Cloud Foundation Enterprise Design

This document contains confidential and proprietary information of Avanade and may be protected by patents, trademarks, copyrights, trade secrets, and/or other relevant state, federal, and foreign laws. Its receipt or possession does not convey any rights to reproduce, disclose its contents, or to manufacture, use or sell anything contained herein. Forwarding, reproducing, disclosing, or using without specific written authorization of Avanade is strictly forbidden.

The Avanade name and logo are registered trademarks in the US and other countries. Other brand and product names are trademarks of their respective owners.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Changes |
| 1 | 3/4/2021 | Jason Berg | Initial draft |
| 2 | 3/22/2021 | Jason Berg | Updated draft with internal review |
| 3 | 4/20/2021 | Virat Dogra | Updated AD DS and Spoke subnets and NSGs |
| 3.1 | 6/9/2021 | Harish Pattona | Added roles to the PIM session (Pg. 14 & 15) |
| 3.2 | 6/10/2021 | Michael Barilla | Updated NSGs and Subnets based on implementation |
| 3.2 | 7/2/2021 | Michael Barilla | Updated Network Peering section and Added User Defined Routes Section. Added Service Endpoints Section and updated DNS with Private DNS zone. |
| 3.2 | 7/11/2021 | Michael Barilla | Added On-Prem Connection Section with information for the US East VPN and ER. Updated UDR Intro. |
| 3.2 | 7/19/2021 | Michael Barilla | Updated West EU VPN and ER configurations. Added JV spokes into Spoke Design. Updated DNS section with Private DNS information. |
| 3.2 | 7/25/2021 | Farhan Ashraf | AD, DNS, MDE |
| 3.2 | 7/26/2021 | Harish Pattona | Backup policy and schedules |
| 3.3 | 7/28/2021 | Michael Barilla | Updated Edge Security Approach and included draft of firewall run book |
| 3.3 | 8/2/2021 | Harish Pattona | PIM eligible roles updated based on Job role |
| 3.4 | 8/2/2021 | Harish Pattona | Microsoft Defender ATP updated |
| 3.5 | 8/9/2021 | Harish Pattona | Added active services |
| 3.5 | 10/1/2021 | Michael Barilla | Updated Network Design based on Environment (HC Prod/Non prod |
| 3.6 | 10/6/2021 | Michael Barilla | Added Private Endpoint Documentation and updated Network Subnets as needed |
| 3.6 | 10/29/2021 | Michael Barilla | Updated Routing information for on-prem to private endpoint traffic |
| 3.7 | 03/01/2022 | Harish Pattona | Updated tagging policy |
| 3.8 | 5/13/2022 | Harish Pattona | Sandbox architecture |
| 3.9 | 8/2/2023 | Devika Pr | Updated for IAM and VWE |
| 3.10 | 5/17/2023 | Harish Pattona | Updated OU change in Active directory (Page 74) |
| 3.11 | 6/7/2023 | Ranjeet | Updated   * West US HUB details * SAP Spokes details * Private DNS Zones * Citrix w365 nva East US and West EU HUBs Details * Subscriptions * Peerings * AD groups * East US Local gateways * West EU Local gateways |

Table of Contents

[1 Introduction 4](#_Toc1254553757)

[1.1 What This Document Is 5](#_Toc644937113)

[1.2 What This Document Is Not 5](#_Toc1958481483)

[1.3 Audience 5](#_Toc598575240)

[1.4 Document Notes 5](#_Toc494748274)

[2 Cloud Governance 6](#_Toc1784104136)

[2.1 Avanade Recommendations 7](#_Toc1970201000)

[2.1.1 Align with the Business 7](#_Toc499545169)

[2.1.2 Access 7](#_Toc1233037722)

[2.1.3 Azure Regions 7](#_Toc547687606)

[2.1.4 Management group/subscription design 7](#_Toc1650227259)

[2.1.5 Resource group strategy 7](#_Toc1682508454)

[2.1.6 Naming convention 8](#_Toc1207582878)

[2.1.7 Cost Management 8](#_Toc708869191)

[2.1.8 Azure Policy 8](#_Toc1788466920)

[2.2 Design Decisions / Requirements 9](#_Toc2042164530)

[2.2.1 Access 10](#_Toc1203657589)

[2.2.2 Azure Regions 10](#_Toc725603283)

[2.2.3 Management Group/Subscriptions 10](#_Toc1852930452)

[2.2.4 Azure Policy 10](#_Toc488658971)

[2.2.5 Naming Conventions 12](#_Toc1825654994)

[2.2.6 Cost Management 15](#_Toc727400019)

[2.3 Design 15](#_Toc890287314)

[2.3.1 Access 15](#_Toc60017348)

[2.3.2 Azure Regions 20](#_Toc1915277603)

[2.3.3 Management Groups/Subscriptions 20](#_Toc1632797976)

[2.3.4 Azure Policy 22](#_Toc1395284505)

[2.3.5 Naming Conventions 25](#_Toc2133461375)

[2.3.6 Resource Groups 26](#_Toc259840959)

[2.3.7 Resource Locks 28](#_Toc2040125909)

[2.3.8 Cost Management 28](#_Toc2008229668)

[2.3.8.1 Reserved VM Instances 29](#_Toc478738467)

[2.3.8.2 Azure Hybrid Use Benefit 29](#_Toc102167471)

[2.3.8.3 Auto Shutdown 29](#_Toc570203229)

[2.3.8.4 Azure Advisor 30](#_Toc1294929164)

[2.3.8.5 Azure Cost Analysis 30](#_Toc623266625)

[2.3.8.6 Azure Budgets 30](#_Toc1401497208)

[2.3.8.7 Cost Management Using Power BI 30](#_Toc1201696185)

[3 Network 31](#_Toc334372641)

[3.1 Avanade Recommendations 32](#_Toc544677387)

[3.1.1 Connectivity 32](#_Toc388982914)

[3.1.2 Remote Access 32](#_Toc1659048580)

[3.1.3 Vnets and subnets 32](#_Toc383649786)

[3.1.4 Network Security 32](#_Toc1483359496)

[3.2 Design Decisions / Requirements 32](#_Toc1165129657)

[3.2.1 Connectivity 32](#_Toc2142764318)

[3.3.1 Vnets and Subnets 33](#_Toc1299205102)

[3.3.2 Network Security 33](#_Toc619549258)

[3.3 Design 33](#_Toc638452445)

[3.3.1 Connectivity 33](#_Toc1962300797)

[3.3.2 High-level Vnet design 33](#_Toc1599214317)

[3.3.3 IP Addressing 34](#_Toc1263956047)

[3.3.3.1 On-Premises Addressing 34](#_Toc1748744836)

[3.3.3.2 Azure Addressing 34](#_Toc1098415227)

[3.3.4 Hub Design 40](#_Toc191202470)

[3.3.4.1 High-Level Design 40](#_Toc1957078245)

[3.3.4.2 East US HUB 41](#_Toc123821016)

[Function-App1-10.124.2.128-27 41](#_Toc1906454898)

[DomainJoin-10.124.2.192-27 41](#_Toc1858527497)

[Domain Join 41](#_Toc349879647)

[3.3.4.3 West Europe HUB 42](#_Toc825272063)

[3.3.4.4 West US HUB 43](#_Toc1839029128)

[3.3.5 Spoke Design 44](#_Toc1094541889)

[3.3.5.1 High-Level Design 44](#_Toc560705700)

[3.3.5.2 East US Prod Spoke 44](#_Toc1447743518)

[3.3.5.3 East US NonProd Spoke 45](#_Toc327031824)

[3.3.5.4 East US HC Prod Spoke 46](#_Toc8733405)

[3.3.5.5 East US HC NonProd Spoke 46](#_Toc773205049)

[3.3.5.6 West EU Prod Spoke 47](#_Toc1365661498)

[3.3.5.7 West EU NonPod Spoke 47](#_Toc115452546)

[3.3.5.8 West EU HC Prod Spoke 49](#_Toc1076454912)

[3.3.5.9 West EU HC Non-Prod Spoke 49](#_Toc979240376)

[3.3.5.10 Joint Venture Prod Spoke 50](#_Toc295546462)

[3.3.5.11 Joint Venture NonProd Spoke 50](#_Toc1688890629)

[3.3.5.12 VWE Non Prod Spoke 51](#_Toc405085765)

[3.3.5.13 SAP PreProd Spoke 51](#_Toc2028283980)

[3.3.5.14 SAP Prod Spoke 52](#_Toc1688605875)

[3.3.5.15 SAP Non Prod Spoke 52](#_Toc138966919)

[3.3.5.16 1.1.1.1 SPK3-TESTING-US 52](#_Toc760904615)

[3.3.5.17 1.1.1.2 NIC-bhazl04110006d-001 53](#_Toc1390462038)

[3.3.5.18 1.1.1.3 SPK3-TESTING-WESTUS 53](#_Toc598701715)

[3.3.5.19 1.1.1.4 BHCAzureC- EastUS-dev-01 53](#_Toc689342255)

[3.3.5.20 1.1.1.5 BHCAzureC-EastUS-dev-02 54](#_Toc340490556)

[3.3.5.21 1.1.1.6 BHCAzureC-EastUS-dev-09 55](#_Toc1385225045)

[3.3.5.22 1.1.1.7 BHCAzureC-EastUS-dev10-10 55](#_Toc770712323)

[3.3.5.23 1.1.1.8 BHCAzureC-EastUS-preprod-01 56](#_Toc1598703065)

[3.3.5.24 1.1.1.9 BHCAzureC-EastUS-preprod-04 56](#_Toc1714956701)

[3.3.5.25 1.1.1.10 BHCAzureC-EastUS-prod-01 57](#_Toc893335267)

[3.3.5.26 1.1.1.11 BHCAzureC-EastUS-prod-02 57](#_Toc191117635)

[3.3.5.27 1.1.1.12 BHCAzureC-EastUS-prod-09 58](#_Toc695176709)

[3.3.5.28 1.1.1.13 BHCAzureC-WestEU-dev-01 59](#_Toc566772409)

[3.3.5.29 1.1.1.14 BHCAzureC-WestEU-dev-02 59](#_Toc787423952)

[3.3.5.30 1.1.1.15 BHCAzureC-WestEU-dev-12 60](#_Toc1748169791)

[3.3.5.31 1.1.1.16 BHCAzureC-WestEU-dev-13 61](#_Toc69620611)

[3.3.5.32 1.1.1.17 BHCAzureC-WestEU-dev11-11 63](#_Toc210331862)

[3.3.5.33 1.1.1.18 BHCAzureC-WestEU-preprod-02 63](#_Toc753379540)

[3.3.5.34 1.1.1.19 BHCAzureC-WestEU-prod-02 64](#_Toc1847858654)

[3.3.5.35 1.1.1.20 BHCAzureC-WestEU-prod-04 65](#_Toc911682365)

[3.3.5.36 1.1.1.21 BHCAzureC-WestUS-prod-01 66](#_Toc1262796405)

[3.3.5.37 1.1.1.22 DBKSCM-Prod-EastUS 66](#_Toc1900174993)

[3.3.5.38 1.1.1.23 DBKSCM-Prod-WestEU 67](#_Toc740970989)

[3.3.5.39 1.1.1.24 IAM\_C3\_Dev\_Non\_Prod\_westeu 67](#_Toc413376932)

[3.3.5.40 1.1.1.25 IAM\_C3\_PreProd\_westeu 68](#_Toc738352952)

[3.3.5.41 1.1.1.26 IAM\_Dev\_NON\_PROD\_WestEU 68](#_Toc607963589)

[3.3.5.42 1.1.1.27 IAM\_Pet\_Non\_Prod\_EastUS 69](#_Toc781532057)

[3.3.5.43 1.1.1.28 IAM\_PreProd\_EastUS 70](#_Toc1431434769)

[3.3.5.44 1.1.1.29 \_IAM\_Prod\_EastUS 71](#_Toc749541388)

[3.3.5.45 1.1.1.30 iam\_qa\_non\_prod\_EastUS 71](#_Toc2062638207)

[3.3.5.46 1.1.1.31 Non\_HC\_PreProd\_EastUS 72](#_Toc1045146161)

[3.3.5.47 1.1.1.32 Non\_HC\_PreProd\_WestEU 73](#_Toc1915697858)

[3.3.5.48 1.1.1.33 SAP\_ANF\_Prod\_USEast 74](#_Toc1895597816)

[3.3.5.49 1.1.1.34 SAP\_ANF\_ProdDR\_WestUS 74](#_Toc300345614)

[3.3.5.50 1.1.1.35 Trials\_BHC3\_Dev\_Non\_Prod\_EastUS 75](#_Toc2045763293)

[3.3.5.51 1.1.1.36 Trials\_BHC3\_Pre-Prod\_EastUS 75](#_Toc306244705)

[3.3.5.52 1.1.1.37 VWE\_PROD\_EastUS 76](#_Toc55408917)

[3.3.5.53 1.1.1.38 . VWE\_PROD\_WestEU 77](#_Toc405813686)

[3.3.6 Peerings 78](#_Toc1574760962)

[3.3.6.12 Hub to Spoke Peering 78](#_Toc1258926213)

[3.3.6.13 Spoke to Hub Peering 82](#_Toc1253972946)

[3.3.6.14 Hub to Hub Peering 84](#_Toc399408908)

[3.3.7 On-Premises Connectivity 84](#_Toc802341142)

[3.3.7.12 ExpressRoute 84](#_Toc1443310408)

[Connection: CX-ER-USWest 88](#_Toc1406158676)

[3.3.7.13 VPN Tunnel 88](#_Toc131068893)

[Local Gateway1 : Local-HUB-USWest-GW 92](#_Toc1354940666)

[Connection: CX-VPN-USWest 92](#_Toc1430468829)

[Local Gateway: Local-HUB-USWest-GW2 93](#_Toc1418247410)

[Connection: CX-VPN-USWest2 93](#_Toc2078982349)

[3.3.8 User Defined Routing 93](#_Toc285203002)

[3.3.8.12 Hub Route Tables 94](#_Toc1207459346)

[Route Table Route\_HUB\_Citrix\_w365\_nva\_GatewaySubnet has the following configuration: 98](#_Toc1095553353)

[3.3.8.13 Spoke Route Tables 99](#_Toc1435607824)

[3.3.9 Service Endpoints (a.k.a. Public Endpoints) 108](#_Toc1164906035)

[3.3.10 Private Endpoints 109](#_Toc847871032)

[3.4 Security 110](#_Toc1672361952)

[3.4.1 Edge security approach 110](#_Toc1797045831)

[3.4.1.12 Azure Firewall 110](#_Toc2030644557)

[3.4.2 Inter-subnet security approach 110](#_Toc1826214344)

[3.4.3 Internet egress approach 111](#_Toc1132855803)

[3.4.4 Governance 111](#_Toc451668428)

[4 Identity 112](#_Toc1354591615)

[4.1 Avanade Recommendations 113](#_Toc608034679)

[4.1.1 Azure AD 113](#_Toc604146056)

[4.1.2 Privileged Role Assignments/Administrative Accounts 113](#_Toc403895611)

[4.1.3 User and Group Management 113](#_Toc1908261350)

[4.1.4 DeterSynchronization 113](#_Toc1511343879)

[4.1.5 External Identities 113](#_Toc277775801)

[4.1.6 Extending AD DS into Azure 113](#_Toc1976189160)

[4.2 Design Decisions/Requirements 113](#_Toc1746786611)

[4.2.1 Azure AD 113](#_Toc1555699465)

[4.2.2 Privileged Role Assignments/Administrative Accounts 113](#_Toc2138308453)

[4.2.3 User and Group Management 113](#_Toc1021329083)

[4.2.4 Synchronization 114](#_Toc801135313)

[4.2.5 External Identities 114](#_Toc305786310)

[4.2.6 Extending AD DS into Azure 114](#_Toc347888536)

[4.3 Design 114](#_Toc1728959002)

[4.3.1 Azure AD 114](#_Toc1768844683)

[4.3.2 Privileged Identity Management 114](#_Toc716753759)

[4.3.3 Extending AD DS into Azure 115](#_Toc1692589847)

[4.3.3.1 Domain Controller Build 116](#_Toc729966335)

[4.3.3.2 High Availability 117](#_Toc909816216)

[4.3.3.3 Storage 117](#_Toc519524042)

[4.3.3.4 Encryption 117](#_Toc1084246639)

[4.3.3.5 Patch Management 117](#_Toc1441374982)

[4.3.3.6 DC Access from Azure 117](#_Toc296817050)

[4.3.3.7 Time Sync 118](#_Toc1170142088)

[4.3.3.8 AD Site 118](#_Toc2062301457)

[4.3.3.9 Autoscaling and Temporary Workloads 118](#_Toc1852687810)

[4.3.4 DNS 118](#_Toc638270472)

[4.3.4.2 DNS Diagram 121](#_Toc1669039015)

[5 Security 121](#_Toc1537883819)

[5.1 Avanade Recommendations 122](#_Toc478859798)

[5.1.1 Network Security 122](#_Toc684825146)

[5.1.2 Identity Management 122](#_Toc101325997)

[5.1.3 Monitoring and Incident Management 122](#_Toc719197341)

[5.1.4 Data Protection 122](#_Toc2088933179)

[5.2 Design Decisions/Requirements 122](#_Toc1230906326)

[5.2.1 Network Security 122](#_Toc1524500097)

[5.2.2 Identity Management 123](#_Toc479700179)

[5.2.3 Data Protection 123](#_Toc97844508)

[5.2.4 Monitoring and Incident Management 123](#_Toc1145346802)

[5.2.5 Vulnerability Management 124](#_Toc1565121386)

[5.2.6 Endpoint Security 124](#_Toc379076922)

[5.3 Design 124](#_Toc234954995)

[5.3.1 Network Security 125](#_Toc493055399)

[5.3.1.1 Network Security Groups 125](#_Toc1383966476)

[5.3.1.2 Azure Firewall 125](#_Toc1440601895)

[5.3.1.3 Azure DDoS 125](#_Toc108681069)

[5.3.2 Identity Management 125](#_Toc1072896842)

[5.3.2.1 Defender for Identity 125](#_Toc1179145889)

[5.3.2.2 Identity Protection 126](#_Toc144021946)

[5.3.2.3 Multi-Factor Authentication 127](#_Toc519241138)

[5.3.2.4 Privileged Identity Manager (PIM) 127](#_Toc304458377)

[5.3.3 Data Protection 127](#_Toc25014631)

[5.3.3.1 Azure Policies 127](#_Toc2092229425)

[5.3.3.2 Encryption 128](#_Toc1562577181)

[5.3.3.3 Storage Accounts 128](#_Toc733457130)

[5.3.4 Monitoring and Incident Management 128](#_Toc1199142534)

[5.3.5 Security Center 128](#_Toc1538494491)

[5.3.6 Azure Sentinel 130](#_Toc909619254)

[5.4 Vulnerability Management 132](#_Toc164870345)

[5.5 Endpoint Security 132](#_Toc585641759)

[5.5.1 Microsoft Defender for Endpoint 132](#_Toc1600188981)

[Antivirus for Windows and Linux VMs 133](#_Toc1744643955)

[6 VMs, Storage, and Backup 134](#_Toc1321066435)

[6.1 Avanade Recommendations 135](#_Toc295037186)

[6.1.1 VMs 135](#_Toc1668445285)

[6.1.2 Storage 135](#_Toc213614613)

[6.1.3 Backup 135](#_Toc1894446401)

[6.2 Design Decisions / Requirements 141](#_Toc919776520)

[6.3 Design 141](#_Toc722066011)

[6.3.1 VMs 141](#_Toc2111659561)

[6.3.2 Backups 142](#_Toc606965762)

[6.3.3 Snapshots 142](#_Toc2055093945)

[6.3.4 High Availability 142](#_Toc866004185)

[7 Disaster Recovery 143](#_Toc214318131)

[7.1 Avanade Recommendations 144](#_Toc1522880506)

[7.2 Design Decisions/Requirements 144](#_Toc1475801374)

[7.3 Design 144](#_Toc2136785917)

[8 Operations 144](#_Toc2136847672)

[8.1 Avanade Recommendations 145](#_Toc1959634746)

[8.1.1 -Logging and Monitoring 145](#_Toc1906730322)

[8.1.2 For AV for VMs 145](#_Toc268370151)

[8.1.3 Patch Management 145](#_Toc1517944696)

[8.1.3.1 Azure Update Management High Level Overview 145](#_Toc1925222088)

[8.1.3.2 OS Requirements 146](#_Toc144520281)

[8.1.3.3 RBAC Access 146](#_Toc980514663)

[8.1.3.4 Limitations 147](#_Toc1152073300)

[8.1.3.5 Network Requirements 147](#_Toc477692677)

[8.1.3.6 Schedule 149](#_Toc155620816)

[8.1.4 Infrastructure as Code 150](#_Toc185590725)

[8.1.5 Service introduction 150](#_Toc1057935632)

[8.1.6 IT Service Management 150](#_Toc460816346)

[8.1.7 SMTP 150](#_Toc1789661337)

[8.1.8 Active Services in use (Dynamic list) 151](#_Toc115284823)

[9 Sandbox design and architecture 154](#_Toc899130038)

[9.1.1 IP Addressing 155](#_Toc1854761585)

[a. On-Premises Ranges 155](#_Toc1622927859)

[b. Sandbox Ranges 155](#_Toc266176238)

[9.1.2 Hub Design 155](#_Toc1779784139)

[c. High Level Design 156](#_Toc1418266422)

[d. US East Hub 156](#_Toc227294639)

[e. West Europe Hub 156](#_Toc1653967570)

[9.1.3 Spoke Design 156](#_Toc306038699)

[f. High Level Design 156](#_Toc1512733588)

[g. US East Spoke 157](#_Toc1602070359)

[h. Bastion 157](#_Toc1868503118)

[East US IP - 10.22.161.197 157](#_Toc361953594)

[i. West Europe Spoke 157](#_Toc136270089)

[9.1.4 Connectivity 158](#_Toc386609538)

[j. On-Prem 158](#_Toc971855543)

[i. ExpressRoute 158](#_Toc1678585)

[ii. VPN Tunnel 158](#_Toc2122167061)

[k. Peering 158](#_Toc618577826)

[i. Hub to Spoke Peering 158](#_Toc785851311)

[ii. Spoke to Hub Peering 158](#_Toc1695459204)

[iii. Hub-Hub 158](#_Toc163342952)

[l. Routing 159](#_Toc1428335551)

[i. Hub Route Tables 159](#_Toc1866753849)

[9.1.4.1 GatewaySubnet 159](#_Toc1023159542)

[9.1.4.2 AzureFirewallSubnet 159](#_Toc115540649)

[9.1.4.3 AzureBastionSubnet 160](#_Toc1167670469)

[9.1.4.4 SharedServicesSubnet 160](#_Toc436975203)

[9.1.4.5 AppGatewaySubnet 161](#_Toc1197984867)

[ii. Spoke Route Tables 161](#_Toc1410921792)

[9.1.4.6 FrontEndSubnet & BackEndSubnet 161](#_Toc414451494)

[9.1.4.7 AppGatewaySubnet 162](#_Toc707325085)

[9.1.4.8 SqlMISubnet 162](#_Toc2021209413)

[9.1.4.9 PrivateLinkSubnet 163](#_Toc655783483)

[9.1.5 Security 163](#_Toc1835850073)

[m. Network Security Groups 163](#_Toc2078147559)

[i. Hub Networks 163](#_Toc1613451492)

[9.1.5.1 GatewaySubnet 163](#_Toc1782702588)

[9.1.5.2 AzureFirewallSubnet 163](#_Toc1949830779)

[9.1.5.3 AzureBastionSubnet 163](#_Toc616214889)

[9.1.5.4 SharedServicesSubnet 164](#_Toc1976951558)

[9.1.5.5 AppGatewaySubnet 164](#_Toc1205541289)

[ii. Spoke Networks 164](#_Toc1879886472)

[9.1.5.6 FrontEndSubnet 164](#_Toc1058229401)

[9.1.5.7 BackEndSubnet 164](#_Toc742900178)

[9.1.5.8 AppGatewaySubnet 164](#_Toc964512325)

[9.1.5.9 SqlMISubnet 164](#_Toc2061786760)

[9.1.5.10 PrivateLinkSubnet 164](#_Toc1322686158)

[n. Firewall 164](#_Toc1001696027)

[i. Network Rules 164](#_Toc65359305)

[9.1.5.11 Service Tags 165](#_Toc712411073)

[9.1.5.12 Network Deny Rules 165](#_Toc1868878637)

[9.1.5.13 Network Allow Rules 165](#_Toc1816711761)

[ii. Application Rules 165](#_Toc1055256549)

[9.1.5.14 Web Categories 165](#_Toc106953082)

[9.1.5.15 FQDN Rules 165](#_Toc640586354)

[iii. SNAT Rules 165](#_Toc1664583405)

# Introduction

This document details the security and governance workshop conducted from <Removed>. This document describes the current state of the Subscription model in Azure, the network connectivity design as it applies to those Subscriptions, and the Identity and Access design. It also follows with recommendations around future state for each of these areas, additional areas of governance that can be applied to the Subscription model, storage recommendations, and logging and monitoring recommendations based on discussed pain points.

## What This Document Is

This document is a recommendation document covering several areas of guidance as they apply to client based on Avanade/Microsoft recommended practices as well as the requirements discussed during the workshop that are unique to this organization.

## What This Document Is Not

This document is not an infrastructure design or deployment document. It does not discuss deployment process, effort, or duration. This document also does not address application architecture patterns or designs.

## Audience

This document assumes a 300-level knowledge of Azure concepts and services.

**Level 300**: Advanced material. In-depth understanding of features in a real-world environment, and strong coding skills. Provides a detailed technical overview of a subset of product/technology features, covering architecture, performance, migration, deployment, and development.

## Document Notes

Throughout the document Avanade will summarize the outputs of each section. These outputs can be categorized under the following headings:

|  |  |
| --- | --- |
|  | ***Note***  *This header is to make the reader aware of something specific in the document and will give some additional context to the section.* |

|  |  |
| --- | --- |
|  | ***Important Note***  *This header is to ensure the reader is fully aware of the point being highlighted. The information provided should be fully considered when understanding the context of the section.* |

|  |  |
| --- | --- |
|  | ***Recommendation***  *A recommendation being made by Avanade, but not necessarily a design decision.* |

|  |  |
| --- | --- |
|  | ***Assumption***  *Based on the workshops and knowledge of client infrastructure, assumptions on configurations and requirements are listed.* |

|  |  |
| --- | --- |
|  | ***Design Decision***  *A design decision based on client requirements and Avanade/Microsoft recommended best practices.* |

# Cloud Governance



## Avanade Recommendations

### Align with the Business

* Have a cloud strategy that addresses the business drivers the business is looking to achieve by going to Azure
* Create a cloud center of excellence that has clear goals and objectives and individuals to driving the cloud adoption

### Access

* Keep management group and subscription level RBAC assignments to a minimum
* Use resource groups to delegate administrative authority.
* Manage RBAC assignments either through individual assignments or Azure AD group assignments. Avoid, where possible, making group assignments in AD DS and using the synchronized Azure AD group for RBAC assignments.
* Only use Azure AD accounts for RBAC assignments (as opposed to Microsoft accounts)
* Make all RBAC assignments (higher than Reader) temporary (assigned through PIM)
* Read-only at the subscription level
* Balance between IT security and control and user experience. Poor user experiences typically generate service desk calls.
* Use custom roles when a built-in role is too broad or delegates too much authority
  + Network consumer
  + Security Incident
* Use custom roles sparingly

### Azure Regions

* Follow the Azure fabric regional pairing for primary/secondary for ease of access to geo-redundant resources. There are specific cases when availability of specific resource types (HANA large instances, for example) force acceptance of using non-paired regions

### Management group/subscription design

* Keep the number of subscriptions as low as possible
* Use management groups to group subscriptions that have common RBAC and/or policy application
* Keep the number of management group/subscription privileged RBAC assignments to a minimum
* Use a top-level MG to apply security policies to all subscriptions / environments.
* Don’t create a MG for a single subscription unless to plan for growth or separate business entity.
* Have a well-defined criterion for creating new management groups/subscriptions
  + Business requirement
  + Technical limitation (number of RGs for example)
  + Approval by architectural board

### Resource group strategy

* One resource group per application per environment.
* Maintain a separate resource group for infrastructure resources (Vnets, DCs, etc.)
* Use the Delete resource lock on resource groups housing key resources (infrastructure, prod apps, etc.).
  + Have your CI/CD pipeline remove the lock before deployment and replace it after deployment
* Create a tag taxonomy.
* Enforce tag use through Azure Policy.
* Recommended tags:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tag Name | State | Description | Tag Value | Example |
| AppTaxonomy | Required | Documents who own the resource group what purpose it serves within their organization | Organization\Team | Finance\Payroll\TaxApp |
| EnvironmentType | Required | Documents how the resource group is to be used | Dev, Test, UAT, Prod, etc. | Test |
| BillingIdentifier | Required | Designates a charge code or other billing identifier for reporting or charge-back | Bill code, cost center, etc. | A12345 |

### Naming convention

* Use short, easy to read and remember names (i.e. there is an 80-character limit on scripting parameters, therefore, long names will cause issues when attempting to automate deployments, as we have already experienced)
* Use 10.124.1.88
* Don’t include data in the name that is available from other sources
  + Built-in metadata (resource type, region, etc.)
  + Tags (environment, cost center, owner, etc.)
* For VM names, be as consistent as possible with the on-premises server naming convention
* Account for resource-specific naming limitations (e.g., storage accounts)

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-name-rules>

* Microsoft recommendations (the examples regularly violate the above recommendations)

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/naming-and-tagging>

### Cost Management

* Use PowerBI Desktop w/ Azure Consumption Insights connector.
* Create a Power BI dashboard that is connected to Azure EA using the ACI connector. The dashboards will then display costs in multiple ways: monthly, month vs month, monthly drilldown, cost analysis per resource group, resource group drilldown, among others. Tags should be used in these dashboards as filters for further drilldown. Any modification should be made in Power BI Desktop before publishing it to Power BI Online.

|  |  |
| --- | --- |
|  | ***Recommendation***  *We recommend installing Power BI Desktop with the Azure* Consumption Insights connector *to view all the resources in the resource group and create a comprehensive dashboard for monitoring and analyzing the data in Azure Monitor.* |

### Azure Policy

* As an initial first step toward governing the new client landing zone, Avanade recommends the following Azure Policies at the Subscription Level (unless noted otherwise):
  + “Require a tag and its value on resource groups”
  + “Allowed locations”
  + “Allowed storage account SKUs”
  + “Allowed virtual machine size SKUs”
  + “Network Watcher should be enabled”
  + “A maximum of 3 owners should be designated for the subscription”
* Avanade does not recommend these Azure Policies:
  + Limit Public IP Addresses (Audit Mode)
    - Preferred Method – Install NSGs on every subnet (deny all inbound)
  + Force Naming Convention
    - This should only be implemented as a policy if all names for all resources have a consistent format
    - See our recommendations in the Naming Convention section 2.1.6 (above)
  + Password Policy – This should be implemented in Azure Active Directory
    - Account lockout duration: 30
    - Number of failed logon attempts allowed: 5
    - Reset failed logon attempts count after 30 minutes
    - Maximum password age (lifetime): 90 days
    - Minimum password length (characters): 7
    - Passwords must meet complexity requirements
  + MFA – This should be implemented in Active Directory
  + Blueprints and DSC – Azure DevOps CI/CD is the preferred method for desired state configuration / automation

## Design Decisions / Requirements

### Access

* BH to identify top level groups. Groups are already in place for RBAC.

### Azure Regions

* Require a region to support BH Datacenter in Texas and in Europe.

### Management Group/Subscriptions

* Create Subscription / Management Group Model
* Deploy Management Groups to support growth of subscriptions due to technical constraints (reaching limit of Resource Groups)
* MG/Subscription model to map to current AWS account setup.
* Subscriptions will map to zones: Prod, Non-Prod, HC Prod, HC Non-Prod, Infrastructure, Sandbox
* Dev subscriptions will not be implemented, only EA subscriptions will be deployed.

### Azure Policy

* Tagging policy will be deployed at top level MG
* Tags were supplied
* Recommendations to be provided
* Accenture Security Team will deploy Azure Policies
* Avanade recommends the following policies be applied:

|  |  |  |
| --- | --- | --- |
| Policy | Description | Recommended Scope |
| Require a tag and its value on resource groups | Enforces a required tag and its value on resource groups. | Management Group |
| Require a tag and its value on resources | Enforces a required tag and its value. Does not apply to resource groups. | Management Group |
| Deploy network watcher when virtual networks are created | This policy creates a network watcher resource in regions with virtual networks. You need to ensure existence of a resource group named NetworkWatcherRG, which will be used to deploy network watcher instances. | Management Group |
| Flow log should be configured for every network security group | Audit for network security groups to verify if flow log resource is configured. Flow log allows to log information about IP traffic flowing through network security group. It can be used for optimizing network flows, monitoring throughput, verifying compliance, detecting intrusions and more. | Management Group |
| Network interfaces should not have public Ips | This policy denies the network interfaces which are configured with any public IP. Public IP addresses allow internet resources to communicate inbound to Azure resources, and Azure resources to communicate outbound to the internet. This should be reviewed by the network security team. | Management Group |
| Network Watcher should be enabled | Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end-to-end network level view. Network diagnostic and visualization tools available with Network Watcher help you understand, diagnose, and gain insights to your network in Azure. | Management Group |
| RDP access from the Internet should be blocked | This policy audits any network security rule that allows RDP access from Internet | Management Group |
| SSH access from the Internet should be blocked | This policy audits any network security rule that allows SSH access from Internet | Management Group |
| Deploy Advanced Threat Protection on Storage Accounts | This policy enables Advanced Threat Protection on Storage Accounts. | Management Group |
| Secure transfer to storage accounts should be enabled | Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking | Management Group |
| Deploy default Microsoft IaaSAntimalware extension for Windows Server | This policy deploys a Microsoft IaaSAntimalware extension with a default configuration when a VM is not configured with the antimalware extension. | Management Group |
| Microsoft Antimalware for Azure should be configured to automatically update protection signatures | This policy audits any Windows virtual machine not configured with automatic update of Microsoft Antimalware protection signatures. | Management Group |
| Microsoft IaaSAntimalware extension should be deployed on Windows servers | This policy audits any Windows server VM without Microsoft IaaSAntimalware extension deployed. | Management Group |
| Only approved VM extensions should be installed | This policy governs the virtual machine extensions that are not approved. | Management Group |
| Require automatic OS image patching on Virtual Machine Scale Sets | This policy enforces enabling automatic OS image patching on Virtual Machine Scale Sets to always keep Virtual Machines secure by safely applying latest security patches every month. | Management Group |
| An activity log alert should exist for specific Administrative operations | This policy audits specific Administrative operations with no activity log alerts configured. | Management Group |
| An activity log alert should exist for specific Policy operations | This policy audits specific Policy operations with no activity log alerts configured. | Management Group |
| An activity log alert should exist for specific Security operations | This policy audits specific Security operations with no activity log alerts configured. | Management Group |
| Azure Monitor should collect activity logs from all regions | This policy audits the Azure Monitor log profile which does not export activities from all Azure supported regions including global. | Management Group |

### Naming Conventions

* Naming conventions proposed

|  |  |  |
| --- | --- | --- |
| Resource | Convention | Example |
| Subscription | <BH>\_<Data classification>\_<Env> | BH\_HC\_NON\_PROD1 |
| Resource Group | RG-< application>-<subscription>-location-dev  Exclude BH in the subscription name and no “-“  Maximum 60 characters | rg-petclinic-nonhcnonprod-eastus-dev |
| Vnet | [HUB/SPOKE-PROD/SPOKE-Env-NONPROD]-[Region]-## | HUB-EastUS2-01  SPOKE-NONPROD-EastUS2-01 |
| vNet | Spoke\_app\_env\_Prod/NonProd-Location | Spoke\_BHC3\_Dev\_NonProd\_EastUS |
| Automation Account | AA-<Region>-<Subscription>-## | AA-EastUS2-Infra1-01 |
| Subnet | SNET-Project name-Env-Use for  Maximum 32 characters | SNET-BHC3-Dev-AppsVM |
| Network interface (NIC) | NIC-<resource name>-<serialization> | NIC-Vmapp04p-01, NIC-DC01-01 |
| Public IP address | PIP-<resource name> | PIP-Vmapp04p |
| App Gateway (internal) | AGW-app-env-location | AGW-bhge-dev-eus |
| App Gateway (external) | Agw-external-location-env {subscription without BH} | AGW-External-WEU-NonHC-NonProd |
| Vnet Gateway | [Vnet Name]-GW-# | HUB-EastUS2-01-GW-1 |
| LB | LB-app-env | LB-Phantom-Portainer-dev |
| Storage Account | stvm<function><serialization><env> | stvmdb01p |
| VM | BHAZ<Linux/Windows><serialization><Env>  **Please refer to the table below to this one** | BHAZW00000001P |
| IP | IP- <resource name> | IP-Vmapp04p |
| Network Security Group (NSG) | [Subnet Name]-NSG | Infra-10.64.0.192-27-NSG |
| Application Security Group (ASG) | ASG-<resource/application>-<env> | ASG-app01-prod |
| Application | <application name>-<env> | App01-prod |
| Express Route | EX-<Provider>-<Connection City> | EX-Verizon-Fairfax |
| Connection | CX-Type(EX for ExpressRoute/VPN for VPN)-Region | CX-EX-East2 |
| Log Analytics | LOG-<Env>-### | LOG-EA-001 |
| Traffic Manager | TM-<application> | TM-Sitecore |
| SQL Server | App-env-sqlsrv-subscription | mji-dev-sqlsrv-nonprod |
| SQL managed instances | Bhazms{random}{env}  Env - t, d, p or sbx | bhazms0222001t |
| PostgreSQL | bhazpo{random}({env}  Env -t,d,p or sbx  **Please refer to the Paas DB table below to this one** | bhazpo0312001p |
| MySQL | bhazms {random}({env}  Env - t, d, p or sbx  **Please refer to the Paas DB table below to this one** | bhazms0410017q |
| Availability Set | AS-<application/tier>-<serialization> | AS-PaloAlto-001 |
| Azure Site Recovery Vault | ASR-<Subscription>-<region>-<serialization> | ASR\_ACC\_EA\_EAST2\_01, ASR\_ACC\_Dev\_Central\_01 |
| Azure Bastion | [Vnet Name]-Bastion | HUB-EastUS2-01-Bastion |
| Azure Firewall | [Vnet Name]-Firewall | HUB-EastUS2-01-Firewall |
| IP Groups | [Vnet Name]-[Subnet Name]-IpGroup | HUB-EastUS2-01-Infra-10.64.0.192-27-IpGroup |
| Route Table | Route-[HUB]-[Region]  Route-[Spoke]-[ENV]-[Region]-XX | Route-HUB-EastUS2  Route-Spoke-Prod—EastUS2-1 |
| Key Vault | KV-app-<Subscription>-## | KV-FW-Infra1-01 |
| DDOS Protection Plan | DDOS-<Subscription> | DDOS-Infra1 |
| cosmos dB | App##-service-environment | mji01-cosmosdb-preprod |
| Webapp | App##-service-environment | centrum-integrity01-webapp-mji-preprod |
| function app | App##-service-environment | mji01- funcApp -preprod |

Nomenclature for VM/DB

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | OS | Digit1 | Digit2 | Digit3 | Digit4 | Digit5 | Digit6 | Digit7 | Digit8 | Env Name |
| BHAZ | L/W | Subscriptions | Subscriptions | Location | Server Role | Random | Random | Random | Random | P/D/Q/T/PP |
|  | Linux |  |  |  | App |  |  |  |  |  |
|  | Windows |  |  |  | DB |  |  |  |  |  |
| BHAZ | L | A | A | 1 | 1 | 0 | 0 | 0 | 1 | D |
|  |  |  |  |  |  |  |  |  |  |  |

 PaaS DB:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | DB engine (MY for MySQL, PO for PostGre) | Digit1 | Digit2 | Digit3 | Digit4 | Digit5 | Digit6 | Digit7 | Digit8 | Env Name |
|  |  | Subscriptions | Subscriptions | Location | Server Role | Random | Random | Random | Random | P/D/Q/T /PP |
| BHAZ | PO |  |  |  |  |  |  |  |  |  |
| BHAZ | MS | A | A | 1 | 2 | 0 | 0 | 0 | 1 | D |
|  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Digit3 | | Digit4 | |
| East-US-DC1 | 1 | App | 1 |
| East-US-DC2 | 2 | DB | 2 |
| East-US-DC3 | 5 | Infra | 3 |
| West Europe-DC1 | 3 | Web | 4 |
| West Europe-DC2 | 4 | Middleware | 5 |
| West Europe-DC3 | 6 | Shared (DNS,DC) | 6 |
| West- US | 7 | PAAS | 7 |
| QatarCentral | 8 |  |  |

|  |  |  |
| --- | --- | --- |
| SUBSCRIPTION | Digit1 | Digit2 |
| BH\_INFRA\_1 | 1 | A |
| BH\_HC\_NON\_PROD1 | 2 | B |
| BH\_HC\_PROD1 | 3 | C |
| BH\_NON\_HC\_PROD1 | 4 | D |
| BH\_NON\_HC\_NON\_PROD1 | 5 | E |
| BH\_SANDBOX1 | 6 | F |
| BH\_JV\_NON\_PROD1 | 7 | G |
| BH\_JV\_PROD1 | 8 | H |
| BH\_INFRA\_VWE\_NON\_PROD | 9 | I |
| BH\_IAM\_NON\_PROD1 | A | J |
| BH\_INFRA\_VWE\_PROD1 | A | K |
| [BH\_IAM\_PROD1](https://portal.azure.com/) | A | L |
| [BH\_MARKETPLACE1](https://portal.azure.com/) | A | M |
| [BH\_BHC3\_NON\_PROD1](https://portal.azure.com/) | A | N |
| [BH\_BHC3\_PROD1](https://portal.azure.com/) | A | O |
| BH\_SAP\_NON\_PROD1 | A | P |
| BH\_SAP\_PROD1 | A | Q |
| BH\_SAP\_PREPROD1 | A | R |
| BH\_SAP\_PROD\_DR1 | A | S |
| PRD-SUB-000007 | B | B |
| PRE-SUB-000008 | B | C |
| BH\_NON\_HC\_PREPROD1 | 5 | F |
| BH\_HC\_PREPROD1 | A | U |

### Cost Management

* A cost management strategy will be deployed, including budget tools and reservations, auto-shutdown, and other cost savings strategies.

