AWS CodeCommit

DevOps is a popular culture and AWS being a popular cloud provider and both are in demand. So how to implement DevOps on AWS?
AWS responded to this with a set of services that ensured one could carry out the process of continuous and integration and continuous deployment on the cloud and one of those services is **AWS CodeCommit.**

Overview Of AWS CodeCommit

AWS CodeCommit is a version control service hosted by Amazon Web Services (AWS) that you can use to privately store and manage assets such as documents, source code, and binary files. It is an in-house repository or infrastructure that lets you host or hold repositories. AWS CodeCommit basically gives you an environment where you can actually go ahead commit your code, code push it, or pull it.

AWS CodeCommit is a fully-managed source control service that hosts your secure Git-based repositories. It makes it easy for groups to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your source control system or worry about scaling its infrastructure. CodeCommit securely stores anything from source code to binaries, and it runs seamlessly with your existing Git tools.

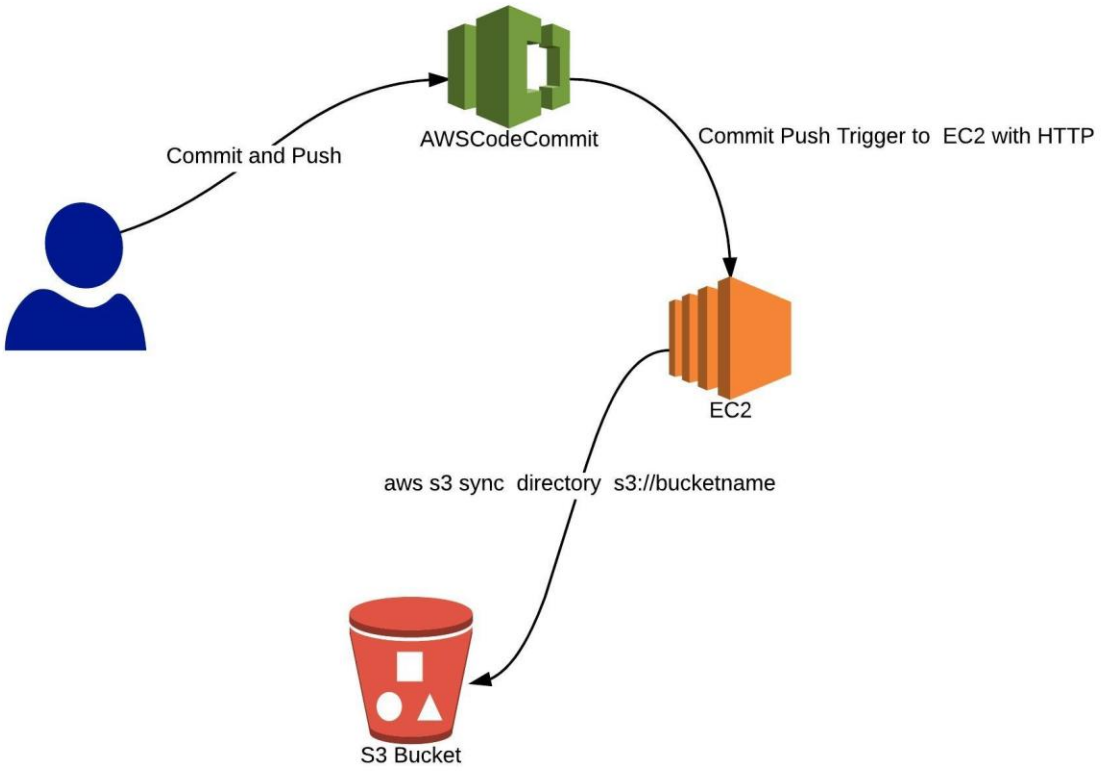
Benefits Of AWS CodeCommit

- **Store any type of Code:** AWS CodeCommit lets you store any type of code as there are very fewer restrictions on the type and the extensions of the code that you store.
- **Fully Managed:** AWS CodeCommit eliminates the need to host, maintain, back up, and scale your own source control servers. The service automatically scales to meet the growing needs of your project.
- **Highly Secure:** Security is something which you don't need to worry about with AWS Code Commit., like the code, you push or pull is encrypted. CodeCommit is integrated with AWS

Identity and Access Management (IAM) allowing you to customize user-specific access to your repositories.

