



**"D:\dev\doc-
generator\data\metatron_infraestrutura\Infraestrutura.md"**

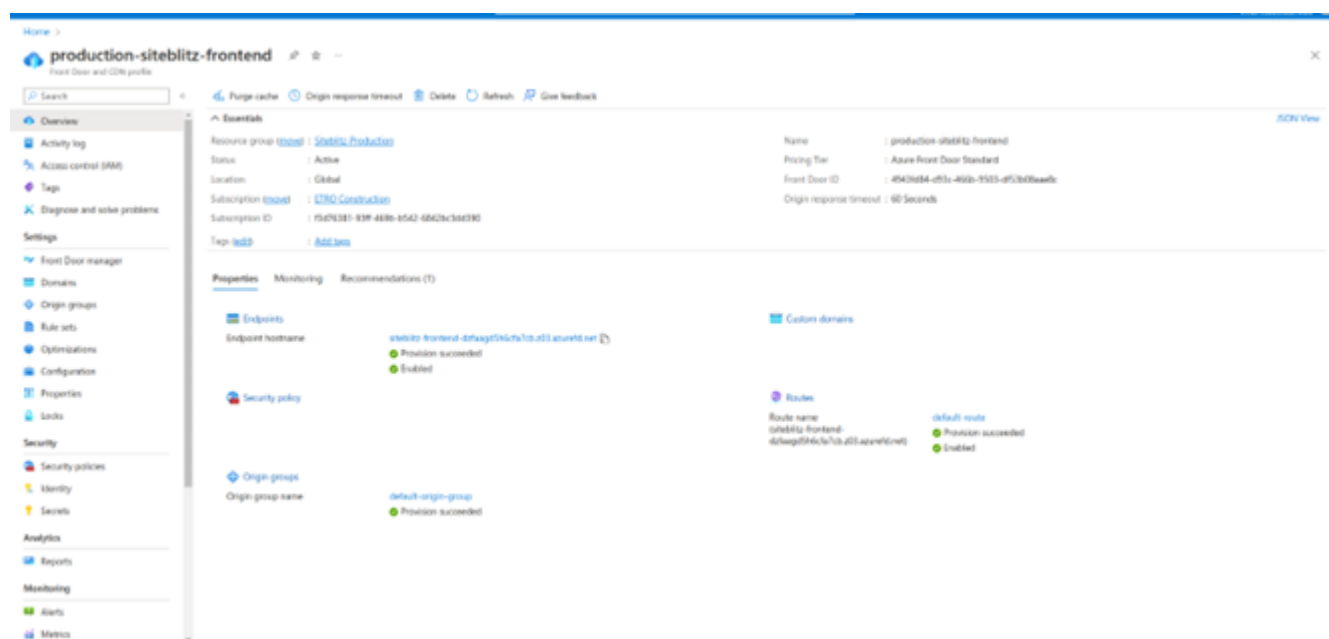
www.audaztecnologia.com.br

SUMÁRIO

1. Infraestrutura	3
2. Armazenamento de objetos	3
2. Backend do Siteblitz	4
3. Máquinas virtuais	4
4. Dados	5
6. Kubernetes (k3s)	6
6.1 Pods	6
6.2 Services	6
6.3 Ingress	6
7. Rede	7
8. Zona DNS	8
9. Gateway de rede virtual	8
10. Gateway de rede local	8
11. Balanceamento de carga (gateway de aplicativo)	8
12. Segurança	8
13. WAF	8
14. Registro de contêiner	9
15. Gateway VPN	9
16. VPN Site-to-site (IPsec)	9
17. VPN Site-to-site (IPsec) ETRO CONSTRUCTION com METATRON	9
18. VPN Site-to-site (IPsec) ETRO CONSTRUCTION com AUDAZ TECNOLOGIA	9

1. Infraestrutura

Este é um documento as-built para a infraestrutura de nuvem do Azure que foi criada para o cliente ETRO CONSTRUCTION. Esta infraestrutura foi criada para o aplicativo Siteblitz.



