



Amazon OpenSearch Service セキュリティベストプラクティス AWS Black Belt Online Seminar

Yu Sato

Professional Services
2023/04

AWS Black Belt Online Seminarとは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWS の技術担当者が、AWSの各サービスやソリューションについてテーマごとに動画を公開します
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます
- 以下のURLより、過去のセミナー含めた資料などをダウンロードすることができます
- <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>

内容についての注意点

- 本資料では 2023 年 04 月時点のサービス内容および価格についてご説明しています。最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっております。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

名前：佐藤 悠 (Yu, Sato)

所属：アマゾンウェブサービスジャパン
プロフェッショナルサービス本部
ビッグデータコンサルタント

経歴：大手 SI 会社でデータ分析基盤の構築や運用、
加工パイプラインの作成、機械学習モデルの
システム化などに従事

好きなAWSサービス: Amazon OpenSearch Service,
AWS Glue, AWS Lake Formation



トピック

1. アクセスコントロール
2. データ保護
3. 監査
4. ベストプラクティス

Amazon OpenSearch Service の多層セキュリティ



- ① SAML および Cognito、IAM (Identity Access Management) と統合された Dashboards アクセスコントロール
- ② IAM (Identity Access Management) による API エンドポイントへのアクセスコントロール
- ③ VPC 内にデプロイされたエンドポイントへのセキュリティグループを利用したアクセス制御
- ④ OpenSearch のきめ細やかなアクセス制御機能によるデータおよびダッシュボードの保護
- ⑤ 転送データの暗号化
- ⑥ 保管されたデータの暗号化

1. アクセスコントロール

アクセスコントロールの全体像

AWS サービス独自の IAM 等を使用したアクセス制御に加えて、Security プラグインが提供する詳細なアクセス制御を組み合わせることで多層的なアクセスコントロールを実現



認証

- OpenSearch API は複数の認証手段を併用可能



OpenSearch API

- Dashboards は認証手段の併用不可。いずれか 1 つの認証手段を選択する



OpenSearch Dashboards

- 認証方法によって、アクセス制御による認可で参照される情報が異なる

認証方式

きめ細やかなアクセス制御による認可で参照される情報



ID + Password



User ID



AWS IAM



IAM User / IAM Role



Anonymous



N/A



Amazon Cognito



IAM Role



JSON Web Token



SAML



SAML Token



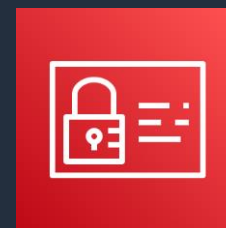
ID + Password



User ID

認証の種類

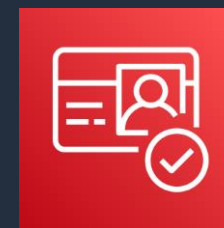
- Basic 認証
 - ユーザーネームとパスワード
 - 内部 DB で管理
- IAM 認証
 - AWS STS を使用
 - コンテナ、EC2 などを含む SigV4
- Amazon Cognito
 - ユーザープール、ID プールを使用
- SAML 認証
 - サードパーティ ID プロバイダーを使用
 - プロバイダーで認証



