# Azure Environment Summary for Subscription: 14568c6d-0c6a-4128-810e-83b0d94859ee

*Report generated on: 2025-05-11 14:34:01 UTC*

This report provides an AI-generated summary and a curated list of core resource details for Azure resources, grouped by common categories, based on data retrieved via Azure Resource Graph.

## Compute Overview

**AI-Generated Analysis:**

Your Azure environment, specifically within the ‘Compute Overview’ category, primarily consists of Virtual Machines (VMs) with a single App Service Plan supporting a web application. These resources are consistently deployed in the westus2 region and adhere to a structured naming convention, such as BSIS-PROD-<ROLE>-<ID>, which aids in identifying their purpose (e.g., Domain Controllers, SQL Servers, Web Servers). The VMs support a mix of operating systems: Windows Server 2022 (Datacenter and Datacenter Azure editions) for Active Directory, SQL databases, and various application/utility servers, and multiple versions of Linux (Ubuntu LTS) for jump boxes, security tooling, and the “BigSIS V2” web tier. The deployment pattern for critical services includes redundancy, exemplified by dual Domain Controllers, a paired SQL Server VM configuration, and multiple web server instances for both “BigSIS V1” and “V2” applications, indicating an architecture designed for high availability.

Several key configuration choices are evident across your compute resources. VM sizes vary, ranging from burstable B-series (e.g., Standard\_B2as\_v2 for a Domain Controller, Standard\_B8as\_v2 for SQL VMs) to general-purpose D-series (e.g., Standard\_D2ads\_v5 for a Domain Controller) and memory-optimized E-series (e.g., Standard\_E4as\_v5 for V1 web servers), reflecting tailored resource allocation for different workloads. Storage for OS disks predominantly utilizes Premium\_LRS (Locally Redundant Storage), providing SSD performance, with some exceptions using StandardSSD\_LRS. Notably, the SQL VMs (BSIS-PROD-DB01A, BSIS-PROD-DB01B) employ Premium\_ZRS (Zone-Redundant Storage) for their data, log, tempdb, and quorum disks, enhancing data durability across availability zones. These SQL VMs also leverage TrustedLaunch capabilities (Secure Boot and vTPM), improving boot integrity. Most VMs have EncryptionAtHost enabled, providing an additional layer of data encryption. Patch management is generally configured to AutomaticByPlatform. The BSIS-PROD-LoginWebApp-Plan is a Linux-based App Service Plan on a Small worker size in Dedicated compute mode, currently not configured for zone redundancy. A pattern of using SSH key-based authentication for Linux VMs is observed, enhancing security by disabling password authentication.

From a security and optimization perspective, several points arise. The consistent use of EncryptionAtHost and TrustedLaunch for SQL VMs demonstrates a strong security posture. However, the BSIS-PROD-QUALYS1 VM, intended for security scanning, is in a Failed provisioning state and is an older Gen1 VM, which presents a gap in security tooling and should be remediated. While tags like Environment and Product are well-utilized, governance tags such as Owner and Technical\_Owner are consistently empty; populating these would improve accountability and resource management. For optimization, the mixed VM SKUs within functionally similar groups (e.g., BSIS-V1-WEB servers using Standard\_E4as\_v5, Standard\_B8as\_v2, and Standard\_E4as\_v4) suggest an opportunity for rightsizing by analyzing performance metrics to standardize on the most cost-effective SKU. The SQL VMs utilizing B-series (Standard\_B8as\_v2) should be monitored for sustained performance, as burstable instances might not be ideal for all production database workloads. The entire compute footprint resides in westus2 with no evidence of inter-region disaster recovery mechanisms in this dataset; this is a critical consideration for business continuity. The App Service Plan BSIS-PROD-LoginWebApp-Plan lacks zone redundancy, which should be enabled for production login services to improve availability. Finally, inconsistencies exist, such as differing VM SKUs for the two Domain Controllers (Standard\_D2ads\_v5 vs. Standard\_B2as\_v2) and differing OS disk types and encryption status for TeamCity build agents (BSIS-PROD-BLD1 vs. BSIS-PROD-BLD2), which should be standardized for operational consistency.

