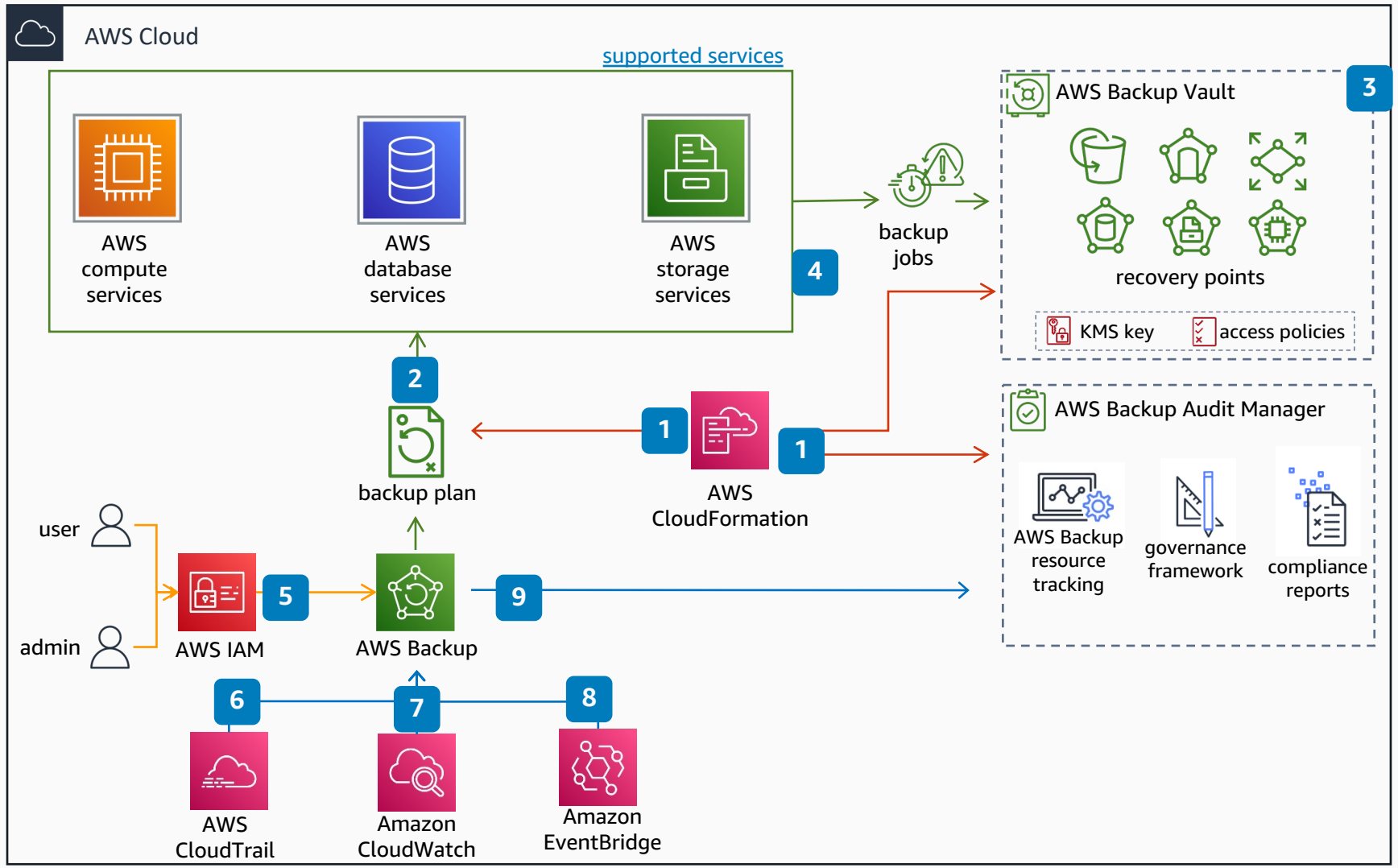
Data Protection Reference Architectures with AWS Backup

Reviewed for technical accuracy July 29, 2022

AWS Reference Architecture

Cloud-native data protection with AWS Backup

This reference architecture describes how AWS Backup is implemented in a single AWS account to protect multiple services in an automated way.