AWS IAM



AWS STS



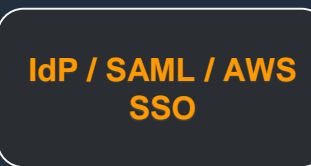
Amazon Cognito

プロバイダー例

Auth0

onelogin

okta

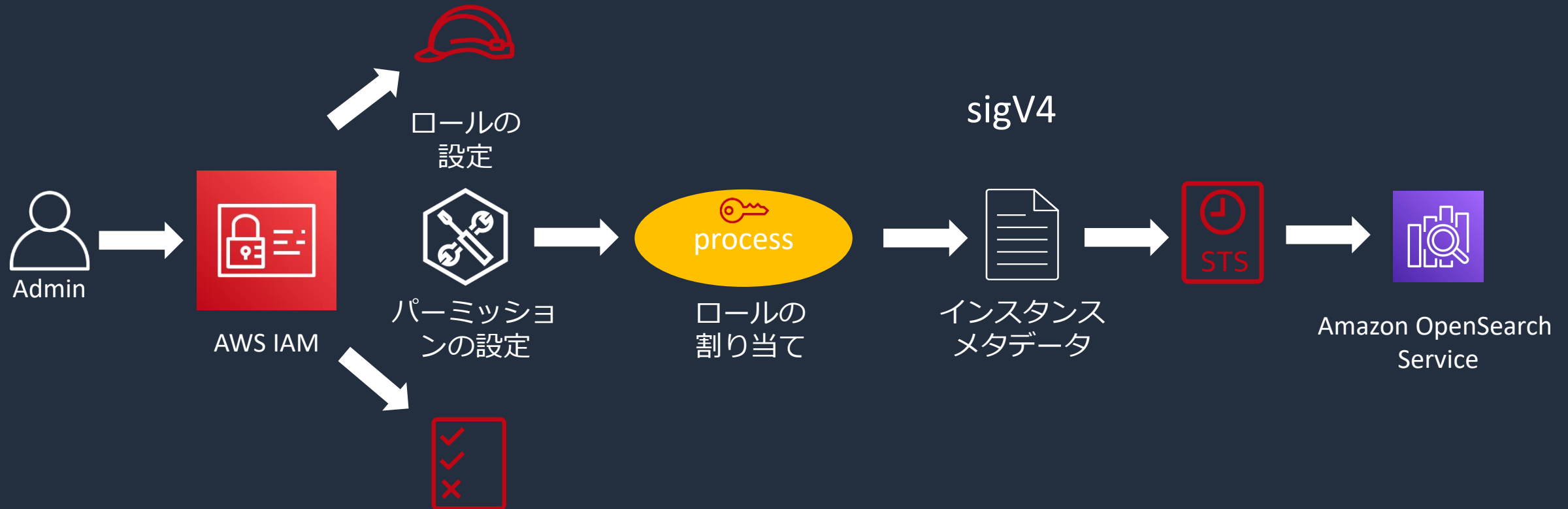


Ping Identity

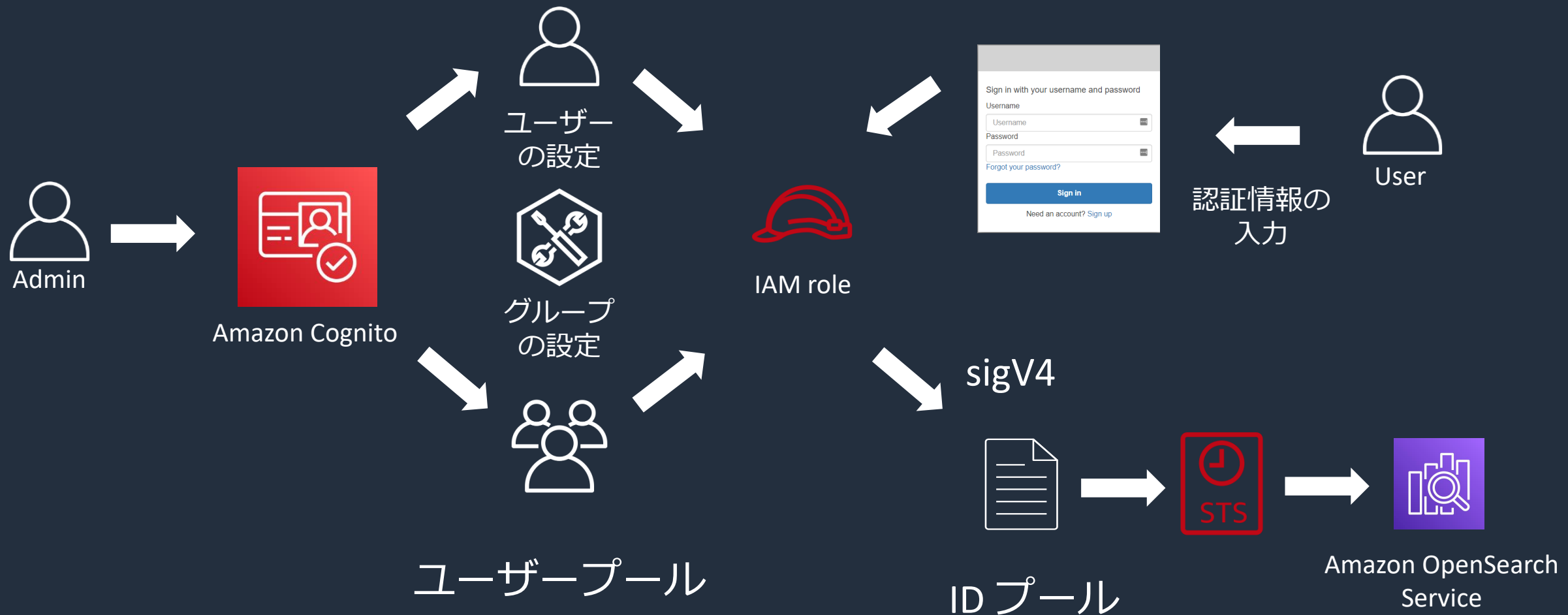
認証の流れ – Basic 認証



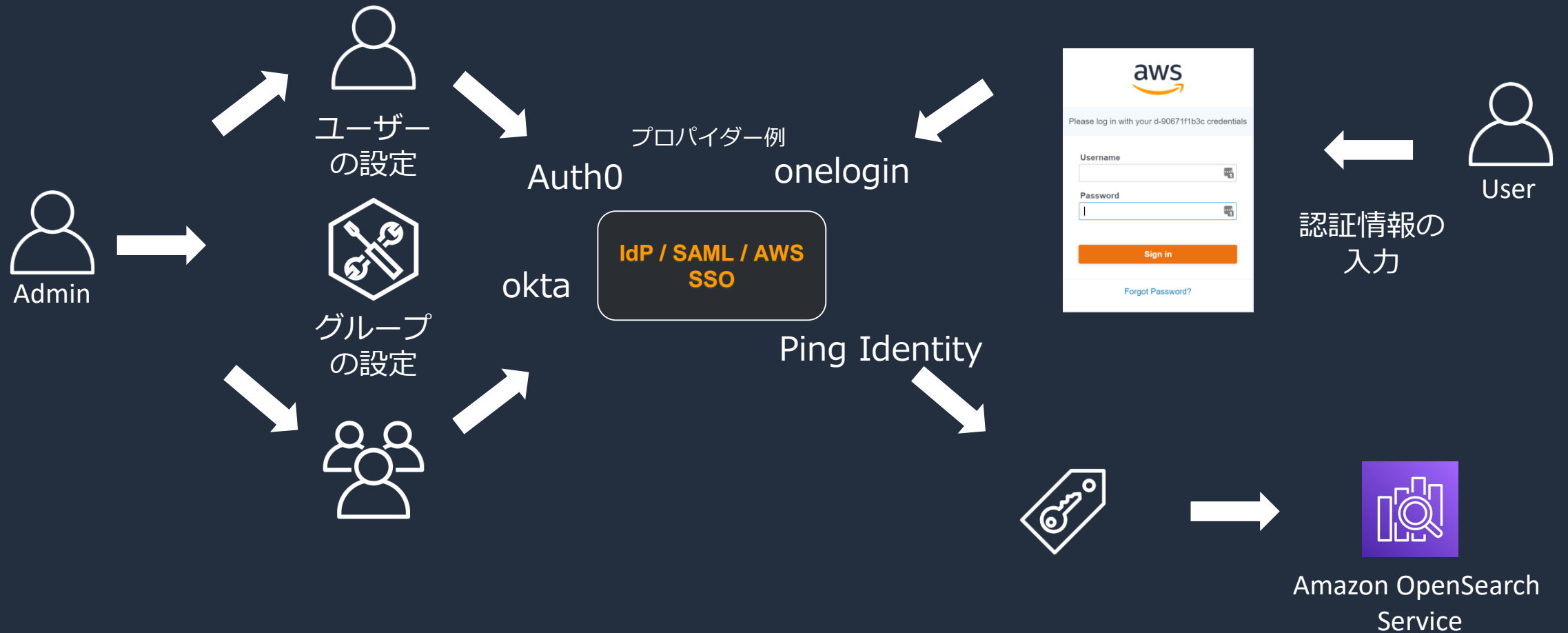
認証の流れ – IAM 認証



認証の流れ - Amazon Cognito



認証の流れ – SAML 認証



NWベースのアクセス制御

• パブリック接続

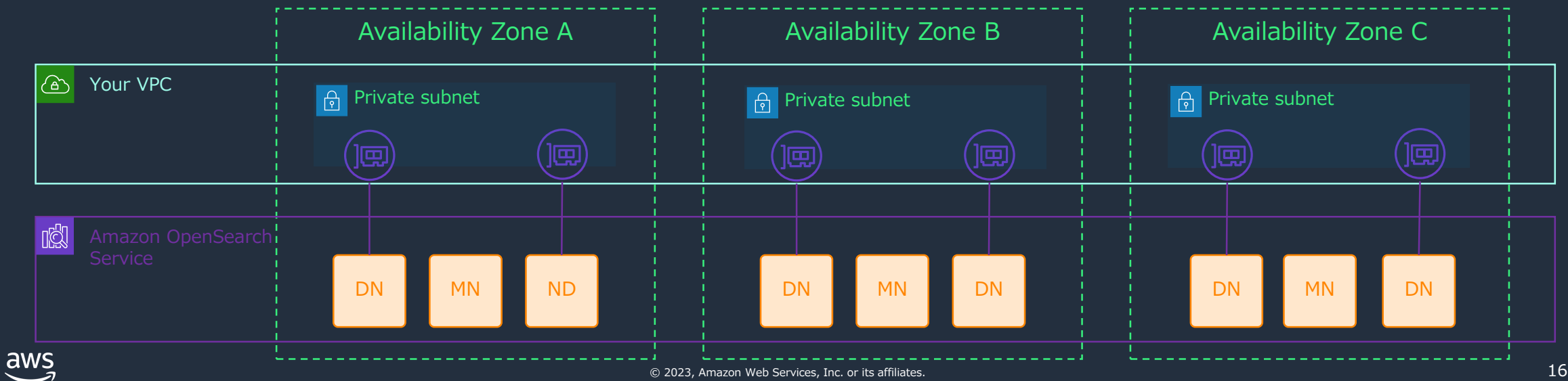
- Amazon OpenSearch をパブリックに公開する
- アクセス可能な IP アドレスリストを用いて通信を許可する
- プライベート通信オプションを除くすべてのセキュリティ機能を活用可能

• VPC によるプライベート接続

- Amazon OpenSearch をプライベートにデプロイする
- ENI を任意の VPC にデプロイ
- セキュリティグループを使って通信を許可
- 全てのセキュリティ機能を活用可能

VPC によるプライベート接続

- VPC のセキュリティグループを利用したアクセス制御が可能に
- VPC に構築したドメインに対して、インターネットから直接アクセスすることはできない (Public 接続と VPC 接続は排他関係)
- VPC Peering 等を活用することで、異なる VPC、リージョン、アカウントからのアクセスも可能
- 各サブネットには、AZ に割り当てられたデータノード数の 3 倍の IP アドレスが必要。
大規模なドメインを作成する場合は専用サブネットの確保を推奨



VPC ドメインへ外部から接続する方法

- 同一 VPC ではない外部からアクセスする場合、何らかのサービスを経由する必要あり
- アクセス元によって使用可能なサービスが異なる

他拠点からのインターネットもしくはプライベート接続



AWS Client VPN



プロキシサーバー
(Apache, Nginx 等)



VPN connection



AWS Systems Manager



AWS Direct Connect



Amazon WorkSpaces
Web

別 VPC、別アカウント、別リージョン (*) からのアクセス



AWS PrivateLink



AWS Resource
Access Manager



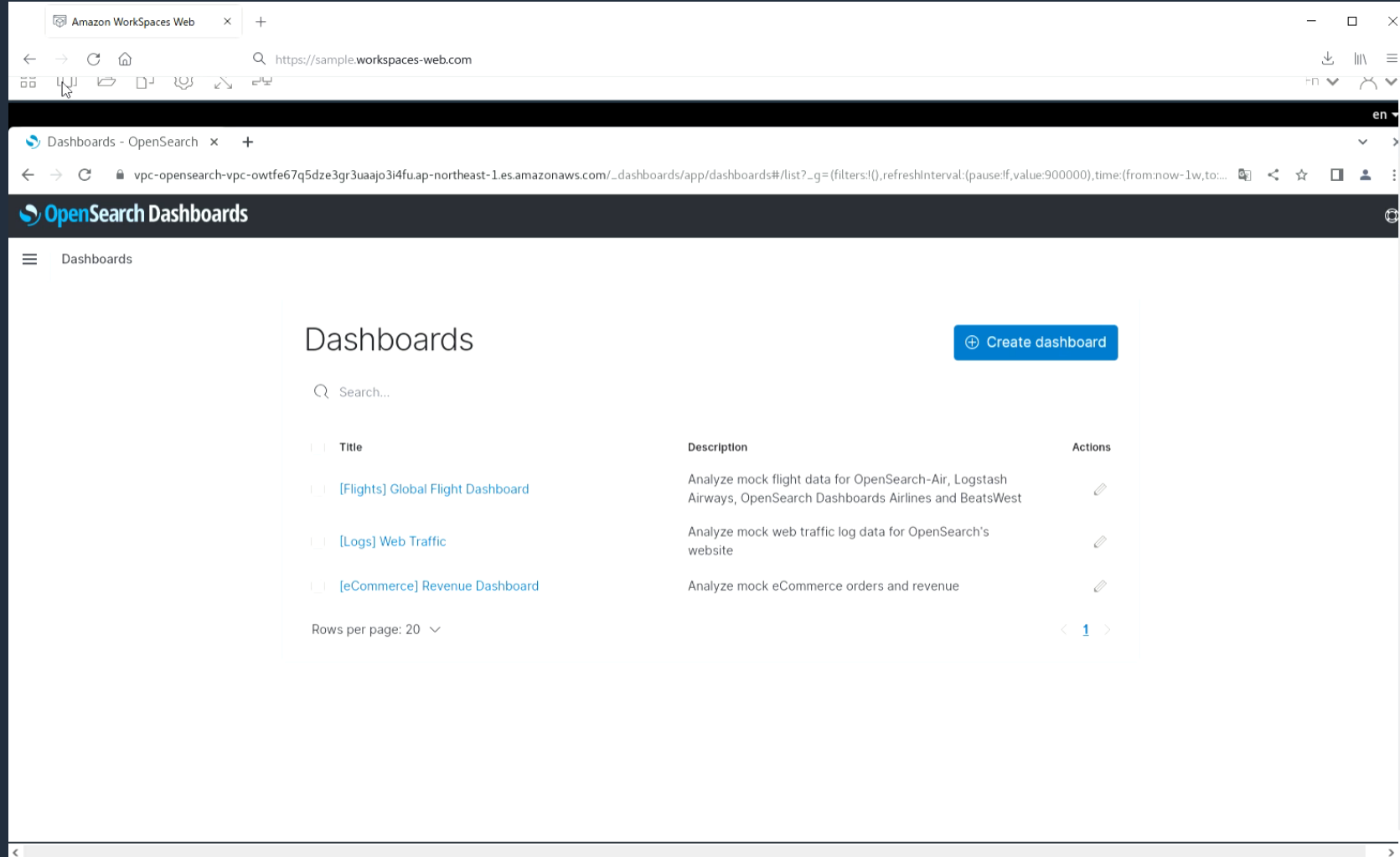
AWS Transit
Gateway (*)



VPC Peering (*)

サービス例① WorkSpaces Web

- ブラウザから VPC 内の OpenSearch Dashboards へのアクセスが可能
- 画面イメージのみをストリーミング配信。実データは転送されない



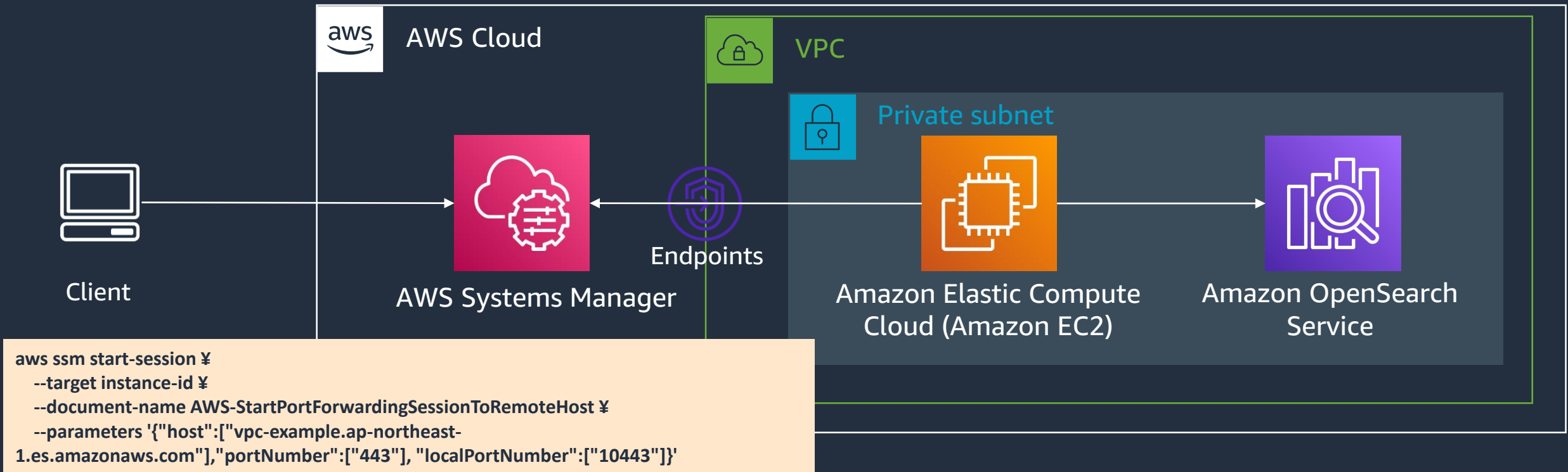
The screenshot displays a browser window titled "Amazon WorkSpaces Web" with the URL "https://sample.workspaces-web.com". The main content area shows the "OpenSearch Dashboards" interface. At the top, there is a "Dashboards" header and a "Create dashboard" button. Below this is a search bar and a table of existing dashboards. The table has three columns: "Title", "Description", and "Actions".

