Architecture of SAS Viya

Introduction
This section provides a concise summary for new administrators.

Here are related topics:
- To get started with SAS Viya administration, see SAS Viya Administration: Orientation.
- To learn about benefits of SAS Viya, see SAS Viya on the SAS website.

Key Components
Here are software components that might be of particular interest to administrators.
Cumulative Functionality

Among some of the products on SAS Viya, available functionality is cumulative.

- SAS Visual Analytics provides baseline functionality, including reporting and basic analytics.
- SAS Visual Statistics provides an additional set of advanced analytic functions.
- SAS Visual Data Mining and Machine Learning provides a second additional set of advanced analytic functions.

For example, if you have SAS Visual Data Mining and Machine Learning, the objects that are available in the SAS Visual Analytics web application are as follows:

TIP For information about other components, search the SAS Viya administration documentation.
Note: All three of the preceding products offer both programming and visual interfaces.

Selective Deployment (Optional)

By default, all of your software is deployed. As a convenience for special circumstances, it is possible to deploy only a subset of components. A programming-only deployment excludes general services and visual interfaces.
For example, a programming-only deployment of SAS Visual Analytics does not include the SAS Visual Analytics web application.
Security in SAS Viya

Authentication

Authentication is the aspect of security that verifies the identity of a user or service account. When you sign in, one of the following authentication patterns is used:

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host authentication</td>
<td>Requests are sent to the appropriate host and processed by any authentication mechanism supported by that host. Programming-only deployments</td>
<td>When you sign in to SAS Studio, the associated object spawner asks its host (which is also the host of the SAS Studio web application) to validate your credentials. That validation enables the object spawner to launch a workspace server for you.</td>
</tr>
<tr>
<td></td>
<td>use dual authentication for sign in to CAS Server Monitor and access to CAS from SAS Studio. Note: You can configure the host to use pluggable authentication modules (PAM). SAS provides starter PAM configuration files for CAS and SAS Studio. You can create an Authinfo file for use with PAM in command-line access to CAS.</td>
<td>When you access CAS from SAS Studio, you must authenticate to the host of the target CAS server. When you sign in to CAS Server Monitor, you must authenticate to the host of the target CAS server.</td>
</tr>
<tr>
<td>Direct LDAP authentication</td>
<td>Requests are sent to and processed by your designated direct LDAP provider, unless you configure front-end single sign-on using Kerberos, Open Authorization (OAuth), or Security Assertion Markup Language (SAML). User and group information is always obtained from your designated direct LDAP provider. Note: Kerberos, OAuth, and SAML are alternate mechanisms for identity verification by the logon service, not alternate sources of user and group information for the identities service.</td>
<td>When you sign in to a web application that uses the logon service (for example, SAS Visual Analytics or SAS Environment Manager), you must authenticate using this pattern. Before you can submit a command-line request to a general service (for example, the backup service or the transfer service), you must authenticate using this pattern.</td>
</tr>
<tr>
<td>Pattern</td>
<td>Description</td>
<td>Usage</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Dual authentication   | Requests are authenticated using both host authentication and direct LDAP authentication. If the servicesBaseUrl option is specified, CAS requires dual authentication. To facilitate this pattern, use one of these approaches:  
- Ensure that all requests are ultimately processed by the same authentication provider. For example, configure the SAS Studio and CAS hosts to use the same LDAP provider that is designated for direct LDAP authentication requests in your deployment.  
- Ensure that each affected user has a single set of credentials that are valid for all applicable authentication providers. | In a full deployment, dual authentication occurs for sign in to CAS Server Monitor and access to CAS from SAS Studio.  
Note: When you access CAS from a web application such as SAS Visual Analytics or SAS Environment Manager, your OAuth token is validated. |

The following high-level conceptual drawings illustrate key points from the preceding table:
After you sign in, you have seamless access to SAS Viya and, in some contexts, to external data sources.

For more information, see the following documents:

- *SAS Viya Administration: Authentication*
- *SAS Viya Administration: Identity Management*
Authorization

Authorization is the aspect of security that determines which resources are available to which users. The SAS Viya 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. The general authorization system is not applicable in a programming-only deployment.

Initial and default access are restrictive:

- Any access that is not granted is implicitly disallowed.
- Predefined objects are protected by predefined rules or access controls.
- Only members of special groups or roles have access to privileged administrative functionality.
- Access to objects that users add is managed by inheritance, other influencing rules, and any direct settings.
- Regular users have limited Write access. They can write to their personal folder, the shared Public folder, and the shared Public caslib.

