Guest Cluster Log Collection

You can collect guest cluster logs and configuration files. Perform the following steps on each guest cluster node:

1. Log in to the node.
2. Download the Rancher v2.x Linux log collector script and generate a log bundle using the following commands:

   ```
   curl -OLs https://raw.githubusercontent.com/rancherlabs/support-tools/master/collection/rancher/v2.x/logs-collector/rancher2_logs_collector.sh
   sudo bash rancher2_logs_collector.sh
   ```

   The output of the script indicates the location of the generated tarball.

For more information, see The Rancher v2.x Linux log collector script.

Importing of Harvester Clusters into Rancher

After the `cluster-registration-url` is set on Harvester, a deployment named `cattle-system/cattle-cluster-agent` is created for importing of the Harvester cluster into Rancher.

Import Pending Due to `unable to read CA file` Error

The following error messages in the `cattle-cluster-agent-*` pod logs indicate that the Harvester cluster cannot be imported into Rancher.

```
2025-02-13T17:25:22.520593546Z time="2025-02-13T17:25:22Z" level=info msg="Rancher agent version v2.10.2 is starting"
2025-02-13T17:25:22.529886868Z time="2025-02-13T17:25:22Z" level=error msg="unable to read CA file from /etc/kubernetes/ssl/certs/serverca: open /etc/kubernetes/ssl/certs/serverca: no such file or directory"
2025-02-13T17:25:22.529924542Z time="2025-02-13T17:25:22Z" level=error msg="Strict CA verification is enabled but encountered error finding root CA"
```

The root cause is that the `agent-tls-mode` is not effectively configured.

Rancher's `agent-tls-mode` setting controls how Rancher's agents (`cluster-agent` , `fleet-agent` , and `system-agent`) validate Rancher's certificate when establishing a connection. You can set either of the following values:

- `strict` : Rancher's agents only trust certificates generated by the Certificate Authority (CA) specified in the `cacerts` setting. This is the recommended default TLS setting that guarantees a higher level of security.

  The `strict` option enables a higher level of security, it requires Rancher to have access to the CA which generated the certificate visible to the agents. In the case of certain certificate configurations (notably, external certificates), this is not automatic, and **extra configuration is needed**. See the installation guide for more information on which scenarios require extra configuration.

- `system-store` : Rancher's agents trust any certificate generated by a public Certificate Authority specified in the operating system's trust store. Use this setting if your setup uses an external trust authority and you don't have ownership over the Certificate Authority.

:::important

Using the `system-store` setting implies that the agent trusts all external authorities found in the operating system's trust store including those outside of the user's control.

:::

The default value of this setting depends on the Rancher version and installation type. For more information, see Rancher issue #45628.

Type	Versions	Default Value
New installation	v2.8	`system-store`
New installation	v2.9 and later	`strict`
Upgrade	v2.8 to v2.9	`system-store`

Follow the steps below to configure the different TLS setting options.

1. Log in to the Rancher UI.
2. Go to **Global Settings > Settings**.
3. Select **agent-tls-mode**, and then select ⋮ **> Edit Setting** to access the configuration options.
4. Set **Value** to **System Store** or **Strict**.
5. Click **Save**.

Related issues:

- Harvester: #7105 and [#7284]https://github.com/harvester/harvester/issues/7284
- Rancher: #45628