Title	Description	Actions
[Flights] Global Flight Dashboard	Analyze mock flight data for OpenSearch-Air, Logstash Airways, OpenSearch Dashboards Airlines and BeatsWest	
[Logs] Web Traffic	Analyze mock web traffic log data for OpenSearch's website	
[eCommerce] Revenue Dashboard	Analyze mock eCommerce orders and revenue	

At the bottom of the table, it indicates "Rows per page: 20" and a pagination control showing page 1 of 1.

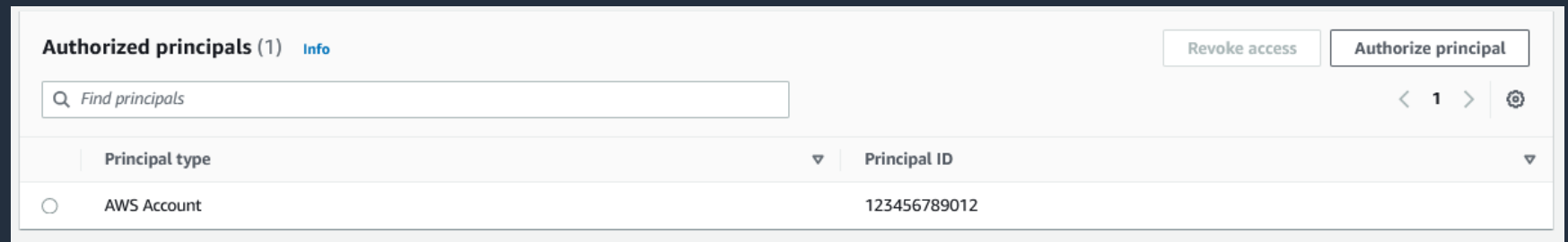
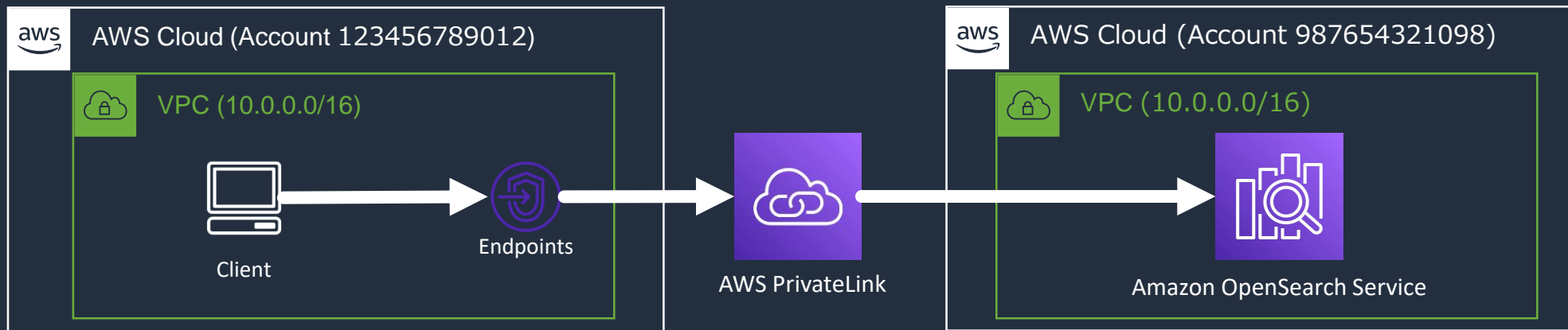
サービス例② Session Manager

- Systems Manager の VPC Endpoint を用意することで、踏み台ホストを Private Subnet 上に配置可能
- クライアントは AWS CLI を実行しセッションを確立



サービス例③ Private Link

- 異なる VPC 上の Amazon OpenSearch Service ドメインに接続
 - CIDR が重複している VPC からの接続も可能
- ドメイン毎に、Amazon OpenSearch Service 側で設定。
アカウント ID 単位で Private Link アクセスを許可



Private Link 利用上の考慮事項

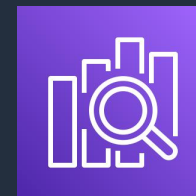
- ドメイン毎にアカウント単位でアクセス許可を付与する必要あり
 - 組織 ID 単位でのアクセス許可には非対応
 - 同一アカウント内でのアクセスについてはアクセス許可不要
- 以下の制限あり
 - 50 エンドポイント / アカウント
 - 10 エンドポイント / ドメイン
 - 10 許可対象アカウント / ドメイン
- カスタムエンドポイント (任意の FQDN でドメインにアクセス) は利用不可
- Private Link の利用料が別途発生する
 - 同一 VPC 内からの接続については通常のエンドポイントへのアクセスを推奨

ポリシーでのアクセス制御

2つの組み合わせで最終的な認可を実施



AWS Identity & Access
Management



Amazon OpenSearch
Service

- アイデンティティ (IAM) ベースのアクセスポリシー
 - コントロールプレーンとデータプレーン
 - デプロイ
 - 一時的な認証情報
 - シークレットキー / アクセスキー
 - SigV4 リクエストの署名が必要
- リソースベースのアクセスポリシー
 - IAM のように記載
 - IP アドレス制限を提供
 - コントロールプレーンとデータプレーン
 - IAM で SigV4 リクエスト署名を使用

アイデンティティ (IAM) ベースのアクセスポリシー

- タグ、ドメイン、URL パス (インデックス や API など) 単位でアクセス制御が可能
- API のアクセス制御はメソッド単位で行う (ex. ESHttpGet)
- アイデンティティベースのアクセスポリシーを使用する場合、クライアントは IAM ユーザー、IAM ロールの権限を取得し署名をリクエストに付与する必要あり

```
{  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Action": ["es:ESHttpGet", "es:ESHttpPut"],  
    "Effect": "Allow",  
    "Resource": "arn:aws:es:us-east-1:123456789012:domain/test-domain/test-index/_search",  
    "Condition": {"ForAnyValue:StringEquals": {"aws:ResourceTag/environment": ["production"]}}  
  }]  
}
```

リソースベースのアクセスポリシー

- ドメイン単位で IAM ロールや IAM ユーザーに対してアクセス許可を付与することが可能
- ベーシック認証や SAML 認証など IAM を使わない認証を使用する場合は、Principal を * に指定し匿名アクセスを許可する必要がある。そのままだとセキュリティレベルが低下するため、Public ドメインの場合は IP レンジによるアクセス制御を、VPC ドメインの場合はセキュリティグループを使用することを推奨

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": ["arn:aws:iam::123456789012:user/test-user"]
      },
      "Action": ["es:ESHttp*"],
      "Resource": "arn:aws:es:us-east-1:123456789012:domain/test-domain/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": ["arn:aws:iam::123456789012:user/test-user"]
      },
      "Action": ["es:ESHttp*"],
      "Resource": "arn:aws:es:us-east-1:123456789012:domain/test-domain/*",
      "Condition": {"IpAddress": {"aws:SourceIp": ["192.0.2.0/24"]}}
    }
  ]
}
```

IAM ユーザーからのアクセスは
アクセス元を問わず許可

決められた IP レンジからのア
クセスについては 署名が付与さ
れていないリクエストでも許可

アイデンティティベースとリソースベースポリシーの関係

- 2つのポリシーは組み合わせ可能
- 組み合わせでは常に Deny が勝る。いずれのポリシーでも許可されない場合、暗黙の Deny により拒否される
- 別アカウントからドメインにアクセスする場合、“リソースベースのアクセスポリシー”、“アイデンティティベースのアクセスポリシー”の両方で明示的にアクセスを許可する必要あり

アイデンティティベース

リソースベース

	Allow	Deny	指定なし
Allow	Allow	Deny	Allow
Deny	Deny	Deny	Deny
指定なし	Allow	Deny	Deny

https://docs.aws.amazon.com/ja_jp/opensearch-service/latest/developerguide/ac.html

きめ細やかなアクセス制御 (Fine-Grained Access Control※)

- ユーザーレベルの詳細なアクセス権限管理を提供する機能。以下に対するアクセス管理が可能
 - インデックス>ドキュメント>フィールド
 - テナント>ダッシュボード、ビジュアルなど
- 複数の権限を持つ“ロール”をグループ、ユーザーに割り当てる
- フィールドマスキング機能もサポート

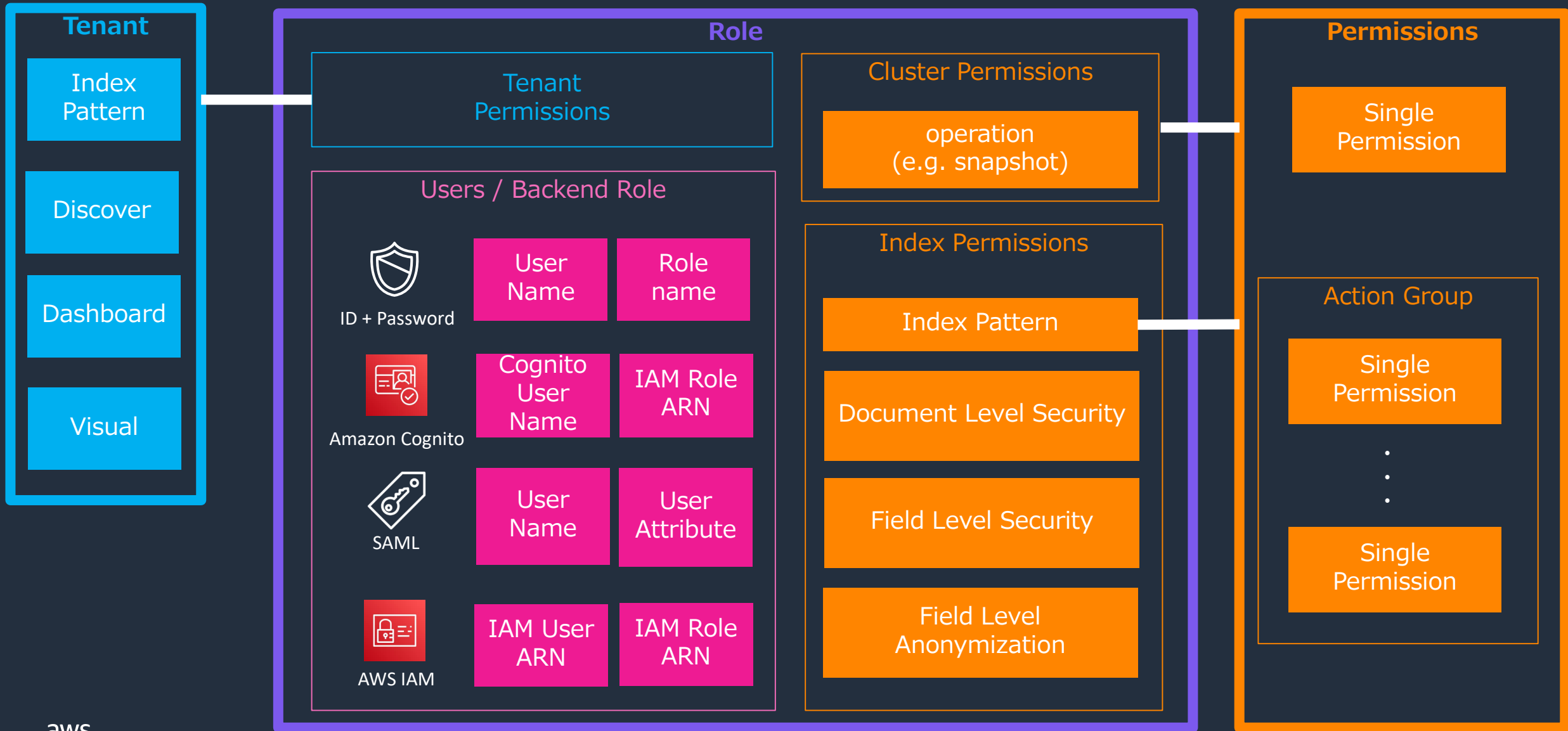
```
> Mar 4, 2020 @ 21:31:49.000
  "ipaddress": "9625fde554f696050c455961ccb2c74b24479008623c517f5c021209f6fa96dd"
  "currentTemperature": 89
  "sensorId": 13
  "status": "OK"
  "timestamp": "Mar 4, 2020 @ 21:31:49.000"
  "_id": "496047839822562735379407828496708895611491503146228776962.0"
  "_type": "_doc"
  "_index": "workshop-log"
  "_score": -
```

The screenshot displays the AWS IAM console interface for configuring permissions. It is divided into several sections:

- Index permissions:** Shows a dropdown for the index name, currently set to "workshop-log". Below it, there is a section for "Index permissions" with a dropdown set to "read". A "Create new permission group" button is visible on the right.
- Document level security - optional:** This section is highlighted with an orange box. It contains a JSON snippet defining a query filter:


