AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

STG341-R2

AWS Backup to protect cloud-native resources and hybrid environments

Priyesh Bansal

Senior Product Manager, AWS Backup
AWS

Rolland Miller

Global Solutions Architect, AWS Backup
AWS

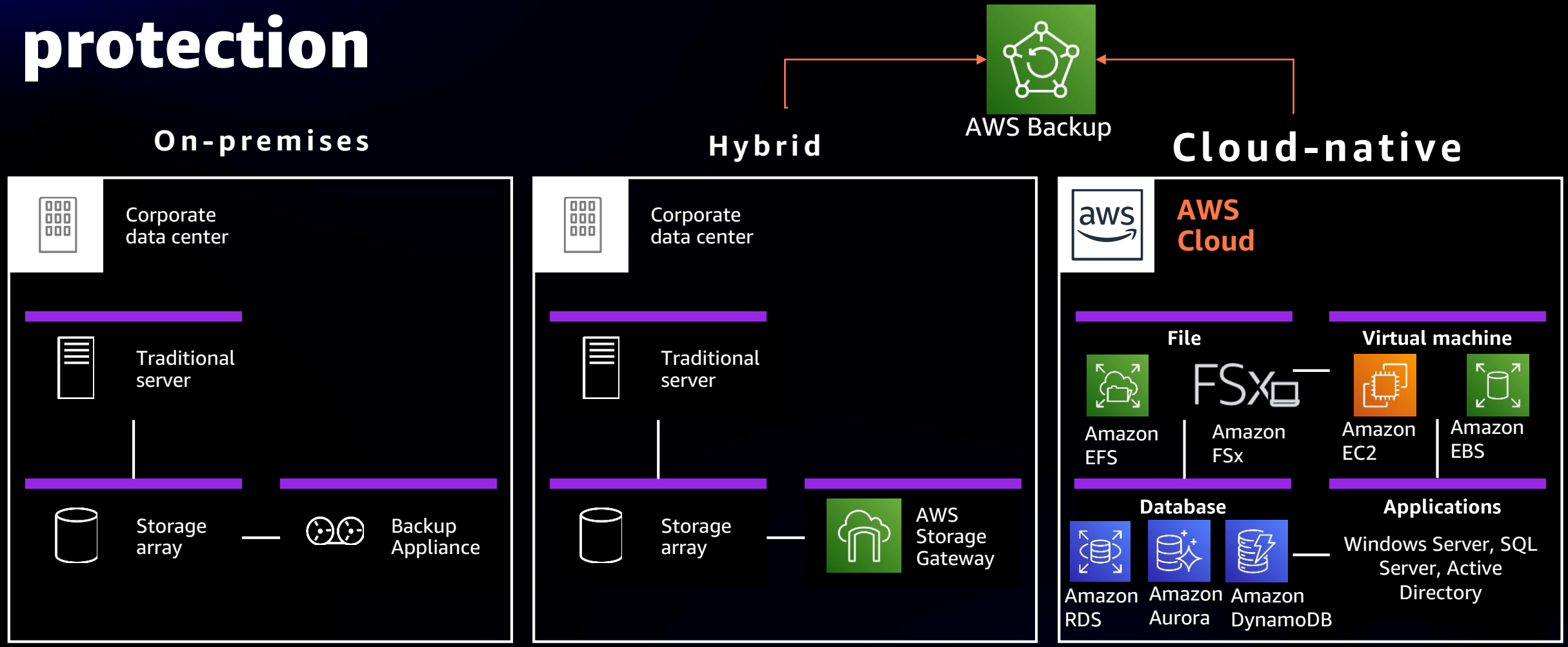
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Typical customer journey with AWS



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

An AWS-native solution for centralized data protection



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why centralized data protection?

