文章
Li Yan · 一月 13, 2021 阅读大约需 15 分钟

面向 Microsoft Azure Resource Manager (ARM) 的 InterSystems 示例参考架构

本文提供了一个参考架构，作为示例说明基于 InterSystems Technologies（适用于 Caché、Ensemble、HealthShare、TrakCare 以及相关的嵌入式技术，例如 DeepSee、iKnow、Zen 和 Zen Mojo）提供的强大性能和高可用性应用。
Azure 有两种用于创建和管理资源的不同部署模型：Azure Classic 和 Azure Resource Manager。本文中的详细信息基于 Azure Resource Manager (ARM) 模型。

摘要

Microsoft Azure 云平台为基础设施即服务 (IaaS) 提供功能丰富的环境，其作为云提供完备的功能，支持所有的 InterSystems 产品。
与任何平台或部署模型一样，必须留心以确保考虑到环境的各个方面，例如性能、可用性、操作和管理程序。 本文将阐述所有这些方面。

性能

在 Azure ARM 中，有多个可用于计算虚拟机 (VM) 的选项以及相关的存储选项，与 InterSystems 产品最直接相关的是网络连接 的IaaS 磁盘，其作为 VHD 文件存储在 Azure 页面的 Blob 存储中。 还有其他几个选项，例如_ Blob（块）、文件_等，但是这些选项更特定于单个应用程序的要求，而非支持 Caché 的操作。
磁盘存储有两种类型的存储： 高级存储 和 标准存储 。
高级存储更适合这样的生产工作负载：要求保证可预测的低延迟每秒输入/输出操作 (IOP) 和吞吐量。
标准存储是针对非生产或存档类型工作负载的更经济选择。 选择特定的 VM 类型时务必小心，因为并非所有的 VM 类型都可以访问高级存储。

虚拟 IP 地址和自动故障转移

大多数 IaaS 云提供商缺乏提供虚拟 IP (VIP) 地址的能力，这种地址通常用在数据库故障转移设计中。 为解决这一问题，Caché 中增强了几种最常用的连接方法，尤其是 ECP 客户端和 CSP 网关，从而不再依赖 VIP 功能使它们实现镜像状态感知。

xDBC、直接 TCP/IP 套接字等连接方法，或其他的直接连接协议，均需要使用 VIP。
为解决这些问题，InterSystems 数据库镜像技术使用 API 与 Azure 内部负载均衡器（ILB）交互以实现类 VIP 功能，使得 Azure 中的那些连接方法实现自动故障转移，从而在 Azure 中提供完整而强大的高可用性设计 。
有关详细信息，请参见社区文章无虚拟 IP 地址的数据库镜像。

备份操作

无论使用传统的文件级备份，还是基于快照的备份，在云部署中执行备份都面临着挑战。
如今，在 Azure ARM 平台中，使用 Azure Backup 和 Azure Automation Run
Books 配合 InterSystems 外部冻结及解冻 API
功能，即可实现这一切，从而实现真正的 24x7 全天候操作弹性并确保干净的常规备份。
或者，可以在 VM
本身中部署备份代理，利用文件级备份
，并结合逻辑卷管理器 (LVM) 快照，来使用市面上的许多第三方备份工具。

示例架构

作为本文档的一部分，这里为您提供一个示例 Azure
架构，作为您特定应用部署的入门参考，并可用作各种部署的可能性的指南。
此参考架构显示了一个强大的 Caché
数据库部署，其中包括可实现高可用
性的数据库镜像成员、使用 InterSystems 企业缓存协议（ECP
）的应用程序服务器、使用 InterSystems
CSP 网关的 Web 服务器，以及内部和外部 Azure 负载均衡器。

Azure 架构

在 Microsoft Azure 上部署任何基于Caché 的应用都需要特别注意某些方面。
本部分讨论通用的方面，对于您的应用的特定技术要求不做阐述。

本文档中提供了两个示例，一个基于 InterSystems
TrakCare *统一医疗信息系统，另一个基于完整的 InterSystems HealthShare 健康信息学平台部署，包括：Information Exchange 、Patient Index、Health Insight、Personal Community 和 Health Connect。*

虚拟机

Azure 虚拟机 (VM) 分为两层：基本层和标准层。 两种类型提供对规模的选择。
基本层不提供标准层中的某些功能，例如负载均衡和自动伸缩。
因此，将标准层用于 TrakCare 部署。

标准层 VM 具有不同规模，按不同系列分组，即： A、D、DS、F、FS、G 和 GS。 DS、GS
和新的 FS 支持 Azure 高级存储的使用。

生产服务器通常需要使用高级存储来实现可靠性、低延迟和高性能。
因此，本文档中详细介绍的示例 TrakCare 和 HealthShare 部署架构将使用 FS、DS 或 GS 系列
VM。 注意，并非所有的虚拟机规模在所有区域中都可用。

有关虚拟机规模的详细信息，请参见：

- Windows 虚拟机规模
- Linux 虚拟机规模

存储

TrakCare 和 HealthShare 服务器需要 Azure 高级存储。
高级存储将数据存储在固态硬盘 (SSD)
上，以低延迟提供高吞吐量；而标准存储将数据存储在硬盘驱动器 (HDD) 上，会导致性能的降低。