```
{
  "bool": {
    "must": {
      "match": {
        "status": "OK"
      }
    }
  }
}
```
- Field level security - optional:** This section includes a dropdown menu set to "Exclude" and a text input field labeled "Type in field name".
- Anonymization - optional:** This section is also highlighted with an orange box and shows a dropdown menu with "ipaddress" selected.

きめ細やかなアクセス制御の全体像



テナント

- テナントとは、ダッシュボードの各コンポーネント (Index pattern, Visualize, Dashboard etc...) の管理単位
- 部署ごとにテナントを分けることで、複数部署のユーザーでダッシュボードの利用分割が可能

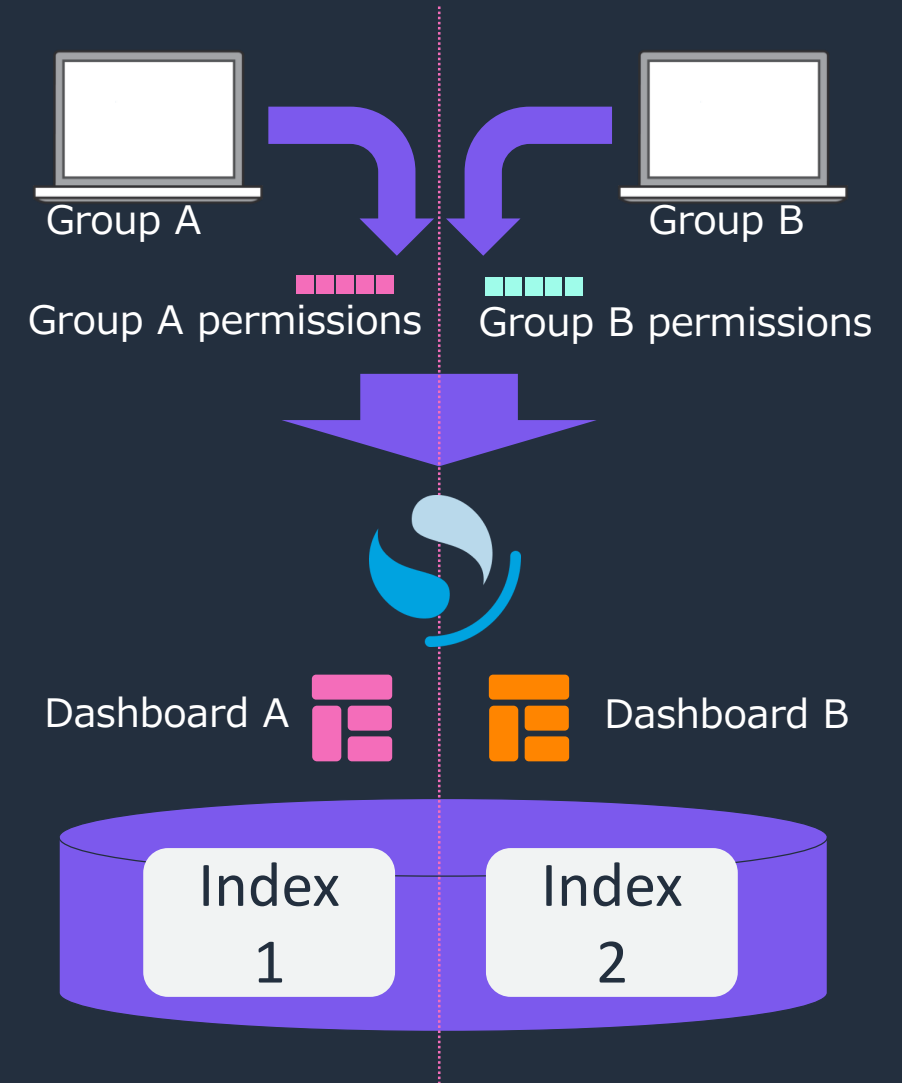
Tenants (2)

Tenants in OpenSearch Dashboards are spaces for saving index patterns, visualizations, dashboards, and other OpenSearch Dashboards objects. Use tenants to safely share your work with other OpenSearch Dashboards users. You can control which roles have access to a tenant and whether those roles have read or write access. The "Current" label indicates which tenant you are using now. Switch to another tenant anytime from your user profile, which is located on the top right of the screen. [Learn more](#)

Find tenant

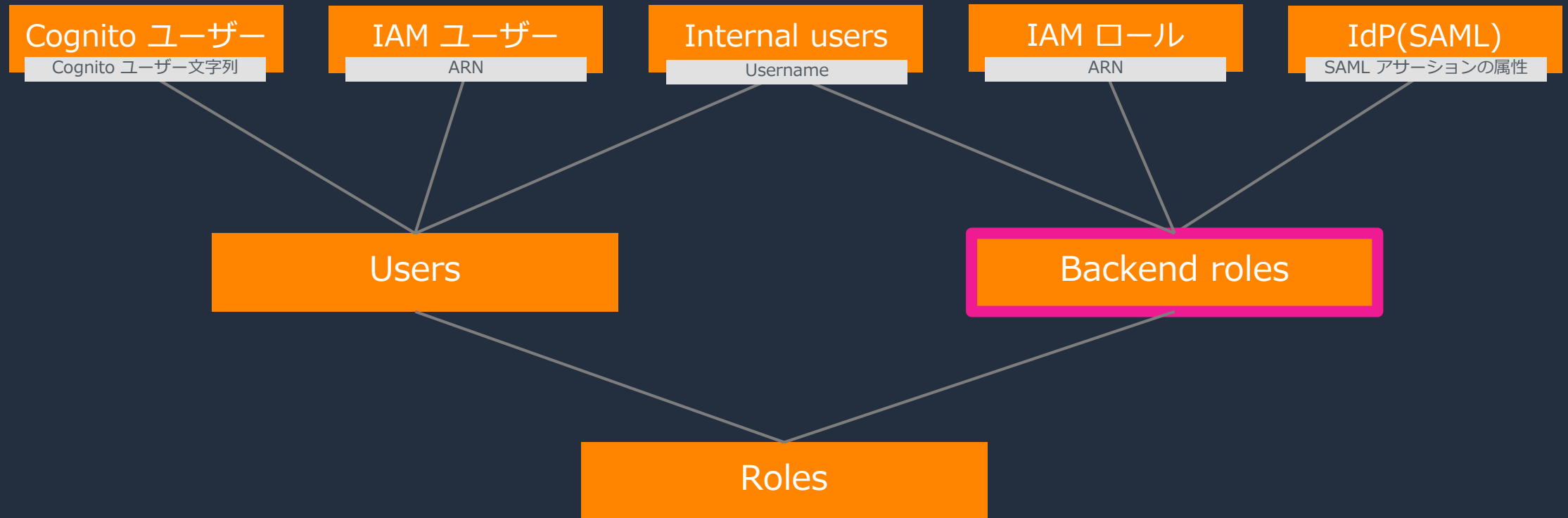
<input type="checkbox"/>	Name	Description	Dashboard	Visualizations	Customization
<input type="checkbox"/>	Global	Everyone can see it	View dashboard	View visualizations	Reserved
<input type="checkbox"/>	Private	Only visible to the current logged in user	View dashboard	View visualizations	Reserved

Rows per page: 10 < 1 >



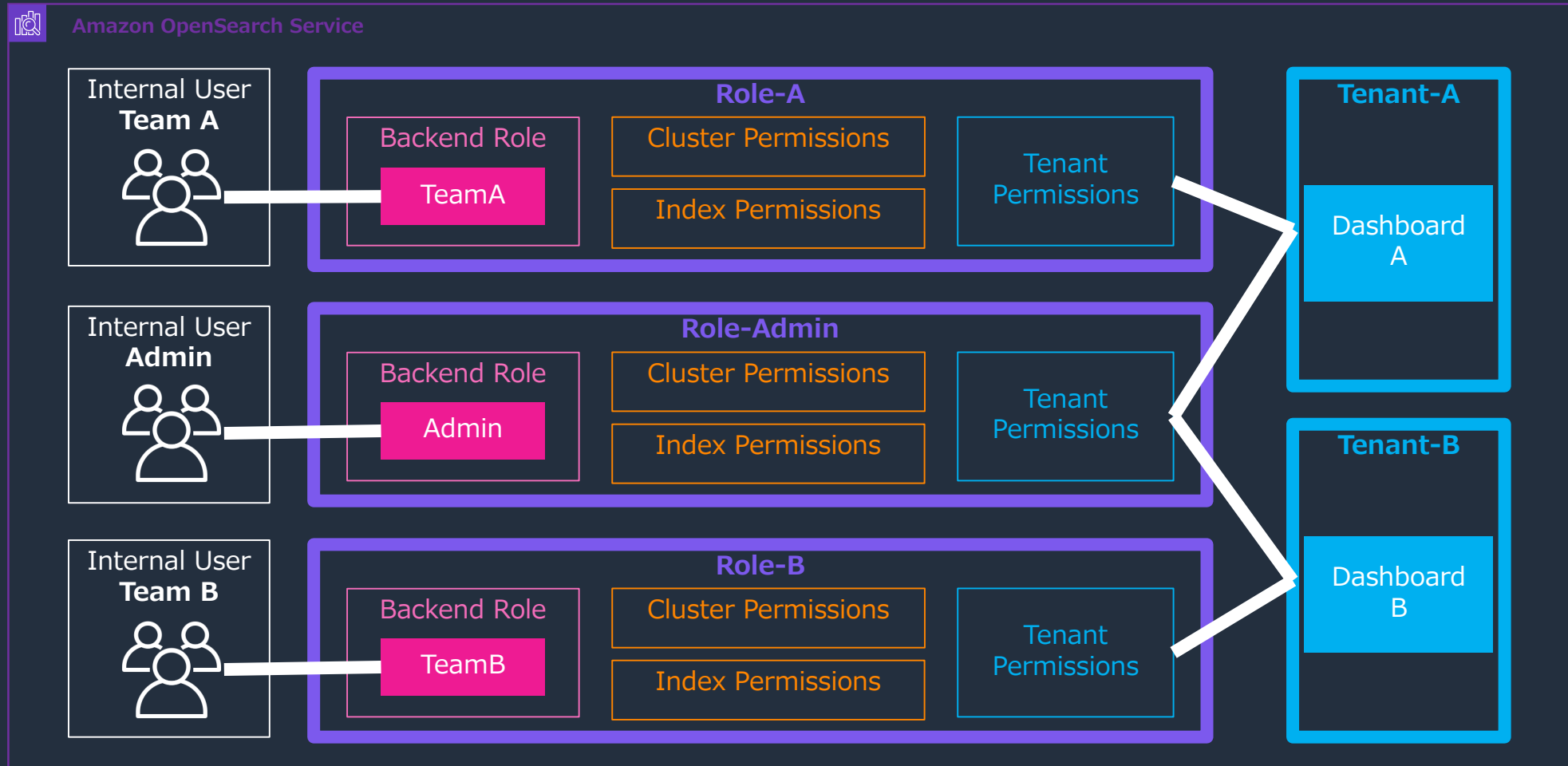
バックエンドロール

- バックエンドロールは、ロールをユーザーにマッピングする方法の一つ
- ロールに直接ユーザーを紐づけるのではなく、バックエンドロールを介して紐づけることが可能 (グループのように利用できる)



バックエンドロールを使った構成例

- テナントをチームごとに作成し、それぞれの参照権限を持つ Role-A, B を作成
- 両方のテナントに管理者権限を持つ Role-Admin を作成



既存ドメインの FGAC 有効化 - 猶予期間

- 既存ドメインの FGAC を有効化する際、猶予期間を設定可能
- 猶予期間中は、オープンアクセスポリシー (Public ドメインでの利用は非推奨) もしくは IP ベースのアクセスポリシーで許可された通信については認証がバイパスされる
- 利用者は猶予期間中に、FGAC 設定の追加やテストを行うことができる
- 猶予期間は 30 日間(固定)。猶予期間が満了すると、IP ベースのアクセスポリシーで許可されていた通信についても認証が要求されるようになる

Fine-grained access control

Fine-grained access control is enabled for this domain. After you enable fine-grained access control, you can't disable it. You can swap authentication schemes, specify a new IAM role ARN, and modify the master user for the internal database. Creating a new master user does not delete the existing master user. [Learn more](#)

Enable fine-grained access control

Master user

Set IAM ARN as master user

Create master user

Master username

master

Master usernames must be between 1 and 16 characters.

Master password

••••••••

Master password must be at least 8 characters long and contain at least one uppercase letter, one lowercase letter, one number, and one special character.

Confirm master password

••••••••



Migrate existing open/IP-based access policies into fine-grained access control

By enabling fine-grained access control, existing open/IP-based access policies will no longer work with this domain. We recommend enabling migration period to migrate existing credentials without interruptions. [Learn more](#)

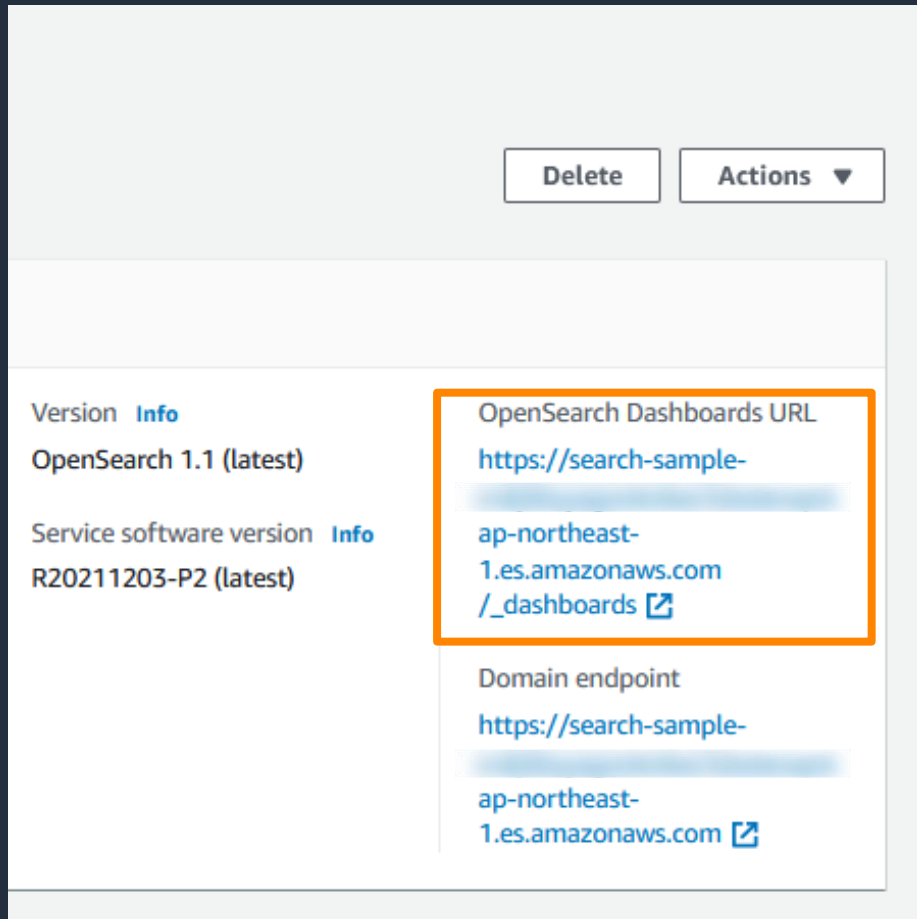
Enable migration period for open/IP-based access policy

Existing credentials in open/IP-based access policies will continue to work up to 30 days. Once the migration period ends, you can no longer enable it.

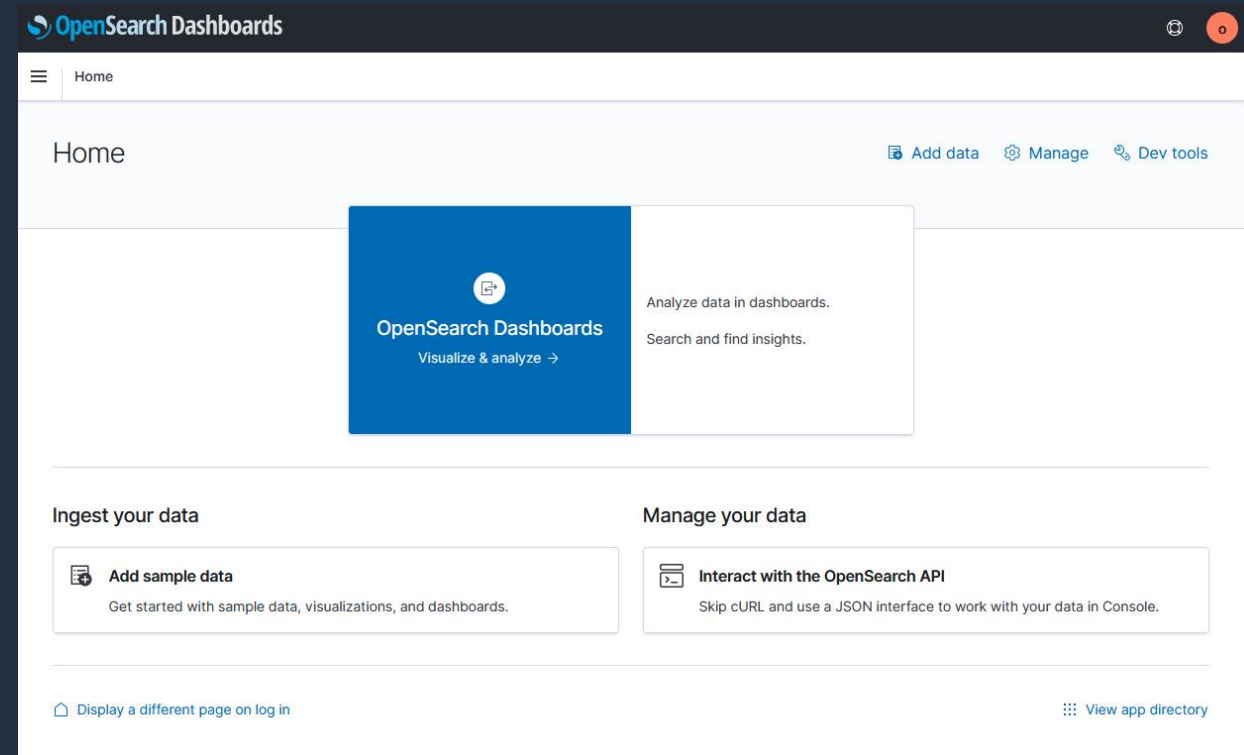


既存ドメインの FGAC 有効化 - ダッシュボードアクセス

IP ベースのアクセスポリシーで許可された IP アドレスから OpenSearch Dashboards の URL へアクセスすると、認証無しでダッシュボードが表示される



Configuration page for OpenSearch Dashboards. The "OpenSearch Dashboards URL" and "Domain endpoint" fields are highlighted with an orange box. The URL is `https://search-sample-
ap-northeast-1.es.amazonaws.com
/_dashboards` and the domain endpoint is `https://search-sample-
ap-northeast-1.es.amazonaws.com`. Other visible text includes "Delete", "Actions", "Version Info", "OpenSearch 1.1 (latest)", and "Service software version Info R20211203-P2 (latest)".



OpenSearch Dashboards home page. The page title is "OpenSearch Dashboards" and the main heading is "Home". The page includes navigation links for "Add data", "Manage", and "Dev tools". A central blue card displays "OpenSearch Dashboards" with the subtext "Visualize & analyze". Below this, there are sections for "Ingest your data" (with "Add sample data" button) and "Manage your data" (with "Interact with the OpenSearch API" button). The footer contains "Display a different page on log in" and "View app directory".

匿名ユーザーの権限

- 猶予期間内に認証無しでアクセスした場合、セッション上は匿名ユーザーとして認識される
- 匿名ユーザーは既存の全リソースへのアクセスが可能。またセキュリティ設定以外の全ての機能を利用可能

