

FORTRA

VCM
2.25

Quick Start Guide
May 2026

Copyright Terms and Conditions

Copyright Help/Systems LLC and its group of companies.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from HelpSystems is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to HelpSystems with appropriate and specific direction to the original content. HelpSystems and its trademarks are properties of the HelpSystems group of companies. All other marks are property of their respective owners.

May 2026

Table of Contents

Introduction	4
Installing VCM	5
Accessing VCM	6
Licensing VCM	7
Configuring VCM vSphere Datasources	8
Configuring AppDynamics Datasources	11
Amazon CloudWatch Datasources	13
Configuring Amazon CloudWatch Datasources	14
Microsoft Azure Monitor Datasources	16
Configuring Microsoft Azure Monitor Datasources	17
Google Cloud Monitoring Datasources	19
Configuring Google Cloud Monitoring Datasources	20
Prometheus Datasources	22
Configuring Prometheus Datasources	22
Kubernetes Datasources	25
Configuring Kubernetes Datasources	27
Contacting Fortra	29
Fortra Portal	29

Introduction

VCM is a software product used to optimize the performance and cost of our hybrid IT environment. VCM includes the following components to assist you with the optimization of your site:

- **Key Performance Indicators (KPI)**

KPIs are used to view the current health, provide a prediction of future health, and show how efficiently the environment is being used.

- **Performance Monitor**

Performance Monitor is used to monitor and analyze system performance.

- **Capacity Plans**

Capacity Plans is used to predict future capacity requirements.

- **Automated Analytics**

Automated Analytics is used to view live and historical data and create custom layouts.

This guide includes the following steps to help you get started using VCM:

- Downloading the software.
- Installing the software.
- Configuring a datasource.
- Start using the software.

Installing VCM

To install VCM:

1. Download the **Vityl Bootstrap** package from the **Fortra Community Portal** on the **VCM** download page.
2. Move the **vityl-bootstrap** RPM package to the target system.
3. Open a terminal window on the target system.
4. Install the **vityl-bootstrap** package using the following command:

```
sudo yum install ./vityl-bootstrap-x.x.x-1.el7.noarch.rpm
```

This places all VCM packages in the /opt/vityl/boot directory and registers it as a yum repository for use in the local system.

5. Install the rest of the **VCM** packages using the following command:

```
sudo yum install vcm
```

Accessing VCM

To access VCM:

1. Open a browser window and enter the following URL:
`https://system`
where *system* is where VCM is installed.
2. Enter your username and password.
By default, admin and admin.

Licensing VCM

When you trial or purchase VCM, Fortra sends you a product license key. This license key must be applied to your installation of VCM.

To apply the VCM license key to your installation:

1. Log into **VCM**.

The License page is displayed the first time you log into VCM.

2. Click **Show Hardware ID**.

The Hardware ID dialog is displayed. This dialog includes system information that can be sent to Fortra when requesting a license key.

3. Click **Update License**.

The Update License form is displayed.

4. In the **License Key** text box, type or paste your license key.

5. Click **Apply**.

Next, you need to configure one or more datasources. Skip to the section for the datasource that you are interested in configuring.

Configuring VCM vSphere Datasources

To retrieve data and start using VCM, you need to configure one or more datasources.

To configure a VCM vSphere datasource:

1. From the VCM **Welcome** page, click **Datasources**.
2. From the **Datasources** page, click the **Edit Datasources** link on the bottom left.
3. Log into **Automated Analytics** using your username and password.
By default, sa and sa.
4. Click **File > Edit** to open the **Edit Datasources** dialog.
5. Click **File > New Datasource > VCM vSphere**.

The Create a VCM vSphere Datasource dialog is displayed.

Create a VCM vSphere Datasource

Name:

⚠ This is a required field

Property	Value
protocol	https ▾
host	
port	
user	
password	
connections	4
timeout	5
requestSize	50
DNSHostName	full ▾
priority	10
timezone	▾
mode	realtime ▾
dataFrequency	60

Create

Create/Connect

Cancel

6. In the **Name** text box, type a name for the datasource.

7. In the **protocol** text box, select **HTTP** or **HTTPS**.

NOTE: Fortra recommends using HTTPS.