The screenshot shows the Azure portal configuration for the 'production-siteblitz-frontend' Front Door and CDN profile. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Front Door manager, Domains, Origin groups, Rule sets, Optimizations, Configuration, Properties, Locks, Security, Security policies, Identity, Secrets, Analytics, Reports, Monitoring, Alerts, and Metrics.

Essentials

- Resource group: [Siteblitz-Production](#)
- Status: Active
- Location: Global
- Subscription: [ETRO Construction](#)
- Subscription ID: f5d76381-839f-468b-b542-6842b3a62390
- Tags: [Add tags](#)

Properties

- Name: production-siteblitz-frontend
- Pricing tier: Azure Front Door Standard
- Front Door ID: 4943b684-df1c-468b-b542-6842b3a62390
- Origin response timeout: 90 seconds

Endpoints

- Endpoint hostname: siteblitz-frontend-4fswg9f6v6u7chz03.azurefd.net
- Provision succeeded
- Enabled

Security policy

- Provision succeeded
- Enabled

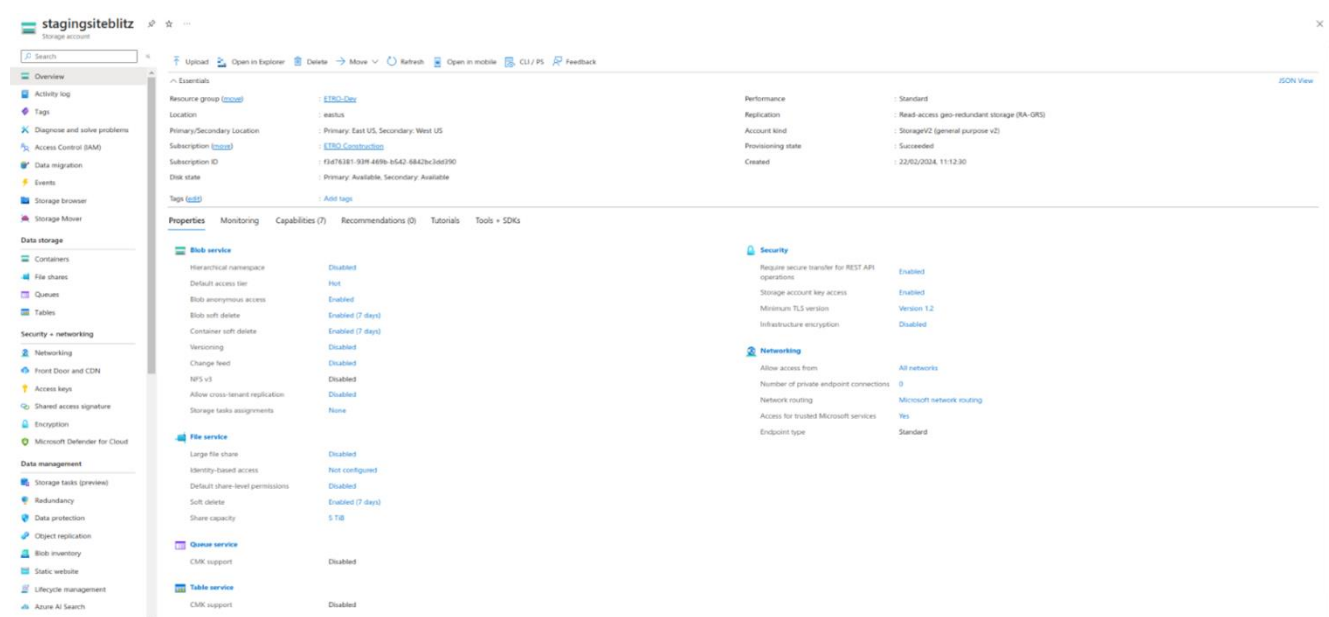
Origin groups

- Origin group name: default-origin-group
- Provision succeeded

Custom domains

- Route name: default-route
- Provision succeeded
- Enabled

2. Armazenamento de objetos



The screenshot shows the Azure portal configuration for the 'stagingsiteblitz' Storage account. The left sidebar contains navigation links for Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Data storage, Containers, File shares, Queues, Tables, Security + networking, Networking, Front Door and CDN, Access keys, Shared access signature, Encryption, Microsoft Defender for Cloud, Data management, Storage tasks (preview), Redundancy, Data protection, Object replication, Blob inventory, Static website, Lifecycle management, and Azure AI Search.

