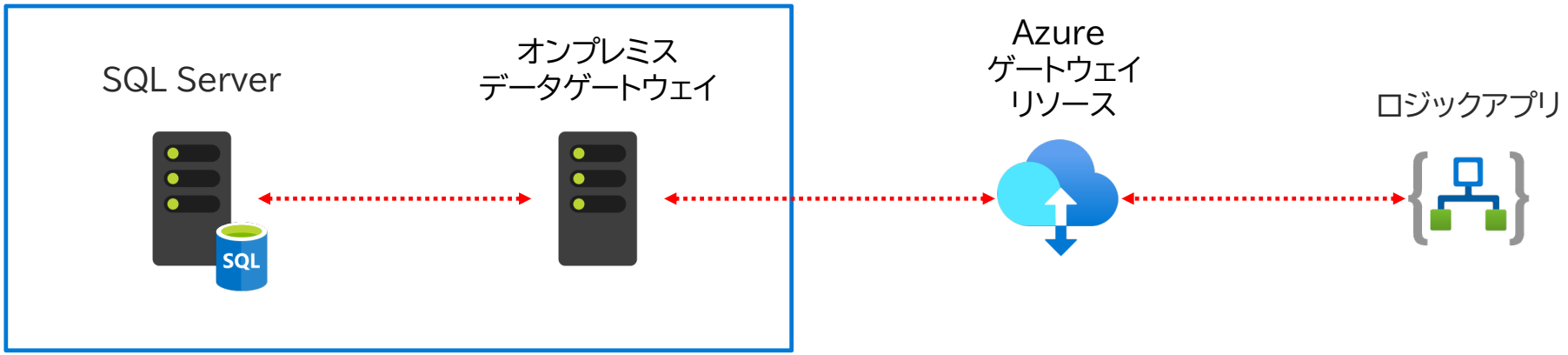
補助資料

AZ-305 : Microsoft Azure Infrastructure Solutions の設計

2022 年 7 月 1.0.0

Azure Logic Apps とオンプレミスの連携

- VPN やインターネットからのアクセス不要のまま、ロジックアプリから SQL Server、SharePoint Server、Oracle DB、ファイル共有などのオンプレミス システムにアクセス可能
- オンプレミスデータゲートウェイと Azure ゲートウェイリソースが必要



BLOB の種類

- BLOB の作成時に指定し、途中で変更不可

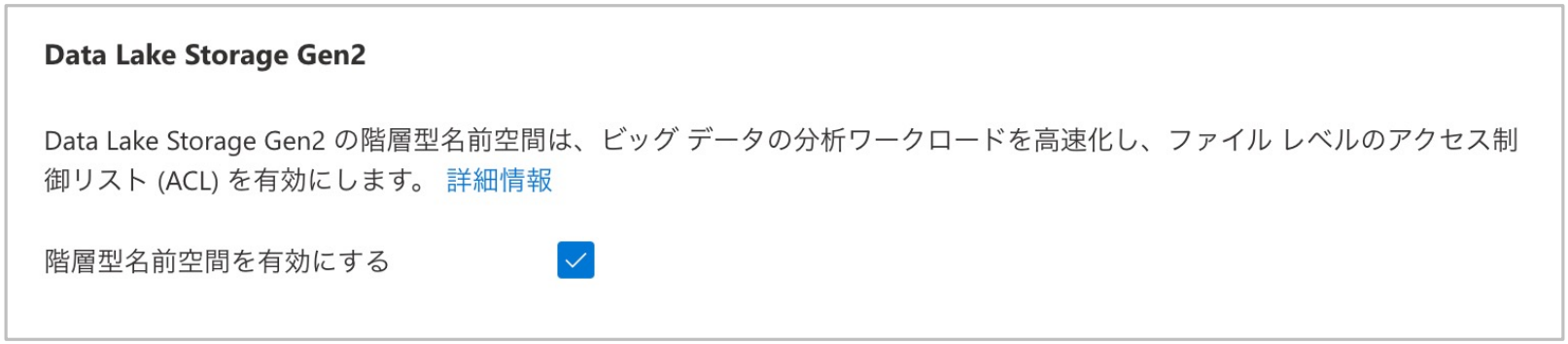
	ブロック BLOB	ページ BLOB	追加 BLOB
特徴	大量のデータの効率的なアクセス	ランダムな読み取りと書き込み	追加操作
最大サイズ	190.7 TB	8 TB	195 GB
主な用途	• 画像 • ドキュメント • ビデオ • オーディオ	• 仮想マシン ディスク • バックアップデータ	• ログ • 監査データ

ストレージアカウントの種類と冗長性

種類	LRS	ZRS	GRS	GZRS
Standard 汎用 v2	○	○	○	○
Premium ブロック BLOB	○	○		
Premium ページ BLOB	○			
Premium ファイル共有	○	○		

