SAS® Viya® Administration: Fast Track

Course Notes

SAS® Viya® Administration: Fast Track Course Notes was developed by Dhaval U. Patel and Erik Pearsall. Additional contributions were made by Sheila Riley and Raymond Thomas. Instructional design, editing, and production support was provided by the Learning Design and Development team.

SAS® Viya® Administration: Fast Track Course Notes

Book code E71719, course code LWSVFT35/SVFT35, prepared date 17Jul2020. LWSVFT35_001

ISBN 978-1-951686-77-2

Table of Contents

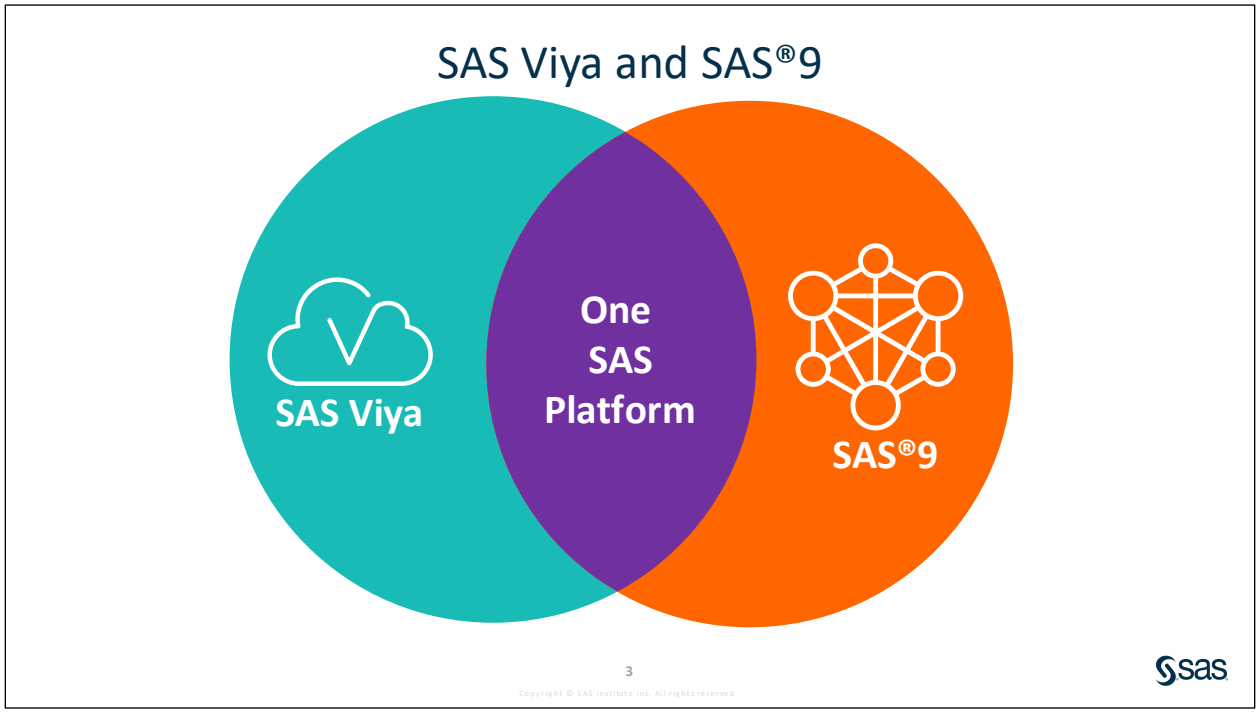
To learn more…

For information about other courses in the curriculum, contact the SAS Education Division at 1-800-333-7660, or send e-mail to training@sas.com. You can also find this information on the web at http://support.sas.com/training/ as well as in the Training Course Catalog.

