# \_

|  |  |
| --- | --- |
| \_Default | 4:35, 4:88, 5:39, 5:44, 5:46-48, 5:50, 5:58, 5:60, 5:62, 5:66 |
| \_Required | 4:35, 4:88, 5:39, 5:44, 5:46-50, 5:58, 5:60, 5:62, 5:66 |

# A

|  |  |
| --- | --- |
| Access Key | 2:99-102, 3:13, 3:23-25, 3:32, 3:34, 3:42-43, 3:46-52, 3:55, 3:58, 3:69, 3:73, 3:155, 4:25 |
| accessKeyID | 3:45, 3:47-48, 3:69, 3:85, 3:122, 3:133, 4:26, 4:47, 4:55 |
| accountName | 2:102 |
| actAs | 5:28 |
| Add-MailboxPermission | 1:47 |
| ADFS | 1:87, 1:97, 2:51 |
| Amazon Machine Image (AMI) | 3:70, 3:84 |
| Amazon Resource Name (ARN) | 3:10, 3:12, 3:36-37, 3:39-42, 3:44-47, 3:69, 4:24 |
| API Calls | 1:91, 1:104, 1:114-115, 1:120, 3:14-15, 3:17-21, 3:27-28, 3:31-32, 3:35, 3:49, 3:52-53, 3:55, 3:58-60, 3:114, 3:147, 4:34, 4:115, 4:117, 5:4, 5:37, 5:79 |
| API Key | 1:23, 3:47, 3:53, 3:61, 4:50, 4:54 |
| Append blobs | 2:96 |
| Application Gateway | 2:105 |
| Application Load Balancer (ALB) | 3:100, 3:102 |
| AssumedRole | 3:37, 3:88 |
| Athena | 3:29, 3:91, 3:119, 3:131-137 |
| ATT&CK | 2:126, 4:82, 4:85-86 |
| AWS Audit Manager | 3:7-8 |
| AWS Detective | 3:29, 3:57 |
| AWS GuardDuty | 3:35, 3:57, 3:59-60, 3:130, 3:138, 3:140, 3:142, 3:144-145 |
| AWS Lambda | 1:19, 3:145-147, 3:149, 3:151 |
| AWS Systems Manager | 3:154-156 |
| AWSAccount | 3:37 |
| awsRegion | 3:36, 3:45, 3:47, 3:70, 3:85, 3:89, 3:122 |
| AWSService | 3:37, 3:42, 3:88 |
| az | 1:24, 1:55, 2:12-13, 2:41, 2:51, 2:78, 3:105, 5:74 |
| AzCopy | 2:88, 2:96, 2:102, 2:119 |
| Azure Active Directory (AAD) | 1:34, 1:87, 2:4, 4:29 |
| Azure Defender | 2:122 |
| Azure Functions | 1:19 |
| Azure Kubernetes Service (AKS) | 4:27-30, 4:36, 5:73 |
| Azure Monitor | 2:78, 3:148 |
| Azure Portal | 1:56, 1:92, 1:95, 2:6, 2:16, 2:19, 2:21, 2:24, 2:47-50, 2:60, 2:65, 2:80, 2:126 |
| Azure Private Link | 2:98 |
| Azure Security Center | 2:53, 2:122 |
| Azure Sentinel | 2:122-123 |
| Azure Storage | 2:45, 2:60-61, 2:64, 2:78-79, 2:96, 2:101-102, 2:116, 2:119-120 |
| Azure Storage Explorer | 2:60-61, 2:64, 2:79, 2:96, 2:101-102, 2:116, 2:119-120 |
| AzureActiveDirectory | 1:33-34, 1:45, 1:94, 1:96, 1:118 |
| AzureActivity | 2:58-59 |

# B

|  |  |
| --- | --- |
| Beats | 1:11, 1:13 |
| Billing | 2:4, 2:72, 3:9, 3:104, 5:5, 5:9, 5:14, 5:18 |
| Bind | 1:51-54, 1:56, 1:59, 1:120, 4:20, 4:46, 4:48, 4:52, 4:56, 5:10, 5:12-15, 5:17-20, 5:22, 5:106-107, 5:114 |
| Blob | 1:29, 2:17, 2:46, 2:61-64, 2:79, 2:88, 2:95-97, 2:99-100, 2:102, 2:116, 2:119-120, 3:32, 4:83, 4:108, 5:28 |
| Blob Storage | 1:29, 2:95-96 |
| Block blobs | 2:96 |
| boto | 1:24, 3:53 |
| Buckets | 2:37, 3:10, 3:14, 3:17, 3:19-20, 3:29-30, 3:34, 3:103-104, 3:113-114, 3:116-119, 3:122-123, 3:126, 3:128, 3:130, 3:135-137, 3:140, 3:144, 4:33, 4:88, 5:4, 5:12, 5:17, 5:24, 5:27, 5:44, 5:46, 5:60, 5:62, 5:66-69, 5:104-107, 5:109-114, 5:116, 5:119-121 |
| Business Email Compromise (BEC) | 1:46, 1:64-65, 4:75, 4:95, 4:111-112 |

