|  |  |  |
| --- | --- | --- |
| Policy Name | Relevant to GKE Autopilot? | Why? |
| active-directory-domain-restrict-default-setupadmin | Yes | Integrates with GKE for secure identity management. |
| active-directory-ensure-to-use-approved-domain-names | Yes | Enforces naming standards for Active Directory domains integrated with GKE. |
| active-directory-ensure-to-use-approved-locations | Yes | Ensures compliance and optimizes performance when using Active Directory with GKE. |
| api-gateway-ensure-to-use-approved-regions | Yes | API Gateways can integrate with Istio in GKE; using approved regions maintains security and compliance. |
| api-gateway-restrict-usage-of-default-service-account | Yes | Enhances GKE security by restricting the default service account. |
| apigee-ensure-custom-roles-with-least-privilege | Yes | Minimizes permissions and attack surface in GKE integrations. |
| apigee-ensure-disk-encryption-used | Yes | Adds extra security for sensitive information in GKE Autopilot. |
| apigee-ensure-runtime-database-encryption-used | Yes | Protects sensitive Apigee data in GKE deployments. |
| apigee-ensure-to-use-approved-region | Yes | Ensures GKE and Apigee deployments comply with regional policies. |
| apigee-restrict-predefined-iam-roles | No | Not directly relevant to GKE. |
| artifact-registry-use-approved-kms-keys | Yes | Ensures GKE Autopilot uses approved keys for container images. |
| assetInventory-feeds-publish-to-topic-within-same-project | Yes | Enhances GKE resource tracking security. |
| bigquery-dataset-in-multiregion-for-ha | Yes | Improves availability for GKE apps accessing BigQuery. |
| bigquery-dataset-table-partition-expiration-time | Yes | Manages BigQuery storage costs and data retention for GKE apps. |
| bigquery-ensure-to-use-cmek | Yes | Protects BigQuery data accessed by GKE workloads. |
| bigquery-restrict-usage-of-bigquery-connection | Yes | Controls GKE workload access to external data sources. |
| bigquery-restrict-usage-of-bigquery-migration | Yes | Secures data transfers to BigQuery from GKE workloads. |
| bigquery-service-account-key-rotation | Yes | Enhances security for GKE workloads accessing BigQuery. |
| bigquery-use-approved-regions | Yes | Aligns BigQuery usage with regional policies for GKE workloads. |
| bigtable-enable-garbage-collection | Yes | Improves Bigtable performance for GKE apps. |
| bigtable-ensure-cluster-replication | Yes | Ensures high availability for Bigtable data used by GKE. |
| bigtable-ensure-to-use-cmek | Yes | Enhances security for GKE apps accessing Bigtable. |
| bigtable-must-interact-with-services-within-perimeter | Yes | Adds security layer for GKE workloads accessing Bigtable. |
| bigtable-restrict-privileged-roles | Yes | Enhances Bigtable security for GKE workloads. |
| bigtable-use-approved-regions | Yes | Enhances Bigtable security for GKE workloads. |
| binary-authorization-ensure-pkixkey-used | Yes | Enhances GKE Autopilot security with PKIX keys for images. |
| binary-authorization-to-use-cluster-admission-rule | Yes | Enforces cluster-specific admission rules for GKE Autopilot. |
| binary-authorization-to-use-default-admission-rule | Yes | Enforces default admission rules for GKE Autopilot deployments. |
| cloudbuild-ensure-image-configured | Yes | Relevant if using Cloud Build for GKE deployments. |
| cloudbuild-ensure-kms-key-is-defined | Yes | Relevant if using Cloud Build with CMEK for GKE. |
| cloudbuild-ensure-machinetype-defined-for-build-trigger | Yes | Optimizes Cloud Build performance for GKE deployments. |
| cloudbuild-ensure-machinetype-defined-for-workerpool | Yes | Optimizes Cloud Build performance for GKE deployments. |
| cloudbuild-ensure-pubsub-triggers-defined | Yes | Relevant if using Pub/Sub to trigger GKE Autopilot builds. |
| cloudbuild-ensure-storageSource-defined | Yes | Optimizes Cloud Build performance for GKE Autopilot. |
| cloudbuild-ensure-to-use-approved-repositories | Yes | Ensures Cloud Build uses approved repositories for GKE Autopilot. |