8. In the **host** text box, type the host name of the VMware vCenter server.

9. In the **port** text box, type the port of the VMware vCenter server. The default port is 443.

10. In the **user** text box, type a user name that has access to the VMware vCenter.

11. In the **password** text box, type the password for the user.

NOTE: The user credentials used to connect to the VMware vCenter must be assigned to a role with at least read-only privileges to retrieve metric data.

12. Click **Create/Connect** to create, verify, and connect to the datasource.

The status changes to connected when the connection is established.

NOTE: You can click Create to create the datasource. The datasource displays a status of inactive. Click Connect to activate the datasource.

The datasource is displayed in the Edit Datasources dialog.

Configuring AppDynamics Datasources

To retrieve data and start using VCM, you must configure one or more datasources.

To configure an AppDynamics datasource:

1. From the **VCM Welcome** page, click **Datasources**.
2. From the **Datasources** page, click the **Edit Datasources** link on the bottom left.
3. Log into **Automated Analytics** using your username and password.

By default, sa and sa.

4. Click **File > Edit** to open the **Edit Datasources** dialog.
5. Click **File > New Datasource > AppDynamics**.

The Create a AppDynamics Datasource dialog is displayed.

Property	Value
host	
port	
account name	
client name	
client secret	
Discover Applications	disabled
Discover Systems	disabled
Discover Databases	disabled
priority	10
timezone	
dataset	production
mode	realtime
dataFrequency	60
connectionTestUrl	https://\$host:\$port/controller/res

6. In the **Name** text box, type a name for the datasource.
7. In the **host** text box, type the hostname of the AppDynamics server.

8. In the **port** text box, type the port number of the AppDynamics server. The default is 443.
9. In the **account name** text box, type a Username that has access to AppDynamics. In AppDynamics, go to **Administration > Users** to either get a list or to add a user with permission roles to view applications, databases, and servers.
10. In the **client name** text box, type an API Client Name. In AppDynamics, go to **Administration > API Clients** to either get a list or to add an API Client with permission roles to view applications, databases, and servers.
11. In the **client secret** text box, type an API Client Secret. In AppDynamics, go to **Administration > API Clients** and get a Client Secret for API Client used in step 10. If the Client Secret is hidden and the Copy button is greyed out, either get the Secret from an Administrator or generate a new secret with the Generate Secret button. Selecting the Generate Secret button will create a visible secret that you can copy. Make sure to select the Save button or the old secret will still be active.
12. In the **Discover Applications** drop-down menu, select **enabled** to discover applications.
13. In the **Discover Systems** drop-down menu, select **enabled** to discover servers.
14. In the **Discover Databases** drop-down menu, select **enabled** to discover databases.
15. Click **Create/Connect** to create, verify, and connect to the datasource.

The status changes to connected when the connection is established.

NOTE: You can click Create to create the datasource. The datasource displays a status of inactive. Click Connect to activate the datasource.

The datasource is displayed in the Edit Datasources dialog.

Amazon CloudWatch Datasources

When you interact with Amazon AWS, you must specify your security credentials to verify your identity and access rights to the requested resources. Access keys are used to sign programmatic requests to Amazon. These keys contain an access key identifier and a secret access key. An Identity and Access Management (IAM) role can also be used to obtain security credentials and access keys.

The user or IAM role associated with the security credentials should have the following permissions or belong to a group that has the following permissions:

- cloudwatch:ListMetrics
- cloudwatch:GetMetricData
- cloudwatch:GetMetricStatistics
- ec2:DescribeInstances
- ec2:DescribeInstanceTypes
- ec2:DescribeVolumes
- pricing:DescribeServices
- pricing:GetAttributeValues
- pricing:GetProducts
- rds:Describe*

Most Amazon AWS services offer regional endpoints or URLs to reduce latency. Resources in one region, such as Amazon EC2 instances, are independent of resources in another region. The region property is used by calls to the SDK so requests can be properly generated in the correct region. For more information on AWS Regions and Endpoints, see <https://docs.aws.amazon.com/general/latest/gr/rande.html>. For more information on Amazon EC2 services, see https://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region.