BLOB の NFS 3.0 プロトコルによるマウント

- Standard 汎用 v2 または Premium ブロック BLOB で利用可能
- [階層型名前空間を有効にする]をチェック

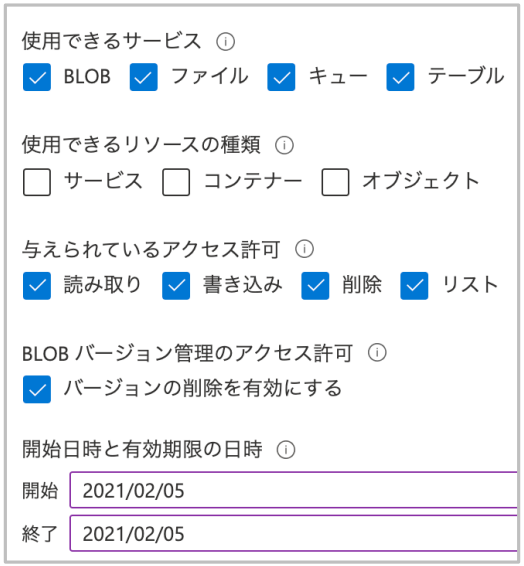


BLOB のアクセス制御

アクセスキー

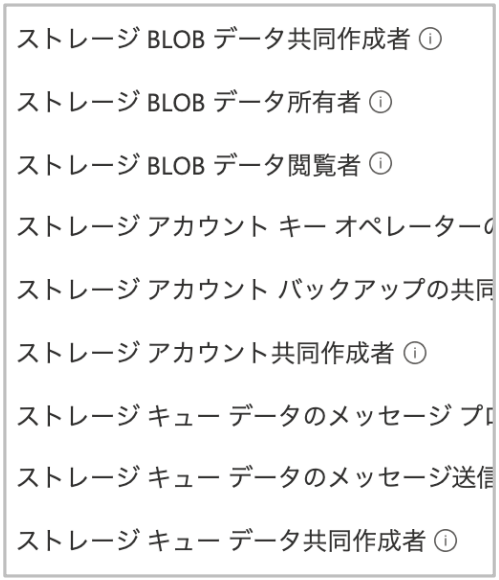
- 完全なアクセス権

Shared Access Signature(SAS)