| cloudbuild-restrict-default-vpc-network | Yes | Enhances security for GKE Autopilot-related builds. |
| cloudbuild-restrict-external-ip | Yes | Enhances security for GKE Autopilot-related builds. |
| cloudbuild-restrict-webhook-triggers | Yes | Enhances security for GKE Autopilot deployments. |
| cloudbuild-serviceAccount-explicitly-defined | Yes | Improves security and auditing for GKE Autopilot builds. |
| cloudbuild-workerpool-resources-must-use-approved-regions | Yes | Aligns Cloud Build workerpool locations with regional policies for GKE Autopilot. |
| cloudidentity-ensure-to-use-sso-idp-and-service-provider | Yes | Enables centralized identity management for GKE. |
| cloudidentity-restrict-group-creation | Yes | Indirectly enhances GKE security through access control. |
| cloudrun-ensure-to-allow-internal-traffic | Yes | Secures communication between GKE Autopilot and Cloud Run. |
| cloudrun-available-in-amex-approved-region | No | Not directly relevant to GKE. |
| cloudrun-ensure-to-use-gen2 | Yes | Aligns Cloud Run usage with GKE Autopilot deployments. |
| cloudrun-restrict-default-service-account | No | Not directly relevant to GKE Autopilot. |
| cloudrun-restrict-unauthenticated-access | No | Not directly relevant to GKE Autopilot. |
| cloudscheduler-ensure-to-use-approved-description-format | No | Not directly relevant to GKE Autopilot. |
| cloudscheduler-ensure-to-use-approved-regions | No | Not directly relevant to GKE Autopilot. |
| cloudscheduler-restrict-app-engine-target | No | Not directly relevant to GKE Autopilot. |
| cloudscheduler-restrict-default-service-account-for-http-targets | No | Not directly relevant to GKE Autopilot. |
| cloudsourcerepo-restrict-default-service-account | No | Not directly relevant to GKE Autopilot. |
| cloudspanner-ensure-to-enable-deletion-protection | Yes | Protects Spanner instances used by GKE Autopilot from accidental deletion. |
| cloudspanner-ensure-to-use-approved-region | Yes | Ensures Spanner instances used by GKE Autopilot comply with regional policies. |
| cloudspanner-ensure-to-use-cmek | Yes | Encrypts Spanner data used by GKE Autopilot with CMEK. |
| cloudspanner-restrict-iam-roles | Yes | Secures Spanner data accessed by GKE Autopilot by restricting IAM roles. |
| cloudspanner-restrict-public-access | Yes | Prevents public access to Spanner instances used by GKE Autopilot. |
| composer-and-network-must-use-same-project | No | Not directly relevant to GKE Autopilot. |
| composer-and-serviceaccount-must-use-same-project | No | Not directly relevant to GKE Autopilot. |
| composer-and-subnetwork-must-use-same-project | No | Not directly relevant to GKE Autopilot. |
| composer-disallow-privately-used-public-ips | No | Not directly relevant to GKE Autopilot. |
| composer-enable-private-endpoint | No | Not directly relevant to GKE Autopilot. |
| composer-ensure-to-use-cmek | No | Not directly relevant to GKE Autopilot. |
| composer-restrict-ip-masquerade | No | Not directly relevant to GKE Autopilot. |
| composer-use-approved-regions | No | Not directly relevant to GKE Autopilot. |
| compute-instance-enable-private-access | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-enforce-to-use-persistent-disks | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-ensure-connection-to-serial-port-is-not-enabled | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-ensure-integrity-monitoring-enabled-for-shielded-instance | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-ensure-secure-boot-enabled-for-shielded-instance | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-ensure-vm-google-image | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-ensure-vmdisk-cmek-encryption | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-ensure-vTPM-enabled-for-shielded-instance | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-restrict-disks-location | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-restrict-instance-location | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-restrict-internet-facing-ip | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-restrict-ip-forwarding-enabled | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-restrict-oslogin-enabled | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-restrict-projectwide-ssh-keys | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-restrict-snapshot-share-permission-in-customrole | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-restrict-snapshot-storage-location | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-restrict-vm-default-serviceaccount | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-restrict-vm-multiple-nic | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-instance-restrict-vm-serviceaccount-scope | No | Not directly relevant to GKE Autopilot (no VM management). |
| compute-snapshot-enable-cmek-encryption | No | Not directly relevant to GKE Autopilot (no VM management). |
| datacatalog-ensure-resources-within-same-project | Yes | Relevant if GKE Autopilot interacts with Data Catalog. |
| datacatalog-ensure-tag-templates-in-approved-region | Yes | Relevant if GKE Autopilot interacts with Data Catalog. |
| datacatalog-ensure-tag-uses-approved-template | Yes | Relevant if GKE Autopilot interacts with Data Catalog. |
| datacatalog-restrict-user-specified-system | Yes | Relevant if GKE Autopilot interacts with Data Catalog. |
| dataflow-ensure-bucket-in-same-project | Yes | Relevant if GKE Autopilot interacts with Dataflow. |
| dataflow-restrict-default-service-account | Yes | Relevant if GKE Autopilot interacts with Dataflow. |
| dataflow-restrict-enable-streaming-engine | Yes | Relevant if GKE Autopilot interacts with Dataflow. |
| dataflow-restrict-public-IP-for-jobs | Yes | Relevant if GKE Autopilot interacts with Dataflow. |
| dataflow-streaming-jobs-prime-dissallowed | Yes | Relevant if GKE Autopilot interacts with Dataflow. |
| dataflow-use-approved-regions | Yes | Relevant if GKE Autopilot interacts with Dataflow. |
| dataflow-use-same-project-for-subnetwork-and-dataflow-jobs | Yes | Relevant if GKE Autopilot interacts with Dataflow. |
| data-fusion-ensure-to-enable-logging-and-monitoring | Yes | Relevant if GKE Autopilot interacts with Data Fusion. |
| data-fusion-instance-use-approved-region | Yes | Relevant if GKE Autopilot interacts with Data Fusion. |
| data-fusion-must-use-private-instance | Yes | Relevant if GKE Autopilot interacts with Data Fusion. |
| data-fusion-restrict-dataproc-default-sa | Yes | Relevant if GKE Autopilot interacts with Data Fusion. |
| dataplex-block-metastore-configuration | Yes | Relevant if GKE Autopilot interacts with Dataplex. |
| dataproc-cluster-creation-approved-region | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-disable-http-access | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-ensure-allowed-image-version | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-ensure-allowed-optional-components | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-ensure-cluster-network-tags-used | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-ensure-initialization-actions-reference-to-bucket | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-ensure-notebooks-reside-within-same-project-as-dataproc | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-ensure-spark-job-driver-logs-enabled | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-ensure-storageaccess-in-same-project | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-ensure-to-use-internalIp-only | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-image-compatible-with-component-gateway | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-mustbe-accessed-via-private-access | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-restrict-auto-creation-of-staging-bucket | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-restrict-auto-creation-of-temp-bucket | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-restrict-cross-realm-trust-access-with-kdc | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-restrict-default-service-account | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dataproc-temp-staging-bucket-from-same-project | Yes | Relevant if GKE Autopilot interacts with Dataproc. |
