System Requirements for the SAS® Viya® Platform

2023.06

This document might apply to additional versions of the software. Open this document in SAS Help Center and click on the version in the banner to see all available versions.

Virtual Infrastructure Requirements

Help with Cluster Setup

Deployment of the SAS Viya platform requires experience with Kubernetes. However, SAS provides tools to help administrators create and configure a cluster that meets the requirements for the SAS Viya platform.

The SAS Viya platform Infrastructure as Code (IaC) projects contain scripts and configuration files that can automatically provision the infrastructure components that are required to deploy the SAS Viya platform on Microsoft Azure, on Amazon Web Services (AWS), on Google Cloud Platform (GCP), and on open source Kubernetes. Each toolkit helps you to meet most of the system requirements that are listed here.

Note: SAS Viya platform IaC tools are not available for a deployment in Red Hat OpenShift or Anthos Clusters on VMware.

Some knowledge of Kubernetes and relevant third-party tools is still necessary. Some required components cannot be provided by these tools. Use of the IaC tools means that some of the procedures in this guide do not apply or require modifications in order to deploy the SAS Viya platform.

For more information, see these GitHub projects:

- SAS Viya 4 Infrastructure as Code (IaC) for Microsoft Azure
- SAS Viya 4 Infrastructure as Code (IaC) for AWS
- SAS Viya 4 Infrastructure as Code (IaC) for GCP
- SAS Viya 4 Infrastructure as Code (IaC) for Open Source Kubernetes

After you use the IaC tools to create the cluster, you can then use the resources in the viya4-deployment GitHub project or another method to deploy the SAS Viya platform.

Be aware that if you use a deployment method other than the viya4-deployment project to deploy the SAS Viya platform, a few additional steps will be required. For example, when you use the SAS Viya Platform Deployment Operator to deploy the SAS Viya platform in AWS, your environment will lack ingress-nginx and two required AWS components. Consult the lists of required cluster components in "Kubernetes Cluster Requirements" and in "Platform-Specific Requirements". Run the SAS Pre-Install Check Utility in order to make sure that your cluster includes the required items before you deploy the SAS Viya platform.

Required Permissions

Deploying the software and running tasks to operate SAS Viya platform components require administrative access to the cluster and to the one or more namespaces that are used. For example, any user who issues kubectl commands to operate or check the status of SAS servers will need this level of access. In the SAS Viya platform documentation, this level of access is referred to as *elevated Kubernetes permissions*.

For more information, see the Kubernetes documentation on role-based access control.

Cluster Requirements for All Environments

The SAS Viya platform runs in a Kubernetes cluster on multiple platforms. The requirements in this section apply to all deployments. The additional requirements for each supported environment are listed in Platform-Specific Requirements on page 11.

Virtual Private Cloud and Network Considerations

The SAS Viya platform supports multiple VPCs (or virtual networks) and multiple subnets per deployment. SAS pods and services consume many private IP addresses. When you plan your deployment, dedicate at least one VPC with subnets that are configured with sufficiently broad CIDR ranges to accommodate these private IP addresses.

For all platforms, consider using separate CIDR blocks for pods and for services, rather than placing pods and services in the same CIDR block.

Your Kubernetes service uses preferred methods for scaling up deployments with multiple IP addresses. For example, GKE supports VPC-native clusters, in which pod IP addresses are not

dependent on static routes. For AKS, SAS has tested with a private CIDR and added a secondary CIDR to support larger deployments with multiple SAS offerings. With EKS, consider setting up a very broad CIDR or a separate secondary IP address range in an additional subnet.

A CNI plug-in can be a helpful addition for IP address management in a Kubernetes cluster. A CNI plug-in is required for SAS Viya with SingleStore and for a deployment with open source Kubernetes.

Kubernetes Cluster Requirements

The SAS Viya platform components run in a Kubernetes cluster. Make sure that your cluster includes the components that are listed in the following table before you start the SAS Viya platform deployment.

Table 1 *Requirements that Apply to All Deployments*

Cluster Setup Task	Notes
Elevated Kubernetes permissions to the cluster and namespace(s)	Deploying the software and running tasks to operate SAS Viya platform components require administrative access to the cluster and to the one or more namespaces that are used.
Cloud account for selected provider	An administrative account with appropriate permissions to deploy SAS components in the cluster is required.
A dedicated namespace per deployment	Sharing a namespace with other software deployments is not generally supported. However, a namespace can be shared with software that SAS recommends in order to support logging, monitoring, and other features. You can determine what namespaces are defined in your cluster by running the following command: `kubectl get namespaces`
Kubernetes cluster that meets platform-specific requirements	Supported versions of Kubernetes are specified in “Platform-Specific Requirements” on page 11. VM resource recommendations are provided in “Sizing Recommendations” on page 35.
Node pools with required labels and taints	For more information about labels and taints, see “Plan the Workload Placement” in *SAS Viya Platform: Deployment Guide*.
Jump server IP address and administrative user	Optional for the deployment.
Persistent volume mounts, storage class, PVCs, and any required provisioners	Storage requirements are partially dependent on the SAS products that you are deploying. For more information, see “Persistent Storage Volumes, PersistentVolumeClaims, and Storage Classes”. The default storage class requires a provisioner.

Cluster Setup Task	Notes
Shared storage that conforms to SAS recommendations	A shared file system is required for multiple purposes, including private user directories. A file server that uses the network file system (NFS) protocol is the minimum requirement. An additional VM might be created for this purpose.
An ingress controller and IP addresses	For more information, see “Cluster Ingress Requirements”.
A certificate generator to enable TLS	The OpenSSL-based certificate generator supplied by SAS is used by default. You can instead use cert-manager if you install it in the cluster and take a few additional steps. For more information, see “TLS Requirements”.

Upgrading Kubernetes

Upgrading to a more recent version of Kubernetes does not require you to redeploy the SAS Viya platform. However, the order in which you upgrade Kubernetes and update the SAS software is important. First, consult the following table to verify Kubernetes version support and compatibility:

Table 2 *Kubernetes Version Support*

SAS Viya Platform Version	Supported Versions of Kubernetes
2023.06 (Stable)	1.24, 1.25, 1.26
2023.05 (Stable)	1.24, 1.25, 1.26
2023.04 (Stable)	1.23, 1.24, 1.25
2023.03 (Stable)	1.23, 1.24, 1.25
2023.03 (LTS)	1.23, 1.24, 1.25
2022.09 (LTS)	1.21, 1.22, 1.23, 1.24

If the version of Kubernetes that is currently running in your environment is not supported for the version of the SAS Viya platform to which you are updating, take the following steps:

1. First, stop all SAS Viya platform services.

   You can run the sas-stop-all CronJob in order to stop all services.

2. Upgrade the Kubernetes cluster to a supported version. Make sure that you upgrade to a version that is supported by both the existing version of the SAS Viya platform and the newer version to which you plan to update.

3. Verify that any dependent components, such as ingress-nginx and the optional cert-manager component, have been upgraded to versions that are compatible with the Kubernetes version to which you are upgrading.
4. Restart all SAS Viya platform services.
5. Update the SAS Viya platform software.

The recommended order of these steps is slightly different if your cluster has a supported version of Kubernetes.

Even if your cluster is already running a supported version of Kubernetes, you might want to upgrade Kubernetes at the same time that you update SAS software. SAS recommends taking the following steps in order to avoid issues:

1. First, update the SAS Viya platform software.
2. Stop all SAS Viya platform services.

   You can run the sas-stop-all CronJob in order to stop all services.
3. Upgrade the Kubernetes cluster.
4. Verify that any dependent components, such as ingress-nginx and the optional cert-manager component, have been upgraded to versions that are compatible with the Kubernetes version to which you are upgrading.
5. Restart all SAS Viya platform services.

Kubernetes Client Machine Requirements

The deployment requires a machine from which the Kubernetes command-line interface, kubectl, manages a Kubernetes cluster. This machine can be running Linux, Windows, or macOS.

The machine that you use to perform a deployment using Kubernetes commands requires the following client software:

- kubectl

  The kubectl version that you use on the client machine can be only one minor version later or earlier than the version of Kubernetes (kube-apiserver) that is used in the cluster. For more information, see the Kubernetes version skew policy.

  Run the following command to verify the version of kubectl on the client machine:

  ```
  kubectl version
  ```

  After kubectl is installed, note the location of the Kubernetes configuration file for use during the deployment process. The default path on Linux is **~/.kube/config**.

- Kustomize 5.0.3

  Kustomize is a client tool that is used to generate Kubernetes manifest files. Each SAS Viya platform release and cadence is optimized for and tested with a single version of Kustomize.

  Run the following command to verify the version of Kustomize on the client machine:

  ```
  kustomize version
  ```

  Download Kustomize here: https://github.com/kubernetes-sigs/kustomize/releases/tag/kustomize%2Fv5.0.3.

Other deployment methods provide the Kubernetes client machine requirements. The SAS Deployment Operator and the sas-orchestration command include supported versions of kubectl and Kustomize to help you deploy and manage the SAS Viya platform. These methods make use of the sas-orchestration image.

The sas-orchestration image requires only a recent version of Docker or another container runtime that is compliant with the Open Container Intiative (OCI) standards.

Note: If you do not use the sas-orchestration image to perform your deployment, you can also access supported versions of these tools by following the instructions in the kubernetes-tools README. After you have downloaded the deployment assets for your software order, you can find these instructions in `$deploy/sas-bases/examples/kubernetes-tools/README.md` or in HTML format in `sas-bases/docs/using_kubernetes_tools_from_the_sas-orchestration_image.htm`.

Node Requirements

The nodes in your Kubernetes cluster have the following requirements:

- A Linux operating system
- A 64-bit x86_64 chipset
- Kubernetes 1.24.*x* - 1.26.*x* installed on each node.

  To check your version of Kubernetes, run the following command:

  ```
  kubectl version
  ```

- (For deployments on open source Kubernetes only) A containerd runtime
- One of the following requirements for OpenSearch:
  - A cluster-wide setting to enable privileged containers
  - Increased virtual memory settings on the nodes that host stateful workloads

  For more information about these requirements, see “OpenSearch Requirements”.

Additional machine requirements are described in “Resource Guidelines”.

Cluster Ingress Requirements

The SAS Viya platform supports ingress-nginx 1.3.0 and later.

Istio Ingress and Istio Gateway are not supported at this time. NGINX Ingress Controller with NGINX or NGINX Plus is not supported at this time.

Make sure that the version of ingress-nginx that you are using is compatible with your cloud provider, and check for updates. Settings might be changed by the cloud provider that affect ingress functionality between existing and newer clusters.

If you have a load balancer, application gateway, or reverse proxy in front of the ingress controller to function as the "front door" to your cluster, see “(Optional) Additional Requirements for Proxy Environments” on page 10 for information about required configuration.

Additional settings are required for your ingress controller. Unless otherwise noted, they apply to all platforms, including VMware environments and those with physical machines:

- A static public IP address, which is created automatically when the Kubernetes LoadBalancer service is created for the ingress controller.

Note: The term *public* in this usage means that the IP address is routable outside the internal VNet. Exposing the public IP address on the internet is not required. However, clients that are positioned both inside and outside the SAS Viya platform Kubernetes cluster must be able to find a network route to the cluster ingress endpoint.

- The public IP address or an equivalent address for the ingress controller must be registered with your DNS provider as an external endpoint.

  Note: Clients that are located outside the SAS Viya platform Kubernetes cluster must be able to resolve the ingress controller host name. Using DNS, they must be able to resolve the host name to a public IP address that is assigned to the ingress controller load balancer. Typically, this routable IP address is the default external address of the load balancer, but it can also be one of multiple IP addresses that are assigned to the load balancer.

  For Microsoft Azure, for GCP, and for Anthos Clusters on VMware, an `A` record must point to the IP address.

  For AWS, a `CNAME` record must point to the fully qualified domain name (FQDN). AWS assigns `A` records (DNS FQDNs) to load balancers. For AWS, you should create the desired DNS name for each load balancer as a `CNAME` record and configure it with the FQDN.

  For open source Kubernetes, you must have an `A` record with the FQDN associated with the load balancer and a `CNAME` record consisting of a wildcard entry pointing to that `A` record.

- An external URL that is configured for the Ingress object and that is reachable from pods that run inside the cluster.
- Firewall rules that allow external traffic to reach the ingress.

  Routes to the ingress should not be subjected to network address translation (NAT). NAT placement before the ingress causes the SAS Viya platform audit service to report incorrect remote addresses.

  Any NodePort or LoadBalancer services that the cluster uses for ingress must have their externalTrafficPolicy set to `Local`. As a result, an ingress pod must be deployed to the node that is receiving connection requests. Be aware of these requirements if you are using kube-proxy or an ingress operator to handle connections to cluster nodes.

- A reasonable time-out setting on the ingress controller.

  The default time-out value might be too low. SAS recommends setting a 300-second time-out in most environments.

- Adequate buffer sizes for request and response headers.

  The SAS Viya platform passes OAuth tokens in the request and response headers. The size of each token varies, depending on the number of group memberships that are associated with each user account. For ingress-nginx, the default configuration uses 32 KB request headers and 16 KB response headers.

  For OpenShift, the default limit is 24 KB for both request and response headers.

- If a reverse proxy server is active between the network and the ingress controller, ingress-nginx configuration changes are required. For more information, see “(Optional) Additional Requirements for Proxy Environments”.

IMPORTANT A vulnerability has been found that affects ingress-nginx, CVE-2021-25742. The SAS Viya platform supports a mitigation for this CVE, the application of a block list. For

more information, see “ingress-nginx Vulnerability Mitigation” in *SAS Viya Platform: Deployment Guide*.

(Optional) Additional Requirements for Load Balancers

A Kubernetes LoadBalancer service is created for the ingress controller when it is installed. The installation triggers the creation of an external (routable) IP address that is associated with an external load balancer, both of which are provisioned by the cloud provider. This IP address is used for all external HTTP/HTTPS connections to SAS Viya platform user interfaces and services. See the section on the LoadBalancer service in the Kubernetes documentation for more information.

Additional Kubernetes load balancers are required in order to enable optional external user access to the CAS controller or to SAS/CONNECT.

An ingress controller is not sufficient to enable (optional) user access to the CAS controller binary port or to the SAS/CONNECT port from outside the cluster. The connections are not HTTP connections. Therefore, you must define a Kubernetes service of type *LoadBalancer* in order to make the non-HTTP ports externally accessible.

The following settings are required for your additional Kubernetes LoadBalancer services:

- A static public IP address.

  Note: The term *public* in this usage means that the IP address is routable outside the internal VNet. Exposing the public IP address on the internet is not required.

- Static DNS names and ports.
- (For AWS only) A reasonable time-out value.

  The default time-out value might be too low. For example, the default time-out for AWS load balancers, 60 seconds, is too low. SAS recommends setting a 300-second time-out in most environments.

  This setting can be changed for all of your CAS load balancers by specifying the `service.beta.kubernetes.io/aws-load-balancer-connection-idle-timeout` annotation in the metadata of the CASDeployment serviceTemplate. An example of the YAML for this modification is included in **`sas-bases/examples/cas/configure/cas-enable-external-services.yaml`**.

In some situations, users might connect directly to a node port or LoadBalancer service from an external IP address or host name, bypassing the ingress controller. Such cases might involve the use of SAS/CONNECT or the CAS programming interfaces, for example. To support TLS, additional configuration is required. For more information, see “TLS Requirements” on page 58.

(Optional) Additional Requirements for Proxy Environments

Your ingress controller requires additional configuration in environments where an application gateway, a load balancer, or a reverse proxy server is set up as a "front door" for the cluster ingress.

A variable in the SAS Viya platform deployment manifest, `SAS_SERVICES_URL`, specifies the host name and port of the ingress controller for use by the compute server component. Similarly, to enable pods to reach the ingress controller, the value for the `{{ NAME-OF-INGRESS-HOST }}` parameter must match the value of the `INGRESS_HOST` variable. All these values should represent the “front door” to your cluster. Therefore, you can specify a load balancer or application gateway as the value for

SAS_SERVICES_URL and INGRESS_HOST. This configuration is also appropriate for external reverse proxies. The load balancer can be for the ingress or external. For more information, see "Initial kustomization.yaml File" in *SAS Viya Platform: Deployment Guide*.

The X-Forwarded-Port and X-Forwarded-Proto headers on incoming traffic enable SAS Viya platform services that are running behind proxies to construct the original URL of each request. Verify that the external proxy server is setting the X-Forwarded-Port and X-Forwarded-Proto headers correctly and that it is forwarding requests to the ingress without changing the URL path.

If you are using a reverse proxy server with ingress-nginx, the ingress-nginx configuration setting use-forwarded-headers must be changed from the default "false" to "true". This change is required in order to enable ingress-nginx to pass incoming X-Forwarded-* headers from the reverse proxy to SAS Viya platform services.

After the deployment has completed, you can use SAS Environment Manager to configure SAS Viya platform services to trust the X-Forwarded-* headers on incoming traffic. For more information, see "Reverse Proxy Servers" in *SAS Viya Platform Identity and Access Management: Fundamentals*.

Requirements that vary according to the supported platform are summarized in "Platform-Specific Requirements" on page 11.

Platform-Specific Requirements

Before you start the SAS Viya platform deployment process, verify that your selected environment has the additional requirements that are described in the following tables.

At this time, only the cloud providers, virtualization platforms, and physical environments that are specified here are supported. Note that SAS does not support the on-premises Kubernetes services that are supplied by the public cloud providers. SAS provides Limited Support for the SAS Viya platform when it is deployed on a distribution of Kubernetes that is not listed here. See https://support.sas.com/en/technical-support/services-policies.html#k8s for the detailed support policy that applies to Kubernetes.

Cluster Requirements for Microsoft Azure

The following table summarizes cluster requirements in a Microsoft Azure environment:

Table 3 *Cluster Requirements for Microsoft Azure*

Required Component	Detailed Requirements
Kubernetes	Microsoft Azure Kubernetes Service (AKS) 1.24.*x* - 1.26.*x*. **Note:** Be aware that some components, such as ingress-nginx and cert-manager, require upgrades to newer releases for use with Kubernetes 1.24.*x* or later. Check the appropriate third-party documentation for these compatibility requirements. In addition, refer to "Upgrading Kubernetes" for a workflow that avoids issues. **IMPORTANT** If you plan to upgrade Kubernetes from 1.22 to 1.23 or later and have an active SAS Viya platform deployment in place, be sure to stop the platform deployment before

Required Component	Detailed Requirements
	upgrading Kubernetes. Once the upgrade is complete, the SAS Viya platform deployment can be safely started.
Node pools	Cloud providers use different terminology to refer to collections of nodes. A minimum of three *dynamic node pools* is required: ■ One default node pool Because SAS Viya platform software is not intended to run on these nodes, minimal resources are required. For more information, see "Default Node Pool Configuration" in *SAS Viya Platform: Deployment Guide*. ■ Two user node pools One of these node pools must be fully dedicated to the CAS server components. After the deployment has completed, if SAS pods are landing on the default node pool in your configuration, reevaluate the size of the VMs in these user node pools. SAS recommends creating five node pools, including the default node pool. Node pools that span multiple availability zones are not recommended and require additional configuration. For example, Azure managed disks (the default storage class for AKS) are not zone-redundant. In this case, SAS recommends that you follow the advice in this Microsoft document. (Optional) If you want to deploy with confidential computing, select only AMD SEV confidential VM instance types. For more information, see "Requirements for Confidential Computing" on page 61. Recommended node sizes are provided in "Sizing Recommendations for Azure".

Cluster Requirements for AWS

Most offerings on the SAS Viya platform support deployment with Amazon Elastic Kubernetes Service. Exceptions are noted in "Software Offerings and Platform Compatibility" on page 84.

The following table summarizes cluster requirements in an AWS environment:

Table 4 *Cluster Requirements for AWS*

Required Component	Detailed Requirements
Kubernetes	Amazon Elastic Kubernetes Service (Amazon EKS) 1.24.*x* - 1.26.*x*. **Note:** Be aware that some components, such as ingress-nginx and cert-manager, require upgrades to newer releases for use

Required Component	Detailed Requirements
	with Kubernetes 1.24.*x* or later. Check the appropriate third-party documentation for these compatibility requirements. In addition, refer to "Upgrading Kubernetes" for a workflow that avoids issues.
A Kubernetes Metrics Server	Kubernetes Metrics Server 0.5.*x* or later is required. For more information, see https://github.com/kubernetes-sigs/metrics-server.
AWS Elastic Block Store (EBS) CSI driver	The EBS CSI driver is required. For more information, see https://docs.aws.amazon.com/eks/latest/userguide/ebs-csi.html.
Kubernetes cluster auto-scaler	The Kubernetes auto-scaler is required. For more information, see https://github.com/kubernetes/autoscaler/.
Managed node groups	Cloud providers use different terminology to refer to collections of nodes. A minimum of three *dynamic node pools* is required: ■ One default node pool Because SAS Viya platform software is not intended to run on these nodes, minimal resources are required. For more information, see "Default Node Pool Configuration" in *SAS Viya Platform: Deployment Guide*. ■ Two additional node pools for SAS pods One of these node pools must be fully dedicated to the CAS server components. After the deployment has completed, if SAS pods are landing on the default node pool in your configuration, reevaluate the size of the machines in these user node pools. SAS recommends creating five node pools, including the default node pool. All machine instances for the SAS Viya platform deployment should be in the same AWS placement group. Recommended node sizes are provided in "Sizing Recommendations for AWS".

Cluster Requirements for Google Cloud Platform (GCP)

Most offerings on the SAS Viya platform support deployment with Google Kubernetes Engine. Exceptions are noted in "Software Offerings and Platform Compatibility" on page 84.

The following table summarizes cluster requirements in a GCP environment:

Table 5 *Cluster Requirements for Google Cloud Platform*

Required Component	Detailed Requirements
Kubernetes	Google Kubernetes Engine (GKE) 1.24.*x* - 1.26.*x*. **Note:** Be aware that some components, such as ingress-nginx and cert-manager, require upgrades to newer releases for use with Kubernetes 1.24.*x* or later. Check the appropriate third-party documentation for these compatibility requirements. In addition, refer to "Upgrading Kubernetes" for a workflow that avoids issues.
Node pools	Cloud providers use different terminology to refer to collections of nodes. A minimum of three *dynamic node pools* is required: ■ One default node pool Because SAS Viya platform software is not intended to run on these nodes, minimal resources are required. For more information, see "Default Node Pool Configuration" in *SAS Viya Platform: Deployment Guide*. ■ Two additional node pools for SAS pods One of these node pools must be fully dedicated to the CAS server components. After the deployment has completed, if SAS pods are landing on the default node pool in your configuration, reevaluate the size of the VMs in these user node pools. SAS recommends creating five node pools, including the default node pool. Node pools that span multiple zones are not recommended. Recommended node sizes are provided in "Sizing Recommendations for GCP and Anthos Clusters on VMware".
(For GKE 1.26 and later) Authentication plug-in	Install the gke-gcloud-auth-plugin on any nodes where you will run kubectl. This step is required before you upgrade the cluster to GKE 1.26. For more information, see Important changes to Kubectl authentication are coming in GKE v1.26. The requirement for the plug-in is the result of a change to the Kubernetes code base that included the removal of all provider-specific code.

Cluster Requirements for Anthos Clusters on VMware

Most offerings on the SAS Viya platform support deployment in Anthos clusters on VMware (GKE on-prem). Exceptions are noted in "Software Offerings and Platform Compatibility" on page 84.

The following table summarizes cluster requirements for Anthos clusters on VMware:

Table 6 *Cluster Requirements for Anthos Clusters on VMware*

Required Component	Detailed Requirements
Kubernetes	Use a version of Anthos clusters on VMware that is compatible with GKE 1.24.*x* - 1.26.*x*. For more information, see Anthos version history. That resource also describes version compatibility with VMware vSphere.
Node pools	Cloud providers use different terminology to refer to collections of nodes. A minimum of three *dynamic node pools* is required: ■ One default node pool Because SAS Viya platform software is not intended to run on these nodes, minimal resources are required. For more information, see "Default Node Pool Configuration" in *SAS Viya Platform: Deployment Guide*. ■ Two additional node pools for SAS pods One of these node pools must be fully dedicated to the CAS server components. After the deployment has completed, if SAS pods are landing on the default node pool in your configuration, reevaluate the size of the VMs in these user node pools. SAS recommends creating five node pools, including the default node pool. Node pools that span multiple zones are not recommended. Recommended node sizes are provided in "Sizing Recommendations for GCP and Anthos Clusters on VMware".

Cluster Requirements for Red Hat OpenShift

Most offerings on the SAS Viya platform support deployment with Red Hat OpenShift. Exceptions are noted in "Software Offerings and Platform Compatibility" on page 84.

IMPORTANT The combination of Red Hat OCP 4.12 and an internal instance of the PostgreSQL database is experimental starting with the 2023.03 release of the SAS Viya platform. *Experimental* software has been tested prior to release, but because it has not necessarily been tested to production-quality standards, it should be used with care.