## Design

### Access

Access will be granted to user groups created in the BHI Master domain and synchronized to Azure AD. In addition, Privileged Identity Management (PIM) has been implemented and the user groups identified in the below table will be granted an eligible assignment with the administrative roles and an active assignment that will be a read role only. Users will be required to authenticate to the Azure Portal using their Azure AD account, Azure Multi-factor Authentication, and then activate the administrative role. Microsoft authenticator used for 2FA while activating PIM roles

Link to latest - [BH Azure Home - Azure Roles (sharepoint.com)](https://bakerhughes.sharepoint.com/sites/BHAzureHome/SitePages/Azure%20Roles.aspx)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Job Function** | ​**Scope** | **​Allowed to request** | ​**Eligible Assignment** | **Active Assignment** |  |  |  |  |  | ​**Role Name** |
| Cloud Operations | BH\_MG | ​Cloud Ops only | Contributor | Reader |  |  |  |  |  | BHCAzureAdmin |
| Security Network | Network Resource Groups | ​​Cloud Ops only | Network Contributor  Classic Network Contributor  CDN Endpoint Contributor  CDN Profile Contributor  DNS Zone Contributor  Private DNS Zone Contributor  Traffic Manager Contributor  Support Request Contributor | Reader |  |  |  |  |  | BHCAzureNetworkAdmin |
| Application Team | Resource Group | ​Application team ​Cloud Ops | Key Vault Administrator  Log Analytics Reader  Logic App Contributor  Logic App Operator  Monitoring Reader  Reader  Reader and Data Access  Storage Blob Data Contributor  Storage File Data SMB Share Contributor  Storage Queue Data Contributor  Storage Table Data Contributor  Tag Contributor  Support Request Contributor | Reader |  |  |  |  |  | BHCAzure\_<app\_ci>\_StandardUser\_<env> |
| ​Application Team | ​Resource Group | ​Application team ​Cloud Ops | ​Key Vault Administrator  Log Analytics Reader  Logic App Contributor  Logic App Operator  Monitoring Reader  Reader  Reader and Data Access  Storage Blob Data Contributor  Storage File Data SMB Share Contributor  Storage Queue Data Contributor  Storage Table Data Contributor  Tag Contributor  Support Request Contributor  **Azure Kubernetes Service Cluster User** | ​Reader |  |  |  |  |  | ​BHCAzure\_<app\_ci>\_StandardPlus\_<env> |
| Application Team | Resource Group (Sandbox only) | ​​Application team ​Cloud Ops | Contributor | Reader |  |  |  |  |  | BHCAzure\_<app\_ci>\_SandboxAdmin\_<env> ​ |
| ​Application Team | ​Spoke VNET associated to RG | ​Application team ​Cloud Ops | ​BH-NetworkAccessForNIC | ​ |  |  |  |  |  |
| ​Application Team | ​bhaz\_goldenimage\_gallery | ​Application team ​Cloud Ops | ​ | ​Reader |  |  |  |  |  |
| Application DevOPs | Resource Group (exception approval required) | ​​Application team ​Cloud Ops | Contributor | Reader |  |  |  |  |  | BHCAzure\_<app\_ci>\_DevOps\_<env> ​ |
| ​Application DevOPs | ​​Spoke VNET associated to RG | ​Application team ​Cloud Ops | ​BH-NetworkAccessForNIC | ​ |  |  |  |  |  |
| ​Application DevOPs | ​bhaz\_goldenimage\_gallery | ​Application team ​Cloud Ops | ​ | ​Reader |  |  |  |  |  |
| Cloud Operations | Subscription | ​​​Cloud Ops only | Virtual Machine Contributor  Network Contributor  Storage Account Contributor  Traffic Manager Contributor  Monitoring Contributor  Log Analytics Reader  Billing Reader  Key Vault Administrator  Support Request Contributor  Log Analytics Contributor  Automation Operator | Reader |  |  |  |  |  | BHCAzureOperations |
| Azure Backup Admin | Subscription | ​​​Cloud Ops only | Backup Contributor  Virtual Machine Contributor  Key Vault Administrator  Storage Account Contributor  Support Request Contributor   Log Analytics Contributor  Automation Operator | Reader |  |  |  |  |  | BHCAzureBackupAdmin |
| Azure PaaS DB Admin | Resource Group | ​​​Cloud Ops only | SQL Server Contributor  SQL Security Manager  SQL Managed Instance Contributor  SQL DB Contributor  Storage Account Contributor  Log Analytics Reader  Key Vault Administrator  Billing Reader  Automation Operator  Cost Management Contributor  Redis Cache Contributor  DocumentDB Account Contributor  CosmosRestoreOperator  CosmosBackupOperator  Cosmos DB Operator  Support Request Contributor   Log Analytics Contributor  Automation Operator | Reader |  |  |  |  |  | BHCAzureDBAdmin |
| Oracle DB Admin | Resource Group | ​​​Cloud Ops only | Storage Account Contributor  Log Analytics Reader  Key Vault Administrator  Billing Reader  Automation Operator  Cost Management Contributor  Virtual Machine User Login  Support Request Contributor   Log Analytics Contributor  Automation Operator | Reader |  |  |  |  |  | BHCAzureOracleAdmin |
| Oracle DB Admin | Subscription | ​​​Cloud Ops only | Support Request Contributor | Reader |  |  |  |  |  | BHCAzureOracleAdmin |
| ​Managed Security Services | ​BH\_MG | ​​​​Cloud Ops only | ​Resource Policy Contributor | ​ |  |  |  |  |  | ​BHCAzureSecurityPolicy |
| Managed Security Services | BH\_MG | ​​​Cloud Ops only | Security Admin  Azure Sentinel Contributor  Log Analytics Contributor  Monitoring Contributor  Support Request Contributor | Security Reader |  |  |  |  |  | BHCAzureSecurityArch |
| Managed Security Services | Resource Group (rg-security-hub-eastus) | ​​​Cloud Ops only | Contributor | Contributor |  |  |  |  |  | BHCAzureSecurityArch |
| Managed Security Services | Azure AD | ​​​Cloud Ops only | Service Support Administrator | Service Support Administrator |  |  |  |  |  | BHCAzureSecurityArch |

Link to the AD security groups for other privileged access - [Azure access rules - detailed v7-19-22.xlsx (sharepoint.com)](https://bakerhughes.sharepoint.com/:x:/r/sites/BHAzureHome/_layouts/15/Doc.aspx?sourcedoc=%7B84150D77-C2D8-484E-BAE8-2C46C5BD788D%7D&file=Azure%20access%20rules%20-%20detailed%20v7-19-22.xlsx&action=default&mobileredirect=true&cid=0fbe1d29-9781-4ab8-9a44-33b8a6e6f131)

### Azure Regions

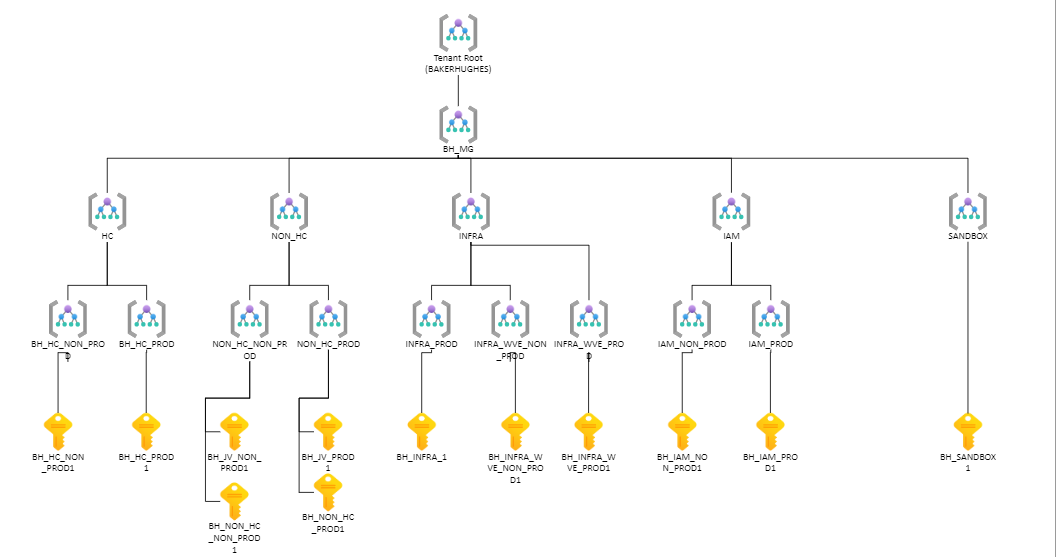
Client has selected the following regions for deployment:

Regions

|  |  |  |
| --- | --- | --- |
| Azure Region | Primary Location | Secondary Location |
| East US | Dallas | Atlanta |
| West Europe | London | Germany |
| West US | Dallas | Alpharetta |

### Management Groups/Subscriptions

Client will use the management group and subscription structure as depicted in the diagram below. Management groups and subscriptions are region agnostic. Resources within subscriptions can be assigned to any region.



Latest MG structure - <https://bakerhughes.sharepoint.com/sites/BHAzureHome/SitePages/BHC-Azure-MG-Structure.aspx>

Management groups and subscriptions are region agnostic. Resources within subscriptions can be assigned to any region. The following table displays the management groups to be created and the parent/child relationships to be established. Subscriptions are assigned to management groups and the management group structure can be modified at any time.

|  |  |  |
| --- | --- | --- |
| Management Group | Parent | Contains |
| BH\_MG | Tenant Root Group | Prod, Non-Prod, Sandbox management groups |
| HC | BH\_MG | HCProd, HCNonProd management groups |
| NONHC | BH\_MG | NONHCProd, NONHCNonProd management groups |
| INFRA | BH\_MG | Infra subscription |
| INFRA\_PROD | INFRA | Shared INFRA resources |
| INFRA\_VWE\_NON\_PROD | INFRA | Shared W365 and AVD nonproduction |
| INFRA\_VWE \_PROD | INFRA | Shared W365 and AVD production |
| SBX | BH\_MG | Sandbox subscription |
| HCPROD | HC | BH\_HCPROD Subscriptionhub |
| HCNONPROD | HC | BH\_HCNONPROD Subscription |
| NONHCPROD | NONHC | BH\_JV\_PROD1, BH\_NON\_HC\_PREPROD1, BH\_NON\_HC\_PROD1, BH\_SAP\_PREPROD1, BH\_SAP\_PROD1, BH\_SAP\_PROD\_DR1 Subscriptions |
| NONHCNONPROD | NONHC | BH\_JV\_NON\_PROD1, BH\_NON\_HC\_NON\_PROD1, BH\_SAP\_NON\_PROD1 Subscriptions |
| IAM | BH\_MG | Industrial Asset Management parent MG |
| IAM\_NON\_PROD | IAM | IAM nonproduction |
| IAM\_PROD | IAM | IAM production |
|  |  |  |

Subscriptions

|  |  |
| --- | --- |
| Subscription | Purpose |
| BH\_PROD\_1 | Contains non-High Confidential Production resources |
| BH\_NONPROD\_1 | Contains non-High Confidential Non-Production resources |
| BH\_HCPROD\_1 | Contains High Confidential Production resources |
| BH\_HCNONPROD\_1 | Contains High Confidential Non-Production resources |
| BH\_INFRA\_1 | Contains networking and infrastructure resources |
| BH\_SBX\_1 | Contains Proof of Concept and sandbox resources |
| IAM\_NON\_PROD | Contains IAM application nonproduction resources |
| IAM\_PROD | Contains IAM application production resources |
| INFRA\_VWE\_NON\_PROD | Contains AVS & W365 application nonproduction resources |
| INFRA\_VWE\_PROD | Contains AVS & W365 application production resources |
| BH\_JV\_NON\_PROD\_1 | Contains JV application nonproduction resources |
| BH\_JV\_PROD\_1 | Contains JV application production resources |

### Azure Policy

The following are recommended policies for initial implementation at the management group level. The Accenture Security team will be deploying Azure Policies at a more granular level and will include these policies in their deployments. Policies will be adjusted as the environment matures:

|  |  |  |
| --- | --- | --- |
| Policy | Description | Recommended Scope |
| Require a tag and its value on resource groups | Enforces a required tag and its value on resource groups. | Management Group |
| Require a tag and its value on resources | Enforces a required tag and its value. Does not apply to resource groups. | Management Group |
| Deploy network watcher when virtual networks are created | This policy creates a network watcher resource in regions with virtual networks. You need to ensure existence of a resource group named networkWatcherRG, which will be used to deploy network watcher instances. | Management Group |
| Flow log should be configured for every network security group | Audit for network security groups to verify if flow log resource is configured. Flow log allows to log information about IP traffic flowing through network security group. It can be used for optimizing network flows, monitoring throughput, verifying compliance, detecting intrusions and more. | Management Group |
| Network interfaces should not have public Ips | This policy denies the network interfaces which are configured with any public IP. Public IP addresses allow internet resources to communicate inbound to Azure resources, and Azure resources to communicate outbound to the internet. This should be reviewed by the network security team. | Management Group |
| Network Watcher should be enabled | Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end-to-end network level view. Network diagnostic and visualization tools available with Network Watcher help you understand, diagnose, and gain insights to your network in Azure. | Management Group |
| RDP access from the Internet should be blocked | This policy audits any network security rule that allows RDP access from Internet | Management Group |
| SSH access from the Internet should be blocked | This policy audits any network security rule that allows SSH access from Internet | Management Group |
| Deploy Advanced Threat Protection on Storage Accounts | This policy enables Advanced Threat Protection on Storage Accounts. | Management Group |
| Secure transfer to storage accounts should be enabled | Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking | Management Group |
| Deploy default Microsoft IaaSAntimalware extension for Windows Server | This policy deploys a Microsoft IaaSAntimalware extension with a default configuration when a VM is not configured with the antimalware extension. | Management Group |
| Microsoft Antimalware for Azure should be configured to automatically update protection signatures | This policy audits any Windows virtual machine not configured with automatic update of Microsoft Antimalware protection signatures. | Management Group |
| Microsoft IaaSAntimalware extension should be deployed on Windows servers | This policy audits any Windows server VM without Microsoft IaaSAntimalware extension deployed. | Management Group |
| Only approved VM extensions should be installed | This policy governs the virtual machine extensions that are not approved. | Management Group |
| Require automatic OS image patching on Virtual Machine Scale Sets | This policy enforces enabling automatic OS image patching on Virtual Machine Scale Sets to always keep Virtual Machines secure by safely applying latest security patches every month. | Management Group |
| An activity log alert should exist for specific Administrative operations | This policy audits specific Administrative operations with no activity log alerts configured. | Management Group |
| An activity log alert should exist for specific Policy operations | This policy audits specific Policy operations with no activity log alerts configured. | Management Group |
| An activity log alert should exist for specific Security operations | This policy audits specific Security operations with no activity log alerts configured. | Management Group |
| Azure Monitor should collect activity logs from all regions | This policy audits the Azure Monitor log profile which does not export activities from all Azure supported regions including global. | Management Group |

The following tags will be deployed at the top-level management group to apply to all environments

1. For Resource Group.

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Mandatory Tags on RG level** | **Source | Value** | **Value From App Master Inventory** |
| 1 | App | App master Inventory | ApplicationName |
| 2 | Application ID | App master Inventory | CIID |
| 3 | Build by | Accenture {Migration | Ops| New Project} future tag - 431 | email | Email@bakerhughes.com |
| 4 | Business | App master Inventory | ProductCompany |
| 5 | Classification | App master Inventory | BHDataClassification |
| 6 | Created\_date | {date} |  |
| 7 | Criticality | App master Inventory | OutageCritical |
| 8 | Env | {dev, stg, qa, prod, pre-prod,sbx} |  |
| 9 | Functional Owner Email | App master Inventory | FuncOwnerEmail |
| 10 | Name | Resource Name |  |
| 11 | Owned by Email | App master Inventory | OwnedByEmail |
| 12 | Owner-Business Unit | App master Inventory | ProductCompany |
| 13 | Sub Business | App master Inventory | Department |
| 14 | Support Group | App master Inventory | SupportGroup |
| 15 | Support Group DL | App master Inventory | SupportTeamDL |

Resources will inherit tags from RG

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Mandatory Tags on VM level** | **Comments** | **Source | Value** | **Value From App Master Inventory** |
| 1 | App | Tag Inherited via RG | App master Inventory | ApplicationName |
| 2 | Application ID | Tag Inherited via RG | App master Inventory | CIID |
| 3 | Build by | Tag Inherited via RG | Accenture {Migration | Ops| New Project} |  |
| 4 | Business | Tag Inherited via RG | App master Inventory | ProductCompany |
| 5 | Classification | Tag Inherited via RG | App master Inventory | BHDataClassification |
| 6 | Created\_date | Tag Inherited via RG | {date} |  |
| 7 | Criticality | Tag Inherited via RG | App master Inventory | OutageCritical |
| 8 | Env | Tag Inherited via RG | dev, stg, qa, prod, pre-prod,sbx |  |
| 9 | Functional Owner Email | Tag Inherited via RG | App master Inventory | FuncOwnerEmail |
| 10 | Name | Tag Inherited via RG | Resource Name |  |
| 11 | Owned by Email | Tag Inherited via RG | App master Inventory | OwnedByEmail |
| 12 | Owner-Business Unit | Tag Inherited via RG | App master Inventory | ProductCompany |
| 13 | Sub Business | Tag Inherited via RG | App master Inventory | Department |
| 14 | Support Group | Tag Inherited via RG | App master Inventory | SupportGroup |
| 15 | Support Group DL | Tag Inherited via RG | App master Inventory | SupportTeamDL |
| 16 | Groups on instance | Added new Tag | Instance HPA group from AD |  |
| 17 | Private IP | Added new Tag | IP address |  |

Dynamic tags will be updated monthly by referring to App master

Following Database connection will be used to run the query to pull App inventory

Server Name:         UI1PCADB001XCB.ent.bhicorp.com\MDB\_PROD

Port Number:         56521

Database Name:    mdb

 MyWizard Rundeck run weekly jobs to update the tag values , source for all tags is App master Inventory

|  |  |
| --- | --- |
|  | ***Important Note***  *Updating tag with PS script is tested, but database connection from Azure firewall request is in progress* |

### Naming Conventions

The following table includes the naming conventions to be used in Azure:

|  |  |  |
| --- | --- | --- |
| Resource | Convention | Example |
| Subscription | <BH>\_<Data classification>\_<Env> | BH\_HC\_NON\_PROD1 |
| Resource Group | RG-< application>-<subscription>-location-dev  Exclude BH in the subscription name and no “-“ | rg-petclinic-nonhcnonprod-eastus-dev |
| Vnet | [HUB/SPOKE-PROD/SPOKE-NONPROD]-[Region]-## | HUB-EastUS2-01  SPOKE-NONPROD-EastUS2-01 |
|  |  |  |
| Automation Account | AA-<Region>-<Subscription>-## | AA-EastUS2-Infra1-01 |
| Subnet | SNET-Project name-Env-Use for  Maximum 32 characters | SNET-BHC3-Dev-AppsVM |
| Network interface (NIC) | NIC-<resource name>-<serialization> | NIC-Vmapp04p-01, NIC-DC01-01 |
| Public IP address | PIP-<resource name> | PIP-Vmapp04p |
| App Gateway (internal) | AGW-app-env-location | AGW-bhge-dev-eus |
| App Gateway (external) | Agw-external-location-env {subscription without BH} | AGW-External-WEU-NonHC-NonProd |
| Vnet Gateway | [Vnet Name]-GW-# | HUB-EastUS2-01-GW-1 |
| LB | LB-app-env | LB-Phantom-Portainer-dev |
| Storage Account | stvm<function><serialization><env> | stvmdb01p |
| VM | BHAZ<Linux/Windows><serialization><Env> | BHAZW00000001P |
| IP | IP- <resource name> | IP-Vmapp04p |
| Network Security Group (NSG) | [Subnet Name]-NSG | Infra-10.64.0.192-27-NSG |
| Application Security Group (ASG) | ASG-<resource/application>-<env> | ASG-app01-prod |
| Application | <application name>-<env> | App01-prod |
| Express Route | EX-<Provider>-<Connection City> | EX-Verizon-Fairfax |
| Connection | CX-Type(EX for ExpressRoute/VPN for VPN)-Region | CX-EX-East2 |
| Log Analytics | LOG-<Env>-### | LOG-EA-001 |
| Traffic Manager | TM-<application> | TM-Sitecore |
| SQL Server | App-env-sqlsrv-subscription | mji-dev-sqlsrv-nonprod |
| SQL managed instances | Bhazms{random}{env}  Env - t, d, p or sbx | bhazms0222001t |
| Availability Set | AS-<application/tier>-<serialization> | AS-PaloAlto-001 |
| Azure Site Recovery Vault | ASR-<Subscription>-<region>-<serialization> | ASR\_ACC\_EA\_EAST2\_01, ASR\_ACC\_Dev\_Central\_01 |
| Azure Bastion | [Vnet Name]-Bastion | HUB-EastUS2-01-Bastion |
| Azure Firewall | [Vnet Name]-Firewall | HUB-EastUS2-01-Firewall |
| IP Groups | [Vnet Name]-[Subnet Name]-IpGroup | HUB-EastUS2-01-Infra-10.64.0.192-27-IpGroup |
| Route Table | Route-[HUB]-[Region]  Route-[Spoke]-[ENV]-[Region]-XX | Route-HUB-EastUS2  Route-Spoke-Prod—EastUS2-1 |
| Key Vault | KV-app-<Subscription>-## | KV-FW-Infra1-01 |
| DDOS Protection Plan | DDOS-<Subscription> | DDOS-Infra1 |
| Private End Point | <resource name>-pe-nic  <resource name>-pe |  |

### Resource Groups

An Azure resource can only belong to a single resource group. Because of this fact, Accenture will use the following resource group strategy:

1. Use separate resource groups for infrastructure and networking components, separated by environment and region. For example, a resource group named rg-Network-Prod-East will contain Vnets and other network and infrastructure for the East US region and a resource group named rg-Network-Prod-East-Prod will be created for the production spoke networking resources. Both resource groups will be created in the Infrastructure subscription. The Network team will have the owner role applied for management of the resources.
2. Group application components that have the same application lifecycle into a single resource group. Grant the owner role to the application owner or other designated user. For example, a resource group named rg-Sitecore-dev can be created to contain all the development components for the Sitecore application as the development components have the same lifecycle.
3. Resource groups should conform to the naming conventions in section Naming Conventions
4. The Azure Architect team will be responsible for creating resource groups and assigning the RBAC roles.

The following table contains the initial resource groups created to support the networking infrastructure for Baker Hughes. Networking components are grouped by type and region.

|  |  |
| --- | --- |
| Resource Group | Description |
| **RG-NetworkHUB-EastUS** | This resource group contains the Vnet for the Hub in the East US region, which holds the common infrastructure components used by the entire environment. The ExpressRoute and backup site-to-site VPN connections for this region are also connected in this Vnet. |
| **RG-NetworkHUB-WestEU** | This resource group contains the Vnet for the Hub in the West Europe region, which holds the common infrastructure components used by the entire environment. The ExpressRoute and backup site-to-site VPN connections for this region are also connected in this Vnet. |
| **RG-NetworkHUB-USWest** | This resource group contains the Vnet for the Hub in the West US region, which holds the common infrastructure components used by the entire environment. The ExpressRoute and backup site-to-site VPN connections for this region are also connected in this Vnet |
| **RG-Network-Spoke-EastUS** | This resource group contains the networking for the US East region spokes. |
| **RG-Network-Spoke-WestEU** | This resource group contains the networking for the US East region spokes. |
| **RG\_SAP\_Infra\_Non\_Prod\_EastUS** | This resource group contains the networking for the US East region SAP Non prod spokes. |
| **RG\_SAP\_Infra\_PreProd\_EastUS** | This resource group contains the networking for the US East region SAP Pre Prod spokes. |
| **RG\_SAP\_Infra\_Prod\_EastUS** | This resource group contains the networking for the US East region SAP Prod spokes. |
| **RG\_HUB\_Citrix\_w365\_nva\_EastUS** | This resource group contains the networking for the US East region Citrix w365 spokes. |
| **RG\_HUB\_Citrix\_w365\_nva\_WestEU** | This resource group contains the networking for the West EU region Citrix\_w365 spokes |

### Resource Locks

Resource locks allow administrators to lock Subscriptions, resource groups, or resources to prevent accidental deletion or modification of critical resources. Unlike RBAC management, locks apply a restriction across all users and roles. A lock on a parent scope applies to all child resources. Resource Locks use the least privilege model, meaning the most restrictive lock in the inheritance takes precedence.

There are two types of locks:

* **Delete** – Authorized users can still read and modify a resource, but they are prevented from deleting it.
* **Read-only** – Authorized users can read from a resource, but they are prevented from modifying or deleting the resource.

Accenture will configure the Delete lock on all networking Resource Groups and all production Resource Groups.

### Cost Management

Accenture recommends using automation and technology to manage costs. To execute this strategy, it is recommended to implement the following:

1. Implement tagging on all resources to group them by application, cost center, and other categories for billing purposes.
2. Enforce tagging requirements by implementing Azure Policy to require tags.
3. Take advantage of cost saving technologies in Azure such as Dev/Test subscriptions, auto shutdown, reservations, etc., detailed further in this section.

The following subsections detail the various technologies and methods that fit the overall strategy.

#### Reserved VM Instances

Microsoft offers reserved instances of VM sizes to reduce costs significantly versus pay-as-you-go pricing. Reserved instances require an up-front payment and a commitment for one or three years. Reserved instances are optimal for production workloads that will rarely if ever be shut down or go off-line for extended periods. Other non-production workloads like staging, development and QA should be evaluated before committing to a one or three years reserved instance. If these workloads are not required to be powered on all the time, cost savings can be realized by implementing auto-shutdown on the VMs.

#### Azure Hybrid Use Benefit

Microsoft introduced Azure Hybrid Use Benefit Pricing to provide significant cost savings to organizations that already have Enterprise Licensing agreements in place. The Azure Hybrid Use Benefit allows organizations to remove the retail license provided in pay-as-you-go pricing and instead use their existing Server licenses on the Azure Windows Server. Organizations must have a current Enterprise Licensing Agreement with Software Assurance to use this benefit.

Enabling Azure Hybrid Use Benefit can be added to deployment ARM templates. To configure the ARM template, the following configuration needs to be added to the JSON file for the master template.

“properties”: {

“licenseType”: “Windows\_Client”,

“hardwareProfile”: {

“vmSize”: “[variables(‘vmSize’)]”

}

#### Auto Shutdown

Low-demand workloads, like staging, development, and QA, should be put into pay-as-you-go instances. To lower costs, it is recommended to shut down VMs when they are no longer needed in the day; for example, after eight hours of use in workhours. There are two ways to fully automate VM shutdown. Auto-shutdown is a free built-in feature on the blade of each VM. Shutdown hour and time zone can be configured, with the option to send an email before shutdown is available. The Start/Stop VMs during off-hours solution is another way to automatically shut down VMs. This feature will start or stop machines on user-defined schedules and insights will be provided through Azure Monitor logs. Using this decentralized low-cost automation option VMs can:

* Be scheduled to start or stop
* Be scheduled to start or stop using Tags
* Auto-stop based on low CPU storage

To enable this feature, follow the steps in [**Enable Azure Automation Start/Stop VMs solution**](https://docs.microsoft.com/en-us/azure/automation/automation-solution-vm-management-enable).

To enable Auto-shutdown follow the steps in [**Azure Virtual Machine auto-shutdown**](https://techcommunity.microsoft.com/t5/educator-developer-blog/azure-virtual-machine-auto-shutdown/ba-p/379342).

|  |  |
| --- | --- |
|  | ***Recommendation***  *Use Auto-shutdown if different auto shutdown configuration is needed for each VM; use Start/Stop VMs during off-hours for larger quantity of VMs and if they should all be shut down at the same hour.* |

#### Azure Advisor

Accenture recommends the daily use of Azure Advisor to get recommendations from the Cost tab on the Advisor dashboard and reduce service costs. Baker Hughes will benefit from this tool because Azure Advisor identifies idle and underutilized resources and makes recommendations to optimize and reduce costs associated with them. These recommendations include:

* Optimizing virtual machine spend by resizing or shutting down underutilized instances
* Deleting or reconfiguring idle virtual gateways
* Buying reserved virtual machine instances to save money over pay-as-you-go costs
* Deleting unassociated public IP addresses to save money
* Using Standard Snapshots for Managed Disks

Azure Advisor recommendations can be automated by implementing an alert in Advisor and also by automating a recommendation digest and scheduling it for a weekly report to be delivered to an Action group.

#### Azure Cost Analysis

To analyze costs in Azure, Accenture recommends organizing resources to maximize cost insights and accountability. This organization has already been started by applying a policy that enforces tagging on resources; these tags can be applied as filters in cost analysis to better understand spend. AFS recommends creating budgets to evaluate actual costs against it in the Cost Analysis tab in Cost Management.

#### Azure Budgets

Azure Budgets set either a cost or usage-based budget with thresholds and alerts. Accenture recommends creating a budget to control and prevent cost thresholds from being surpassed. Accenture recommends reviewing the budgets regularly to view budget burn-down progress and make changes as needed. Alerts can be configured to trigger when a budget threshold is reached. To monitor usage and spending in Azure, Accenture suggests creating cost alerts such as:

* Budget alerts
* Credit alerts
* Spending quota alerts

#### Cost Management Using Power BI

Microsoft provides a connector into Azure to export cost data into Power BI for reporting and consumption. Power BI dashboards provide reporting and visibility into Azure costs as an extension of the Azure provided Cost Management features.

The Power BI dashboard is connected to Azure EA using the connector located at [***https://docs.microsoft.com/en-us/power-bi/connect-data/desktop-connect-azure-cost-management***](https://docs.microsoft.com/en-us/power-bi/connect-data/desktop-connect-azure-cost-management)***.*** The connector establishes a connection into Azure to pull data into Power BI. The dashboards will then display costs in multiple ways: monthly, month vs month, monthly drilldown, cost analysis per resource group, resource group drilldown, among others. Tags will also be used in these dashboards as filters for further drilldown. Any modification and/or new page addition should be made in Power BI Desktop before publishing it to Power BI Online.

# Network

## Avanade Recommendations

### Connectivity

* In the **3.2.2 High-Level Hub Design** below, note the Hub Vnet in East US is peered to the Production and Non-Production Spoke Vnets in the East US region. The East US Hub consists of Shared Services, such as the Firewall, Gateway, Edge/Mid/Internal DCs, as well as Bastion Hosts, and Other Infrastructure.

### Remote Access

* Remote Access to resources within Azure will be achieved using Jump Hosts and Azure Bastion as secondary. Jump Host subnet and Azure Bastion Subnet will reside in the HUB Vnet. Using Vnet peering, resources placed in peered Vnets will be accessible without creating additional Azure Bastion subnets in spoke Vnets.
* MFA will be implemented.
* 

### Vnets and subnets

* There will be one Vnet for each hub in the design. Within the Hub there will be multiple subnets that are defined in the Hub Design section listed below
* Each spoke will be its own Vnet with subnets inside, defined in the Spoke Design section below.
* Limitation: Vnets cannot span subscriptions or Azure regions.

### Network Security

* Avoid attaching network security groups (NSGs) directly to network interfaces, instead attach NSGs to subnets.
* Create application security groups (ASGs) to group similar severs together and use the ASG in NSG rules to reduce the number of subnets necessary.
  + Limitation: ASGs from foreign subscriptions are not visible/usable in NSG rules.
* Use a firewall (Azure Firewall, network virtual appliance (NVA), or an app gateway with the web application gateway (WAF) SKU) for edge security and use NSGs to control east-west traffic (traffic between subnets/Vnets).
* Control internal Vnet traffic on the receiving side (inbound rules).
* Use priority ranges to ensure specific rules are evaluated before more general rules.
* Create NSGs with default deny, allow by exception.
* Use Azure Network Watcher for logging and audit activity.
* Set NSG Flow log retention period to 90 days or more to meet CIS Benchmarks.
* NSGs are disabled on the AzureFirewallSubnet and the GatewaySubnet are not supported.
* Implement Azure DdoS Standard protection on all Vnets containing public IPs. It provides always-on traffic monitoring and real-time mitigation of common network-level attacks.

## Design Decisions / Requirements

### Connectivity

* ExpressRoute connections in Dallas and London. VPN in Atlanta and Germany to provide redundancy.
* Connectivity to AWS will go through BH on Prem and then through the ExpressRoute/VPN to Azure
* Connectivity to India will go through VPN to On Prem and then through the ExpressRoute/VPN to Azure
* Traffic inspection required for traffic traversing the connections.

### Vnets and Subnets

* Vnets to be created to represent the identified zones.
* Vnets created in a hub/spoke architecture with a Shared Services infrastructure connecting the Zones.
* A /19 address space will be deployed in each region. BH to provide IP addressing.

### Network Securityhub

* Azure Firewall to be used unless it doesn’t support a specific requirement.
* WAF required to protect Internet facing applications. Imperva will be deployed
* Traffic between zones must be inspected.
* Traffic between applications must be denied by default and allowed by exception.

## Design

### Connectivity

* Client will use for ExpressRoute connectivity between the MPLS and Azure
* Client will use site-to-site VPN between datacenters and Azure for redundancy

**Connectivity Design**



All data centers are connected to each other through the MPLS network

* The Dallas data center will connect to US East Hub gateway through ExpressRoute
* The London data center will connect to West EU Hub gateway through ExpressRoute
* The Dallas data center will connect to US West Hub gateway through ExpressRoute
* The Atlanta data center will connect to US East Hub gateway using a Site-to-Site VPN for redundancy
* The Germany data center will connect to West EU Hub gateway using a Site-to-Site VPN for redundancy
* The Alpharetta data center will connect to US West Hub gateway using a Site-to-Site VPN for redundancy

In addition to the ExpressRoute and Site-to-Site VPN connections to Baker Hughes data centers, the Accenture India location will connect to the Baker Hughes Azure network through the Baker Hughes Global Connect VPN and then access Azure through the ExpressRoute connection.

### High-level Vnet design

Based on outputs and decisions from the Cloud Foundations Workshop, a hub and spoke design is recommended for Baker Hughes to support workloads which are planned for migration to Azure. A hub and spoke design centralize shared services, such as on-premises connectivity and domain controllers (DC), into a single Vnet which becomes the hub and connects workloads such as VMs placed into separate spoke Vnets. This design provides separation of the Baker Hughes environments (Production, Non-Production, High Confidential Production, High Confidential Non-Production, and Sandbox) into separate Vnets. The high-level hub and spoke design is shown below.

The lines connecting the Vnets spokes to the hubs and from hub to hub are Vnet Peerings. Traffic between peered networks traverses the Microsoft backbone. A peering is established between each regional hub to connect the regions. Peerings are non-transitive and point-to-point only. To establish connectivity between spokes and regions, routing will be configured to direct traffic to the Azure Firewall and then to the other spoke or region. This is accomplished by configuring a User Defined Route (UDR) on each subnet to direct traffic to the Azure Firewall and configuring routing on the Azure Firewall to direct the traffic to the appropriate spoke or other regional hub.

C

The Azure Firewall placed in the diagram is a representation showing that traffic flowing through the hub will pass through an Azure Firewall and be scanned according to Baker Hughes requirements. For further details of the Azure Firewall and the placement in the hub, see section 3.3.3.1 Hub Design and section 3.5.3.1 Azure Firewall.

The diagram shows the hub and spoke architecture in two Azure regions, US East and West Europe. Baker Hughes selection of these regions was based on availability zones feature supported in these regions and the network connectivity speeds and latency between on-premises data centers and the Azure data centers. The network IDs allocated to the regions are shown in the table below.

|  |  |
| --- | --- |
| Azure Region | Network ID |
| US East | 10.124.0.0/22 |
| West Europe | 10.124.32.0/22 |
| US West | 10.127.0.0/22 |

Additional regions to support Disaster Recovery scenarios are not planned at this time.

### IP Addressing

#### On-Premises Addressing

The following table shows the private IP Address ranges that are being used at Baker Hughes. Rows 1-3 are the IANA Private IP Ranges that are predefined to be private ranges. Rows 4-6 show the additional addresses that BH is using as internal address spaces.

|  |  |
| --- | --- |
| **Network ID** | **Description** |
| 10.0.0.0/8 | IANA Private IP Ranges |
| 172.16.0.0/12 |
| 192.168.0.0/16 |
|  |  |

#### Azure Addressing

Baker Hughes has four distinct environment zones: Production, Non-Production, High Confidential Production, High Confidential Non-Production, plus a separate zone for Sandbox. Each of these zones will be supported by a separate Vnet. Vnets will be duplicated for each region. To support the hub and spoke architecture with a hub and five Vnets plus possible expansion, the region network ID was further subdivided into /22 networks of approximately 1,000 IPs per network.

A Joint Venture environment zone also created in the US East hub. This contains four joint venture applications that were defined by Baker Hughes. Their IP range is different since in the future this zone could be transformed to fit future needs without any impact to the hub environment. There are 2 spokes (production and non-prod)

Industrial Asset Management and Windows desktop projects spokes are also added to the existing environment. These spokes support production and Non-production environments.