Essentials

- Resource group: [ETRO-Dev](#)
- Location: eastus
- Primary/Secondary Location: Primary: East US, Secondary: West US
- Subscription: [ETRO Construction](#)
- Subscription ID: f5d76381-839f-468b-b542-6842b3a62390
- Disk state: Primary: Available, Secondary: Available
- Tags: [Add tags](#)

Properties

- Performance: Standard
- Replication: Read access geo-redundant storage (RA-GRS)
- Account kind: StorageV2 (general purpose v2)
- Provisioning state: Succeeded
- Created: 22/02/2024, 11:12:30

Block service

- Hierarchical namespace: Disabled
- Default access tier: Hot
- Blob anonymous access: Enabled
- Blob soft delete: Enabled (7 days)
- Container soft delete: Enabled (7 days)
- Versioning: Disabled
- Change feed: Disabled
- NFS v3: Disabled
- Allow cross-tenant replication: Disabled
- Storage tasks assignments: None

File service

- Large file share: Disabled
- Identity-based access: Not configured
- Default share-level permissions: Disabled
- Soft delete: Enabled (7 days)
- Share capacity: 5 TB

Queue service

- Queue support: Disabled

Table service

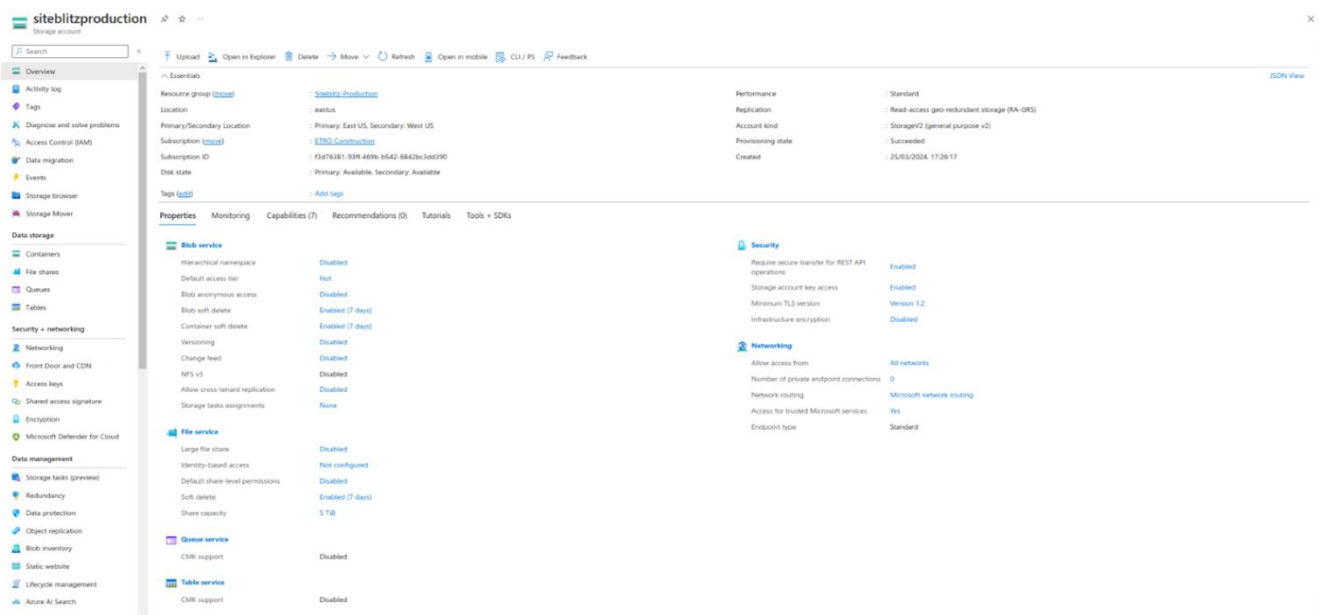
- Table support: Disabled

Security

- Require secure transfer for REST API operations: Enabled
- Storage account key access: Enabled
- Minimum TLS version: Version 1.2
- Infrastructure encryption: Disabled

