Kaspersky Hybrid Cloud Security ～ Public Cloud Security

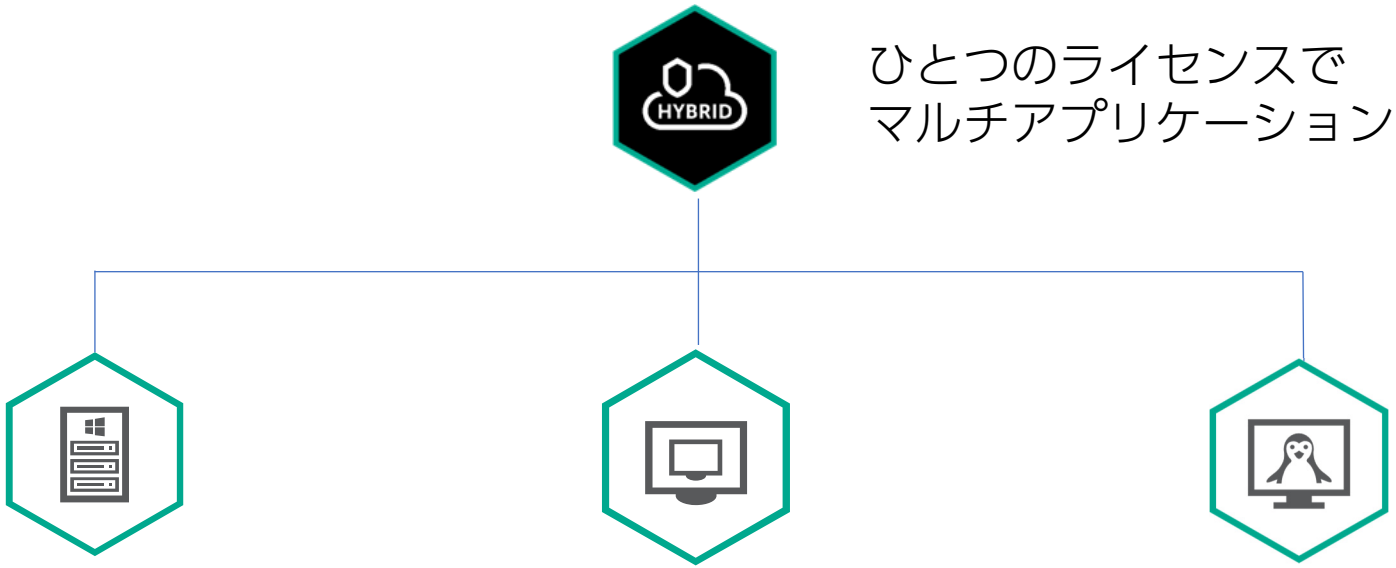
2023年5月23日

株式会社カスペルスキー
セールスエンジニアリング本部

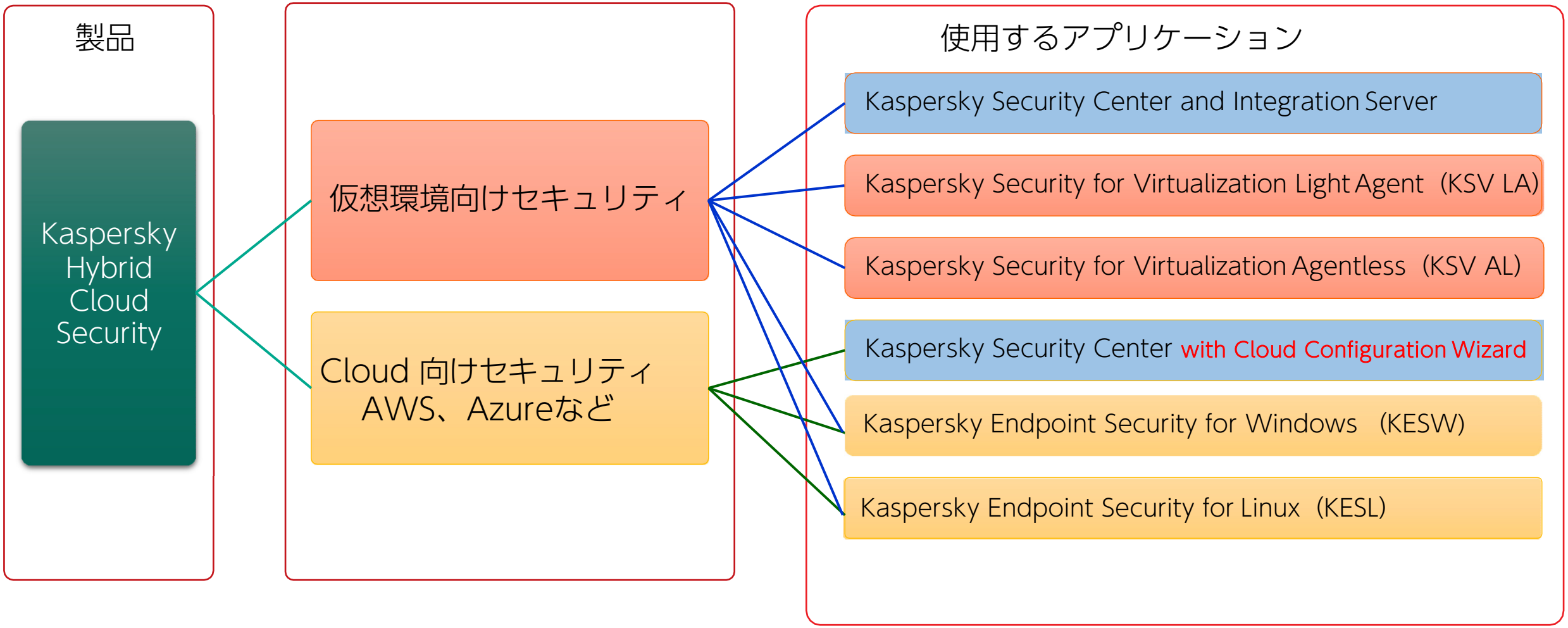
kaspersky

Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Securityは、
クラウド環境、仮想環境、物理サーバーに使用出来る製品です。



