



アーキテクチャ図

AWS GovCloud での Secure Cloud Computing Architecture (SCCA)



AWS GovCloud での Secure Cloud Computing Architecture (SCCA): アーキテクチャ図

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

AWS GovCloud での SCCA i

AWS GovCloud での Secure Cloud Computing Architecture (SCCA) 1

詳細情報 2

図の履歴 2

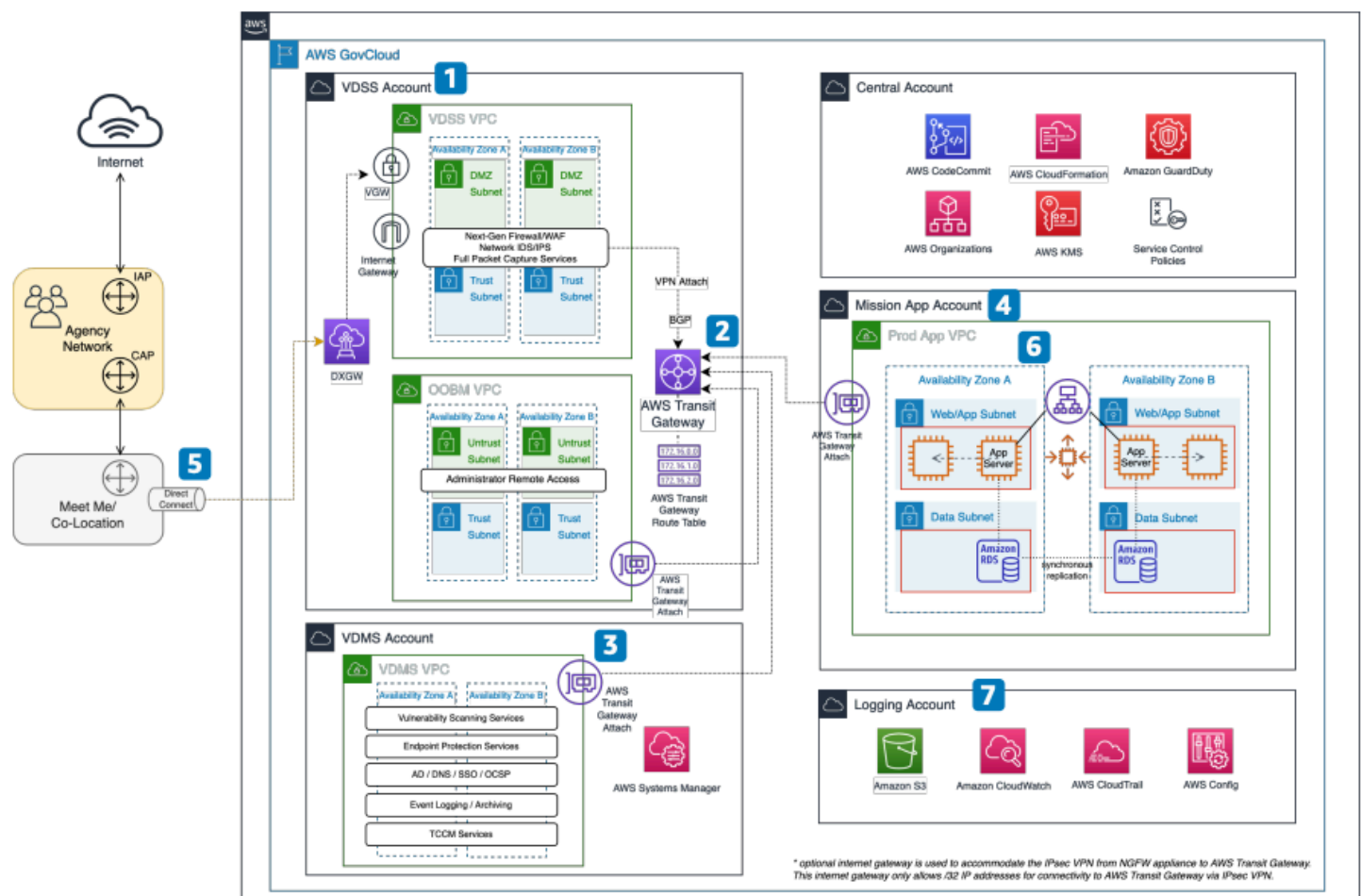
..... iii

AWS GovCloud での Secure Cloud Computing Architecture (SCCA)

公開日: 2022 年 6 月 20 日 ([図の履歴](#))

このアーキテクチャは、AWS GovCloud (米国) に DISA 準拠のランディングゾーンを構築する方法を示しています。この環境で国防総省のワークロードを実行できます。

AWS GovCloud での Secure Cloud Computing Architecture (SCCA)



1. Virtual Data Center Security Stack (VDSS) アカウントは、ミッション所有者アプリケーションを保護するための境界として機能します。
2. AWS Transit Gateway は、スポークとして機能するすべての接続ネットワーク間でトラフィックがどのようにルーティングされるかを制御するハブとして機能します。

3. Virtual Data Center Management Stack (VDMS) アカウントには、HBSS、ACAS、認証システム、その他の一般的なサービスなどの機能が含まれています。
4. コアワークロードは、Mission アプリアカウントにデプロイされます。Mission App VPC との間すべての通信は VDSS を通過し、VPS から共有サービスを消費します。
5. Virtual Private Gateway (VGW) は、国防総省情報ネットワークまたは他の機関ネットワークへの接続を提供します。
6. 一般的な多層ミッションワークロードでは、Elastic Load Balancing、AWS Auto Scaling グループ、複数のアベイラビリティゾーンを使用して高可用性とスケーラビリティを実現します。
7. ログ記録アカウントは、ログが集約および保存されるイミュータブルな場所を表します。

詳細情報

詳細については、「」を参照してください。

- [AWS アーキテクチャアイコン](#)
- [AWS アーキテクチャセンター](#)
- [AWS Well-Architected](#)
- [AWS GovCloud 製品ページ](#)

図の履歴

このリファレンスアーキテクチャ図の更新について通知を受け取るには、RSS フィードにサブスクライブします。

変更	説明	日付
初版発行	リファレンスアーキテクチャ図が最初に公開されました。	2022 年 6 月 20 日

Note

RSS 更新をサブスクライブするには、使用しているブラウザで RSS プラグインが有効になっている必要があります。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。