記事
Toshihiko Minamoto · 2020年7月6日 24m read

Microsoft Azure Resource Manager(ARM)向けInterSystemsサンプルリファレンスアーキテクチャ

この記事では、InterSystems Technologiesに基づく、堅牢なパフォーマンスと可用性の高いアプリケーションを提供するリファレンスアーキテクチャをサンプルとして提供します。Caché、Ensemble、HealthShare、TrakCare、およびDeepSee、iKnow、Zen、Zen Mojoといった関連する組み込みテクノロジーに適用可能です。

Azureには、リソースを作成して操作するための、Azure ClassicとAzure Resource Managerという2つのデプロイメントモデルがあります。この記事で説明する情報は、Azure Resource Managerモデル(ARM)に基づきます。

要約

Microsoft Azureクラウドプラットフォームは、InterSystems製品すべてを完全にサポートできるクラウドサービスとして、IaaS(サービスとしてのインフラストラクチャ)向けの機能の豊富な環境を提供しています。あらゆるプラットフォームやデプロイメントモデルと同様に、パフォーマンス、可用性と運用、管理手順などの環境に関わるすべての側面が正しく機能するように 注 意を払う必要があります。この記事では、こういった分野の詳細について説明しています。

パフォーマンス

Azure ARMには、計算仮想マシン(VM)と関連するストレージオプションに使用できるさまざまなオプションがありますが、InterSystems製品に最も直接関連するのは、AzureページBLOBストレージにVHDファイルとして保管されたネットワーク接続IaaSディスクです。ほかにも Blob(ブロック)やFileなどのオプションがいくつかありますが、それらはCachéの操作をサポートするのではなく、個別のアプリケーションの要件に特化したオプションです。ディスクが作成されるストレージには、PremiumとStandardの2種類があります。Premiumストレージは、確実に予測可能な低レイテンシの入出力操作毎秒(IOPS)とスループットが必要な本番ワークロードに適しています。Standardストレージはより経済的なオプションで、本番以外またはアーカイブタイプのワークロードに適しています。すべてのVMタイプがPremiumストレージにアクセスできるわけではないため、特定のVMタイプを選択する際には 注 意が必要です。

仮想IPアドレスと自動フェイルオーバー

ほとんどのIaaSクラウドプロバイダーには、データベースフェイルオーバー設計で一般的に使用される仮想IP(VIP)アドレスに対応できる能力が欠けていました。これを解決するために、最も一般的に使用されるいくつかの接続方法(特にECPクライアントやCSPゲートウェイ)は、ミラー対応にするVIP機能に依存しないようにCaché内で強化されています。

xDBC、ダイレクトTCP/IPソケット、またはその他のダイレクトネットプロトコルなどの接続方法にはVIPを使用する必要があります。これらに対処するために、InterSystemsのデータベースミラーテクノロジーは、Azure内部ロードバランサー(ILB)とやり取りしてVIPのような機能を実現するAPIを使うことで、Azure内でこれらの接続方法に対して自動フェイルオーバーを提供できるようにしており、したがって、Azure内に完全で堅牢な高可用性計を提供しています。これに関する詳細は、コミュニティ記事「Database Mirroring without a Virtual IP address(仮想IPアドレスを使用しないデータベースミラーリング)」で説明されています。

バックアップ操作

ｸﾗｳﾄﾞ型ﾃﾞﾌﾟﾛｲﾒﾝﾄでは、従来のﾌｧｲﾙﾚﾍﾞﾙのﾊﾞｯｸｱｯﾌﾟまたはｽﾅｯﾌﾟｼｮｯﾄによるﾊﾞｯｸｱｯﾌﾟのいずれかによるﾊﾞｯｸｱｯﾌﾟは困難な場合があります。これは、Azure BackupおよびAutomation Run Booksを、InterSystems External Freeze and Thaw API機能ｾｯﾄに使って達成するようになりました。これにより、実質的な24時間365日の運用ｸﾗｽﾀｰな定期ﾊﾞｯｸｱｯﾌﾟの確実現できます。または、市場に出回っているさまざまのｻｰﾄﾞﾊﾟｰﾃｨ製ﾊﾞｯｸｱｯﾌﾟﾂｰﾙを使用する場合は、VMそのものにﾊﾞｯｸｱｯﾌﾟｴｰｼﾞｪﾝﾄを展開し、論理ﾎﾞﾘｭｰﾑﾏﾈｰｼﾞｬ（LVM）のｽﾅｯﾌﾟｼｮｯﾄと組み合わせてﾌｧｲﾙﾚﾍﾞﾙのﾊﾞｯｸｱｯﾌﾟを活用することができます。

ｻﾝﾌﾟﾙｱｰｷﾃｸﾁｬ

この記事では、ｱﾌﾟﾘｹｰｼｮﾝ固有のﾃﾞﾌﾟﾛｲﾒﾝﾄの開始点として、ｻﾝﾌﾟﾙのAzureｱｰｷﾃｸﾁｬを提供しています。可能性あるさまざまなﾃﾞﾌﾟﾛｲﾒﾝﾄのｶﾞｲﾄﾞﾗｲﾝとしてご利用ください。
このﾘﾌｧﾚﾝｽｱｰｷﾃｸﾁｬでは、高可用性を実現するﾃﾞｰﾀﾍﾞｰｽﾐﾗｰﾒﾝﾊﾞｰ、InterSystems Enterprise Cache Protocol（ECP）を使ったｱﾌﾟﾘｹｰｼｮﾝｻｰﾊﾞｰ、InterSystems CSP Gatewayを使ったWebｻｰﾊﾞｰ、内部および外部のAzureﾛｰﾄﾞﾊﾞﾗﾝｻｰを含んだ、非常に堅牢なCachéﾃﾞｰﾀﾍﾞｰｽﾃﾞﾌﾟﾛｲﾒﾝﾄを紹介しています。

Azureｱｰｷﾃｸﾁｬ

Microsoft AzureにCachéﾍﾞｰｽのｱﾌﾟﾘｹｰｼｮﾝを展開する場合、ある分野に特有の考慮事項があります。このｾｸｼｮﾝでは、ｱﾌﾟﾘｹｰｼｮﾝに必要な通常の機能要件のほかに考慮する必要のある分野について説明します。

