VeeamON 2023

AWS Best Practices:

From Those That Build It!

Neils Engelen

Sr. Product Manager,
Product Management

Dustin Albertson

Director of Product Management,
Cloud & Applications

Agenda

- Introduction
- Best practices discussion
- Customer driven development
- Open forum/Q&A
- Conclusion

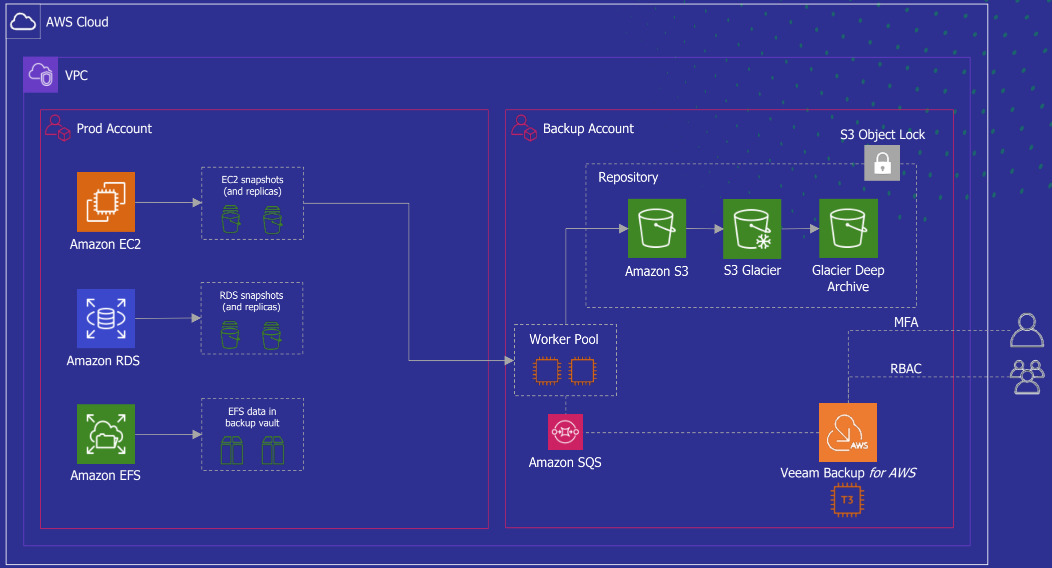
VEEAMON 2023

Introduction

Agenda

Who are we and why are we here?

- Who are we?
- What we are here to talk about today?
- Why we hope you join the conversation?
- Q&A



VeeamON 2023

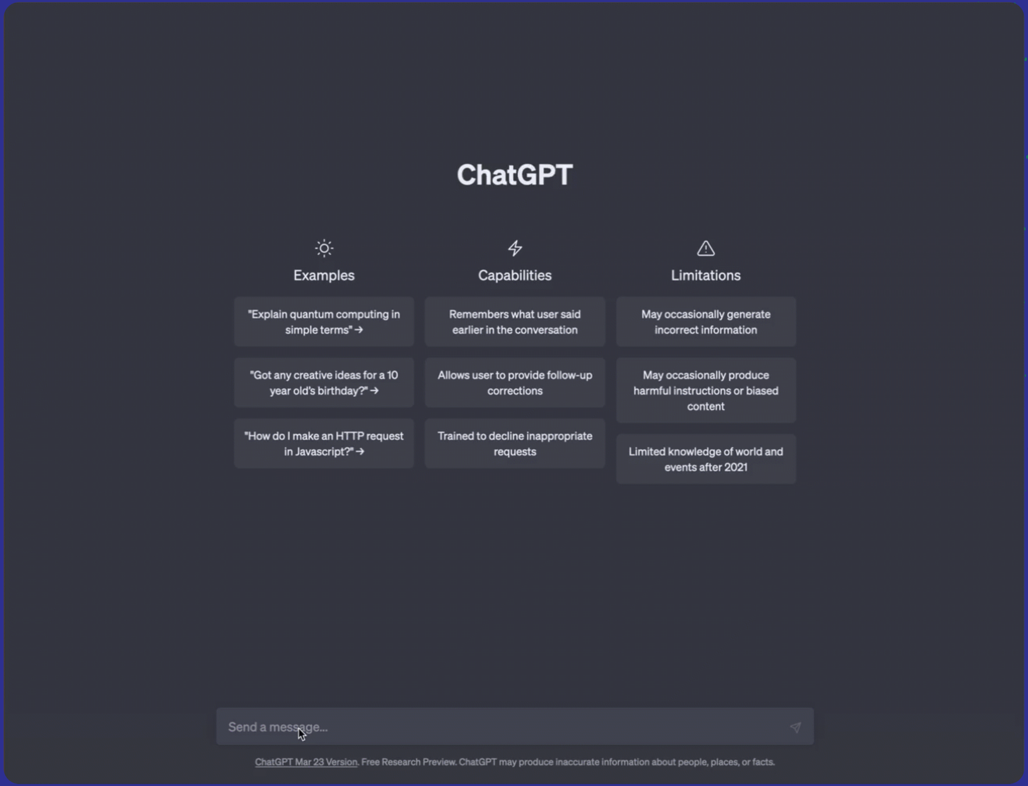
Best practices

AWS best practices

Does A.I. agree with us or not?