The table below details the VNets to be deployed in each region and the network IDs and ranges assigned to each VNet.

|  |  |  |  |
| --- | --- | --- | --- |
| **VNET** | **Naming** | **Network ID** | **Address Range** |
| Hub – US East | HUB-USEast-1 | 10.124.0.0/22 | 10.124.0.1-10.124.3.255 |
| Hub – US West | Hub – US West | 10.127.0.0/22 | 10.127.0.0 - 10.127.3.255 |
| HC Prod – US East | SPOKE-HCProd-USEast-1 | 10.124.4.0/22 | 10.124.4.0-10.124.7.255 |
| Prod– US East | SPOKE-Prod-USEast-1 | 10.124.8.0/21 | 10.124.8.0-10.124.15.255 |
| Non-Prod– US East | SPOKE-Non-Prod-USEast-1 | 10.124.16.0/21 | 10.124.16.0-10.124.23.255 |
| HC Non-Prod – US East | SPOKE-HCNon-Prod-USEast-1 | 10.124.24.0/22 | 10.124.24.0-10.124.27.255 |
| Unused | Available for distribution | 10.124.28.0/22 | 10.124.28.0-10.124.31.255 |
| Hub – West Europe | HUB-WestEU-1 | 10.124.32.0/22 | 10.124.32.1-10.124.35.255 |
| HC Prod – West EU | SPOKE-HCProd-WestEU-1 | 10.124.36.0/22 | 10.124.36.0-10.124.39.255 |
| Prod– West EU | SPOKE-Prod-WestEU-1 | 10.124.40.0/21 | 10.124.40.0-10.124.47.255 |
| Non-Prod– West EU | SPOKE-Non-Prod-WestEU-1 | 10.124.48.0/21 | 10.124.48.0-10.124.55.255 |
| HC Non-Prod – West EU | SPOKE-HCNon-Prod-WestEU-1 | 10.124.56.0/22 | 10.124.56.0-10.124.59.255 |
| Unused | Available for distribution | 10.124.60.0/22 | 10.124.60.0-10.124.63.255 |
| Joint Venture Production | Spoke-JV-Prod | 10.124.64.0/23 | 10.124.64.0-10.124.65.255 |
| Joint Venture NonProduction | Spoke-JV-NonProd | 10.124.66.0/23 | 10.124.66.0-10.124.67.255 |
| Unused | Available for distribution | 10.124.68.0/22 | 10.124.68.0-10.124.71.255 |
| IAM -Nonprod - East US | Spoke\_IAM\_Dev\_NON\_PROD\_EastUS | 10.15.192.0/21 | 10.15.192.0 - 10.15.199.255 |
| 10.15.200.0/23 | 10.15.200.0 - 10.15.201.255 |
| 100.74.128.0/19 | 100.74.128.0 - 100.74.159.255 |
| IAM -C3- Nonprod - East US | spoke\_iam\_C3\_dev\_non\_prod\_eastUS | 10.15.202.0/23 | 10.15.202.0 - 10.15.203.255 |
| 100.74.160.0/21 | 100.74.160.0 - 100.74.167.255 |
| VWE\_Nonprod-East US | Spoke\_VWE\_NON\_PROD\_EastUS | 10.15.128.0/24 | 10.15.128.0 - 10.15.128.255 |
| VWE\_Nonprod-West EU | [Spoke\_VWE\_NON\_PROD\_westEU](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_w365_Infra_NonProd-westEU/providers/Microsoft.Network/virtualNetworks/Spoke_VWE_NON_PROD_westEU) | 10.15.160.0/24 | 10.15.160.0 - 10.15.160.255 |
| SAP Non Prod | Spoke\_SAP\_Non\_Prod\_EastUS | 10.124.107.0/24  10.124.136.0/22 | 10.124.107.0 - 10.124.107.255  10.124.136.0 - 10.124.139.255 |
| SAP Pre Prod | Spoke\_SAP\_PreProd\_EastUS | 10.124.134.0/24 | 10.124.134.0 - 10.124.134.255 |
| SAP Prod | Spoke\_SAP\_Prod\_EastUS | 10.124.128.0/22 | 10.124.128.0 - 10.124.131.255 |
| HUB Citrix w365 East US | HUB\_Citrix\_w365\_nva\_EastUS | 10.15.129.0/24 | 10.15.129.0 - 10.15.129.255 |
| HUB Citrix w365 West EU | HUB\_Citrix\_w365\_nva\_WestEU | 10.15.161.0/24 | 10.15.161.0 - 10.15.161.255 |
| HUB-WestEU | HUB-WestEU | 10.124.32.0/22 | 10.124.32.40, 10.124.32.41 |
| SPK3-TESTING-US | IAMPreProd-SPK3-TESTING-US | 10.126.57.32/27,10.126.57.128/27 | 10.126.57.32 - 10.126.57.63 ,10.126.57.128 - 10.126.57.159 |
| NIC-bhazl04110006d-001 | NIC-bhazl04110006d-001 | 100.64.0.0/17 | 100.64.0.0 - 100.64.127.255 |
| NonHCNonProd-SPK3-TESTING-WESTUS | NonHCNonProd-SPK3-TESTING-WESTUS | 10.127.16.64/26 | 10.127.0.40, 10.127.0.41 |
| BHCAzureC-EastUS-dev-01 | SPOKE-BakerHughes\_BHCAzureC-EastUS-dev-01 | 10.124.190.0/24 | 10.124.0.40, 10.124.0.41 |
| BHCAzureC-EastUS-dev-02 | SPOKE-BakerHughes\_BHCAzureC-EastUS-dev-02 | 10.126.65.0/24 , 100.68.0.0/21 | 10.126.65.0 - 10.126.65.255 , 100.68.0.0 - 100.68.7.255 |
| BHCAzureC-EastUS-dev-09 | SPOKE-BakerHughes\_BHCAzureC-EastUS-dev-09 | 10.126.66.0/23 , 100.68.8.0/21 | 10.126.66.0 - 10.126.67.255 , 100.68.8.0 - 100.68.15.255 |
| BHCAzureC-EastUS-dev10-10 | SPOKE-BakerHughes\_BHCAzureC-EastUS-dev10-10 | 10.126.57.160/29 | 10.126.57.160 - 10.126.57.167 |
| BHCAzureC-EastUS-preprod-01 | SPOKE-BakerHughes\_BHCAzureC-EastUS-preprod-01 | 10.126.57.96/27 | 10.124.0.40, 10.124.0.41 |
| BHCAzureC-EastUS-preprod-04 | SPOKE-BakerHughes\_BHCAzureC-EastUS-preprod-04 | 10.126.160.0/23 | 10.124.0.40, 10.124.0.41 |
| BHCAzureC-EastUS-prod-01 | SPOKE-BakerHughes\_BHCAzureC-EastUS-prod-01 | 10.126.192.0/26 | 10.124.0.40, 10.124.0.41 |
| BHCAzureC-EastUS-prod-02 | SPOKE-BakerHughes\_BHCAzureC-EastUS-prod-02 | 10.126.226.128/25 , 100.92.8.0/21 | 10.126.226.128 - 10.126.226.255 , 100.92.8.0 - 100.92.15.255 |
| BHCAzureC-EastUS-prod-09 | SPOKE-BakerHughes\_BHCAzureC-EastUS-prod-09 | 10.126.196.0/23 , 100.88.0.0/21 | 10.126.196.0 - 10.126.197.255 , 100.88.0.0 - 100.88.7.255 |
| BHCAzureC-WestEU-dev-01 | SPOKE-BakerHughes\_BHCAzureC-WestEU-dev-01 | 10.17.113.96/27 , 10.17.113.128/27 | 10.17.113.96 - 10.17.113.127 , 10.17.113.128 - 10.17.113.159 |
| BHCAzureC-WestEU-dev-02 | SPOKE-BakerHughes\_BHCAzureC-WestEU-dev-02 | 10.17.16.0/25 , 10.17.16.192/27 | 10.17.16.0 - 10.17.16.127 , 10.17.16.192 - 10.17.16.223 |
| BHCAzureC-WestEU-dev-12 | SPOKE-BakerHughes\_BHCAzureC-WestEU-dev-12 | 10.17.16.160/27 , 100.104.0.192/28 , 100.104.0.216/29 , 100.104.0.224/27 | 10.17.16.160 - 10.17.16.191 , 100.104.0.192 - 100.104.0.207 , 100.104.0.216 - 100.104.0.223 , 100.104.0.224 - 100.104.0.255 |
| BHCAzureC-WestEU-dev-13 | SPOKE-BakerHughes\_BHCAzureC-WestEU-dev-13 | 10.17.16.128/28 , 10.17.16.144/28 , 100.104.0.88/29 , 100.104.0.96/27 , 100.104.0.128/26 , 100.104.0.208/29 | 10.17.16.128 - 10.17.16.143 , 10.17.16.144 - 10.17.16.159 , 100.104.0.88 - 100.104.0.95 , 100.104.0.96 - 100.104.0.127, 100.104.0.96 - 100.104.0.127 , 100.104.0.208 - 100.104.0.215 |
| BHCAzureC-WestEU-dev11-11 | POKE-BakerHughes\_BHCAzureC-WestEU-dev11-11 | 10.17.32.128/26 , 100.96.128.0/21 | 10.17.32.128 - 10.17.32.191 , 100.96.128.0 - 100.96.135.255 |
| BHCAzureC-WestEU-preprod-02 | SPOKE-BakerHughes\_BHCAzureC-WestEU-preprod-02 | 10.17.66.0/25, | 10.124.32.40, 10.124.32.41 |
| BHCAzureC-WestEU-prod-02 | SPOKE-BakerHughes\_BHCAzureC-WestEU-prod-02 | 10.127.98.0/23 | 10.124.32.40, 10.124.32.41 |
| BHCAzureC-WestEU-prod-04 | SPOKE-BakerHughes\_BHCAzureC-WestEU-prod-04 | 10.17.96.0/25 , 10.17.96.128/25 , 10.17.97.0/25 , 10.17.100.0/22 , 100.124.0.0/21 , 100.124.8.0/23 , 100.124.10.0/23 | 10.124.32.40, 10.124.32.41 |
| BHCAzureC-WestUS-prod-01 | SPOKE-BakerHughes\_BHCAzureC-WestUS-prod-01 | 10.127.4.0/22 | 10.127.4.0 - 10.127.7.255 |
| DBKSCM-Prod-EastUS | Spoke-DBKSCM-Prod-EastUS | 10.15.221.0/24 , 100.74.168.0/25 | 10.15.221.0 - 10.15.221.255 , 100.74.168.0 - 100.74.168.127 |
| DBKSCM-Prod-WestEU | Spoke-DBKSCM-Prod-WestEU | 10.124.188.0/24 , 100.74.168.128/25 | 10.124.188.0 - 10.124.188.255 , 100.74.168.128 - 100.74.168.255 |
| C3\_Dev\_Non\_Prod\_westeu | Spoke\_IAM\_C3\_Dev\_Non\_Prod\_westeu | 10.124.186.0/23 , 100.77.224.0/21 | 10.124.186.0 - 10.124.187.255 , 100.77.224.0 - 100.77.231.255 |
| IAM\_C3\_PreProd\_westeu | Spoke\_IAM\_C3\_PreProd\_westeu | 10.17.64.0/23 , 100.116.0.0/21 | 10.17.64.0 - 10.17.65.255, 100.116.0.0 - 100.116.7.255 |
| IAM\_Dev\_NON\_PROD\_WestEU | Spoke\_IAM\_Dev\_NON\_PROD\_WestEU | 10.124.208.0/20 , 100.77.240.0/20 | 10.124.208.0 - 10.124.223.255 , 100.77.240.0 - 100.77.255.255 |
| IAM\_Pet\_Non\_Prod\_EastUS | Spoke\_IAM\_Pet\_Non\_Prod\_EastUS | 10.124.144.0/20 , 100.76.32.0/19 | 10.124.144.0 - 10.124.159.255 , 100.76.32.0 - 100.76.63.255 |
| IAM\_PreProd\_EastUS | Spoke\_IAM\_PreProd\_EastUS | 10.126.32.0/20 , 100.74.176.0/20 | 10.126.32.0 - 10.126.47.255 , 10.126.32.0 - 10.126.47.255 |
| IAM\_Prod\_EastUS | Spoke\_IAM\_Prod\_EastUS | 10.15.240.0/20, 100.75.0.0/19 | 10.15.240.0 - 10.15.255.255 , 100.75.0.0 - 100.75.31.255 |
| iam\_qa\_non\_prod\_EastUS | Spoke\_iam\_qa\_non\_prod\_EastUS | 10.15.224.0/20 , 100.74.224.0/19 | 10.15.224.0 - 10.15.239.255 , 100.74.224.0 - 100.74.255.255 |
| Non\_HC\_PreProd\_EastUS | Spoke\_Non\_HC\_PreProd\_EastUS | 10.124.160.0/21 , 100.76.128.0/19 | 10.124.160.0 - 10.124.167.255, 100.76.128.0 - 100.76.159.255 |
| Non\_HC\_PreProd\_WestEU | Spoke\_Non\_HC\_PreProd\_WestEU | 10.124.192.0/21 , 100.76.160.0/19 | 10.124.192.0 - 10.124.199.255 , 100.76.160.0 - 100.76.191.255 |
| SAP\_ANF\_Prod\_USEast | Spoke\_SAP\_ANF\_Prod\_USEast | 10.124.142.128/25 | 10.124.142.128 - 10.124.142.255 |
| SAP\_ANF\_ProdDR\_WestUS | Spoke\_SAP\_ANF\_ProdDR\_WestUS | 10.127.12.0/25 | 10.127.12.0 - 10.127.12.127 |
| BHC3\_Dev\_Non\_Prod\_EastUS | Spoke\_Trials\_BHC3\_Dev\_Non\_Prod\_EastUS | 10.124.108.0/23 | 10.124.108.0 - 10.124.109.255 |
| BHC3\_Pre-Prod\_EastUS | Spoke\_Trials\_BHC3\_Pre-Prod\_EastUS | 10.15.204.0/23 | 10.124.0.40, 10.124.0.41 |
| VWE\_PROD\_EastUS | Spoke\_VWE\_PROD\_EastUS | 10.6.64.0/18 , 10.15.144.0/20 | 10.15.144.0/20 , 10.15.144.0 - 10.15.159.255 |
| VWE\_PROD\_WestEU | Spoke\_VWE\_PROD\_WestEU | 10.15.176.0/20 | 10.124.32.40, 10.124.32.41 |

The /19 address space that was allocated for each region will support 8 /22 networks. There are two unused /22 networks in each region that can be allocated as-is or sub-netted further to support additional IP addressing needs. In addition, Azure supports adding additional IP address spaces to Vnets. Adding additional IP address space to a VNET does require the peering be removed and recreated after the address space has been added, which does cause an outage between Vnets. The outage can be scheduled to minimize downtime.

The initial design will accommodate adding two additional Vnets to each region using the unused IP addresses in the table. If additional IP addresses are needed for growth, an additional IP address range can be created and added to the design. To support growth, the network team would be consulted to obtain a new IP address range, and that range can be sub-netted to support multiple additional Vnets. The UDR and NSGs and Firewall Rules will need to be updated with new IP ranges.

### Hub Design

#### High-Level Design

The hub in each region will contain shared services resources, such as Domain Controllers, monitoring servers, and deployment servers, and connectivity resources, including ExpressRoute connections, VPN, and firewalls. The diagram below shows the subnet configuration and the connectivity points. A VirtualNetworkGateway subnet is implemented to deploy the Virtual Network Gateway which hosts the ExpressRoute and VPN connections. Note that Accenture India will connect to the Baker Hughes data center using Global Connect VPN and then access Azure resources through the ExpressRoute.

A VPN connection from the hub to AWS is proposed and is under consideration. If a direct VPN connection is unable to be deployed due to security regulations, then access to/from Azure and AWS will be performed through the Baker Hughes data center and the corresponding ExpressRoute and Direct Connect connections.

The diagram below displays the subnets that will be created in each hub and the connectivity between the subnets and a reference to peering to spoke Vnets. All traffic from the Internet will flow through a firewall, either the Azure Firewall or a Web Application Firewall (WAF). The WAF is not designed at this time, but a subnet is planned for expansion as externally facing applications are migrated into the Azure environment.



Each hub will contain the following subnets:

* GatewaySubnet: Contains ExpressRoute and VPN connections
* Domain Controller Subnet: Contains Domain Controllers
* AzureFirewallSubnet: Contains the Azure Firewall deployment
* AzureBastionSubnet: Contains the Azure Bastion deployment
* Infrastructure Subnet: Contains infrastructure servers such as deployment servers, monitoring servers, etc.
* MyWizard Subnet: Contains the VMs for the Accenture MyWizard deployment
* AppGateway Subnet: Contains the Application Gateway deployment
* Jump Hosts Subnet: Contains servers to be used as Jump Hosts for Accenture management
* Private Link Subnet: Contains any private endpoints for resources that are hosted within the hubs

Subnets are sized to support the number of connections required with some growth potential. In addition, there is unused space up to 507 IPs which can be allocated or further divided as future needs arise.

Deployment will be completed using Azure Resource Manager (ARM) or Terraform templates to ensure consistency across the cloud environment. The templates will be turned over to Baker Hughes as assets to be used for further builds.

The hub is a core infrastructure production Vnet. The hub will be tested after initial deployment using ARM templates and any necessary changes will be redeployed using a modified ARM template. After initial deployment, any changes made will be in a live production environment and care should be taken.

#### East US HUB

The following tables contain the subnets and configurations in the East US Hub.

Vnet

|  |  |
| --- | --- |
| **HUB-USEast** | **10.124.0.0/22** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet Name | Purpose | Subnet ID | # of Hosts | Subnet Range |
| GatewaySubnet | ExpressRoute and VPN gateway | 10.124.0.0/27 | 27 | 10.124.0.4-10.124.0.30 |
| SNET\_DC\_10.124.0.32\_27 | Domain controllers | 10.124.0.32/27 | 27 | 10.124.0.36-10.124.0.62 |
| AzureFirewallSubnet | Azure Firewall | 10.124.0.64/26 | 59 | 10.124.0.68-10.124.0.126 |
| AzureBastionSubnet | Azure Bastion | 10.124.0.128/26 | 59 | 10.124.0.132-10.124.0.190 |
| SNET\_Infra\_10.124.0.192\_26 | Shared infrastructure services | 10.124.0.192/26 | 59 | 10.124.0.196-10.124.0.254 |
| SNET\_MyWizard\_10.124.1.0\_26 | MyWizard monitoring solution | 10.124.1.0/26 | 59 | 10.124.1.4-10.124.1.62 |
| SNET\_JmpHosts\_10.124.1.64\_26 | Jump Hosts to support management | 10.124.1.64/26 | 59 | 10.124.1.68-10.124.1.126 |
| AppGatewaySNET\_10.124.1.128\_25 | Application Gateway | 10.124.1.128/25 | 123 | 10.124.1.132-10.124.1.254 |
| PrivateLink-HUB-USEast | Private Endpoints | 10.124.2.0/25 | 123 | 10.124.2.4-10.124.2.126 |
| Function-App1-10.124.2.128-27 | Function Apps | 10.124.2.128/27 | 27 | 10.124.2.128 - 10.124.2.159 |
| Function-App2-10.124.2.160-27 | Function Apps | 10.124.2.160/27 | 27 | 10.124.2.160 - 10.124.2.191 |
| Unused | Available to create additional subnets | 10.124.2.0/25 | 123 | 10.124.2.132-10.124.2.254 |
| Unused | Available to create additional subnets | 10.124.3.0/24 | 251 | 10.124.3.4-10.124.3.254 |
| DomainJoin-10.124.2.192-27 | Domain Join | 10.124.2.192/27 | 27 | 10.124.2.192 - 10.124.2.223 |

An NSG will be associated with each subnet except for the Gateway and Azure Firewall Subnets as those two do not permit NSGs.

For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

Vnet

|  |  |
| --- | --- |
| **HUB\_Citrix\_w365\_nva\_WestEU** | **10.15.161.0/24** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet Name | Purpose | Subnet ID | # of Hosts | Subnet Range |
| GatewaySubnet | VPN gateway | 10.15.161.0/27 | 27 | 10.15.161.0 - 10.15.161.31 |
| Citrix\_w365\_nva\_Subnet\_WestEU | VDI connectivity nva | 10.15.161.128/25 | 123 | 10.15.161.128 - 10.15.161.255 |

An NSG will be associated with each subnet except for the Gateway and Azure Firewall Subnets as those two do not permit NSGs.

For more information on NSGs see [Inter-subnet security approach](file:///C:/Users/lohitha.garigipati/Downloads/Baker%20Hughes%20Cloud%20Foundations%20Design%20Document%20v3.10%20-%20HUB%20West%20Us%20and%20SAP%20updated.docx#_Inter-subnet_security_approach)

#### West Europe HUB

Vnet

|  |  |
| --- | --- |
| HUB-WestEU | 10.124.32.0/22 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet Name | Purpose | Subnet ID | # of Hosts | Subnet Range |
| GatewaySubnet | ExpressRoute and VPN gateway | 10.124.32.0/27 | 27 | 10.124.32.4-10.124.32.30 |
| SNET\_DC\_10.124.32.32\_27 | Domain controllers | 10.124.32.32/27 | 27 | 10.124.32.36-10.124.32.62 |
| AzureFirewallSubnet | Azure Firewall | 10.124.32.64/26 | 59 | 10.124.32.68-10.124.32.126 |
| AzureBastionSubnet | Azure Bastion | 10.124.32.128/26 | 59 | 10.124.32.132-10.124.32.190 |
| SNET\_Infra\_10.124.32.192\_26 | Shared infrastructure services | 10.124.32.192/26 | 59 | 10.124.32.196-10.124.32.254 |
| SNET\_MyWizard\_10.124.33.0 \_26 | MyWizard monitoring solution | 10.124.33.0/26 | 59 | 10.124.32.4-10.124.32.62 |
| AppGatewaySNET\_10.124.33.128\_25 | Application Gateway | 10.124.33.128/25 | 123 | 10.124.33.132-10.124.33.254 |
| SNET\_JmpHosts\_10.124.33.64\_26 | Jump Hosts to support management | 10.124.33.64/26 | 59 | 10.124.33.68-10.124.33.126 |
| PrivateLink-HUB-WestEU | Private Endpoints | 10.124.34.0/25 | 123 | 10.124.34.4-10.124.34.126 |
| Unused | Available to create additional subnets | 10.124.34.0/25 | 123 | 10.124.34.132-10.124.34.254 |
| Unused | Available to create additional subnets | 10.124.35.0/24 | 251 | 10.124.35.4-10.124.35.254 |

An NSG will be associated with each subnet except for the Gateway and Azure Firewall Subnets as those two do not permit NSGs.

For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

Vnet

|  |  |
| --- | --- |
| **HUB\_Citrix\_w365\_nva\_EastUS** | **10.15.129.0/24** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet Name | **Purpose** | **Subnet ID** | **# of Hosts** | **Subnet Range** |
| **GatewaySubnet** | VPN gateway | 10.15.129.0/27 | 27 | 10.15.129.0 - 10.15.129.31 |
| **Citrix\_w365\_nva\_Subnet\_EastUS** | VDI connectivity nva East US | 10.15.129.128/25 | 27 | 10.15.129.128 - 10.15.129.255 |

An NSG will be associated with each subnet except for the Gateway and Azure Firewall Subnets as those two do not permit NSGs.

For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

#### West US HUB

The following tables contain the subnets and configurations in the West US Hub.

Vnet

|  |  |
| --- | --- |
| HUB-USWest | 10.127.0.0/22 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet Name | Purpose | Subnet ID | # of Hosts | Subnet Range |
| SNET-DR-DC | ExpressRoute and VPN gateway | 10.127.0.32/27 | 27 | 10.127.0.32 - 10.127.0.63 |
| SNET-DR-MyWizard | MyWizard monitoring solution | 10.127.1.0/26 | 27 | 10.127.1.0 - 10.127.1.63 |
| SNET-DR-JmpHosts | Jump Hosts to support management | 10.127.1.64/26 | 59 | 10.127.1.64 - 10.127.1.127 |
| SNET-DR-AppGateway | Application Gateway | 10.127.1.128/25 | 59 | 10.127.1.128 - 10.127.1.255 |
| SNET-DR-PrivateLink | Private Endpoints | 10.127.2.0/25 | 59 | 10.127.2.0 - 10.127.2.127 |
| AzureFirewallSubnet | Azure Firewall | 10.127.0.64/26 | 59 | 10.127.0.64 - 10.127.0.127 |
| AzureBastionSubnet | Azure Bastion | 10.127.0.192/26 | 123 | 10.127.0.192 - 10.127.0.255 |
| GatewaySubnet | ExpressRoute and VPN gateway | 10.127.0.0/27 | 59 | 10.127.0.0 - 10.127.0.31 |
| SNET-DR-Infra | Shared infrastructure services | 10.127.0.128/26 | 123 | 10.127.0.128 - 10.127.0.191 |

An NSG will be associated with each subnet except for the Gateway and Azure Firewall Subnets as those two do not permit NSGs.

For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

### Spoke Design

#### High-Level Design

NSGs will be implement at Baker Hughes to provide micro-segmentation. The number of NSG rules that can be applied to a single NSG is 1,000. Each spoke will have a /22 address space, which allows for 1024 IPs within the scope. The subnets on each spoke will be divided into /24 address spaces, mainly for ease of use and to provide an easily recognizable subnet identifier.



Figure 1: Spoke subnets

#### East US Prod Spoke

|  |  |
| --- | --- |
| Vnet |  |
| **Spoke-Prod-USEast-1** | **10.124.8.0/21** |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | Subnet CIDR | Subnet Address Range | Subnet Description |
| Internal-App-10.124.8.0-24 | 10.124.8.0/24 | 10.124.8.4-10.124.8.254 | Internal Applications |
| External-App-10.124.9.0-24 | 10.124.9.0/24 | 10.124.9.4-10.124.9.254 | External Applications |
| Internal-DB-10.124.10.0-24 | 10.124.10.0/24 | 10.124.10.4-10.124.10.254 | DBs for Internal Apps |
| External-DB-10.124.11.0-24 | 10.124.11.0/24 | 10.124.11.4-10.124.11.254 | DBs for External Apps |
| Internal-SQLMI-10.124.12.0-24 | 10.124.12.0/24 | 10.124.12.4-10.124.12.254 | Managed Instances for Internal Apps |
| External-SQLMI-10.124.14.0-24 | 10.124.14.0/24 | 10.124.14.4-10.124.14.254 | Managed Instances for External Apps |
| PrivateLink-Spoke-Prod-USEast-1 | 10.124.15.0/25 | 10.124.15.0 - 10.124.15.127 |  |
| Internal-App-10.124.88.128-25 | 10.124.88.128/25 | 10.124.88.128 - 10.124.88.255 |  |
| FlexiServer-MySQL-10.124.15.192-26 | 10.124.15.192/26 | 10.124.15.192 - 10.124.15.255 |  |
| AGW-V2-Spoke-Prod-USEast-1 | 10.124.96.0/24 | 10.124.96.0 - 10.124.96.255 |  |
| Container-Spoke-Prod-USEast-1 | 10.126.192.64/27 | 10.126.192.64 - 10.126.192.95 |  |
| FlexiServer-PostgreSQL-10.124.15.128-26 | 10.124.15.128/26 | 10.124.15.128 - 10.124.15.191 |  |
| Internal-App-10.124.84.0-22 | 10.124.84.0/22 | 10.124.84.0 - 10.124.87.255 |  |
| AGW-Spoke-Prod-USEast-1 | 10.124.13.0/24 | 10.124.13.4-10.124.13.254 | App Gateways for Prod |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

#### East US NonProd Spoke

Vnet

|  |  |
| --- | --- |
| Spoke-NonProd-USEast-1 | 10.124.16.0/21 |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | Subnet CIDR | Subnet Address Range | Subnet Description |
| Internal-App-10.124.16.0-24 | 10.124.16.0/24 | 10.124.16.4-10.124.16.254 | Internal Applications |
| External-App-10.124.17.0-24 | 10.124.17.0/24 | 10.124.17.4-10.124.17.254 | External Applications |
| Internal-DB-10.124.18.0-24 | 10.124.18.0/24 | 10.124.18.4-10.124.18.254 | DBs for Internal Apps |
| External-DB-10.124.19.0-24 | 10.124.19.0/24 | 10.124.19.4-10.124.19.254 | DBs for External Apps |
| Function-App2-10.15.222.32-27 | 10.15.222.32/27 | 10.15.222.32 - 10.15.222.63 |  |
| FlexiServer-PostgreSQL-10.124.20.128-26 | 10.124.20.128/26 | 10.124.20.128 - 10.124.20.191 |  |
| PrivateLink-Spoke-NonProd-USEast-1 | 10.124.20.0/25 | 10.124.20.0 - 10.124.20.127 |  |
| Extended-100.64.0.0-17 | 100.64.0.0/17 | 100.64.0.0 - 100.64.127.255 |  |
| AGW-V2-Spoke-NonProd-USEast-1 | 10.124.176.0/24 | 10.124.176.0 - 10.124.176.255 |  |
| Container-Spoke-NonProd-USEast-1 | 10.126.64.0/27 | 10.126.64.0 - 10.126.64.31 |  |
| Internal-App-10.124.80.0-22 | 10.124.80.0/22 | 10.124.80.0 - 10.124.83.255 |  |
| Internal-SQLMI-10.124.23.0-24 | 10.124.23.0/24 | 10.124.23.4-10.124.23.254 | Managed Instances for Internal Apps |
| External-SQLMI-10.124.22.0-24 | 10.124.22.0/24 | 10.124.22.4-10.124.22.254 | Managed Instances for External Apps |
| Function-App1-10.15.222.0-27 | 10.15.222.0/27 | 10.15.222.0 - 10.15.222.31 |  |
| FlexiServer-MySQL-10.124.20.192-26 | 10.124.20.192/26 | 10.124.20.192 - 10.124.20.255 |  |
| AGW-Spoke-NonProd-USEast-1 | 10.124.21.0/23 | 10.124.21.4-10.124.21.254 | App Gateways for Non Prod |
| PrivateLink-SpokeNonProd-USEast-1 | 10.124.20.0/24 | 10.124.20.4-10.124.20.254 | Private Endpoints |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

#### East US HC Prod Spoke

Vnet

|  |  |
| --- | --- |
| Spoke-HCProd-USEast-1 | 10.124.4.0/22 |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | Subnet CIDR | Subnet Address Range | Subnet Description |
| Internal-App-10.124.4.0-25 | 10.124.4.0/25 | 10.124.4.4-10.124.4.126 | Internal Applications |
| External-App-10.124.4.128-25 | 10.124.4.128/25 | 10.124.4.132-10.124.4.254 | External Applications |
| Internal-DB-10.124.5.0-25 | 10.124.5.0/25 | 10.124.5.4-10.124.5.126 | DBs for Internal Apps |
| External-DB-10.124.5.128-25 | 10.124.5.128/25 | 10.124.5.132-10.124.5.254 | DBs for External Apps |
| Internal-MISQL-10.124.6.0-25 | 10.124.6.0/25 | 10.124.6.4-10.124.6.126 | Managed Instances for Internal Apps |
| External-MISQL-10.124.6.128-25 | 10.124.6.128/25 | 10.124.6.132-10.124.6.254 | Managed Instances for External Apps |
| AGW-Spoke-HCProd-USEast-1 | 10.124.7.0/25 | 10.124.7.4-10.124.7.126 | App Gateways for HC Prod |
| Internal-SQLMI-10.124.6.0-25 | 10.124.6.0/25 | 10.124.6.0 - 10.124.6.127 |  |
| PrivateLink-SpokeHCProd-USEast-1 | 10.124.7.128/25 | 10.124.7.132-10.124.7.254 | Private Endpoints |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

#### East US HC NonProd Spoke

Vnet

|  |  |
| --- | --- |
| Spoke-HCNonProd-USEast | 10.124.24.0/22 |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | Subnet CIDR | Subnet Address Range | Subnet Description |
| Internal-App-10.124.24.0-25 | 10.124.24.0/25 | 10.124.24.4-10.124.24.127 | Internal Applications |
| External-App-10.124.24.128-25 | 10.124.24.128/25 | 10.124.24.132-10.124.24.254 | External Applications |
| Internal-DB-10.124.25.0-25 | 10.124.25.0/25 | 10.124.25.4-10.124.25.127 | DBs for Internal Apps |
| External-DB-10.124.25.128-25 | 10.124.25.128/25 | 10.124.25.132-10.124.25.254 | DBs for External Apps |
| Internal-MISQL-10.124.26.0-25 | 10.124.26.0/25 | 10.124.26.4-10.124.26.126 | Managed Instances for Internal Apps |
| External-MISQL-10.124.26.128-25 | 10.124.26.128/25 | 10.124.26.132-10.124.26.254 | Managed Instances for External Apps |
| AGW-Spoke-HCProd-USEast-1 | 10.124.27.0/25 | 10.124.27.4-10.124.27.126 | App Gateways for HC Prod |
| PrivateLink-SpokeHCProd-USEast-1 | 10.124.27.128/25 | 10.124.7.132-10.124.27.254 | Private Endpoints |
| Internal-App-10.124.89.0-25 | 10.124.89.0/25 | 10.124.89.0 - 10.124.89.127 | Internal Applications |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

#### West EU Prod Spoke

Vnet

|  |  |
| --- | --- |
| SPOKE-Prod-WestEU-1 | 10.124.40.0/21 |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | Subnet CIDR | Subnet Address Range | Subnet Description |
| Internal-App-10.124.40.0-24 | 10.124.40.0/24 | 10.124.40.4-10.124.40.254 | Internal Applications |
| External-App-10.124.41.0-24 | 10.124.41.0/24 | 10.124.41.4-10.124.41.254 | External Applications |
| Internal-DB-10.124.42.0-24 | 10.124.42.0/24 | 10.124.42.4-10.124.42.254 | DBs for Internal Apps |
| External-DB-10.124.43.0-24 | 10.124.43.0/24 | 10.124.43.4-10.124.43.254 | DBs for External Apps |
| Internal-MISQL-10.124.44.0-24 | 10.124.44.0/24 | 10.124.44.4-10.124.44.254 | Managed Instances for Internal Apps |
| External-MISQL-10.124.46.0-24 | 10.124.46.0/24 | 10.124.46.4-10.124.46.254 | Managed Instances for External Apps |
| AGW-Spoke-Prod-WestEU-1 | 10.124.45.0/24 | 10.124.45.4-10.124.45.254 | App Gateways for Prod |
| PrivateLink-SpokeProd-WestEU-1 | 10.124.46.0/24 | 10.124.46.4-10.124.46.254 | Private Endpoints |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

#### West EU NonPod Spoke

Vnet

|  |  |
| --- | --- |
| SPOKE-Non-Prod-WestEU-1 | 10.124.48.0/21 |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | Subnet CIDR | Subnet Address Range | Subnet Description |
| Internal-App-10.124.48.0-24 | 10.124.48.0/24 | 10.124.48.4-10.124.48.254 | Internal Applications |
| External-App-10.124.49.0-24 | 10.124.49.0/24 | 10.124.49.4-10.124.49.254 | External Applications |
| Internal-DB-10.124.50.0-24 | 10.124.50.0/24 | 10.124.50.4-10.124.50.254 | DBs for Internal Apps |
| External-DB-10.124.51.0-24 | 10.124.51.0/24 | 10.124.51.4-10.124.51.254 | DBs for External Apps |
| Internal-MISQL-10.124.53.0-24 | 10.124.53.0/24 | 10.124.53.4-10.124.53.254 | Managed Instances for Internal Apps |
| External-MISQL-10.124.54.0-24 | 10.124.54.0/24 | 10.124.54.4-10.124.54.254 | Managed Instances for External Apps |
| AGW-Spoke-Prod-WestEU-1 | 10.124.52.0/24 | 10.124.52.4-10.124.52.254 | App Gateways for Non Prod |
| PrivateLink-SpokeProd-WestEU-1 | 10.124.55.0/24 | 10.124.55.4-10.124.55.254 | Private Endpoints |
| FlexiServer-MySQL-10.124.55.192-26 | 10.124.55.192/26 | 10.124.55.192 - 10.124.55.255 |  |
| FlexiServer-PostgreSQL-10.124.55.128-26 | 10.124.55.128/26 | 10.124.55.128 - 10.124.55.191 |  |
| Extended-AKS-100.67.0.0-17 | 100.67.0.0/17 | 100.67.0.0 - 100.67.127.255 |  |
| AGW-Spoke-NonProd-WestEU-1 | 10.124.52.0/24 | 10.124.52.0 - 10.124.52.255 |  |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

*3.3.5.6* Industrial Asset Management

Vnet:

|  |  |
| --- | --- |
| **Spoke\_IAM\_Dev\_NON\_PROD\_EastUS** | **10.15.192.0/21** |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| AGW\_nprod\_Subnet\_EastUS | 10.15.201.128/26 | 10.15.201.128 - 10.15.201.191 | App Gateways for Non Prod |
| Extended-AKS-100.74.128.0-21 | 100.74.128.0/21 | 100.74.128.0 - 100.74.135.255 | Kubernetes for Non prod |
| SN-DBKS-10.15.192.0-21 | 10.15.192.0/21 | 10.15.192.0 - 10.15.199.255 | Data bricks for Non prod |
| SN-EXDBKS-100.74.144.0-21 | 100.74.144.0/21 | 100.74.144.0 - 100.74.151.255 | Data bricks for Non prod |
| SN-PostgreSQLFlexi-10.15.201.192-27 | 10.15.201.192/27 | 10.15.201.192 -10.15.201.223 | Postgre SQL |
| Private\_endpoint\_Subnet\_EastUS | 10.15.201.0/25 | 10.15.201.0 - 10.15.201.127 | Private Endpoints |
| SN-DBKS-10.126.48.0-21 | 10.126.48.0/21 | 10.126.48.0 - 10.126.55.255 | DBKS |
| SNET\_AKS\_SPARQ | 100.65.0.0/21 | 100.65.0.0 - 100.65.7.255 | AKS |
| SNET-IAM-Dev-Non-Prod-Functionapp2 | 10.15.201.224/27 | 10.15.201.224 - 10.15.201.255 | FunctionApp |
| SN-EXDBKS-100.74.152.0-21 | 100.74.152.0/21 | 100.74.152.0 - 100.74.159.255 | Extended DBKS |
| IAM\_App\_nprod\_Subnet\_EastUS | 10.15.200.0/24 | 10.15.200.0 - 10.15.200.255 | Internal applications |

3.3.5.7 VWE

Vnet:

|  |  |
| --- | --- |
| **Spoke\_VWE\_NON\_PROD\_EastUS** | **10.15.128.0/24** |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| Internal\_SQMI\_Non\_prod\_Subnet\_EastUS | 10.15.128.192/27 | 10.15.128.192 - 10.15.128.223 | Internal SQL instances |
| W365\_Non\_prod\_Subnet\_EastUS | 10.15.128.0/26 | 10.15.128.0 - 10.15.128.63 | W365 instances |
| Internal\_Non\_prod\_Subnet\_EastUS | 10.15.128.128/26 | 10.15.128.128 - 10.15.128.191 | Internal Applications |
| AVD\_Non\_prod\_Subnet\_EastUS | 10.15.128.64/26 | 10.15.128.64 - 10.15.128.127 | Virtual Desktops |
| NetApp\_Files\_Non\_prod\_Subnet-EastUS | 10.15.206.0/28 | 10.15.206.0 - 10.15.206.15 | NetApp Files |
| Private\_endpoint\_Subnet\_EastUS | 10.15.128.224/27 | 10.15.128.224 - 10.15.128.255 | Private Endpoints |

#### West EU HC Prod Spoke

Vnet

|  |  |
| --- | --- |
| SPOKE-HCProd-WestEU-1 | 10.124.36.0/22 |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | Subnet CIDR | Subnet Address Range | Subnet Description |
| Internal-App-10.124.36.0-25 | 10.124.36.0/25 | 10.124.36.4-10.124.36.127 | Internal Applications |
| External-App-10.124.36.128-25 | 10.124.36.128/25 | 10.124.36.132-10.124.36.254 | External Applications |
| Internal-DB-10.124.37.0-25 | 10.124.37.0/25 | 10.124.37.4-10.124.37.127 | DBs for Internal Apps |
| External-DB-10.124.37.128-25 | 10.124.37.128/25 | 10.124.37.132-10.124.37.254 | DBs for External Apps |
| Internal-SQLMI-10.124.38.0-25 | 10.124.38.0/25 | 10.124.38.4-10.124.38.127 | Managed Instances for Internal Apps |
| External-SQLMI-10.124.38.128-25 | 10.124.38.128/25 | 10.124.38.132-10.124.38.254 | Managed Instances for External Apps |
| AGW-Spoke-HCProd-WestEU-1 | 10.124.39.0/25 | 10.124.39.4-10.124.39.127 | App Gateways for HC Prod |
| PrivateLink-SpokeHCProd-WestEU-1 | 10.124.39.128/25 | 10.124.39.132-10.124.39.254 | Private Endpoints |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

#### West EU HC Non-Prod Spoke

Vnet

|  |  |
| --- | --- |
| SPOKE-HCNon-Prod-WestEU-1 | 10.124.56.0/22 |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | Subnet CIDR | Subnet Address Range | Subnet Description |
| Internal-App-10.124.56.0-25 | 10.124.56.0/25 | 10.124.56.4-10.124.56.127 | Internal Applications |
| External-App-10.124.56.128-25 | 10.124.56.128/25 | 10.124.56.132-10.124.56.254 | External Applications |
| Internal-DB-10.124.57.0-25 | 10.124.57.0/25 | 10.124.57.4-10.124.57.127 | DBs for Internal Apps |
| External-DB-10.124.57.128-25 | 10.124.57.128/25 | 10.124.57.132-10.124.57.254 | DBs for External Apps |
| Internal-SQLMI-10.124.58.0-25 | 10.124.58.0/25 | 10.124.58.4-10.124.58.127 | Managed Instances for Internal Apps |
| External-SQLMI-10.124.58.128-25 | 10.124.58.128/25 | 10.124.58.132-10.124.58.254 | Managed Instances for External Apps |
| AGW-Spoke-HCNon-Prod-WestEU-1 | 10.124.59.0/25 | 10.124.59.4-10.124.59.127 | App Gateways for HC Non Prod |
| PrivateLink-Spoke HCNon-Prod-WestEU-1 | 10.124.59.128/25 | 10.124.59.132-10.124.59.254 | Private Endpoints |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

#### Joint Venture Prod Spoke

Vnet

|  |  |
| --- | --- |
| Spoke-JV-Prod | 10.124.64.0/23 |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | Subnet CIDR | Subnet Address Range | Subnet Description |
| Internal-App-10.124.64.0-26 | 10.124.64.0/26 | 10.124.64.4-10.124.64.63 | Internal Applications |
| External-App-10.124.64.64-26 | 10.124.64.64/26 | 10.124.64.68-10.124.64.127 | External Applications |
| Internal-DB-10.124.64.128-26 | 10.124.64.128/26 | 10.124.64.132-10.124.64.191 | DBs for Internal Apps |
| External-DB-10.124.64.192-26 | 10.124.64.192/26 | 10.124.64.196-10.124.64.254 | DBs for External Apps |
| Internal-SQLMI-10.124.65.0-26 | 10.124.65.0/26 | 10.124.65.4-10.124.65.63 | Managed Instances for Internal Apps |
| External-SQLMI-10.124.65.128-26 | 10.124.65.128/26 | 10.124.65.132-10.124.65.191 | Managed Instances for External Apps |
| AGW-Spoke-JV-Prod | 10.124.65.64/26 | 10.124.65.68-10.124.65.127 | App Gateways for JV Prod |
| PrivateLink-SpokeJV-Prod | 10.124.65.192/26 | 10.124.65.196-10.124.65.254 | Private Endpoints |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

#### Joint Venture NonProd Spoke

Vnet

|  |  |
| --- | --- |
| Spoke-JV-NonProd | 10.124.66.0/23 |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | Subnet CIDR | Subnet Address Range | Subnet Description |
| Internal-App-10.124.66.0-26 | 10.124.66.0/26 | 10.124.66.4-10.124.66.63 | Internal Applications |
| External-App-10.124.66.64-26 | 10.124.66.64/26 | 10.124.66.68-10.124.66.127 | External Applications |
| Internal-DB-10.124.66.128-26 | 10.124.66.128/26 | 10.124.66.132-10.124.66.191 | DBs for Internal Apps |
| External-DB-10.124.66.192-26 | 10.124.66.192/26 | 10.124.66.196-10.124.66.254 | DBs for External Apps |
| Internal-Manage-10.124.67.0-26 | 10.124.67.0/26 | 10.124.67.4-10.124.67.63 | Managed Instances for Internal Apps |
| External-SQLMI-10.124.67.128-26 | 10.124.67.128/26 | 10.124.67.132-10.124.67.191 | Managed Instances for External Apps |
| AGW-Spoke-JV-NonProd | 10.124.67.64/26 | 10.124.67.68-10.124.67.127 | App Gateways for JV Non Prod |
| PrivateLink-Spoke-JV-NonProd | 10.124.67.192/26 | 10.124.67.196-10.124.67.254 | Private Endpoints |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](https://myoffice.accenture.com/personal/lohitha_garigipati_accenture_com/Documents/Desktop/Baker%20Hughes%20Cloud%20Foundations%20Design%20Document%20v3.10.docx#_Inter-subnet_security_approach)

#### VWE Non Prod Spoke

Vnet:

|  |  |
| --- | --- |
| **Spoke\_VWE\_NON\_PROD\_westEU** | **10.15.160.0/24** |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| AVD\_Non\_prod\_Subnet\_westEU | 10.15.160.64/26 | 10.15.160.64 - 10.15.160.127 | Virtual Desktops |
| Internal\_SQMI\_Non\_prod\_Subnet\_westEU | 10.15.160.192/27 | 10.15.160.192 - 10.15.160.223 | Internal Applications |
| W365\_Non\_prod\_Subnet\_westEU | 10.15.160.0/26 | 10.15.160.0 - 10.15.160.63 | W365 instances |
| NetApp\_Files\_Non\_prod\_Subnet\_westEU | 10.124.191.0/28 | 10.124.191.0 - 10.124.191.15 | NetApp Files |
| Internal\_Non\_prod\_Subnet\_westEU | 10.15.160.128/26 | 10.15.160.128 - 10.15.160.191 | Internal Applications |
| Private\_endpoint\_Subnet\_westEU | 10.15.160.224/27 | 10.15.160.224 - 10.15.160.255 | Private Endpoints |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](#_Inter-subnet_security_approach)

#### SAP PreProd Spoke

Vnet

|  |  |
| --- | --- |
| Spoke\_SAP\_PreProd\_EastUS | 10.124.134.0/24 |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | Subnet CIDR | Subnet Address Range | Subnet Description |
| SNET-SAP-PreProd-External-AppsVM | 10.124.134.64/26 | 10.124.66.4-10.124.66.63 | External Applications |
| SNET-SAP-PreProd-Internal-DB | 10.124.134.128/27 | 10.124.66.68-10.124.66.127 | DBs for Internal Apps |
| SNET-SAP-PreProd-PrivateLink | 10.124.134.192/27 | 10.124.66.132-10.124.66.191 | Private end points |
| SNET-SAP-PreProd-AppGateway | 10.124.134.224/27 | 10.124.66.196-10.124.66.254 | Application Gateway |
| SNET-SAP-PreProd-External-DB | 10.124.134.160/27 | 10.124.67.4-10.124.67.63 | DBs for External Apps |
| SNET-SAP-PreProd-Internal-AppsVM | 10.124.134.0/26 | 10.124.67.132-10.124.67.191 | Internal Applications |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](https://myoffice.accenture.com/personal/lohitha_garigipati_accenture_com/Documents/Desktop/Baker%20Hughes%20Cloud%20Foundations%20Design%20Document%20v3.10.docx#_Inter-subnet_security_approach)