| dns-ensure-cloud-dns-logging | Yes | Relevant if GKE Autopilot uses Cloud DNS. |
| dns-ensure-nsec3-DoS-protection | Yes | Relevant if GKE Autopilot uses Cloud DNS. |
| dns-ensure-to-use-approved-ip-for-forwarding-config | Yes | Relevant if GKE Autopilot uses Cloud DNS. |
| dns-ensure-to-use-private-routing | Yes | Relevant if GKE Autopilot uses Cloud DNS. |
| dns-ensure-zonal-dns-enabled | Yes | Relevant if GKE Autopilot uses Cloud DNS. |
| dns-restrict-cross-project-binding | Yes | Relevant if GKE Autopilot uses Cloud DNS. |
| dns-restrict-inbound-forwarding | Yes | Relevant if GKE Autopilot uses Cloud DNS. |
| dns-restrict-peering-for-managed-zones | Yes | Relevant if GKE Autopilot uses Cloud DNS. |
| dns-restrict-public-DNS-zones | Yes | Relevant if GKE Autopilot uses Cloud DNS. |
| dns-restrict-service-directory | Yes | Relevant if GKE Autopilot uses Cloud DNS. |
| function-allow-ingress-setting-to-allow-internal | Yes | Relevant if GKE autopiloy uses Cloud Functions |
| function-in-approved-regions | Yes | Relevant if GKE Autopilot interacts with Cloud Functions. |
| function-restrict-default-service-account | Yes | Relevant if GKE Autopilot interacts with Cloud Functions. |
| function-restrict-egress-to-internet | Yes | Relevant if GKE Autopilot interacts with Cloud Functions. |
| function-restrict-publicly-deployed | Yes | Relevant if GKE Autopilot interacts with Cloud Functions. |
| gke-enable-workload-identity-config | Yes | Improves GKE workload security. |
| gke-restrict-cloudrun-config | Yes | Controls GKE integration with Cloud Run. |
| gke-cloud-logging-enabled | Yes | Enhances GKE logging. |
| gke-cloud-monitoring-enabled | Yes | Enhances GKE monitoring. |
| gke-ensure-alpha-cluster-feature-disabled | Yes | Improves GKE stability. |
| gke-ensure-auth-using-client-cert-is-disabled | Yes | Enhances GKE security. |
| gke-ensure-auto-repair-must-be-enabled | Yes | Ensures GKE cluster health. |
| gke-ensure-auto-update-must-be-enabled | Yes | Ensures GKE cluster is up-to-date. |
| gke-ensure-binary-auth-enabled | Yes | Improves GKE security. |
| gke-ensure-boot-disk-encryption-enabled | Yes | Enhances GKE security. |
| gke-ensure-explicit-deny-firewall-used | Yes | Improves GKE security. |
| gke-ensure-gke-metadata-server-enabled | Yes | Required for GKE Autopilot. |
| gke-ensure-high-availability | Yes | Ensures GKE cluster availability. |
| gke-ensure-ip-alias-enabled | Yes | Improves GKE networking. |
| gke-ensure-legacy-auth-disabled | Yes | Enhances GKE security. |
| gke-ensure-master-authorized-networks-enabled | Yes | Improves GKE security. |
| gke-ensure-metadata-service-disabled | Yes | Enhances GKE security. |
| gke-ensure-pod-security-policy-enabled | Yes | Improves GKE security. |
| gke-ensure-release-channelproperty-set | Yes | Ensures GKE cluster stability. |
| gke-ensure-sandbox-config-enabled | Yes | Improves GKE security. |
| gke-ensure-secure-boot-enabled | Yes | Enhances GKE security. |
| gke-ensure-use-kubernetes-rbac | Yes | Enhances GKE security. |
| gke-ensure-vpc-native-clusters | Yes | Improves GKE networking. |
| gke-integrity-monitoring-enabled | Yes | Enhances GKE security. |
| gke-intranode-visibility-enabled | Yes | Improves GKE security. |
| gke-must-use-container-optimized-os | Yes | Improves GKE performance and security. |
| gke-must-use-private-clusters | Yes | Enhances GKE security. |
| gke-must-use-shielded-nodes | Yes | Improves GKE security. |
| gke-network-policy-enabled | Yes | Enhances GKE security. |
| gke-restrict-database-encryption-disabled | Yes | Enhances GKE security. |
| gke-restrict-ipv6 | Yes | Controls GKE networking. |
| gke-restrict-manual-cluster-container-creation | Yes | Improves GKE security. |
| gke-restrict-over-privileged-accounts | Yes | Enhances GKE security. |