Azure
存储属于冗余且高度可用的系统，但是，请务必注意，可用性集合当前不提供跨存储故障域的冗余，在极少数情况下，这可能会导致问题。 Microsoft
有缓解方案，并正在努力使此过程对最终客户广泛可用且更容易使用。
建议您直接与当地的 Microsoft 团队合作以确定是否需要任何缓解方案。

当针对高级存储帐户配置磁盘时，IOPS 和吞吐量（带宽）取决于磁盘的大小。
当前，有三种类型的高级存储磁盘：P10、P20 和 P30。 每种对 IOPS
和吞吐量都有特定的限制，如下表所示。

高级磁盘类型	**P4**	**P6**	**P10**	**P15**	**P20**	**P30**	**P40**	**P50**
磁盘容量	32GB	64GB	128GB	256GB	512GB	1024GB	2048GB	4096GB
每个磁盘的 IOPS	120	240	500	1100	2300	5000	7500	7500
每个磁盘的吞吐量	25MB/s	50MB/s	100MB/s	125MB/s	150MB/s	200MB/s	250MB/s	250MB/s

注意：确保给定的 VM 上有足够的可用带宽来驱动磁盘流量。

例如，STANDARDDS13 VM 具有每秒 256 MB 的专用带宽，可用于所有高级存储磁盘流量。

这意味着连接到该虚拟机的四个 P30 高级存储磁盘的吞吐量限制为每秒 256
MB，而不是四个 P30 磁盘理论上可以提供的每秒 800 MB 的速度。

有关高级存储磁盘的更
多详细信息和限制，包括预配置的容量、性能
、大小、IO 大小、缓存命中率、吞吐量目标和限制，请参阅：

- 高级存储

高可用性

InterSystems 建议在已定义的可用性集合中拥有两个或更多虚拟机。
之所以
需要此配置，是因为在计划内或计划外的维护活动期间，至少有一个虚拟机可用于满足 99.95%
的 Azure SLA。
这很重要，因为在数据中心更新期间，VM
会被并行关闭、升级并以不特定的顺序重新联机，导致应用程序在此维护窗口期不可用。

因此，高度可用的架
构需要每种服务器至少部署两台，这些服
务器包括负载均衡 Web 服务器、数据库镜像、多个应用程序服务器等。

有关 Azure 高可用性最佳做法的更多信息，请参见：

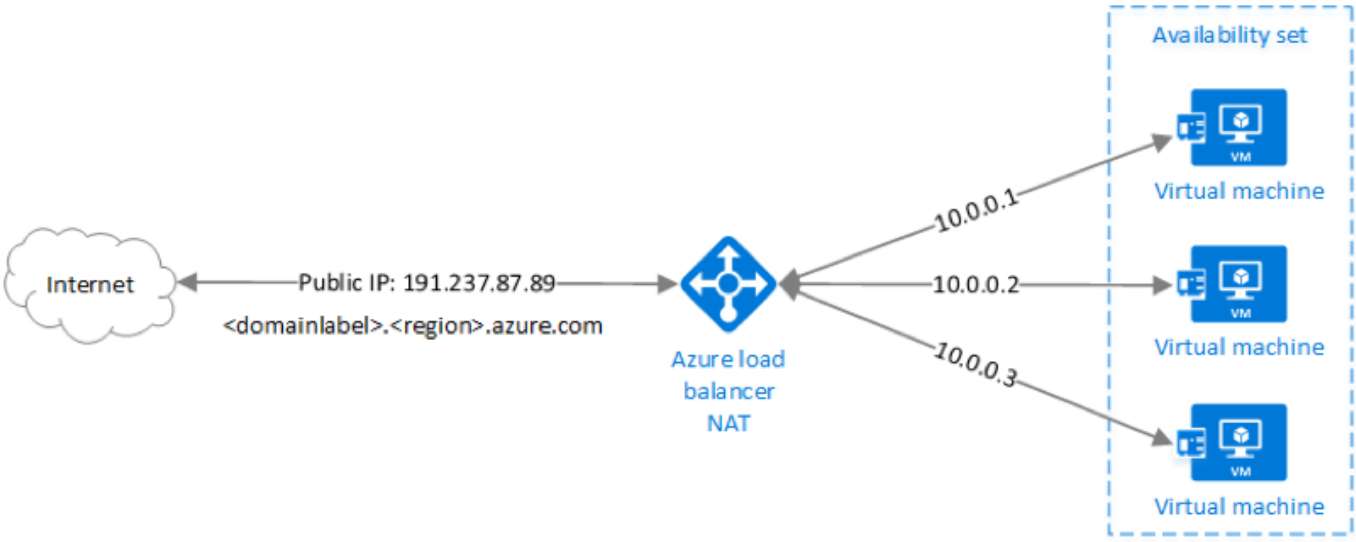
- 管理可用性

Web 服务器负载均衡

基于 Caché 的应用程序可能需要外部和内部负载均衡 Web 服务器。
外部负载均衡器用于通过 Internet 或 WAN（VPN 或 Express
Route）进行的访问，而内部负载均衡器则通常用于内部流量。 Azure 负载均衡器是 4 层 (TCP, UDP)
的负载均衡器，可在负载均衡器集合中定义的云服务或虚拟机中的健康服务实例之间分配传入的流量
。