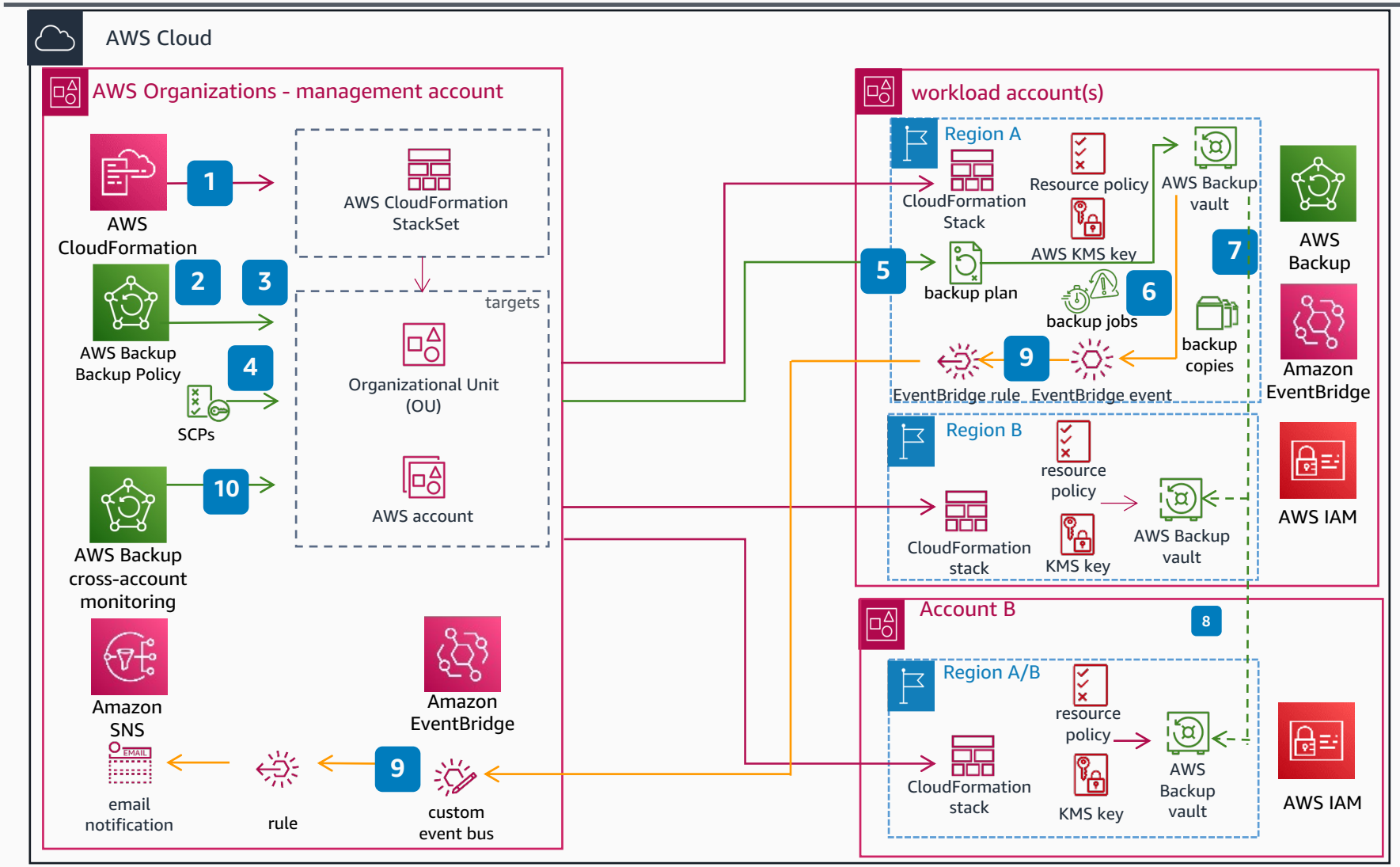
1. Use AWS CloudFormation to create the components that **AWS Backup** uses in this architecture.
2. The **AWS Backup** plan defines the frequency, retention period, lifecycle, backup copy destination and resources to be protected.
3. The **AWS Backup** vault is a logical container that stores and organizes your backups. Encryption of certain backups is enforced through a defined **AWS Key Management Service (AWS KMS)** encryption key.
4. A backup job runs within the backup window defined in the backup plan. Once the job is completed, a recovery point will be available in the vault and can be used to restore.
5. Secure access to your resources through AWS Identity and Access Management **(AWS IAM)** by using AWS-managed policies as a starting point. At the vault level, access policies protect the vault and its contents and can be used to grant/deny access to certain vaults and its underlying operations (delete/restore).
6. **AWS Backup** actions are recorded in AWS CloudTrail as events.
7. Monitor **AWS Backup** service metrics through **Amazon CloudWatch**.
8. Use Amazon EventBridge to monitor **AWS Backup** events, such as when a backup fails or gets deleted.
9. Audit backups and automate reports through **AWS Backup Audit Manager**, which allows you to continuously monitor compliance of your backups.