Internal PostgreSQL is based on Crunchy Data PostgreSQL 5.3, which does not support OCP 4.12 and later. SAS recommends that you deploy on Red Hat OpenShift with OCP 4.11 if you want to use the internal PostgreSQL instance.

The following table summarizes cluster requirements in a Red Hat OpenShift environment:

Table 7 *Cluster Requirements for OpenShift*

Required Component	Detailed Requirements
Kubernetes	Red Hat OpenShift Container Platform (OCP) 4.11 - 4.13 on VMware vSphere 7.0.1 or later. These versions align with the supported versions of Kubernetes (1.24.*x* - 1.26.*x*). SAS has tested only with a user-provisioned infrastructure installation.
Compliant machines	Red Hat Enterprise CoreOS (RHCOS) is the only operating system that Red Hat supports for OCP control plane nodes. Red Hat enables you to use Red Hat Enterprise Linux on the worker nodes, but SAS has tested only with RHCOS. Recommended node sizes are provided in “Sizing Recommendations for OpenShift”.
Cluster ingress	Only the OpenShift Ingress Operator is supported. You must modify the kustomization.yaml file to enable routes. For more information, see “Create the File” in *SAS Viya Platform: Deployment Guide*. Verify that the requirements in “Cluster Ingress Requirements” have also been met.
Kubernetes LoadBalancer services	Usage varies based on the underlying infrastructure. See the endpointPublishingStrategy configuration parameter section of the OpenShift Ingress Operator documentation for information about whether a LoadBalancer service is used by your cluster infrastructure. If you are using a load balancer, application gateway, or reverse proxy to function as the "front door" to your cluster, see “(Optional) Additional Requirements for Proxy Environments” on page 10 for information about required configuration.
Node labels	One or more nodes should be fully dedicated to (that is, labeled and tainted for) the CAS server. This recommendation depends on whether your deployment uses the CAS server. SAS strongly recommends labeling at least one node for compute workloads. **Note:** If your deployment includes SAS Workload Management, you must label at least one node for the compute workload class. For more information, see “Plan the Workload Placement” in *SAS Viya Platform: Deployment Guide*.
A certificate generator to enable TLS	The OpenSSL-based certificate generator supplied by SAS is used by default. You can instead use cert-manager if you install it in the cluster and take a few additional steps. **Note:** SAS Viya platform deployments on OCP 4.11 using cert-manager require a fix that is only available in cert-manager v1.10 and later. For more information about your options for TLS support and certificate management, see “TLS Requirements”.

Required Component	Detailed Requirements
cert-utils-operator	This operator from the Red Hat Communities is required in order to manage certificates for TLS support and to create keystores. For more information, see https://github.com/redhat-cop/cert-utils-operator/blob/master/README.md.

Basic Tuning Suggestions

Multiple default settings for OpenShift in a VMware environment might not provide acceptable performance. The following recommendations have not been systematically tested by SAS. However, in our test environments, they have been shown to improve performance. Performance improvements in your environment are not guaranteed and require testing.

Note: Be aware that manual modifications do not persist after a restart of an OpenShift node. The cluster administrator must use an alternative method to save these settings.

The default process ID (PID) limit setting for the container runtime daemon named CRI-O is very low (1024). Setting the CRI-O `pids_limit` to 65536 might reduce latency. In most environments, you should also set latency sensitivity to `high`.

In the **`/etc/security/limits.conf`** file, configure the following settings:

- set `nofile` to 150000
- set `nproc` to 100000

The Kubernetes parameter SupportPodPidsLimit enables support for limiting the number of processes that are running in a pod. This parameter is enabled by default in OpenShift. It can be enabled or disabled only during the initial deployment of an OpenShift cluster. Consider whether the VM administrator should disable this limit or change this value before you deploy the SAS Viya platform in an OpenShift cluster. For example, consider whether many users will use the SAS Viya or CAS REST APIs. When these APIs are used, the number of active processes increases significantly. A similar increase is not seen when using SAS user interfaces.

The number of PIDs per pod should be set based on the following guidance:

- The maximum number of PIDs that are set for the VM where the pod is running
- The number of PIDs that are required by Kubernetes on the VM
- The number of pods per VM
- Whether the node is fully dedicated to a SAS component

Try setting SupportPodPidsLimit to the same value as is recommended for CRI-O, 65536. Or consider testing with the value set to `max`.

The following command returns the number of processes that are active:

```
ls -1d /prod/*/task/* | wc -l
```

In the **`/etc/sysctl.conf`** file, you can configure networking settings. SAS has tested with the following settings:

- `net.core.somaxconn=2048`
- `net.core.netdev_max_backlog=10000`
- `net.core.netdev_budget=1000`
- `net.core.rmem_max=8388608`

- `net.core.wmem_max=8388608`

Consider whether to change reserved system memory. You can modify worker-custom-config.yaml as follows:

```
apiVersion: machineconfiguration.openshift.io/v1
kind: KubeletConfig
metadata:
  name: custom-worker-config
spec:
  machineConfigPoolSelector:
    matchLabels:
      worker-custom-config: enabled
  kubeletConfig:
    podsPerCore: 10
    maxPods: 180
    systemReserved:
      cpu: 2000m
      memory: 8Gi
```

Red Hat OpenShift documentation describes multiple ways to set node-level parameters. SAS recommends consulting the following OpenShift resources as you test various settings in your environment:

- Customizing nodes
- Post-installation machine configuration tasks

Cluster Requirements for Upstream Open Source Kubernetes

SAS supports the deployment of the SAS Viya platform into clusters that are managed by upstream Kubernetes, the open source software and tools in the GitHub repository that is hosted by the Cloud Native Computing Foundation (CNCF) at https://github.com/kubernetes/kubernetes.

Note: Support for the operation of the SAS Viya platform in a Kubernetes distribution or platform that is not specifically mentioned in this documentation is described in the SAS policy Support for Alternative Kubernetes Distributions. Vendor-packaged upstream Kubernetes distributions—by definition, those that are not installed from the CNCF Kubernetes repository—fall under this policy.

The following table summarizes cluster requirements in an open source Kubernetes environment:

Table 8 *Cluster Requirements for Upstream Open Source Kubernetes*

Required Component	Detailed Requirements
Kubernetes	Kubernetes 1.24.*x* - 1.26.*x*, running on physical machines or on VMs that meet the Kubernetes cluster node requirements on page 8. Deploying SAS Viya on upstream open source Kubernetes using VMs that are running in public cloud environments (such as Azure, AWS, or GCP) is not supported. Use the supported

Required Component	Detailed Requirements
	managed Kubernetes services (such as AKS, EKS, or GKE) instead. **Note:** Check the appropriate third-party documentation to verify the compatibility requirements of components such as ingress-nginx and cert-manager with your version of upstream Kubernetes.
Calico Container Network Interface (CNI) Plug-in	At this time, Calico 3.24.*x* or later is the only software-defined networking layer for Kubernetes that is supported for a SAS Viya platform deployment in open source Kubernetes.
IP address management utility	To manage the required load balancer IP addresses, a utility like kube-vip or MetalLB is required.
A Kubernetes Metrics Server	Kubernetes Metrics Server 0.5.*x* or later is required. Your Kubernetes distribution might provide this component by default. For more information, see https://github.com/kubernetes-sigs/metrics-server.
Nodes	Collections of nodes are required in order to handle jobs from the various SAS Viya platform workload classes and to provide high availability. SAS refers to these designated collections as *node pools*. A minimum of four node pools is required: ■ One node pool for the control plane The control plane is used to manage a Kubernetes cluster. On the supported cloud platforms, these nodes are not accessible to or managed by the user; however, when you are creating and managing your own cluster, you must supply resources for these nodes. For more information about the control plane, see the Kubernetes documentation. ■ One default node pool Because SAS software is not intended to run on these nodes, minimal resources are required. For more information, see "Default Node Pool Configuration" in *SAS Viya Platform: Deployment Guide*. ■ Two additional node pools for SAS pods After the deployment has completed, if SAS pods are landing on the nodes in your default node pool, reevaluate the size of the VMs in these node pools. SAS recommends creating five node pools, including a default node pool and a node pool (with a minimum of one node) for the control plane. Recommended node sizes are provided in "Sizing Recommendations for Open Source Kubernetes".
Node labels	One or more nodes should be fully dedicated to (that is, labeled and tainted for) the CAS server. This recommendation depends on whether your deployment uses the CAS server.

Required Component	Detailed Requirements
	SAS strongly recommends labeling at least one node for compute workloads. **Note:** If your deployment includes SAS Workload Management, you must label at least one node for the compute workload class. For more information, see "Plan the Workload Placement" in *SAS Viya Platform: Deployment Guide*.

Hardware and Resource Requirements

Storage Requirements

Use the information in this section to estimate the sizes of storage devices for your deployment.

Storage Overview

When selecting a storage option, keep in mind that your assortment of SAS product offerings, the number of users, and the amount of data that is processed all affect sizing requirements for performance. The performance of shared storage options is highly vendor-dependent.

The SAS Viya platform requires both high-performing local storage and shared storage. Network-based storage can perform better than locally mounted storage if bandwidth is adequate. However, SAS recommends provisioning the CAS server and compute nodes with both high-performing local storage and shared storage.

In addition to using persistent storage for configuration data and caslibs, the CAS server also uses high-performing storage for the CAS disk cache. Locally attached, ephemeral storage is ideal for this purpose. For more information about CAS storage requirements, see "Persistent Storage Volumes, PersistentVolumeClaims, and Storage Classes" on page 22.

The SAS Programming Run-Time Environment, which includes SAS Compute Server, SAS/CONNECT server, and SAS Batch Server, produces workloads in the compute workload class. These components must be able to create temporary files and data sets in a storage volume. For more information, see "SAS Programming Runtime Environment Requirements" on page 34.

SAS Viya Monitoring for Kubernetes is an optional solution for monitoring SAS Viya platform deployments. If deployed, it requires additional storage for log messages and performance metrics that are collected from the SAS Viya platform. The amount of storage that is required by this monitoring solution is heavily dependent on your retention policies. For more information, see the SAS Viya Monitoring for Kubernetes project in GitHub: https://github.com/sassoftware/viya4-monitoring-kubernetes.

Instructions for modifying storage settings are provided in README files for several SAS Viya platform components. For example, the file titled "Configuration Settings for CAS" explains how to change the storage size for CAS PersistentVolumeClaims (PVCs), how to modify the resource allocation for ephemeral storage, and how to change the accessModes on the CAS permstore and data PVCs. After you have downloaded the deployment assets for your software order, the README

files are located at `$deploy/sas-bases/examples/` (for Markdown format) or at `$deploy/sas-bases/docs/` (for HTML format). To modify storage for any component, first consult its README file.

I/O Throughput and Performance Considerations

The peak I/O throughput requirements of your SAS Viya platform deployment might exceed the capabilities of your storage configuration. SAS generally recommends sequential I/O bandwidth of 90-120 MB per second, per physical CPU core for both persistent and ephemeral storage. For best performance, select VM instance types with the highest available I/O throughput levels. On Microsoft Azure, Premium storage is required in order to achieve these I/O throughput levels.

Although it is high-performing, NVMe offers only ReadWriteOnce (RWO) storage that does not persist after a pod restarts. ReadWriteMany (RWX) storage is required for multiple SAS Viya platform components.

You should consult your cloud provider's storage and compute instance documentation to ensure that the storage environment can provide the level of I/O that is required. SAS Technical Support found that many performance issues reported by SAS customers can be directly attributed to insufficient levels of I/O throughput.

For a more detailed discussion of storage selection for performance, see "Provisioning Hardware for Performance" in *SAS Viya Platform Administration: Tuning*.

Disk Space and Sizing Guidelines

Most SAS Viya platform components use the same base container and Docker layers in order to optimize disk usage. The minimum amount of disk space that is required for the installation and for logging is 48 GB. Therefore, the minimum combined capacity of the Kubernetes worker nodes should be 48 GB.

The number of containers and the size of the images depend on the products in the software order. These images require approximately 30-60 GB of disk space on the host on which you are downloading SAS images and also in the destination registry.

If you are using the optional SAS Mirror Manager, the same sizing guidelines apply to the machine where you run it. After the first run, SAS Mirror Manager creates a local copy of the container images to make the process of mirroring images as quick as possible.

If you are using an NFS server for persistent storage, SAS recommends that you provision it with surplus space in order to manage expected data volumes. NFS management strategies to free up space or to allocate additional space by expanding PV quotas are not effective in the absence of sufficient space. As an example, in the case of the PostgreSQL database that supports SAS Infrastructure Data Server, partially written data sets might might need to be repaired, and other issues can affect the database if the backing store lacks space.

Encrypted File Systems

Your security policies might require encryption in order to secure data stored on disk (that is, data at rest). Cloud providers and Red Hat OpenShift provide encrypted disk StorageClass options. The SAS Viya platform supports these options, as well as solutions for encrypting stored data in attached physical storage devices, managed by open source Kubernetes. The requirements for encrypted disks and Kubernetes storage provisioners depend on your environment.

The SAS Viya platform supports encrypting files at rest in a path location. Path-based caslibs and DNFS caslibs are the only caslibs that support encryption. Keep in mind that the addition of

encryption entails processing overhead and is likely to affect SAS Viya platform performance. Compliance with the requirements that are described in "I/O Throughput and Performance Considerations" on page 21 is strongly recommended.

> **IMPORTANT** Disk encryption does not replace TLS in a SAS Viya platform deployment. Local storage, NFS, or other persisted data requires secured access to the data and TLS for network traffic in addition to encrypted storage.

Generally, SAS recommends using the native encryption options that are offered by your cloud provider. For example, on AWS, use the AWS-provided encryption for Elastic Block Store (EBS). Cloud providers typically provide disk encryption by default. GlusterFS can be used to encrypt storage for OpenShift.

On physical machines or in situations where cloud or virtualized disk encryption options are not available, you can use LUKS or Dm-crypt to encrypt storage. With these options, use local or appliance SSD or NFS provisioners. For more information, see https://gitlab.com/cryptsetup/cryptsetup/ or https://en.wikipedia.org/wiki/Dm-crypt. The VMware vSphere documentation describes how to set up encrypted storage on VMware.

SAS has tested with various Kubernetes SIG provisioners, including local, NFS, and GlusterFS. These provisioners consume block storage that can be encrypted in a SAS Viya platform deployment.

Persistent Storage Volumes, PersistentVolumeClaims, and Storage Classes

Persistent storage is required by multiple SAS Viya platform components. Verify that at least one ReadWriteMany (RWX) StorageClass has been defined and set as your default. Run the following command to verify that a default StorageClass has been defined:

```
kubectl get storageclass
```

Make a note of the names of all storage classes in case you later need to modify storage settings. You must also update the base kustomization.yaml to specify the PVCs that are associated with the RWX StorageClass. For more information, see Specify PersistentVolumeClaims to Use ReadWriteMany StorageClass.

Many storage classes have a reclaimPolicy that is set to **delete** by default. If you delete a namespace that includes such storage classes, the PVCs in that namespace are deleted. If the reclaimPolicy is Delete, the corresponding persistent volumes (PVs) are also deleted, resulting in data loss. For information about changing the reclaimPolicy in Kubernetes, see Change the Reclaim Policy of a PersistentVolume.

Multiple PVCs are configured automatically during the deployment. Here are the default settings for all deployments. Note that the default settings correspond to the minimum recommended sizes:

- redis pod — Redis replaces SAS Cache Server to provide a distributed cache technology. Redis requires three stateful sets, and each has two pods. Each pod is configured to request 1 Gi of persistent storage for a total of 6 Gi of storage; accessMode: ReadWriteOnce (RWO).
- Consul — Supports SAS Configuration Server. It is deployed with high availability (HA) by default, and three replicas, each with a 1 Gi PVC; accessMode: RWO.

  The Consul pod also requires a mount for the Consul data directory. The mount is an empty directory that points to `/consul/data`. It is configured automatically by the deployment process.
- RabbitMQ — Supports SAS Message Broker. It is deployed with HA by default and three replicas, each with a 2 Gi PVC; accessMode: RWO.

- PostgreSQL — Supports SAS Infrastructure Data Server. The requirements depend on whether you deploy the default (internal) PostgreSQL instance or you supply your own PostgreSQL server (external).

  IMPORTANT In SAS Viya platform 2022.10 and later, the internal PostgreSQL server responds to the command to delete the PostgreSQL cluster CustomResource by deleting the PostgreSQL PVCs, potentially causing data loss. You might run this command during an uninstallation. Avoid this risk by setting the reclaimPolicy to `retain`. In previous releases of the SAS Viya platform, which used an earlier version of the Crunchy Data PostgreSQL server, deleting the CR did not affect the associated PVCs.

  The internal PostgreSQL server uses PVs that are dynamically created by the storageClass. For more information about changing the reclaimPolicy of a storage class to have PVs generated with the `retain` setting, see https://kubernetes.io/docs/concepts/storage/storage-classes/.

  Requirements are summarized in the following table:

  Table 9 *SAS Infrastructure Data Server Storage Requirements*

PostgreSQL Deployment	accessMode	Default Size
Internal (the default deployment)	RWO	Deploys with HA by default: ■ Three nodes One primary and two replica data nodes. ■ PVC of 128 GB per node
External (you are responsible for this server)	Not applicable	A minimum of one volume, 128 GB of space.

  A storage class can be selected only during the initial deployment. You cannot change the storage class after the deployment has completed. After you have downloaded your deployment assets, an example file to help you change storage settings for an internal PostgreSQL server is provided in your **`$deploy/sas-bases/examples/crunchydata/storage`** directory. For more information about SAS Infrastructure Data Server requirements, see “PostgreSQL Server Requirements”.

- CAS server — Requirements depend on whether you deploy the CAS server as SMP or MPP. Two PVCs are required in either case:
  - cas-default-permstore — Required in order to store caslib management privileges
  - cas-default-data — The default location for new caslibs; equivalent to the SAS CASDATADIR setting

  Their requirements are summarized in the following table:

  Table 10 *CAS Server Persistent Storage Requirements*

CAS Server	accessMode	Default Size
SMP CAS server	Either RWO or RWX. Set to RWX by default.	cas-default-permstore: 100 Mi

CAS Server	accessMode	Default Size
		cas-default-data: 8 Gi
MPP CAS server	RWX RWX	cas-default-permstore: 100 Mi cas-default-data: 8 Gi

RWX accessMode is required for any backup controllers for CAS. To change the accessMode for either cas-default-data or cas-default-permstore, perform the steps that are described in Change accessMode.

Every CAS pod also requires a mount for the CAS disk cache. The mount is configured automatically by the deployment process. CAS server performance is partially dependent on the storage that you select. For more information, see "CAS Server Resources" on page 33.

You can modify most default resources that are provided for your CAS server. However, the mountPath that is defined for cas-default-permstore and cas-default-data cannot be modified. The associated mount points are `/cas/permstore` and `/cas/data`, respectively. To define mounts that are added to CAS overlays, you can add patchTransformers to your manifests.

- OpenSearch — Supports the search feature. Creates one PVC. Default size: 128 Gi; accessMode: RWO.

  OpenSearch requires fast disk or block storage. Storage can be provided through your virtualization platform or cloud provider, or through locally attached (physical) disk storage. For more information, see "OpenSearch Requirements".

- Backup and restore operations — Require two PVCs, described as follows:
  - sas-common-backup-data — Stores a backup file of settings for SAS Infrastructure Data Server and SAS Configuration Server. Default size: 25 GB; accessMode: RWX.
  - sas-cas-backup-data — Stores a backup of CAS server data and the CAS permstore. Default size: 8 GB; accessMode: RWX.

> **IMPORTANT** These default settings are the minimum recommended sizes. Verify that the ReclaimPolicy for these PVCs is set to **Retain**.

Persistent Volumes for Applications

Some individual products on the SAS Viya platform also require persistent storage. If your software order included these applications, you must set up additional volumes with the required settings:

- SAS Common Planning Service — Requires two volumes:
  - sas-planning-retail — Stores data for offerings that include SAS Common Planning Service. Default size: 100Gi; accessMode: RWX.
  - sas-planning-retail-backup-data — Stores backup files for SAS Common Planning Service. Default size: 100Gi; accessMode: RWX.
- SAS Data Quality — Requires a volume for SAS Quality Knowledge Base data. Default size: 8 Gi; accessMode: RWX.

- SAS Event Stream Processing — Requires a PVC that is set to RWX. In a multi-tenant deployment, one persistent volume is required per tenant. SAS Event Stream Processing Studio must be configured to use the PV. For information about sizing and configuration, see Using SAS Event Stream Processing in a Kubernetes Environment.
- SAS Micro Analytic Service — Requires storage volumes if the optional features, ASTORES or archives, are configured:
  - Volume for ASTORES — Default size: 30 GB; accessMode: RWX. Depending on model complexity and the number of models, more space might be required.

    To resize the PVC for ASTORES, update the overlay with the new size and run it. If models have already been loaded, SAS recommends setting the StorageClass attribute `allowVolumeExpansion` to true. If the provider does not support the StorageClass, resize the volume and then republish all ASTORE models.
  - Volume for archive logs — If the archive feature is enabled in SAS Micro Analytic Service, it stores input and output transaction logs in a persistent volume. Default size: 30 GB; accessMode: RWX.

    This volume grows continuously. SAS recommends that you create regular backups of this data and monitor the available space.
- SAS Studio — Requires persistent storage if users will take advantage of Git integration features.

  To enable Git integration, SAS Studio users require access to a shared file system that is accessible to the pod where the compute server is running (the pod where the compute workload has been placed). Be aware that storage on this pod is temporary unless you configure persistent storage. Configure persistent storage for the compute server if you plan to use the Git integration features. For more information, see "Creating Persistent File Storage" in *SAS Studio: Administrator's Guide*.

  Work that is associated with other SAS Studio tasks is stored in SAS Content, which does not require a persistent volume.
- SAS Viya Monitoring for Kubernetes — Requires additional storage for log messages and performance metrics. The amount of storage depends on the retention policies that you set. In order to store 5 days of logs, a minimum of 140 GB of storage is required.

  SAS Viya Monitoring for Kubernetes is an optional solution for monitoring SAS Viya platform deployments. For more information, see the SAS Viya Monitoring for Kubernetes project in GitHub: https://github.com/sassoftware/viya4-monitoring-kubernetes.
- SAS Configurator for Open Source — Requires persistent storage for Python builds. Default size: 20 GB; accessMode: RWX. The required size depends on the number of Python profiles that you configure, so more space might be required.

Requirements for the CAS Server and Programming Runtime Environment

For the SAS Viya platform components and SAS products that require persistent storage, SAS attempts to support most generally available commercial storage options. However, a few restrictions apply to the storage that you select for the CAS server and the SAS Programming Runtime Environment.

SAS requires a POSIX-compliant file system. In our testing, SAS has found that some common Container Storage Interface (CSI) drivers are not fully POSIX-compliant. These drivers should not be used for the CAS server or SAS Programming components.

In addition, some common CSI drivers do not allow distinct identities, with standard UIDs and GIDs, to own files within the file system.

The Compute component of the SAS Programming Runtime Environment must be able to set file ownership to distinct host or operating-system accounts based on identity so that files in mounted volumes can be accessed securely. For more information, see "File System and Storage Authorization" in *SAS Viya Platform Identity and Access Management: Fundamentals*.

The CAS server can require CAS sessions to run as distinct host or operating-system accounts in some configurations. For more information, see "CAS Server Authentication" in *SAS Viya Platform Identity and Access Management: Fundamentals*.

Here are some examples of common CSI drivers that have been found not to support these common SAS Viya platform file system usage patterns:

- The Microsoft AKS azure-files CSI driver. When using the SMB protocol, this CSI driver does not support the standard POSIX file system operations that SAS processes use to unlink or delete files.
- The Amazon EKS Elastic File Service (EFS) CSI driver does not allow files to be owned by distinct UIDs and GIDs. SAS processes cannot `chown` files that are stored in these volumes.

This is not an exhaustive list of storage options that do not fulfill SAS requirements. Many storage options are available across all the supported cloud platforms and Kubernetes distributions. SAS cannot test with all of them.

More detailed information about these component requirements is provided in "CAS Server Resources" on page 33 and "SAS Programming Runtime Environment Requirements" on page 34.

File System and Shared Storage Requirements

The persistent volumes described previously are required for component and application data. Various SAS Viya platform components also require a shared file system. A shared file system is required for multiple purposes, which include shared data storage and private user directories. A file server that uses the network file system (NFS) protocol is the minimum requirement.

In a Microsoft Azure environment, each VM instance type has a maximum input/output operations per second (IOPS) metric and a throughput metric, as well as a maximum number of disks that can be attached. The Microsoft Azure VM instances that SAS recommends are optimized for IOPS rather than for storage throughput. Striping can be used to increase storage IOPS and throughput, both of which are important for SAS Viya platform performance. The performance of attached disk configurations is constrained by VM limits.

