

TED-TECH MAGAZINE

2021年12月

TED CSP TECH UPDATE  
December, 2021

東京エレクトロンデバイス株式会社



# TEDより お役立ち情報をお届け

TED CSP テクニカルアップデート情報誌  
2021年12月

東京エレクトロンデバイス株式会社



# 目次

## Azure アップデート情報

### Infrastructure as a Service

1. ゲートウェイ ロードバランサーのパブリック プレビュー
2. Azure Disk Storage ライブ サイズ変更のパブリック プレビュー
3. Azure VM での VM ゲストの自動パッチ適用
4. Azure Automation のマネージド ID のサポート
5. Azure Chaos Studio のパブリック プレビュー
6. Azure Bastion ネイティブ クライアントのサポート

### Platform as a Service

1. Application Gateway のワイルドカード リスナーが一般提供
2. Azure Load Testing がパブリック プレビュー
3. AKS ノード イメージの自動アップグレード
4. Azure Functions で Node.js 16 のサポートがプレビュー
5. .NET6 App Services のための Application Insights のオートインストラクション
6. Azure Scheduler が 2022 年 1 月 31 日に廃止

### Identity and Security

1. 条件付きアクセスの概要ダッシュボード
2. 条件付きアクセスのポリシーテンプレート
3. ワークロード ID 用の条件付きアクセス
4. エンタイトルメント管理のカスタム割り当てワークフロー
5. アプリとワークロード ID の新しい認証方法ポリシー
6. Azure AD TLS バージョン 1.0 および 1.1 廃止の追加アナウンス

### Data Platform

1. Azure Machine Learning : Auto ML のテストデータ指定が プレビュー
2. Synapse Analytics : Synapse Spark Pool のオートスケールが GA
3. Azure Data Explorer, Azure Data Factory, Synapse Analytics : Azure Data Explorer のコネクタが GA
4. Azure Database for PostgreSQL - Flexible Server : Azure Database for PostgreSQL フレキシブルサーバーが GA
5. SQL Server on IaaS (Windows / Linux) : IaaS Agent 拡張機能の GA 機能のご紹介

# ゲートウェイ ロードバランサーのパブリック プレビュー

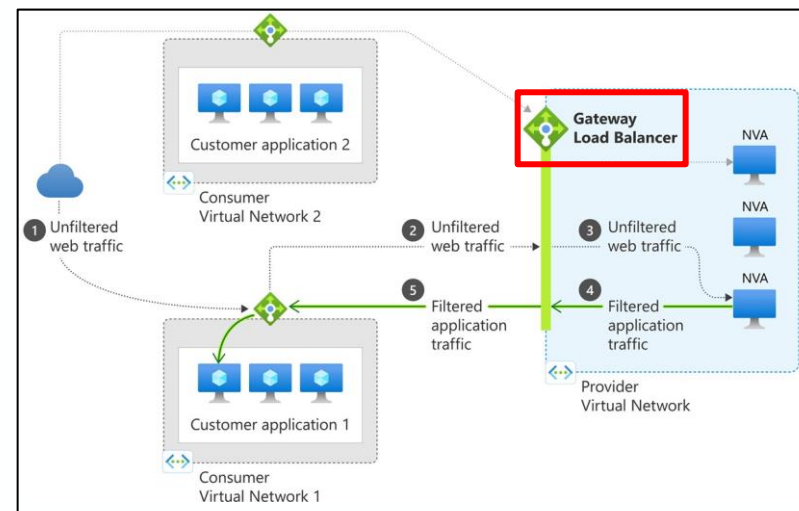
## プレビュー

### Infrastructure as a Service

- 3rd Party の NW 仮想アプライアンス (NVA) を使用する、ハイパフォーマンスかつ高可用性のシナリオに対応するロードバランサー
- FW やパケット分析、IDS/IPS、トラフィックのミラーリングなどの NVA の前段に配置して使用する
- NVA をネットワークパスに透過的に統合することができる
- アプリケーション VM と Gateway Load Balancer が異なる VNet、異なるサブスクリプション、テナント、リージョンに存在していてもチェーン可能
  - テナントが異なる場合はポータルでの設定不可
- NVA 前段の LB で不可分散するため可用性が向上、スケーリングが容易
- ルートテーブルを用いてルート制御をしなくとも対称性を維持できる
  - これまでも NVA を挟むことは可能だったが、よりシンプルに構成することができる

### ポイント

- 1つのゲートウェイロードバランサーに対して複数のチェーンを構成することや、単一のVMとのチェーンを構成することが可能
- チェーンできるのは、パブリックのStandard SKU ロードバランサーか、VM
- ゲートウェイロードバランサーとNVA間の通信はVXLANプロトコルを使用
- 料金は利用時間、チェーン数、データ処理量により変動



- **Gateway Load Balancer now in public preview**  
<https://azure.microsoft.com/ja-jp/updates/gateway-load-balancer-preview/>

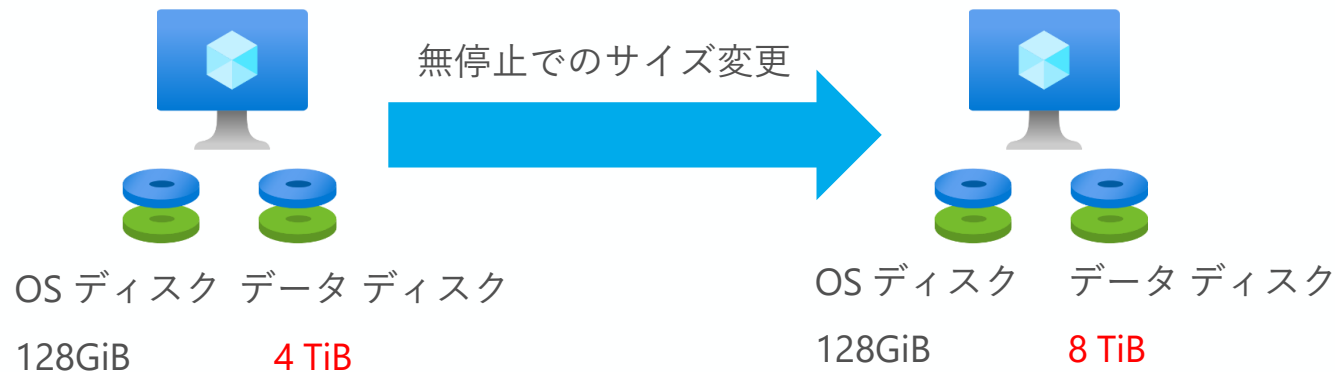
# Azure Disk Storage ライブ サイズ変更のパブリック プレビュー