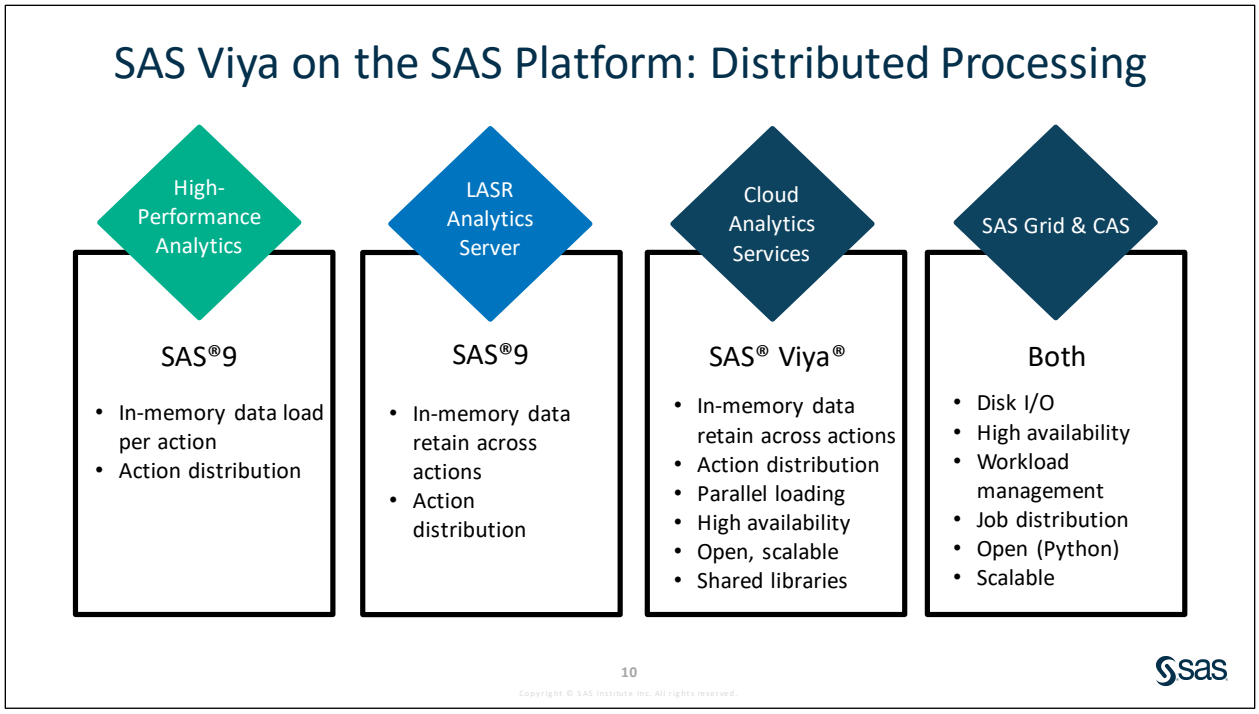
For a list of SAS books (including e-books) that relate to the topics covered in this course notes, visit https://www.sas.com/sas/books.html or call 1-800-727-0025. US customers receive free shipping to US addresses.

Lesson 1 Introduction to SAS® Viya®

1.1 Introduction to SAS Viya



SAS Viya is the latest enhancement of the SAS Platform. SAS Viya introduces new architecture, new product functionality, and interacts with the existing functionality of SAS®9.