- 詳細なアクセス権
- 有効期限の設定

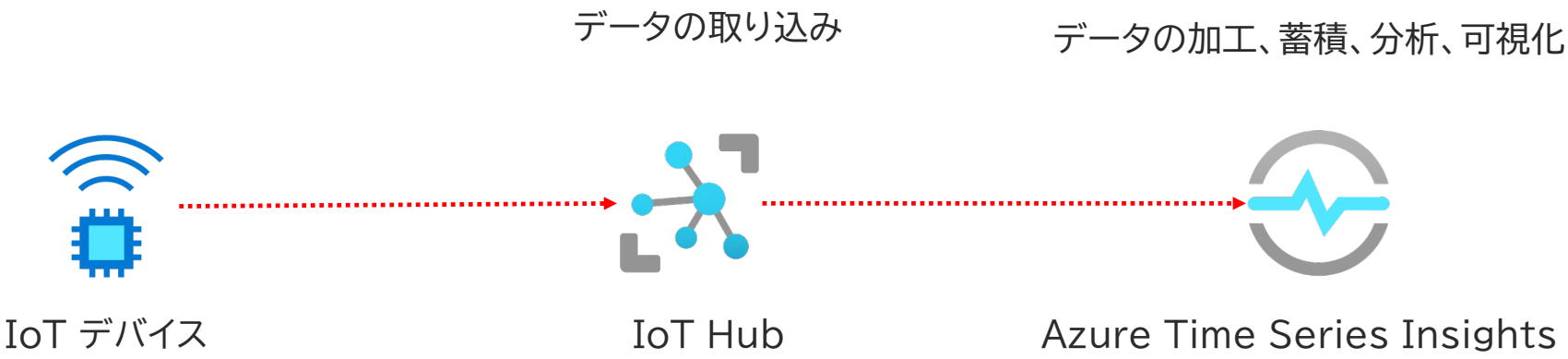
IAM



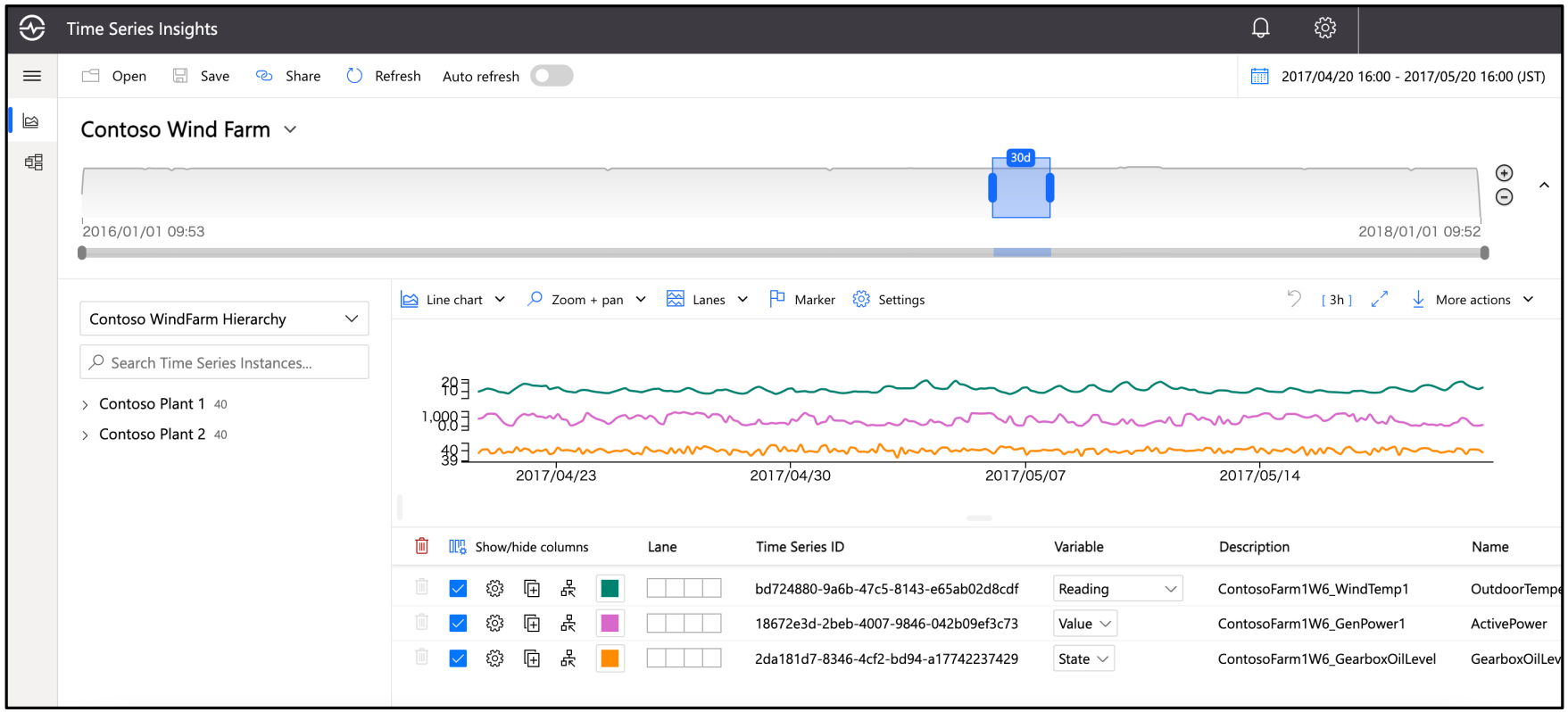
- Azure AD アカウントの使用

Azure Time Series Insights による IoT シナリオ

- IoT データをリアルタイムに可視化

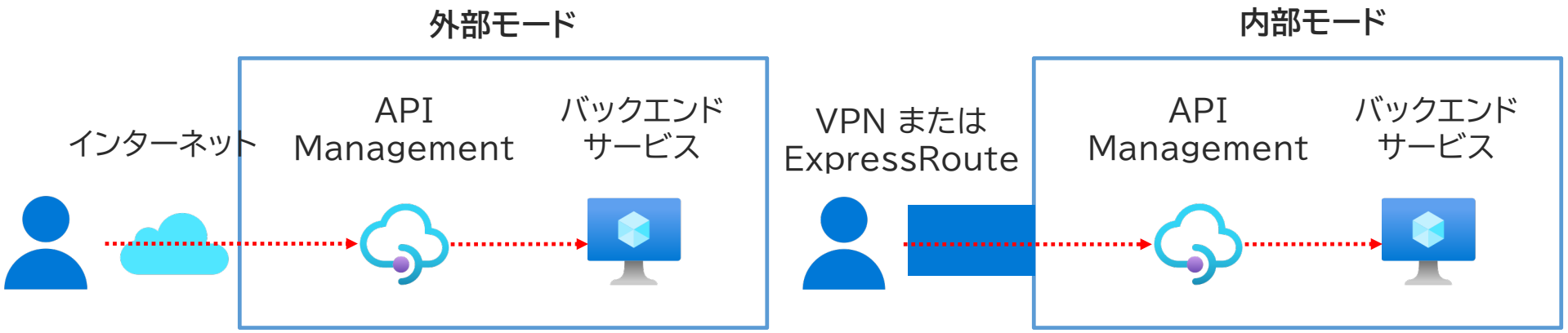


(画面)Azure Time Series Insights



Azure API Management での仮想ネットワークの使用

- Developer プラン または Premium プランでは仮想ネットワークへの配置をサポート



- バックエンドは仮想ネットワークに配置
- インターネットからアクセス可能(VPN 不要)

- バックエンドは仮想ネットワークに配置
- インターネットからアクセス不可
  (仮想ネットワークまたは VPN 経由でアクセス)

Azure AD Privileged Identity Management(PIM)