## プレビュー

### Infrastructure as a Service

- Azure VM のディスク サイズを、VM を停止せずに変更することが可能
- プレビュー機能の登録には以下のコマンドを実行

```
az feature register --namespace Microsoft.Compute --name LiveResize
```



#### ポイント

- 現在は米国中西部リージョンのみ対応
- データ ディスクのみ対応
- 4 TiB 以上のディスクのみ対応
- 実施方法は以下の4つ
  - Azure CLI
  - Azure PowerShell
  - Azure ポータル
- <https://aka.ms/iaasexp/DiskLiveResize> からアクセス
- 2021-04-01 以降の API バージョンを含む Azure Resource Manager テンプレート

- **Live resize of Azure Disk Storage in public preview**  
<https://azure.microsoft.com/ja-jp/updates/live-resize-of-azure-disk-storage-in-public-preview/>
- **Azure CLI を使用して Linux VM の仮想ハード ディスクを拡張する**  
<https://docs.microsoft.com/ja-jp/azure/virtual-machines/linux/expand-disks>

# Azure VM での VM ゲストの自動パッチ適用

一般公開

Infrastructure as a Service

- Azure VM に自動的に更新プログラムを適用する、自動パッチ適用が一般公開
- [重大] または [セキュリティ] に分類されるパッチを自動的にダウンロード、適用
  - パッチの確認は数日毎、または 30 日以内に複数回実施
- VM のピーク外の時間帯に、可用性優先のオーケストレーションに従い適用
  - Az が異なる場合は同時に更新されない、geo ペア リージョンは同時に更新されない、など
- サポート対象の OS イメージ
  - 特定の Azure 提供イメージから作成された VM のみサポート
  - カスタムイメージは現状非サポート

ゲスト OS の更新プログラム

ホットパッチを有効にする (プレビュー) ① ☐

パッチ オーケストレーション オプション ① Azure 調整済み ▼

このイメージでは、一部のパッチ オーケストレーション オプションを使用できません。  
詳細情報

## ポイント

- Windows と Linux どちらでも利用可能
- パッチは、VM のタイムゾーンでピーク外の時間帯に適用される
- すべての VM サイズで利用可能
- 必要に応じて自動で再起動

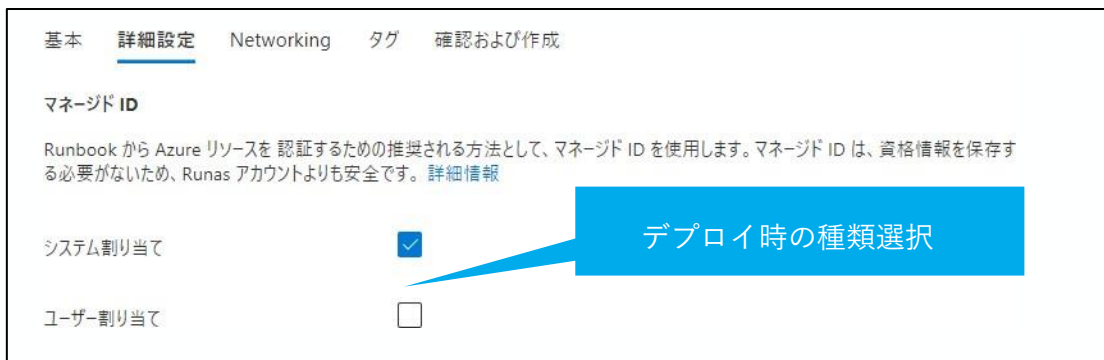
- **Automatic VM guest patching is now generally available**  
<https://azure.microsoft.com/ja-jp/updates/automatic-vm-guest-patching-now-available/>
- **Azure VM での VM ゲストの自動パッチ適用**  
<https://docs.microsoft.com/ja-jp/azure/virtual-machines/automatic-vm-guest-patching>

# Azure Automation のマネージド ID のサポート

一般公開

Infrastructure as a Service

- Azure Automation がマネージド ID の利用に対応
- 今後、Runbook 認証の際はマネージド ID を利用することが推奨
  - 既定の認証方法となり、従来の実行アカウント作成画面は表示されなくなる
  - 実行アカウント利用の Automation が使えなくなるわけではない
- システム割り当て、ユーザー割り当てのどちらの方式にも対応



基本 詳細設定 Networking タグ 確認および作成

マネージド ID

Runbook から Azure リソースを認証するための推奨される方法として、マネージド ID を使用します。マネージド ID は、資格情報を保存する必要がないため、Runas アカウントよりも安全です。詳細情報

システム割り当て ☒

ユーザー割り当て ☐

デプロイ時の種類選択

## ポイント

- 実行アカウントからの移行は以下の流れ
  1. 既存 Automation アカウントでマネージド ID 有効化
  2. 実行アカウントと同じ権限を、マネージド ID に割り当てる
  3. マネージド ID を使用するように、Runbook を更新

- 既存の実行アカウントからマネージド ID に移行する  
<https://docs.microsoft.com/ja-jp/azure/automation/enable-managed-identity-for-automation#migrate-from-existing-run-as-accounts-to-managed-identity>
- Azure Automation support for Managed Identities is now generally available  
<https://azure.microsoft.com/ja-jp/updates/azure-automation-managed-identities-ga/>

# Azure Chaos Studio のパブリック プレビュー

## プレビュー

### Infrastructure as a Service

- システムに意図的に障害を挿入することができる Azure Chaos Studio が登場
  - 実際のインシデントに対するアプリケーションとサービスの回復性を測定、理解、構築するために役立つ
- 挿入可能な障害
  - VM 停止、CPU・メモリ・I/O ストレス、ネットワークの不通、フェールオーバー、Pod 再起動 など
- 非対応な障害
  - VM ホスト障害や、AKS のコントロール プレーンの障害など、ユーザーが意図的に発生させられないもの

**フォールト**

フォールトとは、Chaos Studio がアプリケーションまたはインフラストラクチャに注入する障害です。実験に追加するフォールトを選択してください。各フォールトのサンプル値の詳細については、[フォールトライブラリ](#)にアクセスしてください。🔗

CPU Pressure

**パラメーター**

パラメーターを使用すると、フォールトの影響をカスタマイズできます。

Duration (minutes)