Reviewed for technical accuracy July 29, 2022

AWS Reference Architecture

Cross-account and Region data protection with AWS Backup and AWS Organizations

This reference architecture enables customers to implement a consistent backup strategy through multiple AWS accounts and Regions, and copy backups between them through an automated, policy-driven way.



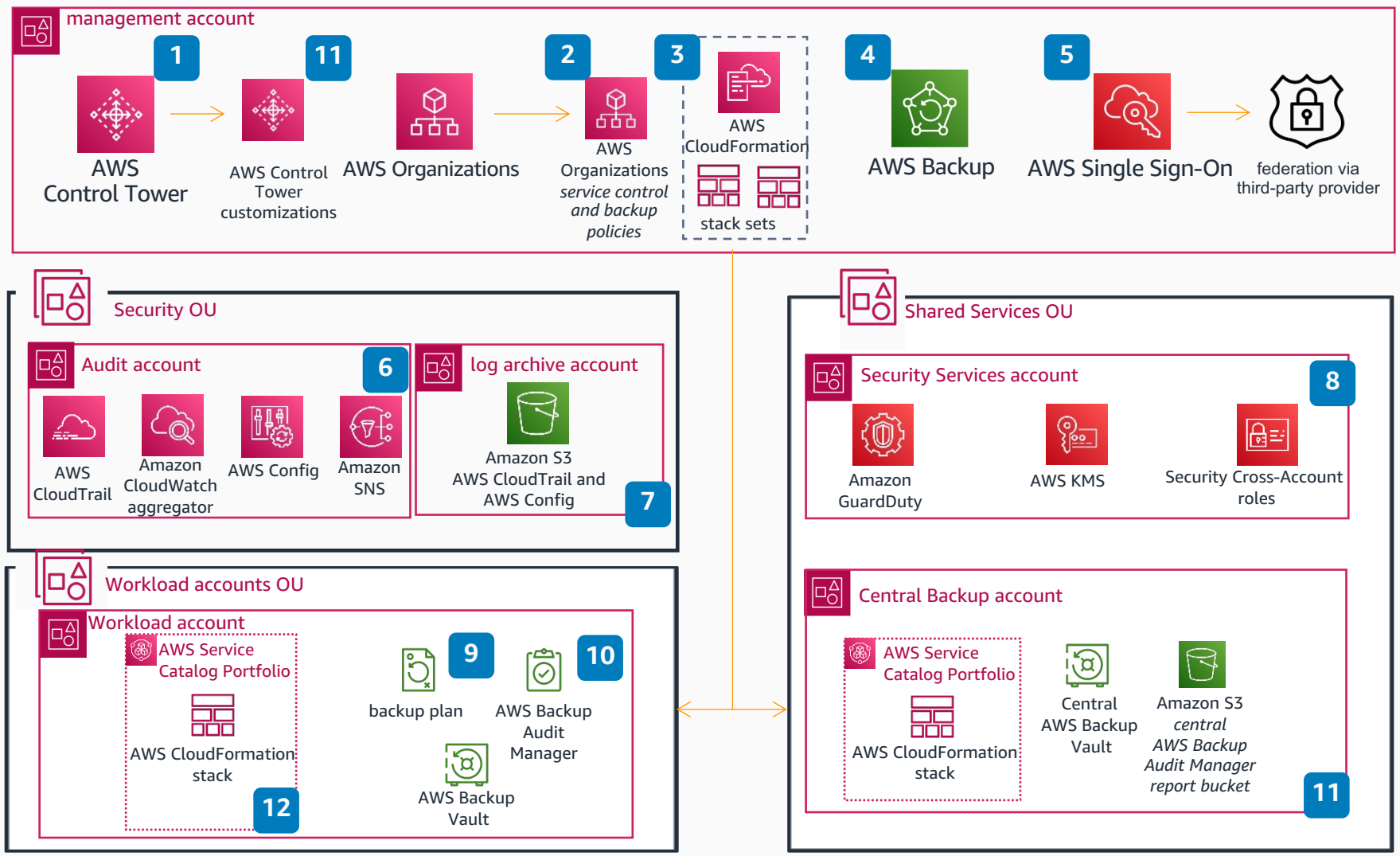
1. Use AWS CloudFormation Stacksets to create **AWS Backup** resources such as an **IAM** role, backup vault, **AWS KMS** key, and access policies.
2. Create a backup policy, define the frequency, retention, lifecycle, backup copy settings and resource assignment tag values then attach the policy to a target
3. StackSets and backup policies support both organizational units (OUs) or specific AWS accounts as targets, re-use the target assignment between both services as possible to bring consistency between required and defined resources.
4. Use Service control policies (SCPs) to protect your **AWS Backup** resources from unwanted modification, deletion or use.
5. Once a backup policy is configured and attached to a target, **AWS Backup** creates a backup plan in all the member accounts that are part of the OU. Plans will be added/deleted based on the OU membership changes.
6. Based on the plan schedule, backup jobs will be run and recovery points will be available in the backup vault afterwards.
7. If cross-account backup copies are required, use a customer managed **AWS KMS** key on the originating resource and source backup vault, then provide the necessary permissions to the key and target vault.
8. Cross-Region backups can occur within the same account as well in a single step to a different account for most supported resources. The backup policy defines the vault name and account where the backup will be copied to. Make sure the vault is available in the desired destination for backup copies to be successfully completed.
9. Backup events can be monitored and alerted in a centralized way by forwarding the events through an **Amazon EventBridge** rule to a central custom event bus, and then triggering email notifications using **Amazon Simple Notification Service (Amazon SNS)**.
10. Cross-account and Region activities can also be monitored through the **AWS Backup** console in the **AWS Organizations** management account.