Web 服务器负载均衡器必须配置客户端 IP 地址会话持续性（2
个元组）和可能的最短探测超时（当前为 5 秒）。 TrakCare 需要在用户登录期间保持会话持续性。

Microsoft 提供的下图显示了 ARM 部署模型中一个简单的 Azure 负载均衡器示例。



有关 Azure
负载均衡器的功能（例如分配算法、端
口转发、服务监视、源 NAT ）和其他类型的可用负载均衡器的详细信息，请参阅：

- 负载均衡器概述

除了 Azure 外部负载均衡器，Azure 还提供 Azure 应用程序网关。 Application
Gateway 是一个 L7 负载均衡器 (HTTP/HTPS)，支持基于 cookie 的会话相关性和 SSL 终端（
SSL 卸载）。 SSL 卸载可减轻 Web 服务器的加密/解密开销，因为 SSL
连接会在负载均衡器处终止。 这种方法简化了管理，因为 SSL
证书是在网关中部署和管理，而不是在 Web 场中的所有节点上。

有关详细信息，请参阅：

- 应用程序网关概述
- 使用 Azure Resource Manager 为 SSL 卸载配置应用程序网关

数据库镜像

在 Azure 上部署基于 Caché 的应用程序时，要为 Caché
数据库服务器提供高可用性，
需要使用同步数据库镜像，以在给定的主 Azure
区域中提供高可用性，并可能使
用异步数据库镜像将数据复制到辅助 Azure
区域中的热备用数据库中，以根据您的运行时间服务水平协议要求来进行灾难恢复。

数据库镜像是两个数据库系统的逻辑分组，也就是所说的故障转移成员，它们在物理上是仅通过网络连接的独立系统。 在这两个系统之间进行仲裁后，镜像会自动将其中一个指定为主系统。
另一个自动成为备份系统。 外部客户端工作站或其他计算机通过镜像虚拟 IP
(VIP) 连接到镜像，该虚拟 IP 在镜像配置期间指定。 镜像 VIP 会自动绑定到镜像主系统上的接口。

注意：在 Azure 中，无法配置镜像 VIP，因此已设计了替代解决方案。

当前，在 Azure 中部署数据库镜像时，建议在同一 Azure 可用性集中配置三个 VM（主 VM
、备份 VM、仲裁器）。
这样可确保在任何给定的时间，Azure 都可以保证至少与其中两个 VM 以 99.95% 的 SLA
建立外部连接，并且每个 VM 都位于不同的更新域和故障域中。
这样可以为数据库数据本身提供足够的隔离和冗余。

可在下列位置找到更多详细信息：

- Azure 可用性集
- Azure 服务水平协议 (SLA)

包括 Azure 在内的任何 IaaS
云提供程序所面临的挑战，就是在没有虚拟 IP
功能的情况下，如何处理连接到应用程序的客户端的自动故障转移。
为了保持客户端连接的自动故障转移，已采取了两种策略。

首先，InterSystems 对 CSP
网关进行了增强，使其能够感知镜像，以此使得
采用 CSP 网关的 Web 服务器到数据库服务器的连接不再需要 VIP。 CSP
网关将自动与两个镜像成员进行协商，并重定向到确定的主镜像成员。 如果使用 ECP
客户端，则将与其已经具备的镜像感知协同工作。

其次，CSP 网关和 ECP 客户端外部的连接仍然需要类 VIP 功能。 InterSystems 建议将轮询方法与_
mirrorstatus.cxw
_运行状况检查状态页面介绍的内容
结合使用，该页面在社区文章无虚拟 IP 地址的数据库镜像中进行了详细说明。

Azure 内部负载均衡器 (ILB) 将提供单一 IP 地址作为类 VIP
功能，将所有网络流量定向到主镜像成员。 ILB 只会将流量分配给主镜像成员。
此方法不会依赖轮询，且在镜像配置内的任何镜像成员成为主成员时，允许立即重定向。
在某些使用 Azure Traffic Manager 的灾难恢复方案中，可将此方法与轮询结合使用。

备份与恢复

备份操作有多个选项。 以下 3 个选项可供您通过 InterSystems 产品进行 Azure 部署。
下面的前 2

个选项采用快照类型的过程，该过程会在创建快照之前将数据库写入到磁盘的操作挂起，然后在快照成功后恢复更新。 可采取以下高级别步骤通过任一快照方法来创建洁净的备份：

- 通过数据库冻结 API 调用暂停对数据库的写入。
- 创建操作系统和数据磁盘的快照。
- 通过数据库解冻 API 调用恢复 Caché 写入。
- 将设施存档备份到备份位置

可以定期添加诸如完整性检查之类的其他步骤，以确保洁净且一致的备份。

决定使用哪种选项取决于您组织的运营要求和策略。 InterSystems 可与您详细讨论各种选项。

Azure 备份

如今，在 Azure ARM 平台中，使用 Azure Backup 和 Azure Automation Run Books 配合 InterSystems 外部冻结及解冻 API 功能，即可实现备份操作，从而实现真正的 24x7 全天候操作弹性并确保干净的常规备份。 有关管理和自动化 Azure 备份的详细信息，可在此处找到。