The following options for shared file storage are recommended:

Table 11 *Storage Recommendations*

Cloud Provider	Standard Deployments	HA Deployments	Notes
Microsoft Azure	Azure Premium SSD Managed Disks with a shared file storage layer. When volumes are mounted to a VM instance that exports them as NFS, they have the	Azure NetApp Files	Both of these storage options are encrypted by default. Microsoft has two VM offerings, the Ebds_v5 Azure VMs, that are memory-optimized and provide increased maximum I/O

Cloud Provider	Standard Deployments	HA Deployments	Notes
	equivalent of RWX accessMode. RAID 5 is recommended.		throughput to external storage.
AWS	EBS, mounted to a VM that exports with NFS. When volumes are mounted to a VM instance that exports them as NFS, they have the equivalent of RWX accessMode.	Amazon Elastic File Share (EFS), with the following options: ■ Performance mode set to **Max I/O** ■ Throughput mode provisioned with **1024 MiB/s** or more	Installing a provisioner for EBS volumes, such as the nfs-provisioner or nfs-subdir-external-provisioner, is recommended.
GCP or Anthos Clusters on VMware	Cloud Storage When volumes are mounted to a VM instance that exports them as NFS, they have the equivalent of RWX accessMode.	Cloud Filestore, SSD tier 5 x 375 GB local SSD (RAID0)	RAID 0 is recommended.

For more information about selecting storage for performance, see “Provisioning Hardware for Performance” in *SAS Viya Platform Administration: Tuning*.

SAS also recommends using a consistent directory structure in your shared storage solution. Consistency is helpful for the following reasons:

- Multiple SAS Viya platform components require data storage.
- Some SAS offerings can also use a shared location for private user directories.
- Shared storage can serve as the location for persistent volumes to be provisioned in a consistent manner.
- The SAS Viya platform uses some shared, open-source binary files.

To optimize your deployment, create the NFS directory structure that is described in the following table:

Table 12 *Shared File System Recommended Directory Structure*

Directory	Description
`/astores`	Location of the shared directory for ASTORES and ASTORE models.
`/bin`	Location for open-source companion software directories.

Directory	Description
`/bin/nfsviyapython` `/bin/nfsviya-r`	Location for your Python binary files. Location for your R binary files.
`/data`	Location for SAS and CAS data.
`/homes`	Location for user private directories. As a best practice, create a subdirectory for each user of SAS Viya offerings.
`/pvs`	Location for persistent volumes that are provisioned using the file system.
`/permstore`	Location for the CAS server to store caslib authorization information.

`/backups`
`/backups/cas`
`/backups/common`
	Locations where SAS Viya platform backup files can be saved.

`/data-drivers/jdbc`	Location where JAR files for JDBC drivers are stored. If you add JDBC drivers for SAS data access, save them in this location so that they are available to the deployment automatically.
`/quality-knowledge-base`	Location where SAS Quality Knowledge Base stores data.

File System Permissions

The SAS Viya platform includes default fsgroup settings that enable file system access. When an fsgroup ID is set for a pod, any files that are written to a volume mounted by a container within that pod inherit that fsgroup as their group ID (GID). The fsgroup ID is the owner of the volume and of any files in that volume.

A Kubernetes administrator might want to change the default container security settings in a SAS Viya platform deployment by modifying settings in the podSpecs. For enhanced security, you might be able to remove the fsgroup settings. If your deployment is using a storage class provider that sets default file system permissions for persistent volumes to 777, the SAS Viya platform fsgroup settings are not required. You can use the remove-fsgroup-transformer resource to remove these settings during the deployment process. After you have downloaded deployment assets, locate the following README file for the instructions: `$deploy/sas-bases/examples/security/container-security/README.md` (for Markdown format) or `$deploy/sas-bases/docs/modify_container_security_settings.htm` (for HTML format).

However, the requirements for these settings are different for Red Hat OpenShift than they are for other deployment environments. If a pod is mounting an NFS volume, an SCC must be tied to the service account that enables it. For more information, see “SCCs and File System Permissions”.

Encrypted File Systems

Your security policies might require encryption in order to secure data stored on disk (that is, data at rest). Cloud providers and Red Hat OpenShift provide encrypted disk StorageClass options. The SAS Viya platform supports these options, as well as solutions for encrypting stored data in attached physical storage devices, managed by open source Kubernetes. The requirements for encrypted disks and Kubernetes storage provisioners depend on your environment.

The SAS Viya platform supports encrypting files at rest in a path location. Path-based caslibs and DNFS caslibs are the only caslibs that support encryption. Keep in mind that the addition of encryption entails processing overhead and is likely to affect SAS Viya platform performance. Compliance with the requirements that are described in “I/O Throughput and Performance Considerations” on page 21 is strongly recommended.

IMPORTANT Disk encryption does not replace TLS in a SAS Viya platform deployment. Local storage, NFS, or other persisted data requires secured access to the data and TLS for network traffic in addition to encrypted storage.

Generally, SAS recommends using the native encryption options that are offered by your cloud provider. For example, on AWS, use the AWS-provided encryption for Elastic Block Store (EBS). Cloud providers typically provide disk encryption by default. GlusterFS can be used to encrypt storage for OpenShift.

On physical machines or in situations where cloud or virtualized disk encryption options are not available, you can use LUKS or Dm-crypt to encrypt storage. With these options, use local or appliance SSD or NFS provisioners. For more information, see https://gitlab.com/cryptsetup/cryptsetup/ or https://en.wikipedia.org/wiki/Dm-crypt. The VMware vSphere documentation describes how to set up encrypted storage on VMware.

SAS has tested with various Kubernetes SIG provisioners, including local, NFS, and GlusterFS. These provisioners consume block storage that can be encrypted in a SAS Viya platform deployment.

Requirements for GPU Support

Some SAS offerings support processing-intensive features that can leverage a GPU for improved performance. For example, deep learning or deep neural network capabilities that are included with SAS Viya or SAS Viya Advanced can leverage a GPU if it is present in the cluster. In addition, SAS IML and SAS Econometrics can enhance the capabilities of the SAS Programming Environment if GPUs are present in the compute node pool and if some additional configuration is performed. A full list of SAS offerings and action sets that support a GPU is provided in “Offerings and Action Sets that Support GPU Capabilities” on page 90.

The following sections describe requirements to take advantage of GPU resources in the environment. GPU support for SAS Event Stream Processing has different requirements, which are listed in “GPU Requirements for SAS Event Stream Processing” on page 31. GPUs that meet the requirements are supported on all supported cloud platforms, with the exception of open source Kubernetes.

Supported GPU Configurations for CAS Action Sets

The following requirements apply to most SAS applications that can take advantage of a GPU:

- [ ] A CUDA-capable GPU.

  SAS has tested with GPUs that have the NVIDIA Compute Unified Device Architecture (CUDA).

  Only the NVIDIA Quadro and Tesla product families are supported.

  NVIDIA Pascal, Volta, Turing, and Ampere architectures are supported.

  Note: If you have multiple GPUs installed on the same node, they must be of the same model.

- [ ] The NVIDIA display driver, version 450.80.02 or later. SAS recommends using the latest version.

  SAS also recommends enabling NVIDIA driver persistence mode at all times. For more information, see the Driver Persistence section of the NVIDIA deployment documentation.

  When you install the NVIDIA display driver on Linux, SAS recommends following the instructions in the NVIDIA CUDA Installation Guide for Linux.

  You can download the current drivers from http://www.nvidia.com/Download/index.aspx?lang=en-us.

- [ ] (For Microsoft Azure Only) N-Series VMs for the node pool that is labeled for CAS workloads. These VMs include GPU capabilities.

- [ ] The NVIDIA device plug-in for Azure or, for other cloud environments, the NVIDIA GPU Operator might be required.

  After you have downloaded and uncompressed the deployment assets, the README file in `$deploy/sas-bases/examples/gpu/` provides installation instructions.

- [ ] `/lib64` is the first path that is defined for the LD_LIBRARY_PATH environment variable on the server where the GPU is installed.

- [ ] For some action sets, PyTorch is also required. These specific action sets are indicated in "Offerings and Action Sets that Support GPU Capabilities" on page 90.

Run the following command on the machine where the GPU is installed in order to check the device type, the driver version, and the CUDA version:

```
nvidia-smi
```

Additional configuration is required in order to enable the SAS GPU reservation service. After you have downloaded and uncompressed the deployment assets, you can find instructions for enabling GPU support in two README files:

- For CAS: `$deploy/sas-bases/examples/gpu/README.md` (for Markdown format) or `$deploy/sas-bases/docs/sas_gpu_reservation_service.htm` (for HTML).
- For SAS Programming Environment: `$deploy/sas-bases/overlays/sas-programming-environment/gpu/README.md` (for Markdown format) or `$deploy/sas-bases/docs/sas_gpu_reservation_service_for_sas_programming_environment.htm (for HTML)`

GPU Requirements for SAS Event Stream Processing

SAS Event Stream Processing supports an optional GPU environment for high-powered analytics calculations, such as scoring with analytic store (ASTORE) files. A GPU enhances the deep learning functionality in SAS Event Stream Processing streaming analytics.

Here are the basic requirements for GPU support in SAS Event Stream Processing environments:

- [ ] GPU with NVIDIA Pascal, Volta, or Ampere architecture

  JetPack 5 is required for installation on NVIDIA edge devices.

- [ ] 10 GB or more of disk space

SAS Event Stream Processing can leverage GPU capabilities in the following ways:

- Deep learning ASTOREs can use NVIDIA GPUs with CUDA or TensorRT.

  Additional actions produce ASTOREs with CUDA: reinforcement learning, style generative adversarial networks (GAN), and tabular GAN.

- ONNX Runtime can be integrated into SAS Event Stream Processing in order to deploy ONNX models into production.

  ONNX Runtime can use NVIDIA GPUs with CUDA or TensorRT, or Intel GPUs with OpenVINO.

  All dependencies for CUDA, TensorRT, and OpenVINO are included with SAS Event Stream Processing.

Resource Guidelines

The topics in this section provide recommendations for workload scheduling, node sizing, and performance optimization.

Factors That Affect Resource Requirements

Several factors affect resource utilization by SAS Viya platform components, such as the following:

- The expected amount of data that SAS Viya platform users will process
- The expected number of concurrent users
- Whether an optional GPU is used in order to leverage certain SAS Viya platform features
- Whether your CAS server implementation is SMP or MPP

Sizing for Migration

If you are migrating to this version of the SAS Viya platform from a previous (3.*x*) version, the resource utilization of both deployments will be similar.

Here is an example: if your SAS Viya 3.5 deployment included three CAS server machines with 256 GB of RAM each, you should reserve nodes with a total of 768 GB of RAM in the Kubernetes cluster and label those nodes for CAS servers.

However, accounting for the typical 90% resource utilization, you can assume that the CAS controller and workers can reliably access only about 691 GB of RAM in this environment. Therefore, one additional node with 64 GB of RAM is recommended.

Sizing Considerations

When you are preparing your environment for a SAS Viya platform deployment, it is helpful to understand some of the factors that affect node resource requirements:

- Your budget and your preference for either increasing the number of (lightly resourced) machines, or adding resources to machines.
- The anticipated number of end users and their usage patterns (such as the amount of concurrency in their usage).

  If many users will submit jobs simultaneously during peak usage times, you might allocate additional resources for the CAS and compute node pools. Supporting a large number of end users also requires more resources in the stateful and stateless node pools. Stateful nodes are used to host the SAS Infrastructure Data Server, which manages user and configuration data.

  Additional lightly resourced nodes in the stateless node pool can be made available to host authorization pods when many users log on simultaneously.
- The average and maximum sizes of data sets that users will load and manipulate. These sizes might affect the amount of disk space that is required for SAS temporary data or the CAS disk cache.
- The component usage profile of the product offerings in your SAS software order.

  For example, SAS Viya requires more CAS resources than SAS Visual Analytics. SAS Viya Advanced requires considerably more RAM than either SAS Visual Analytics or SAS Viya. You should also consider whether multiple offerings will compete with each other for resources.

The following table provides examples of SAS offerings in order to show how their resource requirements might vary, based on the SAS Viya platform components that they use. These values represent minimum resource levels to create a baseline:

Table 13 *Resource Minimums per Offering*

Offering	CAS Node Pool	Compute Node Pool	Stateful and Stateless Node Pools
SAS Visual Analytics	RAM: 64 GB per instance CPU: 8 vCPUs per instance Minimum machines: 1	RAM: 32 GB CPU: 4 vCPUs Minimum machines: 1	RAM: 64 GB per instance CPU: 20 vCPUs per instance Minimum machines: 1 node
SAS Viya	RAM: 128 GB per instance CPU: 16 vCPUs per instance Minimum machines: 1	RAM: 32 GB CPU: 4 vCPUs Minimum machines: 1	RAM: 64 GB per instance CPU: 20 vCPUs per instance Minimum machines: 1 node

Offering	CAS Node Pool	Compute Node Pool	Stateful and Stateless Node Pools
SAS Viya Advanced	RAM: 256 GB per instance CPU: 32 vCPUs per instance Minimum machines: 1	RAM: 64 GB CPU: 8 vCPUs per instance Minimum machines: 1	RAM: 64 GB per instance CPU: 20 vCPUs per instance Minimum machines: 1 node

Note: Two VCPUs should be considered equivalent to a single physical CPU core.

Nodes that handle CAS and compute workloads also require persistent storage. See “CAS Server Resources” on page 33 and “SAS Programming Runtime Environment Requirements” on page 34.

Consult with your cloud vendor before selecting machines and storage options. In addition to CPU and RAM resources, different machine instance types provide different throughput. Disk I/O is a key metric that affects SAS Viya platform performance. VM instance types often have different caps on input/output operations per second (IOPS) and throughput. OS disks and data disks also have these caps.

Network performance is another factor to consider. Virtual machines are also subject to network (specifically NIC) bandwidth caps. Look for 10 GbE or better. For a Kubernetes cluster, a CNI plug-in is likely to perform better than kubenet. (For SAS Viya with SingleStore and for open source Kubernetes deployments, a CNI plug-in is required.)

CAS Server Resources

A CAS server consists of either a single node (SMP), or a set of nodes that include one controller, optionally one backup controller, and multiple workers (MPP). (Although a one-worker MPP configuration is supported, it is not an efficient allocation of resources.) The nodes that you select for the CAS server have the following requirements:

- Adequate RAM and CPU resources.

  By default, auto-resourcing is applied: the CAS operator determines the amount of RAM for your deployment based on available RAM on the nodes where CAS workloads are running.

  The file `sas-bases/examples/cas/configure/cas-manage-cpu-and-memory.yaml` can be applied to the kustomization.yaml file if you instead want to manually specify resource requests and limits. See “Basic CAS Considerations” in *SAS Viya Platform Administration: Tuning* for some guidance if you prefer to specify the resources manually.

- Storage for the CAS disk cache.

  Every CAS pod requires a mount for this caching space. The mount is an empty directory that points to `/cas/cache`. It is configured automatically by the deployment process.

  The CAS disk cache requires storage that is at least large enough to hold all your loaded tables. A workload analysis is recommended to help with sizing it. Storage that uses the SMB protocol on page 25 is not supported.

  Performance improves if you use local storage, such as an SSD volume that is memory-mapped to provide overflow capacity for data that the CAS server processes in memory. Configure the

CASENV_CAS_DISK_CACHE environment variable to point to it. For more information, see Tune CAS_DISK_CACHE.

In a cloud environment, ephemeral storage is typically high-performing.

- Storage for required CAS PVCs.

  These PVCs are described in "Persistent Storage Volumes, PersistentVolumeClaims, and Storage Classes" on page 22.

- Fully dedicated nodes that do not share resources with any other SAS Viya components.

  To create these dedicated resources, apply taints and labels to the appropriate nodes in the CAS node pool. This recommendation ensures that the CAS server has the required resources to provide optimal performance. The recommended node taints prevent Kubernetes from scheduling workloads that could compete for resources with CAS. See Plan Workload Placement for more information.

  If resources on CAS-dedicated nodes are exhausted, CAS might be scheduled to nodes outside of the CAS node pool. If external scheduling occurs, contact your SAS account representative to address issues with CAS node pool sizing. To avoid this situation, SAS recommends that you add taints to other nodes in the cluster in conformance with the SAS workload placement strategy.

  IMPORTANT Tainting all nodes in the cluster limits workloads from components that are not SAS components from being scheduled to these nodes. Otherwise, adjustments to manifests are necessary for workloads that are not SAS components.

- (Optional) A secondary (backup) CAS controller to enable failover.

  In a multi-tenant deployment, you can have multiple backup controllers (one per tenant). MPP CAS is required. For more information, see "Add a Backup Controller for MPP CAS" in *SAS Viya Platform: Deployment Guide*.

- In a multi-tenant deployment, additional nodes that are labeled for CAS.

  Each tenant requires its own dedicated CAS server. Each CAS pod must be placed on its own node with the required nodeAffinity settings that are described in Plan Workload Placement.

SAS Programming Runtime Environment Requirements

The SAS Programming Run-Time Environment, which includes SAS Compute Server, SAS/CONNECT server, and SAS Batch Server, produces workloads in the compute workload class. These components must be able to create temporary files and data sets in a storage volume. The recommended minimum size for SASWORK is 128 GB, but many factors affect this requirement.

By default, sas-programming-environment pods are backed by an emptyDir volume named `viya`. This volume is mounted automatically and uses storage on the node. Using the default emptyDir volume is not recommended because SAS programming components can consume large amounts of storage quickly and cause nodes to shut down.

One example of a critical directory that is allocated on the `viya` volume to support SAS Programming Run-Time Environment components is SASWORK, which can rapidly outgrow a local storage volume. High-performing storage is important in order to avoid degraded SAS Viya platform performance. Ephemeral storage is an option for SASWORK, but you must prevent SAS processes from consuming disk space that is required by the node's kubelet. If your SAS Batch Server will be running jobs in SAS checkpoint/restart mode, persistent external storage is required for the corresponding `viya` volume. This requirement enables the checkpoint information that is stored in SASWORK to be saved in the case of a node failure or job preemption.

For information about modifying storage classes for SAS Programming Run-Time servers, see "External Storage Class for SAS Programming Run-Time Environment" in *SAS Viya Platform: Deployment Guide*.

Note: The name `viya` is required for the volume that supports SAS Programming Run-Time Environment components.

Sizing Recommendations

Sizing Recommendations for Azure

A minimum of three node pools is required in your cluster: one default (system) node pool, where Kubernetes and other components that are not the SAS Viya platform are deployed, and two user node pools for the SAS Viya platform. Refer to "Default Node Pool Configuration" in *SAS Viya Platform: Deployment Guide* for instructions on configuring the system node pool. One user node pool must be fully dedicated to the CAS server. The nodes in the CAS node pool require taints to prevent Kubernetes from scheduling non-CAS workloads on them. The other user node pool can host the remaining (non-CAS) component workloads. Consider creating four user node pools in order to accommodate the required workload classes.

The following table provides resource recommendations for a representative SAS product offering, SAS Viya. Derived from SAS performance testing, these estimates are for a *small* deployment, which was defined as 24 concurrent sessions accessing SAS Viya user interfaces. In SAS testing simulations, data sets were 2-5 GB and batch jobs used file sizes of 5 GB. VM instances all used an Intel Cascade Lake processor. Two vCPUs are equivalent to one physical CPU core.

Table 14 *Minimum Resource Recommendations for an Example Offering*

Workload Class	Resources
Default Node Pool	RAM: 64 GB CPU: 8 vCPUs Example number of machines: 1
CAS	RAM: 64 GB per instance CPU: 8 vCPUs per instance Storage for CAS disk cache: 150 GB Example number of machines: 3 (MPP) or 1 (SMP)
(Optional) Connect	As explained in "Workload Classes" in *SAS Viya Platform: Deployment Guide*, this class is not enabled by default. In most deployments, it is not required. RAM: 16 GB per instance

Workload Class	Resources
	CPU: 2 vCPUs Example number of machines: 1
Compute	RAM: 32 GB per instance CPU: 4 vCPUs per instance Example number of machines: 1
Stateful	RAM: 64 GB per instance CPU: 8 vCPUs per instance Minimum storage: 60 GB Example number of machines: 1
Stateless	RAM: 128 GB per instance CPU: 16 vCPUs per instance Example number of machines: 1

SAS compute workloads consist of pods that host SAS compute server instances, that run batch jobs, or that do both. Dedicating a node or a node pool on which Kubernetes schedules, or prefers scheduling, only SAS compute workloads enables more granular tuning. At least one node with the label ".sas.com/class=compute" is required if your order includes SAS Workload Management.

By default, updates are applied to your deployment using a strategy that minimizes downtime. During each SAS Viya platform software update, Kubernetes starts the updated pods and removes previous pods after verifying that newer ones are running. Therefore, your cluster requires sufficient available resources to enable duplicates of each pod to run temporarily.

Consider the following guidelines as you select image types for the VM instances in your cluster:

- Select VM instance types with Intel chips. Multiple SAS Viya platform processes performed significantly faster on Intel chips in SAS testing.
- For nodes that require PVCs, SAS recommends selecting VM instance types that support premium storage.
- The SAS Viya platform performs better on nodes with a high memory-to-CPU ratio.
- Microsoft does not recommend using machine instance types from different “generations,” such as v3 and v4, because mixing them can add latency.

These guidelines do not attempt to account for all combinations of SAS product offerings, but are intended to illustrate a typical offering. SAS strongly recommends that you consult with a sizing expert to obtain an official hardware recommendation that is based on your requirements. To request sizing expertise, contact your SAS account representative. If you need assistance in determining your SAS account representative, send an email to contactcenter@sas.com.

Sizing Recommendations for AWS

A minimum of three AWS managed node groups is required in your cluster. One node group should be reserved for components that are not the SAS Viya platform, and the remaining managed node groups are required for SAS Viya platform components. The reserved node group is referred to as the

"default node pool" in this document. Refer to "Default Node Pool Configuration" in *SAS Viya Platform: Deployment Guide* for instructions on configuring it. One managed node group must be fully dedicated to the CAS server. The nodes in the CAS node group require taints to prevent Kubernetes from scheduling non-CAS workloads on them. The other managed node group can be dedicated to the remaining (non-CAS) component workloads. Consider creating five managed node groups in order to accommodate the four required workload classes and the default node pool.

The following table provides resource recommendations for a representative SAS product offering, SAS Viya. Derived from SAS performance testing, these estimates are for a *small* deployment, which was defined as 24 concurrent sessions accessing SAS Viya user interfaces. In SAS testing simulations, data sets were 2-5 GB and batch jobs used file sizes of 5 GB. The EC2 VM instances used an Intel Cascade Lake series processor. In AWS, the number of vCPUs for an instance is indicated by a number in the name of the instance type, multiplied by 4. For example, the r5n.2xlarge instance type provides 8 vCPUs, the equivalent of 4 physical CPU cores.

Table 15 *Minimum Resource Recommendations for an Example Offering*

Workload Class	Resources
Default Node Pool	RAM: 64 GB CPU: 8 vCPUs Example number of machines: 1
CAS	RAM: 64 GB per instance CPU: 8 vCPUs per instance Storage for CAS disk cache: 150 GB Example number of machines: 3 (MPP) or 1 (SMP)
(Optional) Connect	As explained in "Workload Classes" in *SAS Viya Platform: Deployment Guide*, this class is not enabled by default. In most deployments, it is not required. RAM: 16 GB per instance CPU: 4 vCPUs Example number of machines: 1
Compute	RAM: 32 GB per instance CPU: 4 vCPUs per instance Example number of machines: 1
Stateful	RAM: 64 GB per instance CPU: 8 vCPUs per instance Minimum storage: 60 GB Example number of machines: 1
Stateless	RAM: 128 GB per instance CPU: 16 vCPUs per instance Example number of machines: 1

SAS compute workloads consist of pods that host SAS compute server instances, that run batch jobs, or that do both. Dedicating a node or a node pool on which Kubernetes schedules, or prefers scheduling, only SAS compute workloads enables more granular tuning. At least one node with the label ".sas.com/class=compute" is required if your order includes SAS Workload Management.

By default, updates are applied to your deployment using a strategy that minimizes downtime. During each SAS Viya platform software update, Kubernetes starts the updated pods and removes previous pods after verifying that newer ones are running. Therefore, your cluster requires sufficient available resources to enable duplicates of each pod to run temporarily.

Consider the following guidelines as you select instance types for the VM instances in your cluster:

- Select VM instance types with Intel chips. Multiple SAS Viya platform processes performed significantly faster on Intel chips in SAS testing.
- The SAS Viya platform performs better on nodes with a high memory-to-CPU ratio.
- In AWS, each node includes ephemeral storage. The default instance storage size is typically adequate.

These guidelines do not attempt to account for all combinations of SAS product offerings, but are intended to illustrate a typical offering. SAS strongly recommends that you consult with a sizing expert to obtain an official hardware recommendation that is based on your requirements. To request sizing expertise, contact your SAS account representative. If you need assistance in determining your SAS account representative, send an email to contactcenter@sas.com.