To use Amazon CloudWatch, you need an Amazon AWS account which allows you to use specific Amazon AWS services to view metrics. For information on signing up for an Amazon AWS account, see <https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/GettingSetup.html>.

When you interact with Amazon AWS, you must specify your Amazon AWS security credentials to verify your identity and permissions to access the requested resources. For

more information on these security credentials, see

<https://docs.aws.amazon.com/general/latest/gr/aws-security-credentials.html>.

There are different types of security credentials that depend on how you interact with Amazon AWS. Access keys are used to sign programmatic requests to Amazon AWS. Access keys include an access key identifier and a secret access key. For more information on the access keys, see <https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html#access-keys-and-secret-access-keys>.

If you already have an access key, you can locate it from the following location in the Amazon AWS console:

```
IAM > users > your username > Access keys
```

Access keys can be difficult to manage across multiple AWS accounts. You can use IAM roles instead to obtain security credentials. For more information on IAM roles, see https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html. For more information on access across AWS accounts, see https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_aws-accounts.html.

Assuming a role requires Automated Analytics to run on an EC2 instance within one of your AWS accounts. The EC2 instance needs to be assigned to an IAM role with the `sts:AssumeRole` permission.

Configuring Amazon CloudWatch Datasources

To configure an Amazon CloudWatch datasource:

1. From the **VCM Welcome** page, click **Datasources**.
2. From the **Datasources** page, click the **Edit Datasources** link on the bottom left.
3. Log into **Automated Analytics** using your username and password.

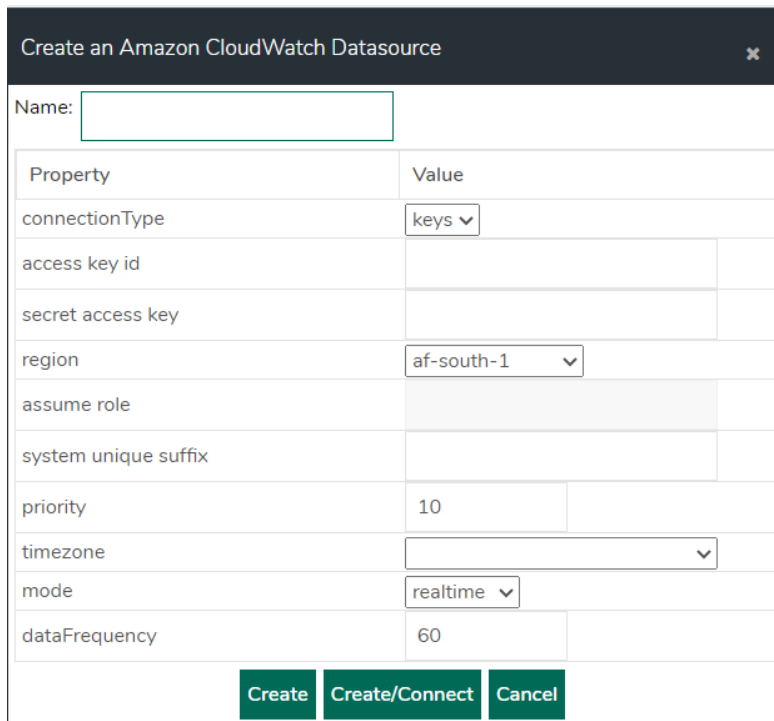
By default, sa and sa.

4. Click **Edit > Datasources**.

The Edit Datasources dialog is displayed.

5. Click **File > New Datasource > Amazon CloudWatch**.

The Create a Amazon CloudWatch Datasource dialog is displayed.