10

pressureLevel

85

障害の種類やパラメーターを指定

### ポイント

- 2021 年 11 月時点の対象リソース
  - Virtual Machines、Virtual Machine Scale Sets
  - Azure Cosmos DB
  - Azure Kubernetes Service (AKS)
  - Network Security Groups (NSG)
  - Azure Cache for Redis
- 2021 年 11 月時点の対応リージョン
  - West Europe、**Japan East**、UK South、Central US、East US、West Central US、West US 2
- 2022 年 4 月 4 日まで無料

- Public preview: Azure Chaos Studio - Systematically improve resilience with controlled chaos  
<https://azure.microsoft.com/ja-jp/updates/public-preview-azure-chaos-studio-systematically-improve-resilience-with-controlled-chaos/>
- クイック スタート: Azure Chaos Studio を使用してカオス実験を作成して実行する  
<https://docs.microsoft.com/ja-jp/azure/chaos-studio/chaos-studio-quickstart-azure-portal>



# Azure Bastion ネイティブ クライアントのサポート

## プレビュー

### Infrastructure as a Service

- Azure Bastion Standard SKU にて、ネイティブ クライアントをサポート
- Windows マシン上のネイティブ クライアント (RDP 接続、Azure CLI の SSH Extension ) で Azure VM へ接続

- 接続用コマンド

- RDP 接続

```
PS C:\Users\kakusaya> az network bastion ssh --name DemoBastion --resource-group BastionTest --target-resource-id /subscriptions/69223c60-0db4-4b29-8990-9ab6269e200b/resourceGroups/BastionTest/providers/Microsoft.Compute/virtualMachines/BastionTest2 --auth-type password --username kkuser
Command group 'network bastion' is in preview and under development. Reference and support levels: https://aka.ms/CLI_refstatus
kkuser@localhost's password:
Last login: Tue Dec  7 06:04:12 2021 from vm000000.internal.cloudapp.net
[kkuser@bastiontest2 ~]$
[kkuser@bastiontest2 ~]$
[kkuser@bastiontest2 ~]$ hostname
bastiontest2
[kkuser@bastiontest2 ~]$ exit
```

```
az network bastion rdp --name "<BastionName>" --resource-group "<ResourceGroupName>" --target-resource-id "<VMResourceId>"
```

- SSH 接続

```
az network bastion ssh --name "<BastionName>" --resource-group "<ResourceGroupName>" --target-resource-id "<VMResourceId>" --auth-type "password" --username "<Username>"
```

- SSH 用拡張機能のインストール

```
az extension add --name ssh
```

#### ポイント

- Key Vault に保存した SSH キーを利用したサインインはサポートされていないため事前にローカルヘダウンドロードする
- Windows VM では RDP (3389) , Linux VM では SSH (22) ポートを開いておく
- Azure AD での認証にも対応

#### Public preview: Azure Bastion native client support

<https://azure.microsoft.com/ja-jp/updates/public-preview-azure-bastion-native-client-support/>

#### Bastion と Windows コンピューター上のネイティブ クライアントを使用して、仮想マシンに接続する (プレビュー)

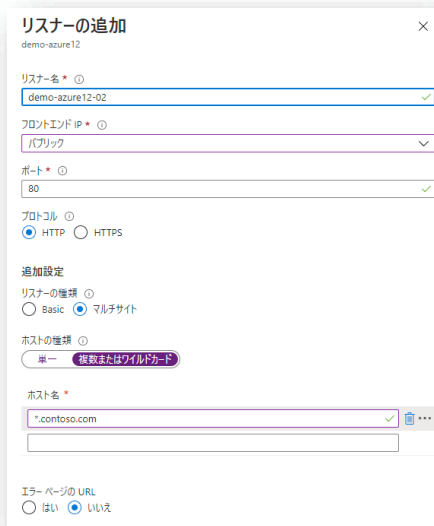
<https://docs.microsoft.com/ja-jp/azure/bastion/connect-native-client-windows>

# Application Gateway のワイルドカード リスナーが一般提供

一般公開

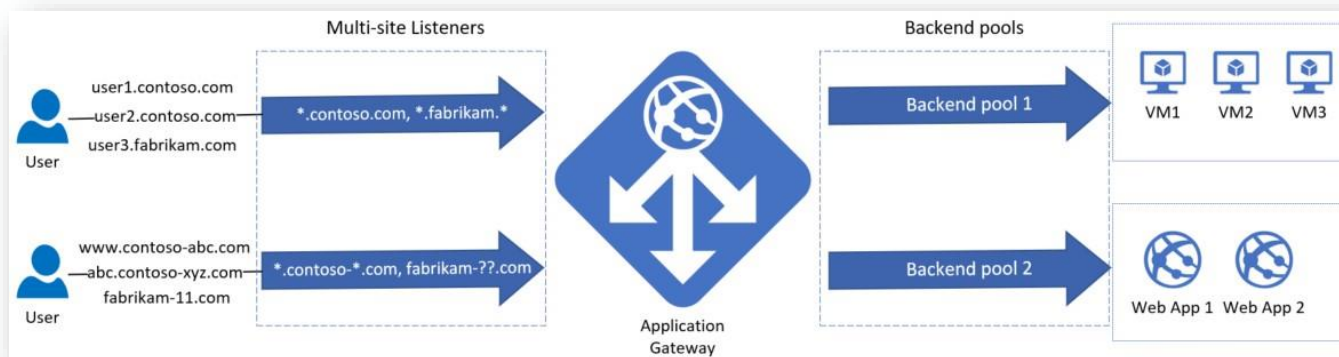
Platform as a Service

- Azure Application Gateway が、マルチサイト HTTP(S) リスナーのホスト名に、アスタリスク (\*) やクエスションマーク (?) などのワイルドカード文字の使用をサポートしました。
- shop.contoso.com、accounts.contoso.com、pay.contoso.com などの複数のホスト名からのリクエストを、\*.contoso.com などのワイルドカードホスト名で構成された1つのリスナーを介して、同じバックエンドプールにルーティングできるようになりました。



## ポイント

- Standard\_v2 および WAF\_v2 SKU でのみ使用できます。



## General availability: Wildcard listener on Application Gateways

<https://azure.microsoft.com/ja-jp/updates/general-availability-wildcard-listener-on-application-gateways/>