Sizing Recommendations for GCP and Anthos Clusters on VMware

A minimum of three node pools is required in your cluster. One node pool should be reserved for components that are not the SAS Viya platform, and the remaining node pools are required for SAS Viya platform components. The reserved node pool is referred to as the “default node pool” in this document. Refer to “Default Node Pool Configuration” in *SAS Viya Platform: Deployment Guide* for instructions on configuring it. One node pool must be fully dedicated to the CAS server. The nodes in the CAS node pool require taints to prevent Kubernetes from scheduling non-CAS workloads on them. The other node pool can be dedicated to the remaining (non-CAS) component workloads. Consider creating five node pools in order to accommodate the four required workload classes and the default node pool.

The following table provides resource recommendations for a representative SAS Viya product offering, SAS Viya. Derived from SAS performance testing, these estimates are for a *small* deployment, which was defined as 24 concurrent sessions accessing SAS Viya user interfaces. In SAS testing simulations, data sets were 2-5 GB and batch jobs used file sizes of 5 GB. The VM instances used an Intel Cascade Lake series processor.

Generally, you should use the same node-sizing recommendations for Anthos Clusters on VMware as you would use for GCP. However, the Anthos Clusters on VMware default settings are likely to be adequate. Differences are noted in the table:

Table 16 *Minimum Resource Recommendations for an Example Offering*

Workload Class	Resources
(For Anthos clusters only) Master nodes	The default settings that create master nodes in VMware are sufficient.

Workload Class	Resources
Default Node Pool	RAM: 64 GB CPU: 8 vCPUs Example number of machines: 1
CAS*	RAM: 64 GB CPU: 8 vCPUs Storage for CAS disk cache: 150 GB Example number of machines: 3 (MPP) or 1 (SMP)
(Optional) Connect*	As explained in "Workload Classes" in *SAS Viya Platform: Deployment Guide*, this class is not enabled by default. In most deployments, it is not required. RAM: 32 GB per instance CPU: 4 vCPUs Example number of machines: 1
Compute*	RAM: 32 GB per instance CPU: 4 vCPUs per instance Example number of machines: 1
Stateful*	RAM: 64 GB per instance CPU: 8 VCPUs per instance Minimum storage: 60 GB Example number of machines: 1
Stateless*	RAM: 128 GB per instance CPU: 16 VCPUs per instance Example number of machines: 1
(For Anthos clusters only) Admin cluster nodes	SAS testing used the default sizings that are specified in the YAML file that Anthos provides for admin cluster creation.

* Indicates workloads that run in the Anthos Clusters for VMware user cluster.

SAS compute workloads consist of pods that host SAS compute server instances, that run batch jobs, or that do both. Dedicating a node or a node pool on which Kubernetes schedules, or prefers scheduling, only SAS compute workloads enables more granular tuning. At least one node with the label ".sas.com/class=compute" is required if your order includes SAS Workload Management.

By default, updates are applied to your deployment using a strategy that minimizes downtime. During each SAS Viya platform software update, Kubernetes starts the updated pods and removes previous pods after verifying that newer ones are running. Therefore, your cluster requires sufficient available resources to enable duplicates of each pod to run temporarily.

Consider the following guidelines as you select an image type for the VM instances in your cluster:

- Select VM instance types with Intel chips. Multiple SAS Viya platform processes performed significantly faster on Intel chips in SAS testing.
- GCP zonal or regional persistent disks can yield improved IOPS and throughput on instances with more vCPUs.
- The SAS Viya platform performs better on machines with a high memory-to-CPU ratio, such as the GCP N2 machine type. The extended memory feature provides more memory per CPU.
- Basic SSD provided adequate disk space in SAS testing. For example, use Google File Store with the Basic SSD service tier for persistent volume storage.

These guidelines do not attempt to account for all combinations of SAS product offerings, but are intended to illustrate a typical offering. SAS strongly recommends that you consult with a sizing expert to obtain an official hardware recommendation that is based on your requirements. To request sizing expertise, contact your SAS account representative. If you need assistance in determining your SAS account representative, send an email to contactcenter@sas.com.

Sizing Recommendations for OpenShift

Note: It is helpful to understand SAS Viya platform workloads so that you can manage them effectively. The workload placement strategy that is described in *SAS Viya: Deployment* might not be appropriate for a SAS Viya platform deployment in a shared OpenShift cluster on VMWare, where high node utilization is the goal. For each installation, you should assess the level of isolation that is required for the SAS Viya platform from other applications in the cluster.

Red Hat recommends allocating three nodes for the Kubernetes control plane. These nodes can have 2–4 CPU cores with 32 GB of RAM. They support load balancing, service discovery, batch execution, and other tasks. Nodes that are not part of the control plane and that do not have taints or labels for a SAS workload class are referred to as “default nodes” in this guide. Review the Red Hat documentation to understand the control plane machine config pool.

SAS also recommends that you dedicate at least one node to CAS by labeling and tainting a node in the worker machine config pool. If you are deploying MPP CAS, label and taint additional nodes. Another option is to create a custom pool for CAS nodes in order to have dedicated auto scaling. In addition, SAS strongly recommends labeling one node in the worker machine config pool for compute workloads. At least one node with the label ".sas.com/class=compute" is required if your order includes SAS Workload Management. The remaining nodes in the worker machine config pool will be targets for the rest of the SAS Viya platform workloads.

The following table provides resource recommendations for a representative SAS Viya product offering, SAS Viya. Derived from SAS performance testing, these estimates are for a *small* deployment, which was defined as 24 concurrent sessions accessing SAS Viya user interfaces. In SAS testing simulations, data sets were 2-5 GB and batch jobs used file sizes of 5 GB. All machines used an Intel Xeon Gold processor. CPUs all used hyperthreading.

Table 17 *Minimum Resource Recommendations for the Worker Node Pool*

Workload Class	Resources per Node
Default	RAM: 64 GB CPU: 8 vCPUs Example number of nodes: 1

Workload Class	Resources per Node
CAS	RAM: 64 GB CPU: 8 vCPUs Storage for CAS disk cache: 150 GB Storage for CAS default data: 2 x 400, SSD (data redundancy is recommended) Example number of nodes: 3 (MPP) or 1 (SMP)
(Optional) Connect	As explained in "Workload Classes" in *SAS Viya Platform: Deployment Guide*, this class is not enabled by default. In most deployments, it is not required. RAM: 16 GB CPU: 2 vCPUs Example number of nodes: 1
Compute	RAM: 32 GB CPU: 4 vCPUs Example number of nodes: 1
Stateful	RAM: 64 GB CPU: 8 CPU cores Recommended minimum storage: 60 GB Example number of nodes: 1
Stateless	RAM: 128 GB CPU: 16 CPU cores Example number of nodes: 1

By default, updates are applied to your deployment using a strategy that minimizes downtime. During each SAS Viya platform software update, Kubernetes starts the updated pods and removes previous pods after verifying that newer ones are running. Therefore, your cluster requires sufficient available resources to enable duplicates of each pod to run temporarily.

Consider the following guidelines as you select machines for your cluster:

- Use machines with Intel chips. Multiple SAS Viya platform processes performed significantly faster on Intel chips in SAS testing.
- For nodes that require local storage PVCs, in order to meet I/O bandwidth requirements, SAS recommends that you select machines with high-performance storage options, such as SSD/NVMe, SAN-attached storage, or similar options.
- The SAS Viya platform generally performs better on machines with a high memory-to-CPU ratio.
- Select machines with good I/O and hyper-threading.

  The latest server generations are preferable for SAS Viya because of their faster CPUs, better local disk performance, and additional RAM. If applicable, set server power settings to maximum.

For all types of storage, SAS recommends sequential I/O bandwidth of 90–120 MB per second, per CPU core. Set up storage with an understanding of the I/O bandwidth performance that your machines can achieve.

- Select a more powerful machine for the CAS server.

These guidelines do not attempt to account for all combinations of SAS product offerings, but are intended to illustrate a typical offering. SAS strongly recommends that you consult with a sizing expert to obtain an official hardware recommendation that is based on your requirements. To request sizing expertise, contact your SAS account representative. If you need assistance in determining your SAS account representative, send an email to contactcenter@sas.com.

Sizing Recommendations for Open Source Kubernetes

It is helpful to understand SAS Viya platform workloads so that you can manage them effectively. For each installation, you should assess the level of isolation that is required for the SAS Viya platform from other applications in the cluster.

Plan for the number of nodes that will provide sufficient capacity for the software to grow within the Kubernetes cluster and enable the movement of pods and workloads as needed. SAS recommends that you dedicate at least one node to CAS and one to compute using labels and taints. If you are deploying MPP CAS, label and taint additional nodes. At least one node with the label ".sas.com/class=compute" is required if your order includes SAS Workload Management.

At least one node should be available to support the Kubernetes control plane, which is used to manage the Kubernetes cluster. A minimum of three nodes is required for high availability. On the supported cloud platforms, these nodes are not managed by the user; however, when you are creating and managing your own cluster, you must supply these nodes.

The following table provides resource recommendations for a representative SAS product offering, SAS Viya. Derived from SAS performance testing, these estimates are for a *small* deployment, which was defined as 24 concurrent sessions accessing SAS Viya user interfaces. In SAS testing simulations, data sets were 2-5 GB and batch jobs used file sizes of 5 GB. One CPU core is equivalent to 2 VCPUs.

Table 18 *Resource Recommendations for an Example Offering*

Workload Class	Resources per Node
Control Plane	RAM 4 GB CPU: 2 CPU cores Disk Space: 100 GB Example number of nodes: 3 or 5 You must have an odd number of nodes and a minimum of 3 for high availability.
Default	RAM: 64 GB CPU: 4 CPU cores Disk Space: 100 GB Example number of nodes: 1

Workload Class	Resources per Node
CAS	RAM: 64 GB CPU: 4 CPU cores Storage for CAS disk cache: 150 GB; use high-performing storage Storage for CAS default data: 2 x 400, SSD (data redundancy is recommended) Example number of nodes: 3 (MPP) or 1 (SMP)
(Optional) Connect	As explained in "Workload Classes" in *SAS Viya Platform: Deployment Guide*, this class is not enabled by default. In most deployments, it is not required. RAM: 16 GB CPU: 2 CPU cores Example number of nodes: 1
Compute	RAM: 32 GB CPU: 2 CPU cores Example number of nodes: 1
Stateful	RAM: 64 GB per instance CPU: 4 CPU cores per instance Minimum storage: 60 GB Example number of machines: 1
Stateless	RAM: 128 GB per instance CPU: 8 CPU cores per instance Example number of machines: 1

Note: CAS and compute nodes require high-performing storage.

By default, updates are applied to your deployment using a strategy that minimizes downtime. During each SAS Viya platform software update, Kubernetes starts the updated pods and removes previous pods after verifying that newer ones are running. Therefore, your cluster requires sufficient available resources to enable duplicates of each pod to run temporarily.

Consider the following guidelines as you select machines for your cluster:

- Use nodes with Intel chips. Multiple SAS Viya platform processes performed significantly faster on Intel chips in SAS testing.
- Select machines with the highest available I/O throughput levels.
- Set up storage with an understanding of the I/O bandwidth performance that your machines can achieve.

  For all types of required storage, SAS recommends sequential I/O bandwidth of 90–120 MB per second, per CPU core.

For local storage, SAS recommends using machines with high-performance storage options, such as SSD/NVMe or SAN-attached storage, in order to meet I/O bandwidth requirements.

- The SAS Viya platform generally performs better on machines with a high memory-to-CPU ratio.
- CPUs should support hyperthreading.

These guidelines do not attempt to account for all combinations of SAS product offerings, but are intended to illustrate a typical offering. SAS strongly recommends that you consult with a sizing expert to obtain an official hardware recommendation that is based on your requirements. To request sizing expertise, contact your SAS account representative. If you need assistance in determining your SAS account representative, send an email to contactcenter@sas.com.

Data Source Requirements

Data Source Requirements

Your software order included SAS/ACCESS products to support your data sources. Data access requires additional customization of your Kubernetes deployment and in some cases also requires installation of other software.

Individual SAS product offerings might support a subset of these data sources. Refer to the lists of data sources that are supported by individual offerings. Then consult the list of requirements for the SAS/ACCESS product that supports your data source for additional system requirements that apply to your environment.

Supported Data Sources

The following external data sources are supported by most offerings that run on the SAS Viya platform, including SAS Visual Analytics, SAS Viya, SAS Viya Advanced, and SAS Viya Enterprise:

- Amazon Redshift
- Google BigQuery
- Greenplum
- Hadoop with Hive
- IBM Db2
- IBM Netezza
- Impala
- IBM Informix
- Data sources accessible with a JDBC driver
- Microsoft SQL Server
- MongoDB
- MySQL
- Data sources accessible with an ODBC driver

- Oracle
- PC files
- PI System
- PostgreSQL
- Salesforce
- SAP ASE
- SAP HANA
- SAP IQ
- SAP R/3
- SingleStore
- Snowflake
- Spark
- Teradata
- Vertica
- Yellowbrick

SAS In-Database Technologies products provide access to additional data sources:

- Amazon Web Services EMR
- Databricks
- Cloudera Data Platform
- Microsoft Azure Synapse Analytics

Data Sources for SAS Visual Investigator

SAS Visual Investigator supports a subset of the data sources that the SAS Viya platform supports. You can use the following data sources with SAS Visual Investigator:

- IBM Db2
- Microsoft Azure SQL Database
- Microsoft Azure SQL Managed Instance
- Microsoft SQL Server (2017 or later)
- Microsoft SQL Server on Azure Virtual Machines
- MySQL
- Oracle
- PostgreSQL
- Teradata

Data Sources for SAS Micro Analytic Service

SAS Micro Analytic Service supports a subset of the data sources that the SAS Viya platform supports. For more information, see "Data Sources Supported for Use with SAS Micro Analytic Service" in *SAS Micro Analytic Service: Programming and Administration Guide*.

General Requirements for SAS/ACCESS

Before you start the deployment, collect the third-party libraries and configuration files that are required for your data sources. Examples of these requirements include the following:

- Third-party drivers
- ODBC drivers
- JDBC drivers
- Hadoop configuration files

When you have collected these files, place them on storage that is accessible to your Kubernetes cluster. This storage could be a mount or a storage device with a persistent volume configured.

SAS recommends organizing your software in a consistent manner on your mount or storage device. Take note of the details for your specific storage solution, as well as the paths to the configuration files within it. You will need this information before you start the deployment.

Requirements for SAS/ACCESS Interface to Amazon Redshift

SAS/ACCESS Interface to Amazon Redshift includes SAS Data Connector to Amazon Redshift.

The required client software is included with your SAS Viya platform installation. Using a Data Source Name (DSN) to connect to Amazon Redshift requires post-installation configuration of your Kubernetes deployment.

Requirements for SAS/ACCESS Interface to DB2

SAS/ACCESS Interface to DB2 includes SAS Data Connector to DB2.

IBM Db2 Connect™ must also be licensed if you plan to connect to IBM Db2 databases that are running on AS/400, VSE, VM, MVS, and z/OS systems. The following DBMS products are supported:

- IBM Db2 version 11.5 or later
- IBM Integrated Analytics System (IIAS)
- Client utilities for IBM Db2 version 11.5 or later

SAS recommends installing the latest FixPack on the client and server.

Requirements for SAS/ACCESS Interface to Google BigQuery

SAS/ACCESS Interface to Google BigQuery includes SAS Data Connector to Google BigQuery.

Required client software is included with your SAS Viya platform installation. No additional software is required.

Requirements for SAS/ACCESS Interface to Greenplum

SAS/ACCESS Interface to Greenplum includes SAS Data Connector to Greenplum.

SAS/ACCESS Interface to Greenplum supports Greenplum Database versions 6.5 or later, and the required client software is included with your SAS Viya platform deployment. Using a Data Source Name (DSN) to connect to Greenplum requires post-installation configuration of your Kubernetes deployment.

Requirements for SAS/ACCESS Interface to Hadoop

SAS/ACCESS Interface to Hadoop includes SAS Data Connector for Hadoop. The requirements in this section also apply to the HADOOP procedure, the FILENAME: HADOOP access method, and SPD Engine in HDFS.

Apache Hive 1.1 or later is required.

SAS/ACCESS Interface to Hadoop supports the following Hadoop distributions:

- Amazon Web Services EMR 5.13
- Cloudera Data Platform (CDP) 7.1 or later (Private Cloud), or CDP 7.2 or later (Public Cloud)
- Google Dataproc 2.0.45 and later
- Microsoft Azure HDInsight 3.6, 4, and 5.0

Support for for Google Dataproc and Microsoft Azure HDInsight 5.0 starts with release 2022.11 on the SAS Viya platform.

The SAS policy that applies to alternative releases or distributions of Hadoop is documented on the SAS Support website.

SAS/ACCESS Interface to Hadoop redistributes CData JDBC driver for Apache Hive. This driver enables you to make a basic Hive connection by defining a Hadoop LIBNAME statement that specifies the target JDBC URL in the URI= LIBNAME statement option. For more information about using the CData driver for Apache Hive, see “Configuring SAS/ACCESS Interface to Hadoop” in *SAS/ACCESS for Relational Databases: Reference*.

In order to access files in the Hadoop Distributed File System (HDFS), you must run the Hadoop Tracer Script in order to install required JAR files. The script has the following requirements:

- The user who is running the script must have authorization to issue HDFS and Hive commands.
- If your Hadoop deployment is secured with Kerberos, obtain a Kerberos ticket for the user before running the script.
- Python and the strace Linux library must be installed on the Hadoop cluster. If necessary, install them from the package repositories for your Linux distribution.

  Python 2.6 or later is required.

Requirements for SAS/ACCESS Interface to Impala

SAS/ACCESS Interface to Impala includes SAS Data Connector to Impala.

SAS/ACCESS Interface to Impala supports Impala Server 3.2 or a later version.

SAS/ACCESS Interface to Impala is supported on Cloudera Data Platform (CDP) Public and Private Cloud.

If you are using SAS/ACCESS Interface to Impala to connect to an Impala server on a Cloudera cluster, you must set up the Cloudera Impala ODBC driver, version 2.6.13 or a later version. For instructions, see Installation Guide for Cloudera ODBC 2.5.x Driver for Impala.

In order to take advantage of SAS/ACCESS bulk loading functionality, you must run the Hadoop Tracer Script. The script installs required JAR files that enable the SAS Viya platform servers to access files in Hadoop. For more information, see “Obtain and Run Hadoop Tracer Script” in *SAS Viya Platform: Deployment Guide*.

Requirements for SAS® In-Database Technologies

SAS In-Database Technologies is a technology bundle that is included with multiple SAS product offerings. It includes products that support distributed data sources and have distinct system requirements. To use SAS In-Database Technologies, SAS Embedded Process must be installed.

Requirements for SAS® In-Database Technologies for Hadoop Cloud Services

SAS In-Database Technologies for Hadoop Cloud Services supports the following deployment platforms:

- Amazon Elastic MapReduce (EMR) 5.30 and 6.0
- Microsoft Azure HDInsight 5.x

For in-database processing in Amazon EMR, the SAS Viya platform must be deployed in AWS. Amazon EMR can be deployed in a separate cluster, but routing must be configured to enable SAS Viya platform components to connect to Amazon EMR.

Requirements for SAS® In-Database Technologies for Cloudera Data Platform

SAS In-Database Technologies for Cloudera Data Platform supports the following distributions of Cloudera:

- Cloudera CDP 7.1 Private Cloud
- Cloudera CDP 7.2 Public Cloud

Execution against Hive tables requires Spark 2.4 or later.

Requirements for SAS® In-Database Technologies for Databricks

SAS In-Database Technologies for Databricks supports Databricks 10.4 LTS or later (with Spark 3.2.*x* or later) for Microsoft Azure or Amazon Web Services.

Requirements for SAS® In-Database Technologies for Azure Synapse Analytics

SAS In-Database Technologies for Azure Synapse Analytics supports Microsoft Azure Synapse Analytics (with Spark 2.4 or Spark 3.1).

Requirements for SAS® In-Database Technologies for Teradata

SAS In-Database Technologies for Teradata supports the following products:

- Teradata Vantage Advanced SQL Engine version 16.20 or later
- Teradata CLIv2 client libraries, TTU 16.20 or later for Linux (64-bit libraries)

SAS In-Database Technologies for Teradata also supports Teradata Vantage on the following cloud platforms:

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- Teradata Cloud
- VMware

Requirements for SAS/ACCESS Interface to Informix

SAS/ACCESS Interface includes SAS Data Connector to Informix.

SAS/ACCESS Interface to Informix uses an ODBC connection. The ODBC driver that is included with Informix Connect must be installed and configured before you can use SAS/ACCESS to access IBM Informix data.

The following products are also required:

- IBM Informix Client SDK 4.10FC4 or later
- IBM Informix Server version 12.10 or later

Requirements for SAS/ACCESS Interface to JDBC

SAS/ACCESS Interface to JDBC includes SAS Data Connector to JDBC. SAS/ACCESS Interface to JDBC enables access to relational databases by means of SQL and the Java Database Connectivity (JDBC) API.

A JDBC driver is required for the data source from which you want to access data. JDBC drivers are available from DBMS vendors and other third-party JDBC driver developers.

The SAS Viya platform includes JAR files to connect to third-party sites using specific JDBC drivers from CData. These JDBC drivers simplify the requirements to make secure connections to these sites and manipulate data. You can access data from these sites as if it were in a relational database, and you can push string, date, and numeric functions to the data. The following CData drivers are included:

- Facebook
- Google Analytics
- Google Drive
- Microsoft OneDrive
- Odata
- Twitter
- YouTube Analytics

For more information, see “Connecting to Third-Party Drivers” in *SAS/ACCESS for Relational Databases: Reference*.

Requirements for SAS/ACCESS Interface to Microsoft SQL Server

SAS/ACCESS Interface to Microsoft SQL Server includes SAS Data Connector to Microsoft SQL Server.

SAS/ACCESS Interface to Microsoft SQL Server supports the following products:

- Amazon RDS Microsoft SQL Server (Microsoft SQL Server 2017 or later)
- Google Cloud Platform Cloud SQL for SQL Server version 2017 or later
- Microsoft SQL Server 2017 or later
- Microsoft Azure SQL Database
- Microsoft Azure SQL Database Managed Instance
- Microsoft Azure SQL Server Big Data Clusters
- Microsoft Azure Synapse

Required client software is included with your SAS Viya platform installation. Using a Data Source Name (DSN) to connect requires some post-installation configuration of your Kubernetes deployment.

A DataDirect ODBC driver that is included with SAS/ACCESS to Microsoft SQL Server enables you to use a Microsoft SQL Server data source with SAS Micro Analytic Service. SAS/ACCESS Interface to Microsoft SQL Server has been tested and certified against DataDirect Technologies Connect ODBC and DataDirect SequeLink ODBC products.

As a best practice, set the EnableScrollableCursors ODBC driver option to 3.

Requirements for SAS/ACCESS Interface to MongoDB

SAS/ACCESS Interface to MongoDB includes SAS Data Connector to MongoDB.

SAS/ACCESS Interface to MongoDB requires the MongoDB C Driver version 1.17 or later (“libmongoc,” the official client library for C applications). You can obtain the latest MongoDB C driver from the following website: http://mongoc.org/.

SAS/ACCESS Interface to MongoDB supports the following databases:

- MongoDB Server 6.0 or later and Client 1.23 or later
- MongoDB Atlas tiers M10 and higher

Requirements for SAS/ACCESS Interface to MySQL

SAS/ACCESS Interface to MySQL includes SAS Data Connector to MySQL.

SAS/ACCESS Interface to MySQL requires MySQL Client version 5.7 or later.

The following DBMS products are supported:

- Amazon Aurora (MySQL engine version 5.7 or later)
- Amazon RDS MariaDB (engine version 10.1 or later)
- Amazon RDS MySQL (engine version 5.7 or later)
- Azure Database for MySQL (engine version 5.7 or later)
- Google Cloud SQL for MySQL (engine version 5.7 or later)
- MySQL Server version 5.7 or later
- MariaDB 10.1 or later
- Oracle MySQL Database

Starting in 2023.03, the ability to access a SingleStore instance using SAS/ACCESS Interface to MySQL has been deprecated. SAS recommends that you use SAS/ACCESS Interface to SingleStore on page 55, which is included with your SAS software order in 2023.03 and later.

Requirements for SAS/ACCESS Interface to Netezza

SAS/ACCESS Interface to Netezza includes SAS Data Connector to Netezza.

SAS/ACCESS Interface to Netezza requires the IBM Netezza ODBC driver from IBM. To obtain the appropriate IBM Netezza ODBC driver, contact IBM Technical Support at (877) 426-6006 or visit the IBM Fix Central website: http://www.ibm.com/support/fixcentral.

SAS/ACCESS Interface to Netezza supports the following DBMS products:

- IBM Netezza 7.2.1 or later
- IBM Netezza Performance Server 11.2.0.0 and 11.2.1.*x*

Requirements for SAS/ACCESS Interface to ODBC

SAS/ACCESS Interface to ODBC includes SAS Data Connector to ODBC. SAS/ACCESS Interface to ODBC enables access to multiple data source types by means of a generic ODBC driver.