**Core Resource Details for Compute Overview:**

| name | resourceType | location | resourceGroup |
| --- | --- | --- | --- |
| BSIS-PROD-DC01 | Virtual Machine | westus2 | bsis-prod-ad |
| BSIS-PROD-DC02 | Virtual Machine | westus2 | bsis-prod-ad |
| BSIS-PROD-JUMP | Virtual Machine | westus2 | bsis-prod-jump |
| BSIS-PROD-LoginWebApp-Plan | App Service Plan | westus2 | bsis-prod-loginwebapp |
| BSIS-PROD-DPA01 | Virtual Machine | westus2 | bsis-prod-monitoring |
| BSIS-PROD-QUALYS1 | Virtual Machine | westus2 | bsis-prod-qualys |
| BSIS-PROD-DB01A | Virtual Machine | westus2 | bsis-prod-sql-clusters |
| BSIS-PROD-DB01B | Virtual Machine | westus2 | bsis-prod-sql-clusters |
| BSIS-PROD-BLD1 | Virtual Machine | westus2 | bsis-prod-teamcity |
| BSIS-PROD-BLD2 | Virtual Machine | westus2 | bsis-prod-teamcity |
| BSIS-PROD-TC01 | Virtual Machine | westus2 | bsis-prod-teamcity |
| BSIS-PROD-TENABLE | Virtual Machine | westus2 | bsis-prod-tenable |
| BSIS-V1-WEB01 | Virtual Machine | westus2 | bsis-prod-v1-web |
| BSIS-V1-WEB02 | Virtual Machine | westus2 | bsis-prod-v1-web |
| BSIS-V1-WEB03 | Virtual Machine | westus2 | bsis-prod-v1-web |
| BSIS-V1-WEB04 | Virtual Machine | westus2 | bsis-prod-v1-web |
| BSIS-V1-WEB05 | Virtual Machine | westus2 | bsis-prod-v1-web |
| BSIS-V1-WEB06 | Virtual Machine | westus2 | bsis-prod-v1-web |
| BSIS-V2-WEB01 | Virtual Machine | westus2 | bsis-prod-v2-web |
| BSIS-V2-WEB02 | Virtual Machine | westus2 | bsis-prod-v2-web |
| BSIS-V1-CONF1 | Virtual Machine | westus2 | bsis-v1-prod-configtool |
| BSIS-PROD-WSUS1 | Virtual Machine | westus2 | enp-bsis-prod-coreresources |

## App Platform & Containers

**AI-Generated Analysis:**

Your App Platform & Containers environment currently consists of Azure Container Instances and Azure App Services deployed to support the “BigSIS” application. Specifically, there is a container instance named bsis-prod-prometheus and a web application BSIS-V1-RSM-Login-VS hosted on an App Service Plan BSIS-PROD-LoginWebApp-Plan. All these resources are consistently located in the westus2 region and tagged for a “Production” environment, serving the “K12” vertical under the “BigSIS” brand. The deployment includes one Linux-based container instance and one Linux-based App Service running a .NET Core 8.0 application.

Examining the configurations, the bsis-prod-prometheus container instance is configured with a single Linux container, a User-Assigned Managed Identity, an Always restart policy, and critically, a private IP address. This private IP configuration indicates it functions as an internal service, likely for monitoring, and is not directly exposed to the internet. The BSIS-PROD-LoginWebApp-Plan is a Basic B1 SKU App Service Plan, operating on Linux with a capacity of a single instance. The associated web application, BSIS-V1-RSM-Login-VS (identified by its hostname login.ravenna-student.com), utilizes a System-Assigned Managed Identity, enforces HTTPS Only, and has Client Affinity disabled, which is optimal for stateless, scalable applications. This login application has Public Network Access enabled. A pattern of consistent tagging for “Environment”, “Product”, “Vertical”, and “Brand” is observed, though key ownership tags remain unpopulated.

From a security and optimization perspective, the private IP for the bsis-prod-prometheus container instance is a sound security choice. The BSIS-V1-RSM-Login-VS web app’s enforcement of HTTPS Only is also a security best practice. However, its Public Network Access being enabled, while necessary for a login portal, highlights the need for robust protection, typically via a Web Application Firewall, which is not detailed within this specific resource set. The Basic B1 SKU with a single instance for the BSIS-PROD-LoginWebApp-Plan presents a significant availability risk for a “Production” login service, as this SKU offers no SLA and lacks high-availability features or support for Availability Zones. For enhanced resilience and performance, an upgrade to a Standard or Premium tier App Service Plan is essential to enable auto-scaling and provide an SLA. Furthermore, all resources are confined to the westus2 region, lacking any geo-redundancy or disaster recovery provisions for the login application. The consistently empty “Owner”, “Infrastructure\_Owner”, and “Technical\_Owner” tags represent a governance gap that should be addressed to improve accountability and resource management.