- 特権アクセスを制限するサービス
- Azure AD Premium P2 または Microsoft 365 E5 プランで使用可能

継続的な特権アクセスの制限

- 最小権限を必要な時間だけ割り当て（Just-in-Time アクセス）
- 承認要求ワークフローを構成可能

特権ロールをもつユーザーの検出

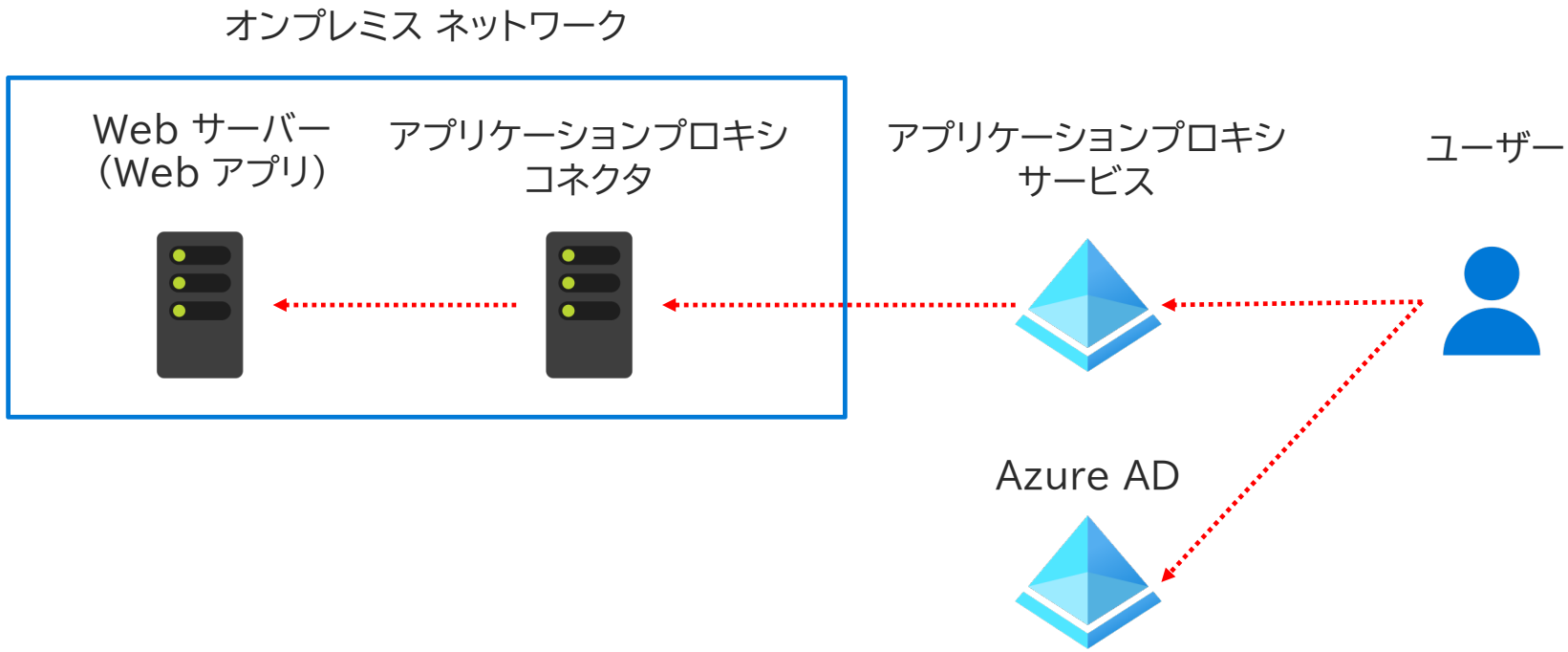
- 永続的な特権ロールを割り当てられているユーザーを容易に検出

アクセスレビュー

- 特権ロールごとのユーザーのアクティビティを確認

Azure AD アプリケーションプロキシ

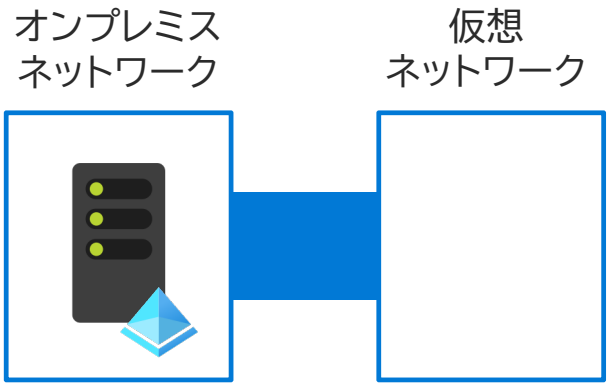
- オンプレミスの Web アプリのリモートアクセスを簡単に実現
- エンタープライズアプリケーションとして Web アプリを発行



AD DS ドメインコントローラーのクラウド配置

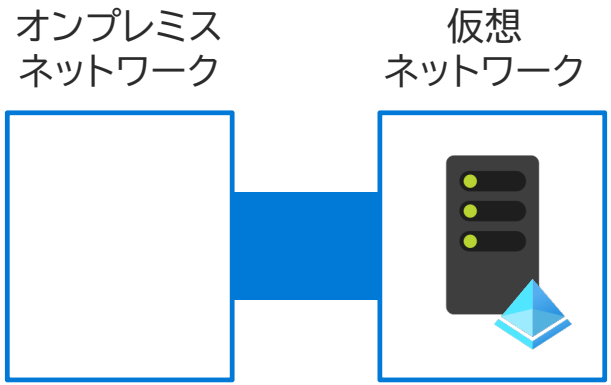
- オンプレミスネットワークと仮想ネットワークの接続後、AD DS ドメインコントローラーはどちらのネットワークに配置しても利用可能