# C

|  |  |
| --- | --- |
| callerIpAddress | 1:50, 2:20, 2:24, 2:32, 2:34-35, 2:38-39, 2:102, 2:108 |
| Chat | 1:104, 1:110, 4:75, 4:89, 4:123-126, 4:128, 4:138 |
| Chronicle | 1:9-10 |
| Cloud Flows | 1:21, 1:26 |
| Cloud Functions | 1:19, 1:29, 5:73-74 |
| Cloud Identity | 4:115, 5:6-7, 5:18 |
| Cloud Pub/Sub | 1:29 |
| Cloud Virtual Network | 1:29 |
| CloudBerry | 3:33 |
| Cloudshell | 1:24, 5:88-89 |
| CloudTrail | 1:13, 1:29, 3:27-38, 3:43-50, 3:53, 3:57, 3:59-62, 3:67, 3:69-72, 3:75, 3:79, 3:85-86, 3:88-90, 3:114, 3:118-119, 3:122, 3:125, 3:130-132, 3:134-137, 3:140, 3:142, 3:144, 3:147, 3:151, 3:154, 3:156, 4:21, 4:37, 4:47 |
| CloudTrail Insights | 3:35, 3:130 |
| CloudWatch | 1:29, 3:27, 3:91, 3:104, 3:107, 3:130, 3:136, 3:144, 3:146-150, 4:18-19, 4:31, 4:35, 4:37 |
| Coldsnap | 3:83 |
| Collection | 1:11, 1:44, 1:65, 1:79, 1:87, 2:11, 2:78, 2:126, 3:12, 3:95, 3:119-120, 3:145, 4:32, 4:78, 5:4, 5:7 |
| Command line (CLI) | 1:13, 1:24, 1:103, 2:6, 2:10, 2:13, 2:41, 2:49-50, 2:100, 2:126, 3:24, 3:33, 3:38, 3:46, 3:49, 3:51, 3:57, 3:82, 3:84, 3:86, 3:122, 3:154, 4:47, 5:15, 5:43, 5:59, 5:65, 5:67, 5:87-89 |
| Compute Engine | 1:29, 5:5, 5:11, 5:25-26, 5:41, 5:73, 5:75, 5:79 |
| Consent | 1:94, 1:97, 1:105, 1:110-111, 2:26, 2:125, 4:83 |
| Console | 1:24, 1:92, 1:103, 2:82, 2:100, 3:19, 3:24-25, 3:27, 3:29, 3:31-33, 3:38, 3:43-50, 3:53, 3:57-58, 3:67-68, 3:70, 3:75, 3:107, 3:117, 3:150, 4:11, 4:30, 4:33, 4:67, 4:71, 4:73, 4:75, 4:77-79, 4:91, 4:120, 4:142, 5:6, 5:15, 5:18, 5:59-60, 5:84, 5:86-89, 5:94 |
| Console Access | 3:25, 3:38, 3:47, 3:58 |
| Console Login | 3:45, 3:49 |
| Containers | 1:19-20, 2:79, 2:99, 3:10, 3:87, 3:147, 4:4-5, 4:7-14, 4:16, 4:19, 4:33-34, 4:39, 4:49, 4:53, 4:57, 4:59, 5:73-74 |
| Control Plane | 1:6, 3:28-29, 3:125, 3:147, 4:10, 4:14, 4:19-20, 4:22, 4:27-28, 4:31-33, 4:35, 4:45, 4:53 |
| correlationId | 2:20, 2:24, 2:32, 2:34-35, 2:38-40, 2:108 |
| createDate | 3:48 |
| CrowdStrike Reporting Tool (CRT) | 1:121 |
| Crypto Mining | 2:18, 2:76, 4:21 |
| Cyber Duck | 3:33 |

# D

|  |  |
| --- | --- |
| Dashboard | 1:11, 3:31, 3:54, 3:104, 3:147, 3:154 |
| Data Event | 3:28, 3:30, 3:32, 3:125, 4:135 |
| Data Transfer | 1:27-28, 2:72, 3:67, 3:80, 3:104, 3:148, 5:123 |
| Defender | 2:37, 2:53, 2:122, 4:11 |
| Detective | 3:29, 3:57, 3:138-140, 3:145 |
| deviceName | 2:35, 3:79 |
| Docker | 1:19-20, 4:11, 4:39 |