# Azure Load Testing がパブリック プレビュー

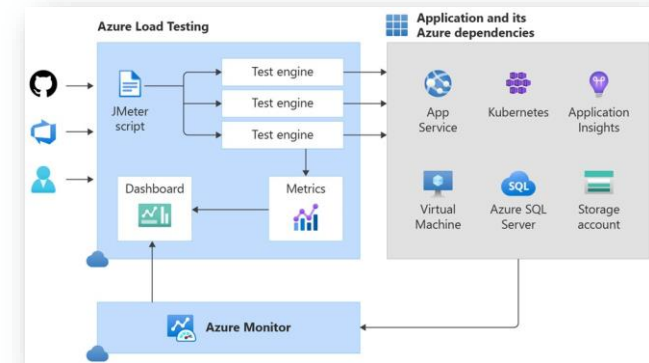
## プレビュー

### Platform as a Service

- Azure Load Testing は、フルマネージドの Azure サービスで、開発者やテスト担当者は、カスタム JMeter スクリプトで大規模な負荷を生成してシミュレーションを実行し、実用的な洞察を得て、大規模なパフォーマンスボトルネックをキャッチして修正し、自動化された CI/CD パイプラインでテストシフトすることができます。
  - インフラの複雑性を排除し、大規模な JMeter スクリプトのパワーを最大限に引き出すことで、負荷テストを簡素化します。
  - アプリケーションのパフォーマンスに関する実用的な洞察を伴う、精選されたクライアントとサーバーのメトリクスの包括的な表示
  - CI/CD ワークフローとの統合により、自動化された協調的な負荷テストを実現
  - 既存の Azure の慣習に基づいて構築された、合理的な課金とテスト管理

## ポイント

- DevOps や GitHub Actions と組み合わせることができます。
- Azure Monitor と統合されて、詳細を取得することができます。



- **Azure Load Testing now available in public preview**  
<https://azure.microsoft.com/ja-jp/updates/azure-load-testing-now-available-in-public-preview/>
- **Introducing Azure Load Testing: Optimize app performance at scale**  
<https://azure.microsoft.com/en-us/blog/introducing-azure-load-testing-optimize-app-performance-at-scale/>

# AKS ノード イメージの自動アップグレード

一般公開

Platform as a Service

- Azure Kubernetes サービス (AKS) の自動アップグレード機能の一般的な可用性を発表します。この機能を使用すると、新しい AKS ノード イメージまたはクラスター バージョンが使用可能になったときに、ノード イメージまたはクラスター バージョンを自動的にアップグレードするようにオプトインできます。
- ノード イメージまたはクラスターを手動でアップグレードする必要がなくなったため、操作が簡素化されます

```
az aks update --resource-group myResourceGroup --name myAKSCluster --auto-upgrade-channel stable
```

```
az aks show --resource-group myResourceGroup --name myAKSCluster
```

```
3    "scaleDownDelayAfterDelete": "10s",
4    "scaleDownDelayAfterFailure": "3m",
5    "scaleDownUnneededTime": "10m",
6    "scaleDownUnreadyTime": "20m",
7    "scaleDownUtilizationThreshold": "0.5",
8    "scanInterval": "10s",
9    "skipNodesWithLocalStorage": "false",
10   "skipNodesWithSystemPods": "true"
11 },
12   "autoUpgradeProfile": {
13     "upgradeChannel": "stable"
14   }
15 }
```

- General availability: AKS node image auto-upgrade  
<https://azure.microsoft.com/ja-jp/updates/general-availability-aks-node-image-autoupgrade/>

# Azure Functions で Node.js 16 のサポートがプレビュー

プレビュー

Platform as a Service

- Azure Functions ランタイム 4.0 で Node.js 16.x の Azure Functions サポートがプレビューになりました。
- 現在の LTS バージョンである Node.js 16.13.0 は、Linux の Functions アプリで利用できます。Windows Functions アプリは、現在バージョン 16.9.1 をサポートしており、2021 年 12 月に LTS バージョンに更新される予定です。
- Azure Functions 上の Node.js を使い始めるには [こちら](#) をご覧ください。

|             |                                                                        |
|-------------|------------------------------------------------------------------------|
| 公開 *        | <input checked="" type="radio"/> コード <input type="radio"/> Docker コンテナ |
| ランタイムスタック * | <div>Node.js</div>                                                     |
| バージョン *     | <div>16 LTS (プレビュー)</div>                                              |
| 地域 *        | <div>Central US</div>                                                  |

- **Public preview: Node.js 16 in Azure Functions**  
<https://azure.microsoft.com/ja-jp/updates/public-preview-nodejs-16-in-azure-functions/>

# .NET6 App Services のための Application Insights のオート インストラクション

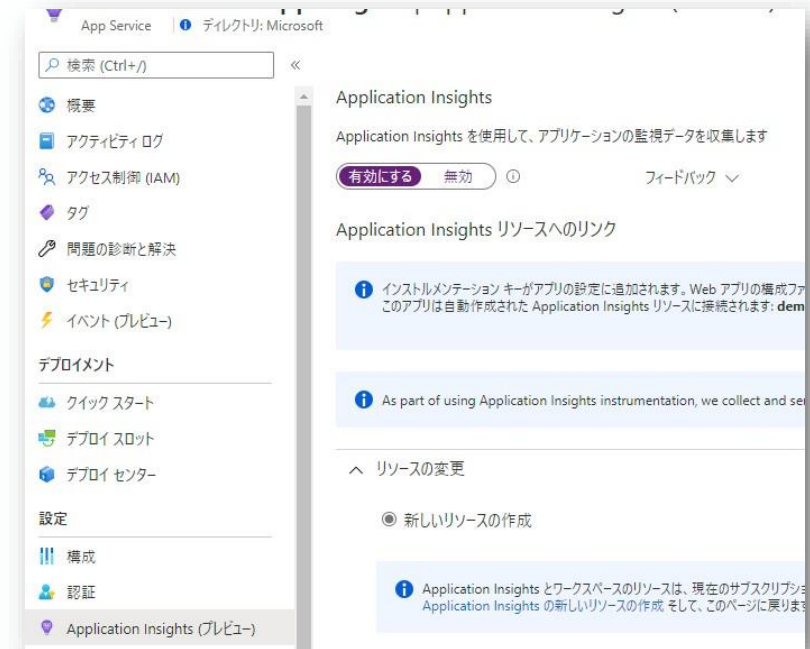
一般公開

Platform as a Service

- Application Insights のオート インストラクションに Windows と Linux の両方の Azure App Services における .NET6 が追加されました。

## ポイント

- Windows のオート インストラクション では、ASP.NET Core の次のバージョンがサポートされています。
  - ASP.NET Core 3.1
  - .NET 5 / .NET 6
- Linux のオート インストラクション では、.NET 6 のみサポートされています。



- Application Monitoring for Azure App Service and ASP.NET Core  
<https://docs.microsoft.com/en-us/azure/azure-monitor/app/azure-web-apps-net-core?tabs=Windows%2CLinux>

