SAS® Viya® Platform: Overview

2023.03 - 2023.04

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.

Introduction to the SAS Viya Platform

About the SAS Viya Platform

Here are essential points for administrators:

- Beginning with 2022.09 the version numbering is changed. The version will now be denoted by year and month, with the month written as a two digit code: 01 for January, 02 for February, and so on.
- The SAS Viya platform (2020.1 and later) is always deployed to a Kubernetes cluster. See "Kubernetes Cluster Requirements" in *System Requirements for the SAS Viya Platform*.
- The SAS Viya platform (2020.1 and later) is updated frequently. You can choose either monthly updates (Stable cadence) or biannual updates (Long-Term Support cadence). Support policies are cadence-based. See "How frequently is software released?" in *Getting Started with SAS Viya Platform Operations*.
- *SAS Viya 4* is a phrase that encompasses all cadence-based releases. Most references omit the number (4) because they are for a specific version (such as 2020.1) or they are for the SAS Viya platform in general. In some references that distinguish between generations of the SAS Viya platform, the number (4) is retained.

Key Elements

User Interfaces

mobile app
: SAS Visual Analytics Apps, which enable mobile device users to view and interact with reports. See "Mobile Platform Support" in *System Requirements for the SAS Viya Platform*.

web apps
: an integrated suite of apps. Here are examples:

Activity	Web App
Manage data.	SAS Data Explorer
Prepare data.	SAS Data Studio
Explore, visualize, and report.	SAS Visual Analytics
Build models.	Model Studio
Manage models.	SAS Model Manager
Share and collaborate.	SAS Drive
Develop SAS code.	SAS Studio
Manage the SAS environment.	SAS Environment Manager

Not all deployments include all apps. For client requirements, see "Web Browsers" in *System Requirements for the SAS Viya Platform*.

command-line interface (CLI)
: sas-viya CLI, which functions as the universal parent CLI for all SAS Viya 4 CLI plug-ins. See *SAS Viya Platform: Using the Command-Line Interface*.

application programming interfaces
: developer interfaces that are available at developer.sas.com.

Core Components

microservices
: a modular set of discrete services, such as Audit, Credentials, and Identities. Each microservice runs in its own process and communicates using HTTP. See *SAS Viya Platform: General Management of Servers and Services*.

SAS Compute Server
: the run-time engine for the SAS language. SAS Viya platform clients submit programs and stored procedures to the server in the form of jobs. The server uses the SAS language to process the jobs that it receives. See "SAS Compute Server and Compute Service" in *SAS Viya Platform: Programming Run-Time Servers*.

SAS Cloud Analytic Services (CAS)
: the analytics engine for the SAS Viya platform. CAS provides the run-time environment in which data management and analytics take place. CAS can be deployed to a single node or across multiple nodes. See *SAS Cloud Analytic Services: Fundamentals*.

Supporting Infrastructure

Consul
: an open-source tool and registry that SAS provides as SAS Configuration Server. The SAS Viya platform uses this component for service discovery and configuration. See "SAS Configuration Server" in *SAS Viya Platform: Infrastructure Servers*.

RabbitMQ
: an open-source message broker that SAS provides as SAS Message Broker. See "SAS Message Broker" in *SAS Viya Platform: Infrastructure Servers*.

Postgres
: an open-source database management system that SAS provides as SAS Infrastructure Data Server. The SAS Viya platform uses this component to store user content. The SAS Viya platform can use either the internal instance that it provides or an external instance that you provide. See "SAS Infrastructure Data Server (Platform PostgreSQL)" in *SAS Viya Platform: Infrastructure Servers*.