**Core Resource Details for App Platform & Containers:**

| name | location | type | kind | appState | aspTier | aspSkuName | kubernetesVersion | containerImage |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| bsis-prod-prometheus | westus2 | microsoft.containerinstance/containergroups |  |  |  |  |  |  |
| BSIS-PROD-LoginWebApp-Plan | westus2 | microsoft.web/serverfarms | linux |  | Basic | B1 |  |  |
| BSIS-V1-RSM-Login-VS | westus2 | microsoft.web/sites | app,linux | Running |  |  |  |  |

## Storage Solutions

**AI-Generated Analysis:**

Your environment’s storage solutions primarily consist of Azure Storage Accounts, specifically the StorageV2 (General Purpose v2) kind, with one exception being an older Storage (General Purpose v1) account. These accounts are all deployed within the westus2 region. The deployment pattern shows a mix of data redundancy strategies: some accounts utilize Standard\_LRS (Locally-Redundant Storage) for scenarios like configuration backups and Prometheus data, while others, particularly those storing application data, TeamCity artifacts, and SQL backups, leverage Standard\_RAGRS (Read-Access Geo-Redundant Storage), providing an additional layer of data durability with a secondary location in westcentralus. All accounts are configured to use the Hot access tier, suitable for frequently accessed data.

Several key configurations define your storage posture. All storage accounts enforce supportsHttpsTrafficOnly: True and allowBlobPublicAccess: False, coupled with a minimumTlsVersion: TLS1\_2. This establishes a strong baseline for data in transit and at rest security by preventing unencrypted connections and anonymous public access. A distinction in network access configuration is observed: while most accounts have networkDefaultAction: Deny, restricting public network access by default, the bigsisv1prodstoragevs, bigsisv2prodstoragevs, and the migrate14568lsa28936 accounts are configured with networkDefaultAction: Allow. This implies that these specific accounts permit access from all networks by default, unless further restricted by firewall rules. The naming convention generally includes product identifiers (bigsisv1, bigsisv2) and purpose (e.g., configsvs, teamcityvs, prodstoragevs), suggesting an organized approach to resource identification. Tagging is consistently applied with keys like “Environment”, “Product”, “Brand”, and “Vertical”, although specific owner-related tag values are uniformly empty.

From a security and compliance perspective, the storage accounts with networkDefaultAction: Allow (bigsisv1prodstoragevs, bigsisv2prodstoragevs, and migrate14568lsa28936) warrant immediate review. Exposing storage accounts to all public networks by default increases the attack surface; these should be transitioned to networkDefaultAction: Deny and access should be managed via private endpoints, service endpoints, or tightly controlled firewall rules. While tags are present, the consistent emptiness of “Owner”, “Infrastructure\_Owner”, and “Technical\_Owner” fields hinders governance and accountability. Populating these tags is crucial for effective resource management and incident response. The migrate14568lsa28936 account, being of the older Storage kind, should be upgraded to StorageV2 to benefit from modern features, potentially better pricing, and improved performance characteristics.

For optimization, evaluate the redundancy choice for bigsisconfigsvcvs (V1 website asset and config backups) and bsisprodprometheusvs. While Standard\_LRS is cost-effective, if this data is critical for business continuity or disaster recovery, upgrading to Standard\_GRS or Standard\_RAGRS would provide enhanced data protection against regional outages. Although RAGRS is used for several key accounts, a comprehensive disaster recovery strategy involves more than just data redundancy; application and service failover to the secondary region (westcentralus) should also be planned and tested. Finally, while all data is currently in the Hot access tier, a lifecycle management policy could be implemented to transition older, less frequently accessed data (e.g., historical backups in bsisprodsqlclubackupvs or older artifacts in bigsisteamcityvs) to Cool or Archive tiers to optimize storage costs.

**Core Resource Details for Storage Solutions:**

| name | location | kind | storageSkuName | storageSkuTier | allowBlobPublicAccess | isHnsEnabled | provisioningState |
| --- | --- | --- | --- | --- | --- | --- | --- |
| bigsisconfigsvcvs | westus2 | StorageV2 | Standard\_LRS | Standard | False |  | Succeeded |
| bigsisteamcityvs | westus2 | StorageV2 | Standard\_RAGRS | Standard | False |  | Succeeded |
| bigsisv1prodstoragevs | westus2 | StorageV2 | Standard\_RAGRS | Standard | False |  | Succeeded |
| bigsisv2demostoragevs | westus2 | StorageV2 | Standard\_RAGRS | Standard | False |  | Succeeded |
| bigsisv2prodstoragevs | westus2 | StorageV2 | Standard\_RAGRS | Standard | False |  | Succeeded |
| bsisprodprometheusvs | westus2 | StorageV2 | Standard\_LRS | Standard | False |  | Succeeded |
| bsisprodsqlclubackupvs | westus2 | StorageV2 | Standard\_RAGRS | Standard | False |  | Succeeded |
| bsisprodstoragevs | westus2 | StorageV2 | Standard\_LRS | Standard | False |  | Succeeded |
| migrate14568lsa28936 | westus2 | Storage | Standard\_LRS | Standard | False |  | Succeeded |

## Networking & Connectivity

**AI-Generated Analysis:**

Your Azure networking and connectivity environment is established with a clear focus on supporting your “BigSIS” application, with distinct configurations for V1 and V2 product versions. The core components include Application Gateways for web traffic management, an Azure Firewall for network security, Standard Load Balancers for specific internal services, a comprehensive set of Network Security Groups for granular traffic filtering, and an extensive deployment of Private Endpoints to secure communication to PaaS services. All these resources are currently located in the westus2 region, indicating a single-region deployment strategy. The overall configuration shows a production environment (BSIS-PROD-\* naming convention) that utilizes multiple Virtual Networks with custom DNS, and User Defined Routes for traffic control, suggesting a hub-spoke or similar segmented network architecture.