Networking

- Allow access from: All networks
- Number of private endpoint connections: 0
- Network routing: Microsoft network routing
- Access to trusted Microsoft services: Yes
- Endpoint type: Standard



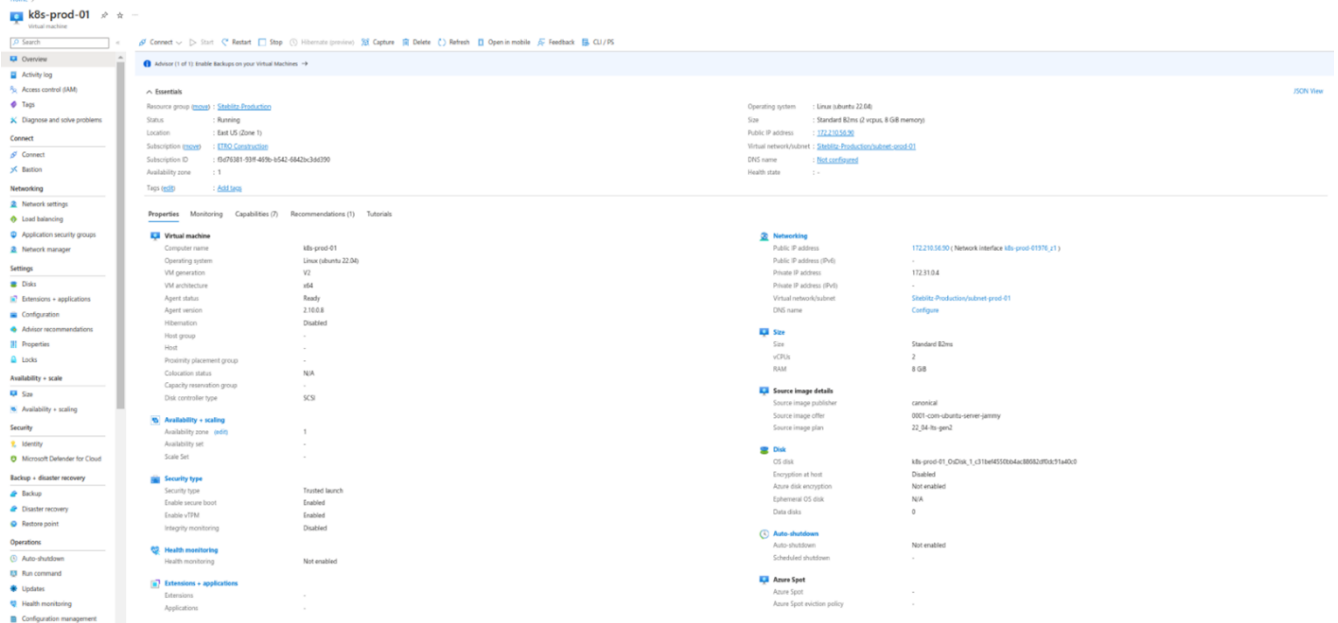
O armazenamento de objetos foi criado para fornecer uma solução de armazenamento escalável e econômica para dados não estruturados, como imagens, vídeos e logs. Ele foi configurado para dimensionar e manipular automaticamente grandes quantidades de dados.

2. Backend do Siteblitz

O backend do Siteblitz foi criado usando o Azure Kubernetes Service (AKS) e o k3s. Ele foi configurado para dimensionar e manipular automaticamente alto tráfego. Ele também foi configurado para usar um registro de contêiner para armazenar e gerenciar imagens de contêiner.

3. Máquinas virtuais

As máquinas virtuais foram criadas para hospedar o aplicativo Siteblitz e outros serviços. Elas foram configuradas para usar os discos gerenciados do Azure para armazenamento e foram colocadas em um conjunto de disponibilidade para garantir alta disponibilidade.