#### SAP Prod Spoke

|  |  |
| --- | --- |
| Spoke\_SAP\_Prod\_EastUS | 10.124.128.0/22 |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | Subnet CIDR | Subnet Address Range | Subnet Description |
| SNET-SAP-Prod-Internal-AppsVM | 10.124.128.0/24 | 10.124.128.0 - 10.124.128.255 | Internal Applications |
| SNET-SAP-Prod-External-AppsVM | 10.124.129.0/24 | 10.124.129.0 - 10.124.129.255 | External Applications |
| SNET-SAP-Prod-Internal-DB | 10.124.130.0/25 | 10.124.130.0 - 10.124.130.127 | DBs for Internal Apps |
| SNET-SAP-Prod-External-DB | 10.124.130.128/25 | 10.124.130.128 -10.124.130.255 | DBs for External Apps |
| SNET-SAP-Prod-PrivateLink | 10.124.131.0/25 | 10.124.131.0 - 10.124.131.127 | Private end points |
| SNET-SAP-Prod-AppGateway | 10.124.131.128/25 | 10.124.131.128 -10.124.131.255 | Application gate ways |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](file:///C:/Users/lohitha.garigipati/Downloads/Baker%20Hughes%20Cloud%20Foundations%20Design%20Document%20v3.10.doc.docx#_Inter-subnet_security_approach)

#### SAP Non Prod Spoke

|  |  |
| --- | --- |
| Spoke\_SAP\_Non\_Prod\_EastUS | 10.124.107.0/24 10.124.136.0/22 |

Subnets:

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | Subnet CIDR | Subnet Address Range | Subnet Description |
| SNET-SAP-NonProd-External-AppsVM | 10.124.137.0/24 | 10.124.137.0 - 10.124.137.255 | External applications |
| SNET-SAP-NonProd-Internal-DB | 10.124.138.0/25 | 10.124.138.0 - 10.124.138.127 | DBs for Internal Apps |
| SNET-SAP-NonProd-External-DB | 10.124.138.128/25 | 10.124.138.128 - 10.124.138.255 | DBs for External Apps |
| SNET-SAP-NonProd-PrivateLink | 10.124.139.0/25 | 10.124.139.0 - 10.124.139.127 | Private end points |
| SNET-SAP-NonProd-AppGateway | 10.124.139.128/25 | 10.124.139.128 - 10.124.139.255 | Application Gateways |
|  |  |  |  |

#### 1.1.1.1 SPK3-TESTING-US

|  |  |  |  |
| --- | --- | --- | --- |
| Vnet |  |  |  |
| **IAMPreProd-SPK3-TESTING-US** | **10.126.57.32/27 , 10.126.57.128/27** |  |  |
|  |  |  |  |
| **Subnet Name** | **Purpose** | **Subnet ID** | **# of Hosts** |
| SNET-IAMPreProd-AppGateway | MyWizard monitoring solution | 10.126.57.32/28 | 27 |
| **SNET-IAMPreProd-AppsVM** | Shared infrastructure services | 10.126.57.48/28 | 27 |
| 1.1.1.2 NIC-bhazl04110006d-001 |  |  |  |
| Vnet |  |  |  |
| **NIC-bhazl04110006d-001** | **100.64.0.0/17** |  |  |
|  |  |  |  |
| **Subnet Name** | **Purpose** | **Subnet ID** | **# of Hosts** |
| Extended-100.64.0.0-17 |  |  | 27 |
|  |  |  |  |
|  |  |  |  |
| 1.1.1.3 SPK3-TESTING-WESTUS Vnet |  |  |  |
| **NonHCNonProd-SPK3-TESTING-WESTUS** | **10.127.16.64/26** |  |  |
|  |  |  |  |
| **Subnet Name** | **Purpose** | **Subnet ID** | **# of Hosts** |
| SNET-NonHCNonProd-AppGateway | Application Gateway | 10.127.16.64/28 | 27 |
| **SNET-NonHCNonProd-AppsVM** | Application VMs | 10.127.16.80/28 | 27 |
| 1.1.1.4 BHCAzureC- EastUS-dev-01 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-EastUS-dev-01** | **10.124.190.0/24** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppGateway | 10.124.190.0/27 | 10.124.190.0 - 10.124.190.31 | application gateway |
| SNET-BakerHughes\_BHCAzureC-EastUS-AKSExtended | 10.124.190.32/27 | 10.124.190.32 - 10.124.190.63 |  |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppsVM | 10.124.190.64/27 | 10.124.190.64 - 10.124.190.95 | Application Vms |
| SNET-BakerHughes\_BHCAzureC-EastUS-PrivateLink | 10.124.190.96/27 | 10.124.190.96 - 10.124.190.127 | private endpoints |
| SNET-BakerHughes\_BHCAzureC-EastUS-Postgres-Flexiserver | 10.124.190.128/27 | 10.124.190.128 - 10.124.190.159 |  |
| SNET-BakerHughes\_BHCAzureC-EastUS-DatabricksCluster | 10.124.190.192/27 | 10.124.190.192 - 10.124.190.223 |  |
| SNET-BakerHughes\_BHCAzureC-EastUS-DatabricksCluster-Extended | 10.124.190.224/27 | 10.124.190.224 - 10.124.190.255 |  |
|  |  |  |  |
| 1.1.1.5 BHCAzureC-EastUS-dev-02 |  |  |  |
|  |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-EastUS-dev-02** | **10.126.65.0/24,** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppsVM | 10.126.65.0/26 | 10.126.65.0 - 10.126.65.63 | Application VMs |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppGateway | 10.126.65.64/28 | 10.126.65.64 - 10.126.65.79 | application gateway |
| SNET-BakerHughes\_BHCAzureC-EastUS-PrivateLink | 10.126.65.96/27 | 10.126.65.96 - 10.126.65.127 | private end points |
| SNET-BakerHughes\_BHCAzureC-EastUS-AKSExtended | 100.68.0.0/21 | 100.68.0.0 - 100.68.7.255 |  |
| SNET-BakerHughes\_BHCAzureC-EastUS-Postgres-Flexiserver | 10.126.65.80/28 | 10.126.65.80 - 10.126.65.95 |  |
|  |  |  |  |
| 1.1.1.6 BHCAzureC-EastUS-dev-09 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-EastUS-dev-09** | **10.126.66.0/23** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppsVM | 10.126.66.0/24 | 10.126.66.0 - 10.126.66.255 | Applicatin VMS |
| SNET-BakerHughes\_BHCAzureC-EastUS-PrivateLink | 10.126.67.0/25 | 10.126.67.0/25 | Application gateway |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppGateway | 10.126.67.160/27 | 10.126.67.160 - 10.126.67.191 | DBs for Internal Apps |
| SNET-BakerHughes\_BHCAzureC-EastUS-AKSExtended | 100.68.8.0/21 | 100.68.8.0 - 100.68.15.255 |  |
| SNET-BakerHughes\_BHCAzureC-EastUS-Postgres-Flexiserver | 10.126.67.128/27 | 10.126.67.128 - 10.126.67.159 |  |
|  |  |  |  |
| 1.1.1.7 BHCAzureC-EastUS-dev10-10 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-EastUS-dev10-10** | **10.126.57.160/29** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-EastUS-PrivateLink | 10.126.57.160/29 | 10.126.57.160/29 | private enpoints |
| 1.1.1.8 BHCAzureC-EastUS-preprod-01 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-EastUS-preprod-01** | **10.126.57.96/27** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-EastUS-DatabricksCluster-Extended | 10.126.57.96/28 | 10.126.57.96 - 10.126.57.111 |  |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppsVM | 10.126.57.112/28 | 10.126.57.112 - 10.126.57.127 | Application VMs |
|  |  |  |  |
|  |  |  |  |
| 1.1.1.9 BHCAzureC-EastUS-preprod-04 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-EastUS-preprod-04** | **10.126.160.0/23** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppsVM | 10.126.160.0/24 | 10.126.160.0 - 10.126.160.255 | Application VMS |
| SNET-BakerHughes\_BHCAzureC-EastUS-Postgres-Flexiserver | 10.126.161.0/27 | 10.126.161.0 - 10.126.161.31 | Application gateway |
| SNET-BakerHughes\_BHCAzureC-EastUS-PrivateLink | 10.126.161.32/27 | 10.126.161.32 - 10.126.161.63 | private endpoints |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppGateway | 10.126.161.64/28 | 10.126.161.64 - 10.126.161.79 | Application gateway |
|  |  |  |  |
|  |  |  |  |
| 1.1.1.10 BHCAzureC-EastUS-prod-01 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-EastUS-prod-01** | **10.126.192.0/26** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppGateway | 10.126.192.0/28 | 10.126.192.0 - 10.126.192.15 | application gateway |
| SNET-BakerHughes\_BHCAzureC-EastUS-PrivateLink | 10.126.192.16/28 | 10.126.192.16 - 10.126.192.31 | Private endpoints |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppsVM | 10.126.192.32/27 | 10.126.192.32 - 10.126.192.63 | Application VMs |
|  |  |  |  |
| 1.1.1.11 BHCAzureC-EastUS-prod-02 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-EastUS-prod-02** | **10.126.226.128/25** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppsVM | 10.126.226.128/27 | 10.126.226.128 - 10.126.226.159 | Application VMs |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppGateway | 10.126.226.160/27 | 10.126.226.160 - 10.126.226.191 | Application gateway |
| SNET-BakerHughes\_BHCAzureC-EastUS-PrivateLink | 10.126.226.224/27 | 10.126.226.224 - 10.126.226.255 | Private endpoints |
| SNET-BakerHughes\_BHCAzureC-EastUS-AKSExtended | 100.92.8.0/21 | 100.92.8.0 - 100.92.15.255 |  |
| SNET-BakerHughes\_BHCAzureC-EastUS-Postgres-Flexiserver | 10.126.226.192/27 | 10.126.226.192 - 10.126.226.223 |  |
|  |  |  |  |
| 1.1.1.12 BHCAzureC-EastUS-prod-09 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-EastUS-prod-09** | **10.126.196.0/23** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppsVM | 10.126.196.0/24 | 10.126.196.0 - 10.126.196.255 | Application VMs |
| SNET-BakerHughes\_BHCAzureC-EastUS-AKSExtended | 100.88.0.0/21 | 100.88.0.0 - 100.88.7.255 |  |
| SNET-BakerHughes\_BHCAzureC-EastUS-AppGateway | 10.126.197.160/27 | 10.126.197.160 - 10.126.197.191 | Application gateway |
| SNET-BakerHughes\_BHCAzureC-EastUS-PrivateLink | 10.126.197.0/25 | 10.126.197.0 - 10.126.197.127 | Private endpoint |
| SNET-BakerHughes\_BHCAzureC-EastUS-Postgres-Flexiserver | 10.126.197.128/27 | 10.126.197.128 - 10.126.197.159 |  |
|  |  |  |  |
| 1.1.1.13 BHCAzureC-WestEU-dev-01 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-WestEU-dev-01** | **10.17.113.96/27** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppGateway | 10.17.113.96/28 | 10.17.113.96 - 10.17.113.111 | application gateway |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppsVM | 10.17.113.128/28 | 10.17.113.128 - 10.17.113.143 | Application Vms |
|  |  |  |  |
|  |  |  |  |
| 1.1.1.14 BHCAzureC-WestEU-dev-02 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-WestEU-dev-02** | **10.17.16.0/25** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppGateway | 10.17.16.112/28 | 10.17.16.112 - 10.17.16.127 | application gateway |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppsVM | 10.17.16.32/27 | 10.17.16.32 - 10.17.16.63 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-PrivateLink | 10.17.16.0/27 | 10.17.16.0 - 10.17.16.31 | Private endpoints |
| SNET-BakerHughes\_BHCAzureC-WestEU-FlexibleMySQL | 10.17.16.96/28 | 10.17.16.96 - 10.17.16.111 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-FunctionApp | 10.17.16.64/27 | 10.17.16.64 - 10.17.16.95 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-FunctionApp1 | 10.17.16.192/28 | 10.17.16.192 - 10.17.16.207 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-FunctionApp2 | 10.17.16.208/28 | 10.17.16.208 - 10.17.16.223 |  |
|  |  |  |  |
| 1.1.1.15 BHCAzureC-WestEU-dev-12 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-WestEU-dev-12** | **10.17.16.160/27 , 100.104.0.192/28 , 100.104.0.216/29 , 100.104.0.224/27** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppsDB | 10.17.16.160/29 | 10.17.16.160 - 10.17.16.167 | DBS for Application |
| SNET-BakerHughes\_BHCAzureC-WestEU-ANF | 10.17.16.168/29 | 10.17.16.168 - 10.17.16.175 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster | 10.17.16.176/29 | 10.17.16.176 - 10.17.16.183 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-AKS-Routable | 10.17.16.184/29 | 10.17.16.184 - 10.17.16.191 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-PostgreSQL-NonRoutable | 100.104.0.192/28 | 100.104.0.192 - 100.104.0.207 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-AKSExtended | 100.104.0.224/29 | 100.104.0.224 - 100.104.0.231 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster-Extended | 100.104.0.232/29 | 100.104.0.232 - 100.104.0.239 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-PostgreSQL-NonRoutable1 | 100.104.0.240/29 | 100.104.0.240 - 100.104.0.247 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster-Extended1 | 100.104.0.248/29 | 100.104.0.248 - 100.104.0.255 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-AKSExtended1 | 100.104.0.216/29 | 100.104.0.216 - 100.104.0.223 |  |
|  |  |  |  |
| 1.1.1.16 BHCAzureC-WestEU-dev-13 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-WestEU-dev-13** | **10.17.16.128/28 , 10.17.16.144/28 , 100.104.0.88/29 , 100.104.0.96/27 , 100.104.0.128/26 , 100.104.0.208/29** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppsDB | 10.17.16.144/29 | 10.17.16.144 - 10.17.16.151 | DBS for applications |
| SNET-BakerHughes\_BHCAzureC-WestEU-AKS-Routable | 10.17.16.152/29 | 10.17.16.152 - 10.17.16.159 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster-Extended | 100.104.0.208/29 | 100.104.0.208 - 100.104.0.215 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppsVM | 10.17.16.128/29 | 10.17.16.128 - 10.17.16.135 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-AKS-Routable1 | 10.17.16.136/29 | 10.17.16.136 - 10.17.16.143 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-AKSExtended | 100.104.0.88/29 | 100.104.0.88 - 100.104.0.95 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-PostgreSQL-NonRoutable | 100.104.0.96/29 | 100.104.0.96 - 100.104.0.103 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster-Extended1 | 100.104.0.104/29 | 100.104.0.104 - 100.104.0.111 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster-Extended2 | 100.104.0.112/29 | 100.104.0.112 - 100.104.0.119 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-PostgreSQL-NonRoutable1 | 100.104.0.120/29 | 100.104.0.120 - 100.104.0.127 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster-Extended3 | 100.104.0.184/29 | 100.104.0.184 - 100.104.0.191 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-AKSExtended1 | 100.104.0.176/29 | 100.104.0.176 - 100.104.0.183 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-AKSExtended2 | 100.104.0.168/29 | 100.104.0.168 - 100.104.0.175 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-PostgreSQL-NonRoutable2 | 100.104.0.160/29 | 100.104.0.160 - 100.104.0.167 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster-Extended4 | 100.104.0.152/29 | 100.104.0.152 - 100.104.0.159 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-PostgreSQL-NonRoutable3 | 100.104.0.144/29 | 100.104.0.144 - 100.104.0.151 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-AKSExtended3 | 100.104.0.136/29 | 100.104.0.136 - 100.104.0.143 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-AKSExtended4 | 100.104.0.128/29 | 100.104.0.128 - 100.104.0.135 |  |
|  |  |  |  |
| 1.1.1.17 BHCAzureC-WestEU-dev11-11 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-WestEU-dev11-11** | **10.17.32.128/26 , 100.96.128.0/21** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppsVM | 10.17.32.160/27 | 10.17.32.160 - 10.17.32.191 | Application Vms |
| SNET-BakerHughes\_BHCAzureC-WestEU-PrivateLink | 10.17.32.128/28 | 10.17.32.128 - 10.17.32.143 | Private endpoints |
| SNET-BakerHughes\_BHCAzureC-WestEU-AKSExtended | 100.96.128.0/21 | 100.96.128.0 - 100.96.135.255 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-Postgres-Flexiserver | 10.17.32.144/28 | 10.17.32.144 - 10.17.32.159 |  |
|  |  |  |  |
| 1.1.1.18 BHCAzureC-WestEU-preprod-02 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-WestEU-preprod-02** | **10.17.66.0/25,** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppsVM | 10.17.66.0/27 | 10.17.66.0 - 10.17.66.31 | Application VMs |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppGateway | 10.17.66.32/27 | 10.17.66.32 - 10.17.66.63 | Application Gateways |
| SNET-BakerHughes\_BHCAzureC-WestEU-PrivateLink | 10.17.66.96/27 | 10.17.66.96 - 10.17.66.127 | Private endpoints |
| SNET-BakerHughes\_BHCAzureC-WestEU-AKSExtended | 100.116.16.0/21 | 100.116.16.0 - 100.116.23.255 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster-Extended | 100.116.24.0/21 | 100.116.24.0 - 100.116.31.255 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster-Extended1 | 100.116.8.0/21 | 100.116.8.0 - 100.116.15.255 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster-Extended2 | 100.116.32.0/26 | 100.116.32.0 - 100.116.32.63 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster | 10.17.66.128/26 | 10.17.66.128 - 10.17.66.191 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-Postgres-Flexiserver | 10.17.66.64/27 | 10.17.66.64 - 10.17.66.95 |  |
|  |  |  |  |
|  |  |  |  |
| 1.1.1.19 BHCAzureC-WestEU-prod-02 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-WestEU-prod-02** | **10.127.98.0/23** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppGateway | 10.127.99.64/28 | 10.127.99.64 - 10.127.99.79 | application gateway |
| SNET-BakerHughes\_BHCAzureC-WestEU-PrivateLink | 10.127.99.32/27 | 10.127.99.32 - 10.127.99.63 | Private end points |
| SNET-BakerHughes\_BHCAzureC-WestEU-Postgres-Flexiserver | 10.127.99.0/27 | 10.127.99.0 - 10.127.99.31 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppsVM | 10.127.98.0/24 | 10.127.98.0 - 10.127.98.255 | Application Vms |
|  |  |  |  |
| 1.1.1.20 BHCAzureC-WestEU-prod-04 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-WestEU-prod-04** | **10.17.96.0/25 , 10.17.96.128/25 , 10.17.97.0/25 , 10.17.100.0/22 , 100.124.0.0/21 , 100.124.8.0/23 , 100.124.10.0/23** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppsVM | 10.17.96.128/27 | 10.17.96.128 - 10.17.96.159 | applicationVMs |
| SNET-BakerHughes\_BHCAzureC-WestEU-PrivateLink | 10.17.96.160/27 | 10.17.96.160 - 10.17.96.191 | Private endpoints |
| SNET-BakerHughes\_BHCAzureC-WestEU-AppGateway | 10.17.96.224/27 | 10.17.96.224 - 10.17.96.255 | Application gateway |
| SNET-BakerHughes\_BHCAzureC-WestEU-AKSExtended | 100.124.0.0/21 | 100.124.0.0 - 100.124.7.255 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster | 10.17.100.0/23 | 10.17.100.0 - 10.17.101.255 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster1 | 10.17.102.0/23 | 10.17.102.0 - 10.17.103.255 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster-Extended | 100.124.8.0/23 | 100.124.8.0 - 100.124.9.255 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-DatabricksCluster-Extended1 | 100.124.10.0/23 | 100.124.10.0 - 100.124.11.255 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-PrivateLink1 | 10.17.96.0/25 | 10.17.96.0 - 10.17.96.127 | Prvate endpoints |
| SNET-BakerHughes\_BHCAzureC-WestEU-Postgres-Flexiserver1 | 10.17.97.0/25 | 10.17.97.0 - 10.17.97.127 |  |
| SNET-BakerHughes\_BHCAzureC-WestEU-Postgres-Flexiserver | 10.17.96.192/27 | 10.17.96.192 - 10.17.96.223 |  |
|  |  |  |  |
| 1.1.1.21 BHCAzureC-WestUS-prod-01 |  |  |  |
| Vnet |  |  |  |
| **SPOKE-BakerHughes\_BHCAzureC-WestUS-prod-01** | **10.127.4.0/22** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-BakerHughes\_BHCAzureC-WestUS-AppsDB | 10.127.6.0/25 | 10.127.6.0 - 10.127.6.127 | applicationDBs |
| SNET-BakerHughes\_BHCAzureC-WestUS-AppsVM | 10.127.4.0/24 | 10.127.4.0 - 10.127.4.255 | Application VMs |
| SNET-BakerHughes\_BHCAzureC-WestUS-AppGateway | 10.127.7.128/25 | 10.127.7.128 - 10.127.7.255 | Application Gateway |
| SNET-BakerHughes\_BHCAzureC-WestUS-PrivateLink | 10.127.7.0/25 | 10.127.7.0 - 10.127.7.127 | Private endpints |
| SNET-BakerHughes\_BHCAzureC-WestUS-AppsVM1 | 10.127.5.0/24 | 10.127.5.0 - 10.127.5.255 | Application VMS1 |
| SNET-BakerHughes\_BHCAzureC-WestUS-AppsDB1 | 10.127.6.128/25 | 10.127.6.128 - 10.127.6.255 | Application DBs |
|  |  |  |  |
| 1.1.1.22 DBKSCM-Prod-EastUS |  |  |  |
| Vnet |  |  |  |
| **Spoke-DBKSCM-Prod-EastUS** | **10.15.221.0/24 , 100.74.168.0/25** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-INF-DBKSCM-Extended | 100.74.168.0/26 | 100.74.168.0 - 100.74.168.63 |  |
| SNET-INF-DBKSCM | 10.15.221.64/26 | 10.15.221.64 - 10.15.221.127 |  |
| SNET-INF-DBKS-PrivateLink | 10.15.221.0/26 | 10.15.221.0 - 10.15.221.63 | Private endpoints |
|  |  |  |  |
| 1.1.1.23 DBKSCM-Prod-WestEU |  |  |  |
| Vnet |  |  |  |
| **Spoke-DBKSCM-Prod-WestEU** | **10.124.188.0/24 , 100.74.168.128/25** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-INF-DBKSCM-Extended | 100.74.168.128/26 | 100.74.168.128 - 100.74.168.191 |  |
| SNET-INF-DBKSCM | 10.124.188.0/26 | 10.124.188.0 - 10.124.188.63 |  |
| SNET-INF-DBKS-PrivateLink | 10.124.188.64/26 | 10.124.188.64 - 10.124.188.127 | Private endpoints |
|  |  |  |  |
|  |  |  |  |
| 1.1.1.24 IAM\_C3\_Dev\_Non\_Prod\_westeu |  |  |  |
| Vnet |  |  |  |
| **Spoke\_IAM\_C3\_Dev\_Non\_Prod\_westeu** | **10.124.186.0/23 , 100.77.224.0/21** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-IAM-C3-DEV-AKS | 100.77.224.0/21 | 100.77.224.0 - 100.77.231.255 |  |
| SNET-IAM-C3-DEV-AppGateway | 10.124.187.128/26 | 10.124.187.128 - 10.124.187.191 | Application Gateway |
| SNET-IAM-C3-DEV-AppsVM | 10.124.186.0/24 | 10.124.186.0 - 10.124.186.255 | Application Vms |
| SNET-IAM-C3-DEV-PrivateLink | 10.124.187.0/25 | 10.124.187.0 - 10.124.187.127 | Private endpoints |
| SNET-IAM-C3-DEV-PostgreSQLFlexi | 10.124.187.192/27 | 10.124.187.192 - 10.124.187.223 |  |
|  |  |  |  |
|  |  |  |  |
| 1.1.1.25 IAM\_C3\_PreProd\_westeu |  |  |  |
| Vnet |  |  |  |
| **Spoke\_IAM\_C3\_PreProd\_westeu** | **10.17.64.0/23 , 100.116.0.0/21** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-IAM-C3-PreProd-AKS | 100.116.0.0/21 | 100.116.0.0 - 100.116.7.255 |  |
| SNET-IAM-C3-PreProd-AppGateway | 10.17.65.128/26 | 10.17.65.128 - 10.17.65.191 | Application Gateway for preprod |
| SNET-IAM-C3-PreProd-AppsVM | 10.17.64.0/24 | 10.17.64.0 - 10.17.64.255 | Application VMs |
| SNET-IAM-C3-PreProd-PrivateLink | 10.17.65.0/25 | 10.17.65.0 - 10.17.65.127 | Private endpoint |
| SNET-IAM-C3-PreProd-PostgreSQLFlexi | 10.17.65.192/27 | 10.17.65.192 - 10.17.65.223 |  |
|  |  |  |  |
| 1.1.1.26 IAM\_Dev\_NON\_PROD\_WestEU |  |  |  |
| Vnet |  |  |  |
| **Spoke\_IAM\_Dev\_NON\_PROD\_WestEU** | **10.124.208.0/20 , 100.77.240.0/20** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-IAM-AppsVM | 10.124.208.0/24 | 10.124.208.0 - 10.124.208.255 | Application Vm |
| SNET-IAM-AKS-Extended | 100.77.240.0/21 | 100.77.240.0 - 100.77.247.255 |  |
| SNET-IAM-AppGateway | 10.124.210.0/26 | 10.124.210.0 - 10.124.210.63 | Application Gateway |
| SNET-IAM-PrivateLink | 10.124.209.0/25 | 10.124.209.0 - 10.124.209.127 | Private endpoint |
| SNET-IAM-DBKS-Extended | 100.77.248.0/21 | 100.77.248.0 - 100.77.255.255 |  |
| SNET-IAM-DBKS | 10.124.216.0/21 | 10.124.216.0 - 10.124.223.255 |  |
| SNET-IAM-PostgreSQLFlexi | 10.124.209.128/25 | 10.124.209.128 - 10.124.209.255 |  |
|  |  |  |  |
| 1.1.1.27 IAM\_Pet\_Non\_Prod\_EastUS |  |  |  |
| Vnet |  |  |  |
| **Spoke\_IAM\_Pet\_Non\_Prod\_EastUS** | **10.124.144.0/20 , 100.76.32.0/19** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-IAM-Pet-Non-Prod-AppsVM | 10.124.144.0/24 | 10.124.144.0 - 10.124.144.255 | applicationVM |
| SNET-IAM-Pet-Non-Prod-AKS-Extended | 100.76.32.0/21 | 100.76.32.0 - 100.76.39.255 |  |
| SNET-IAM-Pet-Non-Prod-AppGateway | 10.124.146.0/26 | 10.124.146.0 - 10.124.146.63 | Application Gateway |
| SNET-IAM-Pet-Non-Prod-PrivateLink | 10.124.145.0/25 | 10.124.145.0 - 10.124.145.127 | Private endpoint |
| SNET-IAM-Pet-Non-Prod-PostgreSQLFlexi | 10.124.145.128/25 | 10.124.145.128 - 10.124.145.255 |  |
| SNET-IAM-Pet-Non-Prod-Functionapp1 | 10.124.147.0/27 | 10.124.147.0/27 |  |
| SNET-IAM-Pet-Non-Prod-DBKS-Extended | 100.76.40.0/21 | 100.76.40.0 - 100.76.47.255 |  |
| SNET-IAM-Pet-Non-Prod-DBKS | 10.124.152.0/21 | 10.124.152.0 - 10.124.159.255 |  |
| SNET-IAM-Pet-Non-Prod-DBKS-Extended1 | 100.76.48.0/26 | 100.76.48.0 - 100.76.48.63 |  |
| SNET-IAM-Pet-Non-Prod-DBKS1 | 10.124.146.64/26 | 10.124.146.64 - 10.124.146.127 |  |
|  |  |  |  |
| 1.1.1.28 IAM\_PreProd\_EastUS |  |  |  |
| Vnet |  |  |  |
| **Spoke\_IAM\_PreProd\_EastUS** | **10.126.32.0/20 , 100.74.176.0/20** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-IAM-PreProd-AppsVM | 10.126.32.0/24 | 10.126.32.0 - 10.126.32.255 | application VM |
| SNET-IAM-PreProd-AKS-Extended | 100.74.176.0/21 | 100.74.176.0 - 100.74.183.255 |  |
| SNET-IAM-PreProd-AppGateway | 10.126.34.0/26 | 10.126.34.0 - 10.126.34.63 | Application Gateway |
| SNET-IAM-PreProd-PrivateLink | 10.126.33.0/25 | 10.126.33.0 - 10.126.33.127 | Private endpoint |
| SNET-IAM-PreProd-PostgreSQLFlexi | 10.126.33.128/25 | 10.126.33.128 - 10.126.33.255 |  |
| SNET-IAM-PreProd-DBKS-Extended | 100.74.184.0/21 | 100.74.184.0 - 100.74.191.255 |  |
| SNET-IAM-PreProd-DBKS | 10.126.40.0/21 | 10.126.40.0 - 10.126.47.255 |  |
|  |  |  |  |
| 1.1.1.29 \_IAM\_Prod\_EastUS |  |  |  |
| Vnet |  |  |  |
| **Spoke\_IAM\_Prod\_EastUS** | **10.15.240.0/20, 100.75.0.0/19** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-IAM-AKS-Extended | 100.75.8.0/21 | 100.75.8.0 - 100.75.15.255 |  |
| SNET-IAM-AppGateway | 10.15.241.0/26 | 10.15.241.0 - 10.15.241.63 | Application Gate way |
| SNET-IAM-AppsVM | 10.15.240.0/24 | 10.15.240.0 - 10.15.240.255 | Application VM |
| SNET-IAM-PrivateLink | 10.15.241.128/25 | 10.15.241.128 - 10.15.241.255 | Private endpoints |
| SNET-IAM-DBKS-Extended | 100.75.0.0/21 | 100.75.0.0 - 100.75.7.255 |  |
| SNET-IAM-DBKS | 10.15.248.0/21 | 10.15.248.0 - 10.15.255.255 |  |
| SNET-IAM-PostgreSQLFlexi | 10.15.242.0/25 | 10.15.242.0 - 10.15.242.127 |  |
|  |  |  |  |
| 1.1.1.30 iam\_qa\_non\_prod\_EastUS |  |  |  |
| Vnet |  |  |  |
| **Spoke\_iam\_qa\_non\_prod\_EastUS** | **10.15.224.0/20 , 100.74.224.0/19** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| AGW\_nprod\_Subnet\_EastUS | 10.15.233.128/26 | 10.15.233.128 - 10.15.233.191 |  |
| IAM\_qa\_App\_nprod\_Subnet\_EastUS | 10.15.232.0/24 | 10.15.232.0 - 10.15.232.255 | Application for QA |
| Extended-AKS-100.74.224.0-21 | 100.74.224.0/21 | 100.74.224.0 - 100.74.231.255 |  |
| SN-EXDBKS-100.74.232.0-21 | 100.74.232.0/21 | 100.74.232.0 - 100.74.239.255 | DBs for External Apps |
| SN-DBKS-10.15.224.0-21 | 10.15.224.0/21 | 10.15.224.0 - 10.15.231.255 |  |
| SNET-IAM-PostgreSQLFlexi-10.15.234.0-27 | 10.15.234.0/27 | 10.15.234.0 - 10.15.234.31 |  |
| Private\_endpoint\_Subnet\_EastUS | 10.15.233.0/25 | 10.15.233.0 - 10.15.233.127 | Private endpoints |
|  |  |  |  |
| 1.1.1.31 Non\_HC\_PreProd\_EastUS |  |  |  |
| Vnet |  |  |  |
| **Spoke\_Non\_HC\_PreProd\_EastUS** | **10.124.160.0/21 , 100.76.128.0/19** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-Non-HC-PreProd-Internal-App | 10.124.160.0/24 | 10.124.160.0 - 10.124.160.255 | internal applications |
| SNET-Non-HC-PreProd-External-App | 10.124.161.0/24 | 10.124.161.0 - 10.124.161.255 | External Applications |
| SNET-Non-HC-PreProd-AKS-Extended | 100.76.128.0/19 | 100.76.128.0 - 100.76.159.255 |  |
| SNET-Non-HC-PreProd-PostgreSQLFlexi | 10.124.167.128/26 | 10.124.167.128 - 10.124.167.191 |  |
| SNET-Non-HC-PreProd-MySQLFlexi | 10.124.167.192/26 | 10.124.167.192 - 10.124.167.255 |  |
| SNET-Non-HC-PreProd-Internal-SQLMI | 10.124.164.0/24 | 10.124.164.0 - 10.124.164.255 | Internal SQLMI instance |
| SNET-Non-HC-PreProd-Internal-DB | 10.124.162.0/24 | 10.124.162.0 - 10.124.162.255 | Dbs for internal |
| SNET-Non-HC-PreProd-External-DB | 10.124.163.0/24 | 10.124.163.0 - 10.124.163.255 | Dbs for External |
| SNET-Non-HC-PreProd-AppGateway | 10.124.165.0/24 | 10.124.165.0 - 10.124.165.255 | Application Gateway |
| SNET-Non-HC-PreProd-PrivateLink | 10.124.167.0/25 | 10.124.167.0 - 10.124.167.127 | Private endpoints |
| SNET-Non-HC-PreProd-Appservice | 10.124.166.0/28 | 10.124.166.0 - 10.124.166.15 |  |
|  |  |  |  |
| 1.1.1.32 Non\_HC\_PreProd\_WestEU |  |  |  |
| Vnet |  |  |  |
| **Spoke\_Non\_HC\_PreProd\_WestEU** | **10.124.192.0/21 , 100.76.160.0/19** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-Non-HC-PreProd-Internal-App | 10.124.192.0/24 | 10.124.192.0 - 10.124.192.255 | internal applications |
| SNET-Non-HC-PreProd-External-App | 10.124.193.0/24 | 10.124.193.0 - 10.124.193.255 | External Applications |
| SNET-Non-HC-PreProd-AKS-Extended | 100.76.160.0/19 | 100.76.160.0 - 100.76.191.255 |  |
| SNET-Non-HC-PreProd-PostgreSQLFlexi | 10.124.198.128/26 | 10.124.198.128 - 10.124.198.191 |  |
| SNET-Non-HC-PreProd-MySQLFlexi | 10.124.198.192/26 | 10.124.198.192 - 10.124.198.255 |  |
| SNET-Non-HC-PreProd-Internal-SQLMI | 10.124.194.0/24 | 10.124.194.0 - 10.124.194.255 | Internal SQLMI instance |
| SNET-Non-HC-PreProd-Internal-DB | 10.124.196.0/24 | 10.124.196.0 - 10.124.196.255 | Dbs for internal |
| SNET-Non-HC-PreProd-External-DB | 10.124.197.0/24 | 10.124.197.0 - 10.124.197.255 | Dbs for External |
| SNET-Non-HC-PreProd-AppGateway | 10.124.195.0/24 | 10.124.195.0 - 10.124.195.255 | Application Gateway |
| SNET-Non-HC-PreProd-PrivateLink | 10.124.198.0/25 | 10.124.198.0 - 10.124.198.127 | Private endpoints |
|  |  |  |  |
| 1.1.1.33 SAP\_ANF\_Prod\_USEast |  |  |  |
| Vnet |  |  |  |
| **Spoke\_SAP\_ANF\_Prod\_USEast** | **10.124.142.128/25** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-SAP\_ANF-Prod-USEast | 10.124.142.128/25 | 10.124.142.128 - 10.124.142.255 |  |
| 1.1.1.34 SAP\_ANF\_ProdDR\_WestUS |  |  |  |
| Vnet |  |  |  |
| **Spoke\_SAP\_ANF\_ProdDR\_WestUS** | **10.127.12.0/25** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-SAP\_ANF-ProdDR-WestUS | 10.127.12.0/25 | 10.127.12.0 - 10.127.12.127 |  |
|  |  |  |  |
| 1.1.1.35 Trials\_BHC3\_Dev\_Non\_Prod\_EastUS |  |  |  |
| Vnet |  |  |  |
| **Spoke\_Trials\_BHC3\_Dev\_Non\_Prod\_EastUS** | **10.124.108.0/23** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-Trials-BHC3-Dev-AppsVM | 10.124.108.64/26 | 10.124.108.64 - 10.124.108.127 | Application Vms |
| SNET-Trials-BHC3-Dev-AKS-Extended | 100.75.32.0/19 | 100.75.32.0 - 100.75.63.255 |  |
| SNET-Trials-BHC3-Dev-AppGateway | 10.124.109.0/24 | 10.124.109.0 - 10.124.109.255 | Applictaion gate way |
| SNET-Trials-BHC3-Dev-PrivateLink | 10.124.108.128/25 | 10.124.108.128 - 10.124.108.255 | Private endpoints |
| SNET-Trials-BHC3-Dev-PostgreSQLFlexi | 10.124.108.0/27 | 10.124.108.0 - 10.124.108.31 |  |
| 1.1.1.36 Trials\_BHC3\_Pre-Prod\_EastUS |  |  |  |
| Vnet |  |  |  |
| **Spoke\_Trials\_BHC3\_Pre-Prod\_EastUS** | **10.15.204.0/23** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| SNET-Trials-BHC3-Pre-Prod-AppsVM | 10.15.204.64/26 | 10.15.204.64 - 10.15.204.127 | application VMS |
| SNET-Trials-BHC3-Pre-Prod-AKS-Extended | 100.74.192.0/19 | 100.74.192.0 - 100.74.223.255 |  |
| SNET-Trials-BHC3-Pre-Prod-AppGateway | 10.15.205.0/24 | 10.15.205.0 - 10.15.205.255 | applicatioGateway |
| SNET-Trials-BHC3-Pre-Prod-PrivateLink | 10.15.204.128/25 | 10.15.204.128 - 10.15.204.255 | Private endpoints |
| SNET-Trials-BHC3-Pre-Prod-PostgreSQLFlexi | 10.15.204.0/27 | 10.15.204.0 - 10.15.204.31 |  |
|  |  |  |  |
| 1.1.1.37 VWE\_PROD\_EastUS |  |  |  |
| Vnet |  |  |  |
| **Spoke\_VWE\_PROD\_EastUS** | **10.6.64.0/18 , 10.15.144.0/20** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| W365\_prod\_Subnet\_EastUS | 10.15.152.0/22 | 10.15.152.0 - 10.15.155.255 | W365 instances |
| AVD\_prod\_Subnet\_EastUS | 10.15.156.0/22 | 10.15.156.0 - 10.15.159.255 | Virtual Desltops |
| Internal\_prod\_Subnet\_EastUS | 10.15.144.64/26 | 10.15.144.64 - 10.15.144.127 |  |
| Internal\_SQMI\_prod\_Subnet\_EastUS | 10.15.144.0/27 | 10.15.144.0 - 10.15.144.31 | Internal for SQMI instance |
| Private\_eandpoint\_Subnet\_EastUS | 10.15.144.32/27 | 10.15.144.32 - 10.15.144.63 | Private endpoints |
| W365\_prod\_Subnet2\_EastUS | 10.6.64.0/19 | 10.6.64.0 - 10.6.95.255 | W365 instances |
| AVD\_prod\_Subnet2\_EastUS | 10.6.96.0/19 | 10.6.96.0 - 10.6.127.255 | Virtual esktops |
|  |  |  |  |
| 1.1.1.38 . VWE\_PROD\_WestEU |  |  |  |
|  |  |  |  |
| Vnet |  |  |  |
| **Spoke\_VWE\_PROD\_WestEU** | **10.15.176.0/20** |  |  |
|  |  |  |  |
| Subnets: |  |  |  |
| **Subnet Name** | **Subnet CIDR** | **Subnet Address Range** | **Subnet Description** |
| Internal\_prod\_Subnet\_WestEU | 10.15.176.64/26 | 10.15.176.64 - 10.15.176.127 |  |
| Private\_endpoint\_Subnet\_WestEU | 10.15.176.32/27 | 10.15.176.32 - 10.15.176.63 | Private endpoints |
| Internal\_SQMI\_prod\_Subnet\_WestEU | 10.15.176.0/27 | 10.15.176.0 - 10.15.176.31 | Internal SQMI instance |
| AVD\_prod\_Subnet\_WestEU | 10.15.188.0/22 | 10.15.188.0 - 10.15.191.255 | Virtual desktops |
| W365\_prod\_Subnet\_WestEU | 10.15.184.0/22 | 10.15.184.0 - 10.15.187.255 | W365 instance |
| W365\_prod\_Subnet2\_WestEU | 10.6.192.0/19 | 10.6.192.0 - 10.6.223.255 | W365 instance |
| AVD\_prod\_Subnet2\_WestEU | 10.6.224.0/19 | 10.6.224.0 - 10.6.255.255 | Virtual desktops |

An NSG will be associated with each subnet. For more information on NSGs see [Inter-subnet security approach](file:///C:/Users/lohitha.garigipati/Downloads/Baker%20Hughes%20Cloud%20Foundations%20Design%20Document%20v3.10.doc.docx#_Inter-subnet_security_approach)

### Peerings

To connect the Vnets and provide communication between resources in the spoke Vnets, all spoke Vnets will be peered to their corresponding regional hub and the regional hubs will be peered together.

Peered networks direct traffic on the Microsoft Azure backbone and traffic never leaves the backbone to traverse the Internet or the Edge network.

