Ashey, Bryce

Optum | Provider

Provider Integration Hub

Supporting legacy platforms

Contents

[Applicable Datacenters & Regional Hubs 3](#_Toc53324119)

[Two Subscriptions 3](#_Toc53324120)

[Statement of Overall Business Goal 3](#_Toc53324121)

[Use Case Definitions Supporting Integration Hub 4](#_Toc53324122)

[Future M&A Datacenter Connectivity 4](#_Toc53324123)

[Developer Access to Cloud Development Resources (Point-to-Site VPN) 4](#_Toc53324124)

[Production Support Access to Cloud Production Resources (Point-to-Site VPN) 4](#_Toc53324125)

[Legacy Domain Controller Support 4](#_Toc53324126)

[Virtual Machine Access Control (Non-Immutable Resources) 4](#_Toc53324127)

[Virtual Machine Configuration (Non-Immutable Resources) 5](#_Toc53324128)

[The Integration Hub is NOT… 5](#_Toc53324129)

[Provider Integration Hub 5](#_Toc53324130)

[Introduction 5](#_Toc53324131)

[Common Design [In Discovery] 7](#_Toc53324132)

[Integration Hub Virtual Network Design [In Discovery] 8](#_Toc53324133)

[Private Connectivity to Other Services 8](#_Toc53324134)

[The PIH Domain [In Discovery] 9](#_Toc53324135)

[Secure Integration 9](#_Toc53324136)

[DNS in the Integration Hub 9](#_Toc53324137)

[Ansible [In Discovery] 9](#_Toc53324138)

[Patching Maintenance [In Discovery] 9](#_Toc53324139)

[Integration Hub ITSM 10](#_Toc53324140)

[Requiring Infrastructure as Code 10](#_Toc53324141)

[Change Management 10](#_Toc53324142)

[Infrastructure Changes 11](#_Toc53324143)

[Observability [Discovery in Progress] 11](#_Toc53324144)

[Integration Hub: General Infrastructure Health 11](#_Toc53324145)

[Backup Methodology 11](#_Toc53324146)

[Disaster Recovery 11](#_Toc53324147)

[Chargeback Model [Discovery in Progress] 11](#_Toc53324148)

[Appendix A: Cost Detail 13](#_Toc53324149)

[Appendix B: IP Allocations 14](#_Toc53324150)

[References 15](#_Toc53324151)

# Applicable Datacenters & Regional Hubs

|  |  |  |
| --- | --- | --- |
| Common Name | M&A or UHG |  |
| Ashburn | M&A | VA730, VA729 |
| Austin | M&A | TX746 |
| Chaska | UHG | MN011 |
| Elk River | UHG | MN053 |
| Georgia RNH | UHG | GA777 |
| NTTA | M&A | VA732 |
| Pennsylvania | M&A | PA007 |
| Sommersville | M&A | MA710 |
| Tampa | M&A | FL750 |

# Two Subscriptions

ASK ID: **UHGWM110-026738**

|  |  |  |
| --- | --- | --- |
| Name | Prod? | Description |
| Integration Hub | Non-Prod | Used for pre-testing any infrastructure changes to the Integration Hub or any components contained within the Integration Hub. |
| Integration Hub | Prod | Host the virtual networks associated with the Integration Hub including the Shared Services virtual network and product specific shared service virtual networks (i.e. for legacy domain controllers). |

# Statement of Overall Business Goal

Provider, as a business, has elected to migrate out of all physical datacenters and move its entire platform onto one or more public cloud providers. This decision is based on the forecasted savings versus continuing to host Provider’s products in various M&A and “core” (Chaska/Elk River) datacenters. To this end, a large sum of L.E.G.O. funding is now available to the teams to facilitate rapid migration.

**During the course of executing this goal, Provider Engineering teams will continue to strive to move to highly isolated environments exposing HTTPS endpoints**. However, there will be instances where Provider chooses speed of migration over technology refactor. Likewise, there will be instances where refactor is not an option (e.g. vendor products). These exceptions are evaluated in each cost-benefit analysis and may be deemed acceptable given Provider’s overall goal of a purely cloud based infrastructure.

In addition to supporting hybrid, business partner, and employee access the Provider Virtual WAN will facilitate operation and maintenance of the systems that cannot be natively migrated. The following section outlines the various use cases, supported by the Virtual WAN, in greater detail.