Applications span across multiple AWS services



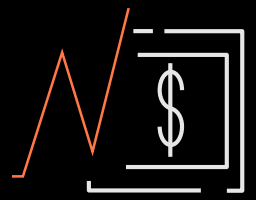
Management

- Centralized monitoring of backup operations
- Auditing distributed logs
- Automated tooling to manage backup of applications



Compliance

- Reporting for audit and compliance
- Automated policy enforcement for data protection
- Managing per-service IAM roles

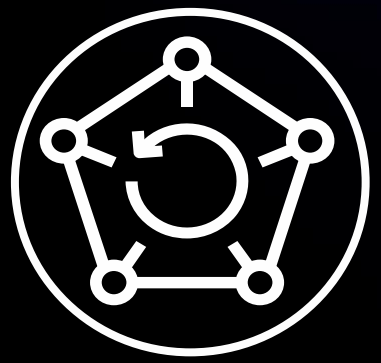


Cost

- Time and resources allocated to building, maintaining, and supporting data protection tools
- Efficiency of disaster recovery and retention practices

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup

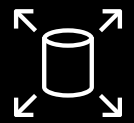


AWS Backup

A fully managed, policy-based backup service that makes it easy to centrally manage and automate the backup of data across AWS services



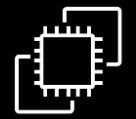
Amazon RDS



Amazon EBS



Amazon EFS



Amazon EC2



FSx for Lustre



AWS Storage Gateway



Amazon DynamoDB



FSx for Windows



Amazon DocumentDB



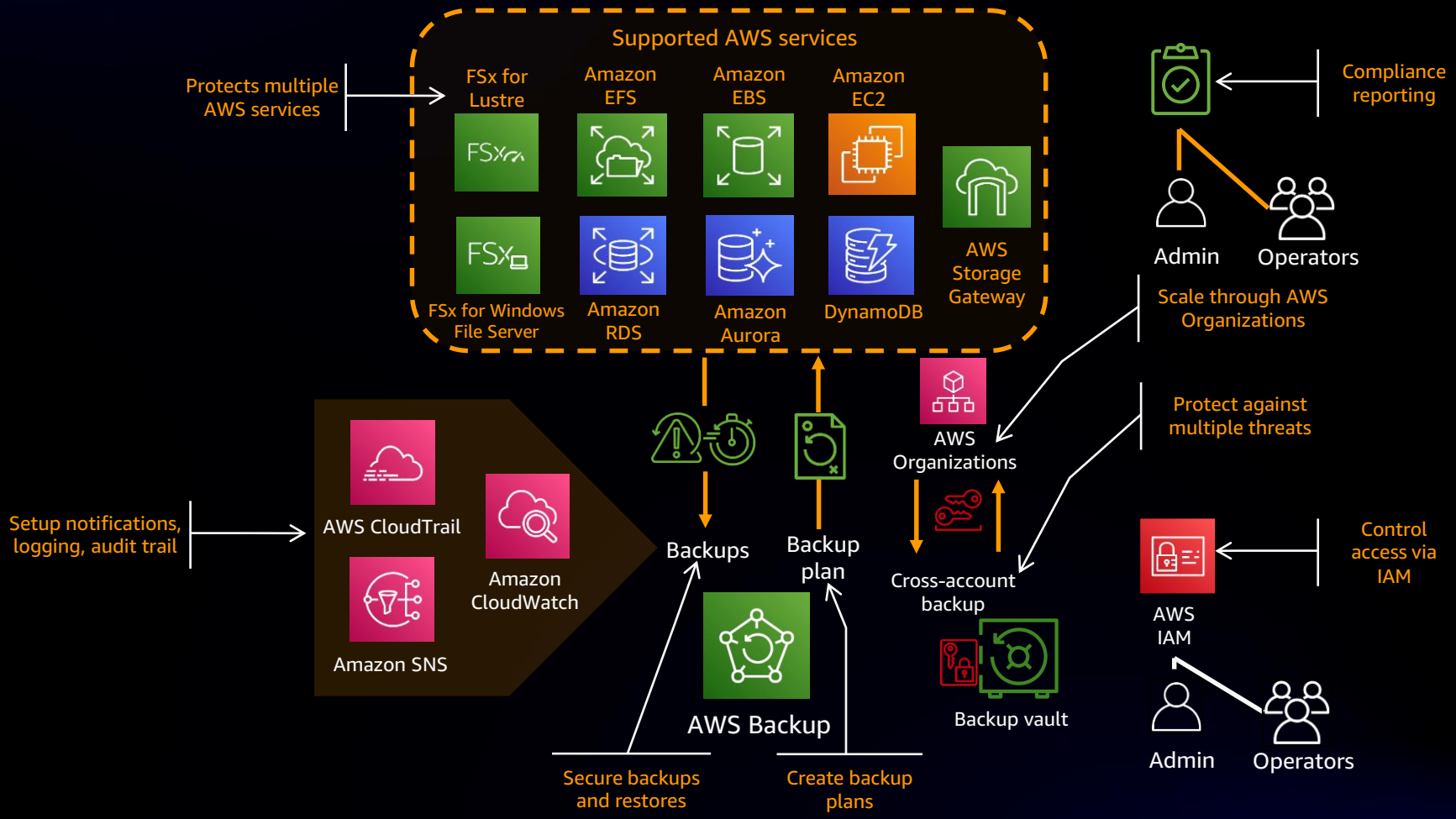
Amazon Neptune



Amazon Aurora

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How AWS Backup works



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key benefits of AWS Backup

Cloud-native data protection



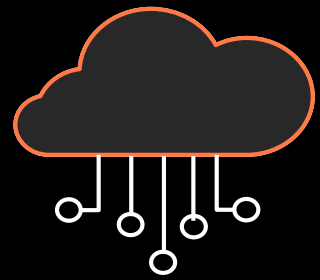
Protect your critical data across AWS services