# E

|  |  |
| --- | --- |
| Elastic Block Store (EBS) | 1:29, 3:10, 3:17, 3:68, 3:77-80, 3:82, 3:84, 3:86-87, 3:92 |
| Elastic Common Schema | 1:9 |
| Elastic Compute Cloud (EC2) | 3:65 |
| Elastic File Store (EFS) | 1:29, 3:73, 3:87-90, 3:97, 3:151 |
| Elastic Kubernetes Service (EKS) | 3:59, 3:136, 3:147, 4:19-20, 4:27, 4:31-32, 4:37, 4:40, 4:42, 4:46-48, 4:56, 5:73 |
| Elastic Stack | 1:11-12 |
| Elasticsearch | 1:11, 1:16 |
| Enumeration | 3:53-54 |
| etcd | 4:22, 4:44, 4:49-50, 4:59 |
| ETW events | 2:78 |
| Event Hub | 1:29, 1:92, 2:16, 2:47, 2:60, 2:65-68, 2:78, 2:95, 2:97, 2:103, 4:28, 5:70 |
| Event logs | 2:78-79, 3:27, 3:91, 4:33, 5:37 |
| Event Tracing for Windows (ETW) | 2:78 |
| Event Triggers | 3:145, 3:151 |
| EventBridge | 3:135, 3:142, 3:146, 3:151 |
| eventID | 2:83, 3:38 |
| eventName | 3:36, 3:45, 3:47, 3:70, 3:85, 3:89, 3:122 |
| eventSource | 1:71, 3:36, 3:45, 3:47, 3:70, 3:85, 3:89, 3:122 |
| eventTime | 3:36, 3:44-47, 3:70, 3:85, 3:89, 3:122, 4:58 |
| eventType | 3:38 |
| Exchange | 1:3, 1:16, 1:31, 1:33-34, 1:37-38, 1:45-50, 1:52-54, 1:56-64, 1:68-69, 1:73, 1:77, 1:82, 1:87, 1:97, 1:102, 1:120-121, 4:97 |
| Exchange Mailbox | 1:48-49, 1:62 |
| Exchange Online | 1:37, 1:63-64, 1:97, 1:102, 1:121 |
| Execution | 1:36, 2:46, 2:84, 3:54, 3:57, 3:143-144, 3:149-150, 3:152, 3:155 |
| Exfiltration | 2:18, 2:97, 2:100-102, 2:117-118, 2:120, 3:110, 3:148, 4:75, 4:91, 4:140-141, 5:120 |
| Exposed API Keys | 3:53 |
| ExpressRoute | 2:104 |

# F

|  |  |
| --- | --- |
| FederatedUser | 3:37 |
| File Storage | 1:29, 2:18, 2:95 |
| File-based logs | 2:78 |
| FileAccessed | 1:34, 1:70-71, 1:76-77, 1:86 |
| FilePreviewed | 1:70-71 |
| Firewall | 1:23, 2:105-106, 3:17-18, 3:65, 3:95-96, 3:99-100, 3:107, 5:56, 5:122, 5:129-134 |
| Firewall Rules | 3:95-96, 3:107, 5:122, 5:129-130, 5:133 |
| Flow logs | 1:13, 1:20, 1:23, 1:26, 2:63, 2:110-114, 2:116-117, 3:12, 3:59, 3:75, 3:90, 3:96, 3:98-101, 3:103-104, 3:110-111, 3:118-119, 3:130, 3:136-137, 3:140, 3:145, 3:147-148, 5:122-123, 5:125, 5:127-128, 5:130, 5:133 |
| Forms | 1:4, 1:6, 1:11, 1:56, 2:5, 2:68, 4:5, 4:95 |
| Functions | 1:19, 1:29, 1:43, 1:105, 3:15, 3:17-18, 3:28, 3:31-32, 3:49, 3:135, 3:142-143, 3:147, 3:150-152, 4:73, 4:82, 5:6, 5:73-74 |