#### Hub to Spoke Peering

The table below shows the peering connections that are from a Hub Vnet to a Spoke Vnet. There are five of these for each regional Hub.

|  |  |  |
| --- | --- | --- |
| **Peering Name** | **Source Network** | **Destination Network** |
| PN\_EASTUSHUB\_EASTUSPROD | HUB-USEast | [Spoke-Prod-USEast-1](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2Fed0ff387-ec1d-4d26-8869-01b07ff3ce8b%2FresourceGroups%2FRG-NONHCPROD1-EastUS%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FSpoke-Prod-USEast-1) |
| [PN\_EASTUSHUB\_WESTEUHUB](https://portal.azure.com/) | HUB-USEast | [HUB-WestEU](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2Fa5d2b45b-f9b1-4ad0-aee5-66160e64052c%2FresourceGroups%2FRG-NetworkHUB-WestEU%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FHUB-WestEU) |
| [SPOKE-JV-NonProd-Peering](https://portal.azure.com/) | HUB-USEast | [Spoke-JV-NonProd](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2Ff9d7ad5d-660f-491c-9f52-426cc2e8457c%2FresourceGroups%2FRG-Spoke-JV-NonProd%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FSpoke-JV-NonProd) |
| [SPOKE-JV-Prod-Peering](https://portal.azure.com/) | HUB-USEast | [Spoke-JV-Prod](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2Ff49cf858-3ed4-4636-a2d2-4487d30a05f3%2FresourceGroups%2FRG-Spoke-JV-Prod%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FSpoke-JV-Prod) |
| [PN\_EASTUSHUB\_EASTUSSANDBOX](https://portal.azure.com/) | HUB-USEast | [Spoke-Sandbox-USEast-1](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2F171023a7-2523-4aef-9f05-91d8031ab624%2FresourceGroups%2FRG-SANDBOX1-EastUS%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FSpoke-Sandbox-USEast-1) |
| [PN\_EASTUSHUB\_EASTUSHCNONPROD](https://portal.azure.com/) | HUB-USEast | [Spoke-HCNonProd-USEast-1](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2F93cd1533-23a2-46a1-a53e-09706aa281a4%2FresourceGroups%2FRG-HCNONPROD1-EastUS%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FSpoke-HCNonProd-USEast-1) |
| [PN\_EASTUSHCPROD\_EASTUSHUB](https://portal.azure.com/) | HUB-USEast | [Spoke-HCProd-USEast-1](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2Fe772571a-b0c5-4791-9c58-ff90e4cb9761%2FresourceGroups%2FRG-HCPROD1-EastUS%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FSpoke-HCProd-USEast-1) |
| [PN\_EASTUSNONPROD\_isolated\_remote](https://portal.azure.com/) | HUB-USEast | asr-vnet-isolated |
| [HUB-USEast](https://portal.azure.com/) | HUB-USEast | [Spoke-NonProd-USEast-1](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2F1752d638-2520-4aaf-81e3-df8c8f548c41%2FresourceGroups%2FRG-NONHCNONPROD1-EastUS%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FSpoke-NonProd-USEast-1) |
| [PN\_EASTUSHUB\_EASTUS\_VWE\_NonProd](https://portal.azure.com/) | HUB-USEast | [Spoke\_VWE\_NON\_PROD\_EastUS](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2F955ddc46-f459-4355-9dad-24bb66f280c6%2FresourceGroups%2FRG_Citrix_BH_w365_Infra_NonProd-eastUS%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FSpoke_VWE_NON_PROD_EastUS) |
| PN\_EASTUSHUB\_EASTUSNon\_PROD\_Dev\_IAM\_C3 | HUB-USEast | [spoke\_iam\_C3\_dev\_non\_prod\_eastUS](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2F49f7b216-0dd7-411f-b7fb-ad3fa4ba76af%2FresourceGroups%2Frg_infra_iam_c3_platform_dev_nonprod_eastus%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2Fspoke_iam_C3_dev_non_prod_eastUS) |
| PN\_EASTUSHUB\_EASTUSNon\_PROD\_Dev\_IAM | HUB-USEast | Spoke\_IAM\_Dev\_NON\_PROD\_EastUS |
| [PN\_WESTEUHUB\_WESTEUPROD](https://portal.azure.com/) | HUB-WestEU | [Spoke-Prod-WestEU-1](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2Fed0ff387-ec1d-4d26-8869-01b07ff3ce8b%2FresourceGroups%2FRG-NONHCPROD1-WestEU%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FSpoke-Prod-WestEU-1) |
| [PN\_WESTEUHUB\_EASTUSHUB](https://portal.azure.com/) | HUB-WestEU | HUB-USEast |
| [PN\_WESTEUHUB\_WESTEUHCNONPROD](https://portal.azure.com/) | HUB-WestEU | [Spoke-HCNonProd-WestEU-1](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2F93cd1533-23a2-46a1-a53e-09706aa281a4%2FresourceGroups%2FRG-HCNONPROD1-WestEU%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FSpoke-HCNonProd-WestEU-1) |
| PN\_WESTEUHCPROD\_WESTEUHUB | HUB-WestEU | [Spoke-HCProd-WestEU-1](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2Fe772571a-b0c5-4791-9c58-ff90e4cb9761%2FresourceGroups%2FRG-HCPROD1-WestEU%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FSpoke-HCProd-WestEU-1) |
| [HUB-WestEU](https://portal.azure.com/) | HUB-WestEU | [Spoke-NonProd-WestEU-1](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2F1752d638-2520-4aaf-81e3-df8c8f548c41%2FresourceGroups%2FRG-NONHCNONPROD1-WestEU%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FSpoke-NonProd-WestEU-1) |
| [Spoke\_VWE\_NON\_PROD\_westEU](https://portal.azure.com/) | HUB-WestEU | [Spoke\_VWE\_NON\_PROD\_westEU](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2F955ddc46-f459-4355-9dad-24bb66f280c6%2FresourceGroups%2FRG_Citrix_BH_w365_Infra_NonProd-westEU%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FSpoke_VWE_NON_PROD_westEU) |
| [PN\_WESTEUHUB\_WESTEU\_VWE\_NonProd](https://portal.azure.com/) | Spoke\_VWE\_NON\_PROD\_westEU | HUB-WestEU |

For these connections, the configuration should be as follows:

* Traffic to Remote Virtual Networks – Allow
* Traffic forwarded from remote virtual network – Allow
* Virtual Network Gateway or Route Server – Use this Virtual Network’s Gateway or Route Server

#### Spoke to Hub Peering

The table below shows the peering connections that are from a Spoke Vnet to a Hub Vnet.

|  |  |  |
| --- | --- | --- |
| Peering Name | Source Network | Destination Network |
| [PN\_EASTUSNONPROD\_isolated](https://portal.azure.com/) | asr-vnet-isolated | [HUB-USEast](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2Fa5d2b45b-f9b1-4ad0-aee5-66160e64052c%2FresourceGroups%2FRG-NetworkHUB-EastUS%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FHUB-USEast) |
| [PN\_EASTUSHCNONPROD\_EASTUSHUB](https://portal.azure.com/) | Spoke-HCNonProd-USEast-1 | [HUB-USEast](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2Fa5d2b45b-f9b1-4ad0-aee5-66160e64052c%2FresourceGroups%2FRG-NetworkHUB-EastUS%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FHUB-USEast) |
| [PN\_WESTEUHCNONPROD\_WESTEUHUB](https://portal.azure.com/) | Spoke-HCNonProd-WestEU-1 | HUB-WestEU |
| [PN\_EASTUSHUB\_EASTUSHCPROD](https://portal.azure.com/) | Spoke-HCProd-USEast-1 | [HUB-USEast](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2Fa5d2b45b-f9b1-4ad0-aee5-66160e64052c%2FresourceGroups%2FRG-NetworkHUB-EastUS%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FHUB-USEast) |
| PN\_WESTEUHUB\_WESTEUHCPROD | Spoke-HCProd-WestEU-1 | [HUB-WestEU](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2Fa5d2b45b-f9b1-4ad0-aee5-66160e64052c%2FresourceGroups%2FRG-NetworkHUB-WestEU%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FHUB-WestEU) |
| [HUB-Peering](https://portal.azure.com/) | Spoke-JV-NonProd | HUB-USEast |
| [HUB-Peering](https://portal.azure.com/) | Spoke-JV-Prod | HUB-USEast |
| [PN\_EASTUSNONPROD\_EASTUSHUB](https://portal.azure.com/) | Spoke-NonProd-USEast-1 | HUB-USEast |
| PN\_WESTEUNONPROD\_WESTEUHUB | Spoke-NonProd-WestEU-1 | HUB-WestEU |
| [PN\_EASTUSPROD\_EASTUSHUB](https://portal.azure.com/) | Spoke-Prod-USEast-1 | [HUB-USEast](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2Fa5d2b45b-f9b1-4ad0-aee5-66160e64052c%2FresourceGroups%2FRG-NetworkHUB-EastUS%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FHUB-USEast) |
| [PN\_WESTEUPROD\_WESTEUHUB](https://portal.azure.com/) | Spoke-Prod-WestEU-1 | HUB-WestEU |
| [spoke\_iam\_C3\_dev\_non\_prod\_eastUS](https://portal.azure.com/) | spoke\_iam\_C3\_dev\_non\_prod\_eastUS | HUB-USEast |
| [Spoke\_IAM\_Dev\_Non\_Prod-eastus](https://portal.azure.com/) | Spoke\_IAM\_Dev\_NON\_PROD\_EastUS | HUB-USEast |
| [Spoke-VWE-NonProd-USEast](https://portal.azure.com/) | Spoke\_VWE\_NON\_PROD\_EastUS | [HUB-USEast](https://portal.azure.com/#blade/Microsoft_Azure_Network/VirtualNetworkBlade/id/%2Fsubscriptions%2Fa5d2b45b-f9b1-4ad0-aee5-66160e64052c%2FresourceGroups%2FRG-NetworkHUB-EastUS%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FHUB-USEast) |
| PN\_SAP\_Spoke\_PreProd\_EASTUSHUB\_EASTUS | Spoke\_SAP\_PreProd\_EastUS | HUB-USEast |
| PN\_EASTUS\_SAP\_Spoke\_Prod\_EASTUSHUB | Spoke\_SAP\_Prod\_EastUS | HUB-USEast |
| PN\_SAP\_Spoke\_NonProd\_EASTUSHUB\_EASTUS | Spoke\_SAP\_Non\_Prod\_EastUS | HUB-USEast |

For these connections, the configuration should be as follows:

* Traffic to Remote Virtual Networks – Allow
* Traffic forwarded from remote virtual network – Allow
* Virtual Network Gateway or Route Server – Use the remote virtual network’s gateway or route server

#### Hub to Hub Peering

The table below shows the peering connections that are from a Hub Vnet to a Hub Vnet. There is one of these which connects US East to West EU.

|  |  |  |
| --- | --- | --- |
| Peering Name | Source Network | Destination Network |
| PN\_EASTUSHUB\_WESTEUHUB | East US Hub | West EU Hub |
| PN\_WESTEUHUB\_EASTUSHUB | West EU Hub | East US Prod |
| PN\_EASTUSHUB\_USWestHUB | East US Hub | West US Hub |
| PN\_WESTEUHUB\_USWestHUB | West EU Hub | West US Hub |

For these connections, the configuration should be as follows:

* Traffic to Remote Virtual Networks – Allow
* Traffic forwarded from remote virtual network – Allow
* Virtual Network Gateway or Route Server – Use this Virtual Network’s Gateway or Route Server

### On-Premises Connectivity

In each region, the Hubs will be connected to the BH On-Premises data centers via ExpressRoute and VPN Tunnels. These will each be connected in separate regions to create a failover should one data center lose connectivity. Additionally, these connections will be made with highly available SKUs. This can be seen because their gateway SUKs each end with Az which stands for Availability Zones. To build this with this setting, the Public IP must be a standard SKU with the desired Zones listed.

#### ExpressRoute

There are two ExpressRoute Circuits built to connect the Azure environment to Baker Hughes On-Premises, with one connection in each region – US East and West EU. Each of these circuits contain two routes, a primary and a secondary. If the primary connection goes down, then the secondary will serve as a failover.

Both of these circuits are with the Equinix Provider with the US East location in Dallas and the West EU in Dublin. For each circuit, there is a gateway, connection, and circuit that need to be configured. Below are the configurations for each of those resources for each region.

With the Express Route Circuit, including a shared key will ensure that the route is built with the encryption that was noted in the design.

##### US East Express Route

**Gateway:** **HUB-USEast-GW-ER**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-EastUS
* Location: East US
* Gateway SKU: ErGw2AZ
* Public IP SKU: Standard
* Public IP Zones: 1, 2, 3

**Circuit 1: EX-Equinix-Dallas**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-EastUS
* Location: East US
* SKU Tier: Standard
* SKU Family: MeteredData
* Provider: Equinix
* Peering Location: Dallas
* Bandwidth: 2000
* Peer ASN: 65512
* Primary Address Prefix: 10.87.4.120/30
* Secondary Prefix: 10.87.4.124/30
* vlanID: 312
* Shared Key: MwFgvqnfUicEQ2VlNjW6zpxYT

**Circuit 2: EX-Equinix-Ashburn-SAP-EastUS**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-EastUS
* Location: East US
* SKU Tier: Standard
* SKU Family: Metered Data
* Provider: Equinix
* Peering Location: Washington DC
* Bandwidth: 10000 Mbps
* Peer ASN: 65181
* Primary Address Prefix: 10.129.254.40/30
* Secondary Prefix: 10.129.254.44/30
* vlanID: 101
* Shared Key: NA

**Connection 1: CX-ER-USEast**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-EastUS
* Location: East US
* Virtual Network: HUB-USEast
* Gateway: HUB-USEast-GW-ER
* Circuit: EX-Equinix-Dallas
* Route Weight: 300

**Connection 2 : CX-ER-SAP-USEast**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-EastUS
* Location: East US
* Virtual Network: HUB-USEast
* Gateway: HUB-USEast-GW-ER
* Circuit: EX-Equinix-Ashburn-SAP-EastUS
* Route Weight: 0

##### West EU Express Route

**Gateway: HUB-WestEU-GW-ER**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestEU
* Location: West Europe
* Gateway SKU: ErGw2AZ
* Public IP SKU: Standard
* Public IP Zones: 1, 2, 3

**Circuit: EX-Equinix-Dublin**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestEU
* Location: West Europe
* SKU Tier: Standard
* SKU Family: MeteredData
* Provider: Equinix
* Peering Location: Dublin
* Bandwidth: 2000
* Peer ASN: 65469
* Primary Address Prefix: 10.163.252.224/30
* Secondary Prefix: 10.163.252.228/30
* vlanID: 1406
* Shared Key: MwFgvqnfUicEQ2VlNjW6zpxYT

**Connection : CX-ER-WestEU**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestEU
* Location: West Europe
* Virtual Network: HUB-WestEU
* Gateway: HUB-WestEU-GW-ER
* Circuit: EX-Equinix-Dublin
* Route Weight: 300

##### West US Express Route

**Gateway:** **HUB-USWest-GW-ER**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestUS
* Location: West US
* Gateway SKU: Standard
* Public IP SKU: Standard
* Public IP Zones: 1, 2, 3

**Circuit: EX-Equinix-Dallas**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestUS
* Location: West US
* SKU Tier: Standard
* SKU Family: MeteredData
* Provider: Equinix
* Peering Location: Dallas
* Bandwidth: 1000
* Peer ASN: 65512
* Primary Address Prefix: 10.87.4.24/30
* Secondary Prefix: 10.87.4.28/30
* vlanID: 315
* Shared Key:

## **Connection:** **CX-ER-USWest**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestUS
* Location: West US
* Virtual Network: HUB-USWest
* Gateway: HUB-USWest-GW-ER
* Circuit: EX-Equinix-Dallas01
* Route Weight: 300

#### VPN Tunnel

The IPSEC tunnel will mainly be used as a failover for the Express Route connection. If the ExpressRoute primary and secondary tunnels go down, then the VPN will serve as the main communication tunnel. These will be connected to separate data centers (Alpharetta in the US and London in EU) from the ExpressRoute to provide geo redundancy. Below is the configuration of the virtual network Gateway, Local Gateway and VPN Tunnel for each connection.

##### US East VPN

**Gateway: HUB-USEast-GW-VPN**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-EastUS
* Location: East US
* Gateway SKU: VpnGw3AZ
* Public IP SKU: Standard
* Public IP Zones: 1, 2, 3
* Gateway ASN: 65515
* VPN Type: Route Based

**Local Gateway: Local-HUB-USEast-GW**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-EastUS
* Location: East US
* Local Gateway Public IP: 147.108.62.14
* BGP Peering IP: 10.250.11.44
* BGP ASN: 65533
* Local Address Prefix: 10.250.11.44/32

**Connection: CX-VPN-USEast**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-EastUS
* Location: East US
* Virtual Network: HUB-USEast
* Gateway: HUB-USEast-GW-ER
* Local Gateway:
* Shared Key: MS8qNsev5gHFiIkTaavI+gm12GVDtODNwVsr6z0eBJ/3
* IKE Encryption: GCMAES256
* IKE Integrity: SHA256
* DH Group: ECP384
* IPSEC Encryption: GCMAES256
* PFS Group: ECP384
* SA Lifetime Seconds: 27000
* SA Data Size (KB): 102400000
* Route Weight: 200

**Gateway 2 : HUB-USEast-NVA-GW-VPN**

* Subscription: BH\_INFRA1
* Resource Group: RG\_HUB\_Citrix\_w365\_nva\_EastUS
* Location: East US
* Gateway SKU: VpnGw3AZ
* Public IP SKU: Standard
* Public IP Zones: 1, 2, 3
* Gateway ASN: 65515
* VPN Type: Route Based

**Local Gateway 2: Local-HUB-USEast-NVA-GW**

* Subscription: BH\_INFRA1
* Resource Group: RG\_HUB\_Citrix\_w365\_nva\_EastUS
* Location: East US
* Local Gateway Public IP: 208.127.231.247
* BGP Peering IP: 10.145.6.8
* BGP ASN: 65534
* Local Address Prefix: 10.145.6.8/32

**Connection 2:** **CX-VPN-NVA-USEast**

* Subscription: BH\_INFRA1
* Resource Group: RG\_HUB\_Citrix\_w365\_nva\_EastUS
* Location: East US
* Virtual Network: HUB\_Citrix\_w365\_nva\_EastUS
* Gateway: HUB-USEast-NVA-GW-VPN
* Circuit: NA
* Route Weight: NA

##### West EU VPN

**Gateway 1: HUB-WestEU-GW-VPN**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestEU
* Location: West Europe
* Gateway SKU: VpnGw3AZ
* Public IP SKU: Standard
* Public IP Zones: 1, 2, 3
* Gateway ASN: 65515
* VPN Type: Route Based

**Local Gateway1:** **Local-HUB-WestEU-GW**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestEU
* Location: West Europe
* Local Gateway Public IP: 147.108.148.14
* BGP Peering IP: 10.250.28.118
* BGP ASN: 65523
* Local Address Prefix: 10.250.28.118/32

**Local Gateway 1.1: Local-HUB-WestEU-GW2**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestEU
* Location: West Europe
* Local Gateway Public IP: 147.108.149.15
* BGP Peering IP: 10.250.28.140
* BGP ASN: 65523
* Local Address Prefix: 10.250.28.140/32

**Connection 1: CX-VPN-WestEU**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestEU
* Location: West Europe
* Virtual Network: HUB-WestEU
* Gateway: HUB-WestEU-GW-ER
* Local Gateway: Local-HUB-WestEU-GW
* Shared Key: MS8qNsev5gHFiIkTaavI+gm12GVDtODNwVsr6z0eBJ/3
* IKE Encryption: GCMAES256
* IKE Integrity: SHA256
* DH Group: ECP384
* IPSEC Encryption: GCMAES256
* PFS Group: ECP384
* SA Lifetime Seconds: 27000
* SA Data Size (KB): 102400000
* Route Weight: 200

**Connection 1.1: CX-VPN-WestEU2**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestEU
* Location: West Europe
* Virtual Network: HUB-WestEU
* Gateway: HUB-WestEU-GW-ER
* Local Gateway: Local-HUB-WestEU-GW2
* Shared Key:
* IKE Encryption: GCMAES256
* IKE Integrity: SHA256
* DH Group: ECP384
* IPSEC Encryption: GCMAES256
* PFS Group: ECP384
* SA Lifetime Seconds: 27000
* SA Data Size (KB): 102400000
* Route Weight: NA

**Gateway 2:** **HUB-EUWest-NVA-GW-VPN**

* Subscription: BH\_INFRA1
* Resource Group: RG\_HUB\_Citrix\_w365\_nva\_WestEU
* Location: West Europe
* Gateway SKU: VpnGw3AZ
* Public IP SKU: Standard
* Public IP Zones: 1, 2, 3
* Gateway ASN: 65515
* VPN Type: Route Based

**Local Gateway 2: Local-HUB-EUWest-NVA-GW**

* Subscription: BH\_INFRA1
* Resource Group: RG\_HUB\_Citrix\_w365\_nva\_WestEU
* Location: West Europe
* Local Gateway Public IP: 134.238.141.18
* BGP Peering IP: 10.15.161.30
* BGP ASN: 65515
* Local Address Prefix: 134.238.141.18/32

**Connection2: CX-VPN-NVA-EUWest**

* Subscription: BH\_INFRA1
* Resource Group: RG\_HUB\_Citrix\_w365\_nva\_WestEU
* Location: West Europe
* Virtual Network: HUB\_Citrix\_w365\_nva\_WestEU
* Local Gateway: Local-HUB-EUWest-NVA-GW(134.238.141.18)
* Shared Key:
* IKE Encryption: AES256
* IKE Integrity: SHA256
* DH Group: DHGroup14
* IPSEC Encryption: AES256
* PFS Group: ECP384
* SA Lifetime Seconds: 27000
* SA Data Size (KB): 102400000

##### West US VPN

##### **Gateway1 : HUB-USWest-GW-VPN**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestUS
* Location: West US
* Gateway SKU: VpnGw3
* Public IP SKU: Standard
* Public IP Zones: 1, 2, 3
* Gateway ASN: 65515
* VPN Type: Route Based

## **Local Gateway1 : Local-HUB-USWest-GW**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestUS
* Location: West US
* Local Gateway Public IP: 147.108.62.14
* BGP Peering IP: 10.250.11.44
* BGP ASN: 65533
* Local Address Prefix: 10.250.11.44/32

## **Connection: CX-VPN-USWest**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestUS
* Location: West US
* Virtual Network: HUB-USWest, HUB-USWest
* Gateway: HUB-USEast-GW-ER
* Local Gateway: Local-HUB-USWest-GW (147.108.62.14)
* Shared Key: MS8qNsev5gHFiIkTaavI+gm12GVDtODNwVsr6z0eBJ/3
* IKE Encryption: GCMAES256
* IKE Integrity: SHA256
* DH Group: ECP384
* IPSEC Encryption: GCMAES256
* PFS Group: ECP384
* SA Lifetime Seconds: 27000
* SA Data Size (KB): 102400000
* Route Weight: 200

## **Local Gateway: Local-HUB-USWest-GW2**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestUS
* Location: West US
* Local Gateway Public IP: 147.108.63.15
* BGP Peering IP: 10.250.11.46
* BGP ASN: 65533
* Local Address Prefix: 10.250.11.46/32

## **Connection: CX-VPN-USWest2**

* Subscription: BH\_INFRA1
* Resource Group: RG-NetworkHUB-WestUS
* Location: West US
* Virtual Network: HUB-USWest, HUB-USWest
* Gateway: HUB-USEast-GW2-ER
* Local Gateway: Local-HUB-USWest-GW2 (147.108.63.15)
* Shared Key: MS8qNsev5gHFiIkTaavI+gm12GVDtODNwVsr6z0eBJ/3
* IKE Encryption: GCMAES256
* IKE Integrity: SHA256
* DH Group: ECP384
* IPSEC Encryption: GCMAES256
* PFS Group: ECP384
* SA Lifetime Seconds: 27000
* SA Data Size (KB): 102400000
* Route Weight: 200

### User Defined Routing

To route traffic within Azure, route tables must be established and attached to the correct Subnets. Within this design, traffic should flow to the firewall for every route except within the subnet. This can be shown with the configuration below. Some subnets do not utilize route tables such as AzureBastion so that will not be listed below.

#### Hub Route Tables

**Routing tables for East US HUB Subnets**

Route Table **Route-HUB-USEast** has the following configuration:

* **Subscription** – BH\_Infra\_1
* **Resource Group –** RG-NetworkHUB-EastUS
* **Region** –East US
* **Propagate Gateway Routes** – No

This route table is attached to the subnets:

* SNET\_DC\_10.124.0.32\_27
* SNET\_Infra\_10.124.0.192\_26
* SNET\_MyWizard\_10.124.1.0\_26
* SNET\_JmpHosts\_10.124.1.64\_26

|  |  |  |  |
| --- | --- | --- | --- |
| Route Name | Address Prefix | Next Hop | Next Hop Address |
| Internet | 0.0.0.0/0 | HUB-USEast-1-Firewall | 10.124.0.68 |
| VirtualNetwork | 10.0.0.0/8 | HUB-USEast-1-Firewall | 10.124.0.68 |
| On-Premises1 | 172.16.0.0/12 | HUB-USEast-1-Firewall | 10.124.0.68 |
| On-Premises2 | 192.168.0.0/16 | HUB-USEast-1-Firewall | 10.124.0.68 |

**Routing tables for East US HUB Subnets**

Route Table **Route-PrivateLink-HUB-USEast** has the following configuration:

* **Subscription** – BH\_Infra\_1
* **Resource Group –** RG-NetworkHUB-EastUS
* **Region** –East US
* **Propagate Gateway Routes** – No

This route table is attached to the subnets:

* PrivateLink-HUB-USEast

|  |  |  |  |
| --- | --- | --- | --- |
| **Route Name** | **Address Prefix** | **Next Hop** | **Next Hop Address** |
| Internet | 0.0.0.0/0 | Virtual appliance | 10.124.0.68 |
| Internet | 0.0.0.0/0 | Virtual appliance | 10.124.0.68 |
| On-Premises2 | 172.16.0.0/12 | Virtual appliance | 10.124.0.68 |
| On-Premises2 | 172.16.0.0/12 | Virtual appliance | 10.124.0.68 |
| On-Premises4 | 147.108.0.0/16 | Virtual appliance | 10.124.0.68 |
| On-Premises5 | 3.0.0.0/8 | Virtual appliance | 10.124.0.68 |
| On-Premises6 | 151.95.0.0/18 | Virtual appliance | 10.124.0.68 |

Route Table **Route-HUB-USEast-AzureFirewallSubnet** has the following configuration:

* **Subscription** – BH\_Infra\_1
* **Resource Group** –RG-NetworkHUB-EastUS
* **Region** –East US
* **Propagate Gateway Routes** – Yes

This route table is attached to the subnet:

* AzureFirewallSubnet

|  |  |  |  |
| --- | --- | --- | --- |
| Route Name | Address Prefix | Next Hop | Next Hop Address |
| AzureWestEUHCNonProdSpoke | 10.124.56.0/22 | HUB-WestEU-1-Firewall | 10.124.32.68 |
| AzureWestEUHCProdSpoke | 10.124.36.0/22 | HUB-WestEU-1-Firewall | 10.124.32.68 |
| AzureWestEUHub | 10.124.32.0/22 | HUB-WestEU-1-Firewall | 10.124.32.68 |
| AzureWestEUNonProdSpoke | 10.124.48.0/21 | HUB-WestEU-1-Firewall | 10.124.32.68 |
| AzureWestEUProdSpoke | 10.124.40.0/21 | HUB-WestEU-1-Firewall | 10.124.32.68 |
| AzureWestEUSandboxSpoke | 10.124.60.0/23 | HUB-WestEU-1-Firewall | 10.124.32.68 |

Route Table **Route-HUB-USEast-GatewaySubnet** has the following configuration:

* **Subscription** – BH\_Infra\_1
* **Resource Group** –RG-NetworkHUB-EastUS
* **Region** –East US
* **Propagate Gateway Routes** – Yes

This route table is attached to the subnet:

* GatewaySubnet

|  |  |  |  |
| --- | --- | --- | --- |
| **Route Name** | **Address Prefix** | **Next Hop** | **Next Hop Address** |
| AzureUSEastHCNonProdSpoke | 10.124.24.0/22 | Virtual appliance | 10.124.0.68 |
| AzureUSEastHCProdSpoke | 10.124.4.0/22 | Virtual appliance | 10.124.0.68 |
| AzureUSEastHub | 10.124.0.0/22 | Virtual appliance | 10.124.0.68 |
| AzureUSEastJVNonProd | 10.124.66.0/23 | Virtual appliance | 10.124.0.68 |
| AzureUSEastJVProd | 10.124.64.0/23 | Virtual appliance | 10.124.0.68 |
| AzureUSEastNonProdSpoke | 10.124.16.0/21 | Virtual appliance | 10.124.0.68 |
| AzureUSEastProdSpoke | 10.124.8.0/21 | Virtual appliance | 10.124.0.68 |
| AzureUSEastSandboxSpoke | 10.124.28.0/22 | Virtual appliance | 10.124.0.68 |
| AzureUSEastIAMNonProdSpoke | 10.15.192.0/21 | Virtual appliance | 10.124.0.68 |
| AzureUSEastIAMNonProdSpoke-23 | 10.15.200.0/23 | Virtual appliance | 10.124.0.68 |
| AzureUSEastVWENonProdSpoke | 10.15.128.0/24 | Virtual appliance | 10.124.0.68 |
| AzureUSEastNonProdSpoke-2 | 10.124.80.0/22 | Virtual appliance | 10.124.0.68 |
| AzureUSEastIAMC3platformonProdSpoke | 10.15.202.0/23 | Virtual appliance | 10.124.0.68 |
| AzureUSEastHCNonProdSpoke-2 | 10.124.89.128/25 | Virtual appliance | 10.124.0.68 |
| AzureUSEastProdSpoke-2 | 10.124.84.0/22 | Virtual appliance | 10.124.0.68 |
| AzureUSEastHCNonProdSpoke-3 | 10.124.88.128/25 | Virtual appliance | 10.124.0.68 |
| AzureUSEastNonProdSpoke-3 | 10.124.88.0/25 | Virtual appliance | 10.124.0.68 |
| AzureUSEastHCNonProdSpoke-4 | 10.124.89.0/25 | Virtual appliance | 10.124.0.68 |
| AzureUSEastNonProdSpoke-4 | 10.124.176.0/24 | Virtual appliance | 10.124.0.68 |

Route Table has **Route\_HUB\_Citrix\_w365\_nva\_GatewaySubnet** the following configuration:

* **Subscription** – BH\_Infra\_1
* **Resource Group** –RG\_HUB\_Citrix\_w365\_nva\_EastUS
* **Region** –East US
* **Propagate Gateway Routes** – Yes

This route table is attached to the subnet:

* GatewaySubnet

| **Route Name** | **Address Prefix** | **Next Hop** | **Next Hop Address** |
| --- | --- | --- | --- |
| AzureUSEastVWENonProdSpoke | 10.15.128.0/24 | VirtualAppliance | 10.15.129.134 |
| AzureUSEastVWEProdSpoke | 10.15.144.0/20 | VirtualAppliance | 10.15.129.134 |
| AzureUSEastVWEProdSpoke2 | 10.6.64.0/18 | VirtualAppliance | 10.15.129.134 |
| AzureUSEastVWENonProdSpoke2 | 10.15.206.0/24 | VirtualAppliance | 10.15.129.134 |

**Routing tables for West EU HUB Subnets**

Route Table **Route-HUB-WestEU** has the following configuration:

* **Subscription** – BH\_Infra\_1
* **Resource Group** –RG-NetworkHUB-WestEU
* **Region** –West Europe
* **Propagate Gateway Routes** – No

This route table is attached to the subnets:

* SNET\_DC\_10.124.33.32\_27
* SNET\_Infra\_10.124.32.192\_26
* SNET\_MyWizard\_10.124.33.0\_26
* SNET\_JmpHosts\_10.124.33.64\_26

|  |  |  |  |
| --- | --- | --- | --- |
| Route Name | Address Prefix | Next Hop | Next Hop Address |
| Internet | 0.0.0.0/0 | HUB-WestEU-1-Firewall | 10.124.32.68 |
| VirtualNetwork | 10.0.0.0/8 | HUB-WestEU-1-Firewall | 10.124.32.68 |
| On-Premises1 | 172.16.0.0/12 | HUB-WestEU-1-Firewall | 10.124.32.68 |
| On-Premises2 | 192.168.0.0/16 | HUB-WestEU-1-Firewall | 10.124.32.68 |

Route Table **Route-PrivateLink-HUB-WestEU** has the following configuration:

* **Subscription** – BH\_Infra\_1
* **Resource Group** –RG-NetworkHUB-WestEU
* **Region** –West Europe
* **Propagate Gateway Routes** – No

This route table is attached to the subnets:

* PrivateLink-HUB-WestEU

|  |  |  |  |
| --- | --- | --- | --- |
| **Route Name** | **Address Prefix** | **Next Hop** | **Next Hop Address** |
| Internet | 0.0.0.0/0 | Virtual appliance | 10.124.32.68 |
| On-Premises1 | 10.0.0.0/8 | Virtual appliance | 10.124.32.68 |
| On-Premises2 | 172.16.0.0/12 | Virtual appliance | 10.124.32.68 |
| On-Premises3 | 192.168.0.0/16 | Virtual appliance | 10.124.32.68 |
| On-Premises4 | 147.108.0.0/16 | Virtual appliance | 10.124.32.68 |
| On-Premises5 | 3.0.0.0/8 | Virtual appliance | 10.124.32.68 |
| On-Premises6 | 151.95.0.0/18 | Virtual appliance | 10.124.32.68 |

Route Table **Route-HUB-WestEU-AzureFirewallSubnet** has the following configuration:

* **Subscription** – BH\_Infra\_1
* **Resource Group** –RG-NetworkHUB-WestEU
* **Region** –West Europe
* **Propagate Gateway Routes** – Yes

This route table is attached to the subnet:

* AzureFirewallSubnet

|  |  |  |  |
| --- | --- | --- | --- |
| **Route Name** | **Address Prefix** | **Next Hop** | **Next Hop Address** |
| AzureUSEastHCNonProdSpoke | 10.124.24.0/22 | Virtual appliance | 10.124.0.68 |
| AzureUSEastHCProdSpoke | 10.124.4.0/22 | Virtual appliance | 10.124.0.68 |
| AzureUSEastHub | 10.124.0.0/22 | Virtual appliance | 10.124.0.68 |
| AzureUSEastJVNonProd | 10.124.66.0/23 | Virtual appliance | 10.124.0.68 |
| AzureUSEastJVProd | 10.124.64.0/23 | Virtual appliance | 10.124.0.68 |
| AzureUSEastNonProdSpoke | 10.124.16.0/21 | Virtual appliance | 10.124.0.68 |
| AzureUSEastProdSpoke | 10.124.8.0/21 | Virtual appliance | 10.124.0.68 |
| AzureUSEastSandboxSpoke | 10.124.28.0/22 | Virtual appliance | 10.124.0.68 |
| Internet | 0.0.0.0/0 | Internet | - |

Route Table **Route-HUB-WestEU-GatewaySubnet** has the following configuration:

* **Subscription** – BH\_Infra\_1
* **Resource Group** –RG-NetworkHUB-WestEU
* **Region** –West Europe
* **Propagate Gateway Routes** – Yes

This route table is attached to the subnet:

* GatewaySubnet

|  |  |  |  |
| --- | --- | --- | --- |
| **Route Name** | **Address Prefix** | **Next Hop** | **Next Hop Address** |
| AzureWestEUHCNonProdSpoke | 10.124.56.0/22 | Virtual appliance | 10.124.32.68 |
| AzureWestEUHCProdSpoke | 10.124.36.0/22 | Virtual appliance | 10.124.32.68 |
| AzureWestEUHub | 10.124.32.0/22 | Virtual appliance | 10.124.32.68 |
| AzureWestEUNonProdSpoke | 10.124.48.0/21 | Virtual appliance | 10.124.32.68 |
| AzureWestEUProdSpoke | 10.124.40.0/21 | Virtual appliance | 10.124.32.68 |
| AzureWestEUVWENonProdSpoke | 10.15.160.0/24 | Virtual appliance | 10.124.32.68 |
| AzureWestEUHCNonProdSpoke-2 | 10.124.91.0/25 | Virtual appliance | 10.124.32.68 |
| AzureWestEUNonProdSpoke-2 | 10.124.90.0/25 | Virtual appliance | 10.124.32.68 |

## Route Table **Route\_HUB\_Citrix\_w365\_nva\_GatewaySubnet** has the following configuration:

* **Subscription** – BH\_Infra\_1
* **Resource Group** –RG\_HUB\_Citrix\_w365\_nva\_WestEU
* **Region** –West Europe
* **Propagate Gateway Routes** – Yes

This route table is attached to the subnet:

* GatewaySubnet

|  |  |  |  |
| --- | --- | --- | --- |
| **Route Name** | **Address Prefix** | **Next Hop** | **Next Hop Address** |
| VWE-WestEU\_Spoke | 10.15.176.0/20 | Virtual appliance | 10.15.161.134 |
| VWE\_WestEU-NonProd\_Spoke2 | 10.124.191.0/24 | Virtual appliance | 10.15.161.134 |
| VWE\_WestEU-Non-Prod\_Spoke2 | 10.6.192.0/18 | Virtual appliance | 10.15.161.134 |
| VWE\_WestEU-Non-Prod\_Spoke | 10.15.160.0/24 | Virtual appliance | 10.15.161.134 |

**Routing tables for West US HUB Subnets**

Route Table[**Route-SNET-DR-DC**](https://portal.azure.com/?feature.msaljs=true) has the following configuration:

* **Subscription** – BH\_Infra\_1
* **Resource Group –** RG-NetworkHUB-WestUS
* **Region** –West US
* **Propagate Gateway Routes** – No

This route table is attached to the subnets:

SNET-DR-DC\_ 10.127.0.32/27

SNET-DR-MyWizard\_10.127.1.0/26

Route-SNET-DR-JmpHosts\_10.127.1.64/26

Route-SNET-DR-AppGateway\_10.127.1.128/25

Route-SNET-DR-PrivateLink\_10.127.2.0/25

Route-SNET-DR-Infra\_10.127.0.128/26

|  |  |  |  |
| --- | --- | --- | --- |
| Route Name | Address Prefix | Next Hop | Next Hop Address |
| Internet | 0.0.0.0/0 | Virtual appliance | 10.127.0.68 |
| On-Premises1 | 10.0.0.0/8 | Virtual appliance | 10.127.0.68 |
| On-Premises2 | 172.16.0.0/12 | Virtual appliance | 10.127.0.68 |
| On-Premises3 | 192.168.0.0/16 | Virtual appliance | 10.127.0.68 |

This route table is attached to the subnets:

GatewaySubnet\_10.127.0.0/27

|  |  |  |  |
| --- | --- | --- | --- |
| Route Name | Address Prefix | Next Hop | Next Hop Address |
| AzureUSWestHUB | 10.127.0.0/22 | Virtual appliance | 10.127.0.68 |

This route table is attached to the subnets:

AzureFirewallSubnet\_10.127.0.64/26

|  |  |  |  |
| --- | --- | --- | --- |
| Route Name | Address Prefix | Next Hop | Next Hop Address |
| Internet | 0.0.0.0/0 | Virtual appliance | 10.127.0.68 |

­­­

#### Spoke Route Tables

##### Propagate Gateway Routes

Based on the network design, traffic should be tunneled directly to the firewall except for specific cases such as app gateways and managed routes. To ensure that traffic moves as expected, it is imperative that on every route table the Propagate Gateway Routes option is set to “No.”

##### Spoke Route Tables

**App and DB Route Tables:**

The following route tables are associated with the Internal and External App and DB subnets for their respective spoke.

Routes:

|  |  |  |  |
| --- | --- | --- | --- |
| Route Name | Address Prefix | Next Hop | Next Hop Address |
| Internet | 0.0.0.0/0 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises1 | 10.0.0.0/8 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises2 | 172.16.0.0/12 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises3 | 192.168.0.0/16 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises4 | 147.108.0.0/16 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises5 | 3.0.0.0/8 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises6 | 151.95.0.0/18 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| VDI\_Route\_1 | 10.15.128.0/24 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |
| VDI\_Route\_2 | 10.15.206.0/24 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |
| VDI\_Route\_3 | 10.6.64.0/18 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |
| VDI\_Route\_4 | 10.15.144.0/20 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |
| VDI\_Route\_5 | 10.6.192.0/18 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |
| VDI\_Route\_6 | 10.15.176.0/20 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |
| VDI\_Route\_7 | 10.15.160.0/24 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |
| VDI\_Route\_8 | 10.124.191.0/24 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |
| SQL\_DB\_WestEU | 10.124.50.19/32 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |
| SQL\_DB\_WestEU\_2 | 10.124.50.29/32 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |
| ContentServer\_EU | 10.124.48.21/32 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |

These routes can be found on the following route tables:

* Route-Spoke-HCNonProd-USEast
* Route-Spoke-HCNonProd-WestEU
* Route-Spoke-HCProd-USEast
* Route-Spoke-HCProd-WestEU
* Route-SPOKE-Non-Prod-WestEU-1
* Route-Spoke-NonProd-USEast-1
* Route-Spoke-Prod-USEast-1
* Route-SPOKE-Prod-WestEU-1
* Route-Spoke-JV-Prod
* Route-Spoke-JV-NonProd
* [Route-Spoke\_VWE\_NON\_PROD\_EastUS-Internal](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_w365_Infra_NonProd-eastUS/providers/Microsoft.Network/routeTables/Route-Spoke_VWE_NON_PROD_EastUS-Internal)
* [Route\_spoke\_iam\_C3\_dev\_non\_prod\_eastUS\_c3app](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/49f7b216-0dd7-411f-b7fb-ad3fa4ba76af/resourceGroups/rg_infra_iam_c3_platform_dev_nonprod_eastus/providers/Microsoft.Network/routeTables/Route_spoke_iam_C3_dev_non_prod_eastUS_c3app)
* [Route\_Spoke\_IAM\_Dev\_NON\_PROD\_EastUS\_IAM\_App](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/49f7b216-0dd7-411f-b7fb-ad3fa4ba76af/resourceGroups/rg_infra_iam_dev_nonprod_eastus/providers/Microsoft.Network/routeTables/Route_Spoke_IAM_Dev_NON_PROD_EastUS_IAM_App)
* [Route\_Spoke\_VWE\_NON\_PROD\_westEU\_Internal\_App](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_w365_Infra_NonProd-westEU/providers/Microsoft.Network/routeTables/Route_Spoke_VWE_NON_PROD_westEU_Internal_App)
* Route-SNET-SAP-PreProd-External-AppsVM
* Route-SNET-SAP-PreProd-Internal-DB
* Route-SNET-SAP-PreProd-External-DB
* Route-SNET-SAP-PreProd-Internal-AppsVM
* Route-SNET-SAP-NonProd-External-AppsVM
* Route-SNET-SAP-NonProd-Internal-DB
* Route-SNET-SAP-NonProd-External-DB
* Route-SNET-SAP-NonProd-Internal-AppsVM
* Route-SNET-SAP-Prod-Internal-AppsVM
* Route-SNET-SAP-Prod-External-AppsVM
* Route-SNET-SAP-Prod-Internal-DB
* Route-SNET-SAP-Prod-External-DB

**App Gateway Route Tables:**

The following route tables are associated with the application gateway subnets for their respective spoke.