Compliance



Simplify management of business & regulatory compliance

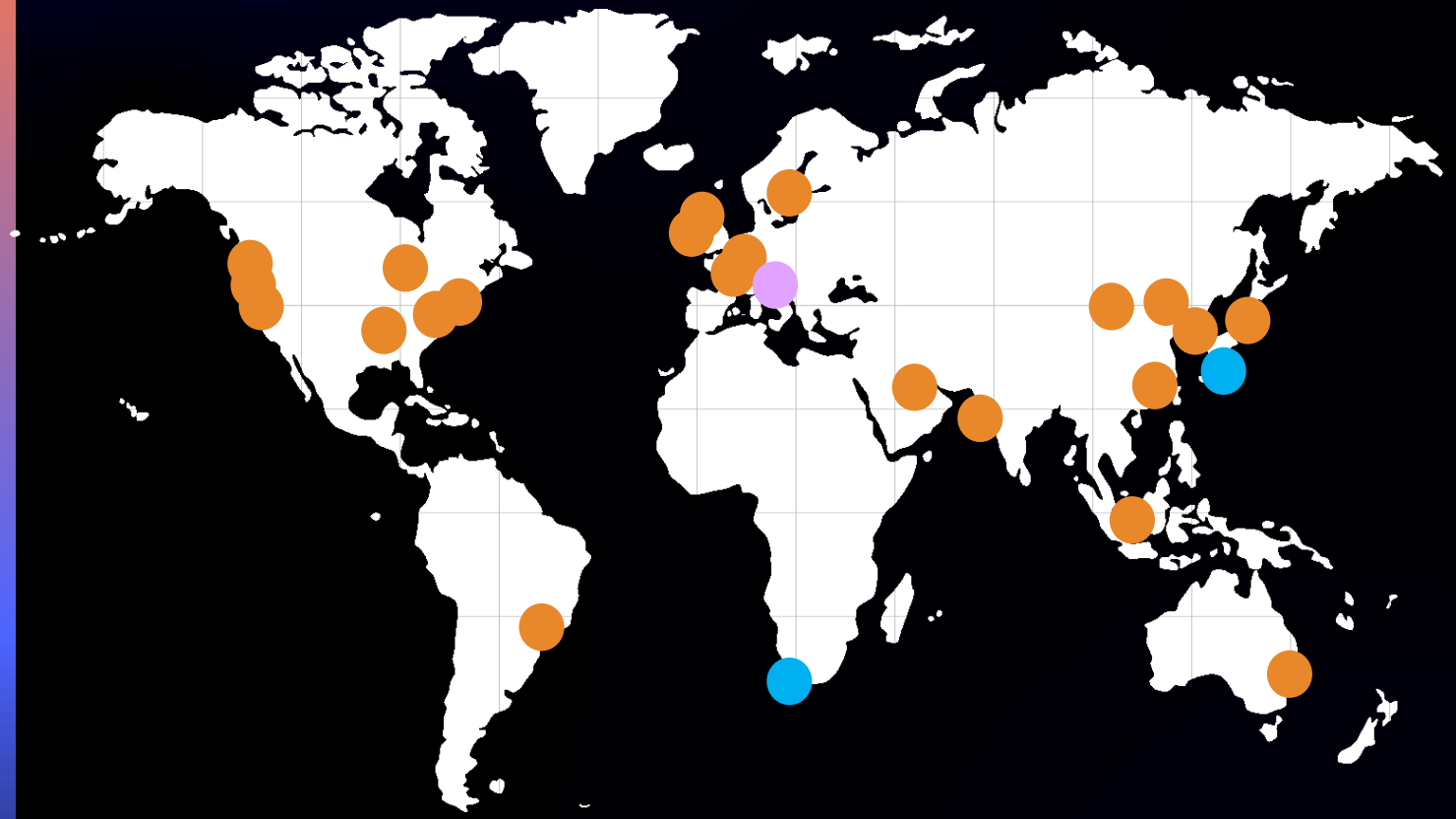
Disaster recovery



Reduce risk of downtime and build foundation for business continuity

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup is live in 25 Regions today



North America
- US-West-2 (Oregon)
- US-West-1 (N. Cal.)
- US-East-1 (N. Va.)
- US-East-2 (Ohio)
- Canada-Central-1 (Montreal)

GovCloud (US)
- GovCloud-East
- GovCloud-West

Europe
- EU-West-1 (Ireland)
- EU-West-2 (London)
- EU-West-3 (Paris)
- EU-Central-1 (Frankfurt)
- EU-North-1 (Stockholm)
- EU-South-1 (Milan)*

South America
- South America-East-1 (São Paulo)

Middle East
- ME-South-1 (Bahrain)

Africa
- Africa-South-1 (Cape Town)*

Asia Pacific
- APAC-Southeast-2 (Sydney)
- APAC-Southeast-1 (Singapore)
- APAC-Northeast-1 (Tokyo)
- APAC-Northeast-3 (Osaka)**
- APAC-Northeast-2 (Seoul)
- APAC-South-1 (Mumbai)