この記事には、InterSystems TrakCare統合医療情報ｼｽﾃﾑとInterSystems HealthShare医療情報ﾌﾟﾗｯﾄﾌｫｰﾑのﾃﾞﾌﾟﾛｲﾒﾝﾄに基づく2つの例が提供されています。後者には、Information Exchange、Patient Index、Health Insight、Personal Community、Health Connectが含まれています。

仮想ﾏｼﾝ

Azure仮想ﾏｼﾝ（VM）には、BasicとStandardの2つのﾚﾍﾞﾙがあります。
どちらのﾀｲﾌﾟでもｻｲｽﾞを選択できますが、Basicﾚﾍﾞﾙには、負荷分散や自動ｽｹｰﾘﾝｸﾞといったStandardﾚﾍﾞﾙに提供される機能がいくつか含まれていません。
このため、TrakCareのﾃﾞﾌﾟﾛｲにはStandardﾚﾍﾞﾙを使用しています。

Standardﾚﾍﾞﾙのﾏｼﾝには、ｼﾘｰｽﾞごとにさまざまなｻｲｽﾞが用意されています。
A、D、DS、F、FS、G、GSというｼﾘｰｽﾞです。DS、GS、および新しいFSのｻｲｽﾞでは、Azure Premium Storageの使用がｻﾎﾟｰﾄされています。

通常、本番ｻｰﾊﾞｰには、信頼性低ﾚｲﾃﾝｼ、高ﾊﾟﾌｫｰﾏﾝｽを得られるPremium Storageを使用する必要があります。このため、このﾄﾞｷｭﾒﾝﾄで説明するTrakCareとHealthShareのｻﾝﾌﾟﾙﾃﾞﾌﾟﾛｲﾒﾝﾄｱｰｷﾃｸﾁｬでは、FS、DS、またはGSｼﾘｰｽﾞのﾏｼﾝを使用します。
提供される仮想ﾏｼﾝのｻｲｽﾞは、地域によって異なることにご 注 意ください。

仮想ﾏｼﾝのｻｲｽﾞの詳細は、以下を参照してください。

- Windows仮想ﾏｼﾝのｻｲｽﾞ
- Linux仮想ﾏｼﾝのｻｲｽﾞ

ｽﾄﾚｰｼﾞ

TrakCareおよびHealthShareｻｰﾊﾞｰには、Azure Premium Storageが必要です。Premium Storageは、ﾃﾞｰﾀをｿﾘｯﾄﾞｽﾃｰﾄﾄﾞﾗｲﾌﾞ（SSD）に格納して低ﾚｲﾃﾝｼで高いｽﾙｰﾌﾟｯﾄを提供しますが、Standard Storageはﾊｰﾄﾞﾃﾞｨｽｸﾄﾞﾗｲﾌﾞ（HDD）に格納するため、ﾊﾟﾌｫｰﾏﾝｽﾚﾍﾞﾙが低下します。

Azure Storageは冗長で可用性高いｼｽﾃﾑですが、現在、可用性ｾｯﾄはｽﾄﾚｰｼﾞ障害ﾄﾞﾒｲﾝ全体の冗長性を提供しておらず、これによってまれに問題が起こることがあることに 注 意しておくことが重要です。ﾏｲｸ

ロソフトは緩和策を備えており、このプロセスを広く利用できるようにするほか、エンドユーザーが簡単に使用できるように取り組んでいます。
お近くのマイクロソフトチームに直接協力し、緩和策が必要かどうかを判断することをお勧めします。

Premium Storageアカウントに対してディスクがプロビジョニングされる場合、IOPSとスループット（帯域幅）はディスクのサイズによって異なります。現在、Premium Storageディスクには、P10、P20 、P30 の3タイプがあります。各タイプのIOPSとスループットには、次の表に示すように特定の制限があります。

Premiumディスクタイプ	P4	P6	P10	P15	P20	P30	P40	P50
ディスクサイズ	32 GB	64 GB	128 GB	256 GB	512 GB	1024 GB	2048 GB	4096 GB
ディスクあたりのIOPS	120	240	500	1100	2300	5000	7500	7500
ディスクあたりのスループット	25 MB/秒	50 MB/秒	100 MB/秒	125 MB/秒	150 MB/秒	200 MB/秒	250 MB/秒	250 MB/秒

注意: 特定のVMにディスクトラフィックを駆動するのに十分な帯域幅があることを確認してください。
たとえば、STANDARD_DS13 VMには、すべてのPremium Storageディスクトラフィックに使用できる毎秒256 MBの専用帯域幅があります。つまり、このVMに4つのP30 Premium Storageディスクが接続されている場合、スループットの制限は毎秒256 MBであり、4つのP30ディスクが理論的に提供される毎秒800 MBではありません。

Premium Storageディスクの詳細、プロビジョニング済みの容量、パフォーマンス、サイズ、IOサイズ、キャッシュヒット数、スループットターゲット、帯域幅調整などの制限については、以下を参照してください。

- Premium Storage

高可用性

InterSystemsは、定義された可用性セットに2台以上の仮想マシンを含めることをお勧めします。
定期または非定期のメンテナンス中に、99.95%のAzure SLAを満たすためには少なくとも1台の仮想マシンが利用可能となるため、この構成が必要になります。データセンターが更新中である場合、VMは筐体してダウン状態になり、アップグレードされた後、適当な順でオンラインとなるため、これは重要なことです。このメンテナンス期間中はアプリケーションが使用できません。

したがって、可用性高いアーキテクチャには、負荷分散されたWebサーバー、データベースミラー、複数のアプリケーションサーバーなど、各種サーバが2台ずつ必要になります。