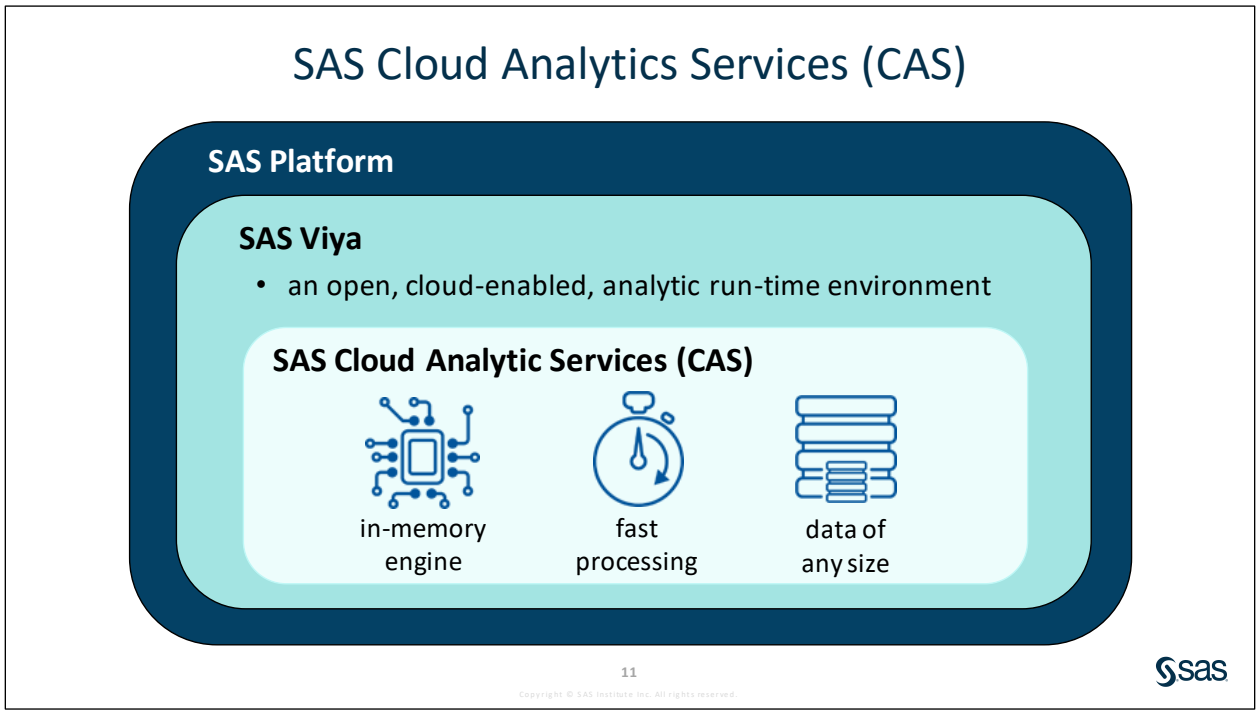
High-Performance Analytics: Distributed processing has been part of the SAS Platform for a number of years starting with high-performance analytics, or HPA. It is in-memory distributed processing of specific actions. Data is loaded into memory for the duration of that action or procedure. The SAS High-Performance Analytics solution is a collection of tools and data management strategies.

LASR Analytic Server: As big data became more prevalent, SAS started the development of an in-memory analytic server to serve the needs of customers who wanted a reliable way to visualize and analyze billions of rows of data at a time without having to read data off of disk. The result of this was the LASR analytic server, which drives SAS Visual Analytics and In-Memory Statistics. With the LASR analytic server, data is retained in memory across procedural calls.

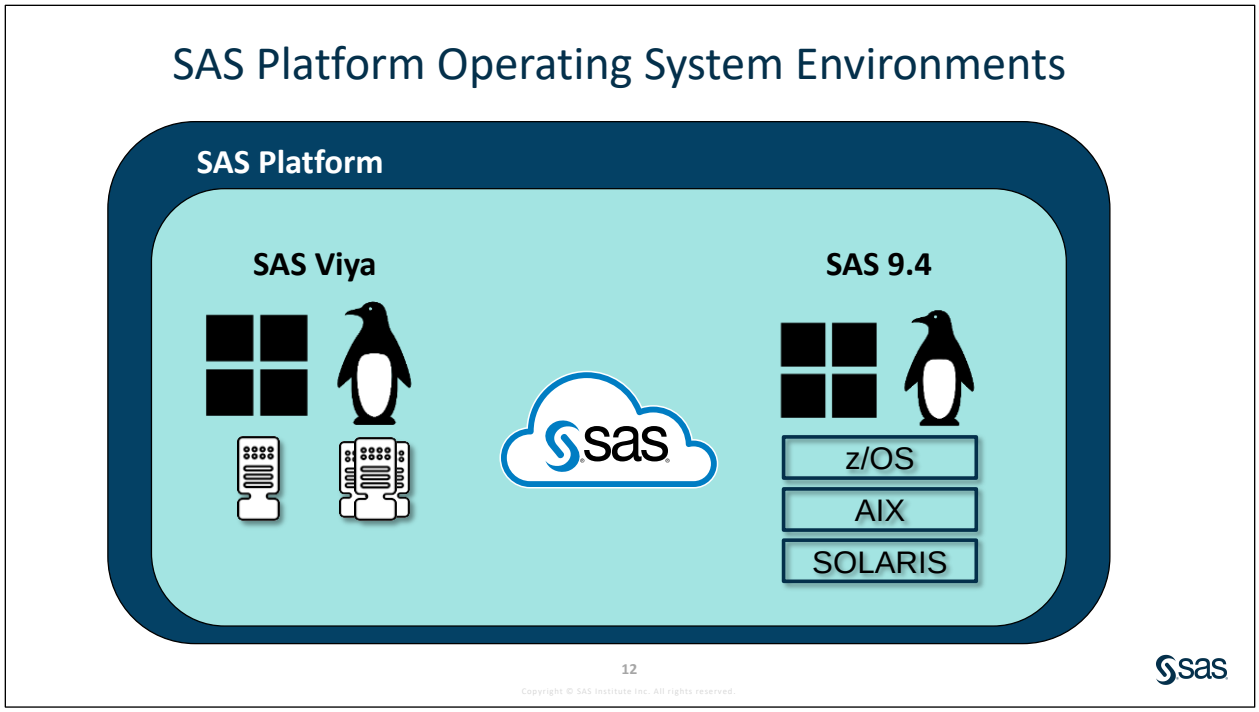
Cloud Analytics Server: SAS Viya technology enters the SAS Platform with Cloud Analytics Services, or CAS. This too is an in-memory server with data retention in-memory and data retention across actions. Parallel data loading is available through CAS, which allows for parallel data loading from Hadoop nodes or Teradata nodes to the CAS worker nodes. If a CAS worker node goes down, other nodes are present to continue the processing seamlessly. CAS is open to other languages such as Python. It is dynamically scalable; you can add nodes to it without bringing the server down to reconfigure. Shared libraries are unique to CAS in which users can access the same data tables in-memory. They do not need their own copies of the data, which saves memory.