- APAC-East-1 (Hong Kong)

China
- China (Beijing) region
- China (Ningxia) region

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup key features

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Backup vaults: logical constructs for additional security



Backup vault

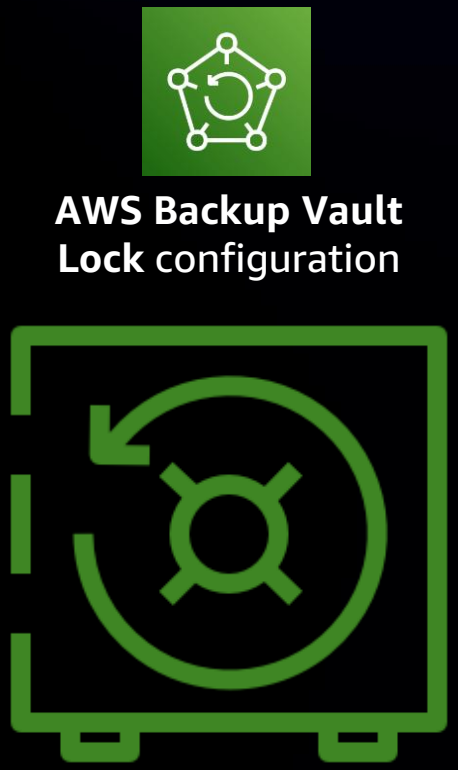


- Logical constructs – backup vaults are AWS Backup managed resources for storing backup data
- Control access – vaults are configurable to support resource level permissions via IAM and to separate permissions for different backups
- Encrypt separately – use a CMK or a service-specific default key for each vault
- Protect against deletion – vault data is visible to the respective service, but managed under vault access policy

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup Vault Lock

AWS Backup Vault Lock protects your backups against malicious or accidental actions