Azureの高可用性に関するベストプラクティスの詳細は、以下を参照してください。

- 可用性管理

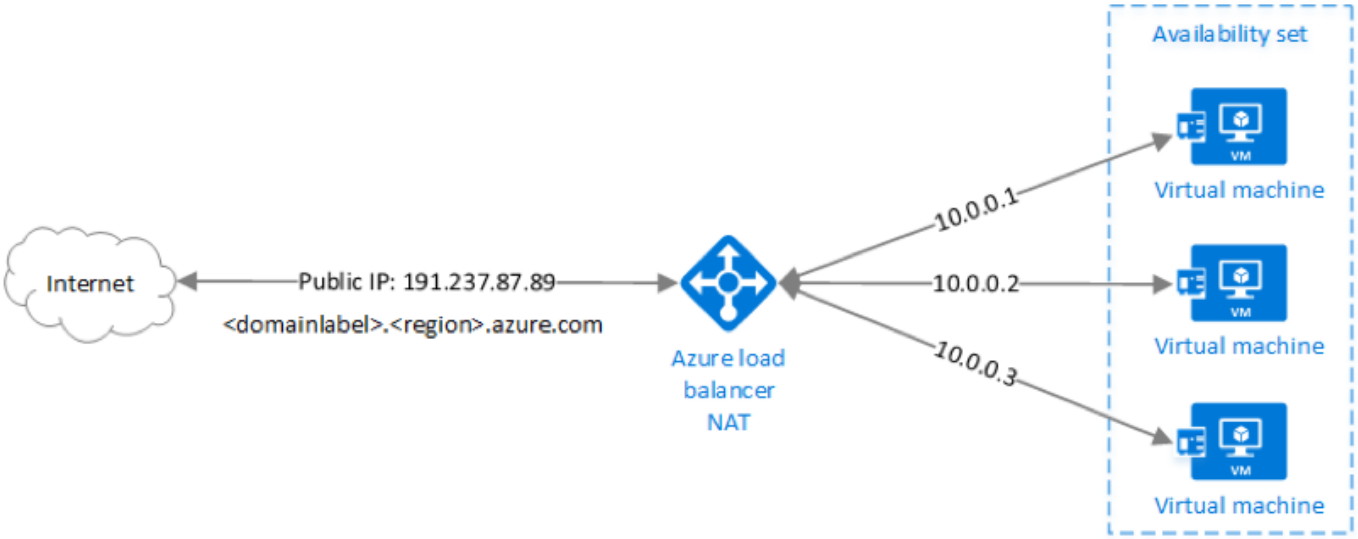
Webサーバの負荷分散

Caché ベースのアプリケーションには、外部および内部の負荷分散されたWebサーバーが必要になる場合があります。外部のロードバランサーはインターネットまたはWAN（VPNまたはExpress Route）経由でのアクセスに使用され、内部のロードバランサーは内部トラフィックに使用される可能性があります。Azure Load Balancerは、レイヤー4（TCP、UDP）タイプのロードバランサーで、ロードバランサー内に定義されたクラウドサービスまたは仮想マシン内の正常なサービスインスタンスに着信トラフィックを分散します。

Webサーバーのロードバランサーは、クライアントIPアドレスセッション永続性（2タプル）と可能な限り短いプ

ロ-ブタイムアウト（現在は5秒）で構成れている必要があります。
TrakCareでは、ユ-ザ-がログインしている期間、セッション永続化が必要です。

マイクロソフトが提供している次の図は、ARMデプロイメントモデル内のAzure Load Balancerの簡単な例を示しています。



分散アルゴリズム、ポ-ト転送、サ-ビス監視、送信元ネットワ-クアドレス変換といったAzure Load Balancerの機能や、各種ロ-ドバランサ-の詳細については、以下を参照してください。

- Load Balancerの概要

Azureは、外部ロ-ドバランサ-のほか、Azure Application Gatewayを提供しています。Application Gatewayは、Cookieベ-スのセッションアフィニティとと SSL終端（SSLオフロ-ド）をサポ-トするL7ロ-ドバランサ-（HTTP/HTTPS）です。SSLオフロ-ド機能は、SSL接続がロ-ドバランサ-で終すするため、暗号化/復号化のオ-バ-ヘッドをWebサ-バ-から取り除きます。このアプロ-チでは、SSL証明書がWebファ-ム内のすべてのノ-ドでではなく、ゲ-トウェイで展開および管理されるため、管理が簡素化されます。

詳細については、以下を参照してください。

- Application Gatewayの概要
- Azure Resource Managerを使ってApplication GatewayにおけるSSLオフロ-ドを構成する

デ-タベ-スミラ-リング

Caché ベ-スのアプリケ-ションをAzureにデプロイする場合、Caché デ-タベ-スサ-バ-に高可用性を提供するには、同期デ-タベ-スミラ-リングを使用して、特定のプライマリAzureリ-ジョンで高可用性を提供し、アップタイムサ-ビスレベル契約の要件によっては、潜在的に非同期デ-タベ-スミラ-リングを使用して、災害復旧用としてセカンダリAzureリ-ジョンのホットスタンバイにデ-タを複製する必要があります。

デ-タベ-スミラ-は、フェイルオ-バ-メンバ-と呼ばれる2つのデ-タベ-スシステムの論理グループです。これらのメンバ-はネットワ-クでのみ接続された物理的に独立したシステムです。ミラ-は、2つのシステムを解決した後、自動的に片方をプライマリシステムとするため、もう片方は自動的にバックアップシステムになります。外部クライアントワ-クステ-ションまたはほかのコンピュ-タは、ミラ-リング構成に指定されたミラ-の仮想IP（VIP）を介してミラ-に接続します。
ミラ-VIPは、ミラ-のプライマリシステムのインタ-フェイスに自動的にバインドされます。
注 意: Azureでは、ミラ-VIPを構成することはできないため、代替ソリュ-ションが考案されています。

Azureにデ-タベ-スミラ-をデプロイするために現在推奨されているのは、同じAzure可用性セットに3つのVM（プライマリ、バックアップ、アビタ-）を構成することです。こうすることで、Azureは常に、99.95%のSL

Aでこれらの VM のうち少なくとも 2 つが外部接続し、それぞれが別々の更新ドメインと障害ドメインに割り当てられるように設定しており、その結果、データベースのデータは自動的かつ適切な分離と冗長性を提供しています。

これに関するその他の詳細は、以下を参照してください。

- Azure可用性セット
- Azureサービスレベルアグリーメント(SLA)

Azureを含むあらゆるIaaSクラウドプロバイダーには、クライアント接続を仮想IP機能がないアプリケーションに自動的にフェイルオーバーする処理に関する課題が伴います。
そこで、クライアント接続の自動フェイルオーバーには、それを維持するための指示がいくつかあります。

まず、InterSystemsは、CSPゲートウェイをミラー対応に拡張し、CSP Gatewayを備えたWebサーバーからデータベースサーバーへの接続にVIPを使用する必要をなくしました。CSPゲートウェイは、両方のミラーメンバーと自動ネゴシエーションし、プライマリメンバーとなった適切なメンバーにリダイレクトします。ECPクライアントを使用している場合は、すでにミラー対応である機能に対応します。