Reviewed for technical accuracy July 29, 2022

AWS Reference Architecture

AWS Landing Zone and AWS Backup reference architecture

This reference architecture aligns to the design tenants of a well-architected, secure, and scalable multi-account AWS implementation with the integration of AWS Backup for data protection. You can use AWS Control Tower or a similar landing zone framework to standardize your data protection strategy.



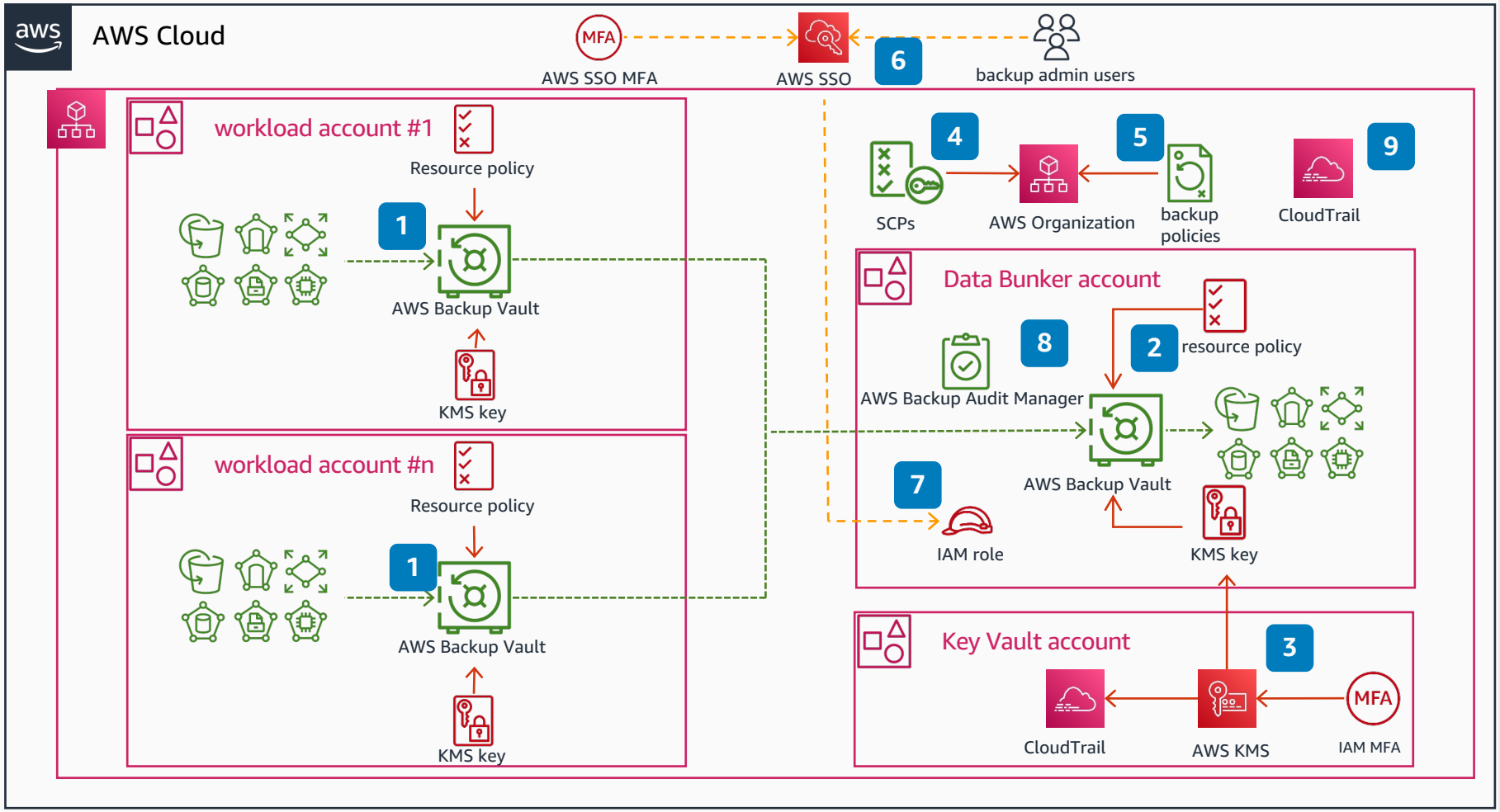
1. Use **AWS Control Tower** and deploy the Customizations for Control Tower (CfCT) resource template to integrate **AWS Backup** in your environment. Use either AWS CodePipeline or an **S3** bucket and **AWS Control Tower** lifecycle event workflow to deploy the **AWS Backup** resources through your multiple accounts.
2. Enable Service Control Policies (SCPs) to set preventive guardrails and backup policies in AWS Organizations to protect resources in the workload accounts.
3. Enable AWS CloudFormation StackSets for your Organization to centrally deploy resources across multiple accounts.
4. Enable **AWS Backup** in your **AWS Organizations** environment and enable the cross-account monitoring and cross-account backup management. Opt-in to the AWS services that will be protected by the backup plans.
5. Centrally manage SSO access to your environment using **AWS Single Sign-On** which integrates with existing corporate identities through federation via a third-party provider.
6. Use services such as **CloudTrail**, **CloudWatch**, and **AWS Config** to maintain audit trails of your organization's activity in a centralized manner.
7. Centralize **AWS Backup CloudTrail** events and **AWS Config** logs in a S3 bucket owned by the *Log Archive* account to restrict log access to the appropriate security/governance personas.
8. Securely manage shared resources, such as **AWS KMS,** to centralize and de-couple key ownership, using **IAM** cross-account roles to control and manage AWS operations.
9. Backup policies managed in the **AWS Control Tower** *Management* account, create backup plans in the target accounts/OUs.
10. Use **AWS Backup Audit Manager** to monitor backup compliance in each account.
11. Centralize backup copies and **AWS Backup Audit Manager** reports across your organization in a central backup account.
12. Provide self-service capabilities to end-users to create/update their backup configuration from a pre-defined catalog using **AWS Service Catalog.**

