with VPN, the VPC can be further isolated from the internet and only accessible through a private tunnel.

Access through the web console requires authentication against an enterprise identity provider using OpenID Connect, based on Oath2.0. Multifactor authentication is available through the Salesforce identity. Accounts at the Identity Provider have an enforced password policy. Once identity is established, the user is passed back to the Web UI for entitlement and access. User access to the Web UI is entirely separate from the database user level. From the Web UI, a user can manage warehouses, list, create, delete or start and stop warehouses. When a warehouse is created, the customer will be able to set up the initial database administrator account from the Web UI. This ensures that no default password exists at any time as part of configuration.

The data warehouse requires database level authentication for DBAs and users with access. Customers can access the data warehouse through standard protocols such as ODBC, JDBC and .NET. Encryption is enforced on these protocols. The Database Administrator has the ability to enable Discretionary and Role-Based Access Control (RBAC) framework to limit access to data. Access can be configured at the database level per user account or user group. Permissions can be granularly configured to allow only view-only access or read, write access, update, select or any combination as necessary.

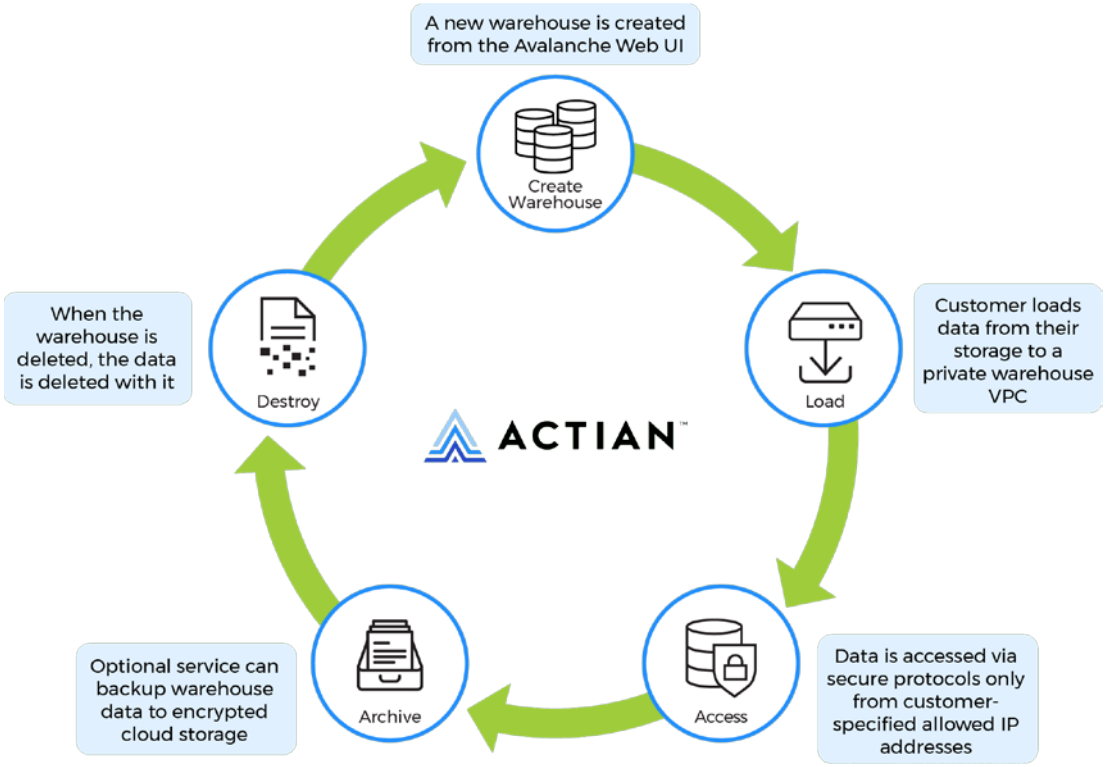
Maintenance and Compliance

Avalanche is hosted in either AWS or Azure data centers that are ISO 27001 certified. These cloud data centers provide high level of physical security, including biometric access and 24/7 surveillance. A customer can specify a region for the creation of a cluster. A Soc 2 Type II attestation is available upon request with signed NDA.

Database-level log events are available within the warehouse. Security events and metadata are logged at the management plane level. These logs can be provided upon request to support auditing requirements. No customer data is logged to the management plane and no passwords are logged anywhere. The management plane is maintained with rolling up-to-date patching and software. The warehouse service instances are regularly patched within the maintenance window.

The Avalanche console is scanned with a PCI-approved scanning vendor (ASV). Additionally, the Web UI is scanned for web application vulnerabilities and resolved in a timely manner. The environment is monitored 24x7 by a global operations team. Current performance and uptime metrics are available at the Avalanche customer portal and through RSS feed.

Data Lifecycle



- **Where is my data?** A warehouse is created from the Web UI and loaded from customer storage into Avalanche.
- **How is it secured?** Database files are stored on AES encrypted block storage dedicated to only that data warehouse.
- **Who can access my data?** The data is only accessible from the IPs in the customer's allow list.
- **How is data accessed?** Customer can access through various standard protocols from the allowed IPs. Support has no direct access to data.
- **What happens to data when I no longer need it?** When the warehouse is closed, the data is deleted.

ACTIAN

2300 Geng Rd, Suite 150, Palo Alto, CA 94303
+1 888 446 4737 [Toll Free] | +1 650 587 5500 [Tel]

© 2020 Actian Corporation. Actian is a trademark of Actian Corporation and its subsidiaries. All other trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. (WP09-0820)