Kaspersky Hybrid Cloud Security（KHCS）



Kaspersky Endpoint Security for Windows11.9以降では、KHCSライセンスが使用出来ます。
仮想環境におけるクライアントOS保護には、Kaspersky Security for Virtualizationを使用します。

Kaspersky Hybrid Cloud Security ライセンスの種類

Kaspersky Hybrid Cloud Securityには5つのライセンス種別があります。

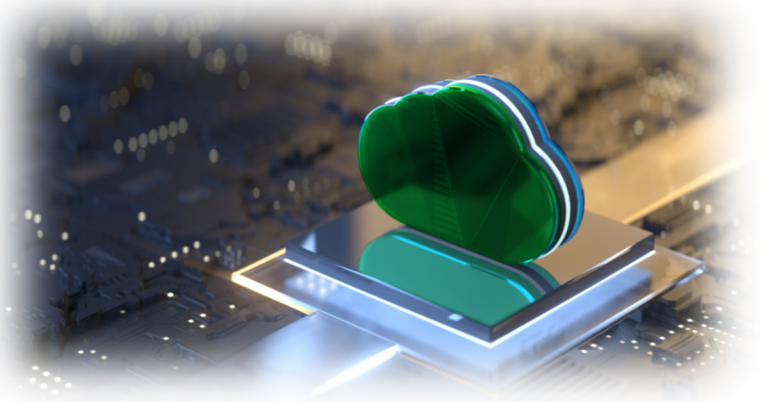
- Kaspersky Hybrid Cloud Security - デスクトップ
  - ✓ VDI向けライセンス。VDI数でカウント。

- Kaspersky Hybrid Cloud Security Enterprise - サーバー
- Kaspersky Hybrid Cloud Security - サーバー
  - ✓ 物理サーバー、仮想サーバー インスタンス、Public Cloud インスタンスに使用。
  - ✓ サーバーインスタンス数でカウント。

- Kaspersky Hybrid Cloud Security Enterprise - CPU
- Kaspersky Hybrid Cloud Security - CPU
  - ✓ 仮想環境向けライセンス。サーバー、クライアントOS（KSV使用時）共に保護対象。
  - ✓ ハイパーバイザー CPU数でカウント。

kaspersky

KHCS クラウド環境での使用



クラウド環境向け特徴

- クラウドAPIを使用した自動化

Kaspersky Security Center は、
AWS APIを使って Amazon EC2 インスタンスを操作
Azure API を使って Azure 仮想マシンを操作

Kaspersky Security Center を
Amazon EC2 インスタンスまたは Microsoft Azure 仮想マシンに導入して、
クラウド環境内のデバイスの保護を管理可能

デプロイの自動化により、Auto Scalingに対応

- 一台から導入可能。ファイルインテグリティなど高度セキュリティも安価に導入可能。

- BYOL（Bring Your Own License：ライセンス持ち込み）
社内サーバー、仮想基盤などと合わせたライセンス管理が可能。

Kaspersky Security Center； カスペルスキー製品を統合管理する管理サーバーアプリケーション

Cloud Configuration ウィザード

Cloud Configuration ウィザードとは

このウィザードを使用して Kaspersky Security Center を設定する場合に必要な項目

AWS クラウド環境で使用する場合

- クラウドセグメントをポーリングする権限が付与された IAM ロール
- またはクラウドセグメントをポーリングする権限が付与された IAM ユーザーアカウント

Microsoft Azure クラウド環境で使用する場合

- Azure アプリケーション ID パスワードとサブスクリプション

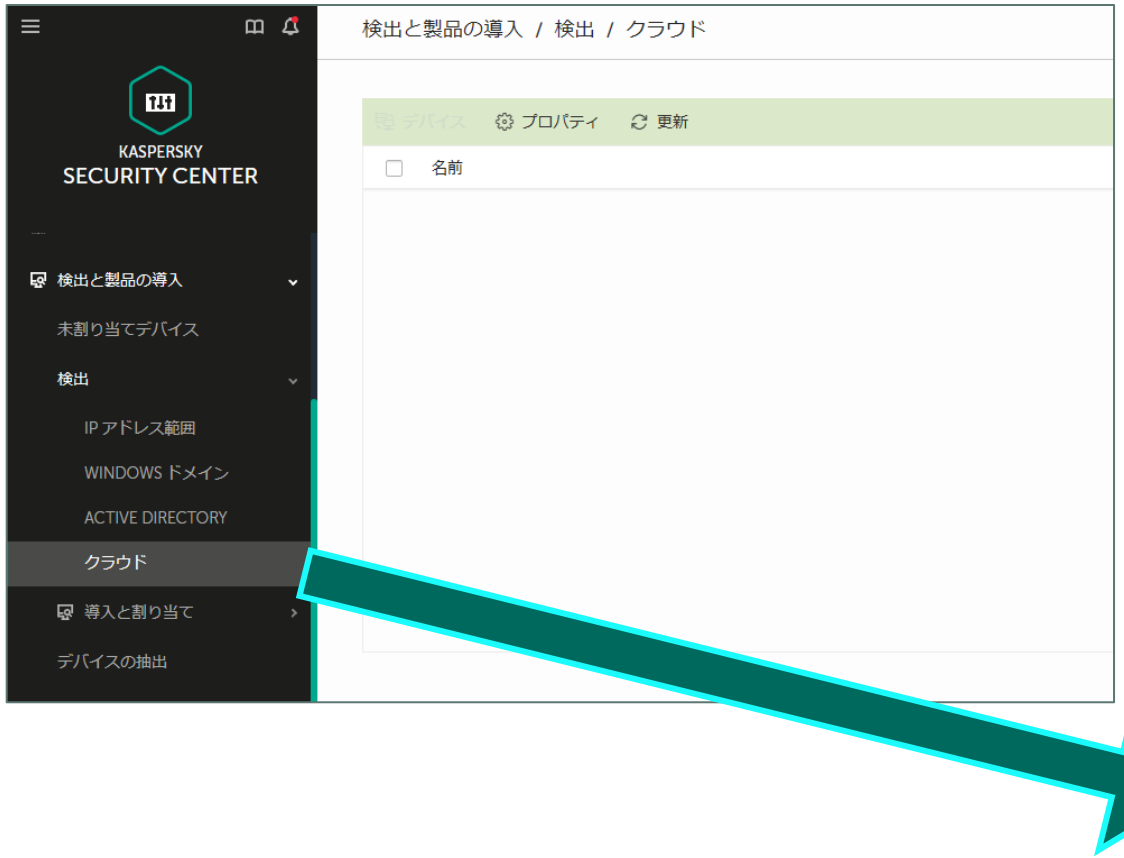
ウィザードでは、次のオブジェクトを作成

- 既定の設定が指定されたネットワークエージェントポリシー
- Kaspersky Endpoint Security for Linux のポリシー
- Kaspersky Security for Windows Server のポリシー
- インスタンス用の管理グループとインスタンスを自動的に管理グループに移動するためのルール
- 管理サーバーデータのデータバックアップタスク
- Linux と Windows を実行しているデバイスに保護をインストールするためのタスク
- 各管理対象デバイスに対するタスク：
  簡易ウイルススキャン
  アップデートのダウンロード