Property	Value
connectionType	keys ▼
access key id	
secret access key	
region	af-south-1 ▼
assume role	
system unique suffix	
priority	10
timezone	
mode	realtime ▼
dataFrequency	60

Buttons: Create, Create/Connect, Cancel

6. In the **Name** text box, type a name for the datasource.
7. In the **connectionType** text box, specify if you are connecting with keys or a role.
8. If the **connectionType** is **keys**, in the **access key id** text box, type the identifier of the access key used to sign programmatic requests made to Amazon AWS.
9. If the **connectionType** is **keys**, in the **secret access key** text box, type the secret access key used to sign the programmatic requests made to Amazon AWS.
10. In the **region** text box, type the region to direct the programmatic requests made to Amazon AWS to.
11. If you set the **connectionType** to **role**, in the **assume role** text box, type the role that you want to use to connect to instead of connecting with an access id.
12. If the **connectionType** is **role**, in the **assume role** text box, type the IAM role to use for obtaining security credentials.
13. In the **system unique suffix** text box, type the suffix you want to append to the system to make systems unique across datasources.
14. Click **Create/Connect** to create, verify, and connect to the datasource.
The status changes to connected when the connection is established.

NOTE: You can click Create to create the datasource. The datasource displays a status of inactive. Click Connect to activate the datasource.

The datasource is displayed in the Edit Datasources dialog.

Microsoft Azure Monitor Datasources

All tasks in the Azure Monitor API use the Azure Resource Manager authentication model where requests must be authenticated with Azure Active Directory (Azure AD). For information on authenticating Azure Monitor requests, see <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/rest-api-walkthrough#authenticating-azure-monitor-requests>.

Use the Azure portal to register the application so it can access resources. For information on using the portal to create an Azure AD application and service principal, see <https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>.

For an application to log in, the `activeDirectoryTenantId`, `applicationId`, and the `authenticationKey` properties are required and created during the registration process.

When an Azure AD application is registered, the following objects are created:

- **application_object**
Represents the application across all Azure AD tenants.
- **service_principal**
This object is created in each tenant where the application is used to allow the application to access resources in a given tenant. Access to more than one Azure AD tenant is not currently supported by the Microsoft Azure Monitor module.

You can find your subscription identifier from the following location in the Microsoft Azure portal:

All services > General > Subscriptions

You can find your tenant and application identifiers from the following location in the Microsoft Azure portal:

All services > Identity > App registrations > *your application name*

You can find your authentication key from the following location in the Microsoft Azure portal:

All services > Identity > App registrations > *your application name*
> Certificates & secrets

Configuring Microsoft Azure Monitor Datasources

To configure a Microsoft Azure Monitor datasource:

1. From the **VCM Welcome** page, click **Datasources**.
2. From the **Datasources** page, click the **Edit Datasources** link on the bottom left.
3. Log into **Automated Analytics** using your username and password.
By default, sa and sa.
4. Click **File > Edit** to open the **Edit Datasources** dialog.
5. Click **File > New Datasource > Microsoft Azure Monitor**.

The Create a Microsoft Azure Monitor Datasource dialog is displayed.

Create a Microsoft Azure Monitor Datasource

Name:

Property	Value
subscriptionId	
activeDirectoryTenantId	
applicationId	
authenticationKey	
priority	10
timezone	
mode	realtime
dataFrequency	60

Create

Create/Connect

Cancel

6. In the **Name** text box, type a name for the datasource.
7. In the **subscriptionId** text box, type the subscription identifier.
Microsoft Windows Azure subscriptions grant and control access to Microsoft Windows Azure services and is the mechanism by which resource usage is reported and billed. Every deployed resource must be associated with only one subscription.
8. In the **activeDirectoryTenantId** text box, type the guid string that identifies the Microsoft Azure Active Directory tenant containing the resources the datasource will have access. For example, virtual machines, storage, and so on.

