# Statement of Direction: Cloud Architecture

This statement of direction (SoD) establishes a framework for transitioning cloud architecture from the current state to the next six months. Longer-term SoDs for domain sub-components (up to 18 months) are included on subsequent pages.

Five organizational units (OUs) handle services at different stages. The OUs are: production (prod), pre-production (pre-prod), non-production (non-prod), development (dev), and sandbox. Use the organizational units as follows.

* **Dev** – wide open use. Disconnected lab data now is allowed in both dev and sandbox. If allowed in dev, then it’s allowed in sandbox, and vice versa.
* **Pre-prod** - validate and test before deploying to production.
* **Non-prod** – contains prod data that’s neither critical nor high-risk; could contain all dev data.
* **Sandbox** – replaces the disconnected lab, which has been deprecated.

The following table lists ARB-approved services for use in AWS.

|  |  |  |
| --- | --- | --- |
| **Technology** | **ARB-Approved Features / Services** | **Acceptable Use Patterns (current - 6 months)** |
| Cloud Containers | Approved for use in dev and sandbox deployments in any configuration.  No production or development approved pattern. | **AWS Elastic Container Service** |
| Cloud ETL | Approved for use in dev and sandbox deployments in any configuration.  Pending submission for ARB approval for multi-account development in production. | **AWS Glue** - TBD |
| Cloud Hadoop | Approved for use in dev and sandbox deployments in any configuration.  Limited use in production and development deployments as approved for Neustar and Data Lake. | AWS Elastic Map Reduce |
| Cloud Logging | Deployed across all accounts. (confirm)  **AWS Cloud Trail** - Logs every API interaction with AWS in any account listed above to S3. This logging is forwarded to Discover Splunk repositories.  **AWS Network logs** – Flow logs are routed to S3 for every account. This logging is forwarded to Discover Splunk repositories.  **CLS Filebeat**– System logs for EC2 IAC module deployed instances can call out the CLS Filebeat cookbook and have logs forwarded to CLS. This is not enabled by default and is required to move EC2 syslogs to CLS. | **AWS Cloud Trail**  **AWS Flow logs**  **Discover Prem Splunk**  **CLS Filebeat** |
| Cloud Mobile Testing | Approved for use in dev and sandbox deployments in any configuration.  No production or development approved pattern. | **AWS Device Farm** |
| Cloud Monitoring | **AWS CloudWatch** is available for use in all AWS accounts. CloudWatch information can be used as triggers to fire events within AWS. Dashboards and other CloudWatch features are approved for any AWS multi-account deployment.  **CloudHealth** currently is used for secondary cloud monitoring.  **CloudCheckr** has been deprecated and is no longer available for any environment. | **AWS CloudWatch**  **CloudHealth** – available for monitoring effective 1 March 2018.  **CloudCheckr** – sunset—no longer available for any environment. |
| Cloud Object Store | Approved for use in dev and sandbox deployments in any configuration.  Approved use for:   * Data Lake storage in production and development * CloudTrail log storage in production and development * Any project that will consume IAC Terraform module – Nginx S3 Proxy | Amazon S3 in US standard. |
| Cloud Serverless | Approved for use in dev and sandbox deployments in any configuration.  Limited use of Lambda using Python 2.7 and 3.6 in production and development for:   * Security tool development * IAC operations tasks * Smartronix AWS support environment   No approved general AD development. | AWS Lambda using Python 2.7 and 3.6 |
| Cloud Virtual Desktop Infrastructure (VDI) | Approved for use in dev and sandbox deployments in any configuration.  Technical Training *replaced the disconnected lab with dev and sandbox* to provide virtual desktop infrastructure (VDI) for training workstations. The VDI is delivered via the HTML5 client. The ability to copy data in and out over the HTML5 client has been disabled. | **AWS Workspaces – Windows 7**  **AWS Workspaces – Windows 10**  **AWS Workspaces – HTML5 Client** |
| Identity and Access Management (IAM) | Production and test/dev:   * **AWS IAM** is integrated with production LDAP and federated with SAML v2.0 via CA SiteMinder. * **EC2 IAM** is integrated with production LDAP and consumed via Centrify. * **Terraform IAM** is integrated with production Vault. LDAP roles are directly integrated with Vault mount points. | **AWS IAM and CA SiteMinder SAML**  **Centrify**  **Vault** |
| Key Management System (KMS) | Approved for use in dev and sandbox deployments in any configuration.  Must use in production and test/dev AWS environments for encryption-at-rest  **KMS** is only approved for the encryption-at-rest of AWS services. It is not approved for any application services. | **Amazon KMS** |
| NoSQL | **AWS DynamoDB**  Used to store key and value pair data for Amazon services configuration and metadata.  Approved for use in prod, dev, and sandbox deployments in any configuration.  Can only be consumed via a VPC endpoint. | AWS DynamoDB  (ARB reviewed 5/31/2018.) |
| NoSQL | **DynamoDB DAX**  DAX needs ARB and Cybersecurity approval before use. | DynamoDB DAX  Acceptable use pattern pending CLS (Centralized Logging) presentation. |