注 Windowsマシンには、Kaspersky Endpoint Security for Windows の使用を推奨します。

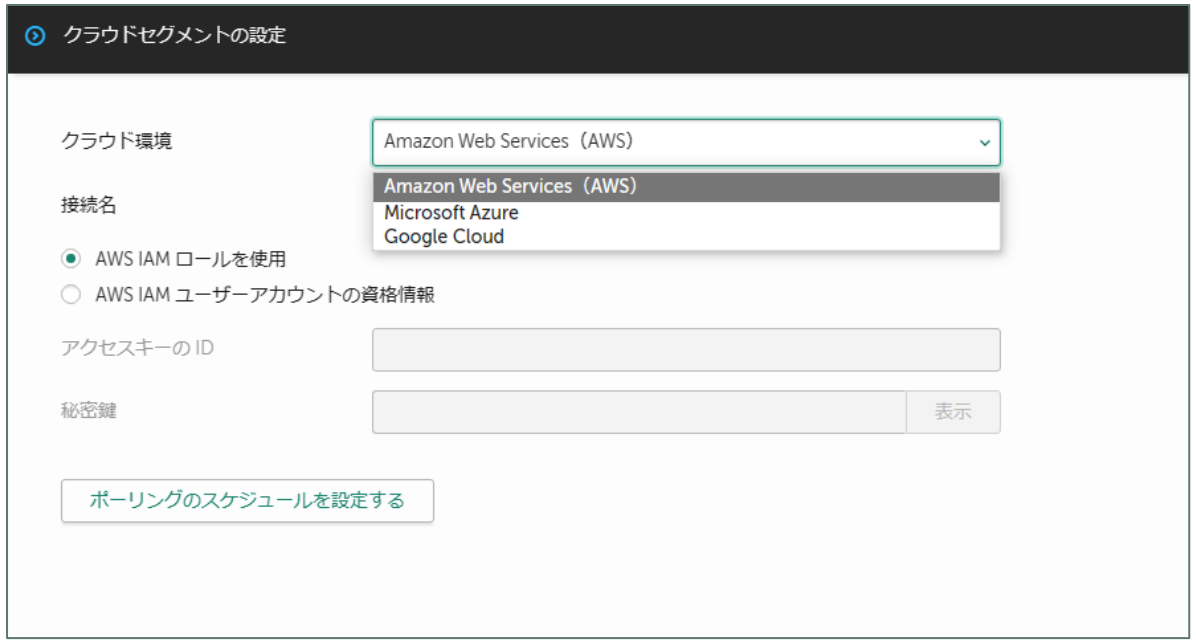
kaspersky

クラウドポーリング



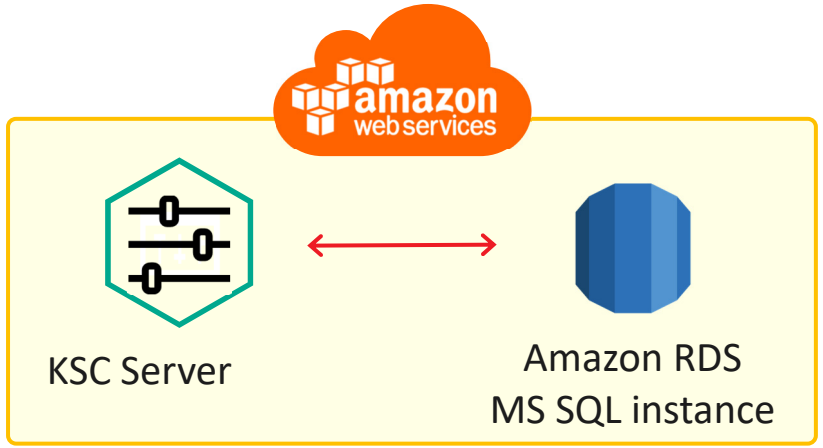
管理サーバーがクラウドセグメントのデバイスに関する情報を受信できるように、クラウドセグメントをポーリング