SAS Grid Computing and CAS: SAS Grid Computing is a distributed architecture as well. It plays an important role in both SAS®9 and SAS Viya deployment. SAS Grid Computing processes data residing on disk. A grid manager handles workload management to ensure that processing is completed in a timely manner. Entire jobs can be executed in the grid, or independent steps can be executed in parallel to decrease run time. SAS Grid Computing and SAS Viya give you both dimensions of parallelization. Actions are distributed to process in-memory data in SAS Viya, and jobs are distributed to nodes to process shared data residing on disk in SAS Grid Computing.

Perhaps the most significant core platform functional difference between SAS 9.4 and SAS Viya is in the way that each handles the distributed processing. SAS Viya leverages the CAS server, and SAS 9.4 uses SAS LASR, which is a high-performance architecture (HPA), or SAS Grid Manager. Even though SAS LASR and HPA will remain as SAS 9.4 approaches, SAS Grid Manager will eventually be available natively in SAS Viya environments. Because the CAS server is the third major evolution of the SAS distributed, in-memory technology, it's no surprise that it offers the most value. Compared to HPA, it performs better because it can retain data from one action to the next action rather than having to reload the same data from disk for each action. In comparison to both HPA and SAS LASR, the CAS server offers dynamic scalability, a virtual memory footprint, high availability, parallel data loading, shared library access, and integration with open source languages and REST APIs. SAS Grid Manager can work in concert with a SAS Viya environment. Even though "the grid" distributes multiple SAS 9.4 jobs from multiple users across a cluster of machines, each job can be parallelized with the DATA step and SAS procedure code that executes across multiple worker nodes in a CAS server that runs in a companion SAS Viya environment.



One of the supporting services of SAS Viya is the SAS Cloud Analytics Services, or CAS. Cloud Analytic Services (CAS) is an in-memory, distributed, analytics engine.
It uses scalable, high-performance, multi-threaded algorithms to rapidly perform analytical processing on in-memory data of any size.

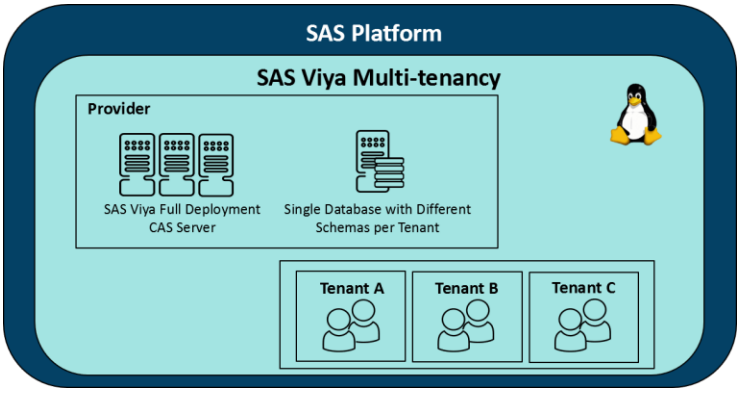


SAS Viya and the SAS 9.4 Business Intelligence Platform can both be installed on Windows and Linux environments. SAS 9.4 can also be deployed on other operating systems (Solaris, AIX, and z/OS, for example). These systems can be either on-premises or in the cloud.