オンプレミスのみ



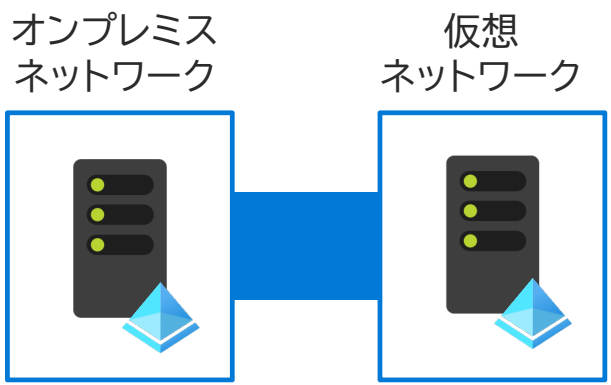
- 追加のドメインコントローラーが不要
- リンク障害時、仮想ネットワーク側からの認証は失敗

仮想ネットワークのみ



- オンプレミス側のリソース管理が不要
- リンク障害時、オンプレミスネットワーク側からの認証は失敗

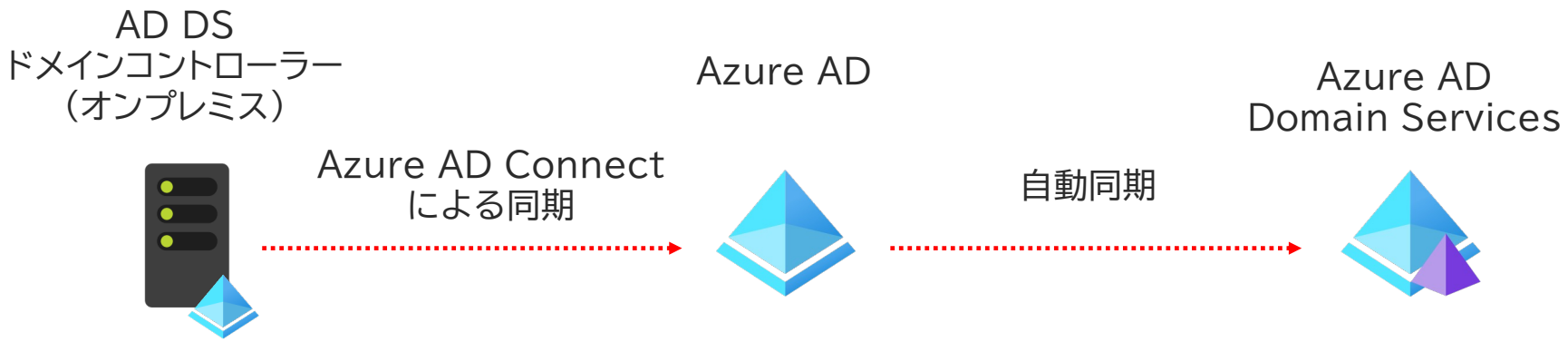
オンプレミスネットワークと仮想ネットワークの両方



- リンク障害時でも、両ネットワークからの認証は影響を受けない

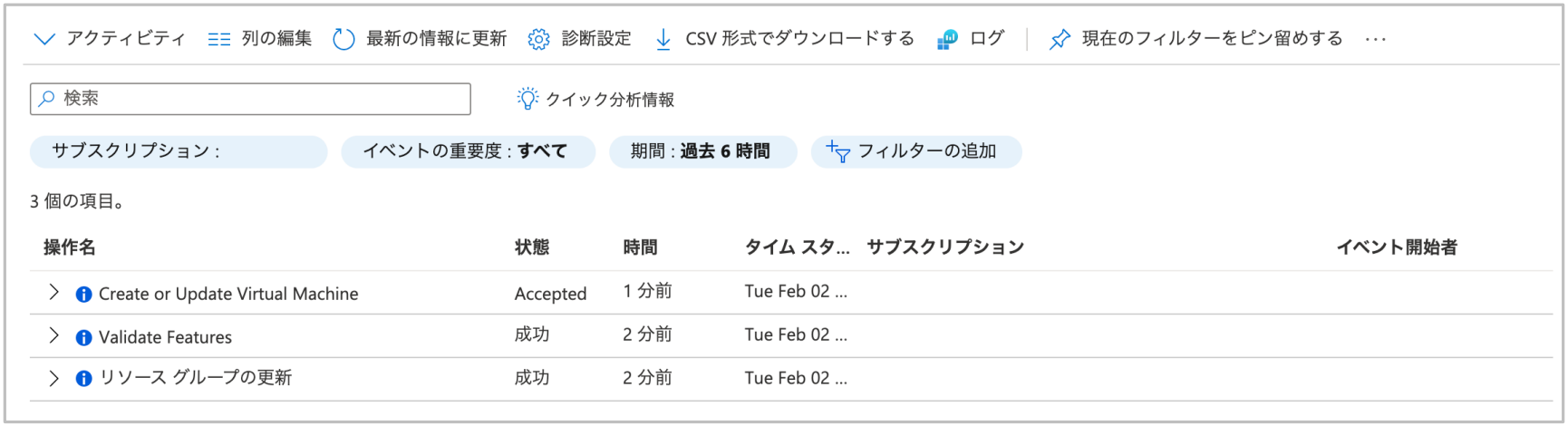
Azure Active Directory Domain Services

- マネージド型の AD DS ドメインコントローラー
- Azure からオンプレへのアクセスは不要



Azure アクテビティログ

- サブスクリプションレベルのイベントの収集
- CSV ファイルをダウンロードして、月次レポート を作成可能



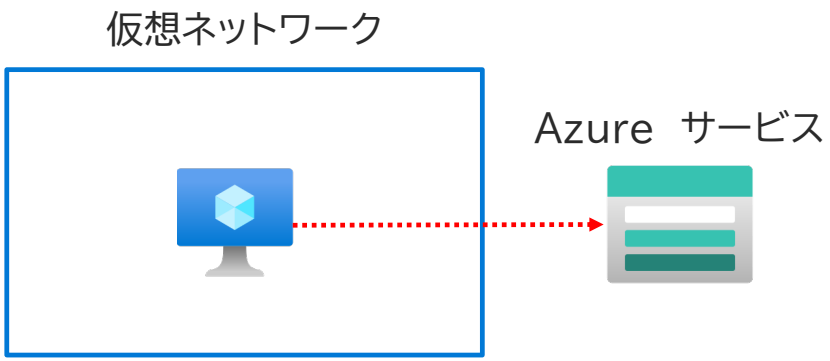
Azure Monitor ログテーブル