# Azure Scheduler が 2022 年 1 月 31 日に廃止

## サービス終了

Platform as a Service

- Azure Scheduler が 2022 年 1 月 31 日に廃止となります。
- Azure Scheduler で設定したジョブを引き続き使用するには、2022 年 1 月 31 日までに Azure Logic Apps に移行して、使い慣れた機能や高度な機能を活用してください。これには次のようなものがあります。
  - ビジュアルデザイナーとコネクターを使用して、Azure Blob storage、Azure Service Bus、Microsoft Outlook、SAP などの多くのサービスと統合します。
  - 各スケジュールを個別の Azure リソースとして管理。
  - 1つのロジックアプリを使って複数のワнтаイムジョブを実行。
  - サマータイムに自動調整するスケジュールを設定。
- 移行ガイドンスと FAQ を確認して、2022 年 1 月 31 日までにスケジュールされたジョブの Logic Apps への移行を開始してください。ご不明な点がある場合は、Microsoft Q&A でコミュニティの専門家から回答を得るか、[logicappsemail@microsoft.com](mailto:logicappsemail@microsoft.com) にお問い合わせください。

- **Azure Scheduler will be retired on 31 January 2022**  
<https://azure.microsoft.com/ja-jp/updates/azure-scheduler-will-be-retired-on-31-january-2022/>
- **移行ガイドンス**  
<https://docs.microsoft.com/en-us/azure/scheduler/migrate-from-scheduler-to-logic-apps>



# 条件付きアクセスの概要ダッシュボード

## プレビュー

### Identity and Security

- Azure AD では、条件付きアクセスの概要ダッシュボードを新たにプレビューで提供開始しました。ダッシュボードでは、組織のサインイン パターンの分析に基づいて、ポリシーを強化するヒントを提供します。また、カバレッジ状況や監視などのサマリ情報を参照することができます。



- ポイント
- ダッシュボードからフィルターされた詳細を可能
  - ヒントを基にテンプレートからポリシー作成をナビゲート

- Ignite における ID 関連の発表まとめ - Azure AD の技術革新による障害耐性の強化  
<https://jpazureid.github.io/blog/azure-active-directory/identity-at-ignite-strengthen-resilience-with-identity/>



# 条件付きアクセスのポリシーテンプレート

## プレビュー

### Identity and Security

- Azure AD では、一般的な条件付きアクセスのポリシーをテンプレートとしてプレビュー提供開始しました。管理者は、ダッシュボードのヒントや新規ポリシーを作成する際に、テンプレートを利用したポリシー展開をすることができます。

ID とデバイスのカテゴリで、それぞれテンプレートを提供

ポリシー名や状態を設定するだけで、推奨ポリシーが作成

#### テンプレートから新しいポリシーを作成 (プレビュー) ...

ツールのカスタマイズ テンプレートの選択 確認と作成

応答に基づいて次のテンプレートをお勧めします

☒ 管理者に多要素認証を要求する

侵害のリスクを軽減するために、特権のある管理アカウントに多要素認証を要求します。このポリシーは、セキュリティの既定値と同じロールを対象とします。

ポリシーの概要を表示する

☐ セキュリティ情報登録の保護

ユーザーが Azure AD 多要素認証とセルフサービス パスワードに登録するタイミングと方法をセキュリティで保護します。

ポリシーの概要を表示する

☐ レガシ認証をブロックする

多要素認証をバイパスするために使用できるレガシ認証エンドポイントをブロックします。

ポリシーの概要を表示する

☐ Azure 管理に多要素認証を要求する

Require multi-factor authentication to protect privileged access to Azure resources.

ポリシーの概要を表示する

☐ 危険なサインインに多要素認証を要求する

サインインリスクが中または高であることが検出された場合、多要素認証を要求します。(Azure AD Premium 2 ライセンスが必要)

ポリシーの概要を表示する

☐ 危険性の高いユーザーにパスワードの変更を要求する

ユーザー リスクが高であることが検出された場合、ユーザーにパスワードの変更を要求します。(Azure AD Premium 2 ライセンスが必要)

ポリシーの概要を表示する

ポリシーに名前をつける

CA001: すべての管理者に多要素認証を要求する

ポリシーの状態

☐ オフ ☐ オン ☒ レポート専用

ツールのカスタマイズ テンプレートの選択 確認と作成

#### 基本

ポリシー名

CA001: すべての管理者に多要素認証を要求する

ポリシーの状態

レポート専用

テンプレート カテゴリ

Identities

ポリシー テンプレート

CA001: すべての管理者に多要素認証を要求する

#### 割り当て

ユーザーとグループ

除外されたユーザー

含められたディレクトリ ロール

現在のユーザー

グローバル管理者  
アプリケーション管理者  
認証管理者  
課金管理者  
クラウド アプリケーション管理者  
条件付きアクセス管理者  
Exchange 管理者  
ヘルプデスク管理者  
パスワード管理者  
特権認証管理者  
特権ロール管理者  
セキュリティ管理者  
SharePoint 管理者  
ユーザー管理者

クラウド アプリまたは操作  
クラウド アプリ

すべてのアプリ

アクセス制御

許可

アクセス権の付与

多要素認証を要求する

テンプレートを基にウィザードでポリシー作成が可能

## Conditional Access templates (Preview)

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policy-common>

# ワークロード ID 用の条件付きアクセス

## プレビュー

### Identity and Security

- Azure AD では、サービス プリンシパルのアクセス制御を可能とするワークロード ID 用の条件付きアクセスをプレビューで提供開始しました。管理者は、サービス プリンシパルを認証に利用する PowerShell バッチ スクリプトを含む、デーモン アプリケーションなどのアクセス元を IP アドレスで制御することができます。

Workload-ID-CA ...

条件付きアクセス ポリシー

削除

シグナルを統合し、意思決定を行い、組織のポリシーを適用するために、条件付きアクセス ポリシーに基づいてアクセスを制御します。詳細情報

名前 \*

Workload-ID-CA

割り当て

ユーザーまたはワークロード ID ①

特定のサービス プリンシパルが含まれている

クラウド アプリまたは操作 ①

すべてのクラウド アプリ

条件 ①

1 個の条件が選択されました

アクセス制御

許可 ①

アクセスのブロック

ワークロード ID では、現時点で場所のみを条件として設定することが可能

UI を前提としないため、アクセス制御は、ブロックのみを提供

アクティビティの詳細: サインイン

基本情報 場所 認証の詳細 条件付きアクセス レポート専用

許可された時刻 2021/11/22 19:38:42 アプリケーション CertServicePrincipalAuth

要求 ID c26e6bf5-c8e6-4641-be52-a11d97615900 アプリケーション ID 0fe122df-445e-482b-a704-95aa11725cba

相関 ID 8c8052ca-69bb-4d91-8e25679310fa5c

状態 失敗

継続的アクセス評価 いいえ

サインインのエラー コード 53003

エラーの理由 Access has been blocked by Conditional Access policies. The access policy does not allow token issuance.

