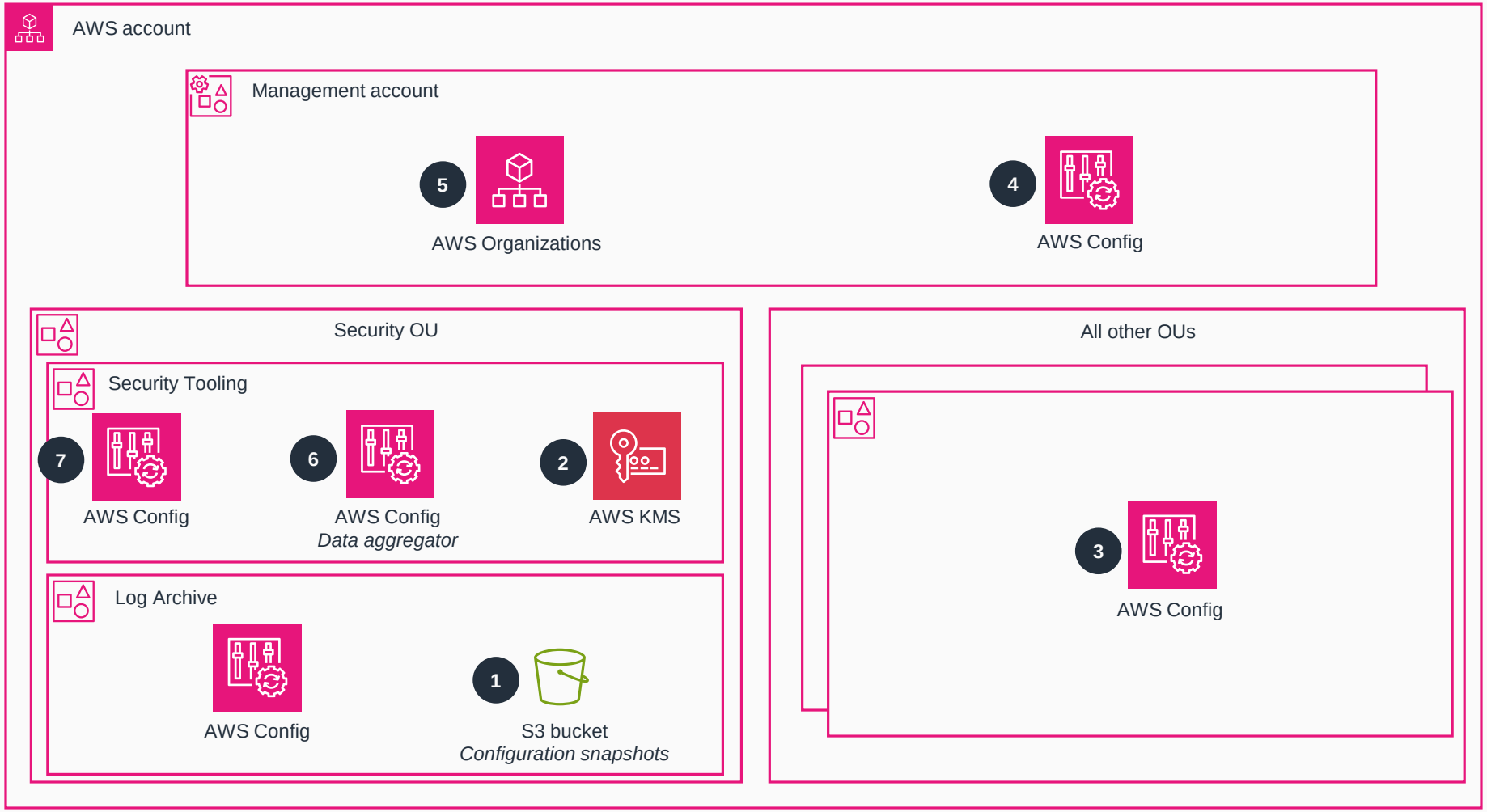
Guidance for Resource Inventory Management on AWS

This architecture diagram shows how to centrally collect, store, and evaluate your resource inventory within a multi-account environment on the cloud.



1. Create an **Amazon Simple Storage Service (Amazon S3) bucket** that will hold the AWS resource configuration snapshots and history.
2. Optionally, create an **AWS Key Management Service (AWS KMS) key** in the Security Tooling organizational unit (OU) account. This account will be used to encrypt configuration history and snapshot files using server-side encryption with **AWS KMS** customer-managed keys (CMKs). If you do not use an **AWS KMS** key, the **AWS Config** data will be encrypted at rest using AES-256 encryption.
3. Deploy an **AWS Config configuration recorder** and **delivery channel** to all operating Regions (Regions that you are not prohibited with **service control policies** [SCPs]) in all member accounts. Configure the **delivery channel** to send resource configuration information to the **S3** bucket in the Log Archive account for audit and retention purposes.
4. Deploy **AWS Config configuration recorder** and **delivery channel** to all available Regions in the Management account. Configure the **delivery channel** to send management account resource configuration information to the **S3** bucket in the Log Archive account.
5. Delegate **AWS Config** administration to the Security Tooling OU account to allow for **AWS Config** administration outside of the management account.
6. Deploy an **AWS Config multi-account, multi-Region data aggregator** in the Security Tooling OU account to aggregate account and Region data for the organization. This will provide visibility to organization resources and **AWS Config configuration compliance**.
7. Deploy **AWS Config Rules** to organization accounts to evaluate resource compliance. You can deploy rules with **organization AWS Config rules**, with **conformance packs**, or by using automation, such as **AWS CloudFormation StackSets**.

Reviewed for technical accuracy November 29, 2023

AWS Reference Architecture