```
GET _plugins/_security/authinfo
{
  "user" : "User [name=opendistro_security_anonymous,
backend_roles=[opendistro_security_anonymous_backendrole], requestedTenant=null]",
  "user_name" : "opendistro_security_anonymous",
  "user_requested_tenant" : null,
  "remote_address" : "27.0.3.153:9200",
  "backend_roles" : [
    "opendistro_security_anonymous_backendrole"
  ],
  "custom_attribute_names" : [],
  "roles" : [
    "default_role"
  ],
  "tenants" : {
    "opendistro_security_anonymous" : true
  },
  "principal" : null,
  "peer_certificates" : "0",
  "sso_logout_url" : null
}
```

Roles (1)

Roles you are currently mapped to by your administrator.

default_role

Backend roles (1)

Backend roles you are currently mapped to by your administrator.

opendistro_security_anonymous_backendrole

既存ドメインの FGAC 有効化 - 猶予期限の確認

- コンソール上のバナー、セキュリティ設定変更画面、API などから確認可能
- 猶予期間を前倒して終了させることも可能

① Migrate existing open/IP-based access policies into fine-grained access control by February 6, 2022, 10:06 (UTC+09:00)

Login to OpenSearch Dashboards with your master username to migrate existing user credentials to use fine-grained access control. After the migration period ends, existing open/IP-based access policies on this domain will no longer work. [Learn more](#)