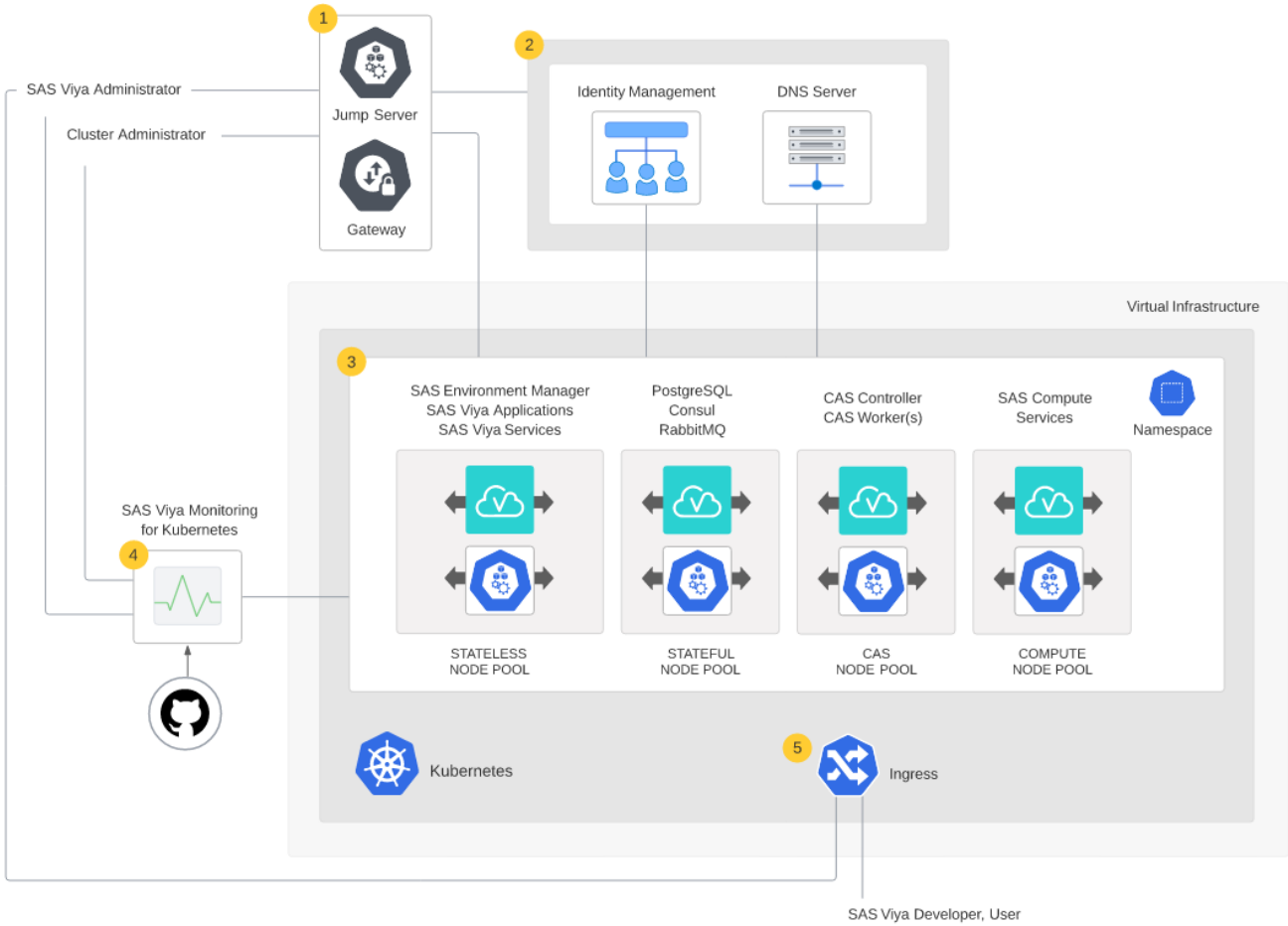
metric-monitoring tools
: GitHub resources and instructions that SAS provides for Prometheus and Grafana. As an alternative, you can use your own commodity services. See "Why Use SAS Viya Monitoring for Kubernetes?" in *SAS Viya Platform: Log and Metric Monitoring*.

log-monitoring tools
: GitHub resources and instructions that SAS provides for OpenSearch, Fluent Bit, and OpenSearch Dashboards. As an alternative, you can use your own commodity services. See "Why Use SAS Viya Monitoring for Kubernetes?" in *SAS Viya Platform: Log and Metric Monitoring*.

Reference Diagram

The following diagram is provided for orientation purposes. Not all components and options are depicted. For additional diagrams by cloud provider, see *Getting Started with SAS Viya Platform Operations*.

For SAS implementations of open-source components, the following diagrams use the common name, not the SAS name. For a mapping of the names, see "Supporting Infrastructure".



1 Administrators access the SAS Viya platform environment through a jump server and gateway. A cluster (Kubernetes) administrator deploys and updates the SAS Viya platform software and keeps the cluster operational. A client with the kubectl command-line tool installed is required in order to deploy and update the software. (This client is not included in the diagram.) A SAS Viya platform administrator uses SAS Environment Manager and other tools provided by SAS to manage the SAS Viya platform environment.