For more information, see the following documents:

SAS Viya Administration: Orientation to Authorization
SAS Viya Administration: Cloud Analytic Services Authorization
SAS Viya Administration: General Authorization
SAS Viya Administration: Identity Management

Encryption

Encryption is the aspect of security that protects data by converting it into an unintelligible form in transmission or in storage.

For data in motion in a new deployment, TLS security is provided and follows the highest standards. At installation SAS Viya provides self-signed certificates to provide HTTP and HTTPS access to SASHome out of the box. You can increase the encryption strength and coverage by completing additional configuration.

For data at rest in a new deployment, encryption is not automatically enabled. You can configure encryption of data that is added to PATH, HDFS, and DNFS caslibs.

For more information, see the following documents:

Encryption in SAS Viya: Data in Motion
Encryption in SAS Viya: Data at Rest
**Web Security**

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

SAS Viya provides properties that are configured, by default, to protect against the web security risks that are listed below. You can disable or change the properties, based on 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.

For more information about the SAS Viya configuration properties, see the following:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-Origin Resource Sharing</td>
<td>Technique for relaxing the browser same-origin policy, allowing Javascript on a web page to consume a REST API served from a different origin.</td>
<td>The following cross-origin requests are configured: &lt;ul&gt;&lt;li&gt;User credentials are used&lt;/li&gt;&lt;li&gt;All HTTP headers are allowed&lt;/li&gt;&lt;li&gt;All HTTP methods are allowed&lt;/li&gt;&lt;li&gt;Same origins are allowed&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>Cross-Site Request Forgery (CSRF)</td>
<td>Prevents attacks that force a user to execute unwanted actions on a web application in which they are currently authenticated.</td>
<td>The following options are configured: &lt;ul&gt;&lt;li&gt;Referers internal to the deployment are allowed&lt;/li&gt;&lt;li&gt;Requests are not blocked if both the origin and referer headers are absent&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>X-Frame-Options</td>
<td>Avoids clickjacking attacks by making sure that your content is not embedded in other sites.</td>
<td>Same origin</td>
</tr>
<tr>
<td>Content-Security-Policy</td>
<td>Exposes and reduces the risk of data injection and cross-site scripting (XSS) attacks.</td>
<td>default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' *.sas.com blob: data:; style-src 'self' 'unsafe-inline'; child-src 'self' blob: data: mailto:;</td>
</tr>
<tr>
<td>X-Content-Type-Options</td>
<td>Prevents the browser from interpreting files as something other than what is declared by the content type in the HTTP headers (content sniffing).</td>
<td>nosniff</td>
</tr>
<tr>
<td>X-XSS-Protection</td>
<td>Stops web browser from loading pages when XSS attacks are detected.</td>
<td>1; mode=block</td>
</tr>
</tbody>
</table>

For information about these web attacks, see the following OWASP pages:
SAS 9 and SAS Viya

Summary

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

- On most hosts, SAS 9.4M5 is tightly integrated with SAS Viya. See SAS 9.4M5 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. See the appendix Sharing Data Between SAS 9 and SAS Viya using SAS/CONNECT in SAS/CONNECT for SAS Viya User’s Guide.

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

- In SAS Environment Manager, interactively load data. See Data Administration: How to (SAS Environment Manager) in SAS Viya Administration: Data.
- 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.
- In any programming interface, write code to load data. See Programming Interfaces in An Introduction to SAS Viya Programming.
- If a more seamless method is not available, use SAS/CONNECT for SAS 9 and SAS Viya to move and share data. See the appendix Sharing Data Between SAS 9 and SAS Viya using SAS/CONNECT in SAS/CONNECT for SAS Viya User’s Guide.

Note: Not all deployments and releases include all products and support all methods.


Considerations: Interacting with SAS 9 Data

Use UTF-8 Encoding

If you access SAS 9 data from SAS Viya, be aware that SAS Viya operates with UTF-8 encoded data. If your SAS 9 data is not UTF-8 encoded, you might need to re-create your data sets. See Migrating to UTF-8 for SAS Viya.

Manage User-Defined Formats

If you access SAS 9 data from SAS Viya, 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

Find CAS
If a SAS 9.4M5 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" <"backup-controller-host-name">) CASPORT=port;
```

Here is an example with a CAS backup controller:

```
CASHOST=("mysrv01" "mysrv02") CASPORT=5570;
```

Here is an example without a CAS backup controller:

```
CASHOST=('mysrv01") CASPORT=5570;
```

For more information, see CASHOST= System Option.

Authenticate to CAS
If a SAS 9.4M5 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 Administration: Authentication.

Conform to CAS Encryption Requirements
If a SAS 9.4M5 client session does not meet the encryption standards of the CAS server, make an appropriate certificate available. See “Configure SAS 9.4 Clients to Work with SAS Viya” in Encryption in SAS Viya: Data in Motion.