# Use Case Definitions Supporting Integration Hub

## Future M&A Datacenter Connectivity

Provider must maintain the ability to integrate future merger & acquisition datacenters into Provider’s platform through both public and private network connectivity. To this end, Provider’s WAN infrastructure must support Site-to-Site VPN (including source/destination NAT) and dedicated line (e.g. ExpressRoute).

## Developer Access to Cloud Development Resources (Point-to-Site VPN)

As Provider’s entire platform shifts to the cloud Developers must be able to access resources that are hosted on both public and private endpoints in the cloud. These resources include databases, cache services, queue services, and other managed services. Access to these resources should be limited to the scope of the resources the team is working with (i.e. one product team should not be able to interact with another product team’s resources).

## Production Support Access to Cloud Production Resources (Point-to-Site VPN)

In similar fashion to developers, production support personnel need to access unmanaged databases and other resources in Production environments for both troubleshooting and maintenance. This access must be tightly controlled and must adhere to all compliance controls.

## Legacy Domain Controller Support

In some migration use cases the teams are unable to refactor their large (30+ terabytes) legacy database implementations within the time frame given for migration (in some cases that refactor is projected to take 3-5 years). This necessitates providing the ability to move those databases to the cloud over time while keeping the on-prem instance in-sync with the cloud instance. Unfortunately, technology limitations with Microsoft SQL Server require that both on-prem and cloud instances utilize the same domain for authentication. This, in-turn, requires that connectivity be maintained and protected for an extended, but still temporary, period.

## Virtual Machine Access Control (Non-Immutable Resources)

Most of Provider’s products adhere to one compliance paradigm or another; perhaps the most common paradigm being SOC2. As part of SOC2 and UHG’s own compliance policies there are a number of controls that are required for user access to virtual machines. These controls cover areas such as least privilege, disallowing shared logins, entitlement reviews, password strength policies, and many more. Any non-immutable unmanaged resources will need to adhere to these policies. Therefore, appropriate connectivity and resources must be created to meet this need.

## Virtual Machine Configuration (Non-Immutable Resources)

Unless under very dire exception all resources within a public cloud must be configured using Configuration as Code techniques. It is outside the scope of this document to describe the reasons why this is a minimum requirement however supporting the connectivity required to allow for Configuration as Code tools is very much within the scope of this document. It is most common for configuration tools (Chef, Puppet, Ansible, etc.) to operate over SSH for Linux and WinRM for Windows. Sufficient connectivity must be maintained to these resources to allow the configuration tools to operate.

## The Integration Hub is NOT…

To clarify before continuing, the Integration Hub is **not** meant to host product software implementations. The services hosted within the Integration Hub represent shared services where higher control is required to ensure proper security. An example would be controlling access to domain controllers required by one or more product virtual networks.

# Provider Integration Hub

## Introduction

The Provider Integration Hub (PIH) is a centralized location to support shared services which support the broader Provider platform. These shared services could be new to the cloud and facilitate a specific use case (i.e. the SQL proxy and email relay) or they could be services supporting legacy implementations that, for one reason or another, could not be migrated to a more native technology stack. These legacy implementations generally consist of virtual machines that may have third-party vendor applications on them that cannot run on anything other than a VM.

The nature of these implementations requires substantial infrastructure to handle their non-immutable configuration. This additional cost has been forefront on many discussions within Provider and is viewed in a strongly negative light. Therefore, visibility will be given to both the Provider COO and CTO on a monthly basis on those services that continue to reside on non-native technologies.

Examples of more legacy services would include legacy Domain Controllers required to enable SQL replication and Ansible for VM configuration as code. As mentioned above, the Integration Hub is not meant to provide a home for any product specific software applications; all services within the Integration Hub must be shared amongst two or more products to qualify for hosting within the Integration Hub.

To enforce this latter control, no product team will be able to deploy infrastructure to the Integration Hub. All deployments must go through the Provider Cloud Enablement team, the Provider DevOps Enablement team, or the production support team. Each unique service within the Integration Hub will be isolated within its own virtual network and connectivity will be enabled using the services established through the Provider Transit Hub (PTH) program.

Management of the services within the Integration Hub falls to the Provider DevOps Enablement team primarily with some duties falling to the Provider Cloud Enablement team. There may be situations where legacy datacenter personnel also manage the services within the Integration Hub. In all scenarios access will be managed via the ENTID domain.