Reviewed for technical accuracy July 29, 2022

AWS Reference Architecture

Creating immutable backups with AWS Backup Vault Lock

This architecture details the key steps involved in setting up a central immutable backup data bunker that follows the principle of least privilege in a multi-account AWS Organization.



backup flow → settings flow ⇢ authentication flow

1. Create a **resource policy** that limits `CopyFromBackupVault` to the Backup Data Bunker Account and apply to the **AWS Backup Vault**(s) in each member account. Create a Customer Managed **KMS** key and apply it to the **AWS Backup** Vault(s) in each member account.
2. Setup a Backup Data Bunker account, create an **AWS Backup Vault,** and set up **Vault Lock** to it. Create a resource policy that limits `CopyIntoBackupVault` actions from specific organizational units (OUs) or accounts and apply to this AWS Backup Vault.
3. Create a Customer Managed **KMS key** in a separate Key Vault account, and share the **KMS** key to the Central Vault Account. Implement additional security controls, including multi-factor authentication (MFA) on critical KMS API calls such as `ScheduleKeyDeletion`.
4. Create a Service Control Policy that restricts access to the appropriate **IAM** roles to create backups which create boundaries on the copy operations into the Backup Data Bunker account, and apply it to the member accounts.
5. Create an AWS Backup policy with a copy operation into the Backup Data Bunker account and apply it to the member accounts.
6. Restrict the access to the Backup Data Bunker account to the specific user base via **AWS SSO and MFA,** that will follow a Break Glass workflow.
7. The authenticated user is granted AWS STS temporary credentials via federation with specific access to the Backup Data Bunker.
8. Create audit reporting using **AWS Backup Audit Manager (BAM)**.
9. Create an organizational **CloudTrail** for recording and monitoring of policy changes and Central Backup Vault Access patterns.

Reviewed for technical accuracy July 29, 2022

AWS Reference Architecture