Several key configuration choices and patterns are evident across your networking resources. Your Application Gateways (BSIS-PROD-V1-AppGw01, BSIS-PROD-V1-AppGw02, BSIS-PROD-V2-AppGw01) are all running with HTTP/2 enabled and a single frontend IP, though specific SKU details or Web Application Firewall (WAF) status are not provided in this data. The central BSIS-PROD-FW01 Azure Firewall is operating with Threat Intelligence in “Alert” mode. Your Load Balancers (BSIS-PROD-TeamCity, BSIS-PROD-WSUS) are Standard SKU, facilitating Private Link services for TeamCity and WSUS connectivity. It is important to note that the properties listed for these load balancers, such as appGwSku, firewallTier, and gatewaySku, are not standard attributes of Azure Load Balancers and likely represent a data reporting anomaly. Network Security Groups are extensively used, with rule counts ranging from 6 to 16, tailored for specific services such as Active Directory, SQL Clusters, and web tiers. The widespread adoption of Private Endpoints for services like Key Vaults, Storage Accounts, and DocumentDB (e.g., BSIS-PROD-V1-Live-KV-endpoint, bigsisv1prodstorage-endpoint) underscores a commitment to securing PaaS data by keeping traffic within your virtual network. All Public IP addresses are configured with Static allocation and Standard SKU. Your Route Tables consistently have BGP route propagation disabled, enforcing User Defined Routes, and your BSIS-PROD-Client-VPN Virtual Network Gateway is a RouteBased VPN, not configured for active-active high availability. The environment uses three main Virtual Networks (BSIS-PROD-V1-VNET-WUS2, BSIS-PROD-V2-VNET-WUS2, BSIS-PROD-VNET-WUS2), each with a consistent custom DNS server (10.183.1.4), and none currently have Azure DDoS Protection Standard enabled.

From a security and optimization perspective, several aspects warrant attention. The presence of ten Static Public IP addresses (e.g., BSIS-PROD-FW01-PUBIP, BSIS-PROD-V1-AppGw01-PUBIP) necessitates rigorous management to minimize the attack surface; ensuring robust NSG rules and WAF policies (if App Gateways are WAF-enabled) is critical. The Azure Firewall’s Threat Intelligence mode set to “Alert” provides visibility but does not actively block identified threats; upgrading to “AlertDeny” or “Deny” for your production firewall would enhance your security posture. The lack of Azure DDoS Protection Standard enabled on your Virtual Networks (ddosProtectionEnabled: False) is a significant security gap for any public-facing services. While tagging is generally good, several key tags like “Owner” and “Technical\_Owner” are consistently empty, which impacts governance. There are also inconsistencies in tagging, such as the BSIS-DEV-JUMP-PUBIP being tagged with "Environment": "Production", and both Private Endpoints named BSIS-PROD-V2-Keyvault-endpoint (one linking to BSIS-DEMO-V2-KV, another to BSIS-PROD-V2-KV) are tagged with "Environment": "Demo", which can lead to operational confusion. The NSG named nic-BSIS-PROD-DC01-00-test-nsg also presents a naming conflict for a production resource. For optimization, the BSIS-PROD-Client-VPN gateway (gatewayActiveActive: False) is a single point of failure for client VPN access; evaluating a highly available SKU or configuration is advisable. The single-region deployment in westus2 presents a business continuity risk; exploring a multi-region architecture should be a priority. Finally, NSGs with specific, potentially temporary purposes like BSIS-PROD-DARA-nsg (“DARA internal pen testing Dec 2023”) should be reviewed to ensure rules are still necessary and adhere to the principle of least privilege.