```
$ aws opensearch describe-domain-config --domain-name sample --query DomainConfig.AdvancedSecurityOptions
{
  "Options": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "AnonymousAuthDisableDate": "2022-02-06T10:06:44.135000+09:00",
    "AnonymousAuthEnabled": true
  },
  "Status": {
    "CreationDate": "2022-01-07T08:42:59.064000+09:00",
    "UpdateDate": "2022-01-07T10:54:47.341000+09:00",
    "UpdateVersion": 25,
    "State": "Active",
    "PendingDeletion": false
  }
}
```



access control

control is enabled for this domain. After you enable fine-grained access control, you can't disable it. You can swap authentication schemes, specify a new IAM role ARN, and modify the master user for the internal database. Creating a new master user does not delete the existing master user. [Learn more](#)

Enable fine-grained access control

Master user

Set IAM ARN as master user

Create master user

Master username

Master usernames must be between 1 and 16 characters.

Master password

Master password must be at least 8 characters long and contain at least one uppercase letter, one lowercase letter, one number, and one special character.

Confirm master password

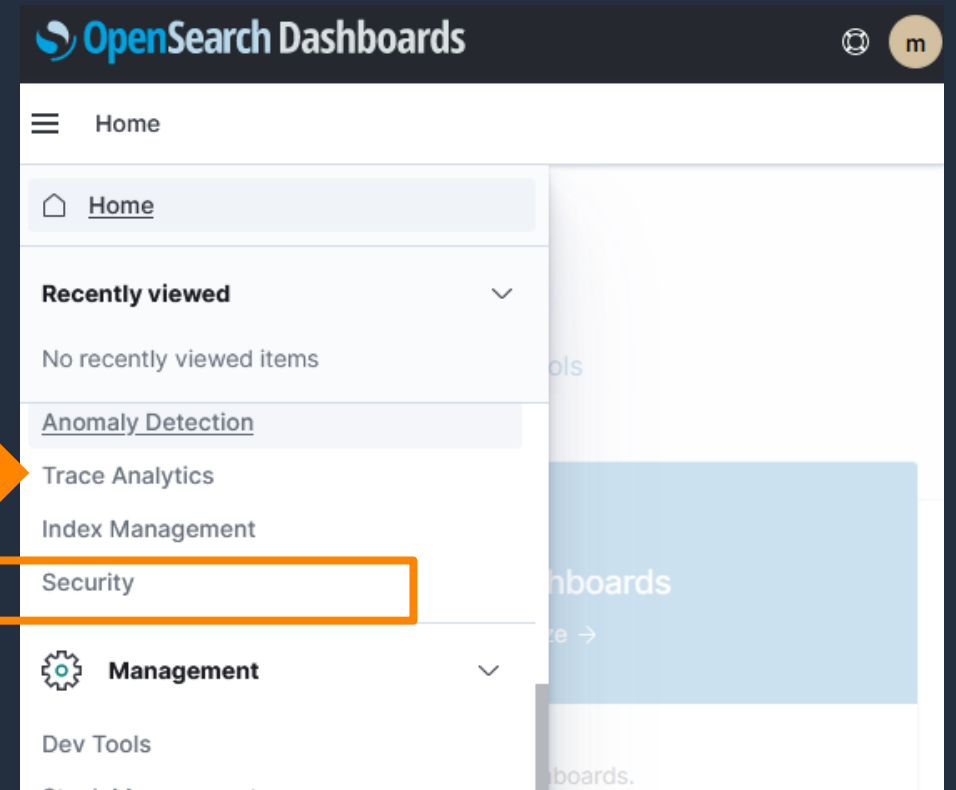
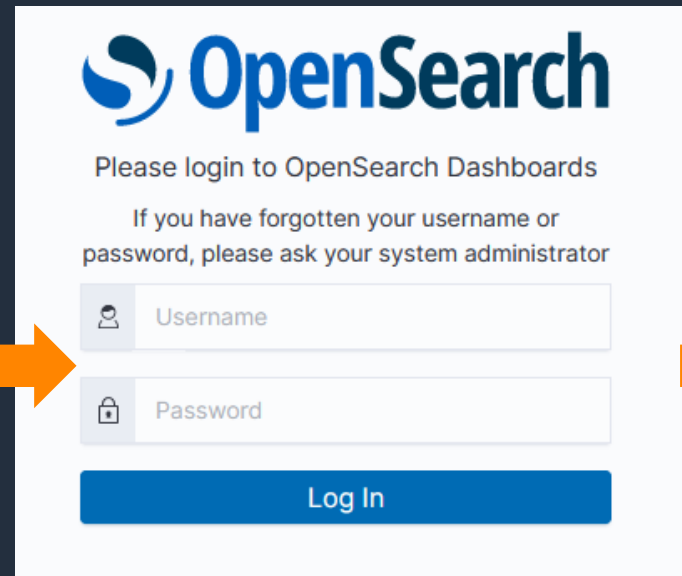
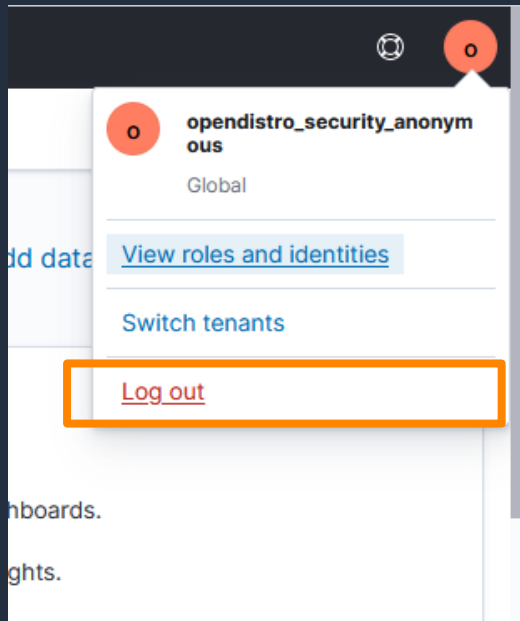
Migration period for open/IP-based access policy

End migration period

Existing credentials in open/IP-based access policies will continue to work until February 6, 2022, 10:06 (UTC+09:00). Once the migration period ends, you can no longer enable it.

セキュリティ設定の変更

- 匿名ユーザーセッションからログアウトし、管理者ユーザーでログインすることでセキュリティ設定の変更が可能
- 直接 `_dashboards/app/login` エンドポイントからログインすることも可能



セキュリティ設定の変更 – 補足

- 匿名ユーザーの Backend role、匿名ユーザー名を security_manager role に直接マップすると匿名ユーザーでもセキュリティ設定の変更は可能だが、セキュリティの観点から推奨しない

The screenshot shows the AWS IAM console for the `security_manager` role. The `Mapped users` tab is active. It displays a table with 2 mapped users. The first user is of type `User` and is named `master`. The second user is of type `Backend role` and is named `opendistro_security_anonymous_backendrole`. A dropdown menu at the bottom indicates "Rows per page: 10".

<input type="checkbox"/>	User type	User
<input type="checkbox"/>	User	master
<input type="checkbox"/>	Backend role	opendistro_security_anonymous_backendrole

The screenshot shows the AWS IAM console for the `security_manager` role. The `Mapped users` tab is active. It displays a table with 2 mapped users. The first user is of type `User` and is named `master`. The second user is of type `User` and is named `opendistro_security_anonymous`. A dropdown menu at the bottom indicates "Rows per page: 10".

<input type="checkbox"/>	User type	User
<input type="checkbox"/>	User	master
<input type="checkbox"/>	User	opendistro_security_anonymous

2. データ保護

暗号化（データ転送）

ノード間転送時のデータ暗号化

- ドメイン作成時にノード間の通信について暗号化の有無を指定可能
- ドメイン作成後にノード間の通信暗号化を有効化することも可能
 - 暗号化を有効から無効に変更することは不可

2021 年のアップ
デートで対応

クライアント - ドメイン間通信の暗号化

- ドメインへのアクセスにおいて HTTPS を必須とするか、HTTP も許可するかを指定可能
- 以下 2 つのポリシーを利用可能
 - Policy-Min-TLS-1-0-2019-07: TLS v1.0 およびそれ以降をサポート (デフォルト)
 - Policy-Min-TLS-1-2-2019-07: TLS v1.2 をサポート



<https://docs.aws.amazon.com/opensearch-service/latest/developerguide/ntn.html>

<https://docs.aws.amazon.com/opensearch-service/latest/developerguide/infrastructure-security.html>

© 2023, Amazon Web Services, Inc. or its affiliates.

暗号化（データ保存）

保管時のデータ暗号化

- ドメイン作成時に以下のデータに対する暗号化の有無を指定可能。有効化した場合、AWS KMS の暗号化キーが使用される
 - ノードに格納されているデータ（インデックス、ログ、スワップファイル、アプリケーションディレクトリのその他全てのデータ）
 - UltraWarm ストレージ上に格納されているインデックス
 - S3 上に格納されている**自動**スナップショット
- 以下のリソースは暗号化の対象外
 - S3 上に格納される**手動**スナップショット（S3 の Server Side Encryption で対応可能）
 - CloudWatch Logs に配信されるスローログ、エラーログ、監査ログ（CloudWatch Logs の保管時データ暗号化機能で対応可能）
- **ドメイン作成後にノード間の通信暗号化を有効化することも可能**
 - **暗号化を有効から無効に変更することは不可**

2021 年のアップデートで対応

3. 監査

監査ログ (Audit Log)

- OpenSearch 上のデータに対するアクセスログを取得
- アクセスログにはユーザー名、アクセス先のインデックス名、アクセス元 IP アドレスなどが含まれる
- インデックス、ドキュメント、フィールド単位でアクセスログの取得可否をコントロール可能
- 特定ユーザー (アプリケーションユーザー) からのアクセスは記録しない、など細かい指定も可能
- Fine-Grained Access Control の有効化が必要