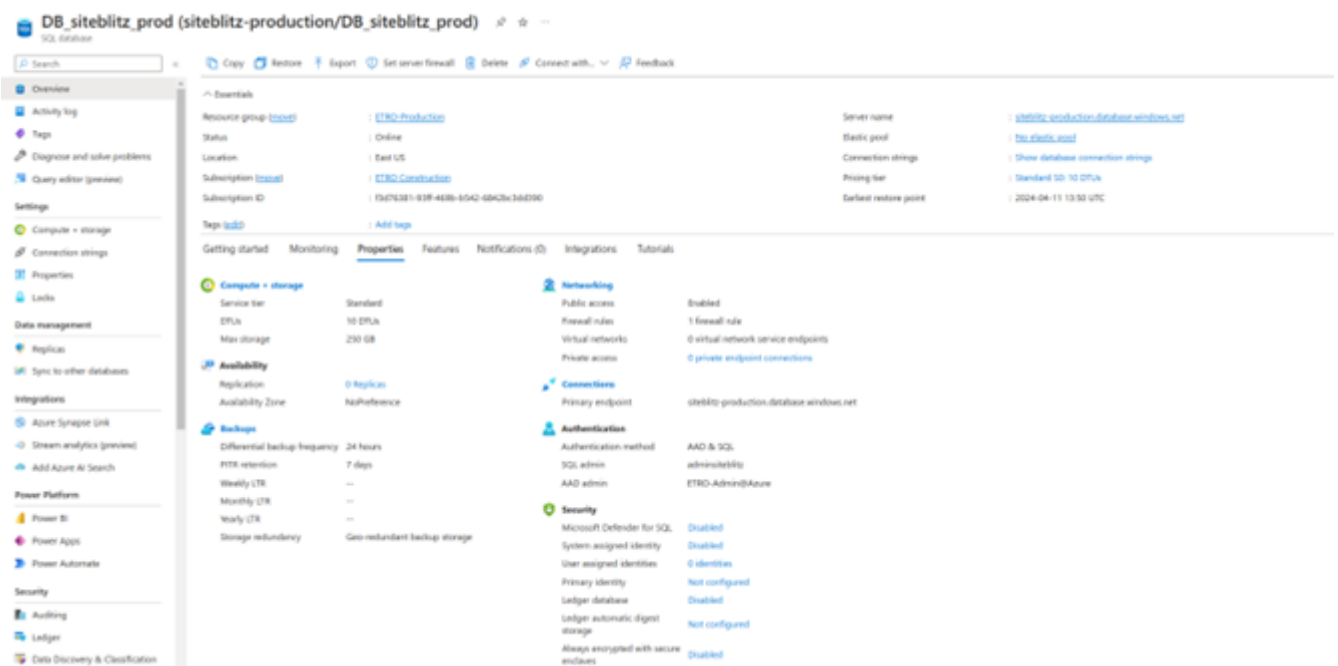


The screenshot displays the Azure portal interface for a virtual machine named 'k8s-prod-01'. The left sidebar shows the navigation menu with categories like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Network settings, Load balancing, Application security groups, Network manager, Settings, Disks, Extensions + applications, Configuration, Advisor recommendations, Properties, Locks, Availability + scale, Security, Backup + disaster recovery, and Operations. The main content area is divided into several sections:

- Essentials:** Shows basic information about the VM, including its status (Running), location (East US Zone 1), subscription (ETRO-Construction), and tags.
- Properties:** A table listing various properties of the VM, such as computer name, operating system, VM generation, VM architecture, agent status, agent version, network interface, host group, host, proximity placement group, calculation status, capacity reservation group, and disk controller type.
- Virtual machine:** A section detailing the VM's configuration, including its name, operating system, VM generation, VM architecture, agent status, agent version, network interface, host group, host, proximity placement group, calculation status, capacity reservation group, and disk controller type.
- Availability + scaling:** A section showing the VM's availability zone, availability set, and scale set.
- Security type:** A section showing the VM's security type, security type, enable secure boot, enable UEFI, and integrity monitoring.
- Health monitoring:** A section showing the VM's health monitoring status.
- Extensions + applications:** A section showing the VM's extensions and applications.
- Networking:** A section showing the VM's network configuration, including its public IP address, private IP address, and virtual network.
- Size:** A section showing the VM's size, size, vCPUs, and RAM.
- Source image details:** A section showing the VM's source image details, including its source image publisher, source image offer, and source image plan.
- Disks:** A section showing the VM's disks, including its OS disk, exception at boot, Azure disk encryption, and data disks.
- Auto shutdown:** A section showing the VM's auto shutdown status.
- Assess Spent:** A section showing the VM's assess spent status.