追加の詳細 If this is unexpected, see the conditional access policy that applied to this request in the Azure Portal.

ワークロード ID 用の条件付きアクセスにより指定された場所以外からのサービスプリンシパル認証をブロック

#### ポイント

- 現時点で、シングルテナント サービスプリンシパルのみをアクセス制限することが可能
- SaaS およびマルチテナント アプリケーションはスコープ外
- マネージド ID についてもポリシー対象外

## Conditional Access for workload identities preview

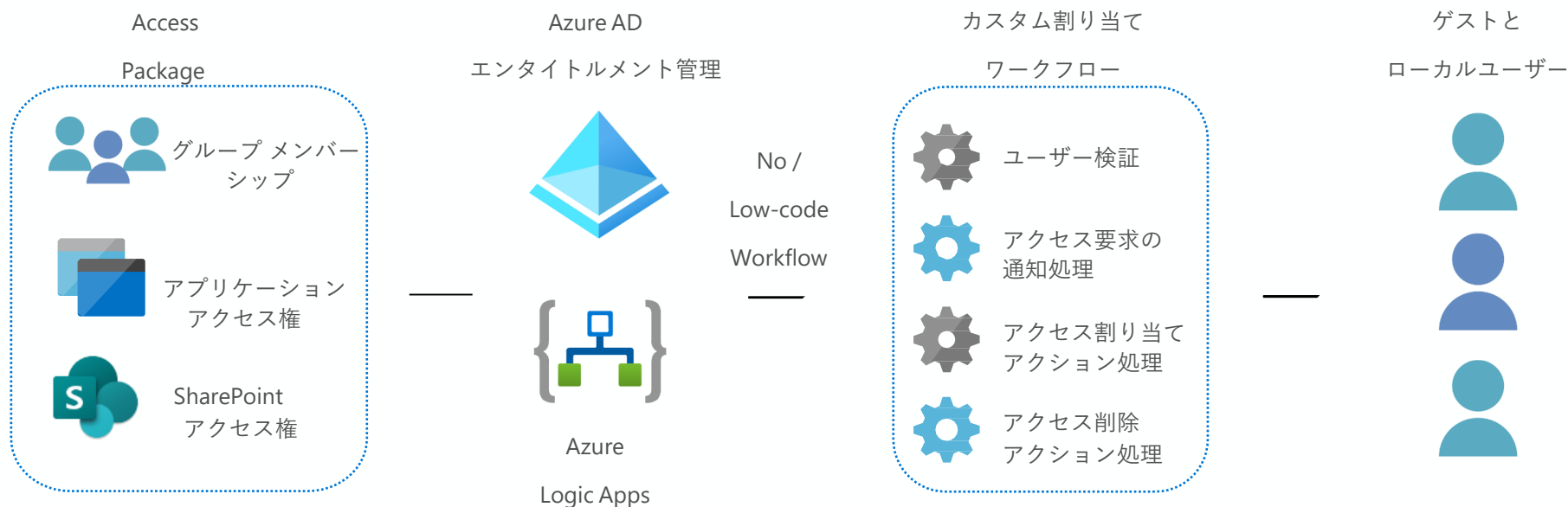
<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/workload-identity>

# エンタイトルメント管理のカスタム割り当てワークフロー

## プレビュー

### Identity and Security

- Azure AD では、エンタイトルメント管理で Logic Apps によるカスタム割り当てワークフローの組み込み機能をプレビューで提供開始しました。管理者は、エンタイトルメント管理での権限要求、付与、失効のタイミングで、ワークフローを構成してカスタム アクションを実行することができます。



## Trigger custom Logic Apps with Azure AD entitlement management

<https://docs.microsoft.com/ja-jp/azure/active-directory/governance/entitlement-management-logic-apps-integration>

# アプリとワークロード ID の新しい認証方法ポリシー

## プレビュー

### Identity and Security

- Azure AD では、アプリケーションの認証方法として非対称キー（証明書）の使用を推奨しています。この推奨を強制するポリシーを Graph API でプレビュー提供開始しました。管理者は、tenantAppManagementPolicy または appManagementPolicy でアプリのセキュリティ強化を開発者およびアプリに準拠させることができます。

| 制限名                   | 説明                          | 例                                                                           |
|-----------------------|-----------------------------|-----------------------------------------------------------------------------|
| passwordAddition      | アプリケーションのパスワードシークレットを完全に制限  | 2019/01/01 以降に作成されたアプリケーションの新しいパスワード（Client Secret）をブロック                    |
| passwordLifetime      | パスワードシークレットの最大有効期間範囲を適用     | 2015/01/01 以降に作成されたアプリケーションでは、すべての新しいパスワードシークレット（Client Secret）を最大 30 日間に制限 |
| symmetricKeyAddition  | アプリケーションの symmetric Key を制限 | 2019/01/01 以降に作成されたアプリケーションの新しい symmetric Key キーをブロック                       |
| symmetricKeyLifetime  | symmetric Key の最大有効期間範囲を適用  | 2019/01/01 以降に作成されたアプリケーションでは、すべての新しい symmetric Key を最大 30 日間に制限            |
| asymmetricKeyLifetime | 非対称キー（証明書）の最大有効期間範囲を適用      | 2019/01/01 以降に作成されたアプリケーションでは、すべての新しい非対称キー（証明書）を最大 30 日間に制限                 |

#### ポイント

- テナント単位での強制か、アプリ単位の強制で tenantAppManagementPolicy または appManagementPolicy を使い分ける
- 現時点で、UI でもポリシー設定画面は未提供

## Azure AD 認証方法 API の概要 (プレビュー)

[Azure AD 認証方法 API の概要 - Microsoft Graph beta](#) | [Microsoft Docs](#)

# Azure AD TLS バージョン 1.0 および 1.1 廃止の追加アナウンス

## アナウンス

### Identity and Security

- Azure AD では、TLS 1.0、1.1、3DES暗号スイートの廃止における追加アナウンスを公開しました。2022 年 1 月 31 日から、Azure AD は廃止予定の TLS バージョンをサポートしなくなります。TLS 1.2 に移行していないお客様は、Azure AD へのリクエストが失敗するため、影響を受ける予定となります。Azure AD のサインイン ログを使用して、「Legacy TLS (TLS 1.0, 1.1, 3DES)」の項目が存在しないかをご確認ください。

Activity Details: Sign-ins

Location Device info Authentication Details Conditional Access Report-only Additional Details

Legacy TLS (TLS 1.0, 1.1, 3DES) True

Root Key Type Unknown

Oauth Scope Info ["email"]

廃止予定の TLS でサインインした場合に該当項目が出力

Sign-in logs

Download Export Data Settings

Want to switch back to the default sign-ins exp

Date: Last 24 hours Show dates as: Lo

User sign-ins (interactive) User sign-ins (n

Date Request ID

10/31/2021, 12:21:37... 5f8dc62a-6002-42f0...