- Veeam® has a guide about them.
- AWS has a guide about them.
- Don’t want to take our word for it? How about we try something new?

AWS best practices



ChatGPT

Examples	Capabilities	Limitations
"Explain quantum computing in simple terms" →	Remembers what user said earlier in the conversation	May occasionally generate incorrect information
"Got any creative ideas for a 10 year old's birthday?" →	Allows user to provide follow-up corrections	May occasionally produce harmful instructions or biased content
"How do I make an HTTP request in Javascript?" →	Trained to decline inappropriate requests	Limited knowledge of world and events after 2021

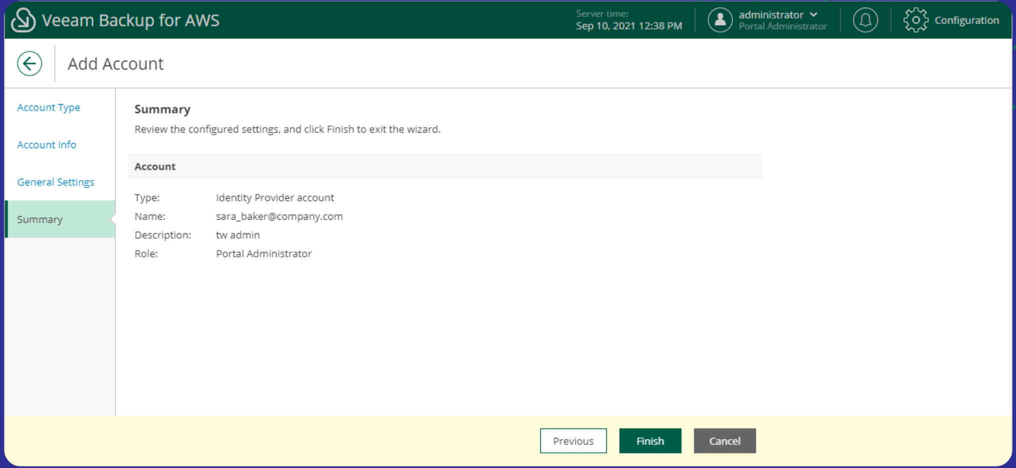
ChatGPT Mar 23 Version. Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts.

Follow the principle of least privilege

Not everyone needs to be an admin.

Limit permissions to only what is necessary for each user or service.

Avoid using overly permissive IAM (identity and access management) policies and regularly review and update permissions to ensure they are necessary and appropriate.



Summary

Review the configured settings, and click Finish to exit the wizard.

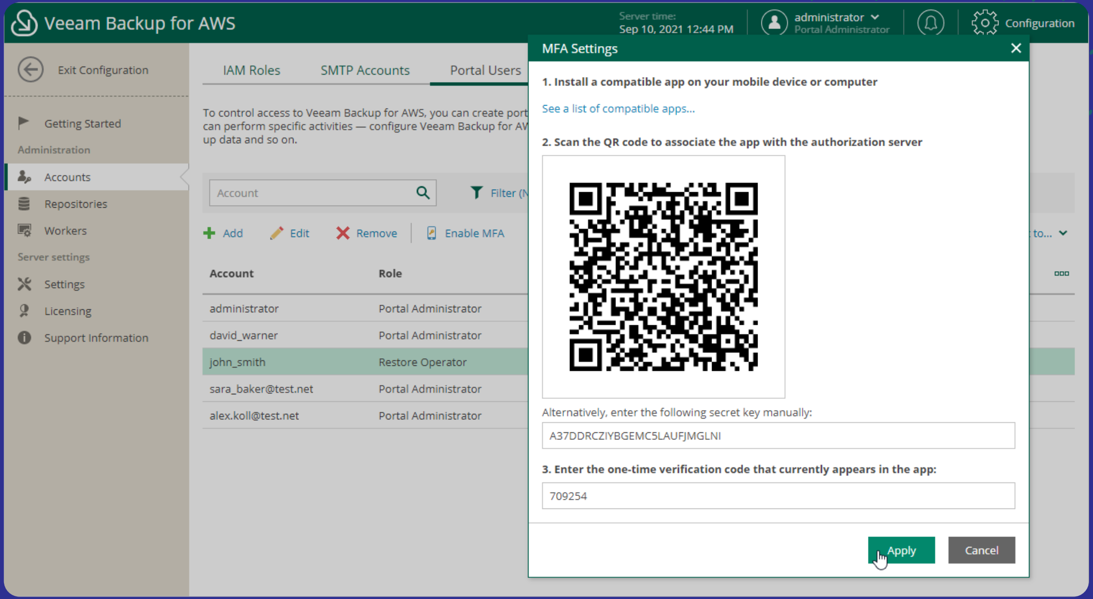
Account

Type:	Identity Provider account
Name:	sara_baker@company.com
Description:	tw admin
Role:	Portal Administrator

Enable Multi-Factor Authentication (MFA)

Prevent unauthorized access or MITM.

Require MFA for all AWS accounts to add an additional layer of security to protect against unauthorized access.



To control access to Veeam Backup for AWS, you can create port
can perform specific activities — configure Veeam Backup for AW
up data and so on.