As of SAS Viya 3.4 or later, single machine on 64-bit Microsoft Windows Server is supported.

For more information about operating system support, see the Extended Learning page.

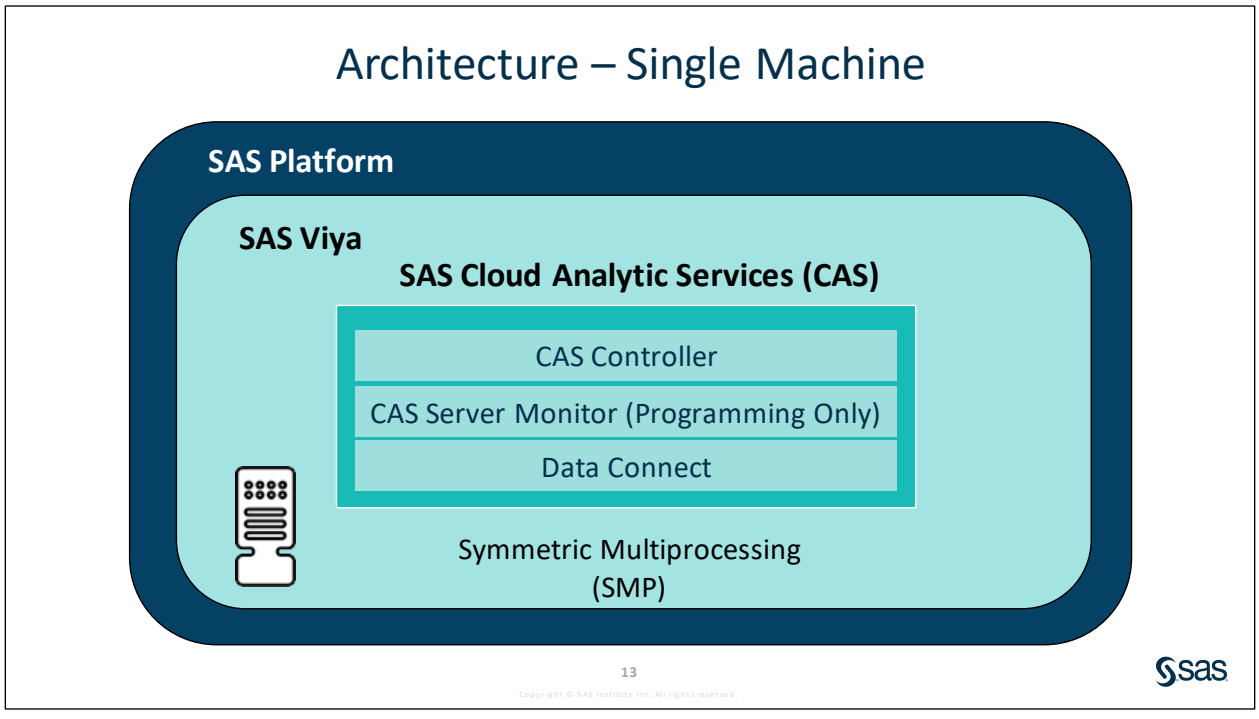
SAS Viya Multi-tenancy



SAS Viya supports a multi-tenant environment where a single instance of the software can serve multiple tenants. If you opt for multi-tenancy, you must enable it during the initial deployment. If you enable multi-tenancy, a provider is created during deployment and the provider has the ability to manage isolated, independent ***tenants*** within a single deployment. After deployment, you can onboard additional tenants. Each tenant has access to the licensed software but has no visibility into the data and workflows of other tenants.

You cannot retrofit multi-tenancy in an environment where multi-tenancy was not enabled in the initial deployment.

Note: Multi-tenancy is supported only for Linux.