2 Third-party identity and access management providers are integrated with SAS Viya platform authentication. Several layers of security prevent unauthorized access to the SAS Viya platform. Routing services are configured with the IP addresses or user IDs of authorized external user accounts that are allowed to bypass the ingress. Identity and access management solutions provide data about internal user accounts to SAS Viya platform identification, authentication, and authorization services.

3 The topology for the SAS Viya platform software is shown across four node pools in a single namespace. The SAS Viya platform software consists of workload classes that are identified by the work that is performed by the associated pods: stateless, stateful, CAS, and compute.

4 SAS Viya Platform Monitoring for Kubernetes provides logging and monitoring tools that are designed specifically for SAS Viya. These tools are deployed from the SAS Viya Monitoring for Kubernetes GitHub site.

5 An ingress controller enables access to the software for SAS Viya platform developers and users.

See Also

- "Plan the Workload Placement" in *SAS Viya Platform: Deployment Guide*
- *System Requirements for the SAS Viya Platform*

Security in the SAS Viya Platform

About the Security Documentation

This section describes two categories of security documentation.

SAS Product Security

SAS product security documentation describes the SAS approach to building and maintaining secure software. Product security encompasses security assurance, privacy, and compliance statements. Product security documentation also includes security bulletins and incident management.

Here are key links to product security documentation:

- SAS Trust Center
- Security Assurance
- Security Bulletins and Updates

SAS Administration

SAS administrative documentation helps you understand and use the security features that SAS software provides. The security-related information in SAS administrative documentation addresses topics such as authentication, identity management, authorization, auditing, and encryption.

SAS administrative documentation is organized as follows:

platform information
: applies across products on the SAS Viya platform. Security information is integrated throughout the administrative documentation. Here are navigation tips:

  - For orientation, see the introduction below and the security section in the SAS Viya platform administration documentation.
  - To find specific information, use the search feature in the SAS Help Center for SAS Viya Platform Administration. That document collection contains all of the deployment, operations, and administration documentation for the SAS Viya platform.
  - When you use the SAS Help Center, make sure the correct release is selected in the banner.

product-specific information
: provides supplementary details for a particular product or solution. The documentation for each product includes any product-specific security information. Here are examples of product-specific security information:

  - SAS Event Stream Processing: Implementing Security
  - SAS Micro Analytic Service Security and Authorization

> **TIP** To access product-specific documentation, go to the SAS Viya: Documentation section on support.sas.com and make a selection from the **Solutions & Offerings for the SAS Viya Platform** list.

Introduction for Administrators

This section describes four aspects of platform security.

Authentication

Authentication is the aspect of security that verifies the identity of a user or service account. Supported authentication patterns include the following:

LDAP
: In this default pattern, SAS Logon Manager displays a sign-in form to the user and submits the entered credentials to the LDAP identity provider.

single sign-on
: In this alternate pattern, SAS Logon Manager uses one of the following technologies to authenticate users:

  - OAuth 2.0 and OpenID Connect (OIDC)
  - Security Assertion Markup Language (SAML)

Kerberos
: In this alternate pattern, SAS Logon Manager uses Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) to authenticate users against the Kerberos Key Distribution Center (KDC).

  In releases 2020.1.4 and later, end-to-end support is provided for Kerberos. You can use Kerberos to authenticate users who are signing in to the environment. You can use Kerberos to secure running jobs. You can configure Kerberos constrained delegation.

Note: In releases prior to 2020.1.4, you cannot configure Kerberos constrained delegation or use Kerberos to secure running jobs.

pluggable authentication module (PAM)
In this supplementary pattern, PAM is used to validate user credentials when users access the CAS server directly. PAM is supported for only CAS connections, not for web logins.

For more information, see the following documents:

SAS Viya Platform Identity and Access Management: Fundamentals

SAS Viya Platform: Authentication

SAS Viya Platform: Identity Management

SAS Viya Platform: External Credentials

Authorization

Authorization is the aspect of security that determines which resources are available to which users. The SAS Viya platform authorization layer consists of two authorization systems:

- CAS authorization system
- general authorization system

Each system uses a distinct model to protect a distinct class of resources.

Here are key points about initial and default access:

- Any access that is not granted is implicitly disallowed.
- Predefined objects are protected by predefined rules or access controls.
- All authenticated users have full access to a personal caslib and a personal folder.
- Only members of special groups or roles have access to highly privileged administrative functionality.
- Access to objects that users add is managed by inheritance, other influencing rules, and any direct settings.
- All authenticated users have Read and Write access to all data in the Public caslib and all content in the Public folder.