種類	説明	テーブル名
Windows イベントログ	システムログやアプリケーションログなどの Windows のイベントログを収集する	Event
Syslog	Linux の Syslog データを収集する	Syslog
パフォーマンスカウンター	Windows または Linux のパフォーマンスデータを収集する	Perf
IIS ログ	Windows の Internet Information Service(IIS) のログを収集する	W3CIISLog
カスタムログ	Windows または Linux の任意のテキストログを収集する	<カスタムログ名>_CL

仮想ネットワークサービスエンドポイント

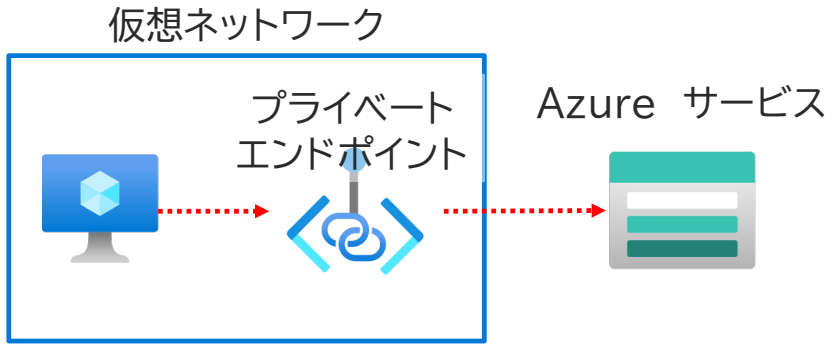
- 仮想ネットワークから Azure サービスへ直接アクセス

サービスエンドポイント



- ルートテーブルによるアクセス
- シンプル
- 無料

プライベートエンドポイント



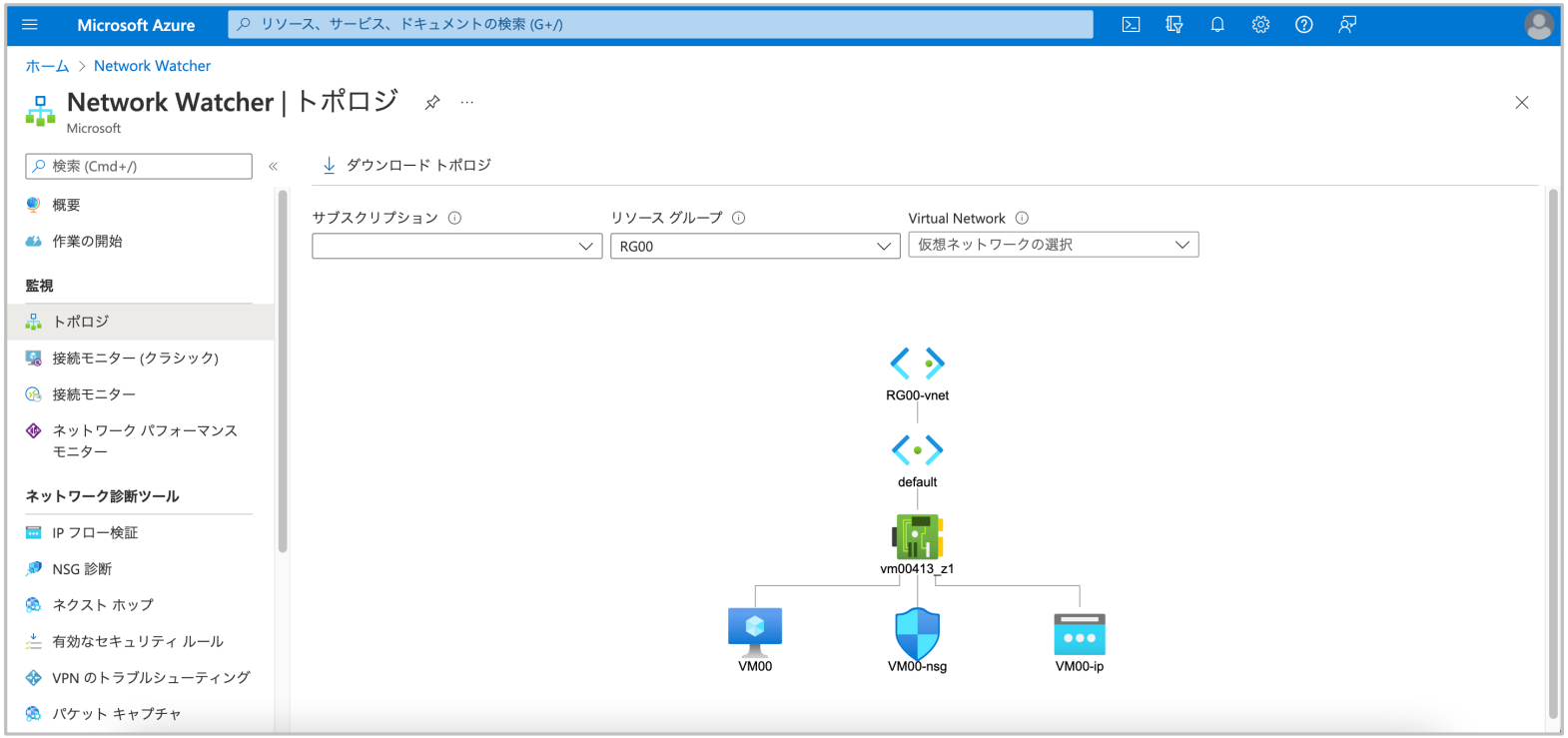
- ネットワークインタフェースによるアクセス
- 特定のリソースのみにアクセスを制限
- オンプレミスからのアクセスに対応