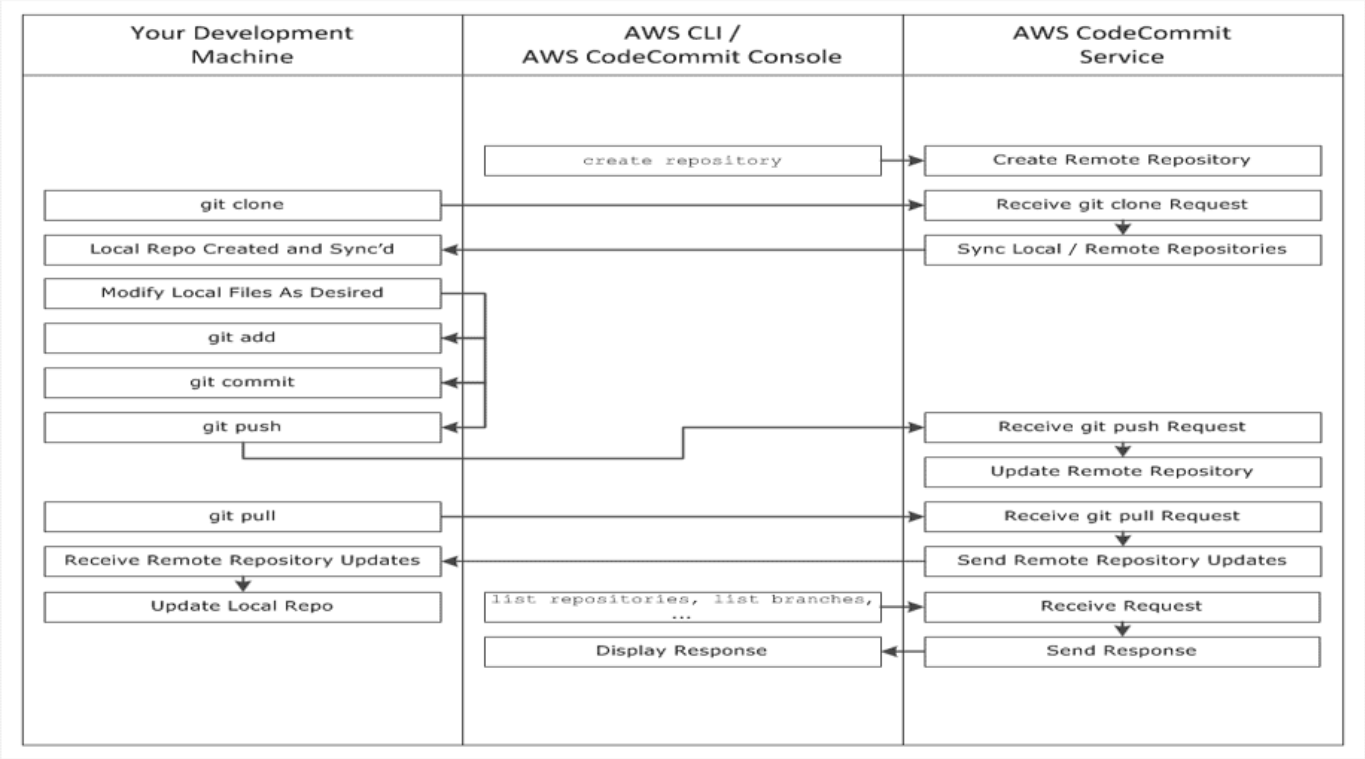
- **Ensures Collaborative Work:** AWS CodeCommit helps you collaborate on code with teammates via pull requests, branching and merging, and you can give proper access to people who can access this piece of code, make changes to it and under different IAM users and under different security groups this process becomes very much engaging and collaborative.
- **Faster development lifecycle:** AWS CodeCommit keeps your repositories close to your build, staging, and production environments in the AWS cloud. You can transfer incremental changes instead of the entire application. This allows you to increase the speed and frequency of your development lifecycle.
- **Scale Easily:** When you talk about cloud platforms and any service, it ensures scalability so does the amount of code you push on this particular service.
- **Integrate with third-party tools:** The best thing about AWS CodeCommit is that it places your code in such locations that it becomes very easy to integrate with your third-party tools. You can keep using your preferred development environment plugins, continuous integration/continuous delivery systems, and graphical clients with CodeCommit.

.



Before creating an AWS CodeCommit Repository lets check its working first.

Working Of AWS Code Commit



AWS Trusted Advisor

AWS Trusted Advisor is your personal cloud expert! It helps you to provide best practices for AWS by inspecting your AWS environment with a motto toward saving money, improving system performance and reliability, and closing security gaps to protect.