Account	Role
administrator	Portal Administrator
david_warner	Portal Administrator
john_smith	Restore Operator
sara_baker@test.net	Portal Administrator
alex.koll@test.net	Portal Administrator

MFA Settings

1. Install a compatible app on your mobile device or computer

See a list of compatible apps...

2. Scan the QR code to associate the app with the authorization server

Alternatively, enter the following secret key manually:

A37DDRCZIYBGEMC5LAUFJMGLNI

3. Enter the one-time verification code that currently appears in the app:

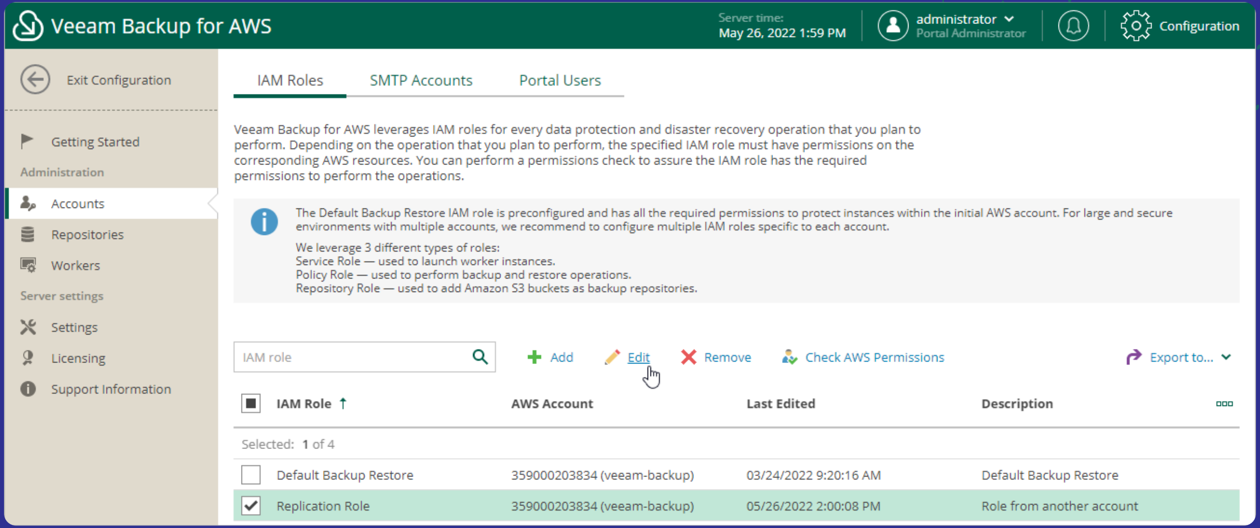
709254

Use AWS identity and access management roles

Least amount of permissions for the least amount of time.

Instead of using long-term access keys, **use IAM roles for EC2** instances, Lambda functions and other AWS resources to manage permissions.

IAM roles provide temporary credentials that are automatically rotated and are more secure than using permanent access keys.



Veeam Backup for AWS leverages IAM roles for every data protection and disaster recovery operation that you plan to perform. Depending on the operation that you plan to perform, the specified IAM role must have permissions on the corresponding AWS resources. You can perform a permissions check to assure the IAM role has the required permissions to perform the operations.

The Default Backup Restore IAM role is preconfigured and has all the required permissions to protect instances within the initial AWS account. For large and secure environments with multiple accounts, we recommend to configure multiple IAM roles specific to each account.

We leverage 3 different types of roles:
Service Role — used to launch worker instances.
Policy Role — used to perform backup and restore operations.
Repository Role — used to add Amazon S3 buckets as backup repositories.

