>

ature is in a pre-release state and might change or have limited support. For more information, see the product launc
(/products/#product-launch-stages).

This page provides a list of reference guides and techniques for remediating Security Health Analytics findings using Security Command Center.

To help investigate security issues and monitor storage consumption, enable access logs and storage information for your Cloud Storage buckets. Access logs provide information for all of the requests made on a specified bucket, and the storage logs provide information about the storage consumption of that bucket.

To remediate this finding, set up logging for the bucket indicated by the Security Health Analytics finding by completing the access logs & storage logs (/storage/docs/access-logs) guide.

To help investigate security issues and monitor usage, it is recommended that you enable Stackdriver Logging (/monitoring/kubernetes-engine) on your clusters.

To remediate this finding:

1. Go to the Kubernetes clusters (https://console.cloud.google.com/kubernetes/list) page in the Cloud Console.
   Go to the Kubernetes clusters page (https://console.cloud.google.com/kubernetes/list)
2. Select the cluster listed in the Security Health Analytics finding.
3. Click **Edit**.

The edit button might be disabled if the cluster configuration recently changed. If you aren't able to edit the cluster settings, wait a few minutes and then try again.

4. On the **Legacy Stackdriver Logging** or **Stackdriver Kubernetes Engine Monitoring** drop-down list, select **Enabled**.

   These options aren't compatible. Make sure that you use either **Stackdriver Kubernetes Engine Monitoring** alone, or **Legacy Stackdriver Logging** with **Legacy Stackdriver Monitoring**.

5. Click **Save**.

To help investigate security issues and monitor usage, it is recommended that you enable Stackdriver Monitoring (/monitoring/kubernetes-engine) on your clusters.

To remediate this finding:

1. Go to the Kubernetes clusters (https://console.cloud.google.com/kubernetes/list) page in the Cloud Console.
   Go to the Kubernetes clusters page (https://console.cloud.google.com/kubernetes/list)
2. Select the cluster listed in the Security Health Analytics finding.
3. Click **Edit**.

   The edit button might be disabled if the cluster configuration recently changed. If you aren't able to edit the cluster settings, wait a few minutes and then try again.

4. On the **Legacy Stackdriver Monitoring** or **Stackdriver Kubernetes Engine Monitoring** drop-down list, select **Enabled**.

   These options aren't compatible. Make sure that you use either **Stackdriver Kubernetes Engine Monitoring** alone, or **Legacy Stackdriver Monitoring** with **Legacy Stackdriver Logging**.

5. Click **Save**.

One or more members in your organization have multiple KMS permissions assigned. It is recommended that no account simultaneously have **Cloud KMS Admin** along with other KMS permissions.

To remediate this finding:

1. Go to the IAM (https://console.cloud.google.com/iam-admin/iam) page in the Cloud Console.
   Go to the IAM page (https://console.cloud.google.com/iam-admin/iam)
2. Click **Edit** next to the member listed in the Security Health Analytics finding.
3. To remove permissions, click **Delete** next to **Cloud KMS Admin**. If you want to remove all of the member's permissions, click **Delete** next to all of the other permissions.
4. Click **Save**.
5. Repeat the preceding steps for each of the members listed in the Security Health Analytics finding.

In Kubernetes, Role-based access control (RBAC) allows you to define roles with rules that contain a set of permissions, and grant permissions at the cluster and namespace level. This provides better security by ensuring that users only have access to specific resources. It is recommended that you disable legacy Attribute-based access control (ABAC)
(/kubernetes-engine/docs/how-to/hardening-your-cluster#disable_abac).

To remediate this finding:

1. Go to the Kubernetes clusters (https://console.cloud.google.com/kubernetes/list) page in the Cloud Console.
   Go to the Kubernetes clusters page (https://console.cloud.google.com/kubernetes/list)
2. Select the cluster listed in the Security Health Analytics finding.
3. Click **Edit**.

   The edit button might be disabled if the cluster configuration recently changed. If you aren't able to edit the cluster settings, wait a few minutes and then try again.
4. On the **Legacy Authorization** drop-down list, select **Disabled**.
5. Click **Save**.

Master authorized networks improve security for your container cluster by blocking specified IP addresses from accessing your cluster's control plane.

To remediate this finding:

1. Go to the Kubernetes clusters (https://console.cloud.google.com/kubernetes/list) page in the Cloud Console.

   Go to the Kubernetes clusters page (https://console.cloud.google.com/kubernetes/list)

2. Select the cluster listed in the Security Health Analytics finding.
3. Click **Edit**.

   The edit button might be disabled if the cluster configuration recently changed. If you aren't able to edit the cluster settings, wait a few minutes and then try again.