次に、CSP GatewayとECPクライアントの外部の接続には、依然としてVIPのような機能が必要です。
InterSystemsは、mirror_status.cxw ヘルスチェックステータスページを使ったポーリング方法を使用することをお勧めします。これは、コミュニティ記事「Database Mirroring without a Virtual IP address仮想IPアドレスを使用しないデータベースミラーリング」に説明されています。

Azure内部ロードバランサー(ILB)は、すべてのネットワークトラフィックをプライマリミラーメンバーに転送するために、VIPのような機能として単一のIPアドレスを提供します。
ILBはプライマリミラーメンバーにのみトラフィックを分散します。この方法はポーリングに依存していないため、ミラー構成のミラーメンバーがプライマリメンバーになった時点で転送することができます。Azure Traffic Managerを使用したDRシナリオでは、ポーリングをこの方法と組み合わせて使用することができます。

バックアップと復元

バックアップ操作には、いくつかのオプションがあります。
InterSystems製品を使用したAzureデプロイメントでは、次の3つのオプションを実行できます。最初の2つのオプションは、スナップショットを作成する前にデータベースによるディスクへの書き込みを一時停止し、スナップショットに成功したら更新を再開するというスナップショットタイプの手順を使用しています。いずれかのスナップショット方式を使用してクリーンなバックアップを作成するには、次のおおまかな手順を実行します。

- データベースのFreeze API呼び出しにより、データベースへの書き込みを一時停止する。
- OSとデータディスクのスナップショットを作成する。
- データベースのThaw API呼び出しにより、Cachéの書き込みを再開する。
- バックアップファシリティはバックアップ場所にアーカイブする。

クリーンで一貫したバックアップを確保するために、整合性チェックなどの追加手順を定期的に追加することができます。

どのオプションを使用するかという決定ポイントは、組織の運用要件とポリシーによって異なります。
さまざまなオプションをさらに詳しく検討するには、InterSystemsにご相談ください。

Azure Backup

Azure BackupとAzure Automation Runbooks、そしてInterSystemsのExternal Freeze and Thaw API機能を使って、Azure ARMプラットフォーム内でバックアップ操作を実施できるようになりました。実質的な24時間365日の運用リジリエンシーとクリーンな定期バックアップを実現できます。Azure Backupの管理と自動化に関する詳細は、こちらを参照してください。

論理ボリュームマネージャのスナップショット

別の方法として、市場に出回っているさまざまのサードパーティ製バックアップツールを使用する場合は、VMそのものにバックアップエージェントを展開し、論理ボリュームマネージャ（LVM）のスナップショットと組み合わせてファイルレベルのバックアップを活用することができます。

このモデルには、WindowsまたはLinuxベースのVMをファイルレベルで復元できるというメリットがあります。このソリューションで 注 意すべき点は、AzureやほとんどのIaaSクラウドプロバイダはテープメディアを提供しないため、すべてのバックアップリポジトリは、短期アーカイブ用のディスクベースであり、長期保存（LTR）にはBLOBまたはバケットタイプの低コストストレージを活用できるということです。このモデルを使用する場合は、ディスクベースのバックアップリポジトリを最も効率的に使用できるように、重複除去テクノロジーをサポートするバックアップ製品を使用することを強くお勧めします。

こういったクラウド対応のバックアップ製品には、Commvault、EMC Networker、HPE Data Protector、Veritas Netbackupなどさまざまな製品があります。
InterSystemsでは、これらの製品の比較検証や推奨は行っておりません。

Caché Online Backup

小さなデプロイメントでは、組み込みのCaché Online Backupファシリティもオプションとして考えられます。InterSystemsのデータベースオンラインバックアップユーティリティは、データベース内のすべてのブロックをキャプチャしてデータベースファイルにデータをバックアップし、出力をシーケンシャルファイルに書き込みます。この、InterSystems独自のバックアップメカニズムは、本番システムのユーザにダウンタイムを引き起こさないように設計されています。

Azureでは、オンラインバックアップが完了した後、バックアップ出力ファイルにシステムが使用中のその他すべてのファイルをAzureファイル共有にコピーする必要があります。
このプロセスは、仮想マシン内でスクリプトとして実行しなければなりません。

Azureファイル共有で最大限の可用性を得るには、Azure RA-GRSストレージアカウントを使用する必要があります。Azureファイル共有の最大共有サイズは5 TB、最大ファイルサイズは1 TB、共有あたりの最大スループットは60 MB/秒（すべてのクライアントで共有）です。

オンラインバックアップは、バックアップに低コストのソリューションを実装したい小規模サイト向けのエントリーレベルのアプローチですが、データベースのサイズが大きくなるにつれ、スナップショットテクノロジーを使った外部バックアップがベストプラクティスとして推奨されます。外部ファイルのバックアップ、より高速な復元時間、エンタープライズ全体データビュー管理ツールなどのメリットがあります。

災害復旧

AzureにCachéベースのアプリケーションをデプロイする場合は、ネットワーク、サーバ、ストレージなどの災害復旧（DR）リソースを異なるAzureリージョンに配置することをお勧めします。指定されたDR Azureリージョンに必要な容量は、組織のニーズによって異なります。ほとんどの場合、DRモードでの運用時には本番容量の100%が必要になりますが、弾 性 デルして必要になるまでは、より少ない容量をプロビジョニングできます。

DR Azureリージョンの仮想マシンに継続して複製するには、非同期データベースミラーリングが使用されます。ミラーリングは、データベースのトランザクションジャーナルを使用して、プライマリシステムのパフォーマンスへの影響を最小限に抑えながら、TCP/IPネットワーク経由で更新を複製します。これらのDR非同期ミラーメンバには、圧縮と暗号化を構成することを強くお勧めします。