9. In the **applicationId** text box, type the guid string that identifies an application accessing Microsoft Azure (the datasource in Automated Analytics).
10. In the **authenticationKey** text box, type the guid string that contains the credentials used to authenticate the application so it can determine the role that the datasource has and whether it has access to the resources in the AD tenant.
11. From the **timezone** list, select the timezone.
12. Click **Create/Connect** to create, verify, and connect to the datasource.
The status changes to connected when the connection is established.

NOTE: You can click Create to create the datasource. The datasource displays a status of inactive. Click Connect to activate the datasource.

The datasource is displayed in the Edit Datasources dialog.

Google Cloud Monitoring Datasources

Google Cloud Monitoring is a cloud computing systems management service. It provides performance and diagnostic data to public cloud users. Google Cloud Monitoring provides support for both Google Cloud and Amazon AWS cloud environments.

The Google Cloud Monitoring module requires the following properties to create a datasource:

- project id
- project region
- project zone
- locations
- credentials file path

Google Cloud Platform (GCP) projects form the basis for creating, enabling, and using all Cloud Platform services. To interact with most Cloud Platform resources, you must provide the identifying project information for every request. The project id property uniquely identifies a project and can be determined when you are logged into the Google Cloud Console.

Compute Engine resources are hosted in multiple locations worldwide. These locations are composed of regions and zones. A region is a specific geographical location where you can host your resources. Each region has one or more zones; most regions have three or more zones. The fully-qualified name for a zone is comprised of <region>-<zone>. When you create a project, a default fully-qualified zone name is associated with the project. The project region and project zone properties are used to specify this default setting.

There is no requirement for all Compute Engine resources in a project to exist in the default project zone. However, for the module to discover all project resources, it must know the fully-qualified zone names where project resources exist. The locations property is a space-delimited list of these additional fully-qualified zones where project resources might exist.

The Google Cloud Monitoring module uses a Service Account for authentication and is the recommended approach for authenticating a server application. When creating a service account, a JSON file is generated with the authentication key, and must be moved to the server where Automated Analytics is installed. The credentials file path property specifies the full path to this JSON file.

Configuring Google Cloud Monitoring Datasources

To configure a Google Cloud Monitoring datasource:

1. From the **VCM Welcome** page, click **Datasources**.
2. From the **Datasources** page, click the **Edit Datasources** link on the bottom left.
3. Log into **Automated Analytics** using your username and password.

By default, sa and sa.

4. Click **File > Edit** to open the **Edit Datasources** dialog.
5. Click **File > New Datasource > Google Cloud Monitoring**.

The Create a Google Cloud Monitoring Datasource dialog is displayed.

Property	Value
project id	
project region	us-central1
project zone	a
credentials file path	
locations	
priority	10
timezone	
mode	realtime
dataFrequency	60

Buttons: Create, Create/Connect, Cancel

6. In the **Name** text box, type a name for the datasource.
7. In the **project id** text box, type the identifier of the Google Cloud project.
8. From the **project region** list, select the geographical location where the project resources are hosted.
9. From the **project zone** list, select the project zone within the project region.

10. In the **credentials file path** text box, type the full pathname of the JSON credentials file generated from the service account used by the datasource to authenticate access to project resources.
11. In the **locations** text box, type the additional fully-qualified zones in the form of the region-zone where project resources exist. This is a space delimited list.
12. In the **timezone** text box, select the timezone.
13. Click **Create/Connect** to create, verify, and connect to the datasource.

The status changes to connected when the connection is established.

NOTE: You can click Create to create the datasource. The datasource displays a status of inactive. Click Connect to activate the datasource.

The datasource is displayed in the Edit Datasources dialog.

Prometheus Datasources

Prometheus is a an open-source monitoring system with a dimensional data model, flexible query language, efficient time series database, and modern alerting approach. Metric data is pulled on a regular time-interval from exporters that expose the metrics coming from applications, operating systems, and other services.

The Prometheus module supports the following exporters:

- **Node Exporter**

Machine-level metrics on Linux such as CPU usage, memory, disk utilization, filesystem fullness, and network bandwidth.