# G

|  |  |
| --- | --- |
| gcloud | 1:13, 1:24, 4:38, 5:12-14, 5:27, 5:59, 5:65-69, 5:88-89, 5:98, 5:106-108, 5:114, 5:117 |
| Get-AzLog | 2:41, 2:77 |
| GitHub | 1:7-8, 1:97, 1:102-103, 2:76, 2:79, 2:103, 2:116, 3:32, 3:34, 3:43, 3:53-54, 3:83-84, 3:136, 4:37, 4:82-84, 4:87, 4:108 |
| Globally Unique Identifier (GUID) | 1:50, 1:115-116, 2:9, 2:20, 2:23, 2:32, 2:38 |
| Glue | 2:104, 3:119, 3:131-135, 3:137, 3:147 |
| Gmail | 1:120, 1:126, 2:127, 3:160, 4:65, 4:75, 4:77, 4:80-82, 4:89, 4:101-108, 4:111, 4:116-117, 4:141, 4:143, 5:29, 5:136 |
| Google Cloud CLI | 5:65 |
| Google Cloud Functions | 1:19 |
| Google Cloud IAM | 5:7 |
| Google Drive (GDrive) | 4:72, 4:75, 4:89, 4:130, 4:133, 4:139, 4:141 |
| Google Group | 4:142, 5:7 |
| Google Kubernetes Engine (GKE) | 4:27, 4:33-34, 4:38, 5:36, 5:73 |
| Google Takeout | 4:75, 4:82, 4:133-135, 4:138 |
| Google Unified Data Model | 1:9 |
| Google Vault | 4:77, 4:89 |
| Graph API | 1:1, 1:3, 1:24, 1:35, 1:50, 1:53, 1:92, 1:102-105, 1:114-116, 1:118-125, 2:51, 2:65, 2:68, 2:100, 2:125 |
| Groups | 1:87, 1:121, 2:4, 2:7, 3:12, 3:68, 3:95, 3:99, 4:46, 4:69, 4:72, 4:89, 5:18 |
| gRPC | 1:24, 3:100, 5:59, 5:71 |
| GSheet | 4:78 |
| GuardDuty | 3:35, 3:57, 3:59-60, 3:130, 3:138, 3:140, 3:142, 3:144-145 |

# H

|  |  |
| --- | --- |
| HardDelete | 1:48, 1:82 |
| hypervisor | 1:6, 1:25, 3:80, 4:5-6 |

# I

|  |  |
| --- | --- |
| IAM | 1:6, 1:20, 1:23, 1:87, 2:24, 3:5-6, 3:10, 3:12-19, 3:22-26, 3:34, 3:36-37, 3:40-45, 3:47-48, 3:50-51, 3:53, 3:55, 3:57-58, 3:61, 3:65, 3:67, 3:69, 3:73-74, 3:85, 3:114-115, 3:122, 3:137, 3:146-147, 3:154-155, 4:20, 4:24-26, 4:31-32, 4:45-48, 4:54-56, 4:62, 5:6-9, 5:12-15, 5:17, 5:24-25, 5:27-29, 5:32-34, 5:39-40, 5:42, 5:54-55, 5:77-78, 5:104, 5:106-107, 5:109, 5:114, 5:116 |
| IAM Policy Simulator | 3:22 |
| IAM Roles | 3:14-15, 3:18, 3:23-26, 3:34, 3:57, 3:65, 3:73, 3:114, 4:45, 4:62, 5:14 |
| IAMUser | 3:37, 3:85, 3:122 |
| ID Prefixes | 3:51-52 |
| Identity | 1:4, 1:6, 1:23, 1:87, 1:93-94, 2:4, 2:14, 2:17, 2:22-23, 2:31, 2:39, 2:43, 2:45-46, 2:51, 2:81, 2:90, 2:92, 2:102, 2:108, 2:117, 3:12, 3:16, 3:36-37, 3:45, 3:47, 3:55, 3:69, 3:73, 3:85, 3:122, 3:133, 4:29, 4:32, 4:88, 4:115, 5:4, 5:6-7, 5:15, 5:18, 5:33, 5:63, 5:67, 5:106-107 |
| Identity and Access Management (IAM) | 1:6, 1:20, 1:23, 1:87, 2:4, 3:5-6, 3:10, 3:12-19, 3:22-26, 3:34, 3:36-37, 3:40-45, 3:48, 3:50-51, 3:53, 3:57-58, 3:61, 3:65, 3:67, 3:69, 3:73, 3:85, 3:114-115, 3:137, 3:146-147, 3:154-155, 4:20, 4:24-25, 4:31-32, 4:45-47, 4:54, 4:62, 5:6-7, 5:9, 5:14-15, 5:17, 5:25, 5:27, 5:29, 5:32-34, 5:39-40, 5:54, 5:78, 5:104, 5:106-107, 5:109 |
| imageId | 3:70 |
| Impact | 1:25, 1:27, 1:57, 2:4, 2:70, 2:105, 3:6, 3:23, 3:65, 4:75, 4:77, 4:138, 5:62 |
| Infrastructure as a Service (IaaS) | 1:3, 1:18, 5:73 |
| Initial Access | 4:95, 4:141 |
| Internet Gateway | 3:95-96, 3:98, 3:102-103 |
| Internet Information Services (IIS) | 2:78, 3:91 |
| Internet Message Access Protocol (IMAP) | 1:52, 1:56, 1:59 |
| invocation id | 1:115, 3:143, 3:149-150, 5:89, 5:99, 5:102 |