**Core Resource Details for Networking & Connectivity:**

| name | location | type | kind | provisioningState | vnetAddressPrefixes | lbSku | appGwSku | firewallTier | gatewayType | dnsZoneType | publicIpAddress |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BSIS-PROD-V1-AppGw01 | westus2 | microsoft.network/applicationgateways |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-V1-AppGw02 | westus2 | microsoft.network/applicationgateways |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-V2-AppGw01 | westus2 | microsoft.network/applicationgateways |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-FW01 | westus2 | microsoft.network/azurefirewalls |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-TeamCity | westus2 | microsoft.network/loadbalancers |  | Succeeded |  | Standard | Standard | Regional |  |  |  |
| BSIS-PROD-WSUS | westus2 | microsoft.network/loadbalancers |  | Succeeded |  | Standard | Standard | Regional |  |  |  |
| BSIS-PROD-AD-NSG | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-BUILD-nsg | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-DARA-nsg | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-DBG-nsg | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-DPA-nsg | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-JUMP-nsg | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-QUALYS1-Nsg-b398 | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-SQL-Clusters-NSG | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-TENABLE-nsg | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-TeamCity | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-V1-Web-NSG | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-V2-Web-NSG | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-WSUS-nsg | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-V1-CONF1-nsg | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSISPRODDARAnsg549 | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| nic-BSIS-PROD-DC01-00-test-nsg | westus2 | microsoft.network/networksecuritygroups |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-DEMO-V2-Keyvault-endpoint | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-SqlClusterBackups-Private-Endpoint-nic | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-V1-Live-KV-endpoint | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-V1-Test-KV-endpoint | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-V2-Keyvault-endpoint | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| bigsis-v1-provisioing-kv-endpoint | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| bigsisconfigservice-endpoint | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| bigsisteamcity-endpoint | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| bigsisv1prodstorage-endpoint | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| bigsisv2demostorage-endpoint | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| bigsisv2demostorage-files-endpoint | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| bigsisv2prodstorage-endpoint | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| bigsisv2prodstorage-files-endpoint | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| bsis-v1-provisioning-db-endpoint | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| bsis-v2-es01-privatelink | westus2 | microsoft.network/privateendpoints |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-DEV-JUMP-PUBIP | westus2 | microsoft.network/publicipaddresses |  | Succeeded |  | Standard | Standard | Regional |  |  | 52.148.128.212 |
| BSIS-PROD-Client-VPN-PUBIP | westus2 | microsoft.network/publicipaddresses |  | Succeeded |  | Standard | Standard | Regional |  |  | 13.66.220.0 |
| BSIS-PROD-DARA-PUBIP | westus2 | microsoft.network/publicipaddresses |  | Succeeded |  | Standard | Standard | Regional |  |  | 52.250.85.245 |
| BSIS-PROD-FW01-PUBIP | westus2 | microsoft.network/publicipaddresses |  | Succeeded |  | Standard | Standard | Regional |  |  | 172.179.49.150 |
| BSIS-PROD-JUMP-PUBIP | westus2 | microsoft.network/publicipaddresses |  | Succeeded |  | Standard | Standard | Regional |  |  | 52.148.162.226 |
| BSIS-PROD-NAT01-PUBIP | westus2 | microsoft.network/publicipaddresses |  | Succeeded |  | Standard | Standard | Regional |  |  | 13.66.211.138 |
| BSIS-PROD-Prometheus-PUBIP | westus2 | microsoft.network/publicipaddresses |  | Succeeded |  | Standard | Standard | Regional |  |  | 52.149.30.169 |
| BSIS-PROD-V1-AppGw01-PUBIP | westus2 | microsoft.network/publicipaddresses |  | Succeeded |  | Standard | Standard | Regional |  |  | 52.156.103.169 |
| BSIS-PROD-V1-AppGw02-PUBIP | westus2 | microsoft.network/publicipaddresses |  | Succeeded |  | Standard | Standard | Regional |  |  | 4.242.97.158 |
| BSIS-PROD-V2-AppGw01-PUBIP | westus2 | microsoft.network/publicipaddresses |  | Succeeded |  | Standard | Standard | Regional |  |  | 4.149.67.217 |
| BSIS-PROD-V1-Routes | westus2 | microsoft.network/routetables |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-V2-Routes | westus2 | microsoft.network/routetables |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-VNET-AD-ROUTES | westus2 | microsoft.network/routetables |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-VNET-APPGATEWAY-ROUTES | westus2 | microsoft.network/routetables |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-VNET-DEFAULT-ROUTES | westus2 | microsoft.network/routetables |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-VNET-GATEWAY-ROUTES | westus2 | microsoft.network/routetables |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-VNET-SQL-ROUTES | westus2 | microsoft.network/routetables |  | Succeeded |  |  |  |  |  |  |  |
| BSIS-PROD-Client-VPN | westus2 | microsoft.network/virtualnetworkgateways |  | Succeeded |  |  |  |  | Vpn |  |  |
| BSIS-PROD-V1-VNET-WUS2 | westus2 | microsoft.network/virtualnetworks |  | Succeeded | ["10.184.0.0/22"] |  |  |  |  |  |  |
| BSIS-PROD-V2-VNET-WUS2 | westus2 | microsoft.network/virtualnetworks |  | Succeeded | ["10.185.0.0/22"] |  |  |  |  |  |  |
| BSIS-PROD-VNET-WUS2 | westus2 | microsoft.network/virtualnetworks |  | Succeeded | ["10.183.0.0/20"] |  |  |  |  |  |  |