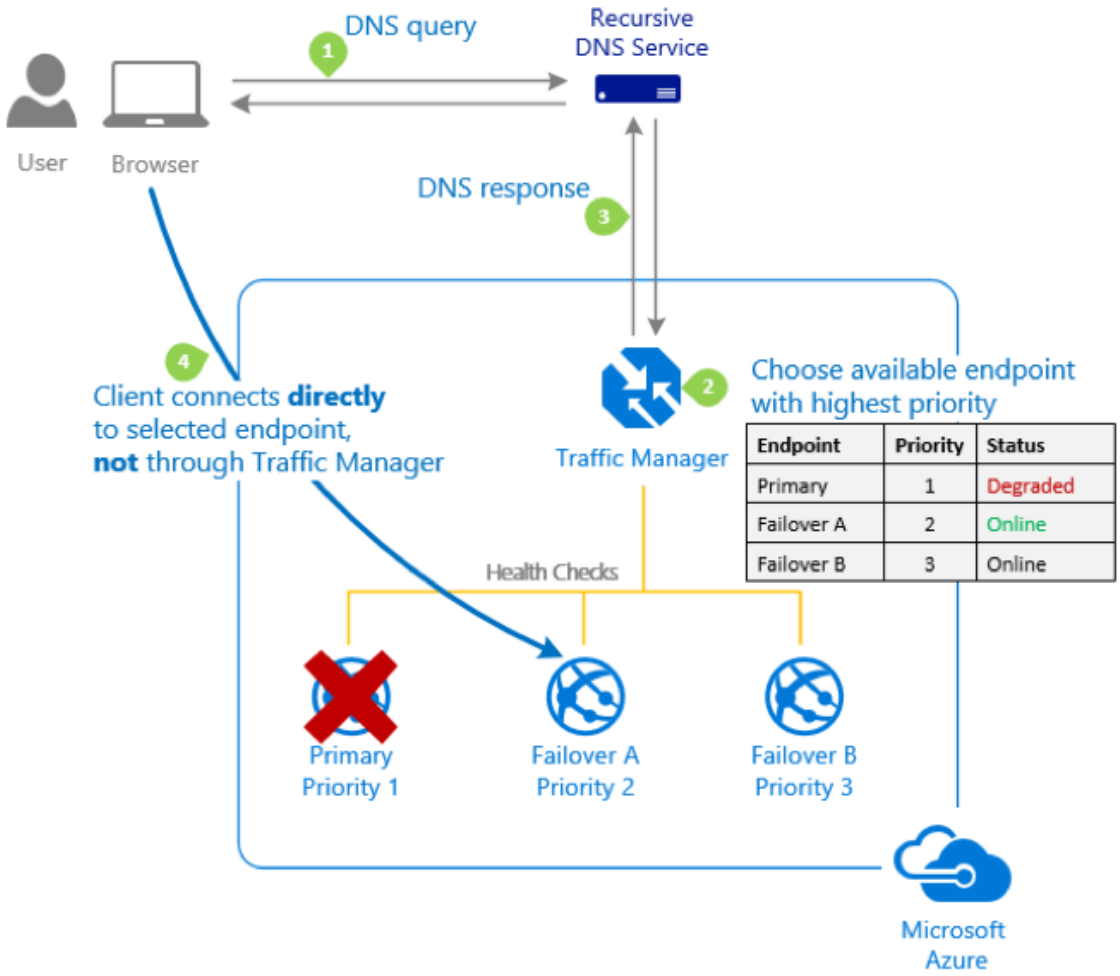
アプリケーションにアクセスする一般インターネット上のすべての外部クライアントは、DNSサービスとしてのAzure Traffic Manager経由でルーティングされます。Microsoft Azure Traffic Manager（ATM）は、トラフィックを現在アクティブなデータセンターに転送するスイッチとして使用されます。Azure Traffic Managerは、エンドユーザがさまざまなサービスエンドポイントにルーティングされる方法を決定する、数のアルゴリズムをサポートしています。各種アルゴリズムの詳細は、 こちら を参照してください。

このドキュメントでは、Traffic Managerのエンドポイント監視とフェイルオーバーと組み合わせて「優先度」付きのトラフィック-ティング方法を使用します。
エンドポイント監視とフェイルオーバーの詳細は、 こちら を参照してください。

Traffic
Managerは、各エンドポイントに通常のリクエストを送信してそのレスポンスを検証することで機能します。
エンドポイントが有効なレスポンスを提供できない場合、Traffic
Managerはそのステータスを「デグレード」として表示します。
DNSレスポンスには含まれなくなり、代わりに利用可能な代替エンドポイントを返します。 このようにして、ユーザートラフィックは障害のあるエンドポイントから離れ、利用可能なエンドポイントに向けられます。

上記の方法を使用すると、特定のリージョンと特定のミラーメンバーのみがトラフィックを許可することになります。 これは、InterSystems CSP Gatewayから提示されるmirror-statusページの「エンドポイント定義」によって制御されており、
プライマリミラーメンバーのみが、モニタープローブからのHTTP
200として「成功」を返すことになっています。

マイクロソフトが提供する次の図は、優先度付きトラフィック-チンアルゴリズムの概要を示しています。



Azure Traffic
Managerは、すべてのクライアントが接続できる「 https://my-app.trafficmanager.net
」といった単一のエンドポイントを生成します。
さらに、「 https://www.my-app-domain.com
」のようなバニティURLを提供するようにAレコードを構成することができます。Azure Traffic
Managerは、両リージョンのエンドポイントのアドレスを含む1つのプロファイルで構成されます。

常に、エンドポイント監視に基いて、1つのリージョンのみがオンライン状態を報告します。
これにより、トラフィックは常に1つのリージョンにのみ流れるようになります。エンドポイント監視は、プライマリAzureリージョンのアプリケーションがダウン状態であり、セカンダリAzureリージョンのアプリケーションがライブになっていることを検出するため、リージョン間のフェイルオーバーにさらに手順を追加する必要はありません。これは、DR非同期ミラーメンバーがプライマリに昇格されるとき、CSP GatewayがTraffic ManagerのエンドポイントHTTP 200を送信するようになっているためです。

上記のソリューションの代案はいくつかあり、組織の運用要件やサービスレベル契約に基いてカスタマイズすることができます。

ネットワーク接続

アプリケーションの接続要件に応じて、インターネット、IPSEC VPN、またはAzure Express Routeを使った専用リンクのいずれかを使った複数の接続モデルがあります。
選択方法は、アプリケーションとユーザーのニーズによって異なります。
これら3つのモデルの帯域幅使用率はそれぞれ異なるため、Azure担当者に相談するかAzure Portalで特定のリージョンで使用可能な接続オプションを確認することをお勧めします。