- **cAdvisor**

Google project that analyzes resource usage and performance characteristics of running Docker containers. It exposes out-of-the box container statistics, such as Prometheus metrics.

Metrics provided from instrumentation or any other exporter are not included in the module at this time. You can update the module to include additional metrics. For an overview and details of Prometheus features and capabilities, see the Prometheus documentation.

Configuring Prometheus Datasources

To configure a Prometheus datasource:

1. From the **VCM Welcome** page, click **Datasources**.
2. From the **Datasources** page, click the **Edit Datasources** link on the bottom left.
3. Log into **Automated Analytics** using your username and password.
By default, sa and sa.
4. Click **File > Edit** to open the **Edit Datasources** dialog.
5. Click **File > New Datasource > Prometheus**.

The Create a Prometheus Datasource dialog is displayed.

Create a Prometheus Datasource

Name:

Property	Value
protocol	https
host	
port	
discoverPods	disabled
discoverContainers	disabled
autoConsolidate	enabled
priority	10
timezone	
mode	realtime
dataFrequency	60
connectionTestUrl	\$protocol://\$host:\$port/

Create
Create/Connect
Cancel

6. In the **Name** text box, type a name for the datasource.
7. In the **host** text box, type the Prometheus host name to connect to.
8. In the **port** text box, type the HTTP port to connect to. HTTPS is not supported.
9. From the **discoverPods** list, select enabled to allow the discovery of pods.
Pods are discovered when they are collected by the Prometheus server, independent of the nodes where they are running. The default is disabled.
10. From the **discoverContainers** list, select enabled to allow the discovery of containers.
Containers are discovered when they are collected by the Prometheus server, independent of the nodes where they are running. The default is disabled.
11. From the **autoConsolidate** list, select enabled to force the module to consolidate points across time into larger point sizes.
Setting this field to enabled overrides the Prometheus behavior of performing no consolidation of points across time. Do not change this field to enabled unless instructed.
12. Click **Create/Connect** to create, verify, and connect to the datasource.
The status changes to connected when the connection is established.

NOTE: You can click Create to create the datasource. The datasource displays a status of inactive. Click Connect to activate the datasource.

The datasource is displayed in the Edit Datasources dialog.

Kubernetes Datasources

Kubernetes datasources require a port. Default ports are 8080 for http connections and 6443 for https connections.

Kubernetes datasources use Bearer Token Authentication. When using Bearer Token Authentication from an http client, the API server expects an Authorization header with a value of Bearer THETOKEN. The Bearer Token must be a character sequence that can be put in an HTTP header value using no more than the encoding and quoting facilities of HTTP. For example, if the bearer token is 31ada4fd-adec-460c-809a-9e56ceb75269 then it appears in an HTTP header as follows:

```
Authorization: Bearer 31ada4fd-adec-460c-809a-9e56ceb75269 .
```

Fortra recommends that you create a Service Account, ClusterRole, and ClusterRoleBinding to provide read-only permissions.

The following is an example yaml file that can be used to create a tqkubernetes Service Account with a Cluster Role of tqkubernetes-role and a Cluster Role Binding of tqkubernetes-role-binding. This ClusterRole is defined with the verbs get, list, and watch which grants read-only access to all resources in the cluster.

```
tqkubernetes.yaml:

apiVersion: v1
kind: ServiceAccount
metadata:
  name: tqkubernetes
  namespace: default
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: tqkubernetes-role
rules:
- apiGroups:
  - ""
  resources:
  - "*"
  verbs:
  - get
  - list
  - watch
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
```

```

metadata:
  name: tqkube-role-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: tqkube-role
subjects:
- kind: ServiceAccount
  name: tqkube
  namespace: default

```

You can grant read-only access with the tqkube Service Account by running the following command to create the ServiceAccount, ClusterRole, and ClusterRoleBinding:

```
kubectl apply -f tqkube.yaml
```

You can create the Bearer Token using the following command:

```

kubectl get secrets -o jsonpath="{.items[?(@.metadata.annotations
['kubernetes\.io/service-
account\.name']=='tqkube')].data.token}"|base64 --delete

```

You can also use your own user or Service Account configuration to provide access by replacing tqkube with your own user or Service Account name to get the Bearer Token.

