Skip this guide and return to Installing the Stackdriver Logging agent (/logging/docs/agent/installation) if you are us
ute Engine VM instance, and you have not yet attempted to install the agent. Compute Engine instances should be pr
ized to run the agent.

This guide explains how to install private-key service account credentials on a VM instance to authorize the Stackdriver Logging agent. Before installing the agent, check that your VM instance has the credentials that the agent needs. The agent must have permission to send information to Logging. Permission is given by using service account credentials that are stored on your VM instance and serve as Application Default Credentials (https://developers.google.com/identity/protocols/application-default-credentials) for the agent.

Read this guide if either of the following applies to you:

- If you're running very old Compute Engine instances or Compute Engine instances created without the default credentials, then you must complete the steps in this guide before installing the agent. These VMs might not have the required private-key credentials. To verify your credentials, complete the Verifying Compute Engine credentials (/logging/docs/agent/troubleshooting#verify-creds) procedures. On newly created Compute Engine VM instances, the default service account on your instance has the credentials that the agents needs.
- If you're running **AWS EC2 VM instances**, you must complete the steps in this guide before installing the agent. Amazon EC2 VM instance don't have the required service account. Instead, you must manually obtain private-key credentials from a service account of the **AWS connector project** (#aws_connector_project). If you think your instance already has private-key credentials, then complete the Verifying private-key credentials (/logging/docs/agent/troubleshooting#verify-key) procedures to check them. To add private-key credentials, skip ahead to Adding credentials (#private_key_authorization).

You can check your authorization scopes on Compute Engine using the following command:

Look for one or more of the following authorization scopes in the output:

Authorization refers to the process of determining what permissions an authenticated client has for a set of resources.

Authorizing the Logging agent on a VM instance involves the following steps:

1. Creating a service account (#create-service-account) with the required privileges and private-key credentials in the Google Cloud project associated with your VM instance. For **Amazon EC2 VM instances**, you do this in the `AWS Link` project that Stackdriver creates when you connect your AWS account.
2. Copying the private-key credentials (#copy-private-key) to your VM instance, where they serve as Application Default Credentials (https://developers.google.com/identity/protocols/application-default-credentials) for software running on your instance.
3. Installing or restarting the agent (#install-or-restart).

ng: The new credentials might overwrite your existing credentials, so check that your current applications still have th credentials when you complete these procedures.

Authentication refers to the process of determining a client's identity. For authentication, we recommend using a service account: a Google account that is associated with your Google Cloud project, as opposed to a specific user. You can use service accounts for authentication regardless of where your code runs: on Compute Engine, App Engine, or on-premise. Read Authentication overview (/docs/authentication/) for more information.

To create a service account, complete the Creating a service account (/docs/authentication/getting-started#creating_a_service_account) procedures with the following

information:

- Select the Google Cloud project in which to create the service account:
  - For Compute Engine instances, choose the project in which you created the instance. If you created your instance in the Workspace hosting project (/monitoring/accounts/#account-project), then choose the Workspace.
  - For Amazon EC2 instances, choose the AWS connector project (/monitoring/accounts/#account-project) created when you connected Logging your AWS account. The connector project's name typically begins with `AWS Link`. **Don't create your service account in the Workspace project.**
- In the **Role** drop-down menu, select the following role:
  - **Logging** > **Logs Writer**. This authorizes the Logging agent.

  If you will also install the Monitoring agent, then add the following role for that agent:
  - **Monitoring** > **Monitoring Metric Writer**. This authorizes the Monitoring agent.
- When creating the key, select **JSON** as the **Key type**.

For your convenience, you can create the variable `CREDS` to point to the credentials file on your workstation. For example:

The rest of these procedures refer to that variable.

After creating the service account, you must copy the private-key file to one of the following locations on your VM instance so that the agent can recognize the credentials. You can use any file-copy tool you wish.

- **Linux only**: `/etc/google/auth/application_default_credentials.json`
- **Windows only**: `C:\ProgramData\Google\Auth\application_default_credentials.json`
- For both Linux and Windows: Any location you store in the variable, `GOOGLE_APPLICATION_CREDENTIALS`. The variable must be visible to the agent's process.

The following file-copy instructions assume that you have a Linux environment on both your workstation and your instance. If you are using a different environment, consult the documentation from your cloud provider for how to copy the private-key file. In the previous step, Creating a service account (#create-service-account), your private-key credentials should have been stored on your workstation at a location you saved in the variable `CREDS`:

If your credential file is not in the previously listed default location, then in addition to the commands in the preceding
bles, you must be sure that **`GOOGLE_APPLICATION_CREDENTIALS`** is defined
s/authentication/getting-started#setting_the_environment_variable) and visible to the agent process.

Your VM instance now has the credentials that the agent needs.

- If you have not yet installed the agent, go to the agent installation page and install the agent. See Installing the agent (/logging/docs/agent/installation) for instructions.
- If you have already installed the agent, restart it to use the new credentials. See Restarting the agent (/logging/docs/agent/installation#restart) for instructions.
- If you would like to double-check the credentials, see Verifying private-key credentials (/logging/docs/agent/troubleshooting/#verify-key).