Express Routeを使用している場合、災害復旧シナリオで有効にできる複数の回線やリージョンアクセスなどのオプションがあります。Express Routeプロバイダーに相談し、プロバイダーがサポートする高可用性災害復旧シナリオを理解することが重要です。

セキュリティ

パブリッククラウドプロバイダーにアプリケーションをデプロイするかどうかを決定するには 注 意が必要です。
組織のセキュリティコンプライアンスを維持するには、組織の標準セキュリティポリシーまたはクラウド専用に作成された新しいポリシーに従う必要があります。クラウドデプロイメントには、クライアントデータセンターと物理的なセキュリティ管理の外にデータが置かれるため、付加リスクが伴います。使用中でないデータ(データベースとジャーナル)と使用中のデータ(ネットワーク通信)には、InterSystemsのデータベースとジャーナル暗号化と合わせて、前者にはAESを、後者にはSSL/TLS暗号化を使用することを強くお勧めします。

すべての暗号化キー管理と同様に、データの安全を確保、不要なデータアクセスやセキュリティ違反を防止するには、組織のポリシーに基いて、適切な手順を文書化し、それに従う必要があります。

インターネット経由でのアクセスが許可されている場合、侵入検知、サービス拒否攻撃などの追加機能を導入するために、サードパーティのファイアウォール装置が必要になる場合があります。

アーキテクチャ図の例

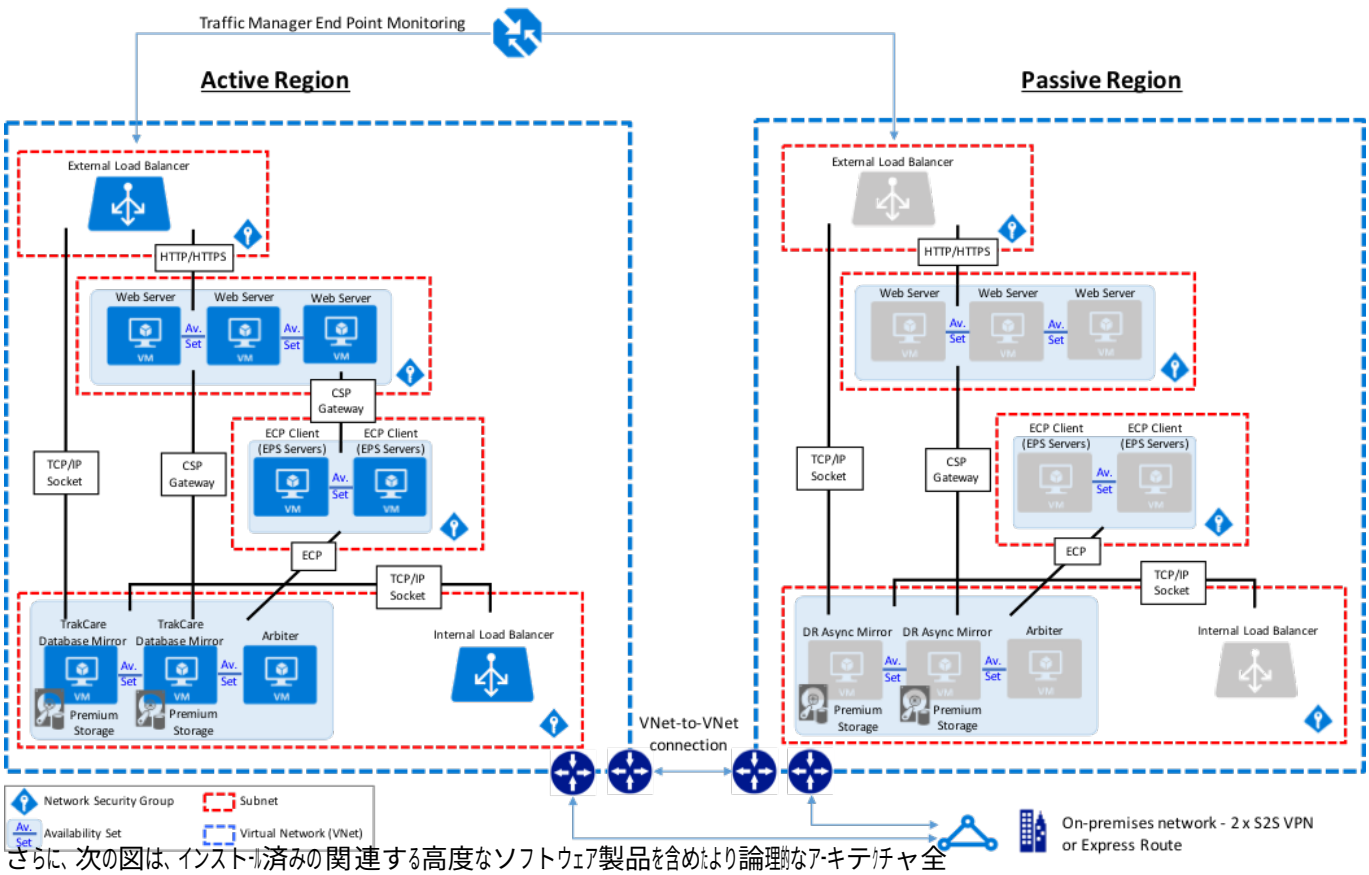
下の図は、データベースミラーリング(同期フェイルオーバーとDR非同期)、ECPを使用したアプリケーションサーバー、負荷分散された複数のWebサーバーの構成高可用性提供する典型的なCachéインストールを示しています。

TrakCareの例

次の図は、負荷分散される複数のWebサーバー、ECPクライアントとしての2台のEPSプリントサーバー、データベースミラーで構成される典型的なTrakCareデプロイメントを示しています。
仮想IPアドレスは、ECPまたはCSP Gatewayに関連付けられていない接続のみ使用されます。
ECPクライアントとCSP Gatewayはミラー対応であり、VIPを必要としません。