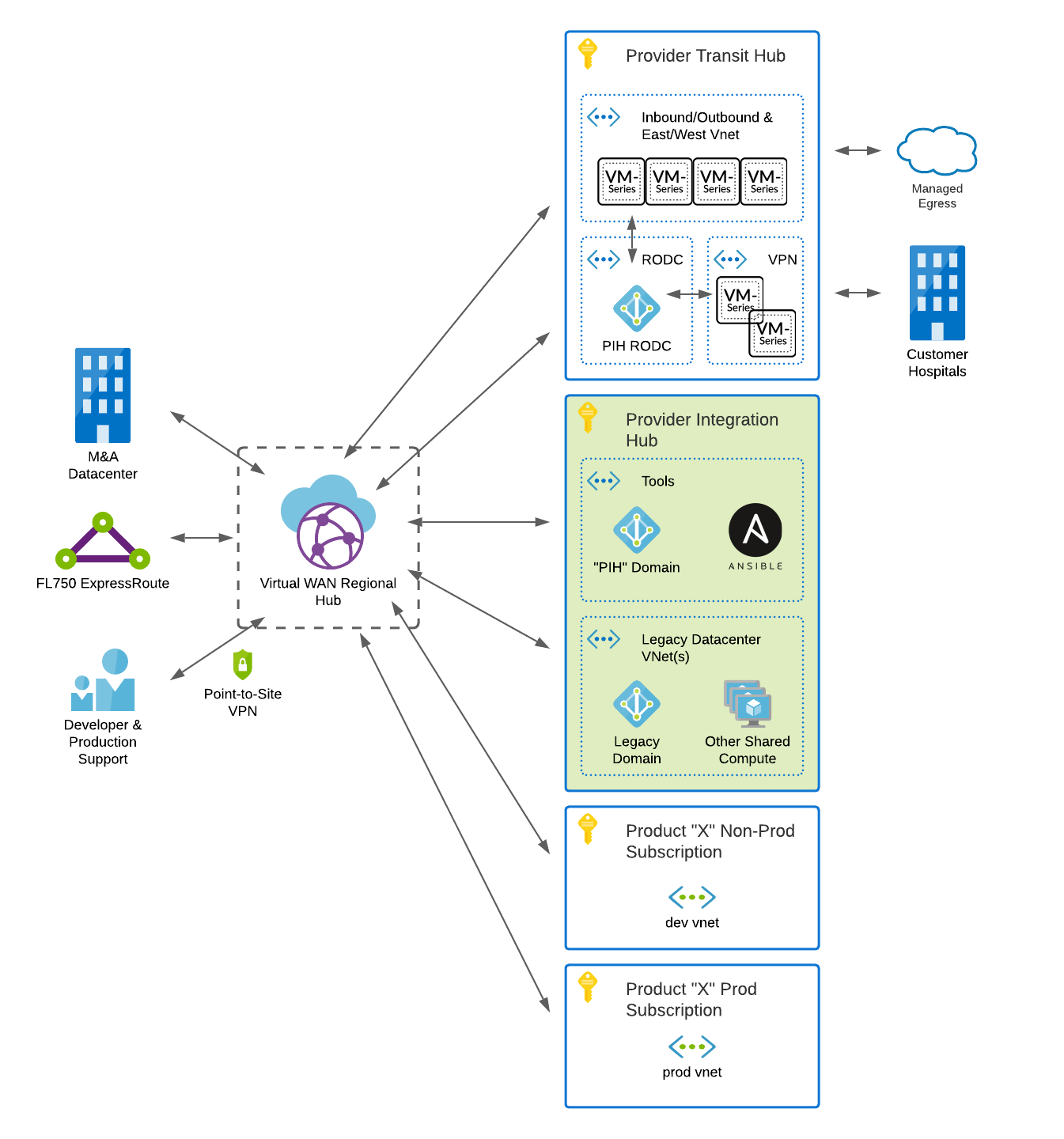


Figure : Provider Virtual WAN with Integration Hub highlighted

## Common Design [In Discovery]

The following table describes the resource groups utilized in the creation of the Provider Integration Hub.

|  |  |
| --- | --- |
| **Resource Group** | **Description** |
| p**i**h-<shared service name>-<namespace> | Contains the virtual network for the shared services being deployed. |
| p**i**h-<product name>-<namespace> | Contains any product specific shared services. Many instances expected. |

## Integration Hub Virtual Network Design [In Discovery]

Per EGRC policy 9D.1.02.01, the Integration Hub will provide a Tools virtual network that will host services common to Provider such as domain controllers, CI\CD tools, patch management, and more. The network is segmented into various subnets which will host services with similar function. The subnets will be isolated from each other and other virtual networks through the use of network security groups.