4. On the **Master authorized networks** drop-down list, select **Enabled**.
5. Click **Add authorized network**.
6. Specify the authorized networks you want to use.
7. Click **Save**.

By default, pod to pod communication is open. Open communication allows pods to connect directly across nodes, with or without NAT. A NetworkPolicy is like a pod-level firewall that restricts connections between pods, unless the connection is explicitly allowed by the NetworkPolicy. Learn how to define a network policy (/kubernetes-engine/docs/how-to/hardening-your-cluster#restrict_with_network_policy).

To remediate this finding:

1. Go to the Kubernetes clusters (https://console.cloud.google.com/kubernetes/list) page in the Cloud Console.

   Go to the Kubernetes clusters page (https://console.cloud.google.com/kubernetes/list)

2. Select the cluster listed in the Security Health Analytics finding.
3. Click **Edit**.

   The edit button might be disabled if the cluster configuration recently changed. If you aren't able to edit the cluster settings, wait a few minutes and then try again.

4. On the **Network policy for master** and **Network policy for nodes** drop-down lists, select **Enabled**.
5. Click **Save**.

A user outside of your organization has Cloud IAM permissions on a project or organization. Learn more about Cloud IAM permissions (/iam/docs/overview).

To remediate this finding:

1. Go to the IAM (https://console.cloud.google.com/iam-admin/iam) page in the Cloud Console.
   Go to the IAM page (https://console.cloud.google.com/iam-admin/iam)
2. Select the checkbox next to users outside your organization.
3. Click **Remove**.

To support the retrieval of objects that are deleted or overwritten, Cloud Storage offers the Object Versioning feature. Enable Object Versioning to protect your Cloud Storage data from being overwritten or accidentally deleted. Learn how to Enable Object Versioning (/storage/docs/using-object-versioning#enable).

To remediate this finding, use the `gsutil versioning set on` command with the appropriate value, like `gsutil versioning set on gs://finding.assetDisplayName`

Firewall rules that allow connections from all IP addresses, like `0.0.0.0/0`, can unnecessarily expose resources to attacks from unintended sources. These rules should be removed or scoped explictly to the intended source IP ranges. Learn about Deleting firewall rules (/vpc/docs/using-firewalls#deleting_firewall_rules).

To remediate this finding:

1. Go to the Firewall rules (https://console.cloud.google.com/networking/firewalls/list) page in the Cloud Console.
   Go to the Firewall rules page (https://console.cloud.google.com/networking/firewalls/list)
2. Click the firewall rule listed in the Security Health Analytics finding, and then click **Edit**.
3. Under **Source IP ranges**, edit the IP values to restrict the range of IPs that are allowed.

OS Login enables centralized SSH key management with Cloud IAM, and it disables metadata-based SSH key configuration on all instances in a project. Learn how to Set up and configure OS Login (/compute/docs/instances/managing-instance-access).

To remediate this finding:

1. Go to the Metadata (https://console.cloud.google.com/compute/metadata) page in the Cloud Console.
   Go to the Metadata page (https://console.cloud.google.com/compute/metadata)
2. Click **Edit**, and then click **Add item**.
3. Add an item with key **enable-oslogin** and value **TRUE**.

A `PodSecurityPolicy` is an admission controller resource that validates requests to create and update pods on a cluster. The `PodSecurityPolicy` defines a set of conditions that pods must meet to be accepted by the cluster.

To remediate this finding, define and authorize `PodSecurityPolicies`, and enable the `PodSecurityPolicy` controller. For instructions, see the Using `PodSecurityPolicies` (/kubernetes-engine/docs/how-to/pod-security-policies) guide.

Private clusters allow nodes to only have private RFC 1918 IP addresses. This limits node outbound internet access. If a cluster node doesn't have a public IP address, it isn't discoverable or exposed to the public internet. You can still route traffic to a node by using an internal load balancer.

You can't make an existing cluster private. To remediate this finding, create a new private cluster:

1. Go to the Kubernetes clusters (https://console.cloud.google.com/kubernetes/list) page in the Cloud Console.
   Go to the Kubernetes clusters page (https://console.cloud.google.com/kubernetes/list)
2. Click **Create Cluster**.
3. Click **Availability, networking, security, and additional features**, and then select the checkboxes for **Enable VPC-native (using alias IP)** and **Private cluster**.