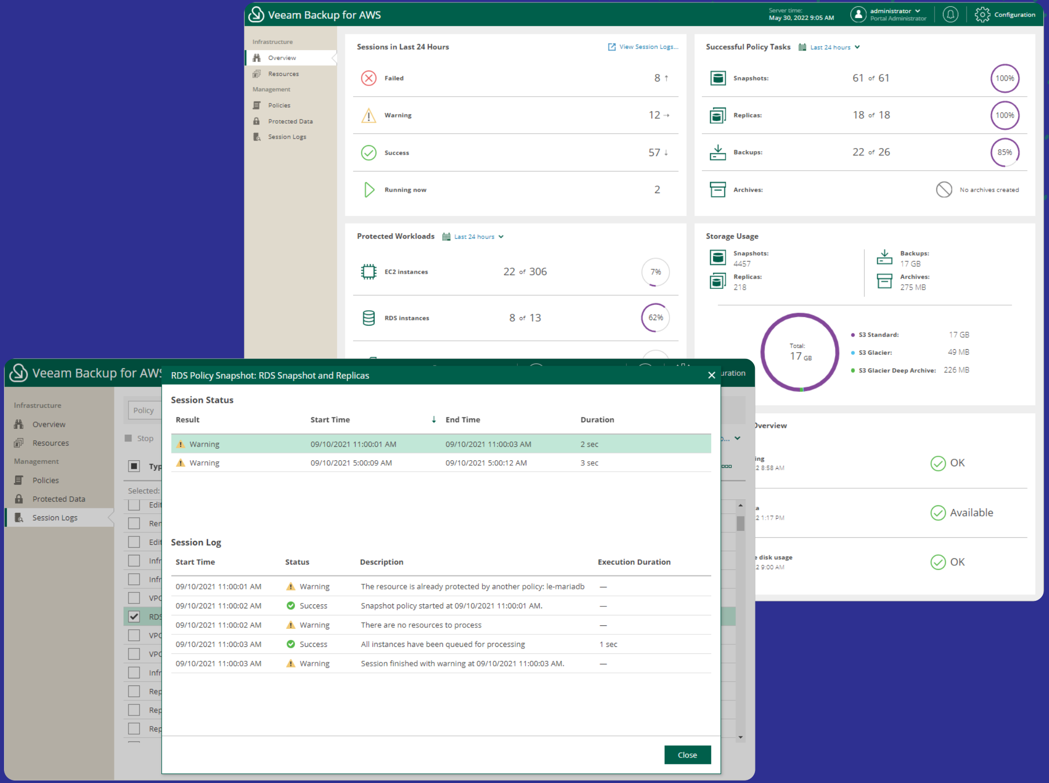
Selected: 1 of 4

■	IAM Role ↑	AWS Account	Last Edited	Description
□	Default Backup Restore	359000203834 (veeam-backup)	03/24/2022 9:20:16 AM	Default Backup Restore
☑	Replication Role	359000203834 (veeam-backup)	05/26/2022 2:00:08 PM	Role from another account

Regularly monitor and audit

Know what's going on.

- **Set up monitoring and logging** for all relevant AWS services to detect and respond to security incidents.
- **Use AWS CloudTrail** to log all API activity and use Amazon CloudWatch to monitor and alert on important metrics.
- **Regularly review** and analyze logs and other security-related events.



Sessions in Last 24 Hours

Failed	8 ↑
Warning	12 →
Success	57 ↓
Running now	2

Successful Policy Tasks

Snapshots:	61 of 61	100%
Replicas:	18 of 18	100%
Backups:	22 of 26	85%
Archives:		No archives created

Protected Workloads

EC2 instances	22 of 306	7%
RDS instances	8 of 13	62%

Storage Usage

Snapshots: 4457
Replicas: 218
Backups: 17 GB
Archives: 275 MB

Total: 17 GB

S3 Standard:	17 GB
S3 Glacier:	49 MB
S3 Glacier Deep Archive:	226 MB

RDS Policy Snapshot: RDS Snapshot and Replicas

Session Status

Result	Start Time	End Time	Duration
Warning	09/10/2021 11:00:01 AM	09/10/2021 11:00:03 AM	2 sec
Warning	09/10/2021 5:00:09 AM	09/10/2021 5:00:12 AM	3 sec

Session Log

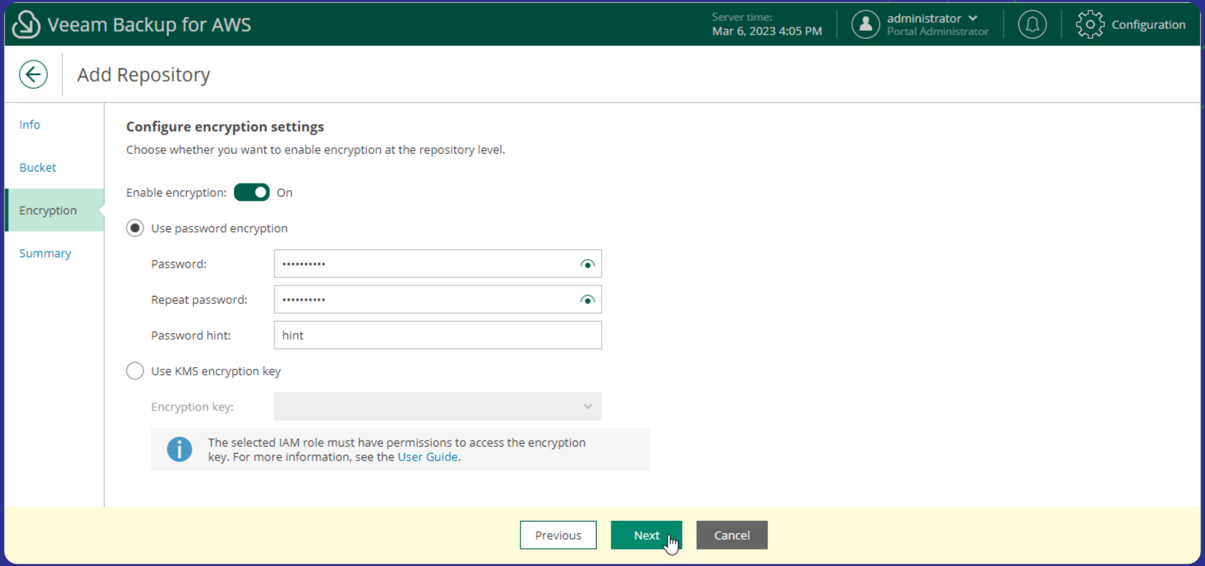
Start Time	Status	Description	Execution Duration
09/10/2021 11:00:01 AM	Warning	The resource is already protected by another policy: le-mariadb	—
09/10/2021 11:00:02 AM	Success	Snapshot policy started at 09/10/2021 11:00:01 AM.	—
09/10/2021 11:00:02 AM	Warning	There are no resources to process	—
09/10/2021 11:00:03 AM	Success	All instances have been queued for processing	1 sec
09/10/2021 11:00:03 AM	Warning	Session finished with warning at 09/10/2021 11:00:03 AM.	—

Encrypt your data

Lock it up!