Azure Firewall Manager

- Azure Firewall ポリシーによる Azure Firewall と Azure Virtual WAN の一元管理
- Azure Firewall ポリシーは親子で構成可能
- 親ポリシーは子ポリシーと同じリージョンにあることが必要

Network Watcher

- ネットワークの診断とパフォーマンスの監視

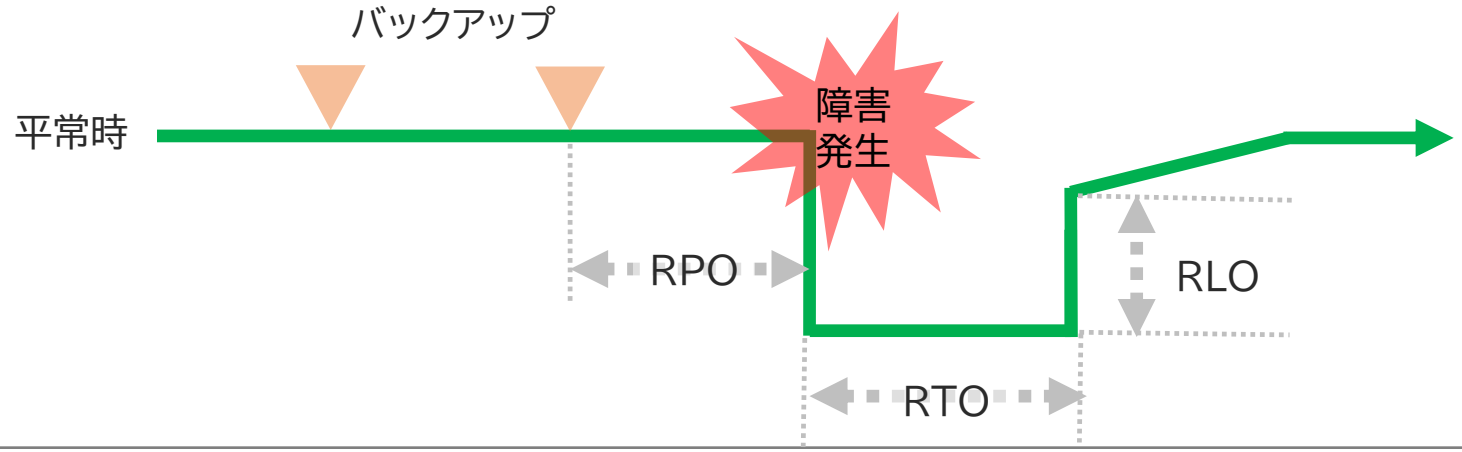


Network Watcher の機能

機能	説明
トポロジ	仮想ネットワーク内のすべてのリソースとその関係を表示する
接続モニター	仮想マシン間の通信を監視する
ネットワーク パフォーマンスモニター	ネットワーク インフラストラクチャ内のさまざまなポイント間のネットワーク パフォーマンスを監視する
NSG 診断	ソースとターゲットに対応した NSG とルール、最終的な許可または拒否を検証すかる
IP フロー検証	仮想マシンから送受信されるパケットの許可または拒否の状況を検証する
ネクストホップ	トラフィックが目的の宛先に転送されているかどうか、またはトラフィックがどこにも送信されていないかどうかを検証する
有効なセキュリティ ルール	ネットワーク セキュリティ グループを監査および診断して、トラフィックが正しく許可または拒否されていることを検証する
VPN のトラブルシューティング	ゲートウェイの正常性を診断する
パケット キャプチャ	仮想マシンとの間で送受信されるトラフィックを追跡するため、パケットをキャプチャする
接続のトラブルシューティング	接続の正常性を診断する
トラフィック分析	ユーザーとアプリケーションのアクティビティを可視化する