| gke-restrict-over-privileged-scopes | Yes | Enhances GKE security. |
| gke-restrict-pod-container-privilege-escalation | Yes | Improves GKE security. |
| gke-restrict-pod-containers-run-as-root | Yes | Improves GKE security. |
| iam-ensure-automatic-grants-for-default-sa-disabled | Yes | Enhances GKE security. |
| iam-ensure-serviceacc-groups-naming-convention | Yes | Improves GKE security management. |
| iam-ensure-to-use-custom-roles-only | Yes | Enhances GKE security. |
| iam-restrict-access-to-saac-at-project-folder-level | Yes | Improves GKE security management. |
| iam-restrict-api-key-usage | Yes | Enhances GKE security. |
| iam-restrict-attribute-mapping-aws | No | Not directly relevant to GKE. |
| iam-restrict-domain-wide-delegation | Yes | Enhances GKE security. |
| iam-restrict-external-cloud-idp | Yes | Enhances GKE security. |
| iam-restrict-permission-changes-custom-roles | Yes | Enhances GKE security. |
| iam-restrict-permissions-to-approved-domains-only | Yes | Enhances GKE security. |
| iam-restrict-permissions-to-users | Yes | Enhances GKE security. |
| iam-restrict-serviceaccount-impersonation | Yes | Enhances GKE security. |
| iam-restrict-usage-of-primitive-iam-roles | Yes | Enhances GKE security. |
| iam-restrict-user-creation | Yes | Enhances GKE security. |
| iam-restrict-user-manged-keys-for-serviced-accounts | Yes | Enhances GKE security. |
| kms-ensure-to-create-kms-key-in-approved-regions | Yes | Aligns KMS key creation with regional policies for GKE. |
| kms-ensure-to-use-approved-encryption-algorithms | Yes | Enforces encryption standards for GKE. |
| kms-ensure-to-use-keys-rotation | Yes | Enhances key security for GKE. |
| kms-import-of-keys-disallowed | Yes | Enhances key security for GKE. |
| kms-restrict-cloudkms-in-perimeter-perimeters | Yes | Restricts access to Cloud KMS within specific perimeters for GKE. |
| kms-restrict-hsm-keys | Yes | Limits the use of HSM-backed keys for GKE, potentially impacting performance. |
| kms-restrict-usage-of-ekms | Yes | Restricts the use of external KMS for GKE. |
| kms-soft-deletion-state-duration | Yes | Impacts key recovery options for GKE. |
| load-balancer-enable-health-check-logging | Yes | Relevant if GKE Autopilot uses load balancers. |
| load-balancer-ensure-SSLCertififate-minTLSVersion-and-profile | Yes | Relevant if GKE Autopilot uses load balancers. |
| load-balancer-ensure-forwarding-rules-uses-network-within-same-project | Yes | Relevant if GKE Autopilot uses load balancers. |
| load-balancer-ensure-forwarding-rules-uses-subnetwork-within-project | Yes | Relevant if GKE Autopilot uses load balancers. |
| load-balancer-ensure-forwarding-rules-uses-target-within-same-project | Yes | Relevant if GKE Autopilot uses load balancers. |
| load-balancer-resources-must-use-approved-regions | Yes | Relevant if GKE Autopilot uses load balancers. |
| load-balancer-restrict-external-load-balancer-org-level-policy | Yes | Relevant if GKE Autopilot uses load balancers. |
| load-balancer-restrict-extrenal-loadbalancer | Yes | Relevant if GKE Autopilot uses load balancers. |
| load-balancer-restrict-google-managed-ssl-cert | Yes | Relevant if GKE Autopilot uses load balancers. |
| load-balancer-restrict-internet-serverless-NEGs | Yes | Relevant if GKE Autopilot uses load balancers. |
| load-balancer-restrict-service-label | Yes | Relevant if GKE Autopilot uses load balancers. |
| load-balancer-restrict-target-pool | Yes | Relevant if GKE Autopilot uses load balancers. |
| load-balancer-restrict-usage-of-ipv6 | Yes | Relevant if GKE Autopilot uses load balancers. |
| logging-ensure-data-access-logs-are-enabled-for-approved-services | Yes | Improves logging for specific services used by GKE Autopilot. |
| logging-ensure-dataaccess-logs-enabled-by-default | Yes | Enhances GKE Autopilot logging. |
| logging-ensure-no-sink-configured-to-route-logs-outsideproject | Yes | Enhances GKE Autopilot logging security. |
| logging-restrict-aws-ec2-logs | No | Not directly relevant to GKE Autopilot. |