Use AWS key management service (KMS) to manage encryption keys and encrypt data at rest and in transit.

Use SSL/TLS for data in transit and server-side encryption for data at rest in S3, RDS and other AWS services.



Configure encryption settings

Choose whether you want to enable encryption at the repository level.

Enable encryption: On

● Use password encryption

Password: ••••••••••

Repeat password: ••••••••••

Password hint: hint

○ Use KMS encryption key

Encryption key:

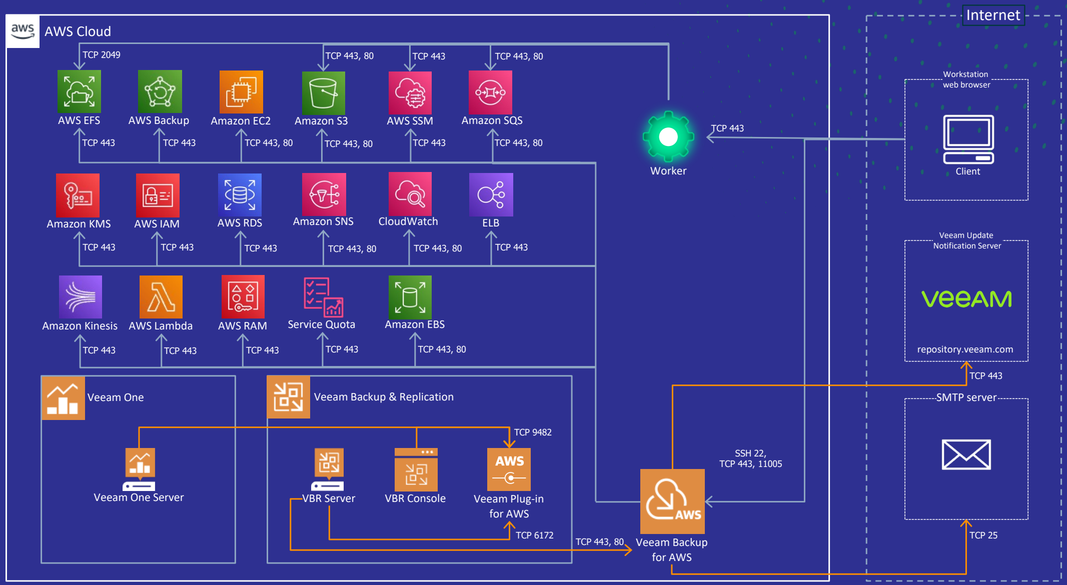
The selected IAM role must have permissions to access the encryption key. For more information, see the User Guide.

VeeamON 2023

Implement network security

Limit to needed ports.

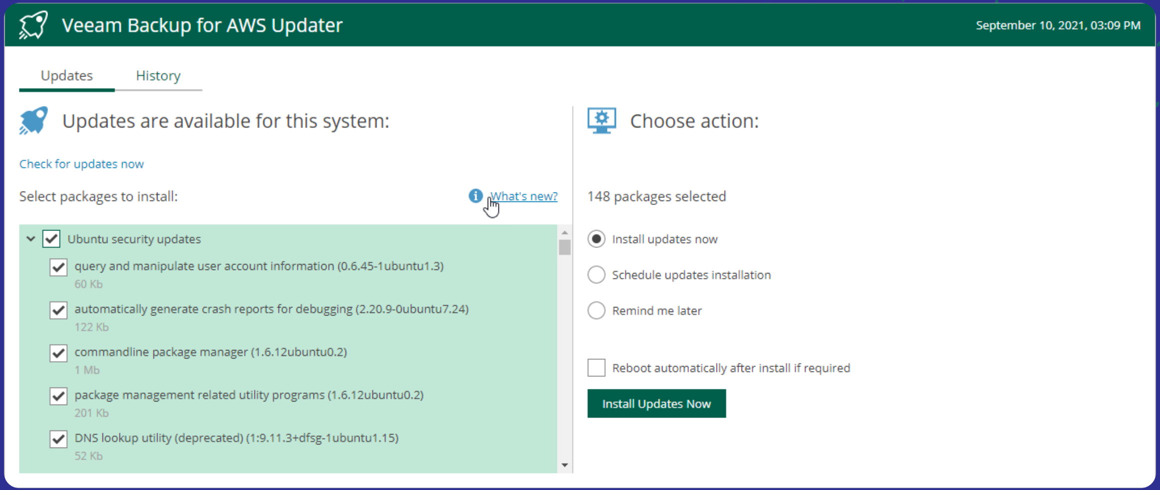
- **Use Amazon virtual private cloud** (VPC) to isolate resources and control network traffic between resources.
- **Use security groups** and network ACLs to restrict inbound and outbound traffic.
- **Limit public-facing access** to only what is necessary.



Patch and update

Update OS and apps.