新しいインスタンスまたは仮想マシンが自動的に検出

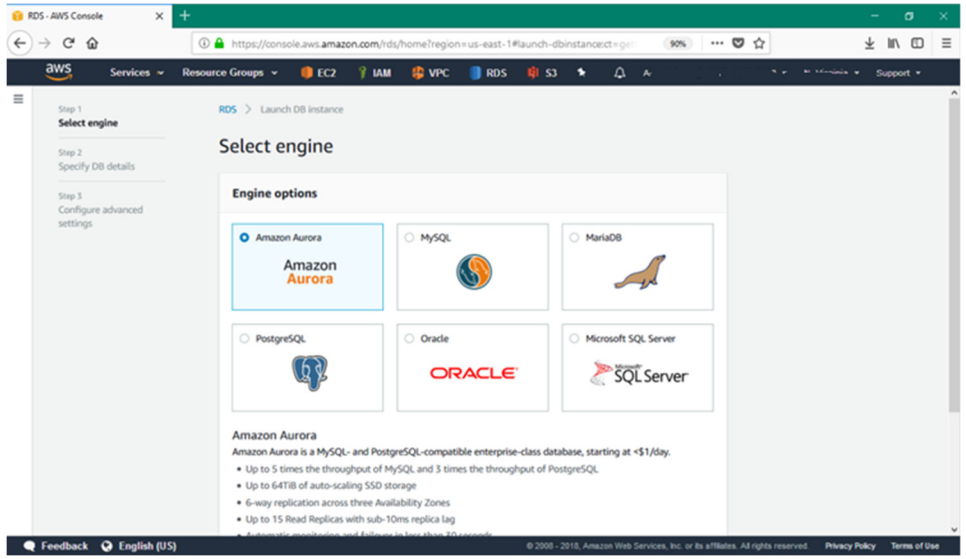


クラウドネイティブデータベースとの統合

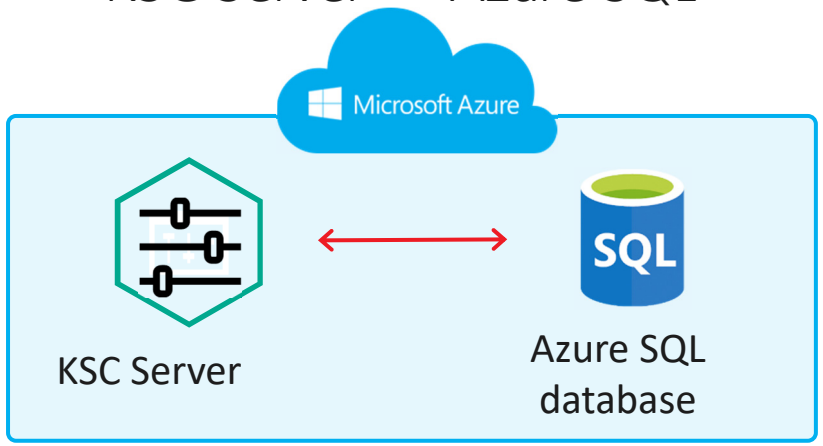
KSC Server ＋ Amazon DRS



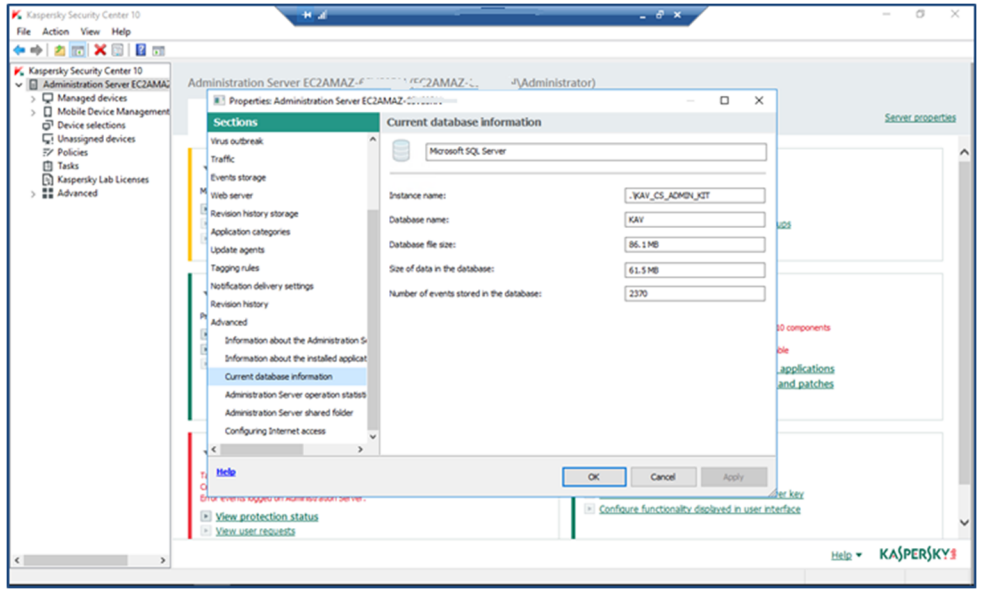
AWS Relational Database Service



KSC Server ＋ Azure SQL



KSC Database configuration



kaspersky

Cloudインスタンスに対するアプリケーション自動インストール

Kaspersky Security Center 14 では次のシナリオをサポート

- クライアントデバイスが API によって検出され、
  製品のインストールも API によって実行される。
  AWS と Azure のクラウド環境では、このシナリオがサポートされる。

- クライアントデバイスが Google API によって検出され、
  製品のインストールが Kaspersky Security Center によって実行される。
  Google Cloud では、このシナリオのみがサポートされる。

- クライアントデバイスが Active Directory のポーリング、Windows ドメインのポーリング、
  IP アドレス範囲のポーリングのいずれかで検出され、
  製品のインストールが Kaspersky Security Center によって実行される。

kaspersky

Cloudインスタンスに対するアプリケーション自動インストール

AWS クラウド環境
IAM ロールとEC2 インスタンスにインストールされている Systems Manager Agent により、
Kaspersky Security Center は 管理者に毎回確認しなくても、
デバイスおよびデバイスのグループに自動的にアプリケーションをインストールできる。

Microsoft Azure クラウド環境
Azure 仮想マシンエージェントにより、自動インストール。
Azure アプリケーション ID に次のロールが付与されている。