Before you can use the SAS Viya platform with ODBC, an ODBC driver is required for the data source from which you want to access data. ODBC drivers are often available from DBMS vendors

and other third-party ODBC driver developers. Your ODBC driver must comply with the ODBC 3.5 (or later) specification.

Note: The ODBC driver that you select might require additional DBMS software in order to enable network access.

Requirements for SAS/ACCESS Interface to Oracle

SAS/ACCESS Interface to Oracle (on SAS Viya platform) includes SAS Data Connector to Oracle.

SAS/ACCESS Interface to Oracle requires the Oracle client 12c or later (64-bit libraries).

The following Oracle instances are supported:

- Amazon RDS Oracle 12c or later
- Oracle Cloud Platform 12c or later
- Oracle Database 12c or later

Obtain the path to the volume on the Oracle server to which you want to point your SAS Viya platform deployment. This information is used later in the deployment.

Requirements for SAS/ACCESS Interface to PC Files

SAS/ACCESS Interface to PC Files includes SAS Data Connector to PC Files.

SAS/ACCESS Interface to PC Files enables access to the following file formats:

- `.jmp`
- `.spss`
- `.stata`
- `.xlsx` or `.xls`

Additional Microsoft file formats can be accessed via the PCFILES LIBNAME engine, which is included with SAS/ACCESS Interface to PC Files.

No additional software is required.

Requirements for SAS/ACCESS Interface to the PI System

SAS/ACCESS Interface to the PI System uses the PI System Web API, which is HTTPS-based and RESTful. No PI System client software is required to be installed on the nodes where SAS is running. However, the PI System Web API (PI Web API 2019 or later) must be installed and activated on the host machine from which the user connects.

Requirements for SAS/ACCESS Interface to PostgreSQL

SAS/ACCESS Interface to PostgreSQL (on SAS Viya platform) includes SAS Data Connector to PostgreSQL.

SAS/ACCESS Interface to PostgreSQL supports:

- Amazon Aurora (PostgreSQL engine version 12.*x* or later)
- Amazon RDS PostgreSQL (engine version 12.*x* or later)
- Azure Database for PostgreSQL (engine version 12.*x* or later)
- CockroachDB 21.1.5 or later

  Bulk load and bulk unload are not supported at this time.
- EnterpriseDB PostgreSQL 12.*x* or later
- Google Cloud Platform Cloud SQL for PostgreSQL (engine version 12.*x* or later)
- PostgreSQL Database 12.*x* or later

Required client software is included with your SAS Viya platform installation. Using a Data Source Name (DSN) to connect requires some post-installation configuration of your Kubernetes deployment.

Requirements for SAS/ACCESS Interface to Salesforce

SAS/ACCESS Interface to Salesforce includes SAS Data Connector to Salesforce.

SAS/ACCESS Interface to Salesforce requires a Salesforce user account that has API access enabled. SAS/ACCESS Interface to Salesforce supports Salesforce API access, version 46.0 or later.

Requirements for SAS/ACCESS Interface to SAP ASE

SAS/ACCESS Interface to SAP ASE requires SAP ASE (formerly Sybase) Open Client SDK, Release 15.7 or later (64-bit libraries).

The database administrator must install two SAP ASE (Sybase) stored procedures on the target SAP server. These files are available in a compressed TGZ archive for download from the SAS Support site at https://support.sas.com/downloads/package.htm?pid=2458.

Note: For compatibility with version 16 of the SAP ASE Open Client SDK, use the SAP ASE 15.*x* stored procedures:

- sas-spdf_15.txt

- sassp2df_15.txt

Requirements for SAS/ACCESS Interface to SAP HANA

SAS/ACCESS Interface to SAP HANA includes SAS Data Connector to SAP HANA.

SAS/ACCESS Interface to SAP HANA supports SAP HANA SPS 11 Server or a later version and requires SAP HANA ODBC Client (64-bit) for SPS 11 or later.

Requirements for SAS/ACCESS Interface to SAP IQ

SAS/ACCESS Interface to SAP IQ includes SAS Data Connector to SAP IQ. The SAS/ACCESS LIBNAME engine for SAP IQ supports bulk loading.

The following components are required:

- SAP IQ Network Client version 16.1 or later
- SAP IQ Database version 16.0 or later

Requirements for SAS/ACCESS Interface to R/3

SAS/ACCESS Interface to SAP R/3 supports SAP NetWeaver 7.0 (Application Server ABAP) or later and requires the 64-bit SAP NetWeaver RFC Library, Release 7.20 or later, which is provided by SAP AG.

Requirements for SAS/ACCESS Interface to SingleStore

SAS/ACCESS Interface to SingleStore includes SAS Data Connector to SingleStore (standard). This data connector provides the standard ability to connect the CAS server with your SingleStore database.

SAS/ACCESS Interface to SingleStore supports SingleStoreDB 7.*x* or later.

An additional data connector for SingleStore is available if you purchase SAS Viya with SingleStore on page 95, a separately licensed product. The SAS Viya with SingleStore data connector provides parallel data transfer and integrated, in-database features in addition to the standard features.

Requirements for SAS/ACCESS Interface to Snowflake

SAS/ACCESS Interface to Snowflake includes SAS Data Connector to Snowflake. The required client software is also included with your SAS Viya platform installation.

Using a Data Source Name (DSN) to connect to Snowflake requires post-installation configuration of your Kubernetes deployment.

Requirements for SAS/ACCESS Interface to Spark

SAS/ACCESS Interface to Spark includes SAS Data Connector to Spark.

Spark SQL 3.1 or later is required.

SAS/ACCESS Interface to Spark supports the following data sources:

- Databricks on Google Cloud 10.4 LTS or later
- Databricks on Amazon Web Services (AWS) 10.4 LTS or later
- Microsoft Azure Databricks 10.4 Long Term Support (LTS) or later
- Microsoft Azure HDInsight 5.0 (support starts with Spark 3.1 and SAS Viya platform 2022.11)

SAS/ACCESS Interface to Spark redistributes JDBC drivers developed by CData Software in order to connect to additional data sources:

- CData JDBC Driver for Databricks
- CData JDBC Driver for Spark SQL

For more information about using CData drivers with SAS/ACCESS, see "Configuring SAS/ACCESS Interface to Spark" in *SAS/ACCESS for Relational Databases: Reference*.

Starting in 2023.05, SAS/ACCESS Interface to Spark supports single sign-on to Databricks in Microsoft Azure. To enable this feature, you must obtain and install version 2.6.15 or later of the JDBC driver from Databricks. Single sign-on with the CData JDBC Driver for Spark SQL and CData JDBC driver for Databricks is not supported at this time. Azure Active Directory must be configured as an OIDC provider. For more information, see "Scenario: OIDC with Azure AD" in *SAS Viya Platform: Authentication*.

Requirements for SAS/ACCESS Interface to Teradata

SAS/ACCESS Interface to Teradata includes SAS Data Connector to Teradata.

SAS/ACCESS Interface to Teradata requires Teradata CLIv2 client libraries, TTU 16.20 or later, and supports Teradata Vantage SQL Engine version 16.20 and later.

SAS/ACCESS Interface to Teradata also supports the following platforms:

- Teradata IntelliCloud
- Teradata Vantage on Amazon Web Services
- Teradata Vantage on Google Cloud Platform
- Teradata Vantage on Microsoft Azure

SAS/ACCESS Interface to Teradata supports TLS 1.2 with Teradata Database 17.10 and later. TTU 17.10 is required to support TLS 1.2. You can then encrypt data that is transferred between Teradata and the SAS Viya platform. Some additional configuration is required. For more information, see "Configure TLS for SAS/ACCESS Connection to Teradata" in *SAS Viya Platform Encryption: Data in Motion*.

Requirements for SAS/ACCESS Interface to Vertica

SAS/ACCESS Interface to Vertica includes SAS Data Connector to Vertica.

SAS/ACCESS Interface to Vertica requires Vertica ODBC Client version 9.1 or later and supports Vertica Analytic Database version 9.1 or later.

To obtain the Vertica Client ODBC driver, contact your database administrator or visit the Vertica website: https://my.vertica.com/download/vertica/client-drivers.

Requirements for SAS/ACCESS Interface to Yellowbrick

SAS/ACCESS Interface to Yellowbrick includes the required PostgreSQL ODBC driver.

Yellowbrick Database version 4.0.0-23452 or later is supported.

Security Requirements

About SAS Viya Platform Security Features

The SAS Viya platform provides Transport Layer Security (TLS) for encryption of data in motion and supports the Advanced Encryption Standard (AES) for encryption of data at rest. With minimal configuration, you can deploy and use the SAS Security Certificate Framework, which contains tools that leverage Kubernetes features to encrypt data in motion for SAS applications.

Multiple methods are supported for user authorization and authentication. Most user account configuration occurs after the deployment has completed. Single sign-on and multi-factor authentication are also supported.

TLS Overview

The deployment supports TLS version 1.2 or 1.3 for connections to the cluster, from SAS Viya platform components to your IT infrastructure, and among the pods. You can deploy in three different modes:

- “Full-Stack TLS”: secure all network connections
- “Front-Door" TLS: secure only those components that are intended to accept connections from outside the Kubernetes cluster, such as the Ingress controller and CAS server
- “No TLS”: no network connections are secured. All network transmissions are unencrypted.

In a multi-tenant deployment, all tenants must use the same TLS mode.

To provide TLS, the SAS Security Certificate Framework manages certificates and integrates SAS Viya platform security with cluster security. The framework supports two options for certificate management. The requirements for each option are described in “TLS Requirements” on page 58.

Deploying in “No TLS” mode is not recommended. The default deployment enables “full TLS,” including TLS for ingress-nginx. To secure the ingress, you can provide your own certificates if desired. Customer-supplied certificates must be in PEM format, and the corresponding private key file is required.

The CAS server supports encryption for tables in caslibs. The SAS Viya platform uses AES with 256-bit keys to encrypt stored data. The encryption applies to source tables, not to tables that are resident in memory. Encryption can be applied to individual tables or to all tables in a library. Each table can have a unique encryption key, or a single key can be set at the library level in order to have a shared key for all tables in the library.

See the “Encryption Overview” in *SAS Viya Platform Encryption: Data in Motion* for relevant conceptual information and procedures for customizing your environment.

TLS Requirements

To apply TLS encryption to your SAS Viya platform deployment, certificates are required. Certificates contain the names of pods, which are ephemeral. Therefore, a certificate generator that is capable of creating certificates instantly, whenever pods are scheduled, is required. You can select either a SAS-supplied distribution of OpenSSL (the default option) or an open-source utility, cert-manager, as the certificate generator. With either option, the generated CA certificate and private key are stored in a Kubernetes secret in the SAS Viya platform namespace. This CA certificate and key are used to issue the server identity certificates that secure the SAS Viya platform back-end servers.

IMPORTANT Additional configuration of your security settings is required. Detailed documentation is provided in the SAS Administration document titled *Encryption in SAS Viya Platform: Data in Motion*. Refer to Certificate Generators for information about your options for certificate management, and refer to kustomize Components to Enable TLS for information about updating the manifest.

The following table summarizes the requirements for each option:

Table 19 *Requirements to Support TLS*

Certificate Generator	Requirements
openssl	The openssl certificate generator is proprietary SAS software that uses the OpenSSL open-source project. The deployment is configured to use it by default. It creates a unique CA certificate and private key during SAS Viya deployment. For more information, see "Configure TLS" in *SAS Viya Platform: Deployment Guide*.
cert-manager	In order to use cert-manager, you must deploy it in your cluster prior to deploying SAS Viya. The SAS Viya platform is compatible with all production releases of cert-manager. Once you have determined the version of Kubernetes that you will be using, check the cert-manager documentation to select a release of cert-manager that is compatible with your version of Kubernetes: https://cert-manager.io/docs/installation/supported-releases/. Do not install more than one instance of cert-manager per cluster. You can download cert-manager from the Jetstack GitHub site. Run the following command to find the currently installed version: `kubectl -n cert-manager describe deployments/cert-manager | grep Image` An issuer is required. You must configure it and the ingress certificate in the kustomization.yaml file in order to enable the cert-manager certificate generator. For instructions, see Certificate Generators. SAS recommends that you configure cert-manager to automatically delete secrets when they are no longer being used. For instructions, see "Delete Secrets That Are No Longer Used" in *SAS Viya Platform Encryption: Data in Motion*. **Note:** If you are updating to a new release of SAS Viya and you need to upgrade cert-manager to a supported version, be sure to upgrade the existing cert-manager instance instead of deleting it. If the SAS Viya platform secrets are owned by cert-manager, which is the recommended configuration, they will be deleted if you delete the cert-manager instance instead of upgrading it. However, if you do delete the secrets, you can create new secrets for the SAS Viya platform deployment. For more information, see "Renew or Replace the SAS Viya Platform Root CA Certificate" in *SAS Viya Platform Encryption: Data in Motion*.

Note: The optional monitoring components in the SAS Viya Monitoring for Kubernetes project apply TLS using separate tools and configuration. Your choice of a SAS Viya platform certificate generator does not constrain your options for applying TLS to SAS Viya Monitoring for Kubernetes, which is deployed and configured after the SAS Viya platform deployment has completed.

To support a multi-tenant deployment, the ingress certificate must include a wildcard entry in the SAN DNS attribute in order to match the various tenant names. This requirement applies to the Full-Stack

or Front-Door TLS modes, regardless of the certificate generator that you select. Without this additional configuration, the browser throws an invalid certificate error as soon as a tenant is onboarded. Multi-tenancy is an optional feature.

Here is an example of a SAN DNS attribute that contains a wildcard: `*.mydomain.mycompany.com`

In an environment where SAS/CONNECT or CAS programming interfaces are used, users might connect directly to a node port or LoadBalancer service from an external IP address or host name, bypassing the ingress controller. If you apply Full-stack TLS to your deployment, additional configuration in the signed certificate that secures the LoadBalancer or NodePort service is required. The certificate's SAN attributes must contain the name or the IP address that is used to connect directly to these services. After you have downloaded the deployment assets for your software order, see "Configure Certificate Attributes" in *SAS Viya Platform Encryption: Data in Motion*.

Pod Security Policies

If your Kubernetes cluster has pod security policies enabled, a conflict with a SAS Viya platform seccomp annotation can cause the deployment to fail. The SAS Viya platform requires **`runtime/default`** to be allowed in the environment. You can check pod security policies by running the following command on your cluster:

```
kubectl get psp restricted -o custom-columns=NAME:.metadata.name,
"SECCOMP":".metadata.annotations.seccomp\.security\.alpha\.kubernetes\.io/
allowedProfileNames"
```

You can resolve this conflict by updating a variable in the pod security policy. For more information, see the following SAS Note: https://support.sas.com/kb/67/349.html.

Support for Federal Information Processing Standards (FIPS)

Starting with 2023.06, the SAS Viya platform supports the use of FIPS 140-2 validated cryptographic modules when executed on Kubernetes nodes that are running in FIPS mode. A few SAS components and products do not support running in a FIPS-enabled environment at this time:

- OpenSearch.

  A workaround has been provided. For more information, see "Additional Configuration for FIPS Compliance" on page 83.
- SAS Workload Orchestrator
- SAS Business Orchestration Services
- SAS Decision Architecture (SAS Fraud Decisioning)

Customers who want to deploy with FIPS-enabled nodes should verify that supporting third-party components have been FIPS-validated. For example, builds of cert-manager that are available for a standard download do not use FIPS-validated cryptographic modules. However, SAS has tested with openssl as the certificate generator on nodes where FIPS is enabled.

In addition, certain types of storage might not work properly in a FIPS-enabled environment. Consult the documentation from the third-party vendor and implement workarounds where required.

DNS Requirements for Multi-Tenancy

As the users within each tenant access SAS Viya platform components, the host name that they use to access the SAS deployment identifies their tenant membership. Therefore, DNS records for tenant-specific subdomains are required.

Each tenant is reachable by a URL that is derived from the provider's URL. Here is the format for a typical tenant URL

tenant-ID.provider-ingress

Here is an example of a provider URL:

```
sasviya.mycompany.com
```

Here is an example of a tenant URL:

```
mytenant.sasviya.mycompany.com
```

You must verify that the DNS server for your enterprise is configured to route to these address spaces. You can create a wildcard subdomain entry as a time-saving step.

Requirements for Confidential Computing

Confidential computing encrypts data in memory and provides verification before processing it. Data has an additional layer of protection while it is in use. SAS uses AMD SEV technology to support confidential computing in Microsoft AKS deployments. At this time, Microsoft Azure is the only SAS Viya platform deployment environment that supports confidential computing.

Virtual machines that support confidential computing must be running in the region where the AKS cluster for the SAS Viya platform deployment was created. Select these machine types for all node pools, including the default node pool. Only the following VM instance types are supported for confidential computing:

- DCasv5 or DCasv5-series
- ECasv5 or ECasv5-series

Note: AMD SEV confidential VM instance types are available in the Azure East US, West US, West EU, and North EU regions.

Adding confidential computing to an existing deployment is not supported. To configure confidential computing before the SAS Viya platform deployment, follow the steps that are documented in "Confidential Computing" in *SAS Viya Platform: Deployment Guide*.

Identity Provider and Authentication Requirements

The SAS Viya platform supports LDAP and the System for Cross-domain Identity Management (SCIM) for user and group identities. Multiple identity providers are supported, including Microsoft Azure Active Directory.

IMPORTANT The security of your SAS Viya deployment is directly affected by the availability and integrity of your authentication and identity providers. It is essential that the selection, configuration, and operation of these components provide a level of security that meets or exceeds the requirements of your SAS Viya deployment.

Supported Authentication Methods

The SAS Viya platform supports the following methods for authenticating users who are signing in to the environment:

- LDAP, Kerberos, and single sign-on
- Single sign-on using Security Assertion Markup Language (SAML) or OpenID Connect

  Single sign-on support is limited to web log-ins.
- A pluggable authentication module (PAM) can be used to validate the user's credentials when accessing the CAS server.

  PAM is supported only for CAS connections, not for web log-ins. This type of authentication enables support for users to launch CAS server sessions under their host identities.

  PAM uses the operating system for user and password authentication, which means that you must also set up System Security Services Daemon (SSSD) and enable host authentication. Similar requirements apply to Kerberos.

Host Authentication

Users launch CAS sessions under a shared identity by default. For various reasons, you might instead want to enable them to launch sessions under their host (operating-system) accounts. With host identities, users launch CAS and compute server sessions under their own user accounts, defined in the operating system. Configure host authentication in order to enable Kerberos authentication, to facilitate access to NFS volumes, to enable some users to deploy models written in Python or R, or to integrate with a SAS®9 deployment.

The ability to launch CAS sessions under a host identity is disabled by default. To enable it, you must apply an overlay to the base kustomization.yaml file and perform additional configuration when the deployment has completed. For more information, see "Enable Host Launch" in *SAS Viya Platform: Deployment Guide*.

LDAP Requirements

When the deployment completes, the SAS Viya platform is configured by default to use LDAP. The following requirements apply to your LDAP server:

- The SAS Viya platform must have Read access to your LDAP server.
- In order to bind to the LDAP server, the SAS Viya platform requires either a system account (with a userDN and password) or anonymous binding.
- If the mail attribute is specified for LDAP accounts, it must have a non-null value that is unique for each user.

- LDAPS is supported, but the required certificates are not configured automatically by the deployment process.

You will configure SAS identities as a post-deployment step. Instructions for setting up identities with LDAP are provided in Identity Management.

Additional LDAP Requirements for Multi-Tenancy

You cannot use multiple LDAP servers for a single tenant. However, you have the following options:

- One LDAP server per tenant

  You can specify custom LDAP properties for each tenant.

- A single LDAP server for all tenants

  You can specify custom LDAP properties for each tenant.

  A separate OU per tenant and an OU named “provider” are required if you also use the same LDAP directory structure for all tenants.

You should either set up or plan your tenant structure in LDAP before you start the deployment. Determine whether you will use the same directory structure for the users and groups within all tenants (a “fixed” LDAP structure), or will use a custom structure that varies per tenant. Based on these decisions, you can then perform tenant onboarding as a post-deployment task.

Multi-tenancy requires some post-deployment configuration in SAS Environment Manager. By default, the values that you specify for tenant LDAP connection parameters are automatically applied to the provider and to the users and groups within all tenants. However, you will have an option to selectively apply LDAP connection settings. This option enables you to deploy a custom directory structure for each tenant. For example, you can use a single LDAP server across all tenants while using custom parameters, such as the baseDNs or search filters, for each tenant. In such a case, you would select the option to **Apply configuration only to this tenant (provider)** for the provider’s group and user connections.

During tenant onboarding, if you select the option to apply the configuration only to the provider, you must use the fixed directory structure that is described in “Preparing to Use a Single LDAP Server for All Tenants” on page 69. The reason is that the SAS Viya platform requires an OU for the provider and separate OUs for each tenant if the option is not selected.

For more information about your options for setting up tenants in LDAP, see “Requirements for Multi-Tenant Deployments” on page 69.

SCIM Requirements

The SAS Viya platform supports SCIM 2.0.

When the platform deployment completes, it is configured by default to use LDAP. If you intend to use SCIM, you must disable LDAP by logging in to SAS Environment Manager after the deployment process has completed.

Single sign-on using SAML or OpenID Connect (OIDC) is required if you configure a SCIM identity provider.

With SCIM, you can use Okta or Microsoft Azure Active Directory to populate SAS user and group identities. In a Google Cloud Platform (GCP) environment, Google Identity is not yet supported for user provisioning; use Okta or Azure Active Directory instead. SCIM requires network access to the SAS Viya platform using HTTPS, and it requires a certificate signed by a public certificate authority. The SCIM IdP also requires a long-lived token to access the SAS Viya platform APIs.

Check your firewall settings so that IP addresses used by the SCIM IdP are allowed to reach the SAS Viya platform ingress. In Microsoft Azure, you can configure your network security group to allow Azure Active Directory to communicate with resources in your virtual network by enabling inbound access for the AzureActiveDirectory service tag.

If you use OIDC, SAS Logon Manager must construct the correct redirect_uri parameter to send as part of the authentication request to the IdP. This parameter incorporates header values from the request to SAS Logon Manager. The relevant values are from the Host, X-Forwarded-Proto, and X-Forwarded-Port headers. The redirect_uri parameter must match the value or values that are registered with the OIDC provider. Its value is also used by the OIDC provider to redirect the client browser back to SAS Logon Manager after authentication with the authorization code. Therefore, these header values must correspond to the external address that is used by SAS users.

In an OIDC environment with a reverse proxy server in front of the ingress-nginx, the NGINX configuration setting `use-forwarded-headers` must be changed from the default "false" to "true". Changing this setting enables the ingress controller to pass the incoming X-Forwarded-* headers from your reverse proxy to SAS Logon Manager. SAS Logon Manager can then build the redirect_uri parameter correctly based on those headers.

You configure SAS identities as a post-deployment step. Instructions for setting up identities with SCIM are provided in Identity Management.

Additional SCIM Requirements for Multi-Tenancy

SCIM configuration for a deployment with multi-tenancy occurs after the SAS Viya deployment has completed. The first step is to onboard tenants. You can then register an OAuth client on each tenant. Although you can typically register a client manually or programmatically, using the SAS Viya Command-Line Interface, a multi-tenant deployment only supports a manual client registration. See “Register an OAuth Client ID” in *SAS Viya Platform: Authentication* for the steps.

SCIM setup procedures are described in detail in “Configure SCIM Provisioning in the Identity Provider ” in *SAS Viya Platform: Identity Management*. The configuration steps must be repeated for each tenant.

Kerberos Requirements

Configure Kerberos delegation before you start the deployment. If you plan to use SAS/ACCESS Interface to Hadoop to connect to a Hadoop data source, only unconstrained delegation is supported.

Enabling Kerberos in your deployment also requires that you enable host authentication. By default, users connect to the CAS server and launch sessions under a shared service account. However, use of the shared account is not supported in a Kerberos environment.

You have two options for enabling host authentication for Kerberos. Both options require post-deployment steps. For more information, see “Configure Kerberos” in *SAS Viya Platform: Authentication*.

Requirements for User Accounts and Services

About Roles and Permissions

The Kubernetes specification accepts system-delineated roles and user-facing roles. The SAS Viya platform applies a *least-privileges* model that grants to each role the minimum access that is required to deploy and run the application. SAS Viya platform resources are controlled by labels that describe installation requirements and that determine the privileges for enabling access to these resources.

To deploy the SAS Viya platform, an administrator or administrators with sufficient permissions must run the commands to apply the application resources to the cluster. The requirement to use label selectors applies to kubectl commands that require the highest level of access: `kubectl apply` and `kubectl delete`. For `kubectl apply`, the label selector explicitly avoids race conditions. Typical race conditions occur when the Kubernetes API processes objects in parallel that have dependencies on each other.