In the event that remote access to these services is needed Bastion will be used. Access will be controlled via Provider’s normal production access policies which adhere to all policies found in Section 8 of EGRC security policies.

Graphical user interface, application

Description automatically generated

Figure 2: Integration Hub Tools Virtual Network Detail

Some services may expose themselves via the public internet. In those cases, the services will be hosted in isolated virtual networks with no peering to other virtual networks.

## Private Connectivity to Other Services

In the majority of use cases, services within the Integration Hub will connect to other virtual networks via the Transit Hub’s use of Azure Virtual WAN and the associated regional hubs established therein. The methodology for this connectivity can be found within the [Transit Hub](https://github.optum.com/FICS-DEVOPS/azure-provider-transit-hub) documentation.

## The PIH Domain [In Discovery]

The Provider Cloud Enablement team spent extensive time and resources working to discover if there was support for managing logins and group policy via Azure Active Directory; unfortunately, the support that is currently available is very “young” and not yet available for most operating systems.

Due to this lack of functionality a traditional set of Domain Controllers and a traditional Active Directory domain will be established. This Domain will be named “pih.provider.engineering” or “PIH” for short. All virtual machines, which are not immutable, will be joined to this domain. This will allow the Provider operational team to push controls to virtual machines via Group Policy. These controls encompass many of the requirements in Sections 5, 8, and 12 of EGRC security policy.

### Secure Integration

The need to facilitate policy requirements such as annual entitlement reviews dictates that the PIH domain, if at all possible, be integrated with Secure. The Provider Cloud Enablement team has engaged the Secure team (RITM1194098) and will work to establish a common methodology for Secure integration with the cloud.

### DNS in the Integration Hub

Due to the functionality of Active Directory, the Domain Controllers will become the default DNS servers for all virtual machines in the Integration Hub, Transit Hub, and any virtual networks utilizing the Integration Hub services.

Azure will be listed as the upstream DNS provider for the PIH domain servers.

Research still needs to be completed in terms of integrating Azure Private DNS zones with Active Directory.

## Ansible [In Discovery]

While the preferred methodology, for virtual machines, is immutable images there are some services (skeletons?) in Provider’s technology landscape that cannot be easily migrated to an immutable deployment model. For these services, Ansible will be used.

Ansible will utilize SSH (TCP 22) and WinRM (using HTTPS: TCP 5986) and the aforementioned PIH domain credentials to push configuration changes to the virtual machines it manages.

## Patching Maintenance [In Discovery]

The Provider operational team is currently researching options for managing patches across the virtual machines. The team’s general guidance is that patching must accomplished at least monthly regardless of operating system. As with the Ansible service the patching server will leverage PIH domain credentials to log into servers under management.

# Integration Hub ITSM

Managing the operation and maintenance of Provider’s Virtual WAN falls to the Provider DevOps Enablement group, the production support team(s), production database administrators, and the Application Operations Center (AOC). The Provider Cloud Enablement team will provide support, guidance, and enhancements whenever and wherever there is a need. At the time of this writing those teams are managed by Bryan Moore, John Harrast, Girum Fida, and Chris Dutilly respectively. These teams will leverage the tools and processes outlined below to manage Provider’s Virtual WAN.

## Requiring Infrastructure as Code

Wherever and whenever possible it is expected that all changes will be implemented via code and deployed via a continuous delivery pipeline (such as Jenkins). In some cases, custom coding may be required to create the change via API. The Cloud Enablement team will strive to codify these more complex updates within the ProviderRM terraform provider.

In rare exceptions, for instance mapping fiber circuits to Azure ExpressRoute, changes can only be completed manually via the Azure Portal. When a change must be done manually that change must have detailed steps documented within the change ticket and must have a corresponding rollback plan. Manual changes must not subsequently break the terraform deployments (i.e. terraform state must be kept in sync or somehow exclude the manual changes).