逻辑卷管理器快照

或者，可以在 VM 本身中部署单个备份代理，利用文件级备份，并结合逻辑卷管理器 (LVM) 快照，来使用市面上的许多第三方备份工具。

该模型的主要优点之一是能够对基于 Windows 或 Linux 的 VM 进行文件级恢复。 此解决方案需要注意的几点是，由于 Azure 和大多数其他 IaaS 云提供商都不提供磁带媒体，因此所有的备份存储库对于短期归档均基于磁盘，并利用 Blob 或存储桶类型的低成本存储来进行长期保留 (LTR)。 强烈建议您使用此方法来使用支持重复数据删除技术的备份产品，以最有效地利用基于磁盘的备份存储库。

这些具有云支持的备份产品的示例包括但不限于：Commvault、EMC Networker、HPE Data Protector 和 Veritas Netbackup。 InterSystems 不会验证或认可一种备份产品是否优于其他产品。

Caché 在线备份

对于小型部署，内置 Caché 在线备份工具也是可行的选择。 该 InterSystems 数据库在线备份实用工具通过捕获数据库中的所有块来备份数据库文件中的数据，然后将输出写入顺序文件。 这种专有的备份机制旨在使生产系统的用户不停机。

在 Azure 中，在线备份完成后，必须将备份输出文件和系统正在使用的所有其他文件复制到 Azure 文件共享中。 该过程需要在虚拟机中编写脚本并执行。

Azure 文件共享应使用 Azure RA-GRS 存储帐户以实现最大可用性。 注意，Azure 文件共享的最大共享大小为 5TB，最大文件大小为 1TB，每个共享（所有客户端共享）的最大吞吐量为 60 MB/s。

在线备份是入门级方法，适合于希望实施低成本备份解决方案的小型站点。
但是，随着数据库的增大，建议将使用快照技术的外部备份作为最佳做法，因为其具有以下优势：备份外部文件、更快的恢复时间，以及企业范围的数据和管理工具。

灾难恢复

在 Azure 上部署基于 Caché
的应用程序时，建议将包括网络、服
务器和存储在内的灾难恢复 (DR) 资源放置在不同的 Azure 区域中。 指定的 DR
Azure 区域所需的容量取决于您组织的需求。 在大多数情况下，以 DR 模式运行时需要 100%
的生产能力，但是，在需要更多的生产能力作为弹性模型之前，可以配置较小的生产能力。

异步数据库镜像用于连续复制到 DR Azure 区域的虚拟机。
镜像使用数据库事务日志在 TCP/IP 网络上复制更新，其采用对主系统性能影响最小的方式。
强烈建议对这些 DR 异步镜像成员配置压缩和加密。

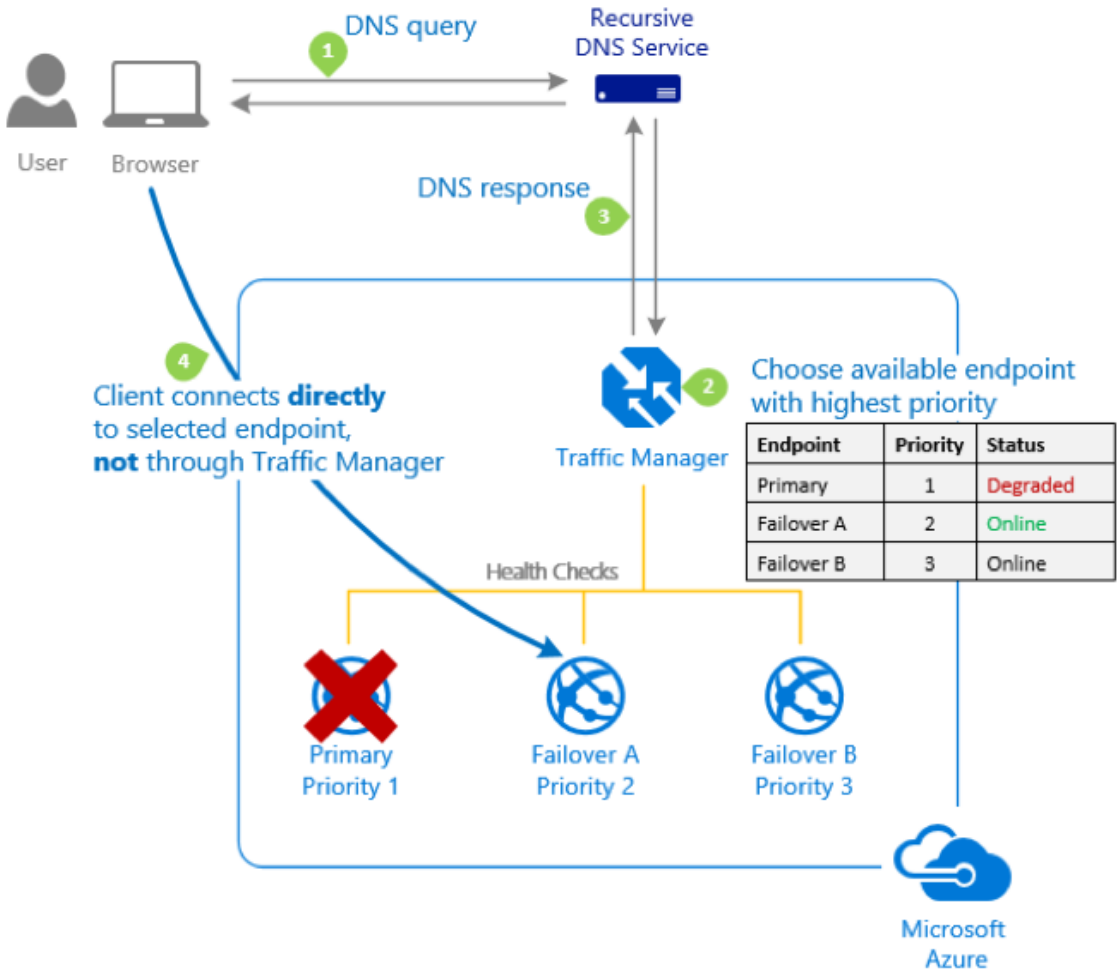
互联网上希望访问应用程序的所有外部客户端都将通过 Azure Traffic
Manager 作为 DNS 服务进行路由。 Microsoft Azure Traffic
Manager（ATM）用作交换机，负责将流量定向到当前活动的数据中心。 Azure Traffic
Manager 支持多种算法来确定如何将最终用户路由到各个服务端点。
有关各种算法的详细信息，可在此处找到。