Here is an example of a kubectl command that uses a label selector:

```
kustomize build | kubectl apply --kubeconfig=cluster-admin.conf --selector="sas.com/admin=cluster-wide" -f -
```

The selector `sas.com/admin=cluster-wide` indicates that the command can be executed only by a user with the default cluster-admin ClusterRole. This role grants the equivalent of super-user privileges.

To provide granular privileges and to ensure that the least-privileges model is enforced, SAS applies a custom resource label to one category of SAS Viya platform resources. The following table summarizes SAS Viya platform resources and their corresponding labels:

Table 20 *SAS Viya Platform Label Selectors*

Label	Description	Examples of SAS Viya Resources
cluster-wide	Applies to resource modifications that affect the entire cluster. This category includes global objects, such as CRDs or ClusterRoles, that could affect deployments in other namespaces. Interacting with resources in this category also requires cluster-admin permissions. These resources are defined under Cluster APIs in the Kubernetes API Reference documentation.	CustomResourceDefinition; ServiceAccount; ClusterRole; Role; PersistentVolume
cluster-local	A SAS custom label for resources that require cluster-admin permissions, but it limits the impact of changes to the	ResourceQuota; LimitRange; Secret; ConfigMap; RoleBinding;

Label	Description	Examples of SAS Viya Resources
	namespace, with a reduced impact on the cluster. These resources are defined under Config and Storage APIs in the Kubernetes API Reference.	ClusterRoleBinding; PersistentVolumeClaim; PodTemplate
cluster-api	A Kubernetes label for cluster-wide resources that are specific to CustomResourceDefinitions. This includes the CRDs themselves as well as any supporting conversion webhook resources. As CRDs extend the API supported by the cluster where they are created, they might require additional consideration.	CustomResourceDefinition; Deployment; Service
namespace	Applies to the following resource types: ■ resources for managing and running containers ■ resources that provide external access to workloads by means of a LoadBalancer or NodePort service These resources are defined under Workloads APIs, Service APIs, and Metadata APIs in the Kubernetes API Reference.	Service; Deployment; ReplicaSet; ReplicationController; Job; CronJob; StatefulSet; DaemonSet

Note: A Kubernetes user with sufficient permissions to create these SAS Viya resources must also have permissions to get, list, watch, update, patch, and delete these resources.

Some Kubernetes Role-Based Access Control (RBAC) policies are enabled by default. Because objects of each kind are deployed, permissions for each resource should be granted to the appropriate role. During RBAC planning for your SAS Viya platform deployment, consider that some user-facing ClusterRoles need to allow admin users to include rules for custom resources.

Cluster Resources and Roles That Require Elevated Permissions

As a cluster administrator, you should understand the full set of requirements for administrators and have some knowledge of the cluster-wide resources that are used by the SAS Viya platform. Cluster administrators can assign permissions to other users, such as namespace administrators. These delegated administrators might perform some deployment steps, or they might need permissions to view pod-level or cluster-level information after the deployment has completed.

Depending on the security architecture that is in use, the cluster administrator must deploy certain cluster-level resources as part of a SAS Viya platform deployment. These resources might include custom resource definitions (CRDs), Roles, RoleBindings, and PodTemplates. Once the resources

have been deployed, SAS recommends providing a delegated, namespace-level administrator with the "get", "list," and "watch" permissions on all resources cluster-wide.

With these permissions, the delegated administrator has broad Read-Only access to relevant cluster-level resources. In order to effectively monitor the SAS workload, the namespace-level administrator might also be granted permissions to view cluster metrics (for example, by using Lens, an integrated development environment for Kubernetes). These Read-Only permissions might range more broadly than absolutely required, but they provide the delegated administrator with an enhanced ability to monitor the cluster and make recommendations to the cluster administrator.

A SAS Viya platform deployment adds custom API extensions (“API groups”) to the cluster. The delegated administrator should receive full permissions (all verbs, cluster-wide) for these custom API groups. The following table provides a list of the custom API groups and CRDs that SAS provides:

Table 21 *Custom SAS Viya API Groups*

API Group	CRD	Purpose
opendistro.sas.com	OpenDistroCluster	Used to deploy the OpenSearch database.
(For only SAS Event Stream Processing or SAS Analytics for IoT) iot.sas.com	ESPConfig	Used to configure the ESP operator and its custom resources.
	ESPLoadbalancer	Used to manage the load balancers for SAS Event Stream Processing.
	ESPRouter	Used to manage the process of connecting SAS Event Stream Processing sources to destinations.
	ESPServer	Used to manage ESP servers.
	ESPUpdate	Used to manage operations across multiple ESP servers.
viya.sas.com	CASDeployment	Used to deploy the CAS server.
webinfdsvr.sas.com	data servers	Stores information that is required to manage a PostgreSQL cluster.
(For an internal PostgreSQL server only) postgres-operator.crunchydata.com	PostgresCluster	Stores information that is required to manage a PostgreSQL cluster.
	PGUpgrade	Stores information that is required to perform major version upgrades to existing PostgreSQL clusters.

API Group	CRD	Purpose
(Optional) orchestration.sas.com	SASDeployment	Used when you deploy SAS Viya by using the SAS Viya Deployment Operator.
redis.kun	DistributedRedisCluster	Used to deploy a Redis cluster for SAS Cache Server.

The delegated administrator might also need Write access to a minimal set of resources in the SAS Viya platform namespace. The following namespace-level permissions enable the administrator to execute a command in a container within a pod. For example, the administrator can inspect processes, check user and group IDs, verify that persistent volumes have been mounted and get their paths, and more:

```
rules:
- apiGroups: [""]
  resources: ["pods/exec"]
  verbs: ["create"]
```

IMPORTANT If you use the SAS Viya Deployment Operator for the deployment, the SASDeployment CR is also deployed before you begin the actual SAS Viya platform deployment process. The CRD is associated with the orchestration.sas.com api group. The SAS Viya Deployment Operator requires cluster-admin privileges in order to create the CR. After it is deployed, the operator runs with cluster-admin privileges.

If your security architecture allows namespace-level administrators to create role bindings, a few role bindings require specific RBAC permissions. These permissions are in addition to those that are already granted to namespace-level accounts that have the default “admin” or “edit” cluster roles. The following table summarizes these permission requirements and provides examples of roles, which vary based on the offerings in your order:

Table 22 *SAS Viya Platform Custom Permissions by Role*

Examples of Roles	Custom Permissions	Description
sas-data-server-operator-leader-election-role sas-opendistro-operator sas-opendistro-operator-leader-election	Permissions to "delete", "patch", or "update" events	Roles that manage SAS Viya platform components (SAS Infrastructure Data Server, SAS OpenSearch, and SAS Cache Server).
(For only Red Hat OpenShift) sas-cas-operator	Permissions to specific API groups: monitoring.coreos.com, route.openshift.io, and projectcontour.io	
sas-data-server-operator	Permissions to specific API group: coordination.k8s.io	

User Accounts

You can set up users and groups with SAS Environment Manager after your software has been deployed.

Some pods run system-critical processes under the UID 1001. This UID acts as the owner of CAS server sessions by default and cannot be changed, with one exception: the OpenSearch pods have an option to change the run user. Verify that no user accounts in your LDAP directory are using this UID. This run user is comparable to the sas user account in previous versions of SAS, but it does not exist outside of the container where it runs.

An account that is named sasboot is also created during the deployment and has a password that will expire when used. It is an administrator account that is used for preliminary logon to SAS Environment Manager. It is internal only to SAS and does not exist in your identity provider. For more information, see Sign In as the sasboot User.

Requirements for Multi-Tenant Deployments

Requirements for multi-tenancy depend on whether you intend to use a single LDAP server for all tenants, or one LDAP server per tenant. SAS recommends that you prepare the LDAP server before you start a deployment with multi-tenancy enabled.

User Account Requirements for Multi-Tenancy

For each tenant user account that you define in LDAP, the following requirements apply:

- User accounts must be unique within each tenant. However, a user account can be added to multiple tenants.
- The homeDirectory attribute must be set to a value that is appropriate for the tenant's environment.
- The loginShell attribute must be set to **`/bin/bash`**.

Preparing to Use a Single LDAP Server for All Tenants

The LDAP directory structure that is described here is recommended if you plan to apply the same connection settings to the provider and to users and groups within all tenants during tenant onboarding (a post-deployment task). In addition to configuring a single LDAP server that is used for all tenants, you can use a custom structure that applies different settings to different tenants, or you can use a separate LDAP server per tenant.

Here is an overview of the process to configure a single-LDAP tenant structure:

1. Create the provider OU. Here is an example:

```
dc=example,dc=com
       ou=tenant-1
           ou=groups
           ou=users
```

```
ou=tenant-2
    ou=groups
    ou=users
...
ou=provider
    ou=groups
    ou=users
```

Here is an example that uses LDIF syntax:

```
dn: cn=sas,ou=groups,ou=provider,dc=sas,dc=com
distinguishedName: cn=sas,ou=groups,ou=provider,dc=sas,dc=com
displayName: Tenant-admin-group-for-provider
gidNumber: value
objectClass: groupOfUniqueNames
objectClass: extensibleObject
uniqueMember: uid=sas,ou=people,ou=provider,dc=sas,dc=com
cn: sas
```

Note: The provider DN must be specified as **`provider`**. Tenant OU names are equivalent to the tenant IDs that the onboarding job uses.

2. Before deployment, add at least one user to the provider OU. This user later becomes the first SAS administrator in the provider tenant.
3. Before deployment, add at least one user to each tenant OU. When tenants are onboarded as a post-deployment task, these users become the first SAS administrators for their respective tenants.

   Instruct each tenant SAS administrator that they should not create a new LDAP configuration for their tenant.
4. When the deployment has completed, log on to SAS Environment Manager using the predefined sasprovider account in order to configure connection settings for tenants.

You can set up separate groups for administrative users and for non-administrative users within each tenant in LDAP, and you can add tenant users to one of these groups. The tenant onboarding process provides these groups with access to critical files and other resources that are restricted to the tenant.

Preparing to Use a Separate LDAP Server per Tenant

SAS Viya supports an environment in which a separate LDAP server is used for each tenant. You can customize the LDAP directory structure or use your existing structure. To prepare for your multi-tenant environment with a separate LDAP server per tenant, take the following steps:

1. Before deployment, prepare the LDAP server for the provider tenant and add at least one user account. After deployment, this user will become the first SAS administrator in the provider tenant.
2. Obtain and record connection information for the LDAP server for each new tenant.

   When the deployment has completed, you will configure settings for the following parameters to enable the identities service to authorize the provider:

   ```
   sas.identities.providers.ldap.connection
   sas.identities.providers.ldap.group
   sas.identities.providers.ldap.user
   ```

3 Add one user to each LDAP server. After onboarding, these users will become the first SAS administrators in their respective tenants.

4 Instruct the SAS administrator for each new tenant to add users and groups, as described in "How to Configure LDAP" in *SAS Viya Platform: Identity Management*.

5 When the deployment process has completed, log on to SAS Environment Manager using the predefined sasprovider account. Add at least one user to the SAS Administrators group in the provider tenant.

IMPORTANT Do not select the option to **Apply configuration only to this tenant (provider)**, which is available when you create a new LDAP configuration using SAS Environment Manager. This option restricts the application of LDAP connection settings to the provider.

Service Accounts

During the deployment process, required infrastructure services are automatically started in separate containers within the SAS Viya platform namespace. Some of these services are owned by a Kubernetes service account, which is created by the deployment process. Each service account has a very limited role. The use of multiple service accounts to run services makes it easier to secure your SAS Viya platform environment because each service account has only the specific privileges that it requires to run one service and has no additional privileges.

The following Kubernetes service accounts are created by the deployment process:

Table 23 *Required Kubernetes Service Accounts*

Service Account	Description
sas-rabbitmq-server	Owner of the SAS Message Broker service.
sas-cas-operator	Owner of the CAS server operator.
sas-cas-server	Owner of the CAS server pods. It enables CAS server pod security policies. This account has both a role and a role binding of sas-cas-server.
sas-config-reconciler	Owner of the service that keeps pods synchronized with configuration data, relaunching them when their configuration changes.
sas-consul-server	Owner of the Consul key-value store. SAS Configuration Server is based on HashiCorp Consul.
sas-data-server-operator	Owner of a required account to support SAS Infrastructure Data Server. Manages Consul registration and PostgreSQL validation. It runs in a container that is separate from the PostgreSQL Operator.

Service Account	Description
	This container is always present, regardless of whether you deployed with an internal or external PostgreSQL instance.
sas-launcher	Owner of a service that launches Kubernetes jobs and checks the status of those jobs.
sas-prepull	A service account that improves start-up times by pre-staging the sas-programming image to nodes that require it.
sas-programming-environment	Supports a group of components that include the compute server, the batch server, and SAS/Connect.
sas-viya-backuprunner	A service account that is used for backup operations.

Additional service accounts might be present if you deployed SAS products that require them.

To run on Red Hat OpenShift, some of these service accounts require a security context constraint (SCC) statement. For more information, see “Requirements for Security on Red Hat OpenShift” on page 72.

Requirements for Security on Red Hat OpenShift

If you are deploying the SAS Viya platform on Red Hat OpenShift, a few additional steps are required to prepare the cluster for the deployment. If you are not deploying on OpenShift, you can skip this section.

SCCs and Pod Service Accounts

In a Red Hat OpenShift environment, each Kubernetes pod is started with an association with the restricted security context constraint (SCC) provided by Red Hat, which limits the privileges that each pod can request.

Most SAS Viya platform pods are deployed in the restricted SCC, which applies the highest level of security. Two other OpenShift predefined SCCs are used by default. In addition, a few custom SCCs are either required by essential SAS Viya platform components, such as the CAS server, or associated with specific SAS offerings that might be included in your software order.

For a full list and description of the required SCCs, see “Security Context Constraints and Service Accounts” in *SAS Viya Platform: Deployment Guide* .

SCCs and File System Permissions

The SAS Viya platform includes default fsGroup settings that enable file system access. When an fsGroup ID is set for a pod, any files that are written to a volume within that pod inherit that fsGroup as their group ID (GID). The fsGroup ID is the owner of the volume and of any files in that volume.

For additional security, most pods are set to use an fsGroup value (1001) that is not supported by the OpenShift restricted SCC. These values must be modified before you start the deployment process.

The following table summarizes the default fsGroup settings:

Table 24 *Default fsGroup Values*

SAS Viya Component	Default fsGroup Value	Explanation
CAS server	1001	Changing this value is optional because a custom SCC definition enables the shared service account to access the CAS server. The `$deploy/sas-bases/examples/cas/configure/cas-server-scc.yaml` file grants SCCs for the service account GID by default. If you plan to enable users to launch CAS sessions under their host identities, use cas-server-scc-host-launch.yaml instead in order to set the correct capabilities and privilege escalation. For more information, see "Security Context Constraints and Service Accounts" in *SAS Viya Platform: Deployment Guide* .
OpenSearch	1000	The OpenSearch components are assigned to a custom SCC with the same restrictions on the fsGroup as the OpenShift restricted SCC. The default fsGroup setting does not enable deployment and must be modified in a pre-deployment step.
All other pods	1001	All remaining pods are assigned to the OpenShift restricted SCC. This SCC does not enable containers to use the default fsGroup settings and must be modified in a pre-deployment step.

SAS provides the update-fsgroup.yaml file to help you update the fsGroup in targeted manifests with the correct GID value. The required steps to change the fsGroup setting are provided in the Container Security README. For more information, see Additional Security for Red Hat OpenShift.

If you use the optional section in update-fsgroup.yaml to update the fsGroup for CAS pods, make sure that you also update the fsGroup range in the SCC that is applied to the CAS service account by using one of the provided YAML files that are specific to CAS.

Removing the seccomp Profile

Most pods run under the restricted SCC. However, some settings cannot be included in the podSpec if it runs under the restricted SCC, such as a seccomp profile. These settings must be removed for a deployment on OpenShift.

The Container Security README provides instructions for removing the seccomp profile using customizations provided by SAS. For more information, see Additional Security for Red Hat OpenShift.

PostgreSQL Server Requirements

SAS Infrastructure Data Server stores SAS Viya platform user content, such as reports, authorization rules, selected source definitions, attachments, audit records, and user preferences. The SAS Viya platform uses a PostgreSQL database instance for this required component and, for the products that require it, for SAS Common Data Store on page 78. Take some time to consider your options for deploying a PostgreSQL instance to support the infrastructure data server.

Internal versus External PostgreSQL Instances

IMPORTANT The combination of Kubernetes 1.26 and an internal instance of the PostgreSQL database is experimental in the 2023.06 release of the SAS Viya platform. *Experimental* software has been tested prior to release, but because it has not necessarily been tested to production-quality standards, it should be used with care.

Internal PostgreSQL is based on Crunchy Data PostgreSQL 5.3, which does not yet support Kubernetes 1.26. SAS recommends that you configure an external PostgreSQL instance if you want to deploy with Kubernetes 1.26. PostgreSQL versions 11 - 14 are supported. You can also defer upgrading to Kubernetes 1.26 if you want to continue using an internal instance.

IMPORTANT The combination of Red Hat OCP 4.12 and an internal instance of the PostgreSQL database is experimental in the 2023.06 release of the SAS Viya platform. *Experimental* software has been tested prior to release, but because it has not necessarily been tested to production-quality standards, it should be used with care.

Internal PostgreSQL is based on Crunchy Data PostgreSQL 5.3, which does not support OCP 4.12 and later. SAS recommends that you configure an external PostgreSQL instance if you want to deploy with OCP 4.12. You can also deploy on Red Hat OpenShift with OCP 4.11 if you prefer to use the internal PostgreSQL instance.

An instance of PostgreSQL is required for the SAS Data Infrastructure Server component. You can allow SAS to automatically deploy an instance of PostgreSQL, which is referred to as an *internal* instance, or you can provide your own PostgreSQL, which is an *external* instance.

Note: After the SAS Viya platform has been deployed, you cannot change the PostgreSQL deployment type without redeploying the entire software package.

The following offerings do not support an external PostgreSQL database instance:

- SAS Cost and Profitability Management
- SAS Retail products (SAS Inventory Optimization, SAS Markdown Optimization, and SAS Size Optimization)
- SAS Revenue Optimization products (SAS Markdown Optimization, SAS Promotion Optimization, and SAS Regular Price Optimization)

PostgreSQL Server Storage Requirements

SAS Infrastructure Data Server requires 128 GB of disk space. Three machines are the minimum requirement for high availability (HA).

Both types of PostgreSQL instance require persistent storage and PVCs. For more information, see "Persistent Storage Volumes, PersistentVolumeClaims, and Storage Classes" on page 22.

If a single PostgreSQL server supports multiple SAS Viya platform deployments that are typical in size, use the following guidance to determine storage space:

- For 1–2 deployments, use at least 128 GB of storage space.
- For 3–4 deployments, use at least 512 GB of storage space.

In a Microsoft Azure deployment, the Azure File (azure-file) storage class is not compatible with SAS Infrastructure Data Server. Use another storage class, such as Azure Disk (azure-disk) or NFS for the PostgreSQL server. A storage class can be selected only during the initial deployment. You cannot change the storage class after the deployment has completed.

Internal PostgreSQL Requirements

IMPORTANT The combination of Kubernetes 1.26 and an internal instance of the PostgreSQL database is experimental in the 2023.06 release of the SAS Viya platform. *Experimental* software has been tested prior to release, but because it has not necessarily been tested to production-quality standards, it should be used with care.

SAS deploys a comprehensive PostgreSQL container operator suite provided by Crunchy Data for the internal PostgreSQL instance.

A Kubernetes cluster that contains multiple deployments of SAS Viya with internal instances of PostgreSQL is a supported topology. However, multiple deployments that run in separate namespaces might share deployment resources. If your deployments are not updated to the same version of the SAS Viya platform, the different Crunchy Data instances might create compatibility issues.

External PostgreSQL Requirements

With an external instance of PostgreSQL, you configure and maintain the PostgreSQL deployment. Providing your own instance means that you have more control over updates and can rely on a third party for support if desired. The following requirements apply:

- PostgreSQL versions 11 - 14 are the only supported versions of PostgreSQL for a SAS Viya external data server.

  Note: SAS Viya platform 2022.10 or later is required if you want to use PostgreSQL 13. SAS Viya platform 2023.03 or later is required for PostgreSQL 14.

- Managed PostgreSQL instances that are hosted by your cloud provider are supported. See "Supported Distributions for External PostgreSQL" on page 77 for version information.
- SAS recommends configuring PostgreSQL servers for HA. You can follow your selected vendor's documentation to complete this setup.
- The plpgsql extension is required. (Typically, it is included by default.)
- The external PostgreSQL instance must already be running and the database owner must be created before you start the SAS Viya deployment.
- An external PostgreSQL server should support a maximum number of connections, max_connections on some providers, and max_prepared_transactions of at least 1024. See "Tuning the PostgreSQL Server" in *SAS Viya Platform Administration: Tuning* for additional recommendations. If the cloud provider (such as Microsoft Azure) limits the number of allowed connections in proportion to the size of the server, be sure to select a server with a size that is sufficient to meet this requirement.
- Depending on the database that you provided, the database or schema owner requires permissions to Create, Read, Update, and Delete (CRUD). For example, if the SAS Viya platform database has not yet been created on the PostgreSQL instance that you provide, the deployment process creates it for you, using the database owner that you provided. Adjust user roles, database permissions, and attributes accordingly.
- To enable some SAS Viya platform features, such as backup, restore, and multi-tenancy, the user ID of the database owner should be created with CREATE ROLE and CREATEDB permissions. In addition, this user must be the owner of the initial database that is created for the SAS Viya platform in the external PostgreSQL instance.

  The user that is the database owner must also have CONNECT privileges on the system database named `postgres` to enable SAS Viya platform services to start up.

  Refer to the following PostgreSQL documentation for details: https://www.postgresql.org/docs/12/ddl-priv.html.
- A low-latency, high-bandwidth environment is required.

  Placing the external PostgreSQL database in a separate data center, region, or availability zone from the rest of your SAS Viya platform components might lead to increased latency and reduced bandwidth. Such conditions are likely to cause a degraded overall performance of the environment. Before attempting to deploy the SAS Viya platform with an external PostgreSQL database, it is important to test with it in order to balance cost and performance considerations and to confirm that performance is not adversely affected.
- (GCP only) You must use Google's Cloud SQL Proxy to access your Cloud SQL for PostgreSQL server.

Security Considerations

SAS strongly recommends the use of TLS (SSL) to secure data in transit. You should follow the documented best practices provided by your cloud platform provider for securing access to your database using TLS.

The CA certificate that is used to apply TLS to the PostgreSQL server must be added to your SAS Viya platform deployment. As part of securing the PostgreSQL server, your cloud provider might provide such a certificate. Make this CA certificate available during the deployment process so that it can be imported into the SAS Viya platform certificate infrastructure. For more information about how certificates are managed, see "Incorporate Additional CA Certificates" in *SAS Viya Platform Encryption: Data in Motion*.

Additional steps are required in order to support full TLS. For more information, see the README file at `$deploy/sas-bases/examples/postgres/configure/README.md` (for Markdown format) or at `$deploy/sas-bases/docs/configure_postgresql.htm` (for HTML).

Supported Distributions for External PostgreSQL

For an external PostgreSQL server, the SAS Viya platform supports PostgreSQL 11 - 14.

Note: SAS Viya platform 2022.10 or later is required if you want to use PostgreSQL 13. SAS Viya platform 2023.03 or later is required if you want to use PostgreSQL 14.

The SAS Viya platform supports the following PostgreSQL distributions from the supported cloud providers:

- PostgreSQL (Open Source)

  IMPORTANT Open Source PostgreSQL is not highly available by default. Attempting to deploy Open Source PostgreSQL with HA is a challenging task. SAS Viya platform components are designed for HA, but deploying with a non-HA single instance of Open Source PostgreSQL for SAS Infrastructure Data Server introduces a single point of failure that could compromise the availability of the entire SAS Viya platform.

- Microsoft Azure Database for PostgreSQL - Single Server (PostgreSQL 11 only; Microsoft is retiring this product)
- Microsoft Azure Database for PostgreSQL - Flexible Server
- Amazon RDS for PostgreSQL
- GCP: Cloud SQL for PostgreSQL

SAS recommends that your PostgreSQL servers be configured for HA. You can follow your selected vendor's documentation to complete this setup.

PostgreSQL Requirements for a Multi-Tenant Deployment

SAS Infrastructure Data Server is an important component for multi-tenancy and provides data isolation. You have two options for setting up this isolation:

- a separate PostgreSQL database for each tenant

  A separate database instance is provisioned for each tenant. However, each tenant must have a unique database connection pool, which might significantly increase the total connection count that the back-end database server must support. Additional tuning is required.

- a shared PostgreSQL database that is partitioned to provide tenant isolation

  A single database is shared by all tenants, but each tenant is partitioned into separate schemas. The schema's name is generated based on the application and tenant name (such as identities_tenantA).