Regularly apply patches and updates to all AWS resources, including EC2 instances, RDS databases and other services, to address security vulnerabilities and ensure they are up-to-date with the latest security patches.



Veeam Backup for AWS Updater

September 10, 2021, 03:09 PM

Updates are available for this system:

Check for updates now

Select packages to install:

What's new?

☑ Ubuntu security updates

- ☑ query and manipulate user account information (0.6.45-1ubuntu1.3)
  60 Kb
- ☑ automatically generate crash reports for debugging (2.20.9-0ubuntu7.24)
  122 Kb
- ☑ commandline package manager (1.6.12ubuntu0.2)
  1 Mb
- ☑ package management related utility programs (1.6.12ubuntu0.2)
  201 Kb
- ☑ DNS lookup utility (deprecated) (1:9.11.3+dfsg-1ubuntu1.15)
  52 Kb

Choose action:

148 packages selected

● Install updates now

○ Schedule updates installation

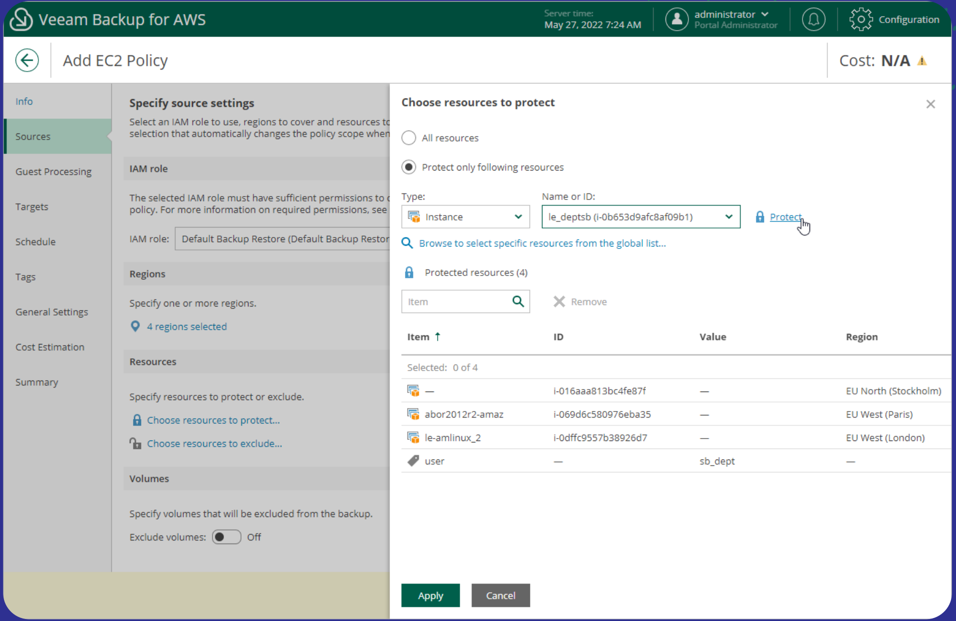
○ Remind me later

□ Reboot automatically after install if required

Use AWS security services

Prevent accidents before they happen.

Implement regular backups of critical data and store backups in a separate AWS region or account to protect against data loss and enable data recovery in case of an incident.



Specify source settings

Select an IAM role to use, regions to cover and resources tc
selection that automatically changes the policy scope when

IAM role

The selected IAM role must have sufficient permissions to c
policy. For more information on required permissions, see

IAM role: Default Backup Restore (Default Backup Restor

Regions

Specify one or more regions.

4 regions selected

Resources

Specify resources to protect or exclude.

Choose resources to protect...

Choose resources to exclude...

Volumes

Specify volumes that will be excluded from the backup.

Exclude volumes: Off

Choose resources to protect

○ All resources

● Protect only following resources

Type: Instance

Name or ID: le_deptsb (i-0b653d9afc8af09b1)

Protect

Browse to select specific resources from the global list...

Protected resources (4)

Item

Remove

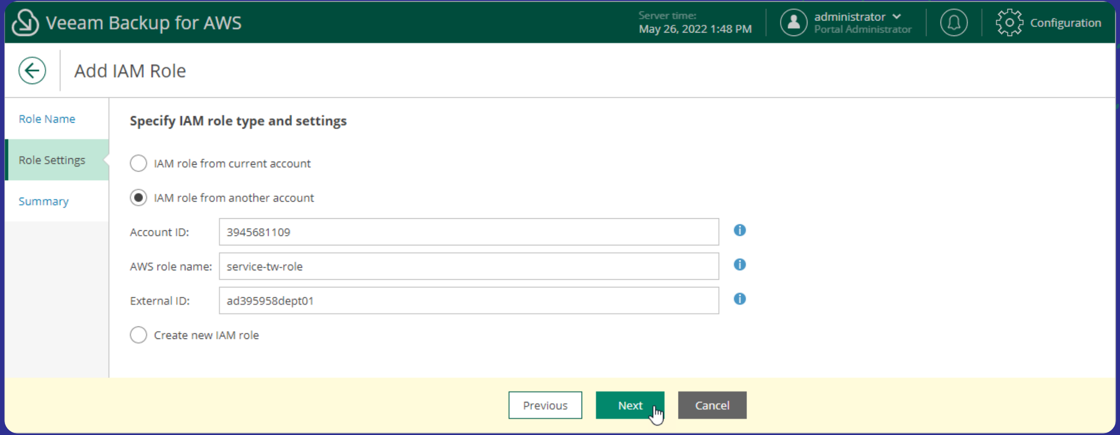
Selected: 0 of 4

Item ↑	ID	Value	Region
—	i-016aaa813bc4fe87f	—	EU North (Stockholm)
abor2012r2-amaz	i-069d6c580976eba35	—	EU West (Paris)
le-amlinux_2	i-0dffc9557b38926d7	—	EU West (London)
user	—	sb_dept	—

Use AWS security services

Prevent accidents before they happen.