# J

|  |  |
| --- | --- |
| JavaScript Object Notation (JSON) | 1:13, 1:36, 1:40, 1:42-43, 1:89, 1:118, 1:121, 2:6, 2:36, 2:41-42, 2:79, 2:111, 3:15, 3:31, 3:38, 3:90, 3:133, 4:32, 4:78, 4:81, 4:108, 5:28, 5:43, 5:64 |

# K

|  |  |
| --- | --- |
| Key Logs | 1:23, 2:51, 4:28, 4:35, 4:81 |
| keyName | 3:70 |
| Kibana | 1:11, 2:107-110 |
| Kroll Artifact Parser and Extractor (KAPE) | 2:86 |
| Kube-APIServer | 4:24-25, 4:28, 4:47, 4:50-51, 4:54 |
| Kube-Scheduler | 4:20 |
| Kubelet | 4:24-26, 4:45 |
| Kubernetes | 1:4, 1:13-14, 1:19-20, 3:136, 3:147, 4:1, 4:4-5, 4:7-11, 4:13-14, 4:16, 4:18-20, 4:22, 4:24-35, 4:39-42, 4:44-51, 4:53-55, 4:57-59, 4:62, 5:36, 5:39, 5:56, 5:73, 5:125 |
| Kusto Query Language (KQL) | 2:54, 3:148 |

# L

|  |  |
| --- | --- |
| Lag Time | 3:28, 4:77 |
| Lambda | 1:19, 1:29, 3:15, 3:18, 3:28, 3:32, 3:49, 3:119, 3:142-147, 3:149-152, 3:157, 3:159, 5:73 |
| Lateral Movement | 2:18, 3:158, 4:18, 4:21, 5:26-27 |
| Lightsail | 3:55, 3:75-76, 3:92, 3:94, 5:73 |
| Load Balancer | 2:105-106, 3:65, 3:95, 3:100-102, 3:118, 3:130, 3:136 |
| Log Analytics | 1:29, 2:16, 2:47-55, 2:60-61, 2:65, 2:78, 2:97, 2:103, 2:112, 2:123, 4:28-30, 4:35, 5:128 |
| Log Buckets | 4:33, 5:44, 5:46, 5:60, 5:62, 5:66-67 |
| Log Explorer | 1:29, 3:34, 4:38, 4:88, 5:43, 5:123 |
| Log Ingestion | 1:33, 3:134, 4:78 |
| Log Retention | 1:31, 4:88 |
| Log Storage | 1:20, 5:45, 5:51 |
| Logstash | 1:11-14, 2:17, 2:38, 2:116, 3:38, 4:108 |

# M

|  |  |
| --- | --- |
| Mail Clients | 1:34, 1:56, 4:106 |
| MailItemsAccessed | 1:33-34, 1:47-48, 1:50-54, 1:57-59, 1:69, 1:77, 1:82, 1:120 |
| Management Event | 3:28, 3:31-32, 3:125 |
| Management groups | 2:4 |
| Metadata Service | 2:81, 2:92, 3:52, 4:53-54, 4:59 |
| Metrics | 2:78, 3:7, 3:91, 3:130, 4:19, 4:30 |
| Microsoft 365 | 1:1, 1:3, 1:12-13, 1:18, 1:31, 1:33, 1:35-38, 1:42-45, 1:47, 1:74, 1:87, 1:97, 1:102-105, 1:121, 2:68, 2:125, 3:29, 3:36, 3:38 |
| Microsoft Graph API | 1:3, 1:35, 1:53, 1:102-105, 1:120, 2:51, 2:68 |
| Microsoft Incident Response Playbooks | 2:122, 2:125 |
| Microsoft Purview | 1:24, 1:35-36, 1:48, 1:60-62 |
| MITRE ATT&CK | 2:126, 4:82, 4:85-86 |
| MoveToDeletedItems | 1:47-48, 1:82 |
| MultiFactor Authentication (MFA) | 1:37, 1:87, 1:95, 1:111, 2:24-27, 2:35, 3:25, 3:44-45, 4:29, 4:99-100, 4:138 |

# N

|  |  |
| --- | --- |
| NetFlow | 1:13, 1:21, 1:26, 3:105, 3:118 |
| Network Address Translation (NAT) | 2:104, 3:98, 4:13 |
| Network Security Group (NSG) | 2:63, 2:73, 2:98, 2:104, 2:106-113, 3:95-98, 3:104, 3:145 |
| Node.js | 3:143, 5:71 |
| Nodes | 4:9-10, 4:13-14, 4:20, 4:25, 4:28, 4:31-33, 4:39, 4:45 |
| NSG flow logs | 2:111-113 |