本文档中， 优先级 流量路由方法将与 Traffic Manager 端点监视和故障转移结合使用。
有关端点监视和故障转移的详细信息，可在此处找到。

Traffic Manager 的工作是向每个端点发出常规请求，然后验证响应。
如果端点未提供有效的响应，则 Traffic Manager 会将其状态显示为 降级 。
它将不会再被包含在 DNS 响应中，而是会返回一个备用的可用端点。
通过这种方式，将用户流量从失败的端点定向到可用端点。

使用上述方法，只有特定区域和特定镜像成员才允许流量通过。
这由端点定义控制，可从 InterSystems CSP 网关的 mirrorstatus 页面设置端点定义。
只有主镜像成员才能通过监控器探测来报告 HTTP 200 为 成功 。

Microsoft 提供的下图在高级别上显示了优先级流量例程算法。



Azure Traffic
Manager
会产生一个所有客户端都可以连接到的端点，例如：“*https://my-app.trafficmanager.net* ”。
此外，可以配置 A 记录来提供虚 URL，例如 “*https://www.my-app-domain.com* ”。Azure Traffic
Manager 必须配置一个包含两个区域端点地址的配置文件。

在任何给定时间，只有其中的一个区域会根据端点监视在线报告。
这样可以确保流量在给定的时间仅流向一个区域。
区域之间的故障转移无需其他步骤，因
为端点监控将检测到主 Azure
区域中的应用程序已关闭，并且该应用程序现在位于辅助 Azure 区域中。 这是因为 DR
异步镜像成员被提升为主成员，然后允许 CSP 网关将 HTTP 200 报告给 Traffic Manager 端点监视。

上述解决方案有很多替代方案，可以根据您组织的运营要求和服务水平协议进行自定义。

网络连接

根据您应用程序的连接要求，有多种连接模型可用：使用 Internet、IPSEC
VPN 的连接模型，或使用 Azure Express Route 的专用链接。
选择方法取决于应用程序和用户需求。
三种方法的带宽使用情况各不相同，最好与您的 Azure 代表或 Azure
门户联系以确认给定区域的可用连接选项。

如果您正在使用 Express
Route，则可为灾难恢复方案启用包括多线路和多区域访问在内的多个选项。 与 Express
Route 提供商合作以了解他们支持的高可用性和灾难恢复方案至关重要。

安全

决定在公共云提供程序中部署应用程序时需要格外小心。
应遵循您组织的标准安全策略或专门为云开发的新安全策略，以维护您组织的安全合规性。
就客户端数据中心之外的数据以及物理安全控制方面，云部署的风险逐渐加大。
强烈建议对静态数据（数据库和
日志）及飞行数据（网络通信）使用 InterSystems
数据库和日志加密，分别使用 AES 和 SSL/TLS 加密。