  This option is recommended when database connection resources are limited. A single connection pool is used for all tenants. In addition, because connections for all tenants come from

a single connection pool, a single tenant can consume all connection resources, depriving other tenants.

Mixing separate and shared database modes among tenants is not supported. Similarly, mixing internal and external PostgreSQL database instances among tenants is not supported.

For either option (separate databases per tenant or separate schemas per tenant), you should configure additional connections on the database server. Spikes in connection usage have been observed during tenant onboarding and when users log in and start using the SAS Viya platform. The baseline recommendation for the SAS Viya platform is to set `max_connections` to a minimum of 1024 for an external data server. The internal data server is set to 1280 max connections by default. However, this setting is partially dependent on the SAS offerings that you have purchased.

For an external or internal PostgreSQL data server, you can use the following baseline formula to size your environment and tune the settings to improve performance:

```
(number of tenants + 1) * 1128 = max_connections
```

For example, if you plan for three tenants, (3 tenants + 1 provider) * 1128 = 4512 max_connections.

In order to prepare for peak usage during tenant onboarding and SAS Viya platform usage, temporarily allocate additional connections:

- 20% more connections for the database-per-tenant option
- 25% more connections for the schema-per-tenant option

You can use a transformer to change the default value for max_connections. After you have downloaded the deployment assets, an example file for an internal PostgreSQL server, crunchy-tuning-connection-params-transformer.yaml, is provided in your **`$deploy/sas-bases/examples/crunchydata/tuning`** directory. You can update max_connections together with max_prepared_transactions as shown in the example file. For more information, see **`$deploy/sas-bases/examples/crunchydata/tuning/README.md`** (for Markdown format) or **`$deploy/sas-bases/docs/postgres_configuration_settings_for_tuning.htm`** (for HTML format).

Note: Additional PostgreSQL tuning might be required after the deployment process has completed. More detailed information is available in "Tuning the PostgreSQL Server" in *SAS Viya Platform Administration: Tuning*.

SAS Common Data Store Requirements

SAS Common Data Store, or CDS PostgreSQL, is an additional PostgreSQL cluster that some services in your SAS Viya platform deployment might use. It is configured separately from the required platform PostgreSQL cluster that supports SAS Infrastructure Data Server.

Only the following offerings on the SAS Viya platform require this separate PostgreSQL cluster; an asterisk indicates that they support it on an internal or external PostgreSQL instance:

- SAS Asset and Liability Management*
- SAS Assortment Planning*
- SAS Cost and Profitability Management
- SAS Demand Planning*
- SAS Dynamic Actuarial Modeling*
- SAS Expected Credit Loss*

- SAS Financial Management*
- SAS Financial Planning*
- SAS Inventory Optimization
- SAS Markdown Optimization
- SAS Model Risk Management*
- SAS Promotion Optimization
- SAS Regular Price Optimization
- SAS Size Optimization
- SAS Stress Testing*

Some offerings on the SAS Viya platform support only an internal PostgreSQL database for CDS. If your deployment includes any of those SAS offerings, you cannot use an external instance for SAS Infrastructure Data Server or for SAS Common Data Store because they must match. SAS offerings that do not support an external PostgreSQL database are listed in "Internal versus External PostgreSQL Instances" on page 74.

Additional configuration is required in order to include SAS Common Data Store in your deployment. For more information, see "Configure CDS PostgreSQL" in *SAS Viya Platform: Deployment Guide*.

OpenSearch Requirements

The SAS Viya platform includes OpenSearch, which is an Apache 2.0-licensed distribution of OpenSearch with enhanced security. The SAS Viya platform uses it to support search features. By default, it is deployed automatically.

Additions to the kustomization.yaml file are required in order to configure OpenSearch. For more information, see Configure OpenSearch.

Internal versus External OpenSearch Instances

An instance of OpenSearch is required for a deployment of the SAS Viya platform. If you decide to deploy an internal instance of OpenSearch, SAS provides the instance and configures the deployment for you. SAS deploys a custom Kubernetes operator, sas-opendistro, for this purpose.

Starting with 2023.03, you can manage your own OpenSearch clusters and integrate these OpenSearch instances with SAS applications that are deployed with the SAS Viya platform ("external OpenSearch"). You can apply a transformer to your deployment in order to configure a connection to an external OpenSearch cluster. You can then use these OpenSearch instances to create and store search indices.

IMPORTANT After you have completed the deployment process for the SAS Viya platform, you cannot change the OpenSearch deployment type without a full redeployment.

Your external OpenSearch cluster can be running on either physical or virtual machines or in a cloud environment. However, it must conform to the remaining requirements that are described in this section.

Modify Default Virtual Memory Resources

The OpenSearch pods require additional virtual memory resources. All nodes that run workloads in the stateful workload class are affected by this requirement. In order to provide these memory resources, a transformer can use a privileged container to set the virtual memory for the mmapfs directory to the required level. However, privileged containers must be permitted by your pod security policies.

If privileged containers are enabled, you can add a transformer, sysctl-transformer.yaml, to the base kustomization.yaml file and configure the corresponding overlay. Otherwise, you have other options for configuring memory resources before you start the deployment process, including modifying settings manually on each node.

If you are using a managed Kubernetes cluster, your cloud provider probably provisions the nodes dynamically. In this instance, be aware that manual modifications do not persist after a restart of a Kubernetes node. The cluster administrator must use an alternative method to save the vm.max_map_count setting.

For information about all of your options for managing memory settings, see Configure Default Virtual Memory Resources.

Provision Storage

Deploying OpenSearch requires a StorageClass that provides persistent block storage or a local file system mount in order to store the search indices. Remote file systems, such as NFS, are not supported for this purpose. However, the default storage class in cloud platforms is typically adequate.

On cloud or virtualization platforms, SAS recommends provisioning the required storage using features that are provided by the platform, such as Azure Disk or vSphere volumes. For physical machines or for virtualization platforms that lack dynamic provisioning, SAS recommends using local storage: persistent volumes with disks of sufficient size and a Kubernetes provisioner for local storage, such as the Kubernetes SIG local persistent volume static provisioner.

Note: If local persistent volumes are used to provide storage for OpenSearch, you should increase the size of the OpenSearch cluster to at least 2 nodes in order to ensure availability, or 3 nodes for high availability. After you have downloaded the deployment assets, you can find instructions for changing the size of the cluster while avoiding downtime in `$deploy/sas-bases/examples/configure-elasticsearch/internal/topology/README.md` (for Markdown format) or `$deploy/sas-bases/docs/configure_a_default_topology_for_opensearch.htm` (for HTML format).

Here are some examples of StorageClass options that meet the minimum requirements:

Table 25 *Storage Options per Platform*

Platform	StorageClass
Microsoft Azure	default (kubernetes.io/azure-disk)

Platform	StorageClass
Amazon Web Services	gp2 (kubernetes.io/aws-ebs)
Google Cloud Platform	standard (kubernetes.io/gce-pd)
Open source Kubernetes	Customer-provided storage class for local disk storage as appropriate for the target cloud platform or infrastructure
Red Hat OpenShift	thin (kubernetes.io/vsphere-volume)

Note: In a multi-tenant deployment, all tenants use the same OpenSearch resources.

A minimum of one PVC is required, with accessMode RWO. The PVC is typically created automatically as part of the deployment, with a default size of 128 Gi.

To help you customize your deployment to apply the required StorageClass and transformer, an example file for OpenSearch has been provided in `$deploy/sas-bases/examples/configure-elasticsearch/internal/storage/`. The README file in the same directory provides instructions, or see `$deploy/sas-bases/docs/configure_a_default_storageclass_for_opensearch.htm` for the instructions in HTML format.

For more information about storage requirements, see "Persistent Storage Volumes, PersistentVolumeClaims, and Storage Classes".

Configure a Storage Class for Red Hat OpenShift

OpenSearch requires a StorageClass that provides persistent storage for the search indices. For OpenShift in a vSphere private cloud, the thin StorageClass is an example of a StorageClass that is appropriate for OpenSearch. However, you must customize your deployment to point to the required StorageClass and transformer.

The example YAML file that is shown in VMware vSphere object definition creates an appropriate storage class on the specified VMware data store. The SAS administrator can then use that data store for the VMware VMDK files.

To help you customize your deployment to apply the required StorageClass and transformer, an example file for OpenSearch has been provided in `$deploy/sas-bases/examples/configure-elasticsearch/internal/storage`. The README file in the same directory provides instructions, or see `$deploy/sas-bases/docs/configure_a_default_storageclass_for_opensearch.htm` for the instructions in HTML format.

On OpenShift, you must also configure permissions in VMware vSphere to enable the provisioning of the storage option that you select. The user that is specified in the install-config.yaml file for the vSphere installation must have the roles and privileges that are required for persistent volume provisioning. The required permissions depend on whether you provision static or dynamic storage.

SAS recommends that you use an OpenShift plug-in for vSphere to enable the StorageClass. The OpenShift documentation describes multiple storage options that the SAS Viya platform supports. You can follow the instructions that Red Hat provides in Persistent storage using VMware vSphere volumes to set up persistent storage for OpenSearch.

Additional Configuration for OpenShift

OpenSearch on OpenShift requires that you apply some Security Context Constraints. Deploying on OpenShift also requires changes to a few kernel settings. For more information, "Security Context Constraints and Service Accounts" in *SAS Viya Platform: Deployment Guide*.

Additional Requirements for External OpenSearch

If you decide to deploy external instance of OpenSearch, you are responsible for every aspect of installing, configuring and managing the external OpenSearch instance. The following requirements apply:

- [ ] SAS Viya platform 2023.03 or later
- [ ] OpenSearch 2.5

  At this time, this is the only currently supported version of OpenSearch. SAS has tested only with non-managed, Helm installations of OpenSearch 2.5.
- [ ] The following OpenSearch plug-ins:
  - analysis-icu
  - analysis-kuromoji
  - analysis-nori
  - analysis-phonetic
  - analysis-smartcn
  - analysis-stempel
  - mapper-murmur3
- [ ] The CA certificate that is used to secure the OpenSearch cluster

  You must make this certificate available during the deployment process so that it can be imported into the SAS Viya platform certificate infrastructure. For more information about certificate management, see "Incorporate Additional CA Certificates" in *SAS Viya Platform Encryption: Data in Motion*.
- [ ] (For SAS Visual Investigator only) A specific configuration of the OpenSearch security plug-in

  For more information, see the README file at `$deploy/sas-bases/examples/configure-elasticsearch/external/securityconfig/README.md` (for Markdown format) or `$deploy/sas-bases/docs/configure_an_external_opensearch_instance.htm` (for HTML).

Finally, you must configure the SAS Viya platform deployment to connect to the external OpenSearch instance. The README file provides instructions. For more information, see `$deploy/sas-bases/examples/configure-elasticsearch/external/README.md` (for Markdown format) or `$deploy/sas-bases/docs/configure_an_external_opensearch_instance.htm` (for HTML).

Additional Configuration for FIPS Compliance

SAS Viya supports the use of FIPS 140-2 validated cryptographic modules when they are executed on Kubernetes nodes that are running in FIPS mode. However, neither the internal nor the external instance of OpenSearch supports running in a FIPS-enabled environment at this time.

In order to enable OpenSearch to start and run in a FIPS-enabled environment, some additional configuration is required. You must apply a transformer to your deployment manifest in order to disable the FIPS-enabled behavior of the Red Hat JDK and allow the use of non-FIPS cryptography. For more information and an example, see “Additional Configuration for FIPS Compliance” in *SAS Viya Platform: Deployment Guide*.

Client Requirements

Web Browsers

End users can access the product user interfaces for applications that run on the SAS Viya platform from a desktop computer, using a supported web browser. Client computers that access SAS application user interfaces should be running a recent version of Windows, Linux, or macOS. Use 64-bit operating systems and 64-bit browsers. The following web browsers are supported:

- Apple Safari (latest stable version)
- Google Chrome (latest stable version)
- Microsoft Edge on Chromium (latest stable version)
- Mozilla Firefox (latest stable version and latest Extended Support Release version)

SAS recommends using the latest versions of these browsers for enhanced performance and security. Your browser must be enabled for JavaScript.

Mobile Platform Support

Some SAS user interfaces are not currently supported on mobile devices.

When SAS Visual Analytics Apps for iOS and Android are installed on a mobile device, users of the following interfaces can view and explore reports on the mobile device:

- SAS Visual Analytics
- SAS Visual Statistics
- SAS Viya

SAS Visual Analytics Apps are supported on iOS and Android smartphones and tablets. Each app is written specifically for its operating system and provides native support for these devices so that you

can view and explore reports on your mobile device using a touchscreen. You can download the apps for free from the Apple App Store or Google Play.

Client Machine Minimum Hardware

End users can access the product user interfaces for SAS applications from a desktop computer, using a supported web browser. Because SAS software is not installed on client machines, the requirements are minimal. The following minimum resources are recommended for client machines:

- A minimum of two CPU cores
- 16 GB of RAM
- Swap space: 1.5 times physical RAM or 250 GB, whichever is less
- Minimum screen resolution of 1536x864.

Support for Map Services

Some applications that run on the SAS Viya platform support multiple third-party map services, including OpenStreetMap, ArcGIS Online, and Esri ArcGIS Enterprise Portal. For Esri ArcGIS Enterprise Portal access, the SAS Viya platform supports an Esri server version 10.4 and later. The server can be installed on premises (Esri ArcGIS Enterprise Portal) or running remotely (ArcGIS Online).

Esri has ended support for the 10.3.1 version as of December 2020. SAS might not be able to assist you if you encounter problems with versions earlier than 10.4.

IMPORTANT The SAS Viya platform currently supports only token-based authentication for Esri. For example, an Esri server that is configured for Integrated Windows Authentication (IWA) is incompatible with the SAS Viya platform.

Product-Specific Requirements

Software Offerings and Platform Compatibility

Some SAS software offerings offer support for only a subset of the cloud providers that SAS Viya supports. The following table lists software offerings that are available for SAS Viya and indicates the environments where they can be deployed:

Table 26 *SAS Programming, Analytics, and Machine Learning Offerings and Cloud Providers*

Offerings	Supported Cloud Providers				
	Microsoft Azure	Amazon Web Services	GCP and Anthos Clusters on VMware	Open Source Kubernetes	Red Hat OpenShift
SAS Data Engineering	✓	✓	✓	✓	✓
SAS Econometrics	✓	✓	✓	✓	✓
SAS IML	✓	✓	✓	✓	✓
SAS Intelligent Decisioning	✓	✓	✓	✓	✓
SAS Studio Analyst	✓	✓	✓	✓	✓
SAS Studio Engineer	✓	✓	✓	✓	✓
SAS Visual Analytics	✓	✓	✓	✓	✓
SAS Visual Forecasting	✓	✓	✓	✓	✓
SAS Visual Statistics	✓	✓	✓	✓	✓
SAS Visual Text Analytics	✓	✓	✓	✓	✓
SAS Viya	✓	✓	✓	✓	✓
SAS Viya Advanced	✓	✓	✓	✓	✓
SAS Viya Enterprise	✓	✓	✓	✓	✓
SAS Viya Programming	✓	✓	✓	✓	✓
SAS Viya with SingleStore	✓	✓		✓	

Table 27 *SAS Offerings for Managing Data, Models, and Workloads and Cloud Providers*

Offerings	Supported Cloud Providers				
	Microsoft Azure	Amazon Web Services	GCP and Anthos Clusters on VMware	Open Source Kubernetes	Red Hat OpenShift
SAS/ACCESS	✓	✓	✓	✓	✓
SAS In-Database Technologies for Azure Synapse Analytics	✓	✓	✓	✓	✓
SAS In-Database Technologies for Cloudera Data Platform	✓	✓	✓	✓	✓
SAS In-Database Technologies for Databricks	✓	✓	✓	✓	✓
SAS In-Database Technologies for Hadoop Cloud Services	✓	✓	✓	✓	✓
SAS In-Database Technologies for Teradata	✓	✓	✓	✓	✓
SAS Information Governance	✓	✓	✓	✓	✓
SAS Model Manager	✓	✓	✓	✓	✓
SAS Workload Management	✓	✓	✓	✓	✓

Table 28 *SAS Fraud and Risk Offerings and Cloud Providers*

Offerings	Supported Cloud Providers				
	Microsoft Azure	Amazon Web Services	GCP and Anthos Clusters on VMware	Open Source Kubernetes	Red Hat OpenShift
SAS Asset and Liability Management	✓	✓	✓	✓	✓
SAS Asset Performance Analytics	✓	✓	✓	✓	✓

Offerings	Supported Cloud Providers				
	Microsoft Azure	Amazon Web Services	GCP and Anthos Clusters on VMware	Open Source Kubernetes	Red Hat OpenShift
SAS Business Orchestration Services	✓			✓	
SAS Dynamic Actuarial Modeling	✓	✓			
SAS Expected Credit Loss	✓	✓	✓	✓	✓
SAS Fraud Decisioning	✓				
SAS Industry Taxonomy Rules	✓	✓	✓	✓	✓
SAS Model Risk Management	✓	✓	✓	✓	✓
SAS Risk Engine	✓	✓	✓	✓	✓
SAS Risk Modeling	✓	✓	✓	✓	✓
Risk Modeling Add-on to SAS Viya	✓	✓	✓	✓	✓
SAS Risk Model Nodes	✓	✓	✓	✓	✓
SAS Stress Testing	✓	✓	✓	✓	✓

Table 29 *SAS Retail Offerings and Cloud Providers*

Offerings	Supported Cloud Providers				
	Microsoft Azure	Amazon Web Services	GCP and Anthos Clusters on VMware	Open Source Kubernetes	Red Hat OpenShift
SAS Assortment Planning	✓			✓	
SAS Cost and Profitability Management	✓			✓	
SAS Demand Planning	✓			✓	

Offerings	Supported Cloud Providers				
	Microsoft Azure	Amazon Web Services	GCP and Anthos Clusters on VMware	Open Source Kubernetes	Red Hat OpenShift
SAS Financial Management	✓			✓	
SAS Financial Planning	✓			✓	
SAS Inventory Optimization	✓			✓	
SAS Markdown Optimization	✓			✓	
SAS Optimization	✓	✓	✓	✓	✓
SAS Size Optimization	✓			✓	

Table 30 *SAS Law Enforcement Offerings and Cloud Providers*

Offerings	Supported Cloud Providers				
	Microsoft Azure	Amazon Web Services	GCP and Anthos Clusters on VMware	Open Source Kubernetes	Red Hat OpenShift
SAS Law Enforcement Intelligence	✓	✓	✓	✓	✓
SAS Visual Investigator	✓	✓	✓	✓	✓

Table 31 *SAS IoT Offerings, Streaming Analytics Offerings, and Cloud Providers*

Offerings	Supported Cloud Providers				
	Microsoft Azure	Amazon Web Services	GCP and Anthos Clusters on VMware	Open Source Kubernetes	Red Hat OpenShift
SAS Analytics for IoT	✓	✓	✓	✓	✓

Offerings	Supported Cloud Providers				
	Microsoft Azure	Amazon Web Services	GCP and Anthos Clusters on VMware	Open Source Kubernetes	Red Hat OpenShift
SAS Asset Performance Analytics	✓	✓	✓	✓	✓
SAS Event Stream Processing	✓	✓	✓	✓	✓
SAS Field Quality Analytics	✓	✓	✓	✓	✓
SAS Intelligent Monitoring	✓			✓	
SAS Production Quality Analytics	✓	✓	✓	✓	✓

Table 32 *SAS Health and Life Sciences Offerings and Cloud Providers*

Offerings	Supported Cloud Providers				
	Microsoft Azure	Amazon Web Services	GCP and Anthos Clusters on VMware	Open Source Kubernetes	Red Hat OpenShift
SAS Field Quality Analytics	✓	✓	✓	✓	✓
SAS Health Cohort Builder	✓	✓		✓	✓
SAS Health Episode Builder	✓				

Note: To find out when a software offering became available per release, see What's New in SAS Viya Platform Operations.

Limitations to Multi-Tenancy Support

The SAS Viya platform can be deployed with multi-tenancy enabled, but a few limitations apply to this feature:

- Authentication with an integrated SAS®9 environment using single sign-on and sign-off is not supported for a multi-tenant deployment.
- Kerberos with multi-tenancy does not support fall-back or password-based authentication in tenants. Password-based authentication only operates correctly in the provider tenant.

  SAS does not recommend using Kerberos with multi-tenancy.
- Mixing of LDAP and SCIM identity providers among tenants is not supported. All tenants must use one or the other.

The following product offerings do not support multi-tenant capabilities at this time:

- SAS Asset and Liability Management
- SAS Cost and Profitability Management
- SAS Viya with SingleStore
- SAS Micro Analytic Service does not support multi-tenancy for Python modules.

At this time, the following Risk products support only the database-per-tenant configuration:

- SAS Expected Credit Loss
- SAS Dynamic Actuarial Modeling
- SAS Model Risk Management
- SAS Stress Testing

Offerings and Action Sets that Support GPU Capabilities

The following SAS product offerings and CAS action sets offer support for a GPU. Depending on whether processing is based on a CAS action set or SAS procedure, the GPU processing capabilities are provided by a CAS server, a personal CAS server, or a compute server. In all cases, a GPU is not required, but offers advanced functionality:

GPU requirements are described in “Requirements for GPU Support” on page 29

Table 33 *GPU Support: Offerings on the SAS Viya Platform*

SAS Offerings	Features	Cloud Providers	Workload Class	Notes
SAS Viya	CAS Deep Learning System CAS action set: deepLearn	Azure, AWS, GCP, OpenShift	cas	
SAS Econometrics **Note:** SAS Econometrics is included with SAS Viya Advanced, with SAS Viya Programming, and	SAS Econometrics using deep learning methods CAS action set: deepecon	Azure, AWS, GCP, OpenShift	cas	GPU usage applies to deep neural network methods.

SAS Offerings	Features	Cloud Providers	Workload Class	Notes
with SAS Viya Enterprise.				
SAS Viya Programming SAS Event Stream Processing SAS Viya **Note:** SAS Event Stream Processing is included with SAS Viya Enterprise.	Analytic store (ASTORE) for deep learning, reinforcement learning, style generative adversarial networks (GAN), and tabular GAN. ONNX Runtime is included; it is used by SAS Event Stream Processing ONNX plug-in and ASTORE for scoring ONNX models. Models that use an OpenVINO device type are also supported.	Azure, AWS, GCP, OpenShift	cas	SAS Event Stream Processing does not use the SAS Viya GPU reservation service.
SAS Viya Enterprise SAS Viya SAS Event Stream Processing	Generative Adversarial Networks CAS action set: generativeAdversarialNet	Azure, AWS, GCP, OpenShift	cas	Some models use PyTorch, which is included automatically.
SAS IML SAS Viya Advanced SAS Analytics Pro Advanced Programming	SAS IML action set (CAS action set: iml) and IML Procedure	Azure, AWS, GCP, OpenShift	cas and compute	GPU usage applies to linear algebra routines.
SAS Viya	Language model CAS action set (langModel) ASTORE/ONNX integration supports all the following features: ■ Scoring data sets using a GPU	Azure	cas	Some models use PyTorch, which is included automatically.

SAS Offerings	Features	Cloud Providers	Workload Class	Notes
	■ YOLOv2, YOLOv3, and YOLOv4 ONNX models ■ SSD ONNX models ■ FasterRCNN ONNX models			
Personal CAS server (a single-user CAS server)	Generative Adversarial Networks Actions to create reinforcement learning agents (CAS action set: reinforcementLearn)	Azure, AWS, GCP, OpenShift	compute*	Some models use PyTorch, which is included automatically.

* A personal CAS server is intended for use by data scientists and users of applications such as SAS Studio. Therefore, it runs on the same node as the associated SAS Compute session.

Some configuration is required in order to start the GPU reservation service. If the action set or procedure uses the cas workload class, follow the steps in `$deploy/sas-bases/examples/gpu/README.md` (for Markdown format) or at `$deploy/sas-bases/docs/sas_gpu_reservation_service.htm` (for HTML format).

If the action set or procedure uses the compute workload class, follow the steps that are described in `$deploy/sas-bases/overlays/sas-programming-environment/gpu/README.md` (for Markdown format) or `$deploy/sas-bases/docs/sas_gpu_reservation_service_for_sas_programming_environment.htm` (for HTML format).

Requirements for SAS® for Microsoft® 365 Clients

SAS for Microsoft 365 enables SAS analytics to access reports directly from Microsoft Excel 365 and Microsoft Outlook 365 and provides integrated features. Some requirements for SAS for Microsoft 365 differ from those of other SAS offerings.

Supported Browsers for the Web Application

After you deploy the SAS Viya platform and configure SAS for Microsoft 365, the SAS for Microsoft 365 web application is available from the Microsoft Office 365 Excel and Microsoft Office 365 Outlook web clients in a supported web browser. When it runs in a browser, the SAS for Microsoft 365 web application supports only the following web browsers:

- Google Chrome 97 and later
- Microsoft Edge on Chromium 97 and later
- Mozilla Firefox 102 and later

- Apple Safari 16.0 and later on macOS (for Excel only)

Browsers running on mobile or touchscreen devices are not supported at this time.