Leverage AWS security services such as AWS WAF (Web Application Firewall), AWS Shield and AWS Security Hub to provide additional layers of security and gain insights into your AWS environment.



Specify IAM role type and settings

○ IAM role from current account

● IAM role from another account

Account ID: 3945681109

AWS role name: service-tw-role

External ID: ad395958dept01

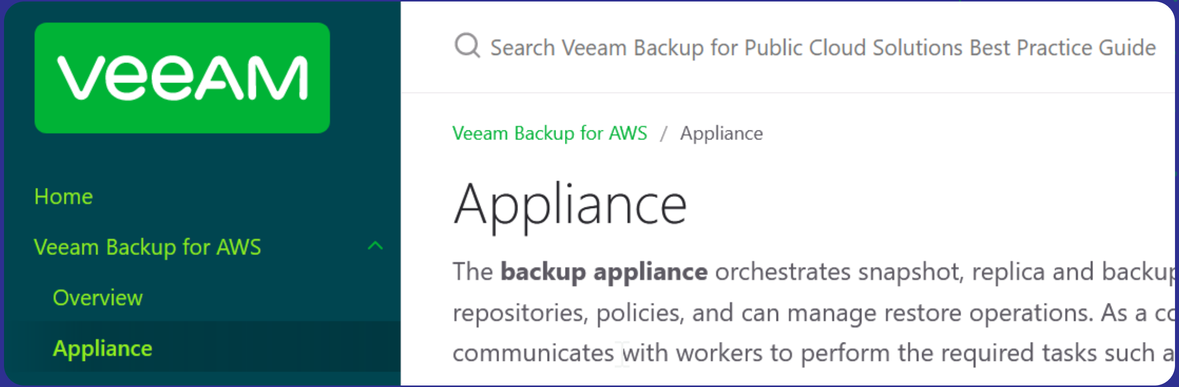
○ Create new IAM role

Follow AWS security best practices

Read up on direct R&D testing and design

Veeam maintains a guide based upon feedback from both customers and QA testing to provide full details on how to best configure policies, repositories, size the appliance...

Follow VB for AWS sizing and scaling guide



Search Veeam Backup for Public Cloud Solutions Best Practice Guide

Veeam Backup for AWS / Appliance

Appliance

The **backup appliance** orchestrates snapshot, replica and backup
repositories, policies, and can manage restore operations. As a co
communicates with workers to perform the required tasks such a

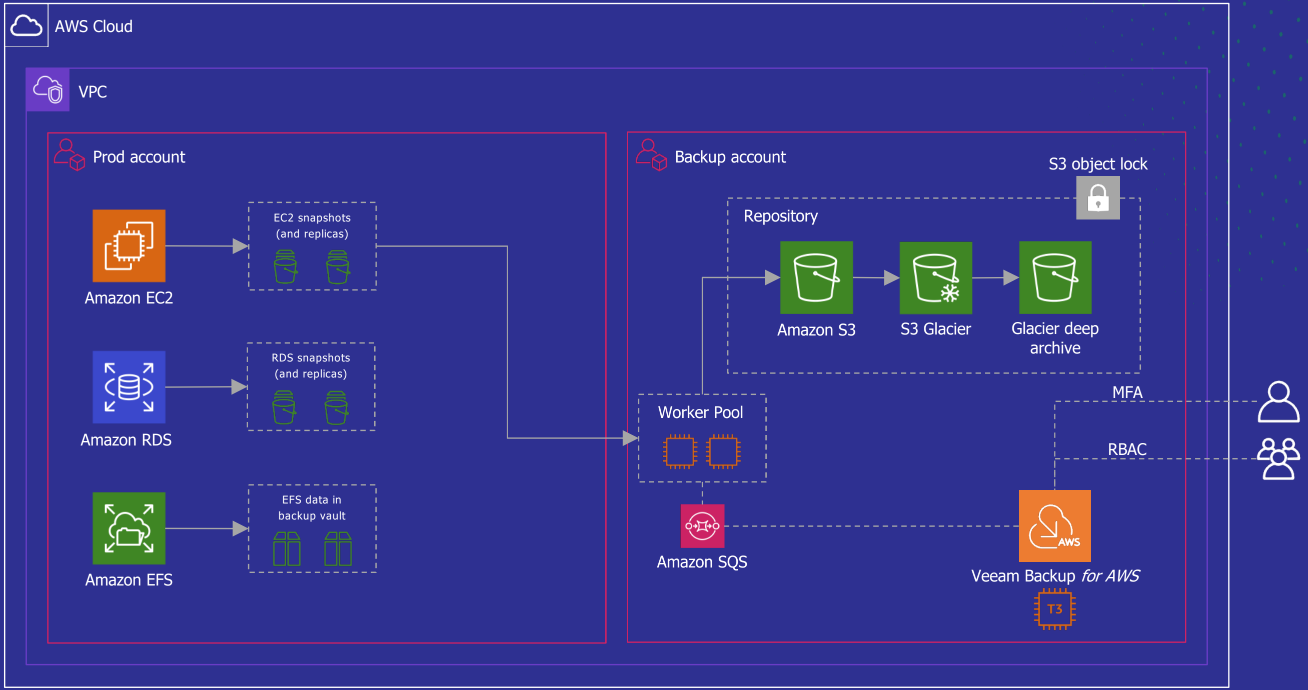
Read up on direct R&D testing and design