- Attached to the backup vault – you enable AWS Backup Vault Lock configuration at the backup vault level
- Protects against deletion – no user, including the root account, can delete your backups
- Protects against lifecycle changes – no user, including the root account, can change your backups' retention periods or update backups' transition to cold storage settings
- Enable AWS Backup Vault Lock using AWS Backup API, CLI, or SDK

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup supports cross-account backup



Cross-account backup

Without AWS Backup
No ability to send a backup to a separate account for controlled workflow productivity, or to help increase recovery options across multiple accounts

With AWS Backup
Automate backups to be copied and isolated across any accounts within an AWS Organization

- **Replaces:** Requiring third-party products, or manual orchestration with other tools
- **Benefit:** Flexible restores for use with DevOps, CI/CD, QA, analytics, and other needs outside normal data protection structure. Isolation of backup data, insurance against compromised AWS Org members, enhanced disaster recovery ,and ransomware protection.
- **How:** Supports SCP access policies through AWS Orgs – further restricts the use of, and the access to, destination vaults

Cross-account backup demo video
https://www.youtube.com/watch?v=dCy7ixko3tE

aws

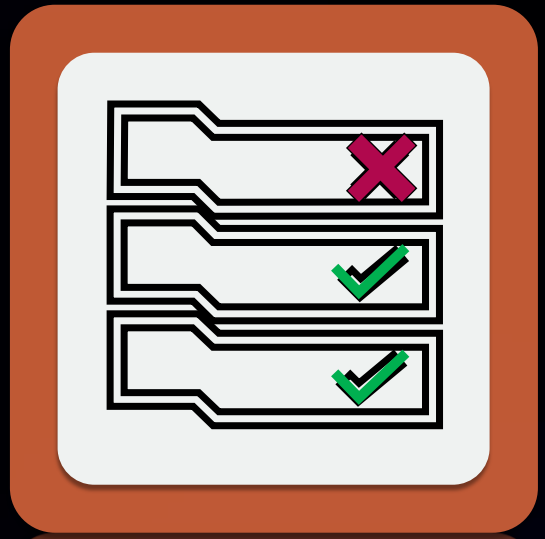
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup Audit Manager

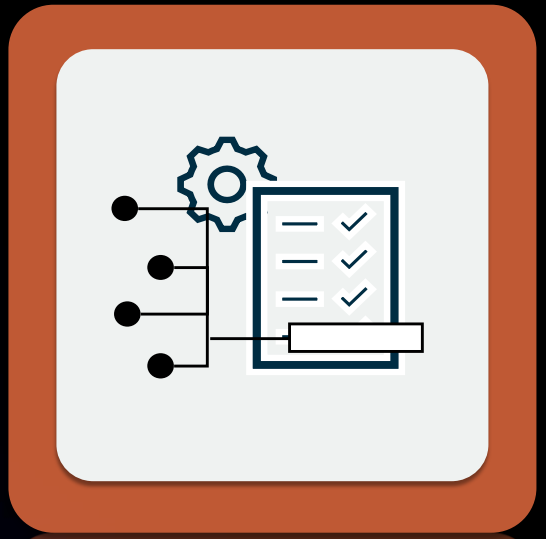
Monitor, evaluate, and demonstrate your backup compliance posture for centralized data governance



Continuously track your backup activities



Automatically audit your backup practices



Generate periodic and on-demand audit reports

aws

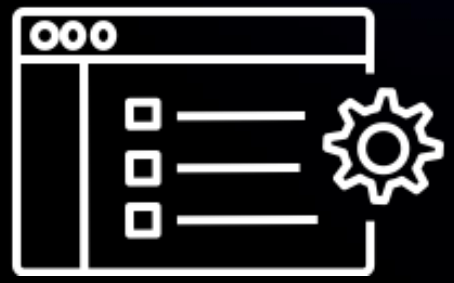
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customer experience

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Getting started

Single backup plan



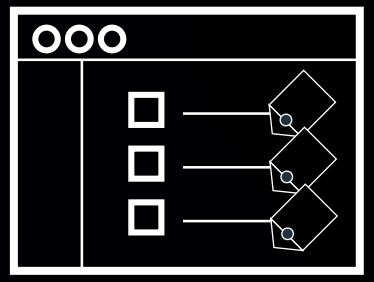
Define a backup schedule to specify the timing and frequency of backups, assign IAM roles