4. Dados

O armazenamento de dados foi configurado usando bancos de dados SQL do Azure. Os bancos de dados foram configurados para dimensionar e manipular automaticamente alto tráfego. Eles também foram configurados para usar o serviço de backup gerenciado do Azure para proteção de dados.



The screenshot displays the Azure portal interface for a SQL database named 'DB_siteblitz_prod'. The left sidebar shows the navigation menu with categories like Overview, Activity log, Tags, Diagnose and solve problems, Query editor (preview), Settings, Compute + storage, Connection strings, Properties, Locks, Data management, Replicas, Sync to other databases, Integrations, Azure Synapse Link, Stream analytics (preview), Add Azure AI Search, Power Platform, Power BI, Power Apps, Power Automate, Security, Auditing, Ledger, and Data Discovery & Classification. The main content area is divided into several sections:

- Essentials:** Shows basic information about the database, including its resource group, status, location, subscription, and tags.
- Compute + storage:** A section showing the database's compute and storage configuration, including its service tier, vCPUs, and max storage.
- Availability:** A section showing the database's availability configuration, including its replication, availability zone, and backup frequency.
- Backups:** A section showing the database's backup configuration, including its differential backup frequency, PITR retention, weekly LTR, monthly LTR, and yearly LTR.
- Networking:** A section showing the database's network configuration, including its public access, firewall rules, virtual networks, and private access.
- Connections:** A section showing the database's connection configuration, including its primary endpoint and connection strings.
- Authentication:** A section showing the database's authentication configuration, including its authentication method, SQL admin, and AAD admin.
- Security:** A section showing the database's security configuration, including its Microsoft Defender for SQL, system-assigned identities, user-assigned identities, primary identity, ledger database, ledger automatic digest storage, and always encrypted with secure enclaves.

6. Kubernetes (k3s)

O Kubernetes foi usado para gerenciar e orquestrar o aplicativo Siteblitz e outros serviços. Ele foi configurado para usar o serviço Kubernetes gerenciado do Azure (AKS) para dimensionamento automático e alta disponibilidade.

6.1 Pods

Os pods foram criados para executar o aplicativo Siteblitz e outros serviços. Eles foram configurados para usar o serviço Kubernetes gerenciado do Azure (AKS) para dimensionamento automático e alta disponibilidade.