与所有加密密钥管理一样，您需要按照您组织的政策记录并遵循正确的程序，以确保数据安全，防止不必要的数据访问或安全漏洞。

当允许通过互联网进行访问时，可能需要第三方防火墙设备来实现其他功能，例如入侵检测、拒绝服务保护等。

架构图示例

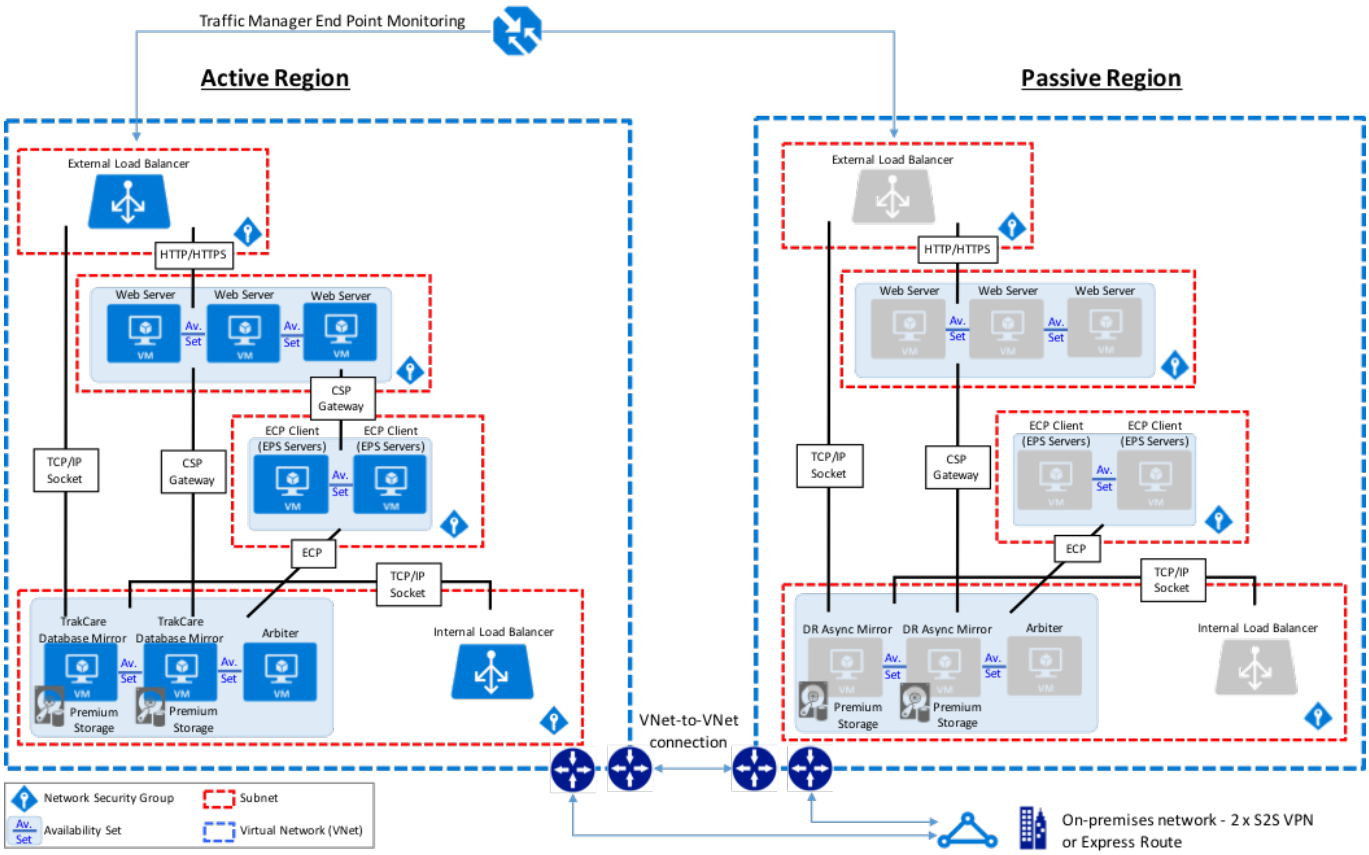
下图说明了典型的 Caché
安装，其以数据库镜像（同步故障转移和 DR 异步）、使用 ECP
的应用程序服务器，以及多个负载均衡 Web 服务器的方式提供高可用性。

TrakCare 示例

下图说明了典型的 TrakCare 部署，其中包含多个负载均衡 Web 服务器，两个作为 ECP
客户端的 EPS 打印服务器，以及数据库镜像配置。 虚拟 IP 地址仅用于与 ECP 或 CSP
网关不关联的连接。 ECP 客户端和 CSP 网关可感知镜像，不需要 VIP。