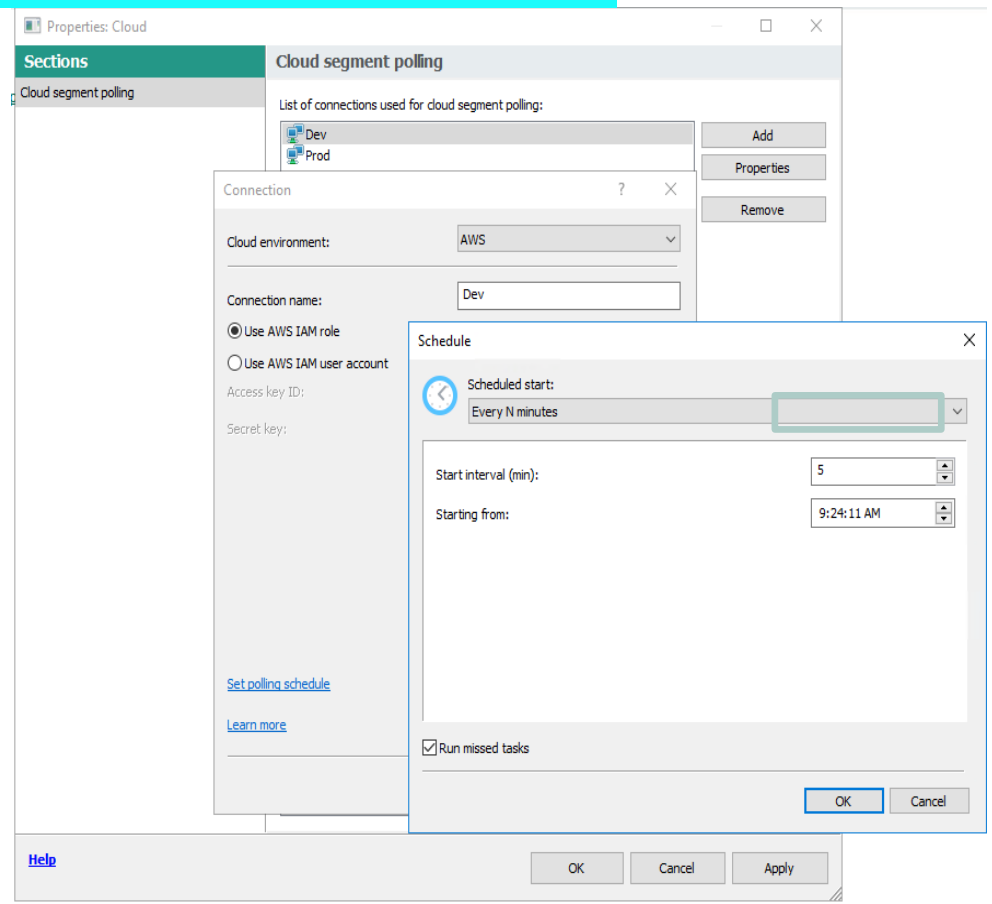
- Reader（ポーリングを使用して仮想マシンを検出するために必要）
- Virtual Machine Contributor（仮想マシンに保護を導入するために必要）
- SQL Server Contributor（Microsoft Azure 環境で SQL データベースを使用するために必要）

kaspersky

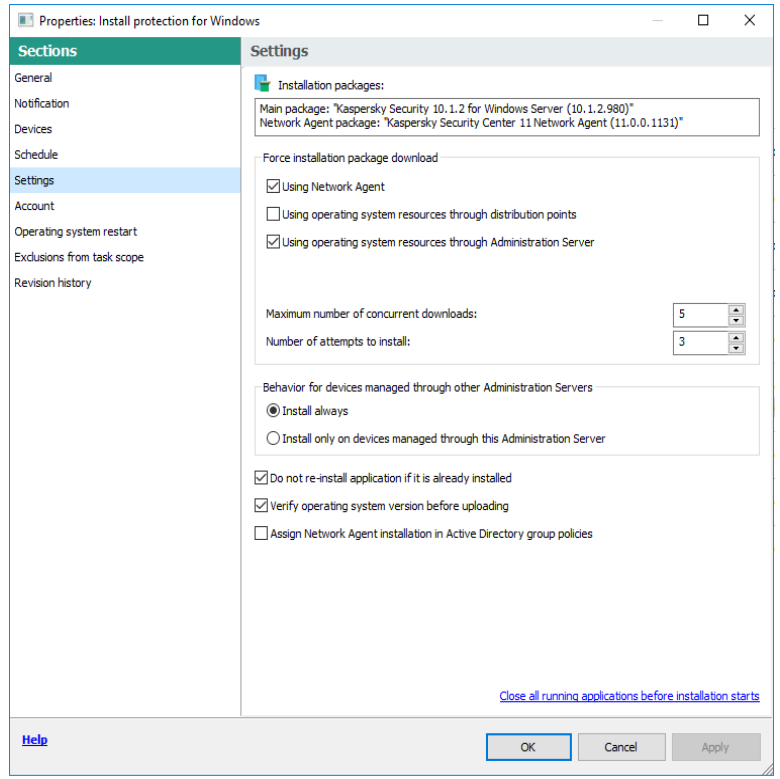
Cloudインスタンスに対するアプリケーション自動インストール

KSCによる保護コンポーネントインストール

5分ごとのAWS polling



「常にインストール」



kaspersky

Cloudインスタンスに対するアプリケーション自動インストール

AWS CloudFormation等を使用したスクリプトベース

winsrv_asg.ps1

```
$ServerAddress = "XXXXXX";
$ServerPort = "14000";
$ServerSSLPort = "13000";

$KSWSLocalFile = "C:¥Distributive¥ksws.zip";
$KSWSRemoteFile = "http://" + "$ServerAddress" + ":8060/Public/KSWS.zip";

New-Item -ItemType directory -Path "C:¥Distributive¥";

$WC = New-Object System.Net.WebClient;
$FTPURI = New-Object System.Uri($KSWSRemoteFile);
$WC.Credentials = New-Object System.Net.NetworkCredential($Username, $Password);
$WC.DownloadFile($FTPURI, $KSWSLocalFile);

$ShellApp = new-object -com shell.application;
$Zip = $ShellApp.NameSpace($KSWSLocalFile);
foreach ($item in $Zip.items()) {
    $ShellApp.Namespace("C:¥Distributive¥").copyhere($item);
}

$KnagentArgs = "/norestart", "/i", "C:¥Distributive¥agent¥klnagent.msi", "/l*xv", "C:¥Distributive¥klnagent.log", "/qn", "EULA=1", "PRIVACYPOLICY=1", "SER
Start-Process msiexec -ArgumentList $KnagentArgs -PassThru -Wait;
Start-Sleep -s 10;

$KNAService = Get-Service klnagent -ErrorAction Continue;
Start-Service -Name $KNAService.Name -ErrorAction SilentlyContinue;

$KSWSArgs = "/norestart", "/i", "C:¥Distributive¥server¥ks4ws_x64.msi", "/l*xv", "C:¥Distributive¥ksws.log", "/qn", "EULA=1", "PRIVACYPOLICY=1", "ADDLOCAL
Start-Process msiexec -ArgumentList $KSWSArgs -PassThru -Wait;
$ConsoleArgs = "/norestart", "/i", "C:¥Distributive¥server¥ks4wstools_x64.msi", "/l*xv", "C:¥Distributive¥kswsconsole.log", "/qn", "EULA=1", "PRIVACYPOLIC
Start-Process msiexec -ArgumentList $ConsoleArgs -PassThru -Wait
```