Routes:

|  |  |  |  |
| --- | --- | --- | --- |
| Route Name | Address Prefix | Next Hop | Next Hop Address |
| Internet | 0.0.0.0/0 | Internet |  |
| On-Premises1 | 10.0.0.0/8 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises2 | 172.16.0.0/12 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises3 | 192.168.0.0/16 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises4 | 147.108.0.0/16 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises5 | 3.0.0.0/8 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises6 | 151.95.0.0/18 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| VDI-PROD-EUS | 10.6.64.0/18 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |
| VDI-PROD-EUS-2 | 10.15.144.0/20 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |
| VDI-PROD-WEU | 10.6.192.0/18 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |
| VDI-PROD-WEU2 | 10.15.176.0/20 | VirtualAppliance | US: 10.124.0.68  EU: 10.124.32.68 |

These routes can be found on the following route tables:

* Route-Spoke-Prod-WestEU-AGW
* Route-Spoke-Prod-USEast-AGW
* Route-Spoke-JV-Prod-AGW
* Route-Spoke-JV-NonProd-AGW
* Route-Spoke-HCProd-WestEU-AGW
* Route-Spoke-HCProd-USEast-AGW
* Route-Spoke-HCNonProd-WestEU-AGW
* Route-Spoke-HCNonProd-USEast-AGW
* Route-NonProd-WestEU-AGW
* Route-NonProd-EastUS-AGW
* [Route\_spoke\_iam\_C3\_dev\_non\_prod\_eastUS\_agw](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/49f7b216-0dd7-411f-b7fb-ad3fa4ba76af/resourceGroups/rg_infra_iam_c3_platform_dev_nonprod_eastus/providers/Microsoft.Network/routeTables/Route_spoke_iam_C3_dev_non_prod_eastUS_agw)
* [Route\_Spoke\_IAM\_Dev\_NON\_PROD\_EastUS\_IAM\_AGW](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/49f7b216-0dd7-411f-b7fb-ad3fa4ba76af/resourceGroups/rg_infra_iam_dev_nonprod_eastus/providers/Microsoft.Network/routeTables/Route_Spoke_IAM_Dev_NON_PROD_EastUS_IAM_AGW)
* Route-SNET-SAP-NonProd-AppGateway
* Route-SNET-SAP-PreProd-AppGateway
* Route-SNET-SAP-Prod-AppGateway

**Internal SQL Managed Instance Route Tables:**

The following route tables are associated with the internal SQL managed instance subnet for their respective spoke.

Routes:

|  |  |  |  |
| --- | --- | --- | --- |
| Route Name | Address Prefix | Next Hop | Next Hop Address |
| Internet | 0.0.0.0/0 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| Sql-managedInstances\_UseOnly\_mi-AzureActiveDirectory | Azure Active Directory | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-AzureCloud.eastus | Azure Cloud EastUS | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-AzureCloud.westus | Azure Cloud WestUS | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-AzureMonitor | Azure Monitor | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-CorpNetPublic | Corp Net Public | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-CorpNetSaw | Corp Net Saw | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-EventHub.eastus | Event Hub EastUS | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-EventHub.westus | Event Hub WestUS | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-SqlManagement | SQL Management | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-Storage | Storage | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-Storage.eastus | Storage EastUS | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-Storage.westus | Storage WestUS | Internet |  |
| Sql-managedInstances\_UseOnly\_subnet-to-vnetlocal | Local Subnet | Virtual Network |  |
| On-Premises1 | 10.0.0.0/8 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises2 | 172.16.0.0/12 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises3 | 192.168.0.0/16 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises4 | 147.108.0.0/16 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises5 | 3.0.0.0/8 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises6 | 151.95.0.0/18 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |

These routes can be found on the following route tables:

* Route-Spoke-JV-NonProd-Internal-SQLMI
* Route-Spoke-JV-Prod-Internal-SQLMI
* Route-Spoke-Non-Prod-USEast-Internal-SQLMI
* Route-Spoke-Non-Prod-WestEU-Internal-SQLMI
* Route-Spoke-Prod-USEast-Internal-SQLMI
* Route-Spoke-Prod-WestEU-Internal-SQLMI
* [Route\_Spoke\_VWE\_NON\_PROD\_westEU\_Internal\_SQLMI](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_w365_Infra_NonProd-westEU/providers/Microsoft.Network/routeTables/Route_Spoke_VWE_NON_PROD_westEU_Internal_SQLMI)
* [Route-Spoke\_VWE\_NON\_PROD\_EastUS-Internal-SQMl](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_w365_Infra_NonProd-eastUS/providers/Microsoft.Network/routeTables/Route-Spoke_VWE_NON_PROD_EastUS-Internal-SQMl)

**External SQL Managed Instance Route Tables:**

The following route tables are associated with the external SQL managed instance subnet for their respective spoke.

Routes:

|  |  |  |  |
| --- | --- | --- | --- |
| Route Name | Address Prefix | Next Hop | Next Hop Address |
| Internet | 0.0.0.0/0 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| Sql-managedInstances\_UseOnly\_mi-AzureActiveDirectory | Azure Active Directory | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-AzureCloud.eastus | Azure Cloud EastUS | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-AzureCloud.westus | Azure Cloud WestUS | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-AzureMonitor | Azure Monitor | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-CorpNetPublic | Corp Net Public | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-CorpNetSaw | Corp Net Saw | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-EventHub.eastus | Event Hub EastUS | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-EventHub.westus | Event Hub WestUS | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-SqlManagement | SQL Management | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-Storage | Storage | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-Storage.eastus | Storage EastUS | Internet |  |
| Sql-managedInstances\_UseOnly\_mi-Storage.westus | Storage WestUS | Internet |  |
| Sql-managedInstances\_UseOnly\_subnet-to-vnetlocal | Local Subnet | Virtual Network |  |
| On-Premises1 | 10.0.0.0/8 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises2 | 172.16.0.0/12 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises3 | 192.168.0.0/16 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises4 | 147.108.0.0/16 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises5 | 3.0.0.0/8 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises6 | 151.95.0.0/18 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |

These routes can be found on the following route tables:

* Route-Spoke-JV-NonProd-External-SQLMI
* Route-Spoke-JV-Prod- External -SQLMI
* Route-Spoke-Non-Prod-USEast- External -SQLMI
* Route-Spoke-Non-Prod-WestEU- External -SQLMI
* Route-Spoke-Prod-USEast- External -SQLMI
* Route-Spoke-Prod-WestEU- External -SQLMI

**Private Link Route Tables:**

The following route tables are associated with the private link subnet for their respective spoke.

Routes:

|  |  |  |  |
| --- | --- | --- | --- |
| Route Name | Address Prefix | Next Hop | Next Hop Address |
| Internet | 0.0.0.0/0 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises1 | 10.0.0.0/8 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises2 | 172.16.0.0/12 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises3 | 192.168.0.0/16 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises4 | 147.108.0.0/16 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises5 | 3.0.0.0/8 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises6 | 151.95.0.0/18 | Regional Firewall | US: 10.124.0.68  EU: 10.124.32.68 |

These routes can be found on the following route tables:

* Route-Spoke-HCNonProd-USEast-PrivateLink
* Route-Spoke-HCNonProd-WestEU-PrivateLink
* Route-Spoke-HCProd-USEast-PrivateLink
* Route-Spoke-HCProd-WestEU-PrivateLink
* Route-SPOKE-Non-Prod-WestEU-PrivateLink
* Route-Spoke-NonProd-USEast-PrivateLink
* Route-Spoke-Prod-USEast-PrivateLink
* Route-SPOKE-Prod-WestEU-PrivateLink
* Route-Spoke-JV-Prod-PrivateLink
* Route-Spoke-JV-NonProd-PrivateLink
* [Route\_Spoke\_VWE\_NON\_PROD\_westEU\_Private\_endpoint](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_w365_Infra_NonProd-westEU/providers/Microsoft.Network/routeTables/Route_Spoke_VWE_NON_PROD_westEU_Private_endpoint)
* [Route\_Spoke\_IAM\_Dev\_NON\_PROD\_EastUS\_Private\_endpoint](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/49f7b216-0dd7-411f-b7fb-ad3fa4ba76af/resourceGroups/rg_infra_iam_dev_nonprod_eastus/providers/Microsoft.Network/routeTables/Route_Spoke_IAM_Dev_NON_PROD_EastUS_Private_endpoint)
* [Route\_spoke\_iam\_C3\_dev\_non\_prod\_eastUS\_Private\_endpoint](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/49f7b216-0dd7-411f-b7fb-ad3fa4ba76af/resourceGroups/rg_infra_iam_c3_platform_dev_nonprod_eastus/providers/Microsoft.Network/routeTables/Route_spoke_iam_C3_dev_non_prod_eastUS_Private_endpoint)
* [Route-Spoke\_VWE\_NON\_PROD\_EastUS-Private\_endpoint](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_w365_Infra_NonProd-eastUS/providers/Microsoft.Network/routeTables/Route-Spoke_VWE_NON_PROD_EastUS-Private_endpoint)
* Route-SNET-SAP-PreProd-PrivateLink
* [Route-SNET-SAP-Prod-PrivateLink](https://portal.azure.com/)
* [Route-SNET-SAP-PreProd-PrivateLink](https://portal.azure.com/)
* [Route-SNET-SAP-NonProd-PrivateLink](https://portal.azure.com/)

**AVD and W365 Route Tables:**

The following route tables are associated with the AVD and W365 subnet for their respective spoke.

|  |  |  |  |
| --- | --- | --- | --- |
| **Route Name** | **Address Prefix** | **Next Hop** | **Next Hop Address** |
| AzureCloud | AzureCloud | Virtual appliance | US: 10.124.0.68  EU: 10.124.32.68 |
| AzureFrontDoor.Frontend | AzureFrontDoor.Frontend | Virtual appliance | US: 10.124.0.68  EU: 10.124.32.68 |
| AzureMonitor | AzureMonitor | Virtual appliance | US: 10.124.0.68  EU: 10.124.32.68 |
| kms.core.windows.net | 23.102.135.246/32 | Virtual appliance | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Prem-internet | 0.0.0.0/0 | Virtual appliance | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises1 | 172.16.0.0/12 | Virtual appliance | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises2 | 192.168.0.0/16 | Virtual appliance | US: 10.124.0.68  EU: 10.124.32.68 |
| On-Premises3 | 10.0.0.0/8 | Virtual appliance | US: 10.124.0.68  EU: 10.124.32.68 |
| WindowsVirtualDesktop | WindowsVirtualDesktop | Virtual appliance | US: 10.124.0.68  EU: 10.124.32.68 |

These routes can be found on the following route tables:

* [Route-Spoke\_VWE\_NON\_PROD\_EastUS-AVD](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_w365_Infra_NonProd-eastUS/providers/Microsoft.Network/routeTables/Route-Spoke_VWE_NON_PROD_EastUS-AVD)
* [Route-Spoke\_VWE\_NON\_PROD\_EastUS-W365](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_w365_Infra_NonProd-eastUS/providers/Microsoft.Network/routeTables/Route-Spoke_VWE_NON_PROD_EastUS-W365)
* [Route\_Spoke\_VWE\_NON\_PROD\_westEU\_AVD](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_w365_Infra_NonProd-westEU/providers/Microsoft.Network/routeTables/Route_Spoke_VWE_NON_PROD_westEU_AVD)
* [Route\_Spoke\_VWE\_NON\_PROD\_westEU\_W365](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_w365_Infra_NonProd-westEU/providers/Microsoft.Network/routeTables/Route_Spoke_VWE_NON_PROD_westEU_W365)

**Extended AKS**

The following route tables are associated with the extended AKS subnet for their respective spoke.

|  |  |  |  |
| --- | --- | --- | --- |
| **Route Name** | **Address Prefix** | **Next Hop** | **Next Hop Address** |
| Internet | 0.0.0.0/0 | Virtual appliance | 10.124.0.68 |
| On-Premises1 | 172.16.0.0/12 | Virtual appliance | 10.124.0.68 |

These routes can be found on the following route tables:

* [Route\_spoke\_iam\_C3\_dev\_non\_prod\_eastUS\_extendedaks](https://portal.azure.com/" \l "@bakerhughes.onmicrosoft.com/resource/subscriptions/49f7b216-0dd7-411f-b7fb-ad3fa4ba76af/resourceGroups/rg_infra_iam_c3_platform_dev_nonprod_eastus/providers/Microsoft.Network/routeTables/Route_spoke_iam_C3_dev_non_prod_eastUS_extendedaks)
* [Route\_Spoke\_IAM\_Dev\_NON\_PROD\_EastUS\_IAM\_Extended\_AKS](https://portal.azure.com/#@bakerhughes.onmicrosoft.com/resource/subscriptions/49f7b216-0dd7-411f-b7fb-ad3fa4ba76af/resourceGroups/rg_infra_iam_dev_nonprod_eastus/providers/Microsoft.Network/routeTables/Route_Spoke_IAM_Dev_NON_PROD_EastUS_IAM_Extended_AKS)

**PostgreSQL**

The following route tables are associated with the Postgre SQL subnet for their respective spoke.

|  |  |  |  |
| --- | --- | --- | --- |
| **Route Name** | **Address Prefix** | **Next Hop** | **Next Hop Address** |
| Internet | 0.0.0.0/0 | Virtual appliance | 10.124.0.68 |
| On-Premises1 | 10.0.0.0/8 | Virtual appliance | 10.124.0.68 |
| On-Premises2 | 172.16.0.0/12 | Virtual appliance | 10.124.0.68 |
| On-Premises3 | 192.168.0.0/16 | Virtual appliance | 10.124.0.68 |
| On-Premises4 | 147.108.0.0/16 | Virtual appliance | 10.124.0.68 |
| On-Premises5 | 3.0.0.0/8 | Virtual appliance | 10.124.0.68 |
| On-Premises6 | 151.95.0.0/18 | Virtual appliance | 10.124.0.68 |

These routes can be found on the following route tables:

* Route\_spoke\_iam\_C3\_dev\_non\_prod\_eastUS\_postgresdb

**DataBricks**

The following route tables are associated with the Databricks subnet for their respective spoke.

|  |  |  |  |
| --- | --- | --- | --- |
| **Route Name** | **Address Prefix** | **Next Hop** | **Next Hop Address** |
| iam-dev-dbr-to-east-dbartifacts | 20.150.90.100/32 | Internet | - |
| iam-dev-dbr-to-east-dbartifacts2 | 20.60.7.36/32 | Internet | - |
| iam-dev-dbr-to-east-dbartifacts3 | 20.60.7.4/32 | Internet | - |
| iam-dev-dbr-to-east-dbartifacts4 | 20.60.128.228/32 | Internet | - |
| iam-dev-dbr-to-east-dbartifacts5 | 13.77.115.36/32 | Internet | - |
| iam-dev-dbr-to-east-dbfs\_root\_blob | 52.239.221.36/32 | Internet | - |
| iam-dev-dbr-to-east-dbfs\_root\_blob2 | 52.239.221.34/32 | Internet | - |
| iam-dev-dbr-to-east-dblog | 52.239.229.100/32 | Internet | - |
| iam-dev-dbr-to-east-dblog2 | 52.239.170.164/32 | Internet | - |
| iam-dev-dbr-to-east-dblog3 | 52.239.171.4/32 | Internet | - |
| iam-dev-dbr-to-east-dblog4 | 20.150.90.4/32 | Internet | - |
| iam-dev-dbr-to-east-event-hub | 40.112.242.0/32 | Internet | - |
| iam-dev-dbr-to-east-event-hub2 | 40.71.10.128/32 | Internet | - |
| iam-dev-dbr-to-east-ext-infra | 20.57.106.0/28 | Internet | - |
| iam-dev-dbr-to-east-metastore | 40.71.83.113/32 | Internet | - |
| iam-dev-dbr-to-east-metastore2 | 40.71.8.203/32 | Internet | - |
| iam-dev-dbr-to-east-us-artifact-blob-primary1 | 52.239.155.196/32 | Internet | - |
| iam-dev-dbr-to-east-us-artifact-blob-primary2 | 20.209.1.65/32 | Internet | - |
| iam-dev-dbr-to-east-us-artifact-blob-primary3 | 52.239.153.36/32 | Internet | - |
| iam-dev-dbr-to-east-us-artifact-blob-primary4 | 52.239.171.228/32 | Internet | - |
| iam-dev-dbr-to-east-us-control-plane-nat1 | 23.101.152.95/32 | Internet | - |
| iam-dev-dbr-to-east-us-control-plane-nat2 | 20.42.4.208/32 | Internet | - |
| iam-dev-dbr-to-east-us-control-plane-nat3 | 20.42.4.210/32 | Internet | - |
| iam-dev-dbr-to-east-us-scc-relay-ip | 52.247.0.200/32 | Internet | - |
| iam-dev-dbr-to-east-us-webapp | 40.70.58.221/32 | Internet | - |
| iam-dev-dbr-to-east-us-webapp2 | 20.42.4.209/32 | Internet | - |
| iam-dev-dbr-to-east-us-webapp3 | 20.42.4.211/32 | Internet | - |
| iam-dev-dbr-to-east-us2-scc-relay-ip | 52.146.50.16/32 | Internet | - |

These routes can be found on the following route tables:

* iam-dev-databricks-route-table

### Service Endpoints (a.k.a. Public Endpoints)

Service endpoints will be used to connect Azure Virtual Networks directly to PaaS service. These settings will be applied to both the US East hub network and the West EU hub network. There are also settings that must be configured on each individual service that will be connected.

On the **HUB-USEast** and **HUB-WestEU** Virtual Networks, the following service endpoints must be enabled for the *AzureFirewallSubnet*:

* Microsoft.AzureCosmosDB
* Microsoft.CognitiveServices
* Microsoft.ContainerRegistry
* Microsoft.EventHub
* Microsoft.KeyVault
* Microsoft.ServiceBus
* Microsoft.Sql
* Microsoft.Storage
* Microsoft.Web

On each service, the connection security settings should have the following configuration:

* **Deny Public Network Access**: No
* **Allow Access to Azure Services**: No
* **VNET rules**: ServiceEndpoint for respective Hub
* **SSL Enforcement**: Enabled
* **Minimum TLS Version**: 1.2

### Private Endpoints

Private endpoints will be used to integrate the PaaS services into the Azure virtual networks by adding a private IP address for each service resource. Effectively, this brings the service inside the internal network.

The following services will have private endpoints enabled:

* Azure Database for PostgreSQL
* Azure Database for MySQL
* Azure Database for MariaDB
* Azure Key Vault
* Azure Event Hubs
* Storage Account – Blob
* Storage Account – Table
* Storage Account - Queue
* Storage Account - File
* Storage Account - Web
* Azure Data Factory
* Azure Data Factory - Portal
* Azure Data Lake File System Gen 2
* Azure SQL Database
* Azure IoT Hub
* Azure Container Registry

##### Network Configuration

Within each Spoke, there will be a PrivateLinkSubnet which will hold all the private link resources. Each subnet will have a dedicated route table so that routes will not impact the app and database subnets. Each subnet will also have a dedicated network security group which will restrict the connections that are allowed.

##### Routing Configuration

For any PaaS services that need to connect to On-Premises, a new specific route will need to be added on the Gateway subnet as defined below. This is based on Microsoft Documentation: [Inspect Traffic with Azure Firewall Scenario 4](https://docs.microsoft.com/en-us/azure/private-link/inspect-traffic-with-azure-firewall#scenario-4-on-premises-traffic-to-private-endpoints)

|  |  |
| --- | --- |
| Destination Address | Next Hop |
| <IP of Private Endpoint>/32 | Regional Firewall  US: 10.124.0.68  EU: 10.124.32.68 |

## Security

### Edge security approach

#### Azure Firewall

Accenture security will define the governance model and submit to Baker Hughes for approval. Accenture will implement the initial firewall rules and manage ongoing firewall rules. The initial firewall rules are contained in the following table.

For more specifics on configuration and implementation of Firewalls Rules, see Firewall RunBook below.



### Inter-subnet security approach

Micro segmentation is achieved by placing an NSG with a default rule of DenyAll and then allow by exception. Initial NSGs are detailed for each subnet in the Hub and Spoke design sections. The following diagram shows applications 1-4 collected into Application Security Groups (ASG) and then a rule applied allowing communication among the ASG. Unless a rule is added that allows communication between App1 and App2, all communication between application servers is denied.

For more specifics on configuration and implementation of NSG Rules, see [Network Security Group RunBook](https://ts.accenture.com/:w:/r/sites/BakerHughes130-AzureCloudTransformation/Shared%20Documents/Azure%20Cloud%20Transformation/12%20-%20Delivery%20%26%20Execution/08_Security%20Workstream/05_FW%20and%20NSG/Azure%20Network%20Security%20Management.docx?d=w5874843a3b5d44a7b9f09259c742e526&csf=1&web=1&e=5zBfGS). 



### Internet egress approach

Baker Hughes has a requirement to scan all outgoing Internet traffic. To accomplish this, it is necessary to direct all Internet traffic to the Azure Firewall. A User Defined Route (UDR) will be configured and applied to each subnet to direct traffic to the Azure Firewall. Those routes can be seen in the user defined routing section above.

### Governance

As rules need to be added to the firewall and network security groups, they will follow a specified governance process. Beginning with a request that will come from the app owner and include Source Address, Target Address, and target Ports. This request will then be formatted for approval. If approved, the rule will be added to the csv file associated with each network resource. The CSV files are automatically versioned to ensure that a track of rule changes is kept along with the ability to quickly revert changes at any time if needed. Using PowerShell scripts, the Azure resources will then be updated with the corrected rules and tested for confirmation. Once testing is completed, a notification will be sent to the app owner letting them know the rule has been implemented.

Below is a diagram showing this process.



# Identity

## Avanade Recommendations

### Azure AD

* Use Azure AD as the enterprise cloud identity store
* Have a single tenant that serves as the O365 tenant
* Register custom domain name

### Privileged Role Assignments/Administrative Accounts

* Minimize the global admin assignments to James Smith’s team.
* Delegate privilege roles to a group and populate the group with trusted users.
* Enable Privileged Identity Management (PIM). Is a security service that requires administrators to activate prior to executing administrative functions, also provides monitoring and logging of administrative actions.
* James Smith team to handle PIM administration.

### User and Group Management

* Continue to manage user and groups via your on-premises management toolset, and allow additions/modifications/deletions to synchronize to Azure

### DeterSynchronization

* Synchronize user accounts from on-premises AD DS forest(s) using Azure AD Connect
  + Use seamless SSO
  + Enable Azure AD Connect Health

### External Identities

* Use B2B guest accounts to grant other organization access to our applications and resources
* Use Access Reviews reporting to view what guest users are doing.

### Extending AD DS into Azure

* Deploy writable domain controllers if AD domain services, Kerberos, or LDAB is required

## Design Decisions/Requirements

### Azure AD

* Azure AD tenant from Office 365 will be used.
* Bakerhughes.com is the domain name
* Additional custom domains have already been entered into Azure for O365.

### Privileged Role Assignments/Administrative Accounts

* BH has E5 licenses for O365 users.
* E5 licenses may not include PIM. More research needed

### User and Group Management

* Users and Groups managed on-premises.
* Workday and Saviant are in place for tools

### Synchronization

* Synchronization in place due to O365.

### External Identities

* Baker Hughes has deployed OKTA for federation and MFA. Decision was made to use OKTA for Azure Portal and BH is responsible for administering OKTA.
* Okta is SSO for applications

### Extending AD DS into Azure

* Install 2 DCs in each region.
* DCs in Azure will be RWDCs.
* Logical/physical design will adhere to current AD design specifications.

## Design

### Azure AD

### Privileged Identity Management

Privileged Identity Management (PIM) is in place for the Baker Hughes Azure portal and Accenture will leverage the existing implementation. The roles identified in section 2.3.1 will be created in PIM and configured with the default configuration options. Accenture recommends deploying using the default options and then reviewing actual operations before making any adjustments, as implementing different configuration options will have an impact on operations. The following are the recommended configuration options:

|  |  |
| --- | --- |
| Notification on activation | Admin, distribution list |
| Require justification | Yes |
| Require approval | No |
| Require MFA to activate | Yes |
| Activation max. duration | 8 hours |

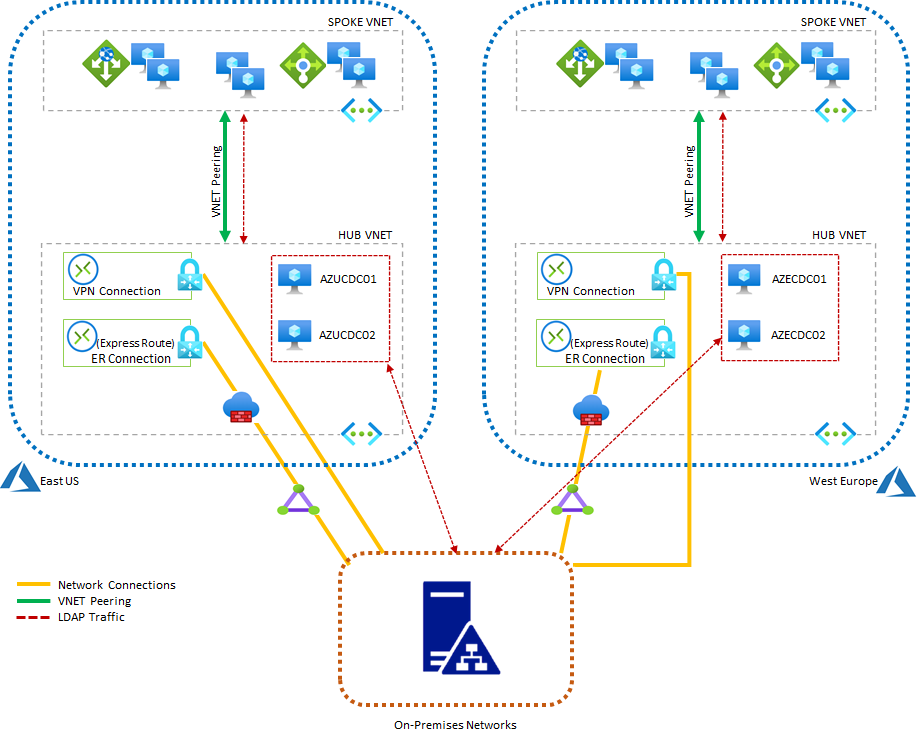
As operations commence, it is common for PIM roles to be misapplied or modified differently than intended. To identify users and groups that have been granted roles in PIM that they should not have or do not need, it is important to monitor and audit on a regular basis. This can be done by selecting the Assignments on any resource and viewing the eligible assignments and the associated users and groups. A resource audit can also be performed from the PIM console. It is recommended to perform auditing on a regular basis.

### Extending AD DS into Azure

To support domain joined VMs in Azure, a domain controller must be available and reachable to the Azure network. To support the requirement, Read Write Domain Controllers will be implemented in the DC subnet in each hub behind a load balancer to ensure availability, reduce dependency and improve performance. The following DCs will be created in Azure to support workloads.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VM Name | IP | Subscription | Region | RG Name | AV Set Name |
| AZECDC01 | 10.124.32.40 | BH\_INFRA\_1 | West Europe | RG-ADDS-WestEU | AS-EUDC01-01 |
| AZECDC02 | 10.124.32.41 | BH\_INFRA\_1 | West Europe | RG-ADDS-WestEU | AS-EUDC01-01 |
| AZUCDC01 | 10.124.0.40 | BH\_INFRA\_1 | East US | RG-ADDS-EastUS | AS-USDC01-01 |
| AZUCDC02 | 10.124.0.41 | BH\_INFRA\_1 | East US | RG-ADDS-EastUS | AS-USDC01-01 |
| AZWUCDC01 | 10.127.0.40 | BH\_INFRA\_1 | West US | RG-ADDS-WestUS | AS-WUCDC-01 |
| AZWUCDC02 | 10.127.0.41 | BH\_INFRA\_1 | West US | RG-ADDS-WestUS | AS-WUCDC-01 |

US will be used for East US and EU for West EU and WU will be used for West US. Domain Controller design to follow current on-premises design, i.e., separate drives for the NTDS file, log files, and SYSVOL, etc. An Active Directory Site will be required to be created in AD Sites and Services and the Network IDs for each region be created as subnets to support VMs ability to locate the closest DC. Site links will also be required to be configured to configure replication. This will be handled by BH AD Team. See AD Design Below:

A load balancer was added in front of AD to eliminate single point of failure for apps which is legacy and do not understand how AD works

**OU Path for Non-production -** **OU=Non-Prod,OU=Managed Servers - Azure,DC=ent,DC=bhicorp,DC=com**

**OU Path for Production -** **OU=Prod,OU=Managed Servers - Azure,DC=ent,DC=bhicorp,DC=com**

VM can be added to domain using the script and automation, please refer this link for the details.

https://github.com/BH-Corporate-Functions/BHCAzure\_Automation\_SBX/tree/master/Scripts/domainJoin

Note- Due to recent OU additions the script need update on OU Path variable.

#### Domain Controller Build

The Accenture team will build the VM and then turn it over to the BH Active Directory team for installation and configuration of Active Directory and tools. The Accenture team will deploy the VMs in Azure and install a marketplace image of Windows Server 2019 and turn the server over to the BH team to perform additional configuration, install agents and software, and then install Active Directory. The Marketplace image contains all updated patches for Windows Server 2019 and all components/features/roles.

Before promoting the domain controller, ensure that the quality of the server build is satisfactory, and that the server is healthy. When it is verified that the server is functioning properly, prepare to answer the installation parameters requested during the install. The VM will be built according to the following specs:

Azure VM

8 Core – 24 GB of RAM (Recommended D4Sv4)

SSD Drives

C: 100 GB - OS

D: 20 GB – Log files

E: 100 GB – NTDS.dit

Windows Server 2019

#### High Availability

Physical racks that have DC VM’s will be managed by Microsoft in their data center. To ensure high availability of the DCs, each pair of DCs will be created in an Availability Set. The following table details the high availability configuration.

|  |  |  |  |
| --- | --- | --- | --- |
| Domain Controllers | DC IP | Availability Set | Region |
| AZUCDC01  AZUCDC02 | 10.124.0.40  10.124.0.41 | **AS-USDC01-01** | East US |
| AZECDC01  AZECDC02 | 10.124.32.40  10.124.32.41 | **AS-EUDC01-01** | West Europe |
| AZWUCDC01  AZWUCDC02 | 10.127.0.40  10.127.0.41 | **AS-WUCDC-01** | West US |

#### Storage

Azure DCs will be provisioned using Managed Storage and storage accounts will not be provisioned specifically for AD Servers due to added complexity. Managed disks have less risk of failure and carry a higher SLA.

#### Encryption

DC disks will be encrypted at rest. The AD team can further secure the disks by enabling BitLocker. Enabling BitLocker may impact performance

#### Patch Management

AD team will use existing SCCM tools to enable patch management.

#### DC Access from Azure

The local Admin / Root account access is removed when DC is promoted to DC status. Password Reset feature will not work from Azure for DCs. No Azure Admins will have access to the VM console since Azure is control plane only. The BH AD team will be responsible and require console access to DCs in Azure for troubleshooting purposes.

#### Time Sync

Accenture recommends setting the time sync on the server to sync with the PDC Emulator and have the PDC Emulator synching from a reliable source, such as Time.windows.com or Time.gov. The server domain time sync will not be overridden by the local host time sync. USN rollback has been mitigated since Server 2012 and is not a factor in Azure.

#### AD Site

AD site will be created in AD to contain the DCs in each region and IP address ranges will be added to the AD site. Site links will be created and configured by the AD team.

#### Autoscaling and Temporary Workloads

VMs can be spun up as required from the hardened golden image. DC can be places in a scale set if required.

**Log file settings in OS.**

|  |  |  |
| --- | --- | --- |
| Log | Setting | Value |
| Application Log | Application Log (maximum) | **16384 KB** |
| Application Log (retention) | Overwrite as needed |
| Security Log | Security Log (maximum) | **204800 KB** |
| Security Log (retention) | Overwrite as needed |
| System Log | System Log (maximum) | **16384 KB** |
| System Log (retention) | Overwrite as needed |

### DNS

Active Directory domain controllers placed in Azure will be configured as DNS servers for all Azure IaaS workloads. DNS setting for all Virtual Networks will be pointed to the domain controller VMs located in Azure. All VMs will get their DNS settings from the Virtual Networks.

##### Azure Private DNS Zones

Azure Private DNS zones will be configured for records of hosted applications and to provide for Private Link (Private Endpoint) capability. These Private DNS zones will all be in the *RG-PrivateDNS* resource group and located in the Infra subscription in east us. These Private DNS zones will be connected to all spoke virtual networks in both East US and West EU regions. The Private DNS zone for domain name azure.bakerhughes.com will be used by the hosted applications. For each service that Private Link is enabled for, there will be a dedicated private DNS zone within Azure. The names for the private DNS zones can be found in the table below.

|  |  |
| --- | --- |
| Resource Type | Private DNS Zone Name |
| Azure Hosted Applications | azure.bakerhughes.com |
| Azure Database for PostgreSQL | privatelink.postgres.database.azure.com |
| Azure Database for MySQL | privatelink.mysql.database.azure.com |
| Azure Database for MariaDB | privatelink.mariadb.database.azure.com |
| Azure Key Vault | privatelink.vaultcore.azure.net |
| Azure Event Hubs | privatelink.servicebus.windows.net |
| Storage Account – Blob | privatelink.blob.core.windows.net |
| Storage Account – Table | privatelink.table.core.windows.net |
| Storage Account - Queue | privatelink.queue.core.windows.net |
| Storage Account - File | privatelink.file.core.windows.net |
| Storage Account - Web | privatelink.web.core.windows.net |
| Azure Data Factory | privatelink.datafactory.azure.net |
| Azure Data Lake File System Gen 2 | privatelink.dfs.core.windows.net |
| Azure SQL Database | privatelink.database.windows.net |
| Azure IoT Hub | privatelink.azure-devices.net |
| Azure Container Registry | privatelink.azurecr.io |
| ODS opinsights | privatelink.ods.opinsights.azure.com |
| OMS opinsights | privatelink.oms.opinsights.azure.com |
| System 1 hosted appliations | system1.azure.bakerhughes.com |
| Kusto West Europe | privatelink.westeurope.kusto.windows.net |
| azmk8s West Europe | privatelink.westeurope.azmk8s.io |
| Cosmos DB | privatelink.table.cosmos.azure.com |
| Azure Redisenterprise Cache | privatelink.redisenterprise.cache.azure.net |
| Redis Cache | privatelink.redis.cache.windows.net |
| Azure Notebooks | privatelink.notebooks.azure.net |
| Azure ADF | privatelink.adf.azure.com |
| Azure automation agentssvc | privatelink.agentsvc.azure-automation.net |
| Azureml API | privatelink.api.azureml.ms |
| Azure automation | privatelink.azure-automation.net |
| Azure Devices provisioning | privatelink.azure-devices-provisioning.net |
| Azure Databricks | privatelink.azuredatabricks.net |
| Azure websites | privatelink.azurewebsites.net |
| Cassandra cosmos DB | privatelink.cassandra.cosmos.azure.com |
| Azure Cognitive services | privatelink.cognitiveservices.azure.com |
| Azure cosmos DB | privatelink.cosmos.azure.com |
| Azure Documents | privatelink.documents.azure.com |
| azmk8s East US | privatelink.eastus.azmk8s.io |
| Kusto East US | privatelink.eastus.kusto.windows.net |
| Azure gremlin cosmos DB | privatelink.gremlin.cosmos.azure.com |
| Azure mongo cosmos DB | privatelink.mongo.cosmos.azure.com |
| Azure Monitor | privatelink.monitor.azure.com |
| Azure sqlx cosmos DB | privatelink.sqlx.cosmos.azure.com |

*\*\* Note: For additional resources, please review* [*Microsoft Documentation*](https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-dns) *for the naming convention*

Each private DNS zone will need to be associated with all spoke VNets. Below are the settings that will be configured for each spoke across all subscriptions:

Link Name: <Virtual network Name>

Subscription: <Virtual network’s Subscription>

Virtual Network: <Virtual Network>

Enable Auto Registration: False

Repeated for all spoke VNets in all subscriptions.

##### DNS Conditional Forwarders On-premises (Active Directory-integrated)

For each Azure Private DNS zone, there will be a dedicated DNS conditional forwarder within Baker Hughes DNS infrastructure currently existing on Active Directory domain controllers. The names of the zones for the DNS conditional forwarders can be found in the table below.

|  |  |
| --- | --- |
| Resource Type | DNS Zone Name |
| Azure Hosted Applications | azure.bakerhughes.com |
| Azure Database for PostgreSQL | postgres.database.azure.com |
| Azure Database for MySQL | mysql.database.azure.com |
| Azure Database for MariaDB | mariadb.database.azure.com |
| Azure Key Vault | vaultcore.azure.net |
| Azure Event Hubs | servicebus.windows.net |
| Storage Account – Blob | blob.core.windows.net |
| Storage Account – Table | table.core.windows.net |
| Storage Account - Queue | queue.core.windows.net |
| Storage Account - File | file.core.windows.net |
| Storage Account - Web | web.core.windows.net |
| Azure Data Factory | datafactory.azure.net |
| Azure Data Lake File System Gen 2 | dfs.core.windows.net |
| Azure SQL Database | database.windows.net |
| Azure IoT Hub | azure-devices.net |
| Azure Container Registry | azurecr.io |

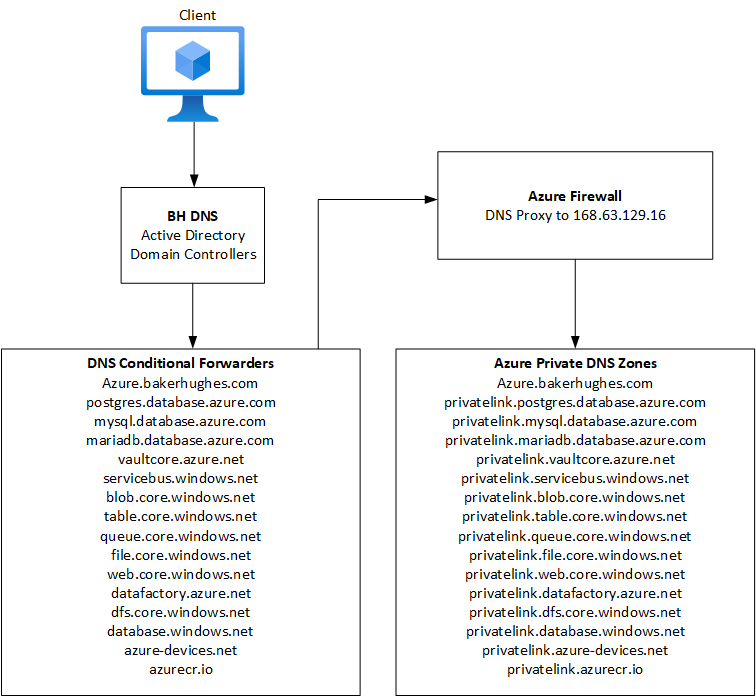
*\*\* Note: For additional resources, please review* [*Microsoft Documentation*](https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-dns) *for the naming convention*

DNS conditional forwarders will forward the requests to the Microsoft Azure DNS service (168.63.129.16) using both East US and West EU Azure Firewalls’ internal IP addresses to proxy’s these requests. DNS conditional forwarders should configured pointing to the two Azure Firewalls as defined in the table below.

|  |  |
| --- | --- |
| Region | DNS Proxy on Azure Firewall |
| East US | 10.124.0.68 |
| West Europe | 10.124.32.68 |
| West US | 10.127.0.68 |

#### DNS Diagram

Internal DNS traffic will traverse as shown below



# Security

## Avanade Recommendations

### Network Security

* Implement AzureFirewall to provide scanning for egress traffic.
* Implement Azure DDoS Standard on all VNets.
* Implement Network Security Groups (NSGs) on all subnets.

### Identity Management

* License users for Azure AD P2.
* Enable Azure Defender for Identity to monitor on-premises Active Directory Domain Controllers’ activities to identify and investigate advanced threats thar occurs around identities.
  + 2FA will be done using MyID.
* Enable Azure Identity Protection policies.
* Enable Just-in-Time Access to VMs.
* Make all Azure AD admin role assignments and Azure subscription RBAC role assignments temporary using Privileged Identity Management.
  + Create “break glass” accounts for key role assignments that are not tied to a named user.

### Monitoring and Incident Management

* Enable Security Center / Azure Defender.
* Create a Log Analytics workspace specifically for Security Center.
* Enable the monitoring agent auto-provisioning.
* Use the built-in vulnerability scanner (powered by Qualys) instead of the stand-alone Qualys product.
* Enable Azure Defender for Endpoint.
* Enable Azure Sentinel to provide intelligent security analytics and threat intelligence for Azure resources, Office 365 instances, and third party and on-premises devices.
* Use a separate workspace for Sentinel.

### Data Protection

* Create Key Vaults for each application and environment depending on whether secrets are environment specific.
* Enable soft-delete and purge- protection settings will be enabled on Azure Key Vaults to ensure recoverability in case of accidental deletion.
* Only use the HSM pricing tier if required.
* Set expiration date on all keys and secrets​.
* Ensure key vault is recoverable.
* Use Microsoft managed keys unless there is a specific business requirement.

## Design Decisions/Requirements

### Network Security

* Azure Firewall
  + It is agreed to use Azure Firewall unless there is a specific requirement that leads to a different product, such as a Palo Alto NVA.
  + Guda provided the following data points for existing AWS firewall security. Azure Firewall Premium may provide a solution. Additional discussion and follow up required.

1. Outbound internet - The PA firewalls are performing URL filtering, web categories, IPS (Azure firewall premium is a good replacement for this service).
2. East-west traffic – The PA firewalls are performing layer 7 application filtering, IPS (Azure firewall premium with stateful firewall and IPS services will suffice).
3. Internet inbound traffic – The PA firewalls perform deep packet inspection along with WAF (I’m not sure if Azure firewall can be leveraged for this feature. If this feature is not supported, I’m ok with us dropping the IPS requirement and leverage Imperva WAF/Azure Application Gateway or Combination for public facing applications. This will enable us to leverage the native firewalls services).
   * Azure Firewall Premium expected to be GA June 2021, per Microsoft.

* NSGs will be implemented at the subnet level with a default deny, then allow by exception using ASG’s per application grouping. Load balancer traffic will be part of applications and ASG.
* DDoS Standard will be implemented on Subscriptions with publicly exposed IPs. Will not be implemented on Subscriptions without publicly exposed IPs.

### Identity Management

* Azure AD Identity Protection will be deployed on DCs.
  + Accenture team responsible for the alerting and management.
* Azure Defender for Identity will be deployed.
* MFA for portal access is provided by Okta.
* PIM is already implemented.

### Data Protection

* Create a policy to enforce HTTPS for storage accounts.
* Follow up regarding traffic on the Microsoft Backbone is required.
* No identified requirement to manage own keys currently. Microsoft keys will be used.

### Logging

### Monitoring and Incident Management

* A single Log Analytics workspace will be implemented for Security Center across all subscriptions (Management Group Deployment).
* Retention policy for LA Workspace will be per application schedule. Logs to be exported to archive to be stored for 60 months per requirement to maintain logs.
* Security Center will be configured with the following configurations:
  + Azure Defender will be enabled for all services.
  + All ASC Default policies will be enabled.
  + Advanced Threat Detection Integration will be enabled.
  + Auto-Provision monitoring agent will be enabled.
  + Email contacts and notification types will be configured.
  + File Integrity Management will be enabled.
  + Adaptive network hardening will be enabled.
* Just-in-Time VM Access – TBD depending on remote access solution.
* Enable Adaptive Application controls – more information required.
* Azure Sentinel will be deployed to support the Accenture security team. Integration with existing SIEM may be required.

