Architecture Diagrams

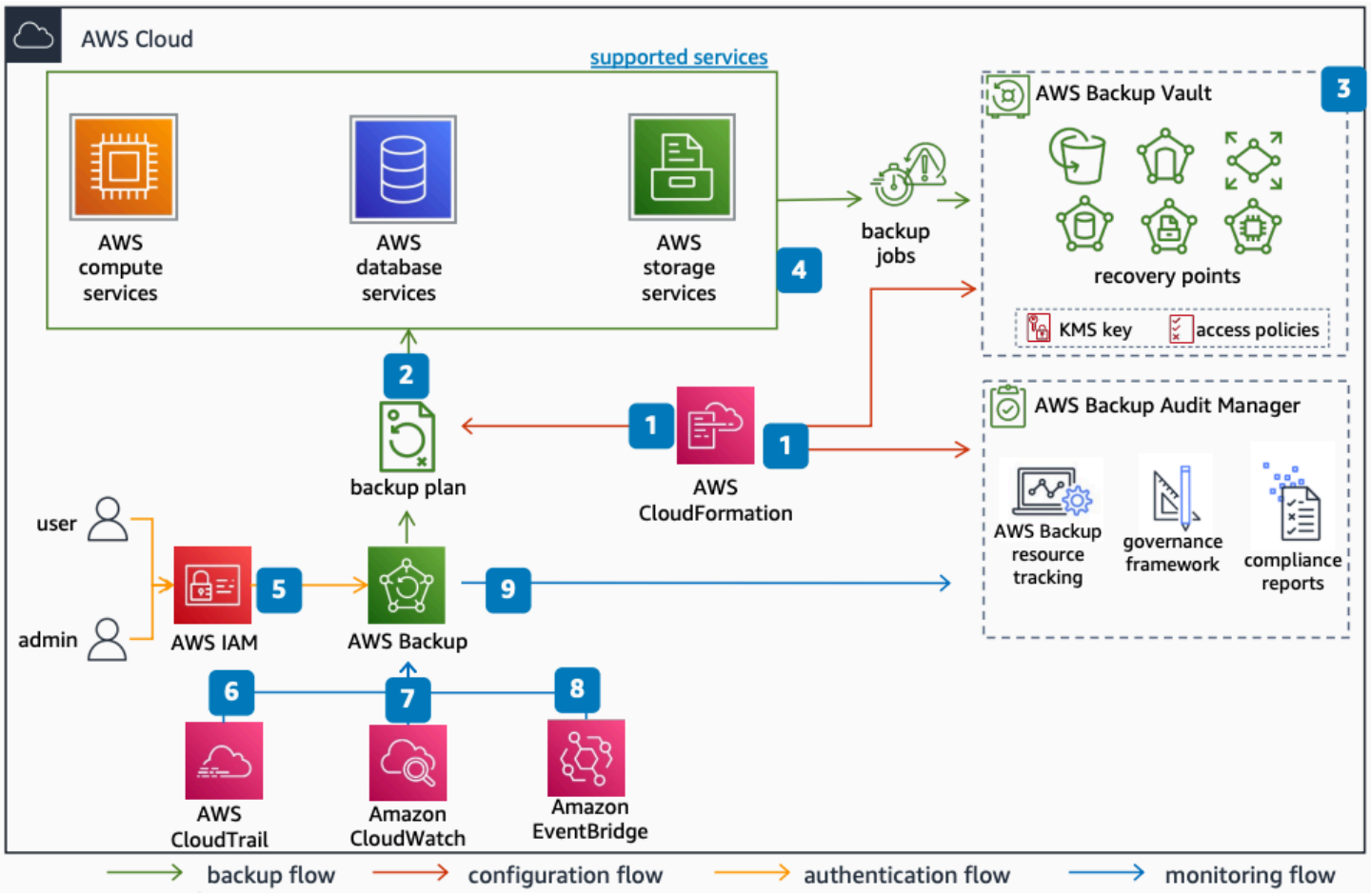
Data Protection Reference Architectures with AWS Backup

Data Protection Reference Architectures with AWS Backup: Architecture Diagrams

Table of Contents

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 protect.
3. The AWS Backup vault is a logical container that stores and organizes your backups. A defined AWS KMS key enforces encryption.
4. A backup job runs within the backup window defined in the backup plan. After the job completes, a recovery point appears in the vault for restore.
5. Secure access to your resources through IAM by using AWS-managed policies as a starting point. At the vault level, access policies protect the vault and its contents.
6. AWS Backup actions record in CloudTrail as events.