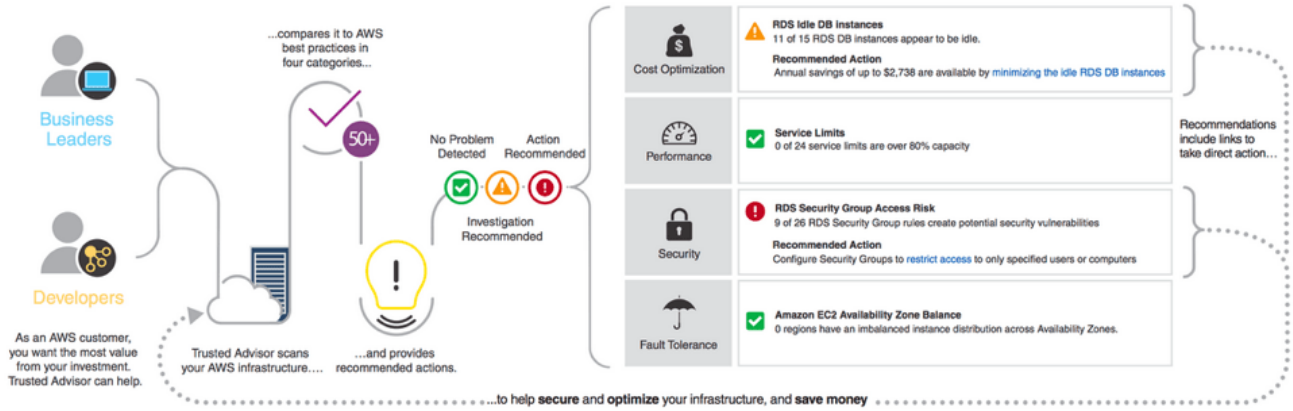
What is AWS Trusted Advisor?

AWS Trusted Advisor is an AWS tool that provides you real-time assistance to help you provision your resources following AWS best practices. It checks to help optimize your AWS infrastructure, provide better security and performance, reduce your overall costs, and also monitor service limits. Whether you want to develop applications, or as part of ongoing improvement, Always take advantage of the recommendations provided by Trusted Advisor it helps keep your solutions provisioned optimally.

How does it Work?

The Trusted Advisor scans an organization's cloud infrastructure and provides recommendations based on the defined best practices. The basic recommendations can be grouped into three categories:

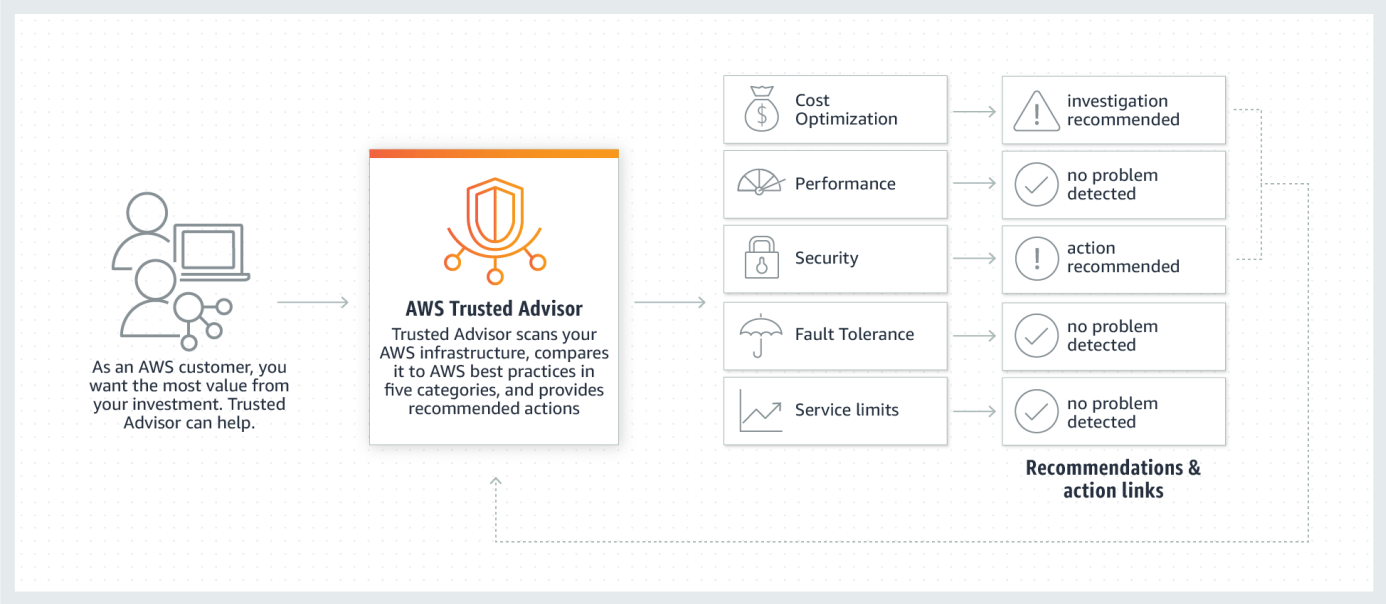
- **No problem detected**—a green check.
- **Investigation recommended**—an orange exclamation mark.
- **Action recommended**—a red exclamation mark.