## Change Management

Optum’s ServiceNow Change Management process will be leveraged to track all changes deployed to the Virtual WAN. This includes any changes to the Virtual WAN itself, firewall changes, Site-to-Site VPN changes, Point-to-Site VPN changes, and the creation or removal of any peering connections within the Virtual WAN. The following devices and device rollups will, initially, be registered with CMDB to allow for tracking of changes:

* Provider FL750 ExpressRoute (rollup for all circuits and devices)
* Provider Virtual WAN
* Provider Virtual WAN Point-to-Site VPN “NNN” (each unique VPN will have an entry)
* Provider Transit Hub Firewall (rollup for all four firewall devices)
* Provider Transit Hub VPN (rollup for both VPN devices)

As stated, this is an initial list and will change over time. CMDB should be considered the source of truth not this document. It is the responsibility of downstream services to manage their dependencies upon the above configuration items. This management can be accomplished through CMDB and Central CI located at <https://ask.optum.com>.

### Infrastructure Changes

All infrastructure changes will require a ServiceNow Change Management ticket with dependent configuration items added for all devices and/or rollups that are being affected by the change.

## Observability [Discovery in Progress]

### Integration Hub: General Infrastructure Health

In general, all systems within the Integration Hub will be monitored by Provider’s Splunk Suite of tools including SignalFx. The standard detectors for VM health (CPU, Memory, Disk, etc.) will be utilized. Any VM logs will be expected to be forwarded to Provider’s Event Hubs either directly or potentially via a Syslog forwarder. Custom detectors are of course encouraged on the platform.

## Backup Methodology

Virtual machines under the purview of the Integration Hub will utilize Azure Site Recovery to manage backups. Backups will always be stored in geo-redundant storage to ensure access is available should an entire Azure Region go offline.

## Disaster Recovery

The services within the Integration Hub will always span Azure Availability zones as the primary means of Disaster Recovery. This provides regional stability within a 300-mile disaster zone.

Should the disaster exceed that perimeter (or should an entire Azure Region go offline) then recovery will take the form of redeploying the network and infrastructure (via CI\CD) to another region. Services will be restored from Azure Recovery Vaults in the new region.

A test of the second scenario must occur at least once annually.

# Chargeback Model [Discovery in Progress]

Much like the other shared services (Splunk, SignalFx, email relay, SQL Proxy, etc.) offered in Provider’s portfolio the Integration Hub, Transit Hub, and any Virtual WAN services are designed to be billed based on usage. At the time of this writing the discussions with finance, operations, and other stakeholders are ongoing as to the exact mechanism with which to perform this chargeback. This section will be updated as that conversation continues.

# Appendix A: Cost Detail

# Appendix B: IP Allocations

10.225.160.0/20 – Original Allocation – Reserved for Product Virtual Networks and FL750 DR

10.225.215.0/20 – New allocation – Reserved for Virtual WAN, Integration Hub, and Transit Hub

# References

Microsoft. (2019, December 30). *Connect Palo Alto Networks to Azure Sentinel*. Retrieved from Microsoft Docs: https://docs.microsoft.com/en-us/azure/sentinel/connect-paloalto

Microsoft. (2020, September 22). *Scenario: Route traffic through NVAs - custom (Preview)*. Retrieved from Microsoft Docs: https://docs.microsoft.com/en-us/azure/virtual-wan/scenario-route-through-nvas-custom

Microsoft. (2020, September 22). *What is Azure Virtual WAN*. Retrieved from Microsoft Docs: https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

Microsoft Docs. (2020, July 06). *Tutorial: Detect threats out-of-the-box*. Retrieved from Microsoft Docs: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-built-in

Palo Alto. (2020, August 19). *Deployment Guide for Azure – Transit VNet Design Model.* Retrieved from Palo Alto Networks: https://www.paloaltonetworks.com/resources/guides/azure-transit-vnet-deployment-guide

Palo Alto. (2020, August 6). *Setup Active/Passive HA on Azure*. Retrieved from Palo Alto Tech Docs: https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-azure/configure-activepassive-ha-for-vm-series-firewall-on-azure.html

VictorOps. (2020, September 27). *Azure Monitoring Integration Guide*. Retrieved from VictorOps Help: https://help.victorops.com/knowledge-base/azure-monitoring-integration-guide-victorops/