```
{
  "audit_cluster_name": "824471164578:audit-docs",
  "audit_node_name": "806f6050cb45437e2401b07534a1452f",
  "audit_category": "COMPLIANCE_DOC_READ",
  "audit_request_origin": "REST",
  "audit_node_id": "saSevm9ASte0-pjAtYi2UA",
  "@timestamp": "2020-08-31T17:57:05.015+00:00",
  "audit_format_version": 4,
  "audit_request_remote_address": "54.240.197.228",
  "audit_trace_doc_id": "config:7.7.0",
  "audit_request_effective_user": "admin",
  "audit_trace_shard_id": 0,
  "audit_trace_indices": [
    "accounts"
  ],
  "audit_trace_resolved_indices": [
    "accounts"
  ]
}
```

<https://opensearch.org/docs/latest/security-plugin/audit-logs/index/>

監査ログ (Audit Log) の具体例



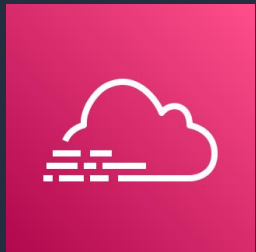
```
{  
  "audit_cluster_name": "755684787623:okta-saml-demo",  
  "audit_rest_request_params": {  
    "pretty": "true"  
  },  
  "audit_node_name": "2ec142acc83a9ca1f648d869f6f6389b",  
  "audit_request_initiating_user": "admin",  
  "audit_rest_request_method": "GET",  
  "audit_category": "AUTHENTICATED",  
  "audit_request_origin": "REST",  
  "audit_node_id": "WlcsmWkMS12sAo-_gm__Wg",  
  "audit_request_layer": "REST",  
  "audit_rest_request_path": "/_cat/shards",  
  "@timestamp": "2020-11-09T14:14:00.139+00:00",  
  "audit_request_effective_user_is_admin": false,  
  "audit_format_version": 4,  
  "audit_request_remote_address": "75.67.145.147",  
  "audit_rest_request_headers": {  
    "Transfer-Encoding": [ "chunked" ],  
    "Connection": [ "close" ],  
    "Host": [ "localhost" ],  
    "Content-Type": [ "application/json" ]  
  },  
  "audit_request_effective_user": "admin"  
}
```

監査ログ (CloudTrail)

- 通常の AWS サービスと同様、API コールのログを CloudTrail に出カ
- Amazon OpenSearch Service の API エンドポイント (es.<region>.amazonaws.com) への API コールが取得対象
- OpenSearch ドメイン上のデータに対する API コールは取得対象外。別途 OpenSearch ドメイン上で、監査ログの取得設定が必要