# O

|  |  |
| --- | --- |
| OAuth | 1:43, 1:88, 1:100, 1:102, 2:81, 4:75, 4:77, 4:80, 4:83, 4:88, 4:97, 4:115-122, 4:126-129, 5:63, 5:67, 5:79 |
| OAuth Abuse | 4:126-128 |
| OAUTH Token | 1:102, 4:115, 4:119 |
| OneDrive | 1:31, 1:33-34, 1:46-47, 1:70-71, 1:76, 1:78-79, 1:86, 4:136 |
| operationName | 2:20, 2:24, 2:32, 2:34-35, 2:38-39, 2:58-59, 2:100, 2:102, 2:108, 2:110 |
| Ops Agent | 5:96-97 |
| Organizational Unit | 3:16, 4:67-68, 4:72 |
| Outlook | 1:47, 1:52-53, 1:55-59, 1:82-83 |
| Outlook Web Access (OWA) | 1:52, 1:54, 1:56, 1:59 |

# P

|  |  |
| --- | --- |
| Packet Capture (PCAP) | 1:26, 3:96 |
| Page blobs | 2:96 |
| PageViewed | 1:34, 1:79 |
| Permissions | 1:23, 1:37-38, 1:43, 1:47, 1:49, 1:77, 1:82, 1:87, 1:102, 1:105, 1:108-111, 1:113, 1:121-122, 2:5, 2:7, 2:11-12, 2:14, 3:12, 3:16-17, 3:25, 3:37, 3:57, 3:61, 3:116-117, 3:126, 3:128, 3:137, 4:46, 4:49, 4:67, 4:71-72, 4:80, 4:130, 4:141-142, 5:4-5, 5:7-17, 5:19, 5:24, 5:26-28, 5:30, 5:32-33, 5:54-55, 5:60, 5:77, 5:79, 5:93, 5:104, 5:106-108, 5:113, 5:116 |
| Persistence | 1:97, 1:102, 1:123, 3:155, 4:91, 4:113, 5:76 |
| Persistent Disks | 1:29, 5:76 |
| Phishing | 1:65, 1:68, 2:125, 3:113, 4:80, 4:111, 4:113 |
| PHP | 1:103, 5:71 |
| Platform as a Service (PaaS) | 1:3, 1:18, 1:20, 5:73 |
| Playbooks | 2:122, 2:125, 3:154 |
| Pods | 4:8-10, 4:13-14, 4:21, 4:30, 4:33-34, 4:46-48, 4:50, 4:54-55 |
| Policy Simulator | 3:22-23 |
| PowerShell | 1:13, 1:24, 1:32, 1:35, 1:37-38, 1:40-45, 1:61, 1:103, 1:112, 1:121, 2:6, 2:10, 2:13, 2:41, 2:49-50, 2:76-77, 2:79-83, 2:100, 2:119-120, 2:126, 3:143, 3:155 |
| Prefixes | 3:51-52 |
| Pricing | 1:21, 1:27-28, 2:70-71, 2:124, 3:67, 3:81, 3:104, 3:118, 3:132, 3:143-144, 3:152 |
| Pricing Calculators | 1:28 |
| privateIpAddress | 3:89-90 |
| Privilege Escalation | 3:53, 5:116 |
| PST | 1:90 |
| Purview Compliance Portal | 1:24, 1:35-36, 1:40, 1:44-45, 1:48, 1:60-62, 1:87 |
| Python | 1:24, 1:103, 2:78-79, 2:116, 3:32, 3:34, 3:53-54, 3:86, 3:122, 3:143, 4:85, 4:128, 5:71, 5:89 |

# Q

|  |  |
| --- | --- |
| Quarantine | 1:60-61, 3:151, 4:80, 4:113-114, 4:138 |
| Query Builder | 5:61 |
| Query Logs | 3:59, 3:106-107, 3:135 |
| Queue | 1:29, 1:36, 2:95, 2:97, 2:99-100, 5:43 |
| Queue Storage | 2:95 |
| Quicksight | 3:40 |

# R

|  |  |
| --- | --- |
| Regions | 1:28, 2:70, 2:104, 3:32, 3:67-68, 3:80, 3:107, 4:64 |
| Relational Database Service (RDS) | 3:28 |
| Remote Desktop Protocol (RDP) | 2:106-107, 3:60 |
| requestParameters | 3:38, 3:45-47, 3:70, 3:86, 3:89, 3:122 |
| Resolver | 3:106-109, 3:136-137 |
| resourceId | 2:24, 2:38-39, 2:108, 2:110, 4:36 |
| responseBodySize | 2:102 |
| responseElements | 3:38, 3:44-46, 3:48, 3:86, 3:90 |
| RESTful | 1:103-104, 3:146 |
| resultSignature | 2:24, 2:39, 2:108 |
| resultType | 2:20, 2:24, 2:39, 2:54, 2:57 |
| RFC 1918 | 2:104, 3:96 |
| RiskyServicePrincipals | 2:51 |
| RiskyUsers | 2:51 |
| Role-Based Access Control (RBAC) | 2:6-7, 2:11, 3:25, 4:19, 4:29, 4:31-32, 4:52, 5:4 |
| Root Account | 3:5, 3:7, 3:13, 3:16, 3:24, 3:37, 3:41, 3:45, 3:60 |
| Route 53 | 3:106-109, 3:130 |
| Routing | 3:95, 3:97-98, 3:100, 5:38, 5:43, 5:45 |