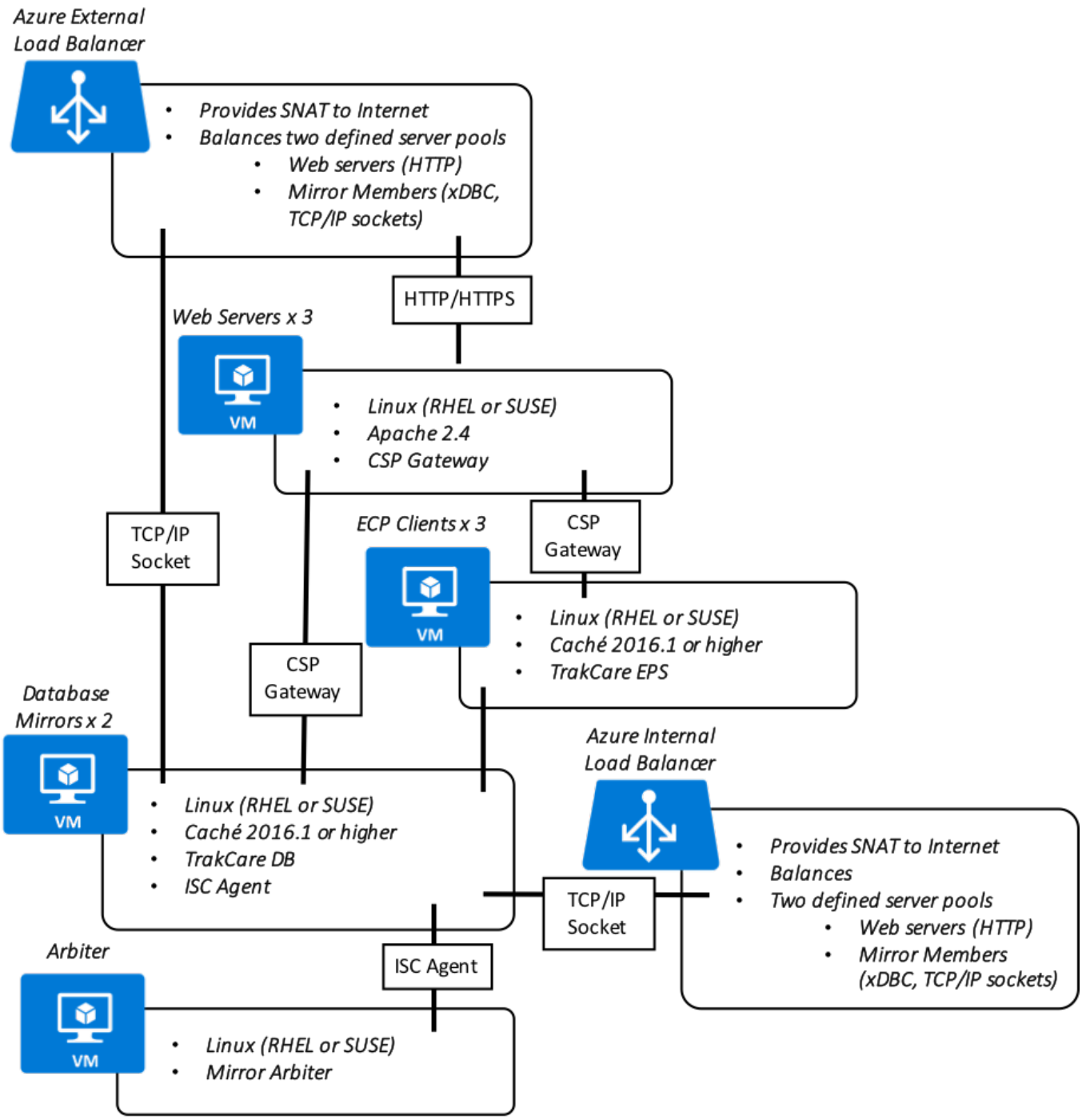
下のサンプルリファレンスアーキテクチャ図には、アクティブまたはプライマリリージョンにおける高可用性プライマリAzureリージョンが利用不可である場合の別のAzureリージョンへの災害復旧が含まれます。
また、この例では、データベースミラーには、1つのミラーセット内にTrakCare DB、TrakCare Analytics、およびIntegrationネームスペースが含まれています。