7. Monitor AWS Backup service metrics through CloudWatch.
8. Use https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-what-is.html 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. With this service, you can continuously monitor compliance of your backups.

Further reading

For additional information, refer to

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected
- AWS Backup product page

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

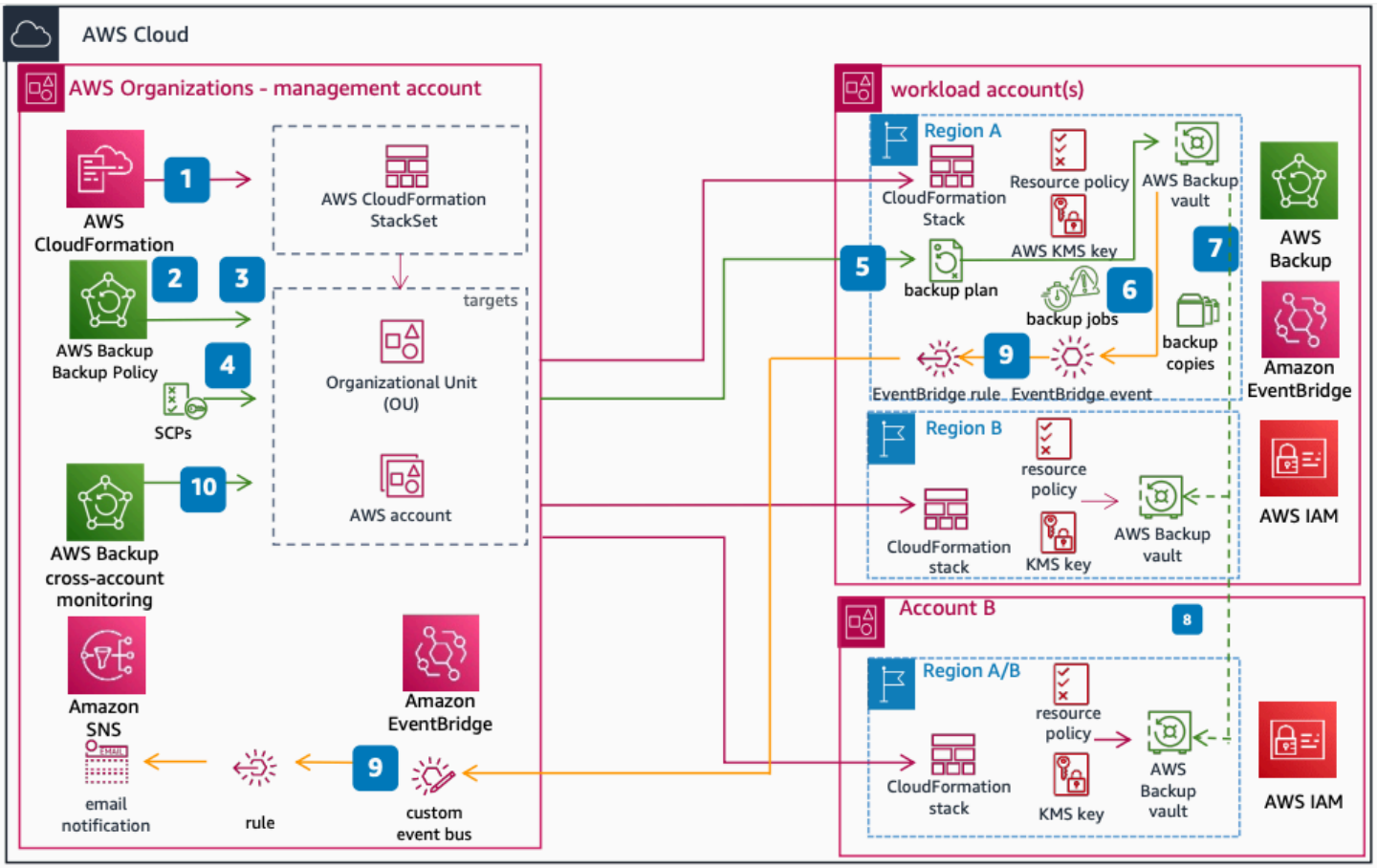
Change	Description	Date
Initial publication	Reference architecture diagram first published.	July 29, 2022
Initial publication	Reference architecture diagram first published.	July 29, 2022
Initial publication	Reference architecture diagram first published.	July 29, 2022
Initial publication	Reference architecture diagrams first published.	July 29, 2022

Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

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

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



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.
4. Use Service Control Policies (SCPs) to protect your AWS Backup resources from unwanted modification, deletion, or use.

5. After configuration and attachment to a target, AWS Backup creates a backup plan in all member accounts that belong to the OU.
6. Based on the plan schedule, backup jobs run and recovery points appear in the backup vault.
7. For cross-account backup copies, 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 or to a different account in a single step. The backup policy defines the vault name and destination account.
9. Forward backup events through an https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-what-is.html rule to a central custom event bus for centralized monitoring. Then trigger email notifications by using Amazon SNS.
10. Monitor cross-account and Region activities through the AWS Backup console in the AWS Organizations management account.

Further reading

For additional information, refer to

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected
- AWS Backup product page

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	July 29, 2022
Initial publication	Reference architecture diagram first published.	July 29, 2022

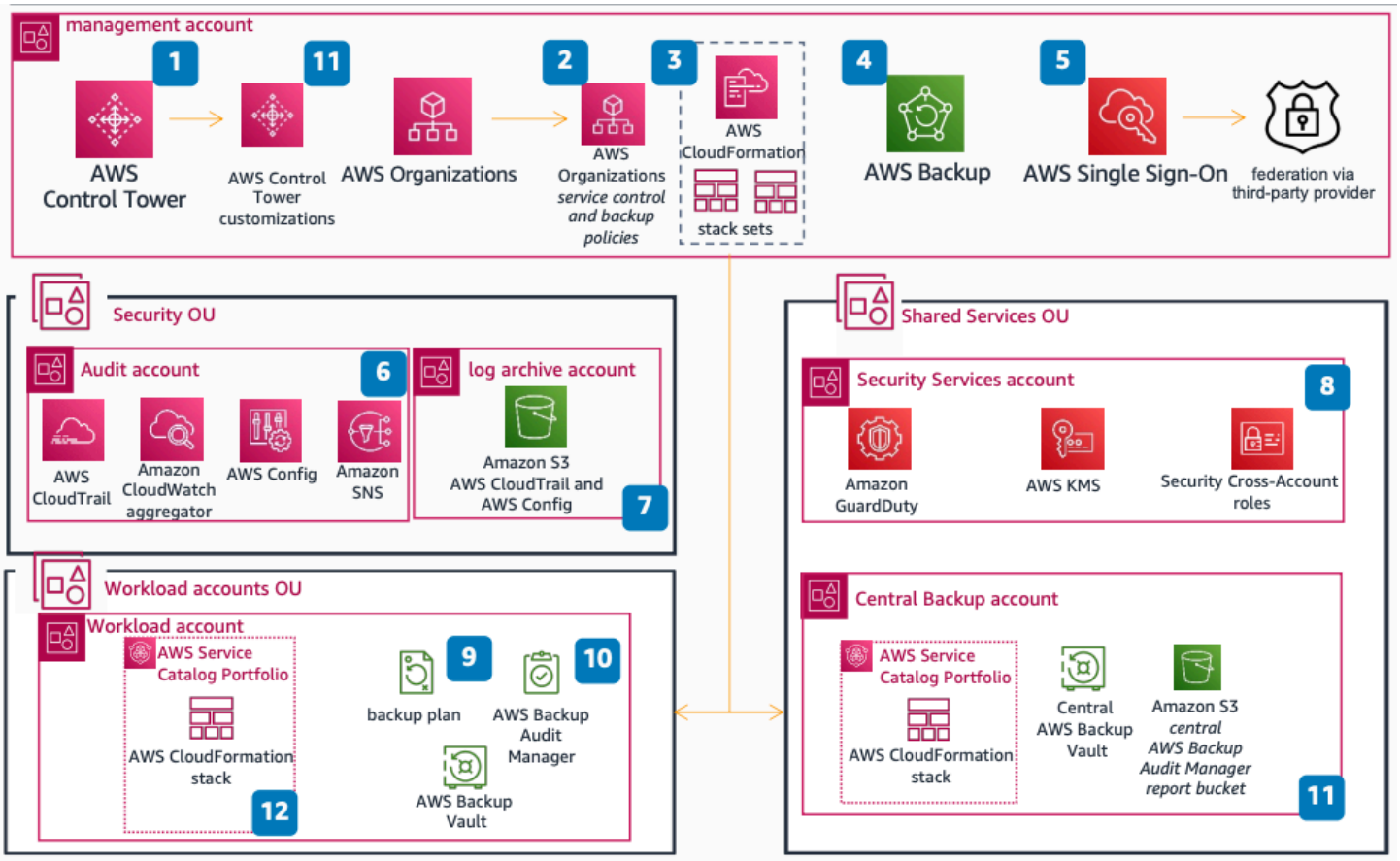
Initial publication	Reference architecture diagram first published.	July 29, 2022
Initial publication	Reference architecture diagrams first published.	July 29, 2022

Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

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 or a similar landing zone framework to standardize your data protection strategy.



1. Use and deploy the Customizations for Control Tower (CfCT) resource template to integrate AWS Backup in your environment.
2. Enable Service Control Policies (SCPs) to set preventive guardrails and backup policies in AWS Organizations.
3. Enable AWS CloudFormation StackSets for your Organization to centrally deploy resources across multiple accounts.
4. Enable AWS Backup in your AWS Organizations environment. Enable cross-account monitoring and cross-account backup management.

5. Centrally manage SSO access to your environment by using . This service integrates with existing corporate identities through federation.
6. Use services such as CloudTrail, CloudWatch, and AWS Config to maintain audit trails in a centralized manner.
7. Centralize AWS Backup CloudTrail events and AWS Config logs in an S3 bucket owned by the Log Archive account.
8. Securely manage shared resources, such as AWS KMS, to centralize and decouple key ownership by using IAM cross-account roles.
9. Backup policies managed in the management account create backup plans in the target accounts and 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. They can create or update their backup configuration from a predefined catalog by using AWS Service Catalog.

Further reading

For additional information, refer to

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected
- AWS Backup product page

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	July 29, 2022

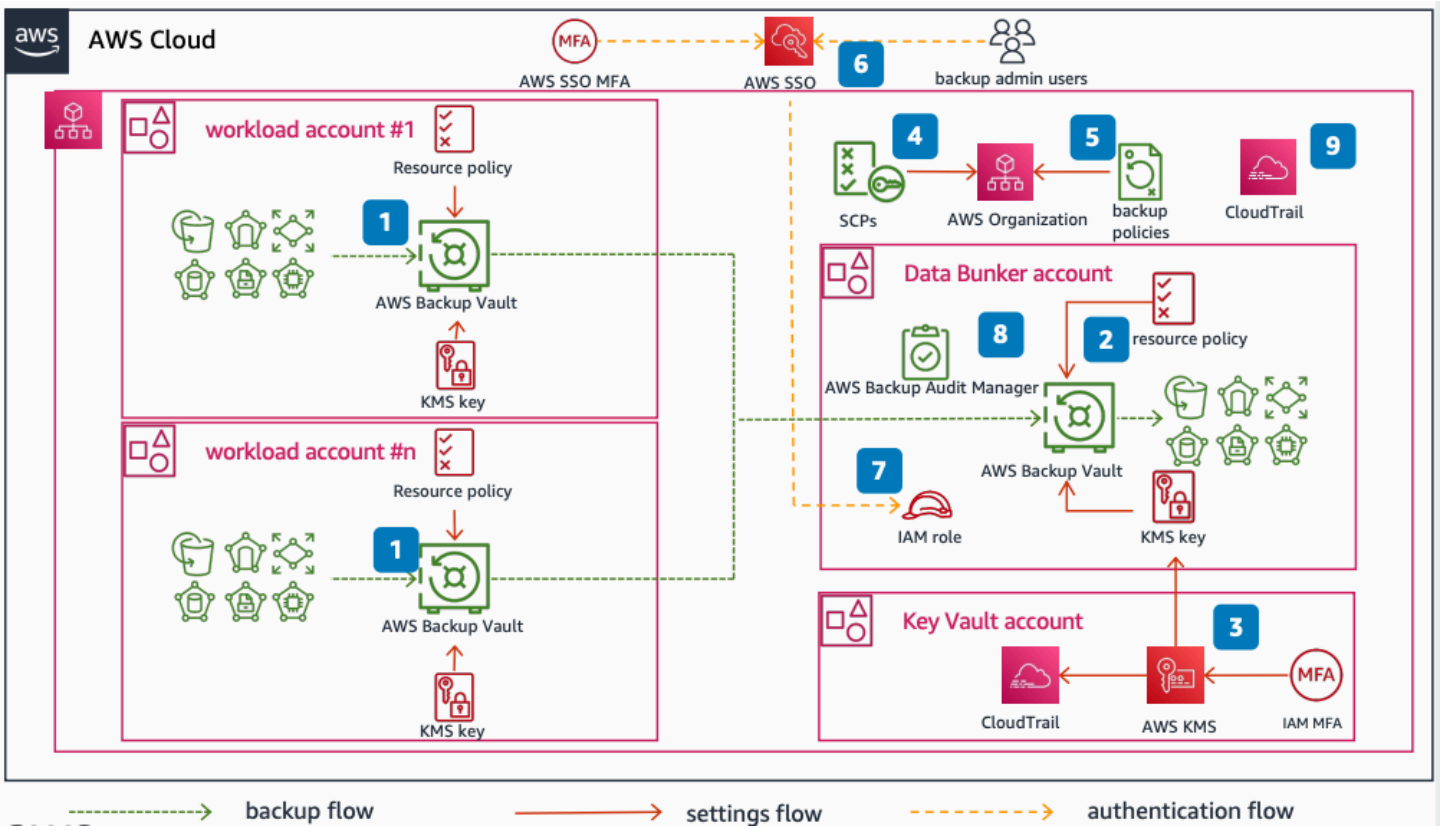
Initial publication	Reference architecture diagram first published.	July 29, 2022
Initial publication	Reference architecture diagram first published.	July 29, 2022
Initial publication	Reference architecture diagrams first published.	July 29, 2022

Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

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.



1. Create a resource policy that limits CopyFromBackupVault to the Backup Data Bunker Account. Apply it to the AWS Backup vaults in each member account. Create a customer-managed KMS key for each vault.
2. Set up a Backup Data Bunker account, create an AWS Backup Vault, and apply Vault Lock. Create a resource policy that limits CopyIntoBackupVault actions from specific OUs or accounts.
3. Create a customer-managed KMS key in a separate Key Vault account and share it with the Central Vault Account. Implement additional security controls, including MFA on critical KMS API calls.
4. Create a Service Control Policy that restricts access to appropriate IAM roles for backup operations into the Backup Data Bunker account.

5. Create an AWS Backup policy with a copy operation into the Backup Data Bunker account. Apply it to the member accounts.
6. Restrict access to the Backup Data Bunker account to specific users through AWS SSO and MFA, following a Break Glass workflow.
7. The authenticated user receives AWS STS temporary credentials through federation. These credentials provide specific access to the Backup Data Bunker.
8. Create audit reporting by using AWS Backup Audit Manager (BAM).
9. Create an organizational CloudTrail for recording and monitoring policy changes and Central Backup Vault access patterns.

Further reading

For additional information, refer to

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected
- AWS Backup product page

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	July 29, 2022
Initial publication	Reference architecture diagram first published.	July 29, 2022
Initial publication	Reference architecture diagram first published.	July 29, 2022
Initial publication	Reference architecture diagrams first published.	July 29, 2022

Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.