| logging-restrict-usage-of-exlusion-filters | Yes | Controls GKE Autopilot logging. |
| memcache-instances-to-use-approved-region | Yes | Relevant if GKE Autopilot uses Memorystore. |
| memorystore-enable-transit-encryption | Yes | Relevant if GKE Autopilot uses Memorystore. |
| memorystore-ensure-auth-enabled | Yes | Relevant if GKE Autopilot uses Memorystore. |
| memorystore-ensure-to-use-private-service-access | Yes | Relevant if GKE Autopilot uses Memorystore. |
| metadata-server-ensure-to-set-vmDnsSetting-to-zonalonly | No | Not directly relevant to GKE Autopilot (no VM management). |
| metadata-server-restrict-external-ip | No | Not directly relevant to GKE Autopilot (no VM management). |
| metadata-server-restrict-guest-attribute | No | Not directly relevant to GKE Autopilot (no VM management). |
| metadata-server-restrict-legacy-endpoint-access | No | Not directly relevant to GKE Autopilot (no VM management). |
| metadata-server-restrict-legacy-endpoints | No | Not directly relevant to GKE Autopilot (no VM management). |
| metadata-server-restrict-nic-forwardedIP | No | Not directly relevant to GKE Autopilot (no VM management). |
| metadata-server-restrict-ssh-keys | No | Not directly relevant to GKE Autopilot (no VM management). |
| monitoring-ensure-to-use-pubsub-email-notification-channel | Yes | Enhances GKE Autopilot monitoring and alerting. |
| monitoring-ensure-to-use-same-project-for-notification-channel-alertpolicy | Yes | Improves organization and security for GKE Autopilot monitoring. |
| monitoring-restrict-aws-scopes | No | Not directly relevant to GKE Autopilot. |
| monitoring-restrict-external-metrics | Yes | Controls external metrics in GKE Autopilot monitoring. |
| monitoring-restrict-to-disable-monitoring-api | Yes | Restricts access to the monitoring API for GKE Autopilot. |
| monitoring-uptime-check-to-use-specific-region | Yes | Ensures regional consistency for GKE Autopilot uptime checks. |
| pubsub-ensure-deadletter-topic-and-subscription-uses-same-project | Yes | Relevant if GKE Autopilot uses Pub/Sub. |
| pubsub-ensure-publisher-and-subscription-uses-same-project | Yes | Relevant if GKE Autopilot uses Pub/Sub. |
| pubsub-restrict-gmek-use-for-topics | Yes | Relevant if GKE Autopilot uses Pub/Sub. |
| pubsub-restrict-http-endpoint | Yes | Relevant if GKE Autopilot uses Pub/Sub. |
| pubsub-restrict-messages-storage-location | Yes | Relevant if GKE Autopilot uses Pub/Sub. |
| pubsub-restrict-public-access-to-topics | Yes | Relevant if GKE Autopilot uses Pub/Sub. |
| pubsub-restrict-push-subscription | Yes | Relevant if GKE Autopilot uses Pub/Sub. |
| pubsub-restrict-usage-of-pubsub-lite | Yes | Relevant if GKE Autopilot uses Pub/Sub. |
| pubsub-topic-message-retention | Yes | Relevant if GKE Autopilot uses Pub/Sub. |
| resource-manager-ensure-all-categories-defined-for-essential-contacts | Yes | Improves contact management for GKE Autopilot projects. |
| resource-manager-restrict-user-project-creation-permission | Yes | Enhances security for GKE Autopilot projects. |
| sql-enforce-required-user-labels | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-ensure-to-use-encryption | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-instance-ensure-to-use-private-ip | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-instance-restrict-public-ip-access | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-instance-use-approved-regions | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-ensure-approved-versions-allowed | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-ensure-authorized-cidr-connections | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-ensure-cloning-from-same-project | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-ensure-cloudiam-userauthentication | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-ensure-dbflag-contained-database-auth-off | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-ensure-dbflag-local-infile-off | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-ensure-pgaudit-log-must-set-to-all | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-ensure-tls-enabled | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-ensure-to-enable-pgaudit-flag | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-ensure-dbflag-cross-db-ownership-chaining-off | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| sql-multiRegion-backup-location-use-approved-regions | Yes | Relevant if GKE Autopilot interacts with Cloud SQL. |