TrakCare Azureﾘﾌｧﾚﾝｽｱｰｷﾃｸﾁｬ図 - 物理ｱｰｷﾃｸﾁｬ



さらに、次の図は、ｲﾝｽﾄｰﾙ済みの関連する高度なソフトｳｪｱ製品を含めたより論理的なｱｰｷﾃｸﾁｬ全容ｲﾒｰｼﾞを示しています。

TrakCare Azureﾘﾌｧﾚﾝｽｱｰｷﾃｸﾁｬ図 - 論理ｱｰｷﾃｸﾁｬ

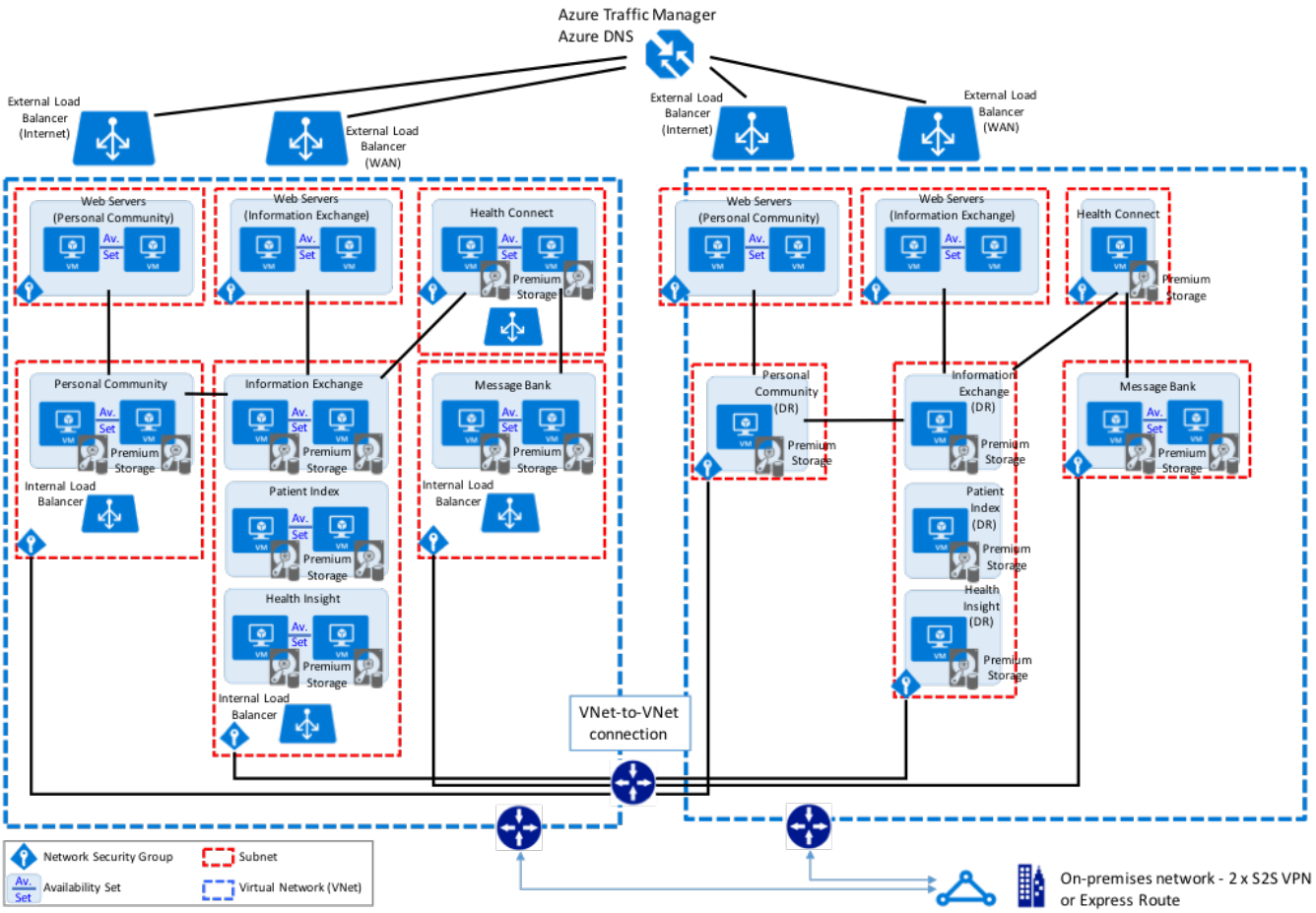


HealthShareの例

次の図は、負荷分散される複数のWebサーバ、Information Exchange、Patient Index、Personal Community、Health Insight、Health Connectといった複数のHealthShare製品による典型的なHealthSharaeデプロイメントを示しています。それぞれの製品は、Azure可用性セット内に1組のデータベースミラーを含めて高可用性を実現しています。仮想IPアドレスは、ECPまたはCSP Gatewayに関連付けられていない接続にのみ使用されます。HealthShare製品間のWebサービス通信に使用されるCSP Gatewayはミラー対応であり、VIPを必要としません。

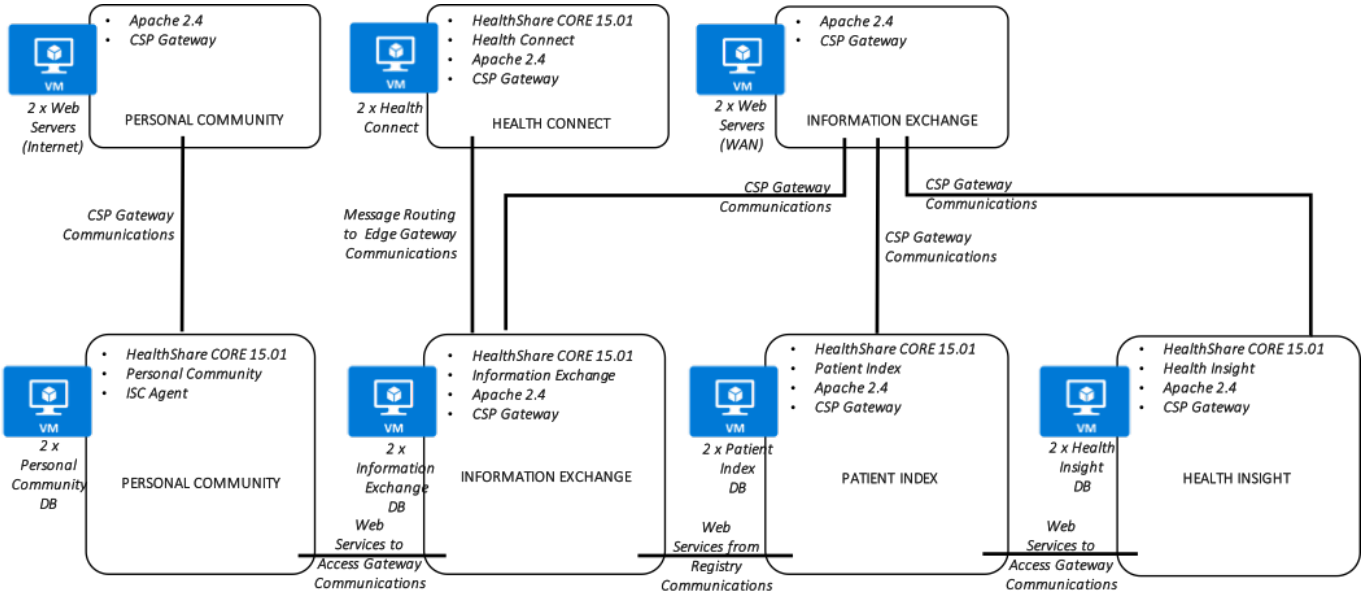
このサンプルリファレンスアーキテクチャ図には、アクティブまたはプライマリリージョンにおける高可用性プライマリAzureリージョンが利用不可である場合の別のAzureリージョンへの災害復旧が含まれます。

HealthShare Azureリファレンスアーキテクチャ図 - 物理アーキテクチャ



さらに、次の図は、インストール済みの関連する高度なソフトウェア製品を含めたより論理的なアーキテクチャ全容、接続要件と方法、およびそれぞれの機能目的を示しています。

HealthShare Azureリファレンスアーキテクチャ図 - 論理アーキテクチャ



#Azure #Mirroring #クラウド #Caché #HealthShare #InterSystems IRIS #InterSystems IRIS for Health

ソースURL: https://jp.community.intersystems.com/post/microsoft-azure-resource-manager%EF%BC%88arm%EF%BC%89%E5%90%91%E3%81%91intersystems%E3%82%B5%E3%83%B3%E3%83%97%E3%83%AB%E3%

83%AA%E3%83%95%E3%82%A1%E3%83%AC%E3%83%B3%E3%82%B9%E3%82%A2%E3%83%BC%E3%82%AD%E3%83%86%E3%82%AF%E3%83%81%E3%83%A3