# S

|  |  |
| --- | --- |
| S3 | 1:29, 1:53, 3:10, 3:14, 3:16-17, 3:19-21, 3:27-29, 3:31-34, 3:40, 3:54, 3:76, 3:91, 3:96, 3:100, 3:103-104, 3:107, 3:113-127, 3:130-132, 3:134-137, 3:140, 3:143-146, 3:150-151, 4:31, 4:37, 5:4, 5:98 |
| S3 Browser | 3:33 |
| S3 Logging | 3:125, 3:131 |
| SAML | 1:97, 3:55, 4:97 |
| Secure Shell (SSH) | 2:106-107, 3:60, 3:70, 3:99, 3:140, 3:154, 5:98, 5:101, 5:130 |
| Security Assertion Markup Language (SAML) | 1:97, 4:97 |
| Security Information and Event Management (SIEM) | 1:3, 1:6, 1:9, 1:12, 1:18, 1:31, 1:35, 1:42, 1:44-45, 2:16, 2:66, 2:68, 2:76-77, 2:112, 2:123, 3:29, 3:59, 3:131, 3:138, 3:150, 4:77, 4:135, 5:43, 5:70 |
| Security Operations and Forensics ELK (SOF-ELK) | 1:3, 1:6, 1:9, 1:12-13, 1:15, 1:26, 1:31, 1:36, 1:42, 1:46, 2:17, 2:37-38, 2:60, 2:73, 2:75, 2:79, 2:116, 3:69, 3:108-109, 4:81-82, 4:84, 4:108, 4:137, 5:128 |
| Security Orchestration Automated Response (SOAR) | 2:123 |
| Security Token Service (STS) | 1:91, 3:10, 3:16, 3:24-25, 3:36, 3:40, 3:42, 3:50-52, 3:55, 3:69, 3:73, 3:115, 4:54 |
| SecurityHub | 3:142 |
| Sentinel | 2:122-124 |
| Serverless | 1:19, 1:29, 3:15, 3:49, 3:142-143, 3:147, 3:151, 5:73-74 |
| Service Account | 1:23, 1:94, 3:24, 3:42, 4:46, 4:50, 4:92, 5:6-7, 5:9, 5:12, 5:14, 5:23, 5:25-34, 5:37, 5:65, 5:77-79, 5:83, 5:85-86, 5:105 |
| ServicePrincipalRiskEvents | 2:51 |
| sessionCredentialFromConsole | 3:38 |
| Set-Mailbox | 1:47, 1:68-69 |
| Shared Access Signature (SAS) | 2:93, 2:99-102, 5:104 |
| Shared Responsibility Model | 1:21-22 |
| SharePoint | 1:3, 1:31, 1:33-34, 1:42, 1:45-47, 1:62, 1:70-72, 1:76, 1:79-80, 1:82-83, 1:86, 1:104 |
| Signin | 1:43, 1:93, 1:109, 1:114, 1:118, 2:14, 2:17, 2:20-21, 2:23-24, 2:28, 2:31, 2:54, 2:56-57, 3:45, 3:49, 3:99, 4:91, 5:37 |
| Simple Queue Service (SQS) | 1:29 |
| Simple Storage Service (S3) | 1:29 |
| Sinks | 5:38-39, 5:43-44, 5:46-48, 5:50, 5:60-61, 5:66, 5:68, 5:70-71 |
| Sites | 1:110, 1:122 |
| Snapshot | 1:21, 1:25, 1:27, 2:72, 2:77, 2:82, 2:85-88, 2:90-91, 2:93, 3:70, 3:76, 3:80-86, 3:92, 3:94, 3:118, 3:145, 4:14, 4:39, 5:84-91, 5:95, 5:99-102 |
| Snapshotid | 3:82, 3:86 |
| SoftDelete | 1:47-48, 1:82 |
| Software as a Service (SaaS) | 1:3-4, 1:18, 4:95 |
| Software Development Kit (SDK) | 1:24, 3:24, 3:38, 3:51, 4:81, 4:83 |
| SolarWinds | 1:102, 1:120 |
| source\_ip | 3:108-109 |
| sourceIPAddress | 3:36, 3:44-47, 3:70, 3:89, 3:122 |
| Splunk Common Information Model | 1:9 |
| Step Functions | 3:135, 3:142, 3:152 |
| Storage Explorer | 2:60-61, 2:64, 2:79, 2:96, 2:101-102, 2:116, 2:119-120, 4:36 |
| Stream | 2:14, 2:66, 3:91, 3:147-150, 4:16, 4:18, 4:20, 4:24-25, 4:30, 4:33, 4:47, 4:50-51, 4:54 |
| Subnet | 1:26, 2:104, 2:106, 2:110-111, 2:113, 3:18, 3:65, 3:68, 3:88-90, 3:95-99, 3:101-105, 3:145, 3:159, 5:122-123, 5:126, 5:131-132 |
| Sync | 1:51-52, 1:56-58, 1:70, 1:78, 3:31, 3:33, 3:114, 3:122, 3:151 |
| Systems Manager | 3:154-156 |