10/31/2021, 12:21:35... a9d20b01-0dea-4d0...

#### ポイント

- 確認方法として、以下を提供  
PowerShell、UX、JSON、Azure モニター
- 「Legacy TLS」の項目はレガシーな TLS サインイン時のみ記録
- CSV では「Legacy TLS」の項目は未出力

- TLS 1.2 へ移行して基盤環境のセキュリティ確保を  
<https://jpazureid.github.io/blog/azure-active-directory/act-fast-by-moving-to-tls-1-2/>

# Azure Machine Learning Auto ML のテストデータ指定が プレビュー

プレビュー

Data Platform

Auto ML のモデル評価にテストデータを与え、モデルをテストする機能がプレビューになりました。

## 今回の更新のポイント

- テストデータを利用したモデル評価により、偏ったモデル評価が 推奨モデルに適用されることを防ぎます。
- テストデータセットを指定することも、トレーニングデータの一部をテストデータとして指定することも可能です。

## 注意事項

- 以下のシナリオでは利用できません。
  - Computer Vision タスク (プレビュー)
  - 多数モデルおよび階層型時系列予測トレーニング (プレビュー)
  - ディープ ラーニング ニューラル ネットワーク (DNN) が 有効になっている予測タスク
  - ローカル コンピューティングまたは Azure Databricks クラスターからの自動 ML 実行



- **Public preview: Azure Machine Learning updates - November 2021**  
<https://azure.microsoft.com/ja-jp/updates/public-preview-azure-machine-learning-updates-november-2021/>
- **Test AutoML models and calculate test metrics**  
<https://aka.ms/automl-test-dataset>

# Synapse Analytics Synapse Spark Pool のオートスケールが GA

一般公開

Data Platform

Synapse Spark Pool の自動スケーリング機能により、クラスター インスタンス内のノード数を自動的に増減できるようになりました。

## 今回の更新のポイント

- ノードの最小数と最大数を指定して自動スケーリングを構成できます。
- 保留中の全ジョブを実行するために必要な CPU コアと メモリの合計を監視し、スケーリング条件を判定します。

## 注意事項

- ノードの最小数を 3 より小さくすることはできません。
- スケーリング操作が完了するまでに、1 分から 5 分 かかる場合があります。

### 新しい Apache Spark プール

基本 • 追加設定 \* タグ 確認および作成

希望する構成で Synapse Analytics Apache Spark プールを作成します。[基本] タブをすべて入力し、[確認と作成] に移動して、スマートな既定値でプロビジョニングするか、各タブに移動してカスタマイズします。

#### Apache Spark プールの詳細

Apache Spark プールに名前を指定し、初期設定を選択します。

Apache Spark プール名 \* demosparkpool

ノード サイズ ファミリー \* メモリ最適化済み

ノード サイズ \* Small (4 仮想コア/32 GB)

自動スケーリング \* ☒ 有効 ☐ 無効

ノード数 \* 3  30

推定価格 ☐ 1 時間あたりの推定コスト  
207.73 から 2077.29 JPY  
[価格の詳細を表示する](#)

エグゼキューターを動的に割り当てる \* ☐ 有効 ☒ 無効

- Dynamic allocation for Apache Spark in Azure Synapse now generally available  
<https://azure.microsoft.com/ja-jp/updates/dynamic-allocation-for-apache-spark-in-azure-synapse-now-generally-available/>



# Azure Data Explorer, Azure Data Factory, Synapse Analytics

## Azure Data Explorer のコネクタが GA

一般公開

Data Platform

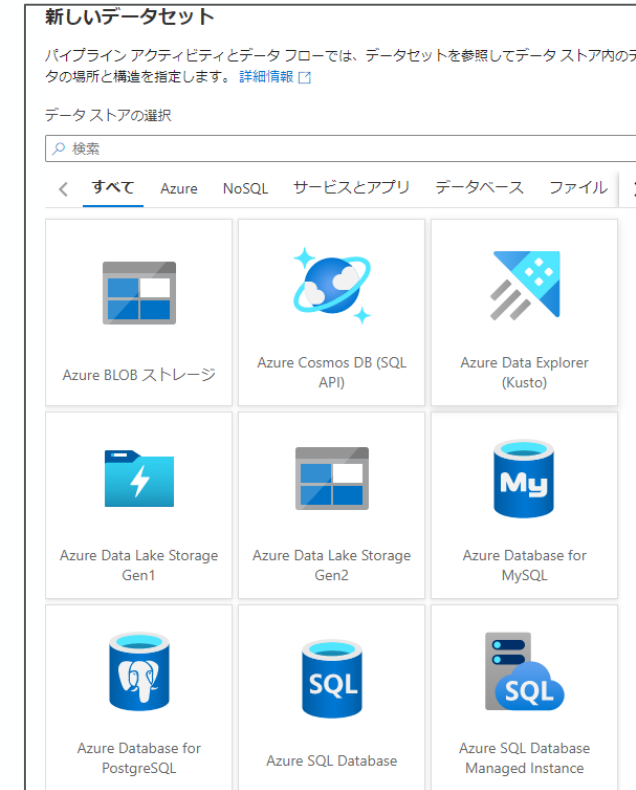
Azure Data Factory, Synapse Pipeline の マッピングデータフロー で Azure Data Explorer のコネクタが利用可能になります。

### 今回の更新のポイント

- ソース/シンク データに Azure Data Explorer を指定して、データ処理を GUI で開発できます。
- Azure Data Explorer 内の大規模データに対し、環境設定なしに Spark 処理を実現できます。

### 注意事項

- セルフホステッド統合ランタイムを使用して、Azure Data Explorer との間でオンプレミス データ ストアから双方向にデータをコピーすることは、バージョン 3.14 以降からサポートされています。