If you are planning to migrate to the AWS cloud or to set up a new cloud application, Trusted Advisor's recommendations can help you to optimize your cloud infrastructure. For example, if you are planning to set up a new RDS instance and receive a notification from AWS Trusted Advisor that two of 15 RDS instances have been idle for more than 30 days, you can investigate and plan to utilize one of the idle instances rather than introducing a new one. This saves costs for your organization.

AWS Trusted Advisor Check large section of services which can be grouped into four categories:

1. **Cost Optimization**—recommendations provided by Trusted Advisor can reduce expenses by highlighting idle resources or by committing reserved resources.
2. **Security**—With the help of AWS Trusted Advisor user can harden their AWS services against intruders by enabling various security features.
3. **Fault Tolerance**—suggestions that enhance the resilience of your applications by highlighting health issues, missing backups, and redundancy shortfalls.
4. **Performance**—recommendations that can increase the overall performance of your applications and cloud infrastructure by checking your service limits and monitoring instances.



Best Practices Of AWS Trusted Advisor At No Charge
The following Trusted Advisor checks are now available to all AWS users:

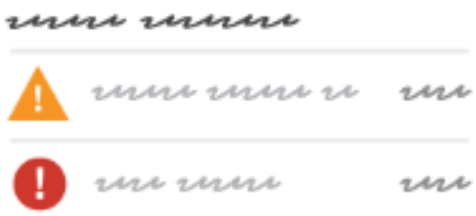
- **Service Limits Check** – This check inspects your usage with regard to the most important service limits for each AWS product. It alerts you when you are using more than 80% of your allocation resources such as EC2 instances and EBS volumes.
- **Security Groups – Specific Ports Unrestricted Check** – This check will look for and notify you of overly permissive access to your EC2 instances and help you to avoid malicious activities such as hacking, denial-of-service attacks, and loss of data.
- **IAM Use Check –** This check alerts you if you are using account-level credentials to control access to your AWS resources instead of following security best practices by creating users, groups, and roles to control access to the resources.
- **MFA on Root Account Check –** This check recommends the use of multi-factor authentication (MFA), to improve security by requiring additional authentication data from a secondary device.

Check Also: Free AWS Training and Certifications

Features and Functionalities

AWS Trusted Advisor provides many features for you to customize recommendations and to proactively monitor your AWS resources.

Recent Changes (Available with Business or Enterprise-level Support Plan)
You can track recent changes in check status on the console dashboard. The most recent changes appear at the top of the list to bring them to your attention.



Exclude Items
The “exclude items” feature allows you to customize the Trusted Advisor report. You can exclude items from the check result if they are not relevant; the excluded items appear separately, and you can restore (include) them at any time.

Action Links (beta)
You can track recent changes in check status on the console dashboard. The most recent changes appear at the top of the list to bring them to your attention.

Access Management
You can use AWS Identity and Access Management (IAM) to control access to specific checks or check categories.

Refresh
You can refresh a check every 5 minutes. You can refresh individual checks or refresh all the checks at once by clicking the Refresh All button in the top-right corner of the summary dashboard.

AWS Trusted Advisor Explorer vs. AWS Systems Manager Explorer

AWS announced on **May 4** that AWS Systems Manager Explorer will provide a multi-account summary of Trusted Advisor checks. There are a few differences between the services:

- Systems Manager Explorer will aggregate all AWS Trusted Advisor checks, including performance, security, and reliability checks. AWS Trusted Advisor Explorer will only aggregate cost optimization recommendations provided after evaluation.
- Systems Manager Explorer is available in maximum regions, while AWS Advisor Explorer is limited to few regions (AWS recommends using US-East region) because it relies on multiple services that are not available in all regions.
- AWS Trusted Advisor Explorer is capable of providing more flexibility since it is a CloudFormation template user can modify. It also allows us to use data queries via AWS Athena (SQL style) and custom dashboards resource tags and external visualization tools. AWS Systems Manager Explorer supports queries via AWS API to create custom reports and custom dashboards are available with pre-set widgets as defined by AWS.