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE	IP	NODE	NOMINATED NODE	READINESS GATES
kube-system	helm-install-traefik-g52pn	0/1	Completed	1	28d	<none>	k8s-prod-01	<none>	<none>
kube-system	helm-install-traefik-crd-8k2s4	0/1	Completed	0	28d	<none>	k8s-prod-01	<none>	<none>
kube-system	fluentd-j42nc	1/1	Running	2 (9d ago)	24d	10.42.0.57	k8s-prod-01	<none>	<none>
monitoring	node-exporter-hn4p4	2/2	Running	4 (9d ago)	24d	172.31.0.4	k8s-prod-01	<none>	<none>
kube-system	svcib-siteblitz-production-service-f7b6f4dd-w0flg	1/1	Running	2 (9d ago)	27d	10.42.0.55	k8s-prod-01	<none>	<none>
kube-system	svcib-grafana-af132220-k8f5j	1/1	Running	2 (9d ago)	24d	10.42.0.61	k8s-prod-01	<none>	<none>
kube-system	coredns-6799fbc05-p2nvd	1/1	Running	2 (9d ago)	28d	10.42.0.59	k8s-prod-01	<none>	<none>
kube-system	local-path-provisioner-5c8658495-82dch	1/1	Running	3 (9d ago)	28d	10.42.0.69	k8s-prod-01	<none>	<none>
monitoring	prometheus-operator-78dd987cb4-vp9xn	2/2	Running	4 (9d ago)	24d	10.42.0.65	k8s-prod-01	<none>	<none>
kube-system	svcib-traefik-abfead36-w25pq	2/2	Running	4 (9d ago)	28d	10.42.0.64	k8s-prod-01	<none>	<none>
production	siteblitz-backend-production-76c747d6bc-knngh	1/1	Running	2 (9d ago)	27d	10.42.0.71	k8s-prod-01	<none>	<none>
monitoring	kube-state-metrics-6bd55cf708-4xb57	3/3	Running	6 (9d ago)	24d	10.42.0.63	k8s-prod-01	<none>	<none>
monitoring	blackbox-exporter-6b5475894-net7v	3/3	Running	6 (9d ago)	24d	10.42.0.78	k8s-prod-01	<none>	<none>
monitoring	alertmanager-main-8	2/2	Running	4 (9d ago)	24d	10.42.0.68	k8s-prod-01	<none>	<none>
monitoring	alertmanager-main-2	2/2	Running	4 (9d ago)	24d	10.42.0.66	k8s-prod-01	<none>	<none>
monitoring	alertmanager-main-1	2/2	Running	4 (9d ago)	24d	10.42.0.67	k8s-prod-01	<none>	<none>
monitoring	grafana-59844d49d5-wvc5d	1/1	Running	2 (9d ago)	24d	10.42.0.60	k8s-prod-01	<none>	<none>
kube-system	metrics-server-67c65894b-9mdkk	1/1	Running	3 (9d ago)	28d	10.42.0.58	k8s-prod-01	<none>	<none>
kube-system	traefik-f4564c4f4-crj36	1/1	Running	2 (9d ago)	28d	10.42.0.62	k8s-prod-01	<none>	<none>
monitoring	prometheus-k8s-0	2/2	Running	4 (9d ago)	24d	10.42.0.53	k8s-prod-01	<none>	<none>
monitoring	prometheus-k8s-1	2/2	Running	4 (9d ago)	24d	10.42.0.56	k8s-prod-01	<none>	<none>
monitoring	prometheus-adapter-74894c5547-9scv1	1/1	Running	3 (9d ago)	24d	10.42.0.54	k8s-prod-01	<none>	<none>
monitoring	prometheus-adapter-74894c5547-3889n	1/1	Running	3 (9d ago)	24d	10.42.0.52	k8s-prod-01	<none>	<none>

6.2 Services

Os serviços foram criados para expor o aplicativo Siteblitz e outros serviços à Internet. Eles foram configurados para usar o serviço Kubernetes gerenciado do Azure (AKS) para dimensionamento automático e alta disponibilidade.

NAMESPACE	NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
default	kubernetes	ClusterIP	10.43.0.1	<none>	443/TCP	28d
kube-system	kube-dns	ClusterIP	10.43.0.10	<none>	53/UDP,53/TCP,9153/TCP	28d
kube-system	metrics-server	ClusterIP	10.43.11.66	<none>	443/TCP	28d
kube-system	traefik	LoadBalancer	10.43.32.83	172.31.0.4	80:30788/TCP,443:32713/TCP	28d
monitoring	alertmanager-main	ClusterIP	10.43.202.0	<none>	9093/TCP,8080/TCP	24d
monitoring	blackbox-exporter	ClusterIP	10.43.109.60	<none>	9115/TCP,19115/TCP	24d
monitoring	kube-state-metrics	ClusterIP	None	<none>	8443/TCP,9443/TCP	24d
monitoring	node-exporter	ClusterIP	None	<none>	9100/TCP	24d
monitoring	prometheus-k8s	ClusterIP	10.43.166.238	<none>	9090/TCP,8080/TCP	24d
monitoring	prometheus-adapter	ClusterIP	10.43.23.172	<none>	443/TCP	24d
monitoring	prometheus-operator	ClusterIP	None	<none>	8443/TCP	24d
kube-system	kubelet	ClusterIP	None	<none>	10250/TCP,10255/TCP,4194/TCP	24d
monitoring	alertmanager-operated	ClusterIP	None	<none>	9093/TCP,9094/TCP,9094/UDP	24d
monitoring	prometheus-operated	ClusterIP	None	<none>	9090/TCP	24d
production	siteblitz-production-service	LoadBalancer	10.43.136.46	172.31.0.4	7070:32416/TCP	27d
monitoring	grafana	LoadBalancer	10.43.186.172	172.31.0.4	3000:32574/TCP	24d

6.3 Ingress

O Ingress foi criado para rotear o tráfego para o aplicativo Siteblitz e outros serviços. Ele foi configurado para usar o serviço Kubernetes gerenciado do Azure (AKS) para dimensionamento automático e alta disponibilidade.