### Vulnerability Management

* Licensed Qualys version will be deployed.
  + BH requested more information on the solution.

### Endpoint Security

* Enable Endpoint Protection Solution will be enabled in Security Center.

## Design



### Network Security

#### Network Security Groups

Micro-segmentation is achieved by implementing NSGs with a default deny rule and then allow by exception rules. Network Security Groups (NSG) will be applied to all subnets hosting workloads and in all hub subnets where possible. (Some subnets, such as the Gateway subnet, do no support NSGs). The NSGs for each subnet are documented in the Network design section.

The diagram below is a representation of allowed/disallowed traffic within a subnet. The Apps are server groupings belonging to an Application Security Group (ASG).



#### Azure Firewall

See the Azure Firewall Section in the Network Design.

#### Azure DDoS

To provide network protection in line with current security requirements, Avanade recommends implementing Azure DDoS Standard protection on all VNets. In addition to the always-on traffic monitoring and real-time mitigation of common network-level attacks provided in the basic tier, standard tier protects internal VNets from the following attacks:

* Volumetric attacks: flooding the network layer with traffic that seems legitimate.
* Protocol attacks: attacks that target protocols in the layer 3 and 4 protocol stack such as SYN flood attacks, reflection attacks, and other protocol attacks.
* Resource (application) layer attacks: HTTP protocol attacks, SQL injection, cross-site scripting attacks, and other layer 7 attacks. Recommend Azure DDoS standard. Outline benefits and functionality.

Accenture will implement Azure DDoS Standard on all Subnets with public IPs. To implement DDoS standard, a DDoS protection plan will be created in the Infrastructure subscription in the SharedSVCs resource group. The DDoS plan can be applied to subnets in all subscriptions.

|  |  |  |
| --- | --- | --- |
| Resource | Name | Resource Group |
| DDoS Protection Plan | DDOS\_Infrastructure | SharedSVCs |

### Identity Management

* Azure AD Identity Protection will be deployed on DCs.
  + Accenture team responsible for the alerting and management.
* Azure Defender for Identity will be deployed.
* MFA for portal access is provided by Okta.
* PIM is already implemented.

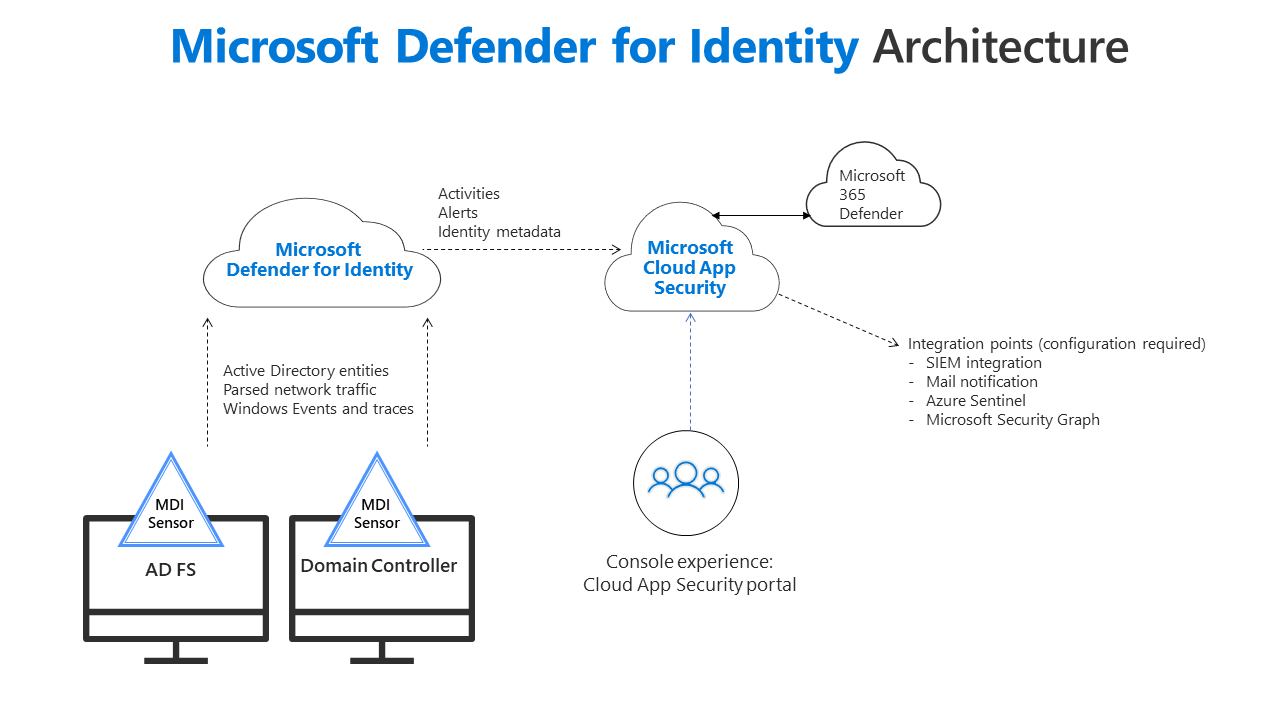
#### Defender for Identity

Azure Defender for Identity, formerly Azure Advanced Threat Protection (ATP) will be deployed and configured on the domain controllers installed in the regional hubs. Azure Defender for Identity is not part of Azure Security Center and requires a separate license. Baker Hughes has purchased the Enterprise Mobility & Security (EMS) E5 suite license, which is required for Azure Defender for Identity.

To deploy Azure Defender for Identity, the following steps are required:

1. Create the Azure Defender for Identity instance by logging into the portal at <https://portal.atp.azure.com/tenantPortal> as a global administrator or security administrator on the Bakerhughes.com Azure AD tenant.
2. Connect the Azure Defender instance to the BHI Master Active Directory forest. An Azure Defender for Identity service account is recommended. The service account is a standard user account on the domain.
3. Download the sensor package from the portal and copy the access key to use during the install.
4. Install the package on the domain controller.

. For more information see <https://docs.microsoft.com/en-us/defender-for-identity/>



#### Identity Protection

Azure AD Identity Protection policies will be configured to provide the following levels of protection:

|  |  |  |  |
| --- | --- | --- | --- |
| Policy | Users | Conditions | Access |
| User Risk Policy | All Users | High | Allow and force password change |
| Sign-in Risk Policy | All Users | Medium & above | Allow and require MFA |

An Azure AD P2 license is required to enable Azure AD Identity Protection, which is included in the Office 365 E5 license currently owned. It is recommended to automate detection and remediation. The following table details the risk detection types detected by Azure AD Identity Protection.

|  |  |
| --- | --- |
| Risk detection type | Description |
| Anonymous IP address | Sign in from an anonymous IP address (for example: Tor browser, anonymizer VPNs). |
| Atypical travel | Sign in from an atypical location based on the user's recent sign-ins. |
| Malware linked IP address | Sign in from a malware linked IP address. |
| Unfamiliar sign-in properties | Sign in with properties we've not seen recently for the given user. |
| Leaked Credentials | Indicates that the user's valid credentials have been leaked. |
| Password spray | Indicates that multiple usernames are being attacked using common passwords in a unified, brute-force manner. |
| Azure AD threat intelligence | Microsoft's internal and external threat intelligence sources have identified a known attack pattern. |
| New country | This detection is discovered by [Microsoft Cloud App Security (MCAS)](https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy#activity-from-infrequent-country). |
| Activity from anonymous IP address | This detection is discovered by [Microsoft Cloud App Security (MCAS)](https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy#activity-from-anonymous-ip-addresses). |
| Suspicious inbox forwarding | This detection is discovered by [Microsoft Cloud App Security (MCAS)](https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy#suspicious-inbox-forwarding). |

#### Multi-Factor Authentication

It is recommended to enable Multi-Factor Authentication for all users that have access to the Azure portal or Azure resources. Baker Hughes currently uses Okta for federation and MFA.

#### Privileged Identity Manager (PIM)

Privileged Identity Manager (PIM) is configured and in use at Baker Hughes. The top-level roles to be deployed for Azure are designed to require PIM activation for use. A description of the roles is in section 2.3.1 Access.

### Data Protection

* Implement Key Vault in the Infrastructure subscription/resource group to support encryption and other needs.
* Each app will deploy their own key vault for use with the application.

#### Azure Policies

The following Data Protection policies are recommended in Azure Policy. All policies will be deployed by Accenture Security.

* Secure transfer to storage accounts should be enabled.

#### Encryption

All storage is encrypted at rest using Microsoft managed keys.

Ensure storage logging is enabled Blob, Table.

#### Storage Accounts

Strongly recommend:

* Enable Secure Transfer (https). – ASC Audit.
* Enable Azure Defender for Storage: Powered by Microsoft Threat Intelligence, the detections in Defender for Storage cover the top storage threats such as anonymous access, compromised credentials, social engineering, privilege abuse, and malicious content. <https://docs.microsoft.com/en-us/azure/security-center/defender-for-storage-introduction>.
* Enable auditing for Secure Transfer.

Other recommendations

* Rotate Access Keys periodically, at least every 90 days (30 days recommended).
* Ensure that shared access signature tokens expire within an hour.
* Ensure that public access level is set to private (unless storage account is intended for public access) – Default Access Level.
* Configure network access to accept traffic from selected networks only.
* Ensure Trusted Microsoft Services is enabled for Storage Account Access (Services use strong authentication and bypass network rules) – Backup, Site Recovery, DevTest Labs, Event Grid, Event Hubs, Networking, Monitor, SQL Data Warehouse.
* Enable Soft Delete.

### Monitoring and Incident Management

Accenture will implement MyWizard for monitoring the infrastructure. See the Accenture documentation for details.

### Security Center

Azure Security Center will be deployed to all subscriptions under the BH\_MG. To support the logging, a Log Analytics workspace, **Log\_SharedSVCS\_01**, will be created in the Infrastructure RG in the Infrastructure subscription. This workspace will be configured with a 90-day retention period of logs. All subscriptions will use the **Log\_SharedSVCS\_01** workspace for Security Center. In addition, logs will be exported to storage for retention of one year.

Security Center will be deployed with the following configurations

|  |  |  |
| --- | --- | --- |
| Security Center Feature | Configuration | Description |
| Azure Defender | Enable for all services | Enabling Azure Defender was previously accomplished by enabling Security Center Standard. Enabling Azure Defender  <https://docs.microsoft.com/en-us/azure/security-center/security-center-wdatp>  Compute: Endpoint Protection  Storage: |
| ASC Default Policies | Turn on all security policies to monitor and get a score. | ASC Default Policies |
| Threat Detection Integration | Allow MCAS and Microsoft Defender for Endpoint to access Security Center Data | https://docs.microsoft.com/en-us/azure/security-center/security-center-wdatp?WT.mc\_id=Portal-Microsoft\_Azure\_Security |
| Monitoring Agent Auto-Provisioning | Enable auto-provisioning for the Log Analytics Agent for Azure VMs | Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent?WT.mc\_id=Portal-Microsoft\_Azure\_Security |
| Email Notification Contacts | Configure with the Azure roles to be notified (Owner, AccountAdmin, ServiceAdmin, contributor) and a Security contact in the additional email addresses field. Set notification to at least Owner and a Security Contact. | Security Center will notify the roles and the security contact when a high-severity alert is triggered. <https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details> |
| Email Notification Types | Enable notification for alerts with at least High Severity | https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details |
| File Integrity Management | Enable | Validates the integrity of Windows files, Windows registry, and Linux files.  <https://docs.microsoft.com/en-us/azure/security-center/security-center-file-integrity-monitoring> |
| Just-In-Time VM Access | Enable | When a user requests access to a VM, Security Center checks that the user has [Role-Based Access Control (RBAC)](https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal) permissions for that VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified.  <https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time> |
| Adaptive application controls | Enable. Must be configured when VMs are added to Azure | Azure Security Center functions as an app-locker for applications installed on monitored devices. Using AI Security Center will create a white list of allowed applications on each monitored device.  <https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application> |
| Adaptive network hardening | Enabled | Adaptive network monitoring analyzes traffic patterns for suspicious behavior, misconfigured NSG rules, and other vectors.  <https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-network-hardening>  ASB <https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security> |

### Azure Sentinel

Azure Sentinel will be deployed on the **Log\_SharedSVCS\_01** workspace being used for the Security Center logs. Deploying on the same workspace will provide Sentinel with the log data collected by Azure Security Center. The following diagram shows the connection points that will be monitored by Azure Sentinel.

Diagram

Description automatically generated

The following connectors will be deployed:

* Azure Active Directory
* Azure Active Directory Identity Protection
* Azure Activity
* Azure DDoS Protection
* Azure Defender
* Azure Firewall
* Azure SQL Databases
* Microsoft 365 Defender
* Microsoft Cloud App Security
* Microsoft Defender for Identity (Preview)
* Microsoft Defender for Office 365 (Preview)
* Office 365
* Security Events
* Syslog
* Windows Firewall

Additional connections that may be useful in the current environment but not implemented in foundations are:

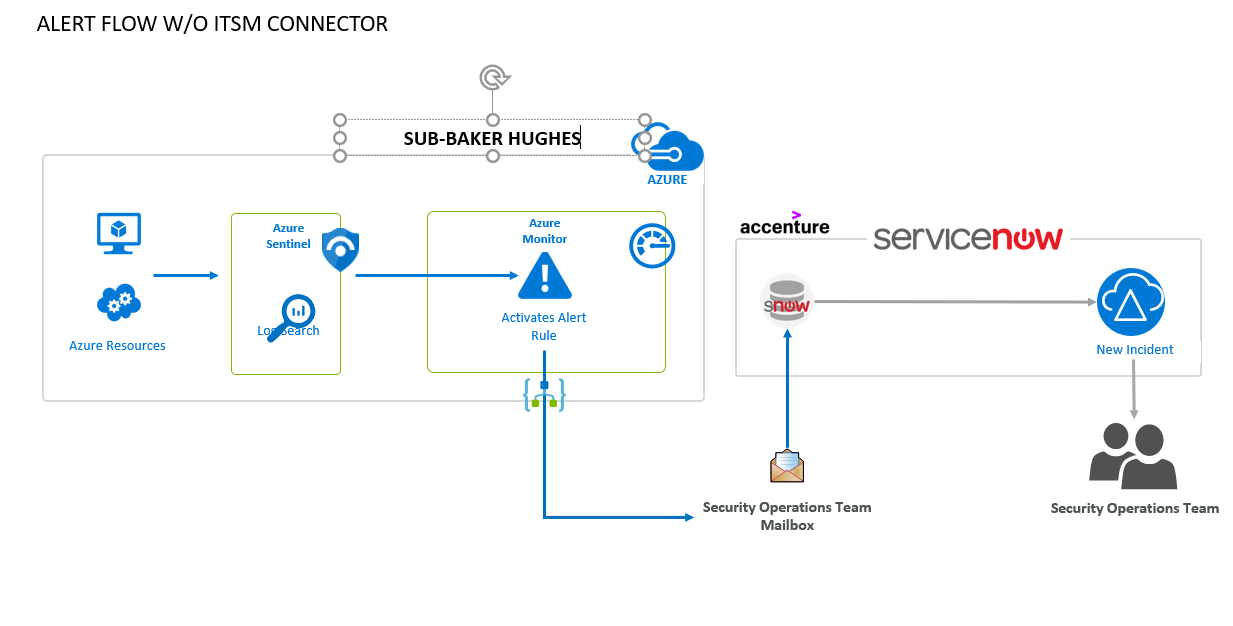
* CyberArk – Preview
* Okta Single Sign-On (Preview)

Accenture Security will review Sentinel Connectors and new features on a regular basis and will deploy additional connectors and tools as they become available and as they meet Baker Hughes requirements.

The following analytics rules will also be deployed:

* Advanced Multistage Attack Detection.
* Create incidents based on Azure Active Directory Identity Protection alerts.
* Create incidents based on Microsoft Cloud App Security alerts.
* Suspicious application consent similar to O365 Attack Toolkit.
* Create incidents based on Azure Active Directory Identity Protection alerts.
* Known Manganese IP and UserAgent activity.
* Create incidents based on Microsoft Cloud App Security alerts.

The Accenture Security team will monitor the Sentinel alerts and incidents.



## Vulnerability Management

The Accenture Security team will deploy the Azure Security Center version of Qualys to provide vulnerability management.

## Endpoint Security

### Microsoft Defender for Endpoint

Windows and Linux VMs will be hosted in the subscriptions. Microsoft defender ATP will be used for all Windows and Linux VMs

**Antivirus Design Architecture**

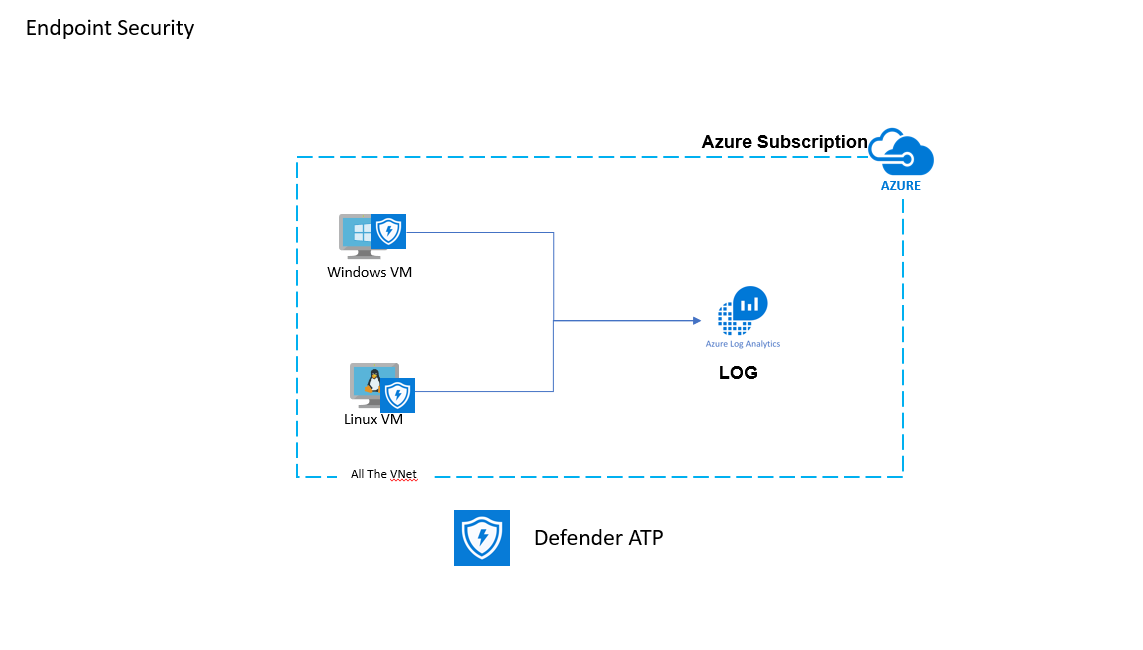


Figure 15: Antivirus High level Design

The above diagram demonstrates the high-level flow of Antivirus related logs. Defender AV logs (for widows and Linux) will be forwarded to Log analytics workspace. Different use case related to definition file update, virus detection will be created to monitor the non-updated and malware affected systems. Automatic SNOW incident will be created for malware detection and for the non-updated (definition file) systems

## **Antivirus for Windows and Linux VMs**

Microsoft Defender Advanced Threat Protection is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

**The services listed below will be enabled**

* Threat & Vulnerability Management
* Attack surface reduction
* Next generation protection
* Endpoint detection and response
* Automated investigation and remediation

Microsoft Defender Security Center is used to monitor and assist in responding to alerts of potential advanced persistent threat activity or data breaches.

[Microsoft Defender Security Center](https://securitycenter.windows.com/) to be utilized for below activities:

* View, sort, and triage alerts from Windows Servers
* Search for more information on observed indicators such as files and IP Addresses
* Change Microsoft Defender ATP settings, including time zone and review licensing information

**Portal-Tenant Configuration**

When accessing [Microsoft Defender Security Center](https://securitycenter.windows.com/) for the first time there will be a set up wizard that will guide through initial steps. At the end of the setup wizard there will be a dedicated cloud instance of Microsoft defender ATP set-up Wizard

1. **Set-up Wizard**

securitycenter.windows.com is the first time set up wizard to configure basic settings. Access to [set-up](https://securitycenter.windows.com/) wizard requires Global Administrator or Security Administrator access on Azure Activity Directory

1. **Set up preferences**

|  |  |
| --- | --- |
| Data storage location | US |
| Data retention | 180 days |
| Enable preview features | Yes |

**Below are the advance featured enabled in ATP portal**

Alert Notification will be configured to Accenture Security Team

Advanced Features

* Automated Investigation-On
* Automatically resolve alerts-On
* Defender Allow or block file-On
* Custom network indicators-On
* Show user details-On
* Skype for business integration-Off
* Azure ATP integration- On
* Web content filtering-On
* Live Response-On
* Office 365 Threat Intelligence connection- On
* Microsoft Cloud App Security- On
* Microsoft Intune connection- On
* Preview features-On

**Network Configuration**

The Microsoft Defender ATP sensor requires Microsoft Windows HTTP (WinHTTP) to report sensor data and communicate with the Microsoft Defender ATP service. The embedded Microsoft Defender ATP sensor runs in the system context using the Local System account. The sensor uses Microsoft Windows HTTP Services (WinHTTP) to enable communication with the Microsoft Defender ATP cloud service.

Below mentioned destinations need to be opened from all Windows VMs for Defender ATP

# VMs, Storage, and Backup

## Avanade Recommendations

### VMs

* Deploy VMs with managed disks
* Use Azure disk encryption where appropriate
* Deploy VMs into availability sets to qualify for the 99.95% SLA
  + For single-instance apps, use premium storage to qualify for the 99.9% SLA
* Make use of availability zones to achieve high availability
* Ensure VMs in an availability set are not sharing a storage account​
* VMs in an availability set must be in the same resource group​
* 5 update domains & 3 fault domains​
* Maximum of 100 VMs​ per availability set
* Store data on data disk(s) (separate from the OS disk) and disable caching on the data disks
* Put only temporary files (e.g., TempDB) on the Temp Drive​
* Right-sizing approach: start with the smallest VM size and scale up as needed
  + Azure Migrate and Movere will make right sizing recommendations
* Use premium disk for production applications (especially databases) and key infrastructure
* Make use of Hybrid Use Benefit (HUB), basically bring your own Windows Server license
* Consider purchasing reserved instances for VMs

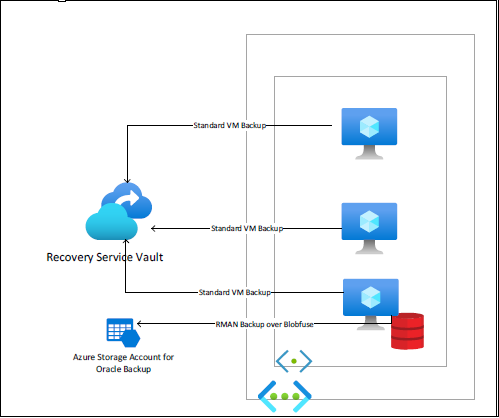
### Storage

* Require secure access to storage accounts (HTTPs, SMB encryption)
  + It’s the default setting
* Do not allow public access to the storage account, use storage access signatures (SAS) for public access.
  + It’s the default setting
* Enable storage tiering
  + General Purpose v2 (GPv2), blob, Premium Block Blob, and Azure Data Lake Storage Gen2
* Enable auditing
* Configure public access level to private
* Configure network access to accept traffic from selected networks only
* Ensure Trusted Microsoft Services is enabled for Storage Account Access
* Enable Secure Transfer
* Enable Azure Defender for Storage, detections cover the top storage threats such as anonymous access, compromised credentials, social engineering, privilege abuse, and malicious content.
* Rotate access keys at least every 90 days
* Expire shared access signature tokens within an hour
* Enable soft delete
* Enable storage logging

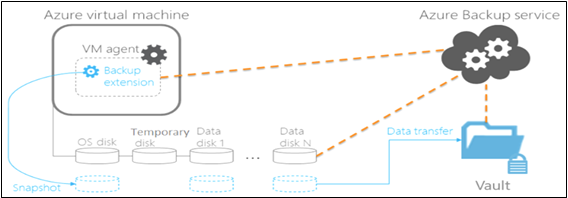
### Backup

* Use a read-only geo-redundant storage account for the recovery services vault

ARCHITECTURAL DIAGRAM:

* 

HIGH LEVEL AZURE BACKUP MECHANISM



RECOVERY SERVICES VAULT

|  |  |  |  |
| --- | --- | --- | --- |
| NAME | RESOURCE GROUP | LOCATION | SUBSCRIPTION |
| rsv-bh\_hc\_non\_prod1-eus-01 | rg-hcnonprod1-eastus | East US | BH\_HC\_NON\_PROD1 |
| rsv-bh\_hc\_prod1-eus-01 | rg-hcprod1-eastus | East US | BH\_HC\_PROD1 |
| rsv-bh\_infra\_1-eus-01 | rg-infra | East US | BH\_INFRA\_1 |
| rsv-bh\_non\_hc\_non\_prod1-eus-01 | rg-nonhcnonprod1-eastus | East US | BH\_NON\_HC\_NON\_PROD1 |
| rsv-bh\_non\_hc\_prod1-eus-01 | rg-nonhcprod1-eastus | East US | BH\_NON\_HC\_PROD1 |
| rsv-bh\_sandbox1-eus-01 | rg-sandbox-eastus | East US | BH\_SANDBOX1 |
| rsv-bh\_hc\_non\_prod1-weu-01 | rg-hcnonprod1-weu | West Europe | BH\_HC\_NON\_PROD1 |
| rsv-bh\_hc\_prod1-weu-01 | rg-hcprod1-weu | West Europe | BH\_HC\_PROD1 |
| rsv-bh\_infra\_1-weu-01 | rg-infra-weu | West Europe | BH\_INFRA\_1 |
| rsv-bh\_non\_hc\_non\_prod1-weu-01 | rg-nonhcnonprod1-weu | West Europe | BH\_NON\_HC\_NON\_PROD1 |
| rsv-bh\_non\_hc\_prod1-weu-01 | rg-nonhcprod1-weu | West Europe | BH\_NON\_HC\_PROD1 |
| rsv-bh\_sandbox1-weu-01 | rg-sandbox-weu | West Europe | BH\_SANDBOX1 |
| rsv-oracle-iaas-non\_hc\_nonprod-weu-01 | rg-oracle-iaas-nonhc-nonprod-weu-01 | West Europe | BH\_NON\_HC\_NON\_PROD1 |
| rsv-oracle-iaas-nonhc-prod-weu-01 | rg-oracle-iaas-nonhc-prod-weu-01 | West Europe | BH\_NON\_HC\_PROD1 |
| rsv-oracle-iaas-non\_hc\_nonprod-eus-01 | rg-oracle-iaas-nonhc-nonprod-eus-01 | East US | BH\_NON\_HC\_NON\_PROD1 |
| rsv-oracle-iaas-nonhc-prod-eus-01 | rg-oracle-iaas-nonhc-prod-eus-01 | East US | BH\_NON\_HC\_PROD1 |
| rsv-oracle-iaas-hc-nonprod-weu-01 | rg-oracle-iaas-hc-nonprod-weu-01 | West Europe | BH\_HC\_NON\_PROD1 |
| rsv-oracle-iaas-hc-prod-weu-01 | rg-oracle-iaas-hc-prod-weu-01 | West Europe | BH\_HC\_PROD1 |
| rsv-oracle-iaas-hc-nonprod-eus-01 | rg-oracle-iaas-hc-nonprod-eus-01 | East US | BH\_HC\_NON\_PROD1 |
| rsv-oracle-iaas-hc-prod-eus-01 | rg-oracle-iaas-hc-prod-eus-01 | East US | BH\_HC\_PROD1 |
| [RSV-INFRA-VWE-NON-PROD1-EUS-01](https://portal.azure.com/?feature.msaljs=false#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_AVD_Infra_NonProd-eastUS/providers/Microsoft.RecoveryServices/vaults/RSV-INFRA-VWE-NON-PROD1-EUS-01) | RG\_Citrix\_BH\_AVD\_Infra\_NonProd-eastUS | East US | [BH\_INFRA\_VWE\_NON\_PROD1](https://portal.azure.com/?feature.msaljs=false#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6) |
| [RSV-INFRA-VWE-NON-PROD1-WEU-01](https://portal.azure.com/?feature.msaljs=false#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_AVD_Infra_NonProd-westEU/providers/Microsoft.RecoveryServices/vaults/RSV-INFRA-VWE-NON-PROD1-WEU-01) | [RG\_Citrix\_BH\_AVD\_Infra\_NonProd-westEU](https://portal.azure.com/?feature.msaljs=false#@bakerhughes.onmicrosoft.com/resource/subscriptions/955ddc46-f459-4355-9dad-24bb66f280c6/resourceGroups/RG_Citrix_BH_AVD_Infra_NonProd-westEU) | West Europe | BH\_INFRA\_VWE\_NON\_PROD1 |
| [RSV-JVNonProd-EUS-01](https://portal.azure.com/?feature.msaljs=false#@bakerhughes.onmicrosoft.com/resource/subscriptions/f9d7ad5d-660f-491c-9f52-426cc2e8457c/resourceGroups/RG-RCvault-JVNonProd-EastUS/providers/Microsoft.RecoveryServices/vaults/RSV-JVNonProd-EUS-01) | RG-RCvault-JVNonProd-EastUS | East US | BH\_JV\_NON\_PROD1 |
| [RSV-JVNonProd-WEU-01](https://portal.azure.com/?feature.msaljs=false#@bakerhughes.onmicrosoft.com/resource/subscriptions/f9d7ad5d-660f-491c-9f52-426cc2e8457c/resourceGroups/RG-RCvault-JVNonProd-WestEU/providers/Microsoft.RecoveryServices/vaults/RSV-JVNonProd-WEU-01) | RG-RCvault-JVNonProd-WestEU | West Europe | BH\_JV\_NON\_PROD1 |
| [RSV-JVProd-EUS-01](https://portal.azure.com/?feature.msaljs=false#@bakerhughes.onmicrosoft.com/resource/subscriptions/f49cf858-3ed4-4636-a2d2-4487d30a05f3/resourceGroups/RG-RCvault-JVProd-EastUS/providers/Microsoft.RecoveryServices/vaults/RSV-JVProd-EUS-01) | RG-RCvault-JVProd-EastUS | East US | BH\_JV\_PROD1 |
| [RSV-JVProd-WEU-01](https://portal.azure.com/?feature.msaljs=false" \l "@bakerhughes.onmicrosoft.com/resource/subscriptions/f49cf858-3ed4-4636-a2d2-4487d30a05f3/resourceGroups/RG-RCvault-JVProd-WestEU/providers/Microsoft.RecoveryServices/vaults/RSV-JVProd-WEU-01) | RG-RCvault-JVProd-WestEU | West Europe | BH\_JV\_PROD1 |
| RSV-BH-INFRA-WUS-01 | RG-bhge-HUB-WestUS | West US | BH\_INFRA\_1 |
| RSV-FS-BH-SAP-NON-PROD1 | RG-SAPNONPROD1-EastUS | East US | BH\_SAP\_NON\_PROD1 |
| RSV-HANA-SAP-NON-PROD1-EUS-01 | RG-SAPNONPROD1-EastUS | East US | BH\_SAP\_NON\_PROD1 |
| RSV-HANA-SAP-Nonhcprod-WEU-01 | RG-o-and-g-gsapi-NonHcProd-WestEU | West Europe | BH\_NON\_HC\_PROD1 |
| RSV-HANA-SAP-PREPROD-EUS-01 | RG\_SAP\_GTS\_QA\_DB\_PreProd\_EastUS | East US | BH\_SAP\_PREPROD1 |
| RSV-SAP-NON-PROD1-EUS-01 | RG-SAPNONPROD1-EastUS | East US | BH\_SAP\_NON\_PROD1 |
| RSV-SAP-NON-PROD1-WEU-01 | RG-SAPNONPROD1-WestEU | West Europe | BH\_SAP\_NON\_PROD1 |
| RSV-SAP-PREPROD-EUS-01 | RG\_SAP\_SCM\_QA\_App\_PreProd\_EastUS | East US | BH\_SAP\_PREPROD1 |
| RSV-SAP-PROD1-EUS-01 | RG-SAPPROD1-EastUS | East US | BH\_SAP\_PROD1 |
| RSV-SAP-PROD1-WEU-01 | RG-SAPPROD1-WestEU | West Europe | BH\_SAP\_PROD1 |
| RSV-SQL-SAP-NON-PROD1-EUS-01 | RG\_SAP\_Mock1\_Non\_Prod\_EastUS | East US | BH\_SAP\_NON\_PROD1 |

RETENTION & SCHEDULE POLICY:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S. No.** | **Policy Name** | **Snapshot Retention** | **Vault Retention** | **Backup schedule** | **Backup Time CT** |
| 1 | p-bh\_hc\_non\_prod1-eus-01 | 2 Days | 30 Days | Daily | 10:00 AM |
| 2 | p-bh\_hc\_prod1-eus-01 | 2 Days | 30 Days | Daily | 10:00 PM |
| 3 | p-bh\_infra\_1-eus-01 | 2 Days | 30 Days | Daily | 7:00 PM |
| 4 | p-bh\_non\_hc\_non\_prod1-eus-01 | 2 Days | 30 Days | Daily | 11:30 AM |
| 5 | p-bh\_non\_hc\_prod1-eus-01 | 2 Days | 30 Days | Daily | 11:30 PM |
| 6 | p-bh\_sandbox1-eus-01 | 2 Days | 30 Days | Daily | 9:00 AM |
| 7 | p-bh\_hc\_non\_prod1-weu-01 | 2 Days | 30 Days | Daily | 10:00 AM |
| 8 | p-bh\_hc\_prod1-weu-01 | 2 Days | 30 Days | Daily | 10:00 PM |
| 9 | p-bh\_infra\_1-weu-01 | 2 Days | 30 Days | Daily | 7:00 PM |
| 10 | p-bh\_non\_hc\_non\_prod1-weu-01 | 2 Days | 30 Days | Daily | 11:30 AM |
| 11 | p-bh\_non\_hc\_prod1-weu-01 | 2 Days | 30 Days | Daily | 11:30 PM |
| 12 | p-bh\_sandbox1-weu-01 | 2 Days | 30 Days | Daily | 9:00 AM |
| 15 | p-oracle-iaas-non\_hc\_nonprod-weu-01 | 2 Days | 30 Days | Daily | 8:00 AM |
| 16 | p-oracle-iaas-nonhc-prod-weu-01 | 2 Days | 30 Days | Daily | 8:00 PM |
| 17 | p-oracle-iaas-non\_hc\_nonprod-eus-01 | 2 Days | 30 Days | Daily | 9:00 AM |
| 18 | p-oracle-iaas-nonhc-prod-eus-01 | 2 Days | 30 Days | Daily | 9:00 AM |
| 19 | p-oracle-iaas-hc-nonprod-weu-01 | 2 Days | 30 Days | Daily | 8:00 AM |
| 20 | p-oracle-iaas-hc-prod-weu-01 | 2 Days | 30 Days | Daily | 8:00 PM |
| 21 | p-oracle-iaas-hc-nonprod-eus-01 | 2 Days | 30 Days | Daily | 9:00 AM |
| 22 | p-oracle-iaas-hc-prod-eus-01 | 2 Days | 30 Days | Daily | 9:00 AM |
| 23 | [P-INFRA-VWE-NON-PROD1-EUS-01](https://portal.azure.com/?feature.msaljs=false#blade/Microsoft_Azure_DataProtection/V1EditAzureIaasVMPolicyBlade/intent/MODIFY/vaultId/%2Fsubscriptions%2F955ddc46-f459-4355-9dad-24bb66f280c6%2FresourceGroups%2FRG_Citrix_BH_AVD_Infra_NonProd-eastUS%2Fproviders%2FMicrosoft.RecoveryServices%2Fvaults%2FRSV-INFRA-VWE-NON-PROD1-EUS-01/policyId/%2Fsubscriptions%2F955ddc46-f459-4355-9dad-24bb66f280c6%2FresourceGroups%2FRG_Citrix_BH_AVD_Infra_NonProd-eastUS%2Fproviders%2FMicrosoft.RecoveryServices%2Fvaults%2FRSV-INFRA-VWE-NON-PROD1-EUS-01%2FbackupPolicies%2FP-INFRA-VWE-NON-PROD1-EUS-01/policyTypesAllowed/%5B%22V1%22%5D) | 2 Days | 30 Days | Daily | 11:30 PM |
| 24 | [P-INFRA-VWE-NON-PROD1-WEU-01](https://portal.azure.com/?feature.msaljs=false#blade/Microsoft_Azure_DataProtection/V1EditAzureIaasVMPolicyBlade/intent/MODIFY/vaultId/%2Fsubscriptions%2F955ddc46-f459-4355-9dad-24bb66f280c6%2FresourceGroups%2FRG_Citrix_BH_AVD_Infra_NonProd-westEU%2Fproviders%2FMicrosoft.RecoveryServices%2Fvaults%2FRSV-INFRA-VWE-NON-PROD1-WEU-01/policyId/%2Fsubscriptions%2F955ddc46-f459-4355-9dad-24bb66f280c6%2FresourceGroups%2FRG_Citrix_BH_AVD_Infra_NonProd-westEU%2Fproviders%2FMicrosoft.RecoveryServices%2Fvaults%2FRSV-INFRA-VWE-NON-PROD1-WEU-01%2FbackupPolicies%2FP-INFRA-VWE-NON-PROD1-WEU-01/policyTypesAllowed/%5B%22V1%22%5D) | 2 Days | 30 Days | Daily | 11:30 PM |
| 25 | [P-JVProd-EUS-01](https://portal.azure.com/?feature.msaljs=false#blade/Microsoft_Azure_DataProtection/V1EditAzureIaasVMPolicyBlade/intent/MODIFY/vaultId/%2Fsubscriptions%2Ff49cf858-3ed4-4636-a2d2-4487d30a05f3%2FresourceGroups%2FRG-RCvault-JVProd-EastUS%2Fproviders%2FMicrosoft.RecoveryServices%2Fvaults%2FRSV-JVProd-EUS-01/policyId/%2Fsubscriptions%2Ff49cf858-3ed4-4636-a2d2-4487d30a05f3%2FresourceGroups%2FRG-RCvault-JVProd-EastUS%2Fproviders%2FMicrosoft.RecoveryServices%2Fvaults%2FRSV-JVProd-EUS-01%2FbackupPolicies%2FP-JVProd-EUS-01/policyTypesAllowed/%5B%22V1%22%5D) | 2 Days | 30 Days | Daily | 9:00 PM |

## Design Decisions / Requirements

No design decisions or requirements regarding VMs or storage.

* The current backup process is to perform a storage snapshot every four hours. Baker Hughes is open to alternate solutions
* RPO is four hours or less. RTO is undefined but expectation is no more than four hours
* Current S3 storage is not backed up but does have versioning capability and is able to restore accidental deletions.
* Have some criteria documented for critical applications. Will send to us for review
* Create separate backup location/vault for DCs.

## Design

Backups and disaster recovery will be like-for-like from AWS where possible. The backup solution here is being provided as a best practice and differs from the current AWS solution. Accenture will deploy a two-pronged strategy for backing up and protecting the VMs and data. To protect VMs and servers, Accenture will implement Azure Backup. To protect data, with a recovery point of 15 minutes or less, Accenture will implement a combination of backups and Always-On or data replication.

* + 1. VMs

VM names will use the following naming convention:

BHAZ<Linux/Windows><serialization><Env>

This naming convention follows the guest OS naming convention. It is intended that the console names match the guest OS names and this naming convention follows this. However, Azure VM names cannot be changed and guest OS names can, so there may be differences between the console name and the guest OS names if changes are made to the guest OS.

The VM name in the Azure portal is only for the management plane and the actual guest OS name may be different. Accenture has followed the Baker Hughes naming convention for servers and has aligned the Azure VM name with the guest OS name.

* + 1. Backups

Azure Backup performs daily application consistent and file level backups of VMs. Accenture will configure Azure

Recovery service to backup all VMs. Azure backup runs once a day and retains backups for up to 99 years configurable. Azure policies will be created to meet specific requirements. Daily backups are appropriate for most VMs and servers as web servers and application servers are mostly in a consistent state with little or no changes. Azure backup also supports SQL backup for IaaS servers with a 15-minute RPO. Azure backup can be used to backup VMs, SQL Servers, Azure Files, Managed Disks, SAP Hana on Azure VMs, Azure Database for PostgreSQL servers (preview) and Azure Blobs (preview).

To support the requirement that all VMs are backed up, the following Azure Recovery Services Vaults will be created and a default backup policy assigned. Two vaults are required for each subscription as VMs must be backed up to a vault within it’s region. In addition, a separate backup vault will be created within the BH\_INFRA\_1 subscription for the domain controllers as they require a separate vault for data security.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Vault Name | Subscription | Resource Group | Location | Storage Replication | Policy |
| RSV-Infra-US-01 | BH\_INFRA\_1 | RG-Infra | East US | LRS | Default |
| RSV-Prod-US-01 | BH\_NON\_HC\_PROD1 | RG-Infra | East US | LRS | Default |
| RSV-NonProd-US-01 | BH\_NON\_HC\_NON\_PROD1 | RG-Infra | East US | LRS | Default |
| RSV-HCProd-US-01 | BH\_HC\_PROD1 | RG-Infra | East US | LRS | Default |
| RSV-HCNonProd-US-01 | BH\_HC\_NON\_PROD1 | RG-Infra | East US | LRS | Default |
| RSV-Infra-WE-01 | BH\_INFRA\_1 | RG-Infra | West Europe | LRS | Default |
| RSV-Prod-WE-01 | BH\_NON\_HC\_PROD1 | RG-Infra | West Europe | LRS | Default |
| RSV-NonProd-WE-01 | BH\_NON\_HC\_NON\_PROD1 | RG-Infra | West Europe | LRS | Default |
| RSV-HCProd-WE-01 | BH\_HC\_PROD1 | RG-Infra | West Europe | LRS | Default |
| RSV-HCNonProd-WE-01 | BH\_HC\_NON\_PROD1 | RG-Infra | West Europe | LRS | Default |
| RSV-DC-US-01 | BH\_INFRA\_1 | RG-Infra | East US | LRS | DC |
| RSV-DC-US-01 | BH\_INFRA\_1 | RG-Infra | West Europe | LRS | DC |
| RSV-BH-INFRA-WUS-01 | BH\_INFRA\_1 | RG-bhge-HUB-WestUS | West US | LRS | Default |

* + 1. Snapshots

Snapshots can be taken of VMs and storage on as needed basis or can be scheduled at intervals using Azure automation.