Step 1



Create a lifecycle policy to define timing of movement and period of retention

Step 2



Assign resources to the backup plan using tags or ARNs

Step 3



Manage and monitor backups

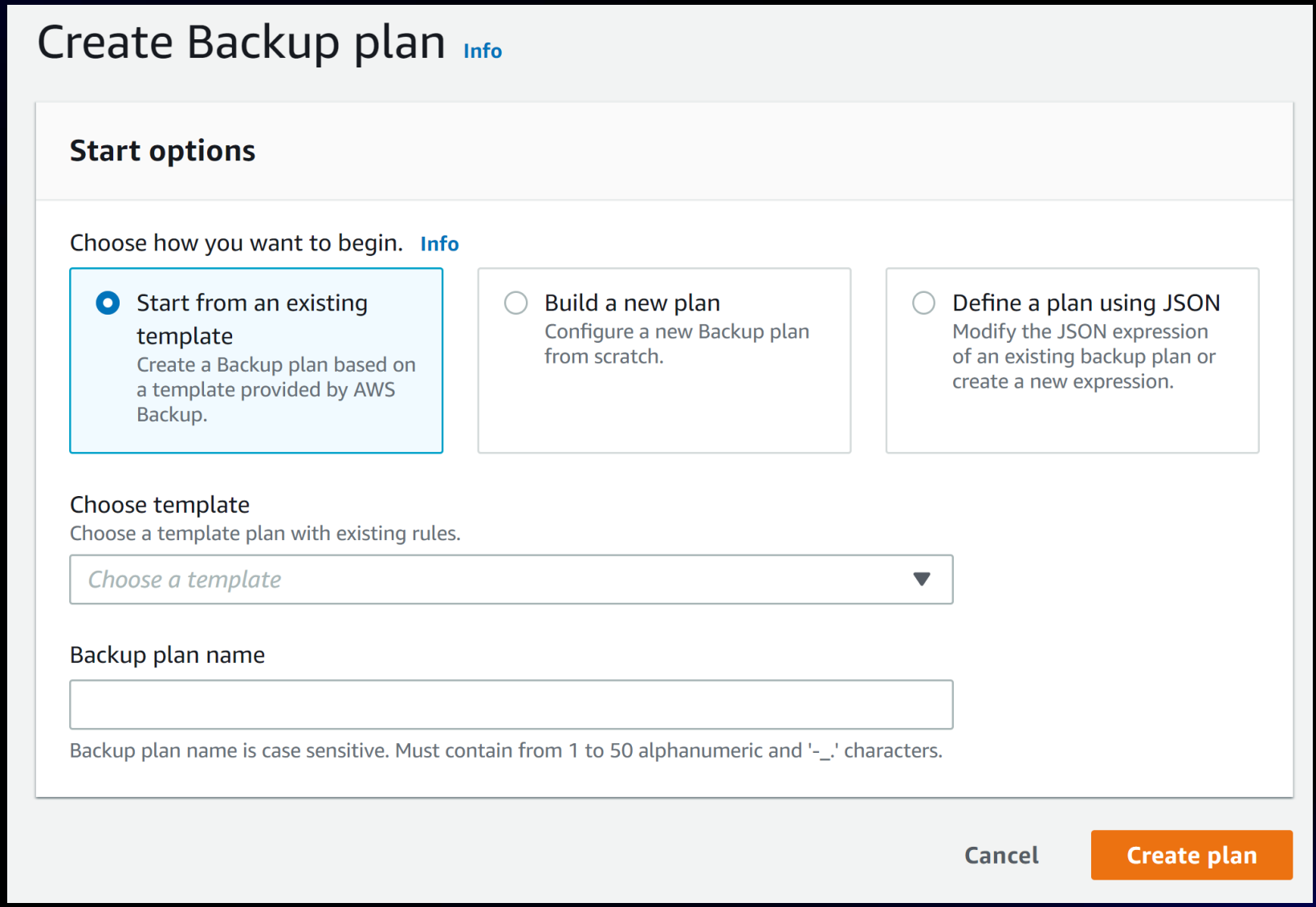
Step 4

A backup policy is a set of rules. Rules are created through these steps.