IMPORTANT The Public caslib and the Public folder facilitate open collaboration. Do not save sensitive data, objects that you need to control, or objects that you need to preserve to these unsecured locations. Instead, save such data and objects to additional folders and caslibs that you create and protect.

For more information, see the following documents:

SAS Viya Platform: CAS Authorization

SAS Viya Platform: General Authorization

SAS Viya Platform: Access to Functionality

SAS Viya Platform Identity and Access Management: Fundamentals

Encryption

Encryption is the aspect of security that converts data into an unintelligible form to increase protection. Each encryption technique and feature is applicable to either transmission (*data in motion*) or storage (*data at rest*).

For data in motion, the default configuration provides full-stack coverage with Transport Layer Security (TLS). Certificates are generated by cert-manager. Here are the key points:

- To implement the default configuration, you must apply the initial kustomization.yaml file that SAS provides.
- Full-stack coverage includes all entry points to the SAS Viya platform and all network connections within the cluster.
- TLS 1.2 is supported. Some services also support TLS 1.3.

For data at rest, encryption is not automatically enabled. You can configure encryption of data that is added to PATH and DNFS caslibs. SAS supports Advanced Encryption Standard (AES) for encryption of data at rest.

For more information, see the following documents:

SAS Viya Platform Encryption: Data in Motion

SAS Viya Platform Encryption: Data at Rest

Web Security

Introduction to Web Security

Web security is the aspect of security that deals with securing against certain types of attacks on web applications and using the security features that are available in modern web browsers.

For more information, see the following OWASP pages:

- Category:Attack
- OWASP Secure Headers Project
- Cross-Site Request Forgery (CSRF)
- Cross-Origin Resource Sharing

Web Security in the SAS Viya Platform

The SAS Viya platform provides properties that are configured, by default, to protect against the web security risks that are listed in the preceding section.

You can disable or change the properties, as appropriate for your environment. For example, you might have to configure Cross-Origin Resource Sharing (CORS) to allow origins in your company's domain. This allows SAS web pages to be included in other web pages inside your company's network.

The following SAS Viya platform configuration properties affect web security:

Property	Description	Default Settings
Cross-Origin Resource Sharing .	Technique for relaxing the browser same-origin policy, allowing Javascript on a web page to consume a REST API served from a different origin.	The following cross-origin requests are configured: ■ User credentials are used ■ All HTTP headers are allowed ■ All HTTP methods are allowed ■ Same origins are allowed
Cross-Site Request Forgery (CSRF)	Prevents attacks that force a user to execute unwanted actions on a web application in which they are currently authenticated.	The following options are configured: ■ All requests that use an authenticated HTTP session, except GET and HEAD requests, must pass a CSRF token specified by the server. ■ Referrers internal to the deployment are allowed.
X-Frame-Options	Avoids clickjacking attacks by making sure that your content is not embedded in other sites.	Same origin
Content-Security-Policy	Exposes and reduces the risk of data injection and cross-site scripting (XSS) attacks.	There is no universal default value. The value can vary by service and release. The configuration of the files service affects the risk of cross-site scripting attacks. See "Managing

Property	Description	Default Settings
		Cross-Site Scripting Risk for File Uploads".
X-Content-Type-Options	Prevents the browser from interpreting files as something other than what is declared by the content type in the HTTP headers (content sniffing).	nosniff
Note: The protections brought by this property are largely superseded by a strong content security policy. It is recommended to use the content-security-policy instead. X-XSS-Protection	Stops web browser from loading pages when XSS attacks are detected.	1; mode=block

Managing Cross-Site Scripting Risk for File Uploads

IMPORTANT To manage XSS risk for file uploads, make sure the files service is appropriately configured.

To reduce the risk of cross-site scripting attacks, the files service blocks uploads of any file that meets both of the following criteria:

- The file service scans the file's contents, because the file's MIME type is listed in the sas.files.scan.tenant.webContentTypes configuration property.
- The scan determines that file poses an unacceptable risk, because the file contains an absolute URL whose domain name is not listed in the sas.files.scan.tenant.domainAllowList configuration property.

When the files service blocks a file upload because the file meets the preceding criteria, the files service returns the error code 400 and the an error message that indicates that the file could not be uploaded because it contains an invalid URL.