AWS Cloud Formation

Jenkins

Octopus Deploy

保護を展開するための展開スクリプト
https://support.kaspersky.co.jp/14713

kaspersky

Kaspersky CWPP（クラウドワークロード保護プラットフォーム） コンポーネント

Multi-layered protection

- Log Inspection
- KSN
- File AV
- Network Protection
- Docker & Windows Server 2016 containers
- File Integrity Monitor
- Exploit Prevention
- Anti-Ransomware
- Behavior Detection

Systems hardening

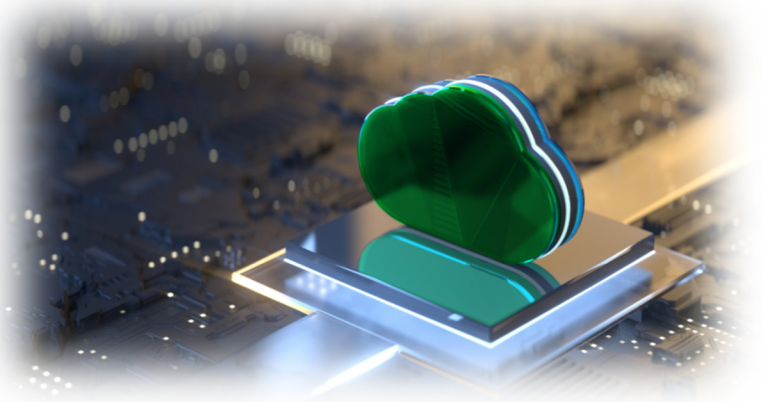
- File Integrity Monitor
- HIPS
- Firewall Management
- Application Control
- Default Deny
- Device Control

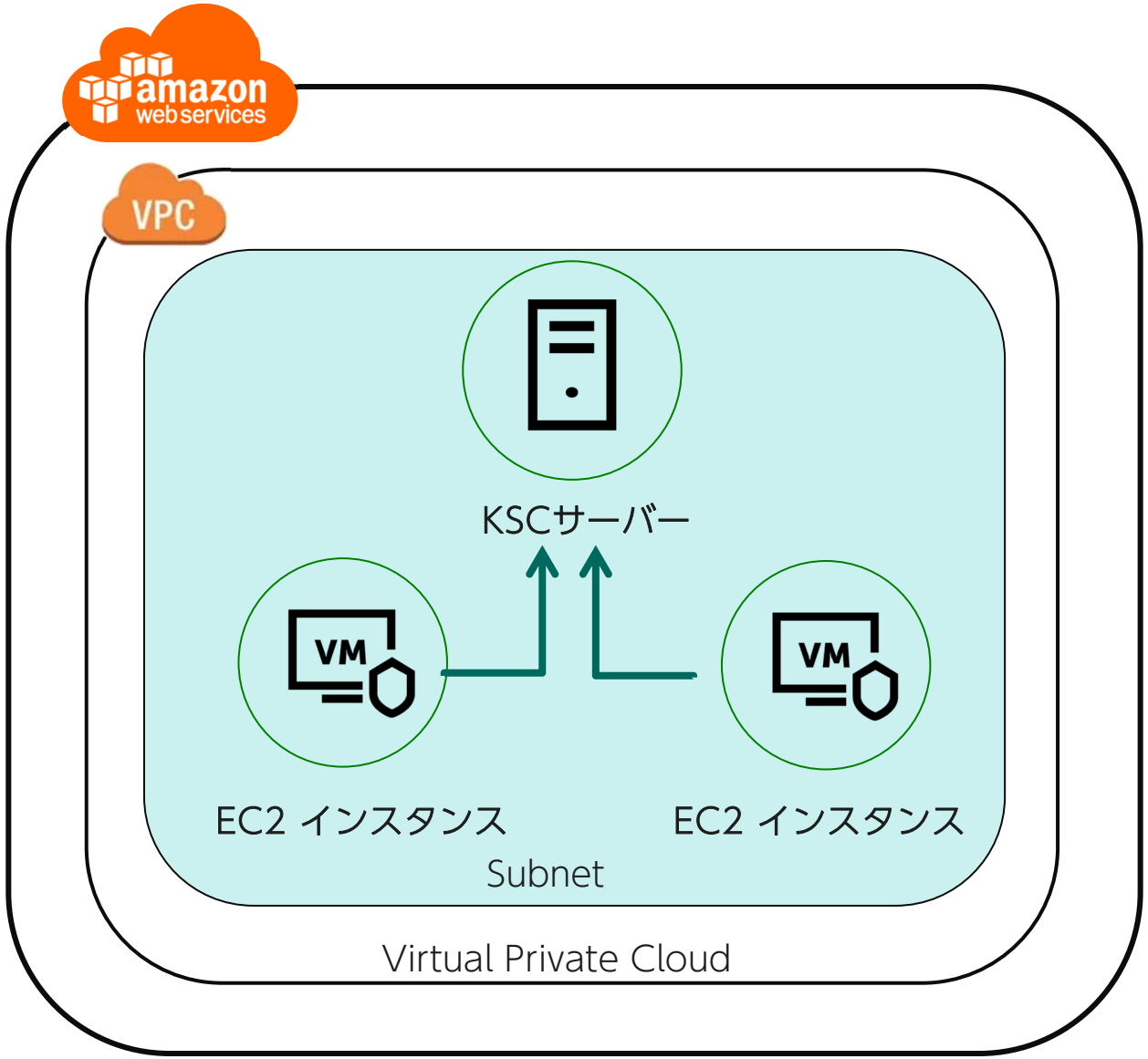
Continuous security: transparency and manageability