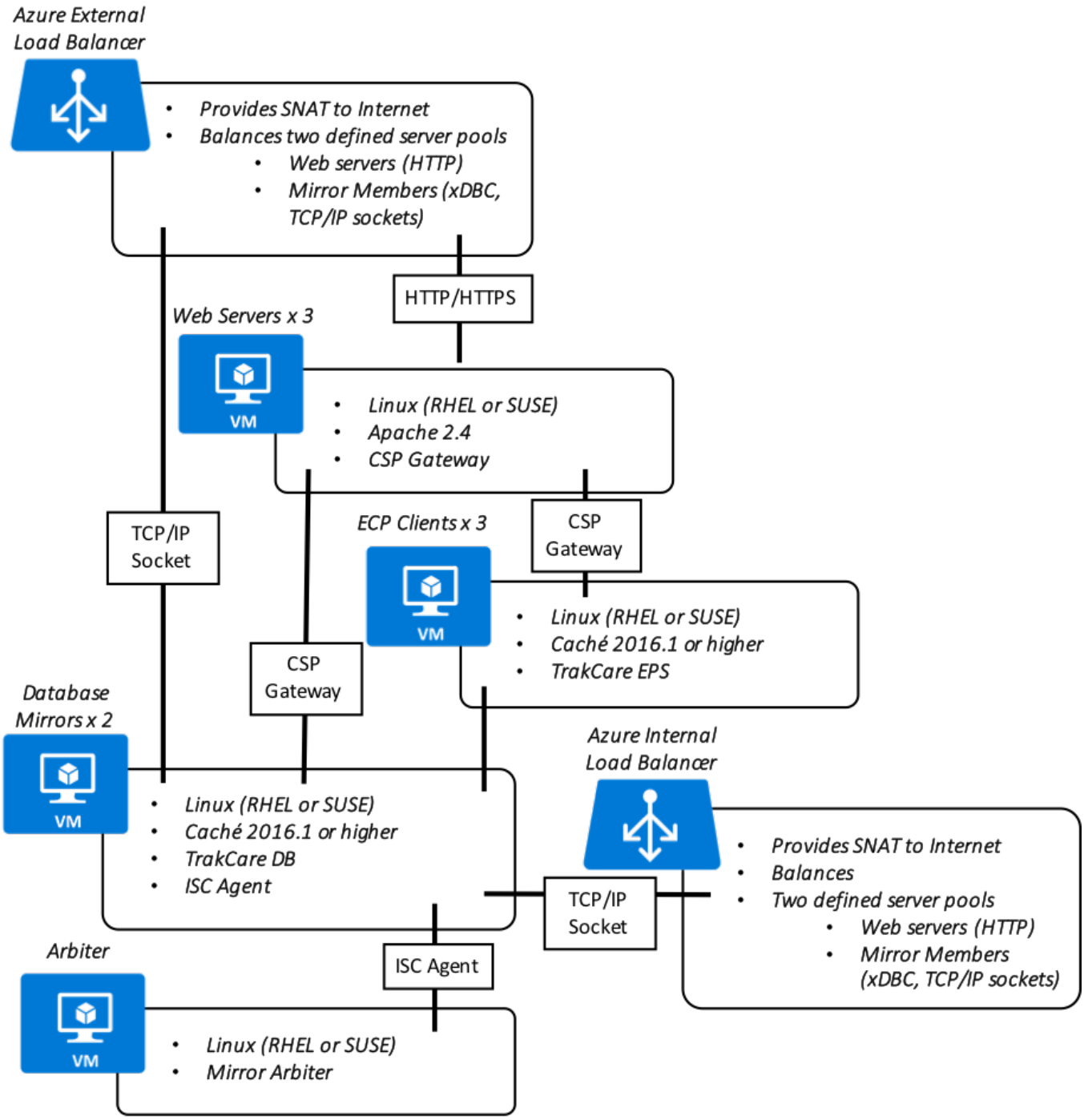
下图中的示例参考架构包括活动或主
区域中的高可用性，可在主 Azure 区域不可用的情况下，执行灾难恢复到另一个 Azure 区域。
同样，在此示例中，数据库镜像包含 TrakCare DB、TrakCare
Analytics 和 Integration 命名空间，这些都在一个镜像集群中。