Veeam maintains a guide based upon feedback from both customers and QA testing to provide full details on how to best configure policies, repositories, size the appliance...

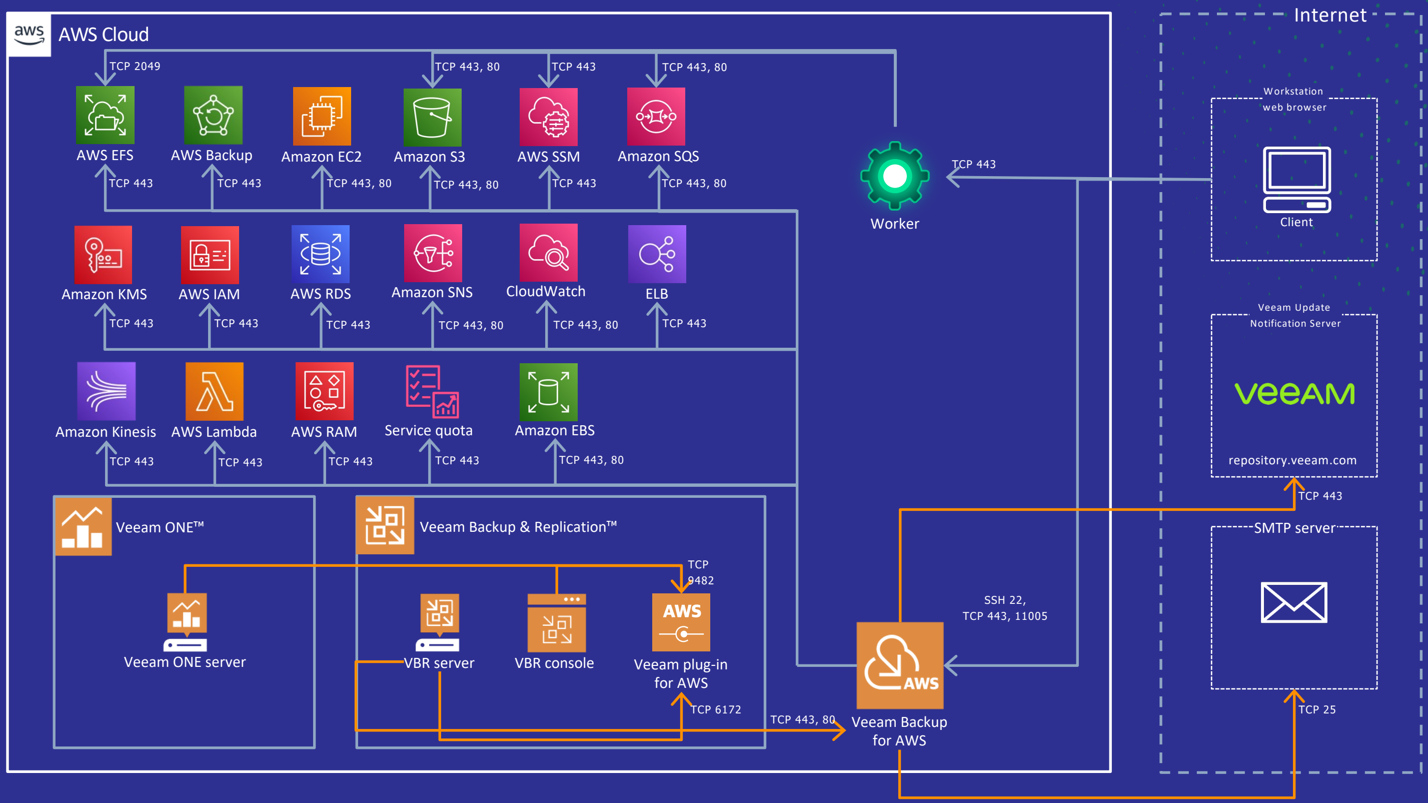
VeeamON 2023

Veeam’s cloud-native backup

What can we protect?



Tight integration with AWS services



VeeamON 2023

Customer driven development

We are here to listen

Veeam is focussed on customers as the #1 priority

- We rely on your feedback, feature requests...
- Veeam R&D Forums are a direct connection to R&D (https://forums.veeam.com).
  Useful for technical questions as well
- Veeam support is available to assist with configuration issues
- Open source (https://github.com/VeeamHub) and script community: VeeamHUB

VeeamON 2023

Q&A

Thank you!

VeeamON 2023