- Monitoring and Reports
- RBAC
- Account Management
- Centralized management
- Azure Integration

kaspersky

KHCS クラウド環境 構成例





内部トラフィックに課金発生せず

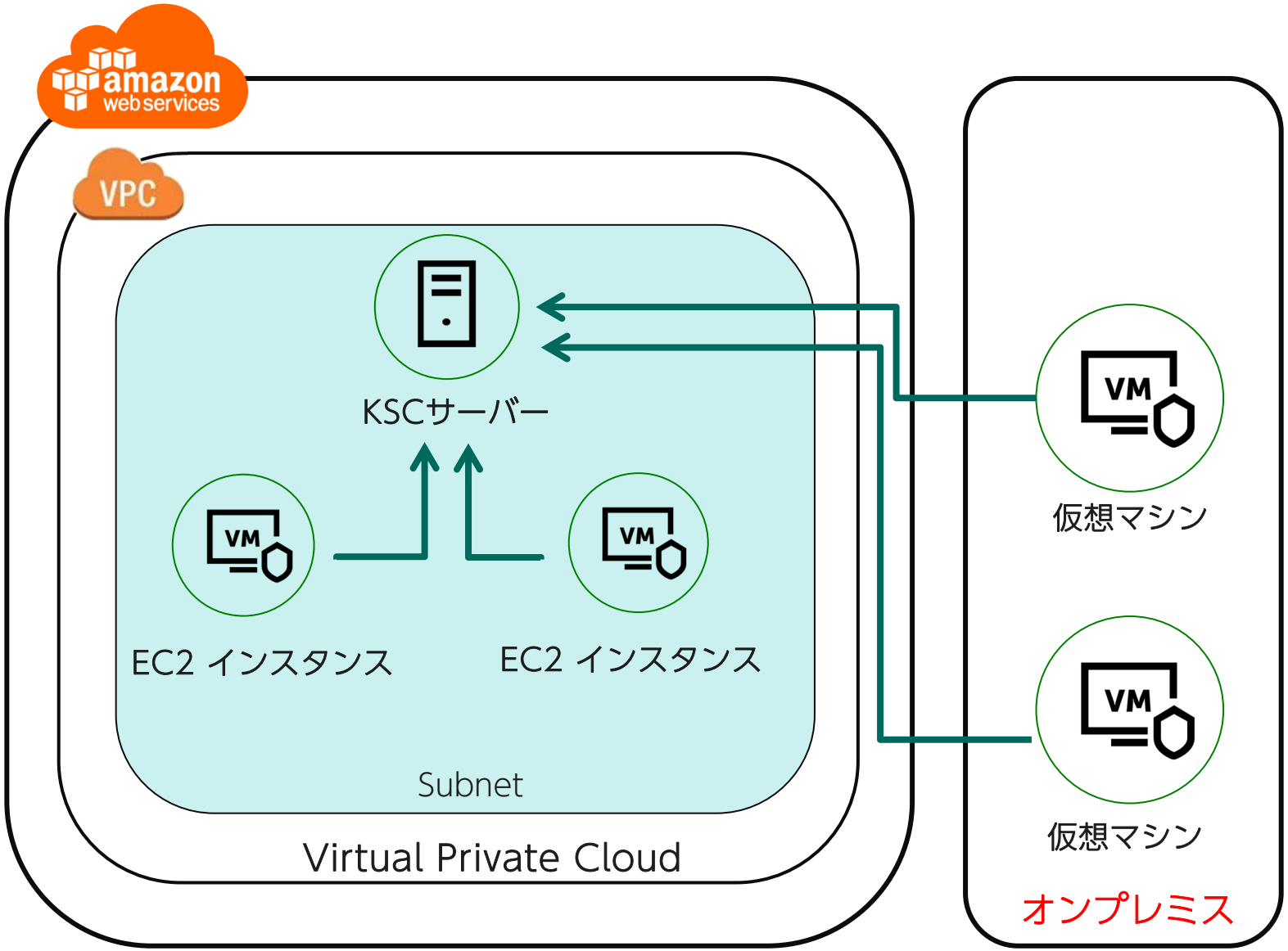
外側からのKSCポートへのアクセス権限が不要

IAMロールを通じたAPI使用の自然な構成

仮想マシンごとのライセンス

お客様使用のライセンスが利用可能
（ストアで購入する必要がない）

kaspersky



KSCアウトバウンドトラフィック
への課金

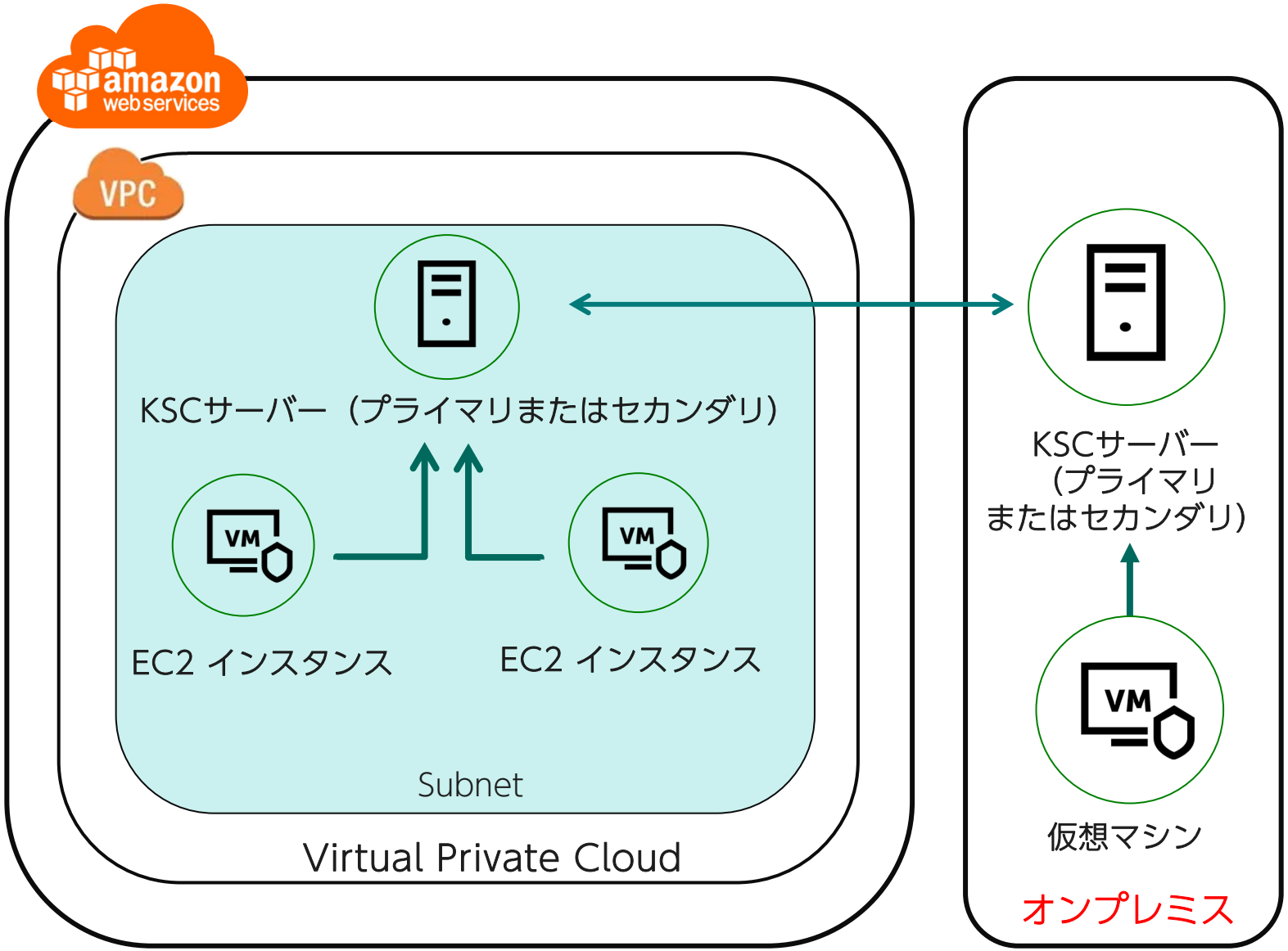