TrakCare Azure 参考架构图 - 物理架构



另外，下图显示了该架构的逻辑图，包含架构所安装的相关高级软件产品及其功能用途。

TrakCare Azure 参考架构图 - 逻辑架构

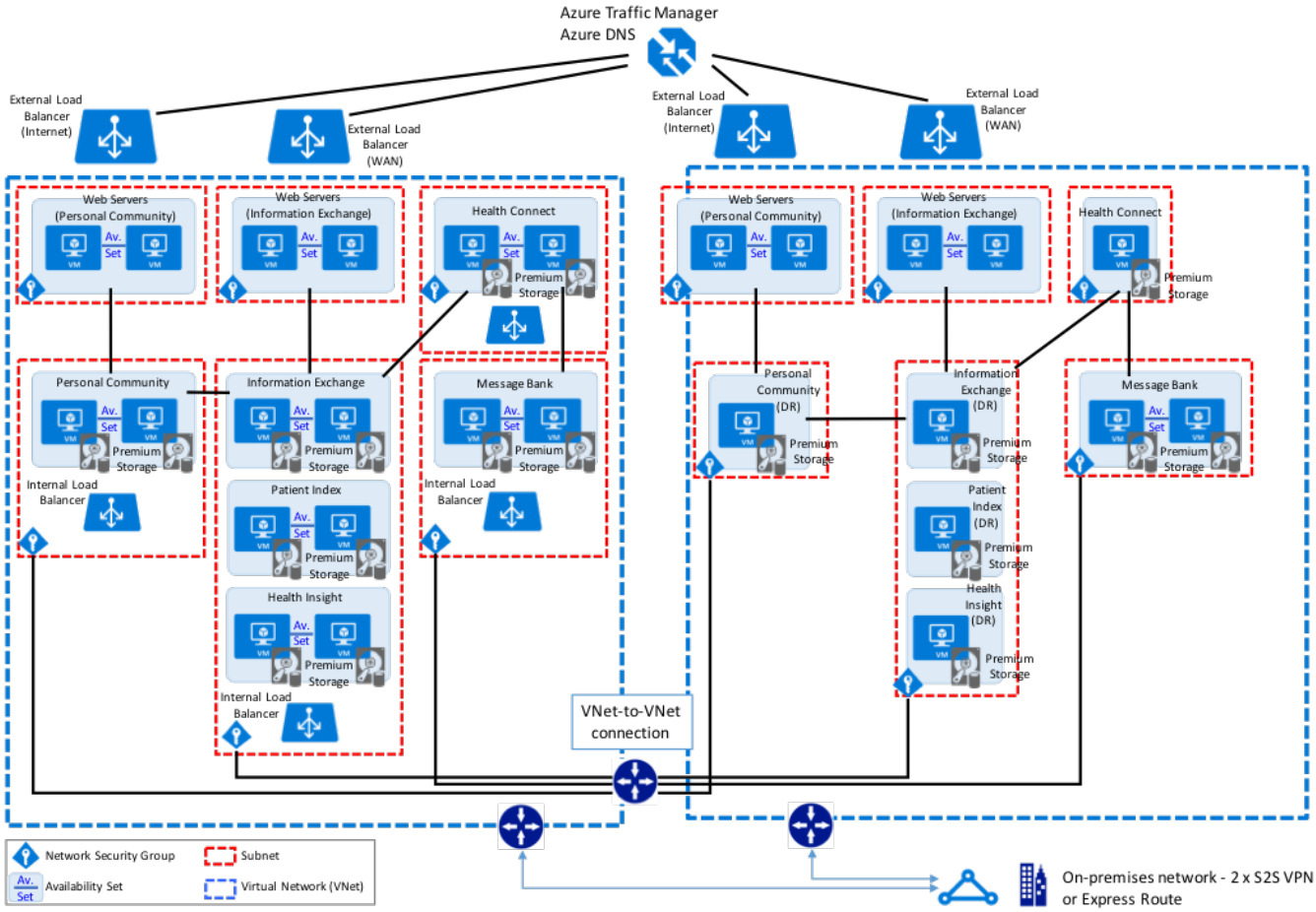


HealthShare 示例

下图显示了一个典型的 HealthShare 部署，其具有多个负载均衡 Web 服务器，以及多个 HealthShare 产品，包括 Information Exchange、Patient Index、Personal Community、Health Insight 和 Health Connect。
这些产品中的每一个都包含一对数据库镜像，以在 Azure 可用性集合中提供高可用性。
虚拟 IP 地址仅用于与 ECP 或 CSP 网关不关联的连接。 HealthShare 产品之间用于 Web 服务通信的 CSP 网关可感知镜像，不需要 VIP。

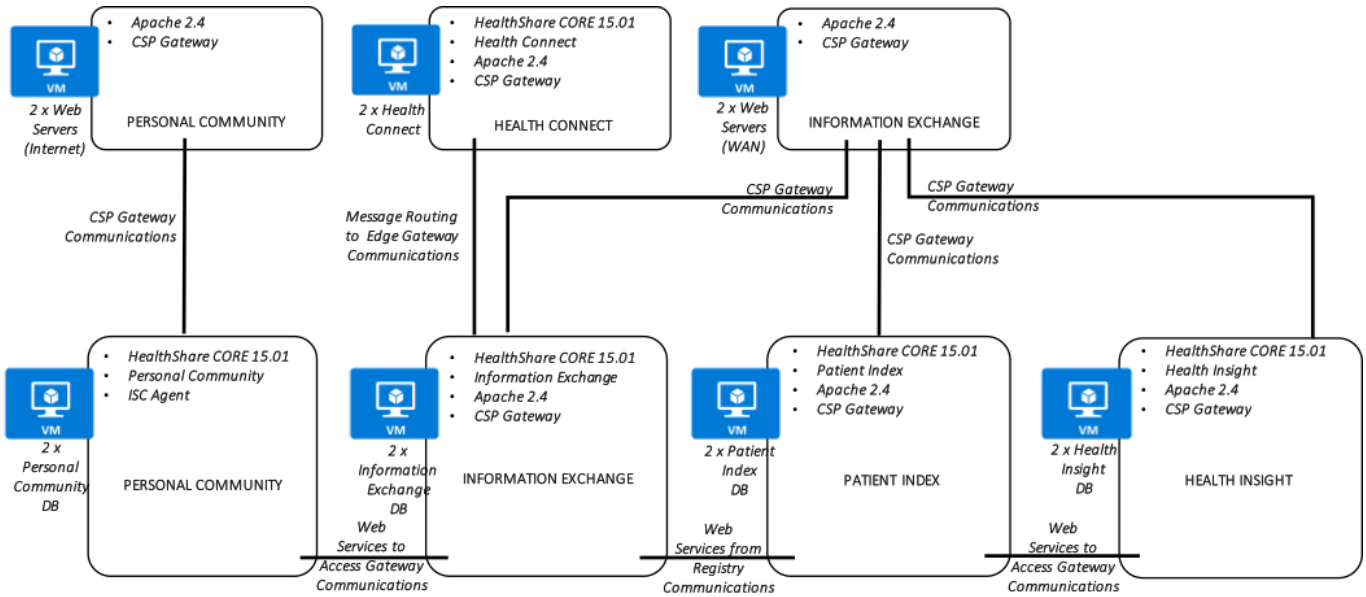
下图中的示例参考架构包括活动或主区域中的高可用性，可在主 Azure 区域不可用的情况下，执行灾难恢复到另一个 Azure 区域。

HealthShare Azure 参考架构图 - 物理架构



另外，下图显示了该架构的逻辑图，包含架构所安装的相关高级软件产品、连接要求、方法及相应的功能用途。

HealthShare Azure 参考架构图 - 逻辑架构



#Azure #InterSystems 业务解决方案和架构 #云 #镜像 #高可用性 #Caché #HealthShare #InterSystems IRIS

#InterSystems IRIS for Health

源URL:https://cn.community.intersystems.com/post/%E9%9D%A2%E5%90%91-microsoft-azure-resource-manager-arm-%E7%9A%84-intersystems-%E7%A4%BA%E4%BE%8B%E5%8F%82%E8%80%83%E6%9E%B6%E6%9E%84