# T

|  |  |
| --- | --- |
| Table Storage | 2:95 |
| Takeout | 4:75, 4:81-82, 4:133-139, 4:141-142 |
| Teams | 1:3, 1:31, 1:70, 3:147-149, 3:151 |
| Threat Hunting | 1:111, 1:126, 2:127, 3:57, 3:150, 4:59, 5:136 |
| Throttling | 1:52 |
| Token | 1:16, 1:88-91, 1:102, 1:105, 1:112, 1:114, 1:116, 2:25, 2:27, 2:35, 2:81, 2:92-93, 2:102, 3:10, 3:16, 3:24-25, 3:36, 3:40, 3:42, 3:50-51, 3:55, 3:73, 3:114-115, 3:146, 4:29, 4:46-47, 4:50, 4:80, 4:97, 4:115, 4:119, 4:126, 4:129, 5:27-28, 5:79 |
| Traffic Analytics | 2:111-112 |
| Transfer Acceleration | 3:119-121 |

# U

|  |  |
| --- | --- |
| Unified Audit Log (UAL) | 1:13, 1:31-33, 1:35-36, 1:38-44, 1:46, 1:57, 1:60, 1:92, 1:95, 1:98-100, 1:120, 3:38 |
| Unified Data Model | 1:9 |
| Uniform Resource Identifier (URI) | 1:114, 1:120, 2:8-10, 3:123, 5:115 |
| UpdateCalendarDelegation | 1:49, 1:82 |
| UpdateFolderPermissions | 1:49, 1:82 |
| UpdateInboxRules | 1:47, 1:49, 1:82 |
| Usage Reports | 4:81 |
| User Log | 1:95, 3:47, 4:79, 4:94-96, 4:98 |
| user\_id | 1:16 |
| user\_principal\_name | 2:43, 2:90, 2:117 |
| userAgent | 1:16, 2:24, 2:102, 3:38, 3:44-47, 3:70, 3:86, 3:89, 3:122, 4:24-26, 4:46-48, 4:50-51, 4:54-55, 5:85, 5:87, 5:89, 5:110-113 |
| userAgentHeader | 2:102 |
| userIdentity | 3:36-37, 3:45, 3:47, 3:69, 3:85, 3:122, 3:133 |
| UserLoggedIn | 1:33-34, 1:41, 1:94 |
| UserRiskEvents | 2:51 |

# V

|  |  |
| --- | --- |
| Vault | 4:66, 4:77, 4:89, 4:102, 4:138 |
| Virtual Hard Drive (VHD) | 1:25, 2:87, 2:96 |
| Virtual Network (VNet) | 1:20, 1:26, 1:29, 2:6-7, 2:73, 2:104, 2:106, 2:111, 2:113, 3:18, 3:95, 3:100, 3:104 |
| Virtual Private Cloud (VPC) | 1:13, 1:29, 3:10, 3:12, 3:59, 3:90, 3:95-98, 3:100, 3:102-107, 3:111, 3:130, 3:136-137, 3:140, 3:145, 3:147-148, 4:18, 4:47, 5:56, 5:94, 5:117, 5:122-125, 5:127-130, 5:133-134 |
| Virtual Private Network (VPN) | 2:104-105, 5:117 |
| Virtual router | 2:105 |
| VNet | 1:29, 2:104, 2:110 |
| Volumeid | 3:82, 3:86 |
| volumeSize | 3:79, 3:82, 3:86 |
| volumeType | 3:79 |
| VPC Flow Logs | 1:13, 3:12, 3:59, 3:103, 3:111, 3:130, 3:136-137, 3:140, 3:147-148, 5:122-123, 5:127-128, 5:133 |
| VPC Subnets | 3:97 |
| vpcId | 3:90 |
| VPN gateway | 2:104-105 |

# W

|  |  |
| --- | --- |
| WAN optimization appliance | 2:105 |
| Web Application Firewalls (WAFs) | 3:65, 3:95, 3:100 |
| Windows Azure Diagnostics (WAD) | 2:78-79 |