GatewaySubnet

Siteblitz-Production

Name

GatewaySubnet

Subnet address range * ⓘ

172.31.1.0/24

172.31.1.0 - 172.31.1.255 (251 + 5 Azure reserved addresses)

☐ Add IPv6 address space ⓘ

NAT gateway ⓘ

None

Network security group

None

Route table

None

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. Select the types of network policies that control traffic going to the private endpoints in this subnet. [Learn more](#)

Private endpoint network policy

0 selected

7. Rede

Uma rede virtual foi criada para isolar o aplicativo Siteblitz e outros serviços da Internet. Ela foi configurada para usar o serviço de rede virtual gerenciada do Azure para dimensionamento automático e alta disponibilidade.

8. Zona DNS

Uma zona DNS foi criada para fornecer um nome de domínio personalizado para o aplicativo Siteblitz. Ela foi configurada para usar o serviço DNS gerenciado do Azure para dimensionamento automático e alta disponibilidade.

9. Gateway de rede virtual

Um gateway de rede virtual foi criado para fornecer conectividade segura entre o aplicativo Siteblitz e outros serviços. Ele foi configurado para usar o serviço de gateway de rede virtual gerenciada do Azure para dimensionamento automático e alta disponibilidade.

10. Gateway de rede local

Um gateway de rede local foi criado para fornecer conectividade segura entre o aplicativo Siteblitz e outros serviços. Ele foi configurado para usar o serviço de gateway de rede local gerenciada do Azure para dimensionamento automático e alta disponibilidade.

11. Balanceamento de carga (gateway de aplicativo)

Um gateway de aplicativo foi criado para fornecer balanceamento de carga e roteamento de tráfego para o aplicativo Siteblitz e outros serviços. Ele foi configurado para usar o serviço de gateway de aplicativo gerenciado do Azure para dimensionamento automático e alta disponibilidade.

12. Segurança

A segurança foi configurada usando o centro de segurança do Azure para fornecer proteção contra ameaças, avaliação de vulnerabilidades e aplicação de políticas de segurança. Ele também foi configurado para usar o serviço de firewall gerenciado do Azure para filtragem de tráfego e controle de acesso.

13. WAF

Um firewall de aplicativo da Web (WAF) foi criado para fornecer proteção contra ataques de aplicativo da Web. Ele foi configurado para usar o serviço WAF gerenciado do Azure para dimensionamento automático e alta disponibilidade.

14. Registro de contêiner

Um registro de contêiner foi criado para armazenar e gerenciar imagens de contêiner para o aplicativo Siteblitz e outros serviços. Ele foi configurado para usar o serviço de registro de contêiner gerenciado do Azure para dimensionamento automático e alta disponibilidade.

15. Gateway VPN

Um gateway VPN foi criado para fornecer conectividade segura entre o aplicativo Siteblitz e outros serviços. Ele foi configurado para usar o serviço de gateway VPN gerenciado do Azure para dimensionamento automático e alta disponibilidade.

16. VPN Site-to-site (IPsec)

Uma VPN site-to-site foi criada para fornecer conectividade segura entre o aplicativo Siteblitz e outros serviços. Ela foi configurada para usar o serviço VPN site-to-site gerenciado do Azure para dimensionamento automático e alta disponibilidade.

17. VPN Site-to-site (IPsec) ETRO CONSTRUCTION com METATRON

Uma VPN site-to-site foi criada para fornecer conectividade segura entre o aplicativo Siteblitz e outros serviços. Ela foi configurada para usar o serviço VPN site-to-site gerenciado do Azure para dimensionamento automático e alta disponibilidade.

18. VPN Site-to-site (IPsec) ETRO CONSTRUCTION com AUDAZ TECNOLOGIA

Uma VPN site-to-site foi criada para fornecer conectividade segura entre o aplicativo Siteblitz e outros serviços. Ela foi configurada para usar a VPN site-to-site gerenciada do Azure