| Orchestration | **CloudFormation** is available for:   * Use with dev and sandbox accounts. * Limited use to manage IAM roles for production, development, and *sandbox* account.   CloudFormation should not be leveraged for any orchestration tasks and all tasks should be deferred to Terraform.  Terraform will be used for all base level orchestration and automation interaction with AWS services. IAC modules will be leveraged to comply with standards set forth for each AWS service. Terraform must be used to deploy patterns at AWS.  **Chef** Is available in all environments. Chef will be used for all instance-level orchestration and configuration management capabilities.  **VRA** [add content]  **Ansible** is available in all environments. Ansible may be used for instance-level orchestration capabilities. Configuration management tasks must be deferred to Chef. | **CloudFormation – YAML**  **Terraform 0.10.4 – TF files**  **Chef**  **VRA**  In the process of sunsetting this platform for AWS  **Ansible 2.0** |
| Public Cloud Application Orchestrators | TBD | **AWS Elastic Container Service**  **OpenShift – TBD**  **PCF – TBD** |
| Public Cloud Data Warehouse | **Redshift** is ARB-approved and available for consumption with dev, prod, and sandbox.  **Snowflake** is ARB-approved and available for consumption with dev, prod, and sandbox. | **Redshift** (ARB approved solution pattern as ARB9207867, at 11-01-2018 ARB meeting.)  **Snowflake** |
| **Public Cloud Relational Database(s)** | **AWS RDS MariaDB**  Approved for use in dev, sandbox, and prod deployments in any configuration.  Development and production:   * Provisioned only via PCF and a broker. PCF broker currently leverages CloudFormation, but is migrating to Terraform. (At 2/8/2018 meeting, ARB approved as Terraform Provisioned RDS – MariaDB, ARB7246847.) * EMR Hive metadata deployed via Terraform. ARB-approved (30 Jan 2018).   Multi-account deployment:   * Deployments for EMR Hive metadata deployed via Terraform. ARB-approved (30 Jan 2018). * Any approved ARB application/solution pattern.   **AWS RDS Postgres**  Approved for use in sandbox in any configuration. | AWS RDS MariaDB  **AWS RDS Postgres** (sandbox only) |
| Public Compute | **Amazon Elastic Compute Cloud (EC2)** deployments allowed in any configuration and any deployment method via the dev and sandbox AWS accounts.  Production and development deploy EC2 via IAC approved Terraform and Chef Kitchen delivery. | Amazon EC2 deployed via Terraform modules   * This deployment pattern allows for EC2 deployments in production and development AWS accounts. The pattern allows for any instance size, memory, and disk, as long as instantiated via Discover IAC standard Terraform modules.   Amazon EC2 CloudFormation delivery   * This deployment method has been deprecated for deploying EC2.   Amazon EC2 vRealize delivery   * This deployment method has been depreciated for deploying EC2 as a catalog item.   Chef Kitchen delivery   * This deployment pattern allows for deploying EC2 in development environments that do not leverage IAC-approved Terraform modules. |
| Service Catalog | **vRealize** will be used for production and development deployments of any catalog-delivered service.  **AWS Service Catalog** can be used in *dev and sandbox*. | **VMware vRealize**  **AWS Service Catalog** |
| Video and Data Stream Processing | **AWS Kinesis** deployments are allowed in any configuration and any deployment method via these AWS accounts:   * Multi-account sandbox * Multi-account development   Production deployments via IaC approved Terraform modules are allowed when deployed via a larger AWS application pattern.  To deploy an application to production, you need an ARB-approved application pattern, and you must use the standard Terraform module. | **Kinesis**  Deployed via Terraform modules, in uninhibited development environments:   * Kinesis Data Streams * Kinesis Data Hose * Kinesis Data Analytics   In development, this solution pattern allows for any deployment, with “x” standing for the service. The solution pattern allows for any deployment of “x,” as long as “x” is instantiated (created) via Discover IaC Terraform modules. |
| Video and Data Stream Processing | **AWS SQS** deployments are allowed in any configuration and any deployment method via these AWS accounts:   * Multi-account sandbox * Multi-account development   Production deployments via IaC approved Terraform modules are allowed when deployed via a larger AWS application pattern.  To deploy an application to production, you need an ARB-approved application pattern, and you must use the standard Terraform module. | **SQS** |

### Document Revision History

|  |  |  |
| --- | --- | --- |
| **Date** | **Revised by** | **Description** |
| 7 Feb 2018 | Scott Peterson | Updated for 2018 |
| 3 Jul 2018 | Scott Peterson, Renée Moore | Updated services. Minor content edits. |
| 2 Oct 2018 | Renée Moore | Minor reformatting. |
| 15 Nov 2018 | Scott Peterson, Renée Moore | Removed or updated references to disconnected lab, which is deprecated. Added organizational units with descriptions (1st page). Replaced disconnected lab with dev and sandbox. |
| 19-20 Nov 2018 | Kavita Chekuri, Scott Peterson, Renée Moore | Added ARB review or approval dates for DynamoDB, MariaDB, and Redshift. Replaced references to dirty and disconnected labs with dev and sandbox. |