## Database Services

**AI-Generated Analysis:**

Your database services environment currently includes a single Azure Cosmos DB account, identified as bigsis-v1-provisioning-db-vs. This database is configured as a GlobalDocumentDB kind, utilizing the Core (SQL) API, as indicated by the defaultExperience tag. It operates on the Standard offer type and is provisioned in the westus2 region. The current deployment consists of a single write region and a single read region, both located in westus2, indicating a single-region operational footprint for data processing and access.

Several key configurations define this Cosmos DB account. It is explicitly tagged for a “Production” environment and associated with the “BigSIS V1” product, providing clear governance context. Network access is configured with cosmosPublicNetworkAccess: Enabled, meaning the database endpoint is accessible over the public internet. Additionally, the redisPublicNetworkAccess: Enabled property suggests that if an integrated cache feature is utilized with this Cosmos DB account, its endpoint is also publicly accessible. A critical choice is the Strong consistency level, which ensures that all reads receive the most up-to-date version of the data, a common requirement for systems needing absolute data integrity. The naming convention bigsis-v1-provisioning-db-vs suggests this database serves a specific provisioning function for the “BigSIS V1” application.

From a security perspective, the cosmosPublicNetworkAccess: Enabled configuration warrants careful review. While access is controlled by keys or Azure AD authentication, exposing database endpoints directly to the public internet increases the attack surface. For production environments, utilizing Azure Private Link to restrict access to your virtual network is the recommended best practice. While essential tags like “Environment” and “Product” are present, fields such as “Owner” and “Technical\_Owner” are empty, which could be improved for better accountability and resource management. For optimization, the single-region deployment in westus2 (one write and one read location) means that high availability is limited to Azure’s intra-regional capabilities (e.g., Availability Zones, if utilized by the service backend) but does not provide inherent geo-redundancy for disaster recovery. Although the GlobalDocumentDB kind supports multi-region distribution, it is not currently leveraged. Furthermore, the Strong consistency level, while ensuring maximum data consistency, incurs the highest latency and RU cost for operations. You should evaluate if this strict consistency is essential for all aspects of the “BigSIS V1” provisioning workload, as a more relaxed consistency level (e.g., Bounded Staleness) could offer performance and cost benefits if appropriate for the application’s requirements.

**Core Resource Details for Database Services:**

| name | location | type | kind | status | sqlTier | dbComputeTier | redisSkuName | cosmosConsistencyLevel | dbHighAvailability |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| bigsis-v1-provisioning-db-vs | westus2 | microsoft.documentdb/databaseaccounts | GlobalDocumentDB |  |  |  |  | Strong |  |

## Analytics & AI/ML Platforms

**AI-Generated Analysis:**

No Azure resources were found (or query failed) in the ‘Analytics & AI/ML Platforms’ category for the subscription ‘14568c6d-0c6a-4128-810e-83b0d94859ee’.

## Identity & Security Posture

**AI-Generated Analysis:**

Your Identity & Security Posture is primarily composed of Azure Monitor alerts and Azure Key Vaults, which are configured to support your “BigSIS” applications, including specific versions “V1” and “V2”. The Azure Monitor alerts are globally deployed and consistently tagged for the “Production” environment, focusing on the health and performance of Application Gateways. These include alerts for general service unavailability, unhealthy host counts in Application Gateway backend pools for both BigSIS V1 and V2, and alerts for high rates of failed requests on specific Application Gateway instances. Your Azure Key Vaults are all centralized in the westus2 region, serving distinct purposes such as certificate storage for firewall TLS inspection, Application Gateway certificates, secrets for live and test production sites, and provisioning. These vaults are tagged to differentiate between “Production” and “Demo” environments and various “BigSIS” product versions.