- General availability: Copy data to/from Azure Data Explorer using Azure Data Factory or Synapse Analytics  
<https://azure.microsoft.com/ja-jp/updates/copy-data-tofrom-azure-data-explorer-using-azure-data-factory-or-synapse-analytics/>



# Azure Database for PostgreSQL - Flexible Server

## Azure Database for PostgreSQL フレキシブルサーバーが GA

一般公開

Data Platform

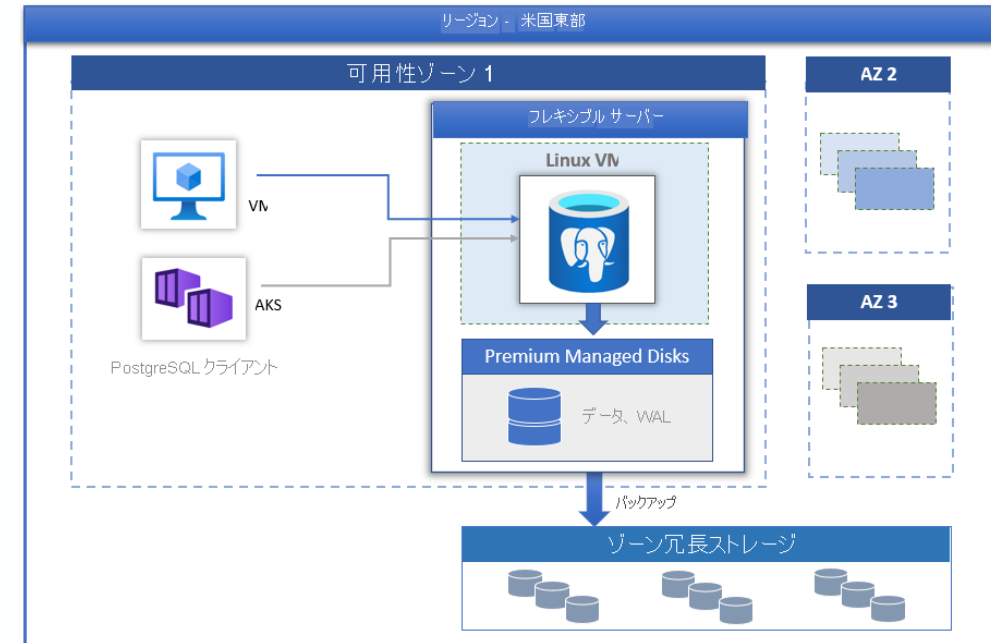
Azure Database for PostgreSQL フレキシブルサーバーが 一般公開されました。

### 今回の更新のポイント

- データベース管理機能と構成設定のよりきめ細かな 制御と柔軟性を実現できます。
- ゾーン冗長などシングルサーバーにない高可用性機能も利用可能です。

### 注意事項

- シングルサーバー と対応している PostgreSQL のバージョンが異なります。



- **Azure Database for PostgreSQL - Flexible Server now generally available**  
<https://azure.microsoft.com/ja-jp/updates/azure-database-for-postgresql-flexible-server-now-generally-available/>
- **シングルサーバーとフレキシブルサーバーの比較**  
<https://docs.microsoft.com/ja-jp/azure/postgresql/flexible-server/concepts-compare-single-server-flexible-server>

# SQL Server on IaaS (Windows / Linux) IaaS Agent 拡張機能の GA 機能のご紹介

一般公開

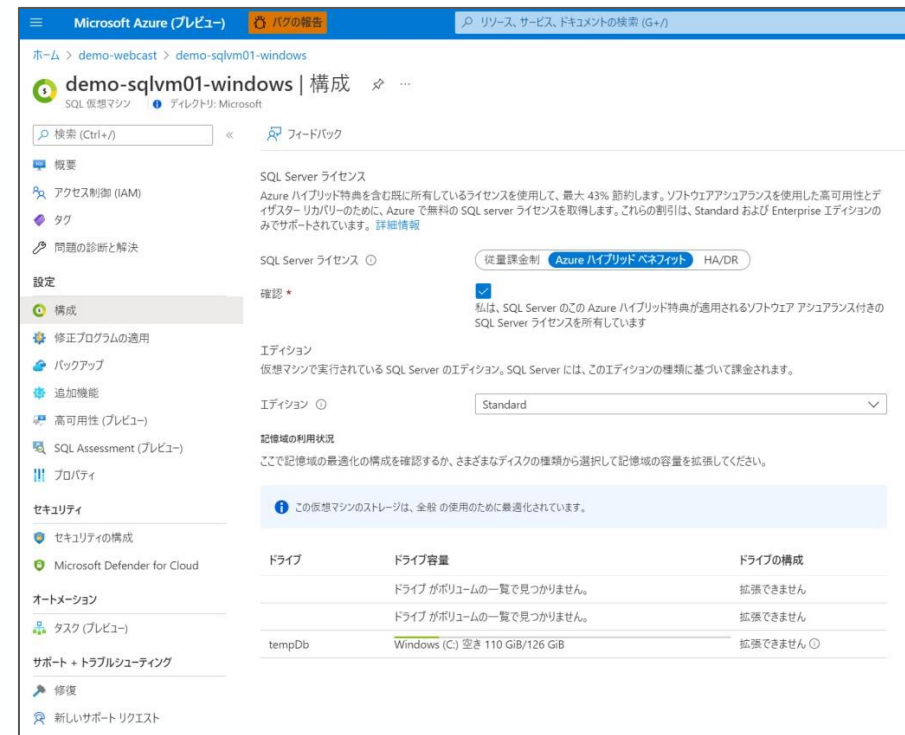
Data Platform

## 今回の更新のポイント

- Windows VM でフル モードの IaaS Agent 拡張機能が SQL Server サービスの再起動なしで導入可能になります。
- Linux VM の IaaS Agent 拡張機能が利用可能になります。

## 注意事項

- Linux VM のサポート対象 OS には制限があります。(Ubuntu Linux のみ等)
- 複数のインスタンスはサポートされていません。



- IaaS Agent extension full mode no restart for SQL VMs generally available  
<https://azure.microsoft.com/ja-jp/updates/iaas-agent-extension-full-mode-no-restart-for-sql-vms-generally-available/>
- SQL Server IaaS Agent extension for Linux SQL VMs generally available  
<https://azure.microsoft.com/ja-jp/updates/sql-server-iaas-agent-extension-for-linux-sql-vms-generally-available/>



# Contact Us

お問い合わせ先：

東京エレクトロデバイス株式会社  
クラウドIoTカンパニー  
エッジクラウドソリューション部

URL: <https://cptechweb.teldevice.co.jp/>



東京エレクトロン デバイス株式会社

---