Desktop Application Requirements

SAS for Microsoft 365 can also run as an installed add-in to a desktop version of Microsoft Office, with support for Excel and Outlook. In order to deploy the SAS for Microsoft 365 installed add-in for Microsoft Office, use a machine that meets the following requirements:

- Microsoft Windows 10 or later, or macOS

  Note: Outlook is not supported in a Safari browser on macOS.

- Microsoft 365 versions of Excel and Outlook, with an active subscription
- Microsoft Excel requires Microsoft Edge on Chromium with WebView2

  For more information, see this Microsoft article.

If you subscribe to the Semi-Annual Enterprise channel for Microsoft Office, an administrator must perform an additional step to enable the use of the WebView2 browser control in Office Version 2102 (July 2021). A new registry key is required. For details, see https://developer.microsoft.com/en-us/microsoft-365/blogs/understanding-office-add-ins-runtime/.

Security Requirements

Microsoft requires add-ins, such as SAS for Microsoft 365, to run in an iframe in the Office 365 web application. To ensure that SAS for Microsoft 365 works properly, your SAS administrator must update these properties in SAS Environment Manager after deployment. After changing properties in SAS Environment Manager, you must restart the SAS Viya platform pods for the changes to take effect.

For more information and step-by-step instructions, see "Configuring SAS for Microsoft 365" in *SAS for Microsoft 365: User's Guide*.

Requirements for SAS® Dynamic Actuarial Modeling

SAS Dynamic Actuarial Modeling requires SAS Common Data Store, or CDS PostgreSQL, an additional PostgreSQL cluster that is configured separately from the PostgreSQL cluster that provides SAS Infrastructure Data Server. The CDS cluster and the SAS Infrastructure Data Server cluster must be of the same type: internal or external. In other words, the two clusters must match. For more information, see "PostgreSQL Server Requirements" on page 74.

Following performance testing, SAS has derived a set of specific hardware implementation requirements for SAS Dynamic Actuarial Modeling on Kubernetes clusters. The following table provides minimum resource recommendations. Derived from SAS performance testing, these estimates are for a *small* deployment, which was defined as 2 concurrent user sessions. In SAS testing simulations, data sets were 50-100 MB, and batch workloads on the compute node were 100 MB. VM instances all used an Intel Cascade Lake processor. Two vCPUs are equivalent to one physical CPU core.

Note: A separate node for the SAS Micro Analytic Service is recommended.

Table 34 *Minimum Resource Recommendations for SAS Dynamic Actuarial Modeling*

Workload Class	Resources
System	RAM: 16 GB per instance CPU: 4 vCPU cores per instance Example number of machines: 1
CAS	RAM: 32 GB per instance CPU: 4 vCPU cores per instance Storage for CAS disk cache: 100 GB Example number of machines: 2 (MPP) or 1 (SMP)
Compute	RAM: 32 GB per instance CPU: 8 vCPU cores per instance Disk space for SASWork: 128 GB Example number of machines: 1
Stateful	RAM: 32 GB per instance CPU: 8 vCPU cores per instance Minimum storage: 60 GB Example number of machines: 1
Stateless	RAM: 32 GB per instance CPU: 8 vCPU cores per instance Example number of machines: 1
SAS Micro Analytic Service	RAM: 32 GB per instance CPU: 8 vCPU cores per instance Example number of machines: 1

SAS recommends using a Standard_E4s_v5 VM for CAS nodes and Standard_D8s_v5 VM for compute nodes.

Be sure to consult the recommendations for your cloud platform in “Sizing Recommendations” on page 35 for more sizing information.

Requirements for SAS® Model Risk Management

SAS Model Risk Management requires SAS Common Data Store, or CDS PostgreSQL, an additional PostgreSQL cluster that is configured separately from the PostgreSQL cluster that provides SAS Infrastructure Data Server. The CDS cluster and the SAS Infrastructure Data Server cluster must be

of the same type: internal or external. In other words, the two clusters must match. For more information, see “PostgreSQL Server Requirements” on page 74.

SAS Model Risk Management supports extensive customization. A Git repository is therefore required to enable the management and versioning of changes and customizations that occur over the lifetime of the deployment. You can use a Git repository from GitLab or Microsoft GitHub.

Your Git repository must have at least one initial default branch (for example, `/main`) with at least one file (for example, Readme.md) in it.

The following information is required in order to set up the connection to the Git repository:

- the protocol that is used to connect to the Git repository (for example, https)
- the user ID that will be used to connect to the repository (for example, mrmadmin)
- the base64-encoded version of the personal access token for the Git user ID
- the name of the repository (for example, mrmrepository)
- the name of the branch (for example, main)
- whether you want to append the namespace name to the branch name (Y or N)
- the full URL to the Git repository, including the protocol (for example, `https://mygitrepo.company.com/mrmrepository.git`)
- the URL of the host of the Git repository (for example, mygitrepo.company.com)

Customizations are required to configure PVCs for SAS Model Risk Management. For more information, see “Specify PersistentVolumeClaims to Use ReadWriteMany StorageClass” in *SAS Viya Platform: Deployment Guide*.

Requirements for SAS® Viya® with SingleStore

If your SAS software order included SAS Viya with SingleStore, some additional requirements apply to your deployment.

Overview

SAS Viya with SingleStore includes a data connector for SingleStore, an instance of SingleStore, and additional software components to manage it. SAS Viya with SingleStore also includes the SAS Embedded Process. The deployment process creates a required service account, sas-singlestore-operator.

When you order SAS Viya with SingleStore, you can choose to license SingleStore as either Standard or Premium. The SingleStore license is included in your software order.

You can deploy SAS Viya with SingleStore into a Kubernetes cluster that is running in Microsoft Azure, in AWS, or in a cluster that is managed by upstream open source Kubernetes. The SAS Viya Infrastructure as Code (IaC) GitHub projects for Microsoft Azure, for AWS, and for open source Kubernetes can be used to deploy SAS Viya with SingleStore. You can also add SAS Viya with SingleStore to a cluster where the SAS Viya platform is already deployed if the cluster meets the requirements that are described in this section.

If you want to add SAS Viya with SingleStore to an existing deployment, see “Adding SingleStore to an Existing SAS Viya Platform Deployment” in *SAS Viya Platform with SingleStore: Administration and Configuration Guide*.

Cluster Requirements for SingleStore

SAS Viya with SingleStore is deployed in a Kubernetes cluster along with the SAS Viya platform. You must deploy it in the same namespace as the platform.

The following table summarizes cluster requirements for this type of deployment:

Table 35 *Cluster Requirements for SAS Viya with SingleStore*

Required Component	Detailed Requirements
Kubernetes	Microsoft Azure Kubernetes Service (AKS), Amazon Elastic Kubernetes Service (Amazon EKS), or upstream open source Kubernetes. Refer to "Upgrading Kubernetes" on page 6 for specific Kubernetes version support.
Nodes	A single node is the minimum requirement for a SAS Viya with SingleStore deployment if you have a SingleStore Standard license. High Availability (HA) (two or more nodes) is required for a Premium license and is optional for a Standard license. SingleStore nodes are deployed in the same cluster as SAS Viya and are labeled for SingleStore. Individual node requirements are described in "SingleStore Node Requirements" on page 97. SAS recommends dedicating a node pool to SingleStore components in order to facilitate resource management.
CNI plug-in	A container network interface (CNI) plug-in is required. A deployment with kubenet is not supported at this time. The following Kubernetes CNI products are supported for a SAS Viya with SingleStore deployment: ■ Azure CNI on Microsoft Azure. ■ Calico CNI for AWS; the default plug-in is supported. ■ Calico CNI for upstream open source Kubernetes. **Note:** After you deploy the SAS Viya platform, you cannot change the container network interface from kubenet to Azure CNI without re-creating your cluster. Some additional configuration is required in order to configure Azure CNI for a deployment that uses SAS Viya 4 Infrastructure as Code (IaC) for Microsoft Azure. For more information, see "Modifying IaC for Azure CNI" in *SAS Viya Platform with SingleStore: Administration and Configuration Guide*.
LoadBalancer service; public IP address for the ingress controller	SingleStore deploys by using a Kubernetes LoadBalancer service. A public IP address for the ingress controller is created automatically when the LoadBalancer service is created. The SingleStore operator checks for an external IP address, and if the check fails, the operator does not create SingleStore pods. If your cluster lacks this external IP address, you might need to modify `/sas-bases/components/sas-singlestore/sas-`

Required Component	Detailed Requirements
	`singlestore-cluster.yaml` in order to specify NodePort for the serviceSpec. Copy this directory and its contents to the `site-config/sas-singlestore/components` directory for the changes to take effect. This file also contains the leafSpec and aggregatorSpec definitions, which you might also want to modify. SAS recommends that you use a utility like MetalLB to assign an IP address to the ingress controller in order to support SingleStore. As an alternative, you can use a NodePort service rather than a LoadBalancer service. **Note:** The kube-vip IP address management utility is not supported with SAS Viya with SingleStore at this time.
Network connections and IP addresses	CAS worker pods must be able to make a network connection to SingleStore aggregator pods. Fast network connections among CAS pods and the SingleStore pods are required. SingleStore recommends against enabling cross-availability zone (AZ) or multi-AZ failover for the cluster. They recommend configuring the network with guaranteed throughput--"10 Gbps" rather than "Up to 10 Gbps," for example. Azure CNI uses IP addresses from your Azure Virtual Network (VNet) pool. Therefore, if you deploy additional applications to the same Azure VNet pool as SingleStore, you reduce the IP addresses that are available to SAS Viya with SingleStore, which could cause operational instabilities in the SAS Viya platform or in SingleStore.
Additional requirements	The remainder of your cluster must conform to the requirements for a SAS Viya platform deployment in your selected cloud platform. For more information, see: ■ “Cluster Requirements for All Environments” on page 4 ■ “Cluster Requirements for Microsoft Azure” on page 11 ■ “Cluster Requirements for AWS” on page 12 ■ “Cluster Requirements for Upstream Open Source Kubernetes” on page 18 SingleStore makes a few additional recommendations on their website.

SingleStore nodes can be scaled up or down independently of the SAS Viya platform nodes in the deployment. The SAS Viya platform does not provide auto-scaling for the SingleStore components. However, you can manually scale the SingleStore deployment up, down, to zero, and from zero.

SingleStore Node Requirements

When you deploy SAS Viya with SingleStore, a supported version of SingleStoreDB 7.x is installed automatically. The deployment also provides an instance of SingleStore Operator.

The machines where you deploy SAS Viya with SingleStore have the following additional requirements:

- A single machine is the minimum requirement with a SingleStore Standard license. Two or more machines are the minimum requirement for a Premium license. However many machines you designate for SingleStore, the following are required:
  - Two or more aggregator nodes
  - Four or more leaf nodes

  For data resilience when running in production, SAS recommends enabling the High Availability mode with a redundancyLevel of 2 or more.

  You can run all SingleStore pods (aggregators and leaf nodes) on one machine if it has been provisioned with adequate CPU and RAM resources and is labeled for SingleStore, as described below.
- A Linux operating system.

  SAS Viya platform images are based on Red Hat Universal Base Image 8. They are not compatible with Windows.
- If you plan to use the CAS server with SAS Viya with SingleStore, the DML endpoint (svc-memsql-cluster-dml) is required.

  This endpoint is created automatically by the SingleStore Operator for Read/Write operations. It is load-balanced among your aggregators.
- At least 8 vCPUs and 64 GiB of RAM per leaf node.

  A SingleStore database unit deploys on a height=1 node (a baseline), which is defined as a pod with 8 vCPUs and 64 GiB of RAM.

  Note: The deployment of SAS Viya with SingleStore adds an operating-system daemon on each SingleStore cluster node. This daemon, sas-singlestore-osconfig, changes some Linux VM settings. SingleStore recommends setting the value of min_free_kbytes to either 1% of system RAM or 4 GiB, whichever is smaller. The default value for min_free_kbytes is 658096. This setting is appropriate for a VM with 64 GiB of RAM. However, for SingleStore nodes with more system RAM, the min_free_kbytes parameter is likely to require modification.
- Port 3306 must be configured for SingleStore access outside the Kubernetes cluster, using Kubernetes networking controls.

  Verify that firewalls are configured to enable communications through this port.

  You can secure this port with TLS by providing your own certificates, or by using one of the SAS Viya certificate generators on page 58.
- Labels and taints for SingleStore.

  Verify that SingleStore workloads will have dedicated resources.

  By default, SingleStore tolerates the label `workload.sas.com/class=singlestore` and has a Preferred Affinity for that label. SAS recommends that you apply this `singlestore` label and taint to all the nodes that will host SAS Viya with SingleStore components.
- Persistent storage. Use SSD disks or better.

  Each aggregator node requires a persistent volume with 512 GB of space.

  Each leaf node requires a persistent volume with 1200 GB of space.

  SAS has tested with the following storage options:
  - Microsoft Azure Premium Storage

- Elastic Block Storage for AWS (the default, gp2)

If these basic requirements do not provide the levels of performance that you require, see "Tuning SAS Viya with SingleStore" in *SAS Viya Platform Administration: Tuning* for additional recommendations.

Security Requirements

SingleStoreDB Studio is supported for managing the SingleStore deployment. However, its default configuration sends cleartext communications between the web application running in a web browser and the SingleStoreDB server, and this configuration is not supported. If you want to use SingleStoreDB Studio with SAS Viya with SingleStore, you must configure a websocket-enabled connection to SingleStore Studio. For more information, see "Enabling Security for SingleStoreDB Studio" in *SAS Viya Platform with SingleStore: Administration and Configuration Guide*.

Authentication to SingleStore requires external credentials. For more information, see "Security" in *SAS Viya Platform with SingleStore: Administration and Configuration Guide*.

Requirements for Backup and Restore Support

SingleStore provides its own support for backup and restore procedures. These procedures are not integrated into the standard SAS Viya platform backup and restore processes. For more information, see Back Up and Restore Data.

Additional Requirements and Configuration

Your next steps in fulfilling the requirements for SAS Viya with SingleStore depend on whether you are deploying the SAS Viya platform or adding SAS Viya with SingleStore to an existing SAS Viya platform deployment.

SAS Viya with SingleStore requires additional configuration after the deployment has completed. For more information about configuring and administering SAS Viya with SingleStore, see *SAS Viya Platform with SingleStore: Administration and Configuration Guide*.

Requirements for SAS® Visual Investigator

Some requirements for SAS Visual Investigator differ from those of other SAS offerings.

Requirements for SAS Infrastructure Data Server

When you deploy SAS Visual Investigator, the PostgreSQL database that serves as the SAS Infrastructure Data Server component requires capacity beyond SAS Viya platform default settings. The PostgreSQL database server must have sufficient storage capacity for the SAS Visual Investigator internal entity data and audits in addition to SAS Viya configuration data.

SAS has provided documentation to help you configure additional storage for the internal PostgreSQL server. After you have downloaded your deployment assets, see `$deploy/sas-bases/examples/postgres/storage/README.md` (for Markdown format) or `$deploy/sas-bases/docs/configuration_settings_for_postgresql_storage_size_storage_class_storage_type_and_storage_access_mode.htm` (for HTML).

See Also

- “PostgreSQL Server Requirements” on page 74
- “Tuning the PostgreSQL Server” in *SAS Viya Platform Administration: Tuning*

Requirements for OpenSearch

The SAS Viya platform includes an Apache 2.0-licensed distribution of OpenSearch that provides search features. By default, the SAS Viya platform deployment process creates one OpenSearch node, which acts as both a controller and a data node. When you deploy SAS Visual Investigator, you should expand the default OpenSearch cluster and provide additional resources to the designated nodes. SAS makes the following sizing recommendations:

- Increase the default heap size for OpenSearch data nodes to at least 8 Gi.
- Increase the number of data nodes to a minimum of 2, or 3 for high availability.
- (Optional) Increase the storage capacity for data nodes.

  The default storage capacity of the PVC that is automatically configured for OpenSearch is 128 Gi per data node.

SAS provides example YAML files to help you modify your OpenSearch cluster topology to accommodate SAS Visual Investigator. For instructions, see the README file that is available at `$deploy/sas-bases/examples/configure-elasticsearch/internal/topology/README.md` (for Markdown format) or `$deploy/sas-bases/docs/configure_a_default_topology_for_opensearch.htm` (for HTML).

See Also

“OpenSearch Requirements” on page 79

Requirements for SAS® Workload Management

If your deployment includes SAS Workload Management, the SAS Workload Orchestrator will be used by the launcher to schedule work that belongs to the compute workload class. To enable this capability, your cluster must include nodes that are labeled for that workload class. When they are used by other SAS offerings, compute servers are launched dynamically, on demand. However, when SAS Workload Management is deployed with the SAS Viya platform, compute servers and other components that are started by the launcher do not run if hosts with the `workload.sas.com/class=compute` label are not found in the cluster. For more information about workload classes, see “Plan the Workload Placement” in *SAS Viya Platform: Deployment Guide*.

In addition, the SAS Workload Orchestrator ClusterRole/ClusterRoleBinding must be applied to the cluster. The ClusterRole/ClusterRoleBinding is used to get information about node resources, enabling SAS Workload Orchestrator to determine CPU and memory resources to be used for scheduling. After you have downloaded and uncompressed the deployment assets, you can find information about applying these settings in the README file at `$deploy/sas-bases/overlays/sas-workload-orchestrator/README.md`.

Requirements for Optional Features

When you take advantage of certain SAS Viya features, additional requirements might apply to your deployment.

Requirements for a Multi-Tenant Environment

Requirements to support multi-tenancy are included in various locations throughout this guide. If you are deploying SAS Viya for multiple tenants, be sure to meet the requirements that are specified in the following sections:

- ☐ CAS server. Each tenant requires a dedicated CAS server. See “CAS Server Resources” on page 33.

  The script that creates a CAS server for each tenant, create-cas-server.sh, requires Bash version 4 or later.
- ☐ SAS Infrastructure Data Server. Both the internal and external PostgreSQL options are supported for multi-tenancy. Some additional requirements apply. See “PostgreSQL Requirements for a Multi-Tenant Deployment” on page 77.
- ☐ TLS certificates. See “TLS Requirements” on page 58.
- ☐ DNS configuration. See “DNS Requirements for Multi-Tenancy” on page 61.
- ☐ User accounts in your LDAP or SCIM identity provider. Additional configuration is required. See “Additional LDAP Requirements for Multi-Tenancy” on page 63 or “Additional SCIM Requirements for Multi-Tenancy” on page 64.

Automated onboarding and offboarding of tenants and CAS servers is supported by the viya4-deployment GitHub project. If you deploy with this project, continue to use this project for subsequent onboarding and offboarding.

Starting in 2023.03, all tenants in a multi-tenant deployment require SAS Programming Environment pod templates. For more information, see the "Create Kubernetes Resources" section of the README file located at `$deploy/sas-bases/examples/sas-tenant-job/README.md` (for Markdown format) or `$deploy/sas-bases/docs/onboard_or_offboard_tenants.htm` (for HTML format).

Multi-tenancy is not supported in every customer environment. For more information, see “Limitations to Multi-Tenancy Support” on page 89.

Integrating Open Source Tools

SAS Viya supports two-way communication between SAS Viya and open source environments. SAS Viya provides integration points with a variety of open source languages, including Python, R, Lua, and Java. The SAS Viya API and toolsets such as the SAS Scripting Wrapper for Analytics Transfer (SWAT) package enable programmers to process data in the CAS and Compute servers, using a language of their choice.

In order to take advantage of open source integration with SAS Viya, you must fulfill some additional requirements.

- [ ] Compatible versions of open source languages.

  Your Python or R source installation within your SAS Viya deployment must consist of Linux binaries that are compatible with Red Hat Universal Base Image 8. SAS Viya is not compatible with Python Windows binaries.

- [ ] Persistent volumes and PVCs.

  SAS Micro Analytic Service requires an ASTORES PVC. For more information, see “Persistent Volumes for Applications” on page 24.

  (Optional) SAS Configurator for Open Source requires a PVC for Python or for R. See below for details.

- [ ] Shared persistent storage.

  Configure shared persistent storage, such as an NFS server. NFS mounts are required for Python and R directories.

- [ ] (Optional) A Kubernetes LoadBalancer service.

  By default, the ingress controller that is configured for your cluster enables connectivity to CAS at an HTTP path. This path provides REST clients, including Python SWAT, with access to CAS from outside the cluster.

  However, an HTTP ingress does not enable external user access to the CAS controller binary port. Connections to the binary port are optional, but they typically perform better and can also be used by SAS Viya 3.5 or SAS 9.4. To use the CAS binary port, you must define a Kubernetes LoadBalancer service, which makes non-HTTP ports externally accessible. For more information, see “Cluster Ingress Requirements” on page 8.

  Python SWAT requires C language libraries in order to use a binary connection to the CAS server.

  For deployments in Microsoft Azure or in AWS, you must configure binary and HTTP services as LoadBalancer rather than NodePort (the default). The service definitions must include the IP addresses or IP address ranges of external users. Be aware that setting the service template to LoadBalancer affects all CAS services.

- [ ] (Optional) An HTTP service.

  This service enables HTTP REST communication and is an alternative to using the default HTTP ingress for external access to the CAS server.

  Both the HTTP service and the LoadBalancer service must be configured in your kustomization.yaml file. For more information, see “Configure External Access to CAS” in *SAS Viya Platform: Deployment Guide*.

- [ ] Authentication for external code configured.

  Enabling Python or R code to run on the SAS Viya cluster under the shared service account might allow for access to sensitive data or expose the CAS or Compute server to malicious code. Additional setup is required in order to enable authentication. For more information, see “Authenticating Users of External Languages” in *SAS Viya Platform Identity and Access Management: Fundamentals*.

SAS recommends that you also configure the following utilities:

- SAS Configurator for Open Source

  This application facilitates the download and management of Python and R from source. It provides a build of Python or R in a PVC. The PVC and the build that it contains are then referenced by pods that require Python or R for their operations.

After you have downloaded your deployment assets, the instructions to deploy SAS Configurator for Open Source are provided in the README file located in `$deploy/sas-bases/examples/sas-pyconfig` (in Markdown format) or `$deploy/sas-bases/docs/sas_configurator_for_open_source_options.htm` (HTML format).

- Python SWAT and R SWAT

  The SAS SWAT packages for Python and R provide interfaces to the CAS server. These interfaces enable Python or R to call CAS workflows, transfer data between CAS and the Python client, perform additional client-side processing in Python or R, or merge with data from other sources. For more information, see:

  - Getting Started with Python SWAT
  - SAS Scripting Wrapper for Analytics Transfer (SWAT) for R

SAS provides additional resources for developers, open-source programmers, and system administrators who want to take advantage of the computational capabilities of SAS Viya from open source coding interfaces. See the SAS Developer Home Page for up-to-date information about the available collections of resources, such as code libraries and APIs for building apps with SAS, SAS Viya and CAS REST APIs, and end-to-end example API use cases.

SAS strongly recommends that you access the README file for open source integration with SAS Viya. This document describes the post-installation steps that are required to install, configure, and deploy Python and R in order to enable integration with SAS Viya. After you have downloaded your deployment assets, it is located at `$deploy/sas-bases/examples/sas-open-source-config/README.md` (for Markdown format) or `$deploy/sas-bases/docs/configure_python_and_r_integration_with_sas_viya.htm` (for HTML format).

Logging and Monitoring Requirements

The SAS Viya platform supports optional tools that handle logging and help you monitor deployment health and performance. The SAS Viya Monitoring for Kubernetes GitHub project provides logging and monitoring tools that are designed to collect, view, and manage metrics from your SAS Viya deployment.

Software requirements for SAS Viya Logging are listed in "Prerequisites" in *SAS Viya Platform: Log and Metric Monitoring*. Persistent storage for the messages and performance metrics that are collected is also required. The amount of storage that is required depends on optional features and on your retention policies. For details about increasing the amount of storage that you have configured, see Increase Storage for Log Messages.

SAS Viya Monitoring for Kubernetes is available for download from a SAS-maintained GitHub repository. SAS recommends that you always use the most recent release. Update your deployment at least every six months in order to run with the latest bug fixes, security updates, and feature enhancements. For more information, see the SAS Viya Monitoring for Kubernetes project in GitHub: https://github.com/sassoftware/viya4-monitoring-kubernetes.

Verify the Environment

Run a Pre-installation Check

SAS recommends that you run the SAS Pre-Install Check Utility before deploying the software.

SAS Pre-Install Check retrieves information about your Kubernetes cluster and verifies that the cluster meets the documented requirements to deploy SAS Viya. The utility generates a report.html that displays the results of the checks that it performs.

The files that are required to create the Pre-Install Check Report and the instructions for running the utility are available at the SAS GitHub site. The README file contains links to “Pre-installation of SAS Viya System Requirements” and other tools that you can use once the deployment has completed.