Several key configuration choices and patterns are evident in your setup. All Azure Key Vaults benefit from SoftDelete and PurgeProtection being enabled, which is a critical data protection best practice for secret management. There is a notable inconsistency in Key Vault access control models: some vaults, like BSIS-DEMO-V2-KV and BSIS-PROD-V1-Live-VS-KV, leverage Azure Role-Based Access Control (keyVaultEnableRbac: True), while others, such as BSIS-PROD-CCACERTS-KV and BSIS-PROD-WEB-CERTS-KV, utilize the older Access Policy model (keyVaultEnableRbac: False). Regarding network access, the production Key Vaults BSIS-PROD-V1-Live-VS-KV and BSIS-PROD-V1-Test-VS-KV correctly have public network access disabled, enhancing their security. However, other Key Vaults, including some designated for production purposes like BSIS-PROD-CCACERTS-KV (for Firewall CA certs) and BSIS-PROD-WEB-CERTS-KV (for App Gateway certs), currently permit public network access. Your monitoring strategy for Application Gateways employs both static thresholds for UnhealthyHostCount (triggering if even one host is problematic for 15 mins) and dynamic thresholds with “Low” sensitivity for FailedRequests, indicating a proactive approach to application availability and performance monitoring. The consistent keyVaultTenantId across all vaults simplifies identity management for these resources. Tagging is generally applied, with Brand: BigSIS and Vertical: K12 consistently used, although some ownership-related tags are unpopulated.

From a security and optimization perspective, several points warrant attention. The configuration of keyVaultPublicNetworkAccess: Enabled on production Key Vaults such as BSIS-PROD-CCACERTS-KV, BSIS-PROD-WEB-CERTS-KV, and bigsis-v1-provision-kv presents an increased security risk. Transitioning these to use private endpoints would significantly harden their security posture. Standardizing all Key Vaults to utilize Azure RBAC (keyVaultEnableRbac: True) instead of Access Policies will provide more granular, modern, and centrally manageable permission controls. Furthermore, the tagging information reveals some inconsistencies and gaps: for instance, BSIS-PROD-V2-KV is named “PROD” but tagged as “Demo,” which can lead to confusion in management and reporting. Similarly, BSIS-PROD-V1-Test-VS-KV is tagged as “Production” while its purpose is noted for “testing production sites.” Ensuring consistency between naming and tagging, and populating the empty Owner, Infrastructure\_Owner, Technical\_Owner, and platform-Group tags across all resources is crucial for effective governance, accountability, and cost management. These actions will enhance the overall security and operational efficiency of your identity and security resources.

**Core Resource Details for Identity & Security Posture:**

| name | location | type | kind | keyVaultSkuName | defenderPlanTier | alertEnabled | policyDisplayName |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Service Unavailable Health Alert | global | microsoft.insights/activitylogalerts |  |  |  | True |  |
| BSIS-PROD-V1-Group1-Pool-Health | global | microsoft.insights/metricalerts |  |  |  | True |  |
| BSIS-PROD-V1-Group2-Pool-Health | global | microsoft.insights/metricalerts |  |  |  | True |  |
| BSIS-PROD-V2-Pool-Health | global | microsoft.insights/metricalerts |  |  |  | True |  |
| Failed Request Alert - BSIS-PROD-V1-AppGw01 | global | microsoft.insights/metricalerts |  |  |  | True |  |
| Failed Request Alert - BSIS-PROD-V1-AppGw02 | global | microsoft.insights/metricalerts |  |  |  | True |  |
| Failed Request Alert - BSIS-PROD-V2-AppGw01 | global | microsoft.insights/metricalerts |  |  |  | True |  |
| BSIS-DEMO-V2-KV | westus2 | microsoft.keyvault/vaults |  |  |  |  |  |
| BSIS-PROD-CCACERTS-KV | westus2 | microsoft.keyvault/vaults |  |  |  |  |  |
| BSIS-PROD-V1-Live-VS-KV | westus2 | microsoft.keyvault/vaults |  |  |  |  |  |
| BSIS-PROD-V1-Test-VS-KV | westus2 | microsoft.keyvault/vaults |  |  |  |  |  |
| BSIS-PROD-V2-KV | westus2 | microsoft.keyvault/vaults |  |  |  |  |  |
| BSIS-PROD-WEB-CERTS-KV | westus2 | microsoft.keyvault/vaults |  |  |  |  |  |
| bigsis-v1-provision-kv | westus2 | microsoft.keyvault/vaults |  |  |  |  |  |

## Management & Governance

**AI-Generated Analysis:**

Your Azure environment’s Management & Governance resources are primarily concentrated in the westus2 region, encompassing Azure Automation, Application Insights, Log Analytics Workspaces, and a Recovery Services Vault. A consistent naming convention, BSIS-PROD-\*, is observed across most resources, clearly designating them for the “Production” environment and supporting the “BigSIS” product, including specific versions like “BigSIS V1” and “BigSIS V2”. Tagging is generally applied, identifying the environment and product, although some ownership-related tags such as “Owner” and “Technical\_Owner” are consistently unpopulated, which can impact accountability and streamlined governance.