aws

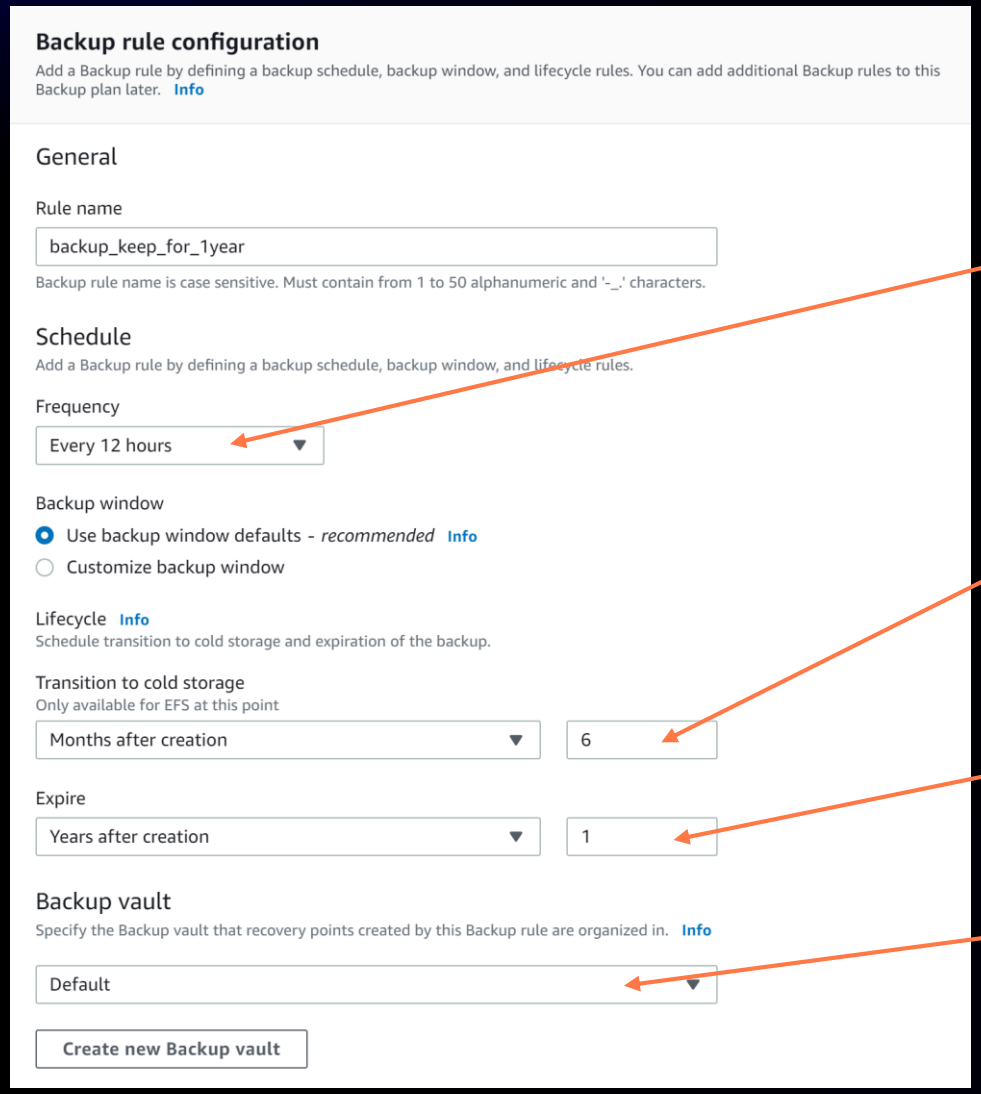
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Backup plans – Creation process



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Backup plans – Create backup rules



Set a frequency and backup window (all supported services)