NOTE: For http connectivity, if you have an anonymous user configured you do not need a Bearer Token.

For more information, see <https://kubernetes.io/docs/reference/access-authn-authz/authentication/>.

Automated Analytics requires a certificate for https connectivity to the Kubernetes API.

To use a self-signed certificate, go to the /surveyor/v11.3/conf directory and run the following commands:

```
/bin/keytool -printcert -sslserver <Kubernets host>:<Kubernetes
port> -rfc > temp.cer
```

```
/bin/keytool -importcert -alias <alias can be anything> -file
temp.cer -keystore webmodule.ts -storepass changeit -noprompt
```

Load the certificate by restarting the Automated Analytics service.

You can use a Certificate Authority signed certificate for a more secure access using the following command:

```
/bin/keytool -importcert -alias <alias can be anything> -file  
casigned.cer -keystore webmodule.ts -storepass changeit -noprompt
```

If your certificate is not valid or if it is configured incorrectly, the following error is displayed:

```
Invalid datasource detected:  
"Connection Error: sun.security.validator.ValidatorException: PKIX  
path building failed:  
sun.security.provider.certpath.SunCertPathBuilderException: unable  
to find valid certification path to requested target". Would you  
like to create this datasource anyway?
```

If your Bearer Token is bad, the following error is displayed:

```
Invalid datasource detected:  
401 Unauthorized Would you like to create this datasource anyway?
```

Configuring Kubernetes Datasources

A Kubernetes datasource is used to retrieve configuration data about Kubernetes environments. This information is used in combination with the VCM Metrics API and the Prometheus modules. This datasource is optional for Kubernetes environments.

To configure a Kubernetes datasource:

1. From the **VCM Welcome** page, click **Datasources**.
2. From the **Datasources** page, click the **Edit Datasources** link on the bottom left.
3. Log into **Automated Analytics** using your username and password.

By default, sa and sa.

4. Click **File > Edit** to open the **Edit Datasources** dialog.
5. Click **File > New Datasource > Kubernetes**.

The Create a Kubernetes Datasource dialog is displayed.

Create a Kubernetes Datasource

×

Name:

Property	Value
protocol	https ▾
host	
port	
token	
priority	10
timezone	▾
mode	historical ▾
dataFrequency	60
connectionTestUrl	\$protocol://\$host:\$port/api

Create

Create/Connect

Cancel

- In the **Name** text box, type a name for the datasource.
- In the **host** text box, type the Kubernetes host to connect to.
- In the **port** text box, type the port to connect to. Kubernetes default ports are 8080 for HTTP connections or 6443 for HTTPS connections.
- In the **token** text box, type the **Authentication Bearer Token** or leave blank for HTTP anonymous access.
- In the **connectionTestUrl** text box, type the URL to connect to and test the connection. The default URL is \$protocol://\$host:\$port/api and should not be changed unless specifically instructed.
- Click **Create/Connect** to create, verify, and connect to the datasource.
The status changes to connected when the connection is established.

NOTE: You can click Create to create the datasource. The datasource displays a status of inactive. Click Connect to activate the datasource.

The datasource is displayed in the Edit Datasources dialog.

Contacting Fortra

Please contact Fortra for questions or to receive information about VCM. You can contact us to receive technical bulletins, updates, program fixes, and other information via electronic mail, Internet, or fax.

Fortra Portal

For additional resources, or to contact Technical Support, visit the [Fortra Support Portal](#).

For support issues, please provide the following:

- Check this guide's table of contents and index for information that addresses your concern.
- Gather and organize as much information as possible about the problem including job/error logs, screen shots or anything else to document the issue.