| storage-buckets-must-be-encrypted | Yes | Relevant if GKE Autopilot uses Cloud Storage. |
| storage-ensure-uniform-bucket-level-access-enabled | Yes | Relevant if GKE Autopilot uses Cloud Storage. |
| storage-restrict-bucket-access-owner-domain | Yes | Relevant if GKE Autopilot uses Cloud Storage. |
| storage-restrict-public-access-to-buckets | Yes | Relevant if GKE Autopilot uses Cloud Storage. |
| storage-restrict-region-for-buckets | Yes | Relevant if GKE Autopilot uses Cloud Storage. |
| storage-restrict-unapproved-domain-users-to-access-buckets | Yes | Relevant if GKE Autopilot uses Cloud Storage. |
| storage-standard-naming-convention-followed-for-buckets | Yes | Relevant if GKE Autopilot uses Cloud Storage. |
| vertex-ai-enable-monitoring | Yes | Relevant if GKE Autopilot uses Vertex AI. |
| vertex-ai-enforce-cmek | Yes | Relevant if GKE Autopilot uses Vertex AI. |
| vertex-ai-ensure-to-use-approved-region | Yes | Relevant if GKE Autopilot uses Vertex AI. |
| vertex-ai-restrict-cmek | Yes | Relevant if GKE Autopilot uses Vertex AI. |
| vertex-ai-restrict-kms-cloud-ekm | Yes | Relevant if GKE Autopilot uses Vertex AI. |
| vpc-block-egress-internet-traffic | Yes | Enhances GKE Autopilot network security. |
| vpc-block-ingress-internet-traffic | Yes | Enhances GKE Autopilot network security. |
| vpc-ensure-dynamic-routes-configured-using-vpn | Yes | Relevant if GKE Autopilot uses VPN. |
| vpc-ensure-to-access-allAPIs-using-private-service-connect | Yes | Enhances GKE Autopilot network security. |
| vpc-ensure-to-enable-firewall-rule-logs | Yes | Enhances GKE Autopilot network security. |
| vpc-ensure-to-enable-vpc-flow-logs | Yes | Enhances GKE Autopilot network security. |
| vpc-ensure-to-restrict-filters-on-flow-logs | Yes | Enhances GKE Autopilot network security. |
| vpc-restrict-auto-creation-of-subnetworks | Yes | Controls GKE Autopilot networking. |
| vpc-restrict-creation-of-external-ips | Yes | Controls GKE Autopilot networking. |
| vpc-restrict-default-network-creation | Yes | Controls GKE Autopilot networking. |
| vpc-restrict-host-project-creation | Yes | Controls GKE Autopilot networking. |
| vpc-restrict-ipv4-address-allocation | Yes | Controls GKE Autopilot networking. |
| vpc-restrict-ipv6-for-subnetworks | Yes | Controls GKE Autopilot networking. |
| vpc-restrict-network-peering | Yes | Controls GKE Autopilot networking. |
| vpc-restrict-non-owned-public-IPv4-for-routes | Yes | Controls GKE Autopilot networking. |
| vpc-restrict-packet-mirroring | Yes | Controls GKE Autopilot networking. |
| vpc-restrict-route-next-hop-to-internal-ipv4 | Yes | Controls GKE Autopilot networking. |
| vpc-restrict-service-project-creation | Yes | Controls GKE Autopilot networking. |
| vpcsc-approved-apis-must-reside-in-service-perimeter-perimeters | Yes | Enhances GKE Autopilot network security. |
| vpcsc-ensure-allowed-services-in-accessible-services-list | Yes | Enhances GKE Autopilot network security. |
| vpcsc-restrict-bridge-service-perimeter-perimeters | Yes | Enhances GKE Autopilot network security. |
| vpcsc-restrict-service-perimeter-perimeters-any-identity | Yes | Enhances GKE Autopilot network security. |
| vpcsc-restrict-service-perimeter-perimeters-wildcard-use | Yes | Enhances GKE Autopilot network security. |
| vpn-ensure-to-use-approved-peer-ip | Yes | Relevant if GKE Autopilot uses VPN. |
| vpn-ensure-to-use-approved-vpc | Yes | Relevant if GKE Autopilot uses VPN. |
| vpn-restrict-classicVPN | Yes | Relevant if GKE Autopilot uses VPN. |