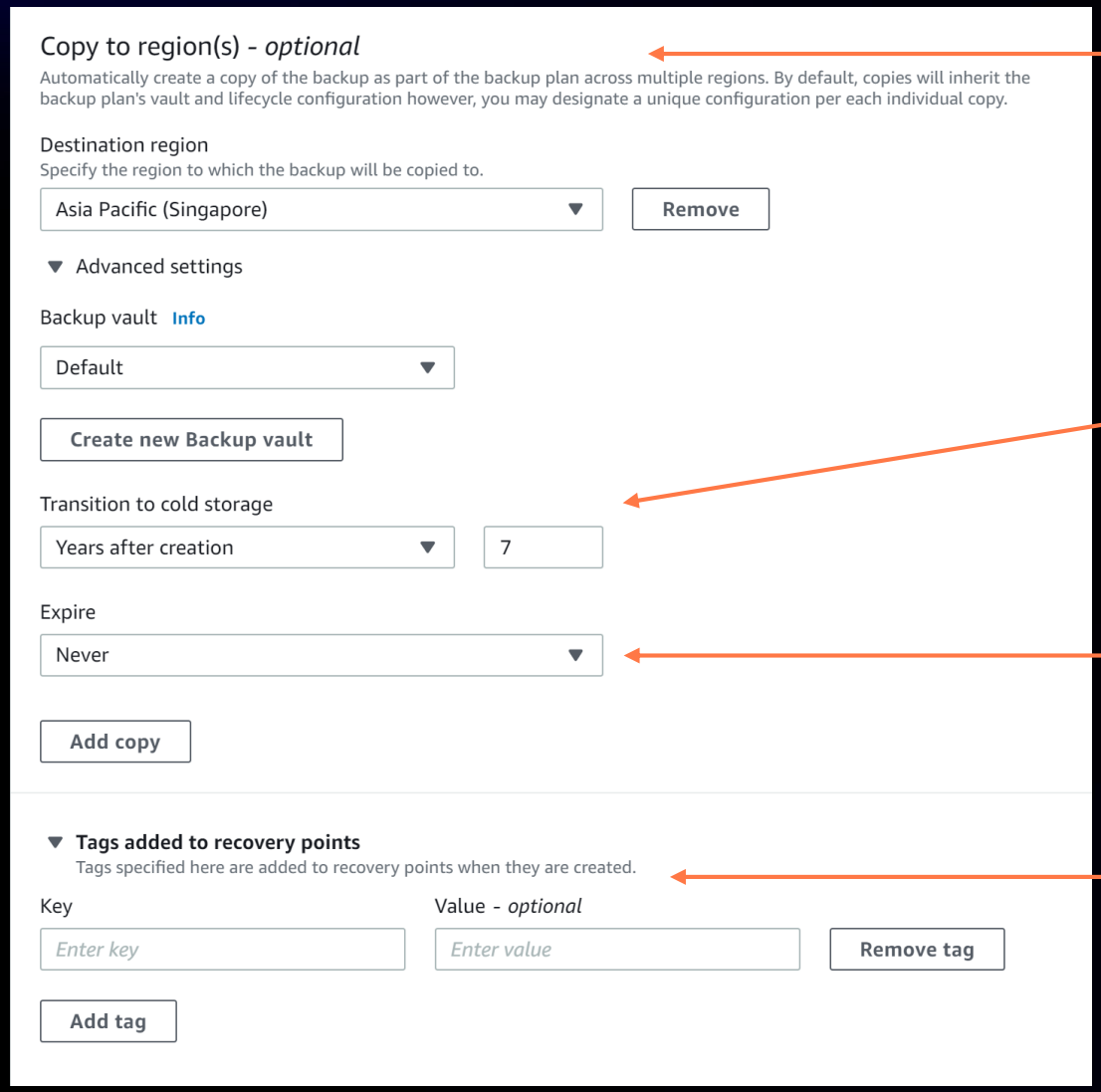
Transition to cold for lifecycle management (starting with Amazon EFS)

Expiry/retention (all supported services)

Backup vault

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Backup plans – Create backup rules



Copy to a different Region

Transition to cold for lifecycle management (starting with Amazon EFS) for cross-Region copy

Expiry/retention (all supported services) for cross-region copy

Tagging system

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.