To specify the file types that are scanned and the domain names that are allowed, adjust configuration properties for the files service.

For instructions, see "Edit Configuration Instances" in *SAS Environment Manager: User's Guide*.

For details about the configuration properties, see "Overview" in *SAS Viya Platform: Configuration Properties*.

SAS 9 and the SAS Viya Platform

Summary

SAS 9 customers continue to benefit from their investment in SAS 9 as they begin to make use of the SAS Viya platform functionality and features. From within familiar SAS 9 interfaces, projects, and code, customers can access the performance enhancements that the SAS Viya platform provides.

- On most hosts, SAS 9.4 is tightly integrated with SAS Viya platform. See SAS 9.4M5 and Later, Integration with SAS Viya in *What's New in Base SAS: Details*. (The exceptions are z/OS and 32–bit Windows.)
- All releases of SAS can use SAS/CONNECT as a bridge to SAS Viya platform. See the appendix "Sharing Data Between SAS 9 and SAS Viya using SAS/CONNECT" in *SAS/CONNECT for the SAS Viya Platform: User's Guide*.
- SAS Viya platform's visual web applications share a single sign-on and logout with the SAS 9 environment.

Here are some of the methods for accessing SAS 9 data from the SAS Viya platform:

- In SAS Visual Analytics, use self-service import. See *SAS Data Explorer: User's Guide*.
- In SAS Environment Manager, interactively load data. See *SAS Environment Manager: User's Guide*.
- In any programming interface, write code to load data. See *SAS Viya Platform Programming: Getting Started*.
- In SAS Enterprise Guide or SAS Add-In for Microsoft Office (7.13 or later), move data from SAS 9 to CAS. See the topic "Configure Your Environment to Use the Upload to CAS Task" in the SAS Enterprise Guide or SAS Add-In for Microsoft Office chapter in *SAS Intelligence Platform: Desktop Application Administration*.
- If a more seamless method is not available, use SAS/CONNECT to move and share data. See the appendix "Sharing Data Between SAS 9 and SAS Viya Platform using SAS/CONNECT" in *SAS/CONNECT for the SAS Viya Platform: User's Guide*.

Note: Your site must license and deploy the SAS Viya platform to access SAS Viya platform functionality. Not all deployments and releases include all products and support all methods.

Considerations: Interacting with SAS 9 Data

Manage User-Defined Formats

If you access SAS 9 data from the SAS Viya platform, you must make any user-defined formats available to your CAS session. See *SAS Cloud Analytic Services: User-Defined Formats*.

Considerations: Accessing CAS from SAS 9.4M5 and Later

IMPORTANT Connections to CAS from outside the Kubernetes cluster (for example, from SAS 9 or SAS Viya 3.5) use binary communication, which must be configured by your Kubernetes administrator. See "Configure External Access to CAS" in *SAS Viya Platform: Deployment Guide*.

IMPORTANT You cannot connect to the SAS 9.4 Metadata Server from the SAS Viya platform.

Find CAS

If a SAS 9.4M5 (or later) client session cannot find CAS, make information about the host and port of the CAS server available. For example, add the following line to your SAS Application Server sasv9_usermods.cfg or appserver_autoexec_usermods.sas file:

```
CASHOST="primary-controller-host-name" CASPORT=port;
```

Here is an example:

```
CASHOST="mysrv01" CASPORT=5570;
```

For more information, see the system options CASHOST= and CASPORT= in *SAS Cloud Analytic Services: User's Guide*.

Authenticate to CAS

If a SAS 9.4M5 (or later) client session cannot authenticate to CAS, create an authinfo file, store CAS credentials in the SAS 9 metadata, or use a different authentication mechanism. See *SAS Viya Platform: Authentication*.

SAS Visual Analytics Administration

SAS Viya platform administration documentation is applicable to SAS Visual Analytics. Links to specific SAS Visual Analytics topics that deserve special attention are included here:

- Granting guest access
- Making data available to CAS
- Managing user-defined formats
- Loading data for reports
- Using the reports alert service
- Using the report data service
- Using the report packages service
- Using the report renderer service
- Promoting data and report content
- Understanding identity management concepts
- Modifying rules that affect access to functionality
- Loading geographic polygon data as a CAS table
- Using the maps service to obtain polygon information
- Synchronizing time zone settings between CAS and the report data service
- SAS Compute Server and Compute Service
- SAS Report Package Reference (this topic is new in 2021.1.5)