4. Click **Create**.

The bucket indicated by the Security Health Analytics finding is public and can be accessed by anyone on the internet.

To remediate this finding:

1. Go to the Storage Browser (https://console.cloud.google.com/storage/browser) page in the Cloud Console.
   Storage Browser (https://console.cloud.google.com/storage/browser)
2. Select the bucket listed in the Security Health Analytics finding.
3. On the **Bucket details** page, click the **Permissions** tab.
4. Under **Role(s)**, click **Delete** to remove all Cloud IAM permissions granted to **allUsers** and **allAuthenticatedUsers**.

One or more members in your organization have multiple Service Account permissions assigned. It is recommended that no account simultaneously have **Service Account Admin** along with other Service Account permissions.

To remediate this finding:

1. Go to the IAM (https://console.cloud.google.com/iam-admin/iam) page in the Cloud Console.
   Go to the IAM page (https://console.cloud.google.com/iam-admin/iam)
2. Click **Edit** next to the member listed in the Security Health Analytics finding.
3. To remove permissions, click **Delete** next to **Service Account Admin**. If you want to remove all of the service account permissions, click **Delete** next to all of the other permissions.
4. Click **Save**.
5. Repeat the preceding steps for each of the members listed in the Security Health Analytics finding.

The MySQL database instances indicated by the Security Health Analytics have no password set for the root account.

To remediate this finding, add a password to the MySQL database instances:

1. Go to the SQL Instances page (https://console.cloud.google.com/sql/instances) page in the Cloud Console.
   Go to the SQL Instances page (https://console.cloud.google.com/sql/instances)
2. Select the instance listed in the Security Health Analytics finding.
3. On the **Instance details** page that loads, select the **Users** tab.
4. Next to the `root` user, click **More**

   , and then select **Change Password**.
5. Enter a new, strong password, and then click **OK**.

The MySQL database instances indicated by the Security Health Analytics finding have a weak password set for the root account.

To remediate this finding, set a strong password for the MySQL database instances:

1. Go to the SQL Instances page (https://console.cloud.google.com/sql/instances) page in the Cloud Console.
   Go to the SQL Instances page (https://console.cloud.google.com/sql/instances)
2. Select the instance listed in the Security Health Analytics finding.
3. On the **Instance details** page that loads, select the **Users** tab.
4. Next to the `root` user, click **More**

   , and then select **Change Password**.
5. Enter a new, strong password, and then click **OK**.

To avoid leaking sensitive data in transit through unencrypted communications, all incoming connections to your SQL database instance should use SSL. Learn more about Configuring SSL/TLS

(/sql/docs/mysql/configure-ssl-instance).

To remediate this finding, allow only SSL connections for your SQL instances:

1. Go to the SQL Instances page (https://console.cloud.google.com/sql/instances) page in the Cloud Console.

   Go to the SQL Instances page (https://console.cloud.google.com/sql/instances)

2. Select the instance listed in the Security Health Analytics finding.
3. On the **Connections** tab, click **Allow only SSL connections**.

The Kubernetes web UI is backed by a highly privileged Kubernetes Service Account, which can be abused if compromised. If you are already using the Cloud Console, the Kubernetes web UI extends your attack surface unnecessarily. Learn about Disabling the Kubernetes web UI (/kubernetes-engine/docs/how-to/hardening-your-cluster#disable_kubernetes_dashboard).

To remediate this finding, disable the Kubernetes web UI:

1. Go to the Kubernetes clusters (https://console.cloud.google.com/kubernetes/list) page in the Cloud Console.

   Go to the Kubernetes clusters page (https://console.cloud.google.com/kubernetes/list)

2. Select the cluster listed in the Security Health Analytics finding.
3. Click **Edit**.

   The edit button might be disabled if the cluster configuration recently changed. If you aren't able to edit the cluster settings, wait a few minutes and then try again.

4. Click **Add-ons**. The section expands to display available add-ons.
5. On the **Kubernetes dashboard** drop-down list, select **Disabled**.
6. Click **Save**.

Workload Identity is the recommended way to access Google Cloud services from within GKE because it offers improved security properties and manageability. Enabling it protects some

potentially sensitive system metadata from user workloads running on your cluster. Learn about Metadata concealment (/kubernetes-engine/docs/how-to/protecting-cluster-metadata#concealment).

To remediate this finding, follow the guide to Enable Workload Identity on an existing cluster (/kubernetes-engine/docs/how-to/workload-identity#enable_workload_identity_on_an_existing_cluster).