Key configurations reveal a structured approach to logging and monitoring. The BSIS-PROD-Automation account leverages a SystemAssigned Managed Identity for secure, automated operations. The BSIS-PROD-V2-AppInsights-WUS2 Application Insights instance is configured for web applications and correctly utilizes Log Analytics workspace integration (appInsightsIngestionMode: LogAnalytics) by sending data to BSIS-PROD-V2-AppInsight-LAW-WUS2. Multiple Log Analytics workspaces are deployed: BSIS-PROD-Application-LogAnalytics (30-day retention), BSIS-PROD-Security-LogAnalytics-WUS2 (90-day retention, appropriate for security data), and version-specific workspaces for “BigSIS V1” (BSIS-PROD-V1-WebApp-LAW-WUS2) and “BigSIS V2” (BSIS-PROD-V2-AppInsight-LAW-WUS2), both with 30-day retention. Two workspaces named D4SQL-\* indicate the use of Microsoft Defender for SQL, with one of these workspaces having more complete production tags. All Log Analytics workspaces are configured with unlimited daily data ingestion quotas (logDailyQuotaGb: -1.0) and have public network access enabled for both ingestion and querying. The BSIS-PROD-BACKUP-VAULT Recovery Services Vault uses the RS0 SKU with Standard tier, configured for “VM Snapshot Backups,” and has specific Azure Monitor alerts enabled for replication issues, failover issues, and job failures.

From a security and compliance perspective, the consistent enabling of publicNetworkAccessLAIngestion and publicNetworkAccessLAQuery across all Log Analytics workspaces presents a configuration that warrants review; restricting access via private endpoints would enhance the security posture. The unpopulated “Owner,” “Infrastructure\_Owner,” and “Technical\_Owner” tags across all listed resources represent a gap in governance, potentially hindering clear accountability and operational management. A notable tagging inconsistency exists with defaultWorkspace-14568c6d-0c6a-4128-810e-83b0d94859ee-test, which, despite its name suggesting a test purpose, is tagged with "Environment": "Production"; this discrepancy should be rectified for accurate asset management and policy enforcement. Additionally, the D4SQL-14568c6d0c6a4128810e83b0d94859ee-westus2 workspace, created by Microsoft Defender for SQL, lacks standard environment and product tags, unlike its counterpart.

For optimization and improvement, while the segregation of Log Analytics workspaces facilitates targeted data analysis and role-based access control, the number of workspaces should be periodically reviewed to ensure it aligns with operational needs without creating undue management complexity. The BSIS-PROD-BACKUP-VAULT Recovery Services Vault, with its RS0 SKU, provides locally redundant storage for backups within westus2. No geo-redundant storage for backups is indicated by this SKU, which is a critical consideration for disaster recovery planning; your business continuity objectives should determine if an upgrade to a geo-redundant SKU is necessary. Furthermore, the alertsForCriticalOperations setting on the Recovery Services vault is “Disabled”; this should be reviewed to ensure that all critical backup and recovery operations trigger appropriate notifications. The presence of two D4SQL-\* workspaces also suggests an opportunity to verify if both are actively used and correctly configured, or if consolidation is possible.

**Core Resource Details for Management & Governance:**

| name | location | type | kind | provisioningState | logSkuName | appInsightsType | automationSkuName | backupVaultSkuName |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BSIS-PROD-Automation | westus2 | microsoft.automation/automationaccounts |  |  |  |  |  |  |
| BSIS-PROD-V2-AppInsights-WUS2 | westus2 | microsoft.insights/components | web | Succeeded |  | web |  |  |
| BSIS-PROD-Application-LogAnalytics | westus2 | microsoft.operationalinsights/workspaces |  | Succeeded |  |  |  |  |
| BSIS-PROD-Security-LogAnalytics-WUS2 | westus2 | microsoft.operationalinsights/workspaces |  | Succeeded |  |  |  |  |
| BSIS-PROD-V1-WebApp-LAW-WUS2 | westus2 | microsoft.operationalinsights/workspaces |  | Succeeded |  |  |  |  |
| BSIS-PROD-V2-AppInsight-LAW-WUS2 | westus2 | microsoft.operationalinsights/workspaces |  | Succeeded |  |  |  |  |
| D4SQL-14568c6d0c6a4128810e83b0d94859ee-westus2 | westus2 | microsoft.operationalinsights/workspaces |  | Succeeded |  |  |  |  |
| D4SQL-c2a3e82072d64da4b565d188e3f1f447-westus2 | westus2 | microsoft.operationalinsights/workspaces |  | Succeeded |  |  |  |  |
| defaultWorkspace-14568c6d-0c6a-4128-810e-83b0d94859ee-test | westus2 | microsoft.operationalinsights/workspaces |  | Succeeded |  |  |  |  |
| BSIS-PROD-BACKUP-VAULT | westus2 | microsoft.recoveryservices/vaults |  | Succeeded | RS0 |  | RS0 | RS0 |