外側からのKSCポートへのアクセス権限

API使用の自然な構成

仮想マシンごとのライセンス

お客様使用のライセンスが利用可能
（ストアで購入する必要がない）

kaspersky



API使用の自然な構成

クラウドからの最小限アウトバウンド
トラフィック

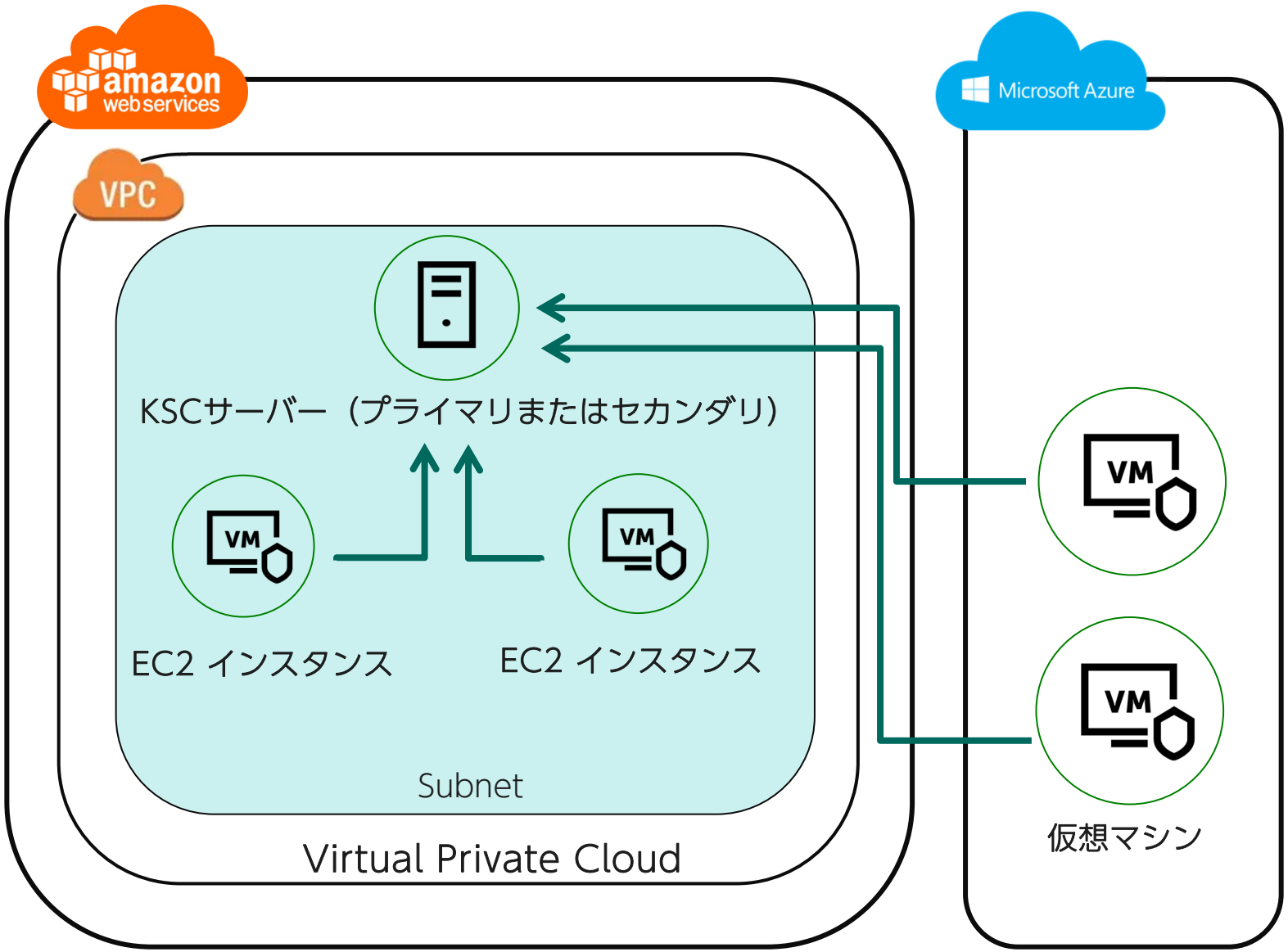
お客様使用のライセンスが利用可能
（ストアで購入する必要がない）

デメリット

イベントデータベースの分断

管理コンソールの分断

kaspersky



KSCアウトバウンドトラフィックへの課金

他クラウドとの統合に必要な設定

仮想マシンごとのライセンス

お客様使用のライセンスが利用可能（ストアで購入する必要がない）

kaspersky