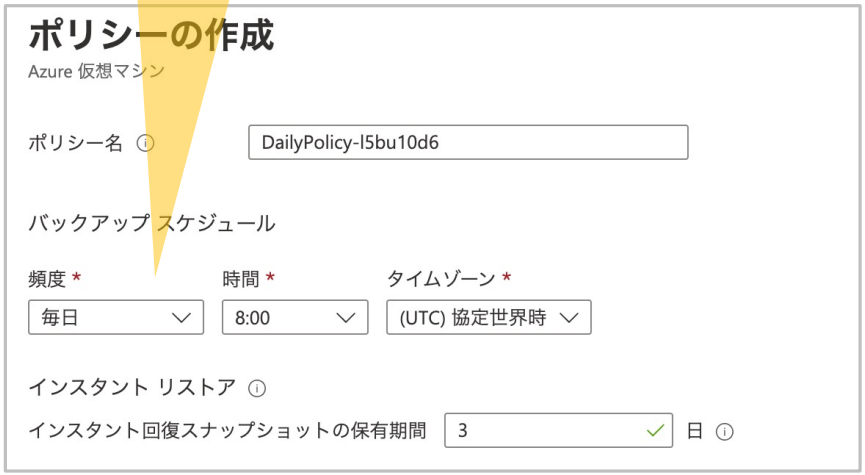
RTO、RLO、RPO

- 目標復旧時間(RTO：Recovery Time Objective)
  - 復旧にかかる時間はどれくらいか？
- 目標復旧レベル(RLO：Recovert Level Objective)
  - 復旧はどのレベルまでできるか？
- 目標復旧ポイント(RPO：Recovery Point Objective)
  - 復旧はどの時点までできるか？



（画面）仮想マシンのバックアップポリシー

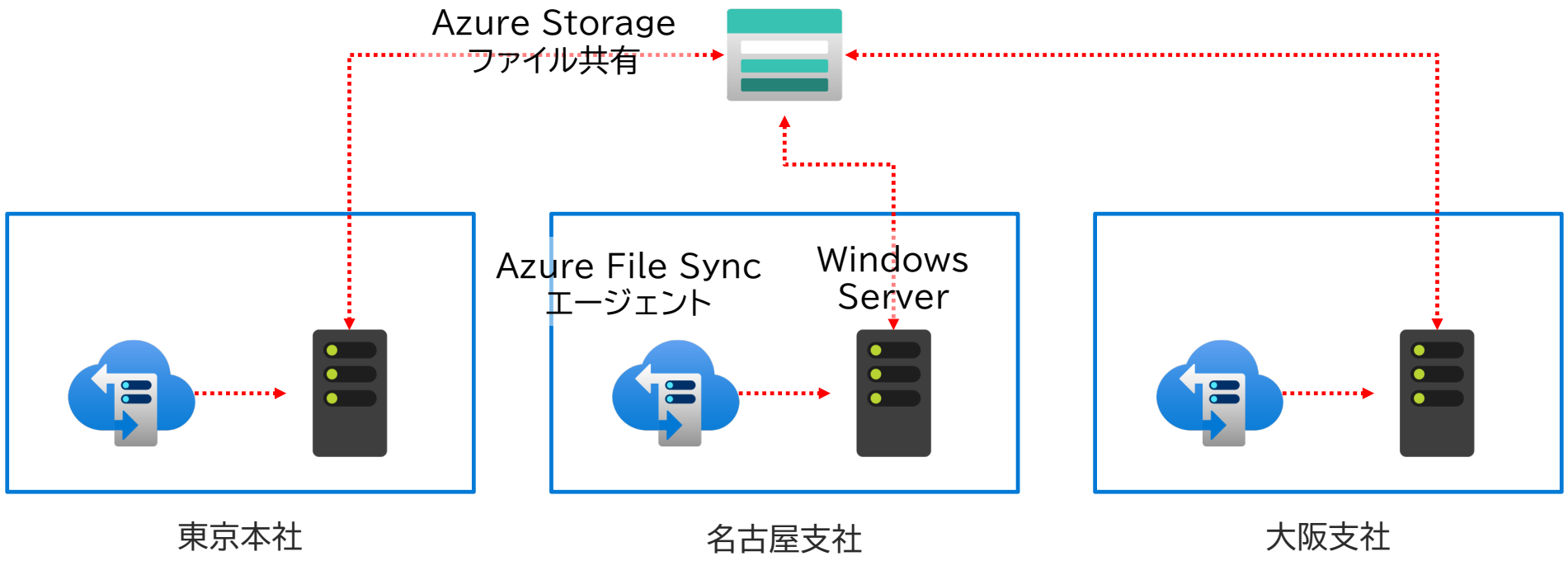
仮想マシンの
RPO は 24 時間



仮想マシンの
回復可能期間は
36ヶ月

オンプレミス ファイルサーバーの可用性の向上

- Azure File Sync による Azure Storage ファイル共有とオンプレミス Windows Server の同期



ビジネス継続性ソリューションの比較

	可用性セット	可用性ゾーン	Azure Backup	Azure Site Recovery
保護範囲	データセンター内	データセンター（地域）	リージョン	リージョン
RTO	小	小	大	中
RPO	小	小	大	中
自動復旧	あり	あり	なし	なし
コスト	高	高	低	低

Azure CycleCloud による HPC シナリオ

- HPC クラスターの簡単な作成と管理