```
{  
  "eventVersion": "1.05",  
  "userIdentity": {  
    "type": "IAMUser",  
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",  
    "arn": "arn:aws:iam::123456789012:user/test-user",  
    "accountId": "123456789012",  
    "accessKeyId": "access-key",  
    "userName": "test-user",  
    "sessionContext": {  
      "attributes": {  
        "mfaAuthenticated": "false",  
        "creationDate": "2018-08-21T21:59:11Z"  
      }  
    }  
  },  
  "invokedBy": "signin.amazonaws.com"  
},  
"eventTime": "2018-08-21T22:00:05Z",  
"eventSource": "es.amazonaws.com",  
"eventName": "CreateElasticsearchDomain",  
"awsRegion": "us-west-1",  
"sourceIPAddress": "123.123.123.123",  
"userAgent": "signin.amazonaws.com",
```

監査ログ (CloudTrail) の具体例



Amazon CloudTrail

CloudTrail > Event history > UpdateDomainConfig

UpdateDomainConfig [Info](#)

Details [Info](#)

Event time	AWS access key	AWS region
September 30, 2021, 16:26:39 (UTC-07:00)	ASIA4KH7XEV42PWVVRVGX	us-east-2
User name	Source IP address	Error code
kxz-lsengard	54.240.196.185	-
Event name	Event ID	Read-only
UpdateDomainConfig	6ac8a041-a28d-4560-a934-e212b1133b49	false
Event source	Request ID	
es.amazonaws.com	e32fbf3d-ede0-46c7-93c2-677a652dc821	

4. ベストプラクティス

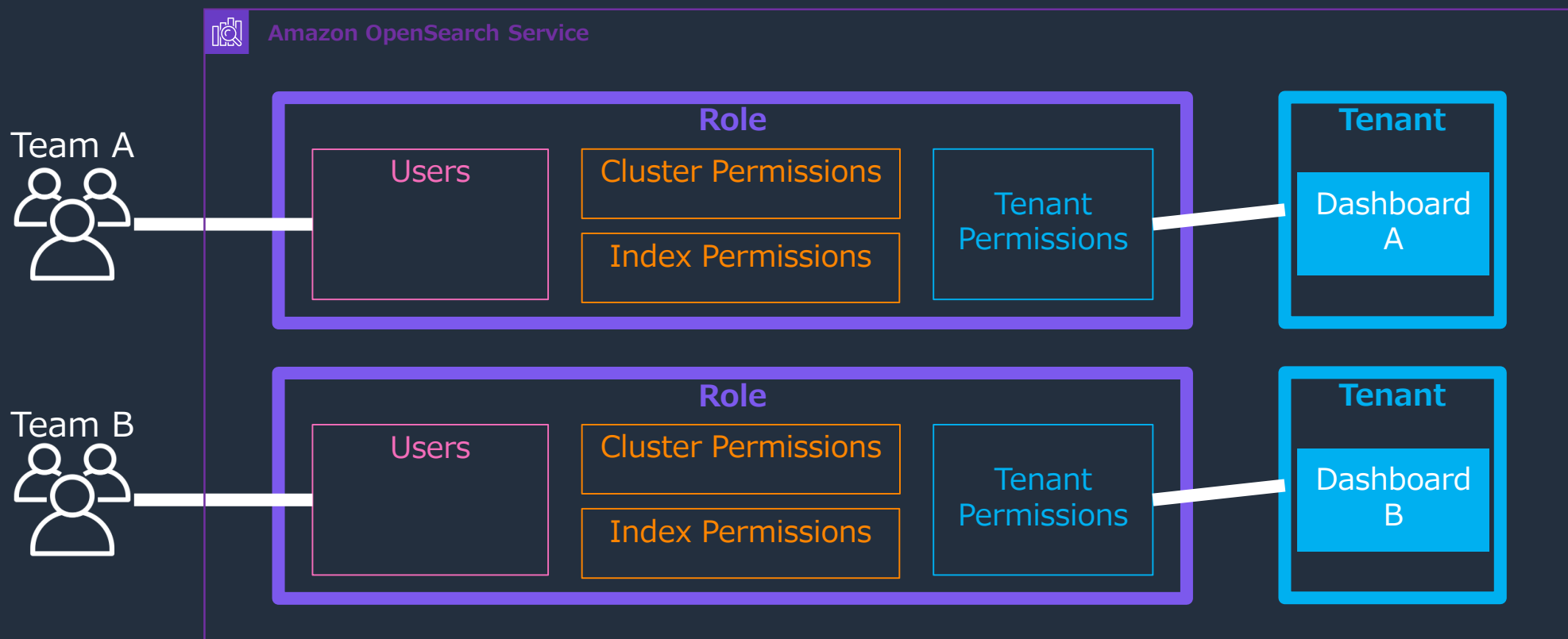
セキュリティベストプラクティス

- きめ細かなアクセスコントロールを有効にする
- VPC 内にドメインをデプロイする
- 制限的なアクセスポリシーを適用する
- 保管中の暗号化を有効にする
- ノード間の暗号化を有効にする

https://docs.aws.amazon.com/ja_jp/opensearch-service/latest/developerguide/bp.html#bp-security

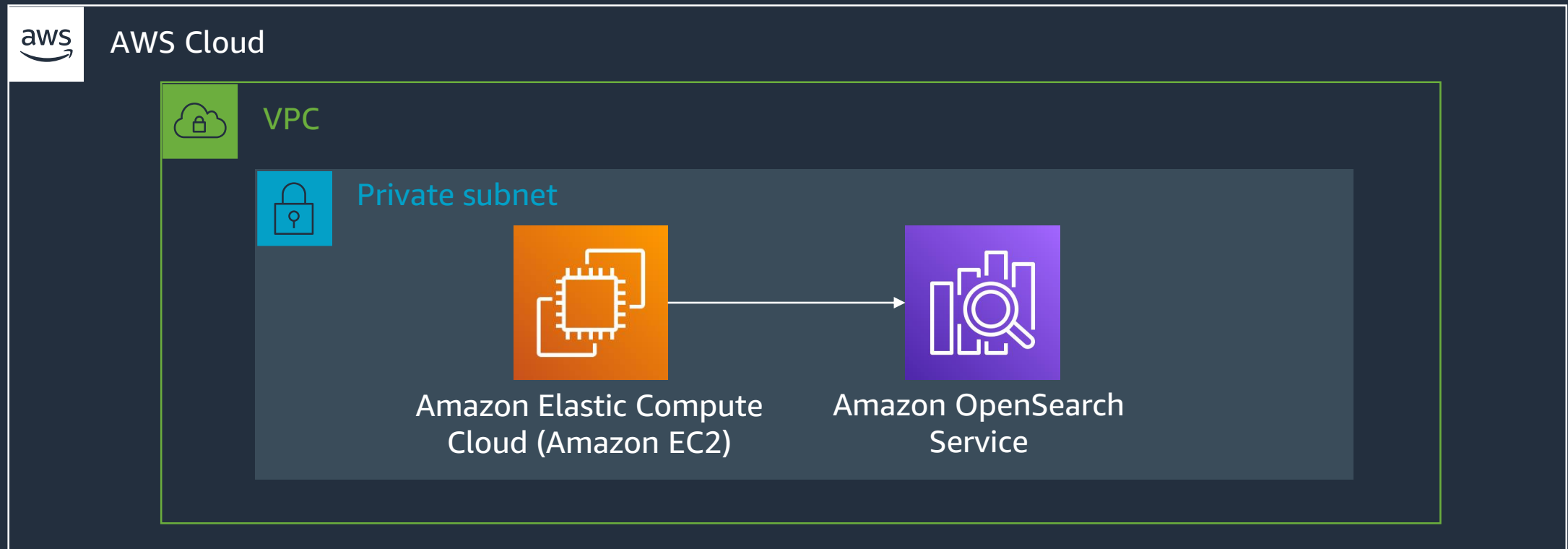
きめ細かなアクセスコントロールを有効にする

- きめ細かなアクセスコントロールでは、各クラスター、インデックス、ドキュメント、およびフィールドに、独自の指定アクセスポリシーが設定可能
- アクセス要件の異なるデータを同じドメインに格納する場合は、有効にすることを推奨



VPC 内にドメインをデプロイする

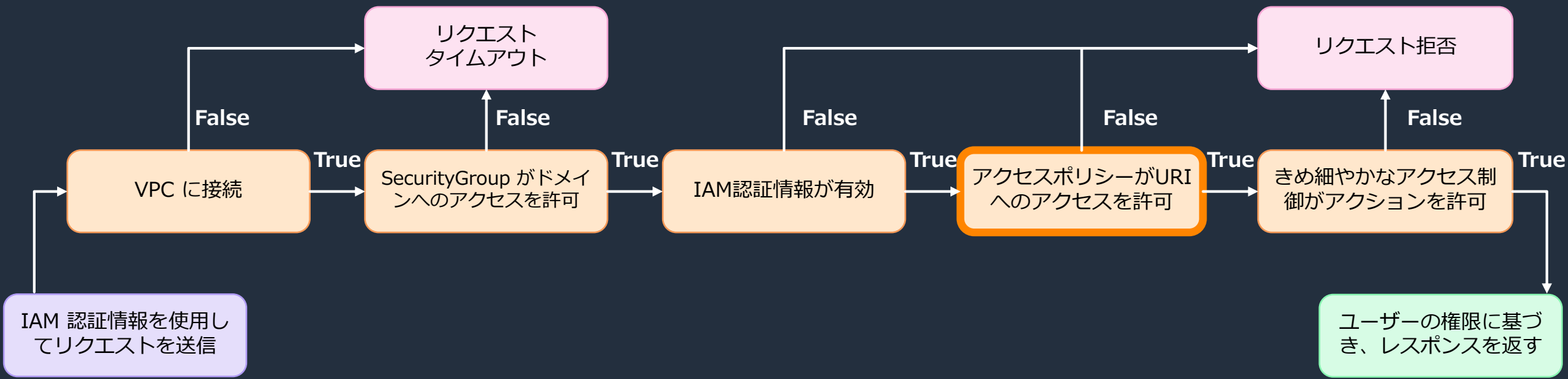
- ドメインを VPC 内に配置することで、インターネットゲートウェイ、NAT デバイス、VPN 接続なしで、他のサービス間との安全な通信を実現



制限的なアクセスポリシーを適用する

- ドメインが VPC 内にデプロイされている場合でも、アクセスポリシーを適用して多層的に保護するのがベストプラクティス
- リソースベースのアクセスポリシーをドメインに適用する際は、最小特権の原則に従う。原則として、アクセスポリシーで “Principal”: {“AWS”: “*”} を使用することは避ける

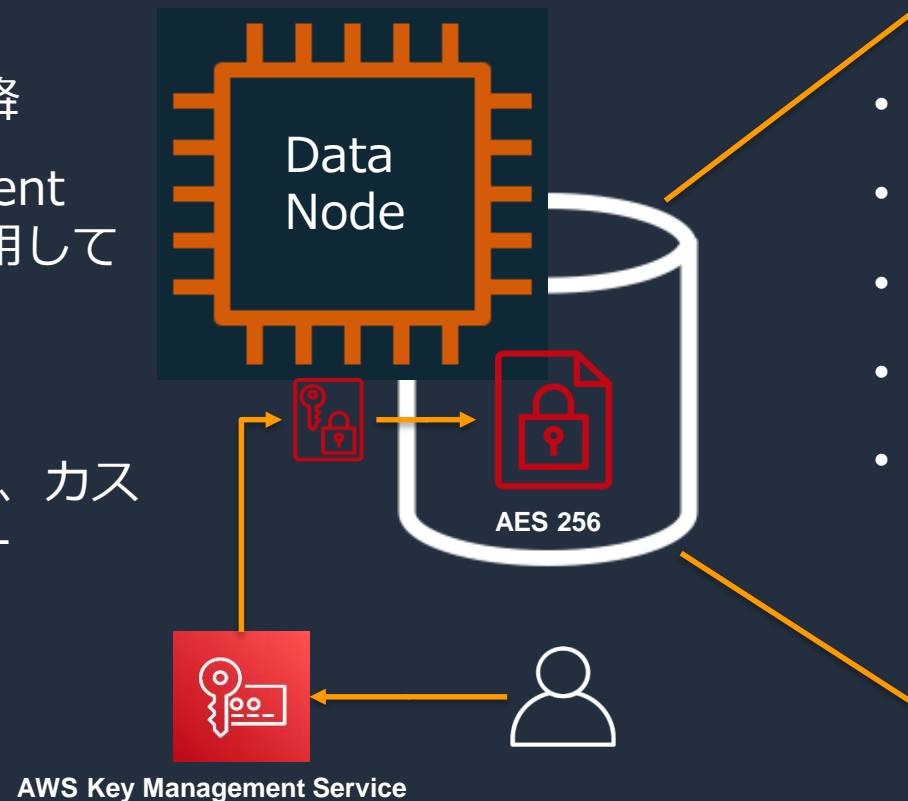
きめ細やかなアクセスコントロールが有効な VPC アクセスドメイン、IAM ベースのアクセスポリシー、IAM マスターユーザーという一般的な構成の例



保管中の暗号化を有効にする

- 保管中の暗号化は、AWS KMS を使用して暗号化キーを管理し、AES-256 を使用して暗号化を実施する

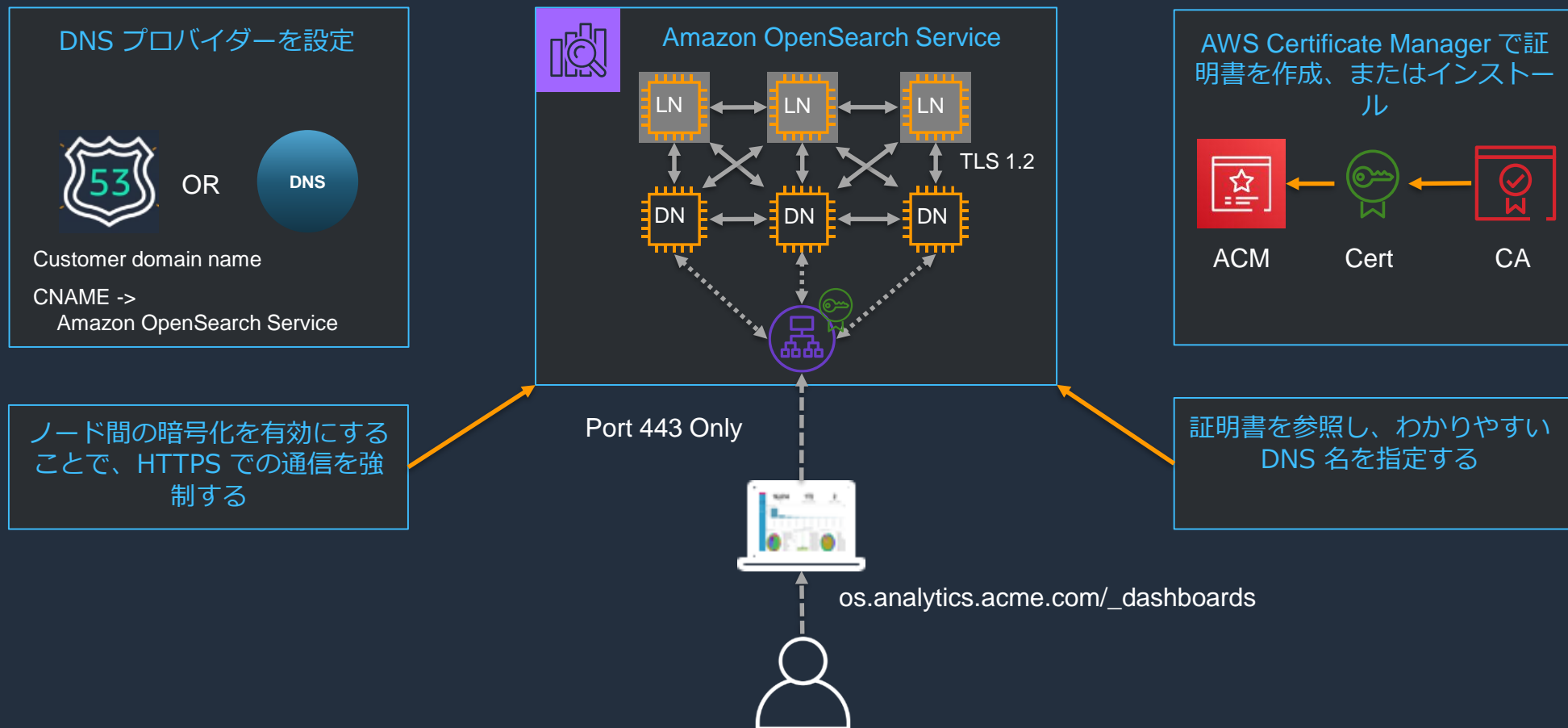
- OpenSearch 1.0 以降
- AWS Key Management Service (KMS) を使用してキーを保存及び管理
- AES 256
- AWS マネージドキー、カスタマーマネージドキー



- 全てのインデックス
- OpenSearch ログ
- スワップファイル
- 自動スナップショット
- アプリケーションディレクトリのその他すべてのデータ

ノード間の暗号間を有効にする

- ノード間の暗号化により、HTTPS 経由でドメインに送信されたデータは、ノード間でレプリケートされる間、転送中も暗号化されたまま



セキュリティベストプラクティスの確認

- AWS Security Hub を利用することで、セキュリティ上のベストプラクティスに沿っているかをチェック可能
- AWS Foundational Security Best Practices の標準を利用する
- Amazon OpenSearch Service ドメインは AWS Config に よってサポートされているため、カスタムルールによる追加のチェックも可能

Compliance Status	Severity	ID	Title	Failed checks
Passed	MEDIUM	Opensearch.3	OpenSearch domains should encrypt data sent between nodes	0 of 23

リファレンス

リファレンス

よくある質問: <https://aws.amazon.com/jp/opensearch-service/faqs/>

トラブルシューティング: https://docs.aws.amazon.com/ja_jp/opensearch-service/latest/developerguide/handling-errors.html

料金: <https://aws.amazon.com/jp/opensearch-service/pricing/>

ベストプラクティス : https://docs.aws.amazon.com/ja_jp/opensearch-service/latest/developerguide/bp.html#bp-security
https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/securityhub-standards-fsdp-controls.html#fsdp-opensearch-1

マルチテナントのデータ分割モデル : <https://aws.amazon.com/jp/blogs/apn/storing-multi-tenant-saas-data-with-amazon-opensearch-service/>

本資料に関するお問い合わせ・ご感想

技術的な内容に関しましては、有料の AWS サポート窓口へお問い合わせください

<https://aws.amazon.com/jp/premiumsupport/>

料金面でのお問い合わせに関しましては、カスタマーサポート窓口へお問い合わせください（マネジメントコンソールへのログインが必要です）

<https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service>

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください



ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

その他コンテンツのご紹介

ウェビナーなど、AWS のイベントスケジュールをご参照いただけます

<https://aws.amazon.com/jp/events/>

ハンズオンコンテンツ

<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/>

AWS 個別相談会

AWS のソリューションアーキテクトと直接会話いただけます

<https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html>



Thank you!