* + 1. High Availability

Accenture will deploy High Availability configurations to protect data down to a 30 second RPO. The following configurations will be deployed as required by applications.

* SQL Always-On High Availability using Availability Zones
* Azure SQL Geo Replication

Site Recovery to an alternate region is currently not in place in the current AWS and is not required. Azure Site Recovery can be deployed later as requirements dictate. To support a DR region, the infrastructure including networking and Active Directory will be required. Governance will remain in force as deployed in the current infrastructure. Deploying a DR region will require additional traffic management to route traffic from the primary data center to the alternate data center. The following diagram shows a Traffic Manager configuration.

# Disaster Recovery

## Avanade Recommendations

* Evaluate individual workloads for RTO/RPO requirements (as a business decision)
* Decompose applications into the smallest functional component rather than viewing the system as a single application
* Do not depend on Microsoft Regional pairings as the primary solution for disaster recovery. Develop and implement solutions to enable control of the failover timing, process, and recovery
* Understand Azure regional limits for specific services and plan accordingly based on RTO/RPO requirements (Key Vault, provisioned capacity, etc.)
  + Use Azure-native solutions where possible to benefit from integration and Microsoft investments
  + PaaS-first approach
* Establish and govern IaaS guidance (availability sets, update domains, fault domains, storage, etc.)
* As a rule, use LRS storage as the default for optimal performance and cost. Look for alternatives before choosing GRS for geo-redundancy, if required.
* Avoid legacy patterns and implement cloud-native approaches, where possible (automation, replication, application architecture, etc.)
* Provide equal focus on both technical and operating model changes
* Test DR/HA scenarios often

## Design Decisions/Requirements

* Disaster recovery to an alternate region is not currently in place.

## Design

Site Recovery to an alternate region is currently not in place in the current AWS and is not required. Azure Site Recovery can be deployed later as requirements dictate. To support a DR region, the infrastructure including networking and Active Directory will be required. Governance will remain in force as deployed in the current infrastructure. Deploying a DR region will require additional traffic management to route traffic from the primary data center to the alternate data center. The following diagram shows a Traffic Manager configuration.

Applications can be designed using HA technologies, such as Availability sets, Availability zones, load balancers, etc. and would-be application specific based on needs.

* 

ASR Vaults are protected by GEO Redundant storage. Traffic manager is a global service managed by Azure.

# Operations

## Avanade Recommendations

### -Logging and Monitoring

* Azure monitor for all IaaS and PaaS.
  + Create recommended alerts
    - Policy Assignment
    - Create or Update NSG
    - Delete NSG
    - Create or Update Security Solution
    - Delete Security Solution
    - Crete, Delete, or Update SQL Server Firewall rule
* Centralized Log Analytics.

### For AV for VMs

* Extend existing solution into Azure or use Microsoft Defender

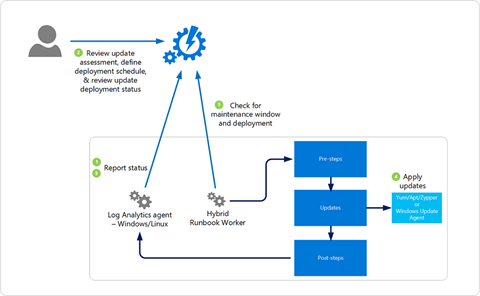
### Patch Management

Patch Management is crucial to security and vulnerability risk mitigation. Using Update Management in Azure Automation to manage OS patches & updates for your Windows & Linux VMs in Azure, as well as physical or VMs on-premises. Update Management helps quickly assess the status of available updates and manage the process of installing required updates for your machines reporting to Update Management. All in an automated fashion. Baker Hughes will use Azure Automation Update Management for its patch management processes.

#### Azure Update Management High Level Overview

Azure Update Management uses the Microsoft Monitoring Agent (MMA) for Windows or Linux, PowerShell Desired State Configuration (DSC) for Linux, an Automation Hybrid Runbook Worker, and Microsoft Update or Windows Server Update Services (WSUS) for Windows servers.

The following diagram illustrates how Update Management assesses and applies security updates to all connected Windows Server and Linux servers.



#### OS Requirements

Update Management supports specific versions of the Windows Server and Linux operating systems. The following table list the supported operating systems for update assessment & patching.

|  |  |
| --- | --- |
| Supported OS | Notes |
| Windows Server 2019 (Datacenter/Datacenter Core/Standard) |  |
| Windows Server 2016 (Datacenter/Datacenter Core/Standard) |  |
| Windows Server 2012 R2(Datacenter/Standard) |  |
| Windows Server 2012 |  |
| Windows Server 2008 R2 (RTM and SP1 Standard) | Update Management supports assessments and patching for this operating system |
| CentOS 6 and 7 (x64) | Linux agents require access to an update repository over the internet. |
| Red Hat Enterprise 6, 7 & 8 (x64) | Linux agents require access to an update repository over the internet. |
| Oracle Linux | Note: Outside Support from Update Management  Approach: Oracle Linux servers are registered with the ULN (Unbreakable Linux Network) repository, and then the yum utilities are used to download and install the required patches. |

|  |  |
| --- | --- |
|  | ***Important Note***  *Oracle Linux VMs will be patched using Ansible playbook and Oracle Unbreakable Linux Network* |

#### RBAC Access

Update Management can be used to assess and schedule update deployments to machines in multiple subscriptions in the same Azure Active Directory (Azure AD) tenant. For more info on RBAC Access see Microsoft documentation: RBAC for Update Management Permissions. The following table lists the permissions needed to manage update deployments. The following table lists the permissions needed to manage update deployments.

|  |  |  |
| --- | --- | --- |
| Resource | Role | Scope |
| Automation Account | Custom Azure Automation Contributor role | Automation account |
| Automation Account | Virtual Machine Contributor | Resource Group for the account |
| Log Analytics workspace Log Analytics Contributor | Log Analytics workspace |  |
| Log Analytics workspace | Log Analytics Reader | Subscription |
| Solution | Log Analytics Contributor | Solution |
| Virtual Machine | Virtual Machine Contributor | Virtual Machine |

**Actions on Virtual Machine**

Below permissions are required for Software Update Configuration.

|  |  |  |
| --- | --- | --- |
| Actions | Permission | Scope |
| View history of update schedule execution | Reader | Automation Account |
| Create update schedule | Microsoft.Compute/virtualMachines/write | For static VM list and resource groups |
| Create update schedule | Microsoft.OperationalInsights/workspaces/analytics/query/action | For workspace resource ID when using non-Azure dynamic list. |

#### Limitations

The following table shows limits for Update Management in Automation account.

|  |  |
| --- | --- |
| Resource | Limit |
| Number of machines per update deployment | 1000 |
| Number of dynamic groups per update deployment | 500 |

#### Network Requirements

See Azure Automation network configuration details.

The following port and URLs are required for the Hybrid Runbook Worker, and for Automation State Configuration to communicate with Azure Automation.

* Port: Only 443 required for outbound internet access to MS repo
* Global URL: \*.azure-automation.net
* ~~Global URL of US Gov Virginia: \*.azure-automation.us~~
* Agent service: https://<workspaceId>.agentsvc.azure-automation.net

The addresses in this table are required both for Update Management and for Change Tracking and Inventory. The paragraph following the table also applies to both. Communication to these addresses uses port 443.

**Azure Public**

* \*.ods.opinsights.azure.com
* \*.oms.opinsights.azure.com
* \*.blob.core.windows.net
* \*.azure-automation.net

Create network group security rules or configure Azure Firewall to allow traffic to the Automation service and the Log Analytics workspace, use the service tags **GuestAndHybridManagement** and **AzureMonitor**. This simplifies the ongoing management of network security rules.

Windows VM in Azure network & internet traffic is routed through Azure firewall, allow them to update either with Automatic updates or Azure Update Management. Below rules added to get through firewall. Firewall Rules should be implemented to properly allow communication (using application rules). Proposed rules are below:

|  |  |  |
| --- | --- | --- |
| Rule # | Rule Type | Rule |
| 01 | FQDN | **Name**: Windows\_Update (No whitespace)**Priority**: 2000 (A number between 100-65000)  **Action**: Allow  **Rule**: FQDN Tags  **Name**: Windows Update  **Source Type**: IP Address  **Source**: Prefix of vNet/Subnet or host, ex. 10.1.0.0/22 or \* (any source)  **FQDN tags**: WindowsUpdate (Select in the dropdown) |
| 02 | Target FQDN | **Name**: Monitoring\_Agent (No whitespace)  **Priority**: 2100 (A number between 100-65000)  **Action**: Allow  **Rule**: Target FQDNs  **Name**: OMS Agent  **Source Type**: IP Address  **Source**: Prefix of vNet/Subnet or host, ex. 10.1.0.0/22 or \* (any source)  **Protocol**: Port: https:443  **Target FQDNs**: \*.ods.opinsights.azure.com,\*.oms.opinsights.azure.com,\*.blob.core.windows.net |
| 03 | Target FQDN | **Name**: Hybrid\_Runbook\_Worker (No whitespace)  **Priority**: 2200 (A number between 100-65000)  **Action**: Allow  **Rule**: Target FQDNs  **Name**:Hybrid Runbook Worker  **Source** Type: IP Address  **Source**: Prefix of vNet/Subnet or host, ex. 10.1.0.0/22 or \* (any source)  **Protocol**:Port: https:443  **Target FQDNs**: \*.azure-automation.net |
| 04 | Target FQDN | **Name**: Allow\_Update  **Priority**: 2300 (A number between 100-65000)  **Action**: Allow  **Rule**: Target FQDNs  **Name**: Allow Updates  **Source** Type: IP Address  **Source**: Prefix of vNet/Subnet or host, ex. 10.1.0.0/22 or \* (any source)  **Protocol**:Port: Https:443,Http:80  **Target FQDNs**: ntservicepack.microsoft.com,download.microsoft.com,download.windowsupdate.com, \*.windowsupdate.microsoft.com,wustat.windows.com,\*.download.windowsupdate.com, \*.windowsupdate.com,windowsupdate.microsoft.com,\*.update.microsoft.com,go.microsoft.com, dl.delivery.mp.microsoft.com |

#### Schedule

The VM’s that are deployed into BH subscription require regular operating system patches to be applied, Azure update Management is being used.

Two components control the application of system updates to infrastructure servers:

An Azure Automation Account

A GPO in the BH domain, which defines the Windows Update configuration. All servers will be in scope of this policy. (This needs to be validated)

The following schedules can be configured on the automation account to manage OS patching.

4 schedules created based on environments. Grouping can subject to change in future.

|  |  |  |  |
| --- | --- | --- | --- |
| UM Schedule Name | OS Type | Groups to update | Schedule |
| Group-1 | Windows/Linux | BH\_NON\_HC\_NON\_PROD  BH\_HC\_NON\_PROD  BH\_SANDBOX1 | Friday after second Tuesday 10 PM to 4 AM Central Time. |
| Group-2 | Windows/Linux | BH\_NON\_HC \_PROD BH\_INFRA\_1 (Exclude DC)  BH\_HC \_PROD | Second Friday after second Tuesday 10 PM to 4 AM Central Time. |
| Group-3 | Windows/Linux |  | Third Wednesday 10 PM – 4 PM Central Time. |

|  |  |
| --- | --- |
|  | ***Important Note***  *Domain Controllers are managed by BH AD team. They should not be part of any of the schedule.* |

The following table defines the classifications that Update Management supports for Windows updates.

|  |  |  |
| --- | --- | --- |
| Classification | Included for patching | Description |
| Critical updates | Yes | An update for a specific problem that addresses a critical, non-security-related bug. |
| Security updates | Yes | An update for a product-specific, security-related issue. |
| Update rollups | Yes | A cumulative set of hotfixes that are packaged together for easy deployment. |
| Feature packs | excluded | New product features that are distributed outside a product release. |
| Service packs | Yes | A cumulative set of hotfixes that are applied to an application. |
| Definition updates | Yes | An update to virus or other definition files. |
| Tools | excluded | A utility or feature that helps complete one or more tasks. |
| Updates | excluded | An update to an application or file that currently is installed. |

The next table defines the supported classifications for Linux updates.

|  |  |  |
| --- | --- | --- |
| Classification | Included for patching | Description |
| Critical and security updates | Yes | Updates for a specific problem or a product-specific, security-related issue. |
| Other updates | excluded | All other updates that aren't critical in nature or that aren't security updates. |

### Infrastructure as Code

* Use automation (ARM / Terraform templates) and DevOps repos, pipeline for deployment. Needs proper design and life cycle mgmt.

### Service introduction

* Assign Azure Product owner (team). Understand, secure, automate, governance with policy and operationalize every Azure service and stamp it “GA at Client”
* Develop Build a service catalog for approved/operationalized Azure services for app teams to consume

### IT Service Management

* Use exiting and extend to support Azure operations. Integrate with Azure Monitor.
* CMDB – extend CMDB to Azure resources or invest on new solution, integrate with ISTM.
  + NOTE: Do not use the Azure resource tagging system as a CMDB replacement/surrogate

### SMTP

* SMTP server name : smtphosthou.bakerhughes.com   port 25 for SMTP authentication and trigger the email alerts.
* Configure postfix service for SMTP.
* Requires a service acct requested from BH Service Catalog.
* Sample table info to be filled and once service account is created then raise a request in service desk for the servers to enable the service account

|  |  |  |
| --- | --- | --- |
| Sl. No | Application Details | Comments |
| 1 | Is the server application from which you are trying to configure emails connected to BHI Internal Network: |  |
| 2 | Please provide the Host Name and IP address of the server: |  |
| 3 | Does the mail sending application support SMTP authentication?    If YES, please request for a SMTP service account at [http://servicecatalog](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Furldefense.proofpoint.com%2Fv2%2Furl%3Fu%3Dhttp-3A__servicecatalog%26d%3DDwMFAw%26c%3DeIGjsITfXP_y-DLLX0uEHXJvU8nOHrUK8IrwNKOtkVU%26r%3DoQtnelxcQjQfJxnGfdu7TjE9kRDv5GXaWQF9-q03c6E%26m%3DY5VQj4GcvmsN3VxgiWsEUou-ccJ5-bLltoPhLZJQ30Y%26s%3DHzbO_HAS_yPp1u6zn1gBvEm-L6db-vAcHpIAKlUT1_o%26e%3D&data=04%7C01%7Cvirat.dogra%40avanade.com%7C6e16ae60665640c0ca5008d92693e414%7Ccf36141cddd745a7b073111f66d0b30c%7C0%7C1%7C637583238898072635%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=VbchGTkFnA0UmmzFcWEguJnuvagRbgdniMAFl5qL5i4%3D&reserved=0) à User Account Services à Special use Network Accounts Service account. In this case, use the SMTP relay server as smtphosthou.bakerhughes.com (172.30.144.130) and Port 25 and use the SMTP service account details to authenticate the SMTP session.    If NO, please fill-in the details requested in point 4, 5 and 6 as we need to allow the IP address of the application server to our SMTP allow list. In this case, the SMTP server name will be altsmtphosthou.bakerhughes.com (172.30.144.129) and port 25. |  |
| 4 | Business / Application Owner email address : |  |
| 5 | Server Owner email address: |  |
| 6 | Business Justification for this operation (Business reason to allow the application to directly relay through BHI SMTP server) |  |

### Active Services in use (Dynamic list)

[Azure Approved Services and C-SCIF Controls (sharepoint.com)](https://bakerhughes.sharepoint.com/sites/BHAzureHome/SitePages/Azure-Security-Services.aspx)

Identity & Security:

* Key Vault
* AAD
* Defender for Endpoint
* Defender for Cloud
* Azure Sentinel
* Azure Policies

Monitor:

* Application Insights
* Log Analytics Workspace
* Azure Monitor

Storage:

* Azure Storage
* Recovery Service Vault

General[:](https://bakerhughes.sharepoint.com/:x:/r/sites/BHAzureHome/Shared%20Documents/Security%20Services/C-SCIF%20Rules%20(Azure%20Policies)/06_General/General.xlsx?d=wb2258660f8f243b4ac2c4f5cd6c6efd6&csf=1&web=1&e=T38Wom)

* Resource Groups
* Guest Configuration (Upcoming- Phase 6)
* Compute Galleries (Upcoming- Phase 6)

Compute:

* Virtual Machines
* App Service
* Function App

Integration:

* API Management
* Logic App
* Service Bus

Internet of Things:

* IoT Hub
* Time Series Insights
* Machine Learning
* Machine Learning Services
* Translators (Upcoming- Phase 6)

Networking:

* Azure Firewall
* Public IP Address
* NSG
* ASG
* NIC
* Load Balancer
* Application Gateway
* Private Endpoint
* Service Endpoint
* Express Route and VPN
* DNS Zones (Upcoming- Phase 6)
* Traffic Manager (Upcoming- Phase 6)
* Application Security Group (Upcoming- Phase 6)

Databases:

* AzureSQL
* MariaDB
* MySQL
* PostgreSQL
* Cosmos DB
* Cache for Redis
* IaaS Oracle
* IaaS MSSQL
* SQL MI
* Postgres and SQL flexiservers
* PostgreSQL Hyperscale

Analytics:

* Azure Data Factory
* Azure Synapse
* Event Hub
* Azure Databricks

Containers:

* Container Registry
* Container Instance
* AKS

Migration:

* Azure Migrate (Upcoming- Phase 6)

Management & Governance:

* Automation Account (Upcoming- Phase 6)
* Automanage (Upcoming- Phase 6)
* Managed Application

# Sandbox design and architecture

### IP Addressing

## On-Premises Ranges

The following table shows the private IP Address ranges that are being used at Baker Hughes. Rows 1-3 are the IANA Private IP Ranges that are predefined to be private ranges. Rows 4-6 show the additional addresses that BH is using as internal address spaces.

## Sandbox Ranges

|  |  |
| --- | --- |
| Network ID | Description |
| 10.0.0.0/8 | IANA Private IP Ranges |
| 172.16.0.0/12 |
| 192.168.0.0/16 |
| 3.0.0.0/8 | BH Provided Internal IP Ranges |
| 147.108.0.0/16 |
| 151.95.0.0/18 |

The sandbox will have only one hub and one spoke per region. All of these networks will be contained within the 10.22.160.0/19 range. This range overlaps with other address spaces, so it is important to note that there is no supported connectivity to the GE network. However, resources can still connect to the Baker Hughes internal network.

This range is divided in half to dedicated a /20 range to each region (US East and West Europe). Within those ranges a /23 is used for a hub and the remaining addresses are associated with the spokes. This provides ample addresses in the spokes to support current services and provide space to grow if needed.

Below is a breakdown of how the address space is divided

|  |  |  |
| --- | --- | --- |
| Sandbox Address Space | Regions | Networks |
| Sandbox Range  10.22.160.0/19 | **US East**  10.22.160.0/20 | **SBX-HUB-US**  10.22.160.0/23 |
| **SBX-SPK1-US**  10.22.162.0/23  10.22.164.0/22  10.22.168.0/21 |
| **West Europe**  10.22.176.0/20 | **SBX-HUB-EU**  10.22.176.0/23 |
| **SBX-SPK1-EU**  10.22.178.0/23  10.22.180.0/22  10.22.184.0/21 |

### Hub Design

## High Level Design

Each regional hub will split into five subnets – GatewaySubnet, AzureFirewallSubnet, AzureBastionSubnet, SharedServices, and AppGatewaySubnet. The hub will serve as the network’s main point for on-prem connectivity and hold any necessary shared services for the spokes.

The VPN and ExpressRoute gateways will be in the GatewaySubnet. Services such as Azure Firewall or Azure Bastion will be in their respective subnets. Shared Services will contain other infrastructure related resources such as jumphosts, domain controllers, etc. Finally, the AppGatewaySubnet will be used for any application gateways with public IPs associated on their front end (i.e. app gateways v2). The CIDRs and masks are listed below for the respective region.



Figure 1 High level hub design.

## US East Hub

The US East Hub and its related resources will be contained within the RG-SBX-HUB-US-Network resource group.

Below is the information about the network’s address space and subnets.

|  |  |  |
| --- | --- | --- |
| Network Name | CIDR Range | Number of Addresses |
| SBX-HUB-US | 10.22.160.0/23 | 512 |

|  |  |  |
| --- | --- | --- |
| Subnet Name | Subnet ID/Mask | Number of Usable Addresses |
| Gateway Subnet | 10.22.160.0/26 | 58 |
| AzureFirewallSubnet | 10.22.160.64/26 | 58 |
| AzureBastionSubnet | 10.22.160.128/26 | 58 |
| SharedServicesSubnet | 10.22.160.192/26 | 58 |
| AppGatewaySubnet | 10.22.161.0/25 | 122 |
| Reserved for Growth | 10.22.161.128/25 | 122 |

## West Europe Hub

The West Europe Hub and its related resources will be contained within the RG-SBX-HUB-EU-Network resource group.

Below is the information about the network’s address space and subnets.

|  |  |  |
| --- | --- | --- |
| Network Name | CIDR Range | Number of Addresses |
| SBX-HUB-EU | 10.22.176.0/23 | 512 |

|  |  |  |
| --- | --- | --- |
| Subnet Name | Subnet ID/Mask | Number of Usable Addresses |
| Gateway Subnet | 10.22.176.0/26 | 58 |
| AzureFirewallSubnet | 10.22.176.64/26 | 58 |
| AzureBastionSubnet | 10.22.176.128/26 | 58 |
| SharedServicesSubnet | 10.22.176.192/26 | 58 |
| AppGatewaySubnet | 10.22.177.0/25 | 122 |
| Reserved for Growth | 10.22.177.128/25 | 122 |

### Spoke Design

## High Level Design

Each spoke will split into four subnets – FrontEndSubnet, BackEndSubnet, AppGatewaysSubnet, and SqlMISubnet. The hub will serve as the network’s main point for on-prem connectivity and hold any necessary shared services for the spokes.

The front-end subnet is designed for application servers and any supporting resources. Those servers will connect to databases that are in the back-end subnet. Some services like SQL managed instances also require their own dedicated route tables and can be moved into the SqlMISubnet. Any application gateways that are needed for the apps can be deployed into the AppGatewaySubnet.

The CIDRs and masks are listed below for the respective region. To use all the necessary addresses in the range, three CIDR ranges are combined to make each spoke.



Figure 2 High level spoke design.

## US East Spoke

The US East Spoke and its related resources will be contained within the RG-SBX-SPK-US-Network resource group.

Below is the information about the network’s address space and subnets.

|  |  |  |
| --- | --- | --- |
| Network Name | CIDR Range | Number of Addresses |
| SBX-SPK1-US | 10.22.162.0/23 & 10.22.164.0/22 & 10.22.168.0/21 | 3584 |

|  |  |  |
| --- | --- | --- |
| Subnet Name | Subnet ID/Mask | Number of Usable Addresses |
| FrontEndSubnet | 10.22.162.0/24 | 252 |
| BackEndSubnet | 10.22.163.0/24 | 252 |
| AppGatewaySubnet | 10.22.164.0/24 | 252 |
| SqlMISubnet | 10.22.165.0/24 | 252 |
| PrivateLinkSubnet | 10.22.166.0/24 | 252 |
| Reserved for Growth | 10.22.167.0/24 | 252 |
| Reserved for Growth | 10.22.168.0/21 | 1020 |

## Bastion

## East US IP - 10.22.161.197

West EU - 10.22.177.196

Access requested via Myaccess and Syed Aali can approve

HPA group for SBX JUMP server- BHCAzure\_sbx\_jump\_HPA

## West Europe Spoke

The West Europe Spoke and its related resources will be contained within the RG-SBX-SPK-EU-Network resource group.

Below is the information about the network’s address space and subnets.

|  |  |  |
| --- | --- | --- |
| Network Name | CIDR Range | Number of Addresses |
| SBX-SPK1-EU | 10.22.178.0/23 & 10.22.180.0/22 & 10.22.184.0/21 | 3584 |

|  |  |  |
| --- | --- | --- |
| Subnet Name | Subnet ID/Mask | Number of Usable Addresses |
| FrontEndSubnet | 10.22.178.0/24 | 252 |
| BackEndSubnet | 10.22.179.0/24 | 252 |
| AppGatewaySubnet | 10.22.180.0/24 | 252 |
| SqlMISubnet | 10.22.181.0/24 | 252 |
| PrivateLinkSubnet | 10.22.182.0/24 | 252 |
| Reserved for Growth | 10.22.183.0/24 | 252 |
| Reserved for Growth | 10.22.183.0/21 | 1020 |

### Connectivity

## On-Prem

### ExpressRoute

The express route connection will be determined later.

### VPN Tunnel

The VPN tunnel will be created using the multiple on-premises devices configuration as described in the [documentation](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-highlyavailable#multiple-on-premises-vpn-devices). There will be two on-prem routers in each region that are configured to connect to two local network gateways. Those gateways will then pass the traffic to a VPN virtual network gateway in Azure which will direct the traffic to the firewall for inspection and logging.

More information on address configuration to come.

## Peering

### Hub to Spoke Peering

The following table shows the peering for each hub to spoke connection. There is one per region connecting to its respective spoke.

|  |  |  |
| --- | --- | --- |
| Peering Name | Source Network | Destination Network |
| SBX-SPK1-US-Peering | SBX-HUB-US | SBX-SPK1-EU |
| SBX-SPK1-EU-Peering | SBX-HUB-EU | SBX-SPK1-EU |

For these connections, the configuration should be as follows:

* Traffic to Remote Virtual Networks – Allow
* Traffic forwarded from remote virtual network – Allow
* Virtual Network Gateway or Route Server – Use this Virtual Network’s Gateway or Route Server

### Spoke to Hub Peering

The table below shows the peering connections that are from a Spoke VNet to a Hub VNet.

|  |  |  |
| --- | --- | --- |
| Peering Name | Source Network | Destination Network |
| SBX-HUB-US-Peering | SBX-SPK1-US | SBX-HUB-US |
| SBX-HUB-EU-Peering | SBX-SPK1-EU | SBX-HUB-EU |

For these connections, the configuration should be as follows:

* Traffic to Remote Virtual Networks – Allow
* Traffic forwarded from remote virtual network – Allow
* Virtual Network Gateway or Route Server – Use the remote virtual network’s gateway or route server

### Hub-Hub

The table below shows the peering connections that are from a Hub VNet to a Hub VNet.

|  |  |  |
| --- | --- | --- |
| Peering Name | Source Network | Destination Network |
| SBX-HUB-EU-Peering | SBX-HUB-US | SBX-HUB-EU |
| SBX-HUB-US-Peering | SBX-HUB-EU | SBX-HUB-US |

For these connections, the configuration should be as follows:

* Traffic to Remote Virtual Networks – Allow
* Traffic forwarded from remote virtual network – Allow
* Virtual Network Gateway or Route Server – Use this Virtual Network’s Gateway or Route Server

## Routing

To ensure that Azure Firewall inspects any traffic that goes between virtual networks, route tables will be used to tunnel traffic to it’s correct destination. Each subnet will have a route table assigned to it. The exception will be the Azure Bastion subnet in each hub which cannot have a route table associated.

Many of the route tables uses specific routes that are defined below to invalidate the default routes that shouldn’t be utilized. The propagate gateway routes setting will have to be configured on each route table to determine if the default on-premises routes should be included in the route table.

### Hub Route Tables

#### GatewaySubnet

Below are the routes for route table, *Route-SBX-HUB-US-GatewaySubnet*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-HUB-US-Network resource group. The *GatewaySubnet* is associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-HUB-US-GatewaySubnet | | |
| Name | **Address Prefix** | **Next Hop** |
| SBX-HUB-US | 10.22.160.0/23 | US Firewall (10.22.160.68) |
| SBX-SPK1-US1 | 10.22.162.0/23 | US Firewall (10.22.160.68) |
| SBX-SPK1-US2 | 10.22.164.0/22 | US Firewall (10.22.160.68) |
| SBX-SPK1-US3 | 10.22.168.0/21 | US Firewall (10.22.160.68) |

Configuration: Propagate Gateway Routes - Yes

Below are the routes for route table, *Route-SBX-HUB-EU-GatewaySubnet*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-HUB-EU-Network resource group. The *GatewaySubnet* is associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-HUB-EU-GatewaySubnet | | |
| Name | **Address Prefix** | **Next Hop** |
| SBX-HUB-EU | 10.22.176.0/23 | EU Firewall (10.22.176.68) |
| SBX-SPK1-EU1 | 10.22.178.0/23 | EU Firewall (10.22.176.68) |
| SBX-SPK1-EU2 | 10.22.180.0/22 | EU Firewall (10.22.176.68) |
| SBX-SPK1-EU3 | 10.22.184.0/21 | EU Firewall (10.22.176.68) |

Configuration: Propagate Gateway Routes - Yes

#### AzureFirewallSubnet

Below are the routes for route table, *Route-SBX-HUB-US-AzureFirewallSubnet*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-HUB-US-Network resource group. The *AzureFirewallSubnet* is associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-HUB-US-AzureFirewallSubnet | | |
| Name | **Address Prefix** | **Next Hop** |
| Internet | 0.0.0.0/0 | Internet |
| SBX-HUB-EU | 10.22.176.0/23 | EU Firewall (10.22.176.68) |
| SBX-SPK1-EU1 | 10.22.178.0/23 | EU Firewall (10.22.176.68) |
| SBX-SPK1-EU2 | 10.22.180.0/22 | EU Firewall (10.22.176.68) |
| SBX-SPK1-EU3 | 10.22.184.0/21 | EU Firewall (10.22.176.68) |

Configuration: Propagate Gateway Routes - Yes

Below are the routes for route table, *Route-SBX-HUB-EU-AzureFirewallSubnet*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-HUB-EU-Network resource group. The Azure*FirewallSubnet* is associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-HUB-EU- AzureFirewallSubnet | | |
| Name | **Address Prefix** | **Next Hop** |
| SBX-HUB-US | 10.22.160.0/23 | US Firewall (10.22.160.68) |
| SBX-SPK1-US1 | 10.22.162.0/23 | US Firewall (10.22.160.68) |
| SBX-SPK1-US2 | 10.22.164.0/22 | US Firewall (10.22.160.68) |
| SBX-SPK1-US3 | 10.22.168.0/21 | US Firewall (10.22.160.68) |

Configuration: Propagate Gateway Routes - Yes

#### AzureBastionSubnet

As per the Microsoft documentation, Azure Bastion services do not allow for the subnet to have a route table associated with it. This subnet does not have any associated route table in the US or EU regions.

#### SharedServicesSubnet

Below are the routes for route table, *Route-SBX-HUB-US-SharedServicesSubnet*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-HUB-US-Network resource group. The *SharedServicesSubnet* is associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-HUB-US- SharedServicesSubnet | | |
| Name | **Address Prefix** | **Next Hop** |
| Internet | 0.0.0.0/0 | US Firewall (10.22.160.68) |
| SBX-HUB-US | 10.22.160.0/23 | US Firewall (10.22.160.68) |
| SBX-SPK1-US1 | 10.22.162.0/23 | US Firewall (10.22.160.68) |
| SBX-SPK1-US2 | 10.22.164.0/22 | US Firewall (10.22.160.68) |
| SBX-SPK1-US3 | 10.22.168.0/21 | US Firewall (10.22.160.68) |

Configuration: Propagate Gateway Routes - No

Below are the routes for route table, *Route-SBX-HUB-EU- SharedServicesSubnet*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-HUB-EU-Network resource group. The *SharedServicesSubnet* is associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-HUB-EU- SharedServicesSubnet | | |
| Name | **Address Prefix** | **Next Hop** |
| SBX-HUB-EU | 10.22.176.0/23 | EU Firewall (10.22.176.68) |
| SBX-SPK1-EU1 | 10.22.178.0/23 | EU Firewall (10.22.176.68) |
| SBX-SPK1-EU2 | 10.22.180.0/22 | EU Firewall (10.22.176.68) |
| SBX-SPK1-EU3 | 10.22.184.0/21 | EU Firewall (10.22.176.68) |

Configuration: Propagate Gateway Routes - No

#### AppGatewaySubnet

Below are the routes for route table, *Route-SBX-HUB-US-AppGatewaySubnet*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-HUB-US-Network resource group. The *AppGatewaySubnet* is associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-HUB-US-AppGatewaySubnet | | |
| Name | **Address Prefix** | **Next Hop** |
| Internet | 0.0.0.0/0 | Internet |
| On-Premises1 | 10.0.0.0/8 | US Firewall (10.22.160.68) |
| On-Premises2 | 172.16.0.0/12 | US Firewall (10.22.160.68) |
| On-Premises3 | 192.168.0.0/16 | US Firewall (10.22.160.68) |
| On-Premises4 | 147.108.0.0/16 | US Firewall (10.22.160.68) |
| On-Premises5 | 3.0.0.0/8 | US Firewall (10.22.160.68) |
| On-Premises6 | 151.95.0.0/18 | US Firewall (10.22.160.68) |

Configuration: Propagate Gateway Routes - No

Below are the routes for route table, *Route-SBX-HUB-EU- AppGatewaySubnet*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-HUB-EU-Network resource group. The *AppGatewaySubnet* is associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-HUB-EU-AppGatewaySubnet | | |
| Name | **Address Prefix** | **Next Hop** |
| Internet | 0.0.0.0/0 | Internet |
| On-Premises1 | 10.0.0.0/8 | EU Firewall (10.22.176.68) |
| On-Premises2 | 172.16.0.0/12 | EU Firewall (10.22.176.68) |
| On-Premises3 | 192.168.0.0/16 | EU Firewall (10.22.176.68) |
| On-Premises4 | 147.108.0.0/16 | EU Firewall (10.22.176.68) |
| On-Premises5 | 3.0.0.0/8 | EU Firewall (10.22.176.68) |
| On-Premises6 | 151.95.0.0/18 | EU Firewall (10.22.176.68) |

Configuration: Propagate Gateway Routes - No

### Spoke Route Tables

#### FrontEndSubnet & BackEndSubnet

Below are the routes for route table, *Route-SBX-SPK-US*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-SPK-US-Network resource group. The *FrontEndSubnet* and *BackEndSubnet* are associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-SPK1-US | | |
| Name | **Address Prefix** | **Next Hop** |
| Internet | 0.0.0.0/0 | US Firewall (10.22.160.68) |
| SBX-HUB-US | 10.22.160.0/23 | US Firewall (10.22.160.68) |

Configuration: Propagate Gateway Routes - No

Below are the routes for route table, *Route-SBX-SPK-EU*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-SPK-EU-Network resource group. The *FrontEndSubnet* and *BackEndSubnet* are associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-SPK1-EU | | |
| Name | **Address Prefix** | **Next Hop** |
| Internet | 0.0.0.0/0 | EU Firewall (10.22.176.68) |
| SBX-HUB-EU | 10.22.176.0/23 | EU Firewall (10.22.176.68) |

Configuration: Propagate Gateway Routes - No

#### AppGatewaySubnet

Below are the routes for route table, *Route-SBX-SPK-US-AppGatewaySubnet*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-SPK-US-Network resource group. The *AppGatewaySubnet* are associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-SPK1-US-AppGatewaySubnet | | |
| Name | **Address Prefix** | **Next Hop** |
| Internet | 0.0.0.0/0 | Internet |
| On-Premises1 | 10.0.0.0/8 | US Firewall (10.22.160.68) |
| On-Premises2 | 172.16.0.0/12 | US Firewall (10.22.160.68) |
| On-Premises3 | 192.168.0.0/16 | US Firewall (10.22.160.68) |
| On-Premises4 | 147.108.0.0/16 | US Firewall (10.22.160.68) |
| On-Premises5 | 3.0.0.0/8 | US Firewall (10.22.160.68) |
| On-Premises6 | 151.95.0.0/18 | US Firewall (10.22.160.68) |
| SBX-HUB-US | 10.22.160.0/23 | US Firewall (10.22.160.68) |

Configuration: Propagate Gateway Routes - No

Below are the routes for route table, *Route-SBX-SPK-EU*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-SPK-EU-Network resource group. The *AppGatewaySubnet* are associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-SPK1-EU-AppGatewaySubnet | | |
| Name | **Address Prefix** | **Next Hop** |
| Internet | 0.0.0.0/0 | Internet |
| On-Premises1 | 10.0.0.0/8 | EU Firewall (10.22.176.68) |
| On-Premises2 | 172.16.0.0/12 | EU Firewall (10.22.176.68) |
| On-Premises3 | 192.168.0.0/16 | EU Firewall (10.22.176.68) |
| On-Premises4 | 147.108.0.0/16 | EU Firewall (10.22.176.68) |
| On-Premises5 | 3.0.0.0/8 | EU Firewall (10.22.176.68) |
| On-Premises6 | 151.95.0.0/18 | EU Firewall (10.22.176.68) |
| SBX-HUB-EU | 10.22.176.0/23 | EU Firewall (10.22.176.68) |

Configuration: Propagate Gateway Routes - No

#### SqlMISubnet

Below are the routes for route table, *Route-SBX-SPK-US-SqlMISubnet*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-SPK-US-Network resource group. The *SqlMISubnet* are associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-SPK1-US-SqlMI | | |
| Name | **Address Prefix** | **Next Hop** |
| Internet | 0.0.0.0/0 | US Firewall (10.22.160.68) |
| SBX-HUB-US | 10.22.160.0/23 | US Firewall (10.22.160.68) |

Configuration: Propagate Gateway Routes - No

Below are the routes for route table, *Route-SBX-SPK-EU- SqlMISubnet*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-SPK-EU-Network resource group. The *SqlMISubnet* are associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-SPK1-EU-SqlMI | | |
| Name | **Address Prefix** | **Next Hop** |
| Internet | 0.0.0.0/0 | EU Firewall (10.22.176.68) |
| SBX-HUB-EU | 10.22.176.0/23 | EU Firewall (10.22.176.68) |

Configuration: Propagate Gateway Routes - No

#### PrivateLinkSubnet

Below are the routes for route table, *Route-SBX-SPK-US-PrivateLinkSubnet*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-SPK-US-Network resource group. The *PrivateLinkSubnet* is associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-SPK1-US-PrivateLinkSubnet | | |
| Name | **Address Prefix** | **Next Hop** |
| Internet | 0.0.0.0/0 | US Firewall (10.22.160.68) |
| SBX-HUB-US | 10.22.160.0/23 | US Firewall (10.22.160.68) |

Configuration: Propagate Gateway Routes - No

Below are the routes for route table, *Route-SBX-SPK-EU-PrivateLinkSubnet*. All the routes direct traffic directly to the Azure Firewall virtual appliance. This resource is located within the RG-SBX-SPK-EU-Network resource group. The *PrivateLinkSubnet* associated with it.

|  |  |  |
| --- | --- | --- |
| Route-SBX-SPK1-EU-PrivateLinkSubnet | | |
| Name | **Address Prefix** | **Next Hop** |
| Internet | 0.0.0.0/0 | EU Firewall (10.22.176.68) |
| SBX-HUB-EU | 10.22.176.0/23 | EU Firewall (10.22.176.68) |

Configuration: Propagate Gateway Routes - No

### Security

## Network Security Groups

Internal network security will be controlled by network security groups (NSG). These will be attached to all subnets and restrict which ports are able to connect with other subnets. The exception would be subnets that are restricted from having an NSG attached, Azure Firewall and Gateway.

Flow logs are enabled for each NSG which captures when traffic is allowed or denied through the rules. For a full list of the rules, refer to the Azure DevOps repository. Below is a high level description of the allowed rules for each subnet

### Hub Networks

#### GatewaySubnet

There is no NSG associated with this subnet since it holds the network gateways

#### AzureFirewallSubnet

There is no NSG associated with this subnet since it holds the Azure Firewall.

#### AzureBastionSubnet

This network security group contains the rules that are defined based on the [Microsoft documentation](https://docs.microsoft.com/en-us/azure/bastion/bastion-nsg#apply)

#### SharedServicesSubnet

This network security group has the default inbound rules and a single outbound rule to separate out Azure Cloud traffic in the logs.

#### AppGatewaySubnet

The rules on this subnet allow the gateway health checks, allow inbound traffic on ports 80 & 443, and denies all other inbound traffic. Outbound, nothing is blocked, allowing the gateway to communicate to the necessary servers.

### Spoke Networks

#### FrontEndSubnet

The inbound rules allow traffic from Jumphosts, Azure Bastion, App Gateways, and other health checks. Outbound is the default rules.

#### BackEndSubnet

The inbound rules allow traffic from the FrontEndSubnet, Azure Bastion, Jumphosts, and other health checks. Outbound is the default rules.

#### AppGatewaySubnet

The rules on this subnet allow the gateway health checks, allow inbound traffic on ports 80 & 443, and denies all other inbound traffic. Outbound, nothing is blocked, allowing the gateway to communicate to the necessary servers.

#### SqlMISubnet

The inbound rules allow traffic from the FrontEndSubnet, Azure Bastion, Jumphosts, and other health checks. Outbound is the default rules. Additionally, once a managed instance is added, specific rules will be added based on the resource’s needs.

#### PrivateLinkSubnet

The inbound rules allow traffic from the FrontEndSubnet, Azure Bastion, Jumphosts, and other health checks. Outbound is the default rules. Additionally, once a managed instance is added, specific rules will be added based on the resource’s needs.

## Firewall

Azure Firewall will be used as the edge security for this environment. Each region will have a premium firewall that inherits its rules from a dedicated firewall policy. The policy will contain network rules, application rules, and SNAT rules. Each of those rulesets are documented in the following tables.

For more information about general Baker Hughes Azure Firewall design, please review the Firewall Design Document as the configuration will mirror the production environment.

### Network Rules

#### Service Tags

Service Tags allow connectivity from the Azure address space to any Azure resources.



#### Network Deny Rules

Network Deny Rules block traffic from one spoke to the other.



#### Network Allow Rules

Network Allow Rules allow traffic from Azure to the on-premises address spaces that were provided by Baker Hughes.

### Application Rules

#### Web Categories

Web Categories filter internet traffic based on host Microsoft categorizes the traffic.



#### FQDN Rules

FQDN Rules allow traffic on an individual website basis. If a website is needed that is not included in the categories above, it can be added here.



### SNAT Rules

To allow routing between Azure and On-Premises, the default internal addresses had to be updated to include those that Baker Hughes is already using. These include those defined in the [On-Premises Ranges](#_On-Premises_Ranges) section above.

BH Non-Routable CIDR list Link

[EXT V-net List.xlsx](https://bakerhughes.sharepoint.com/:x:/r/sites/BHAzureHome/Shared%20Documents/Non%20Routable%20CIDR/EXT%20V-net%20List.xlsx?d=wa98f09a004a1471e94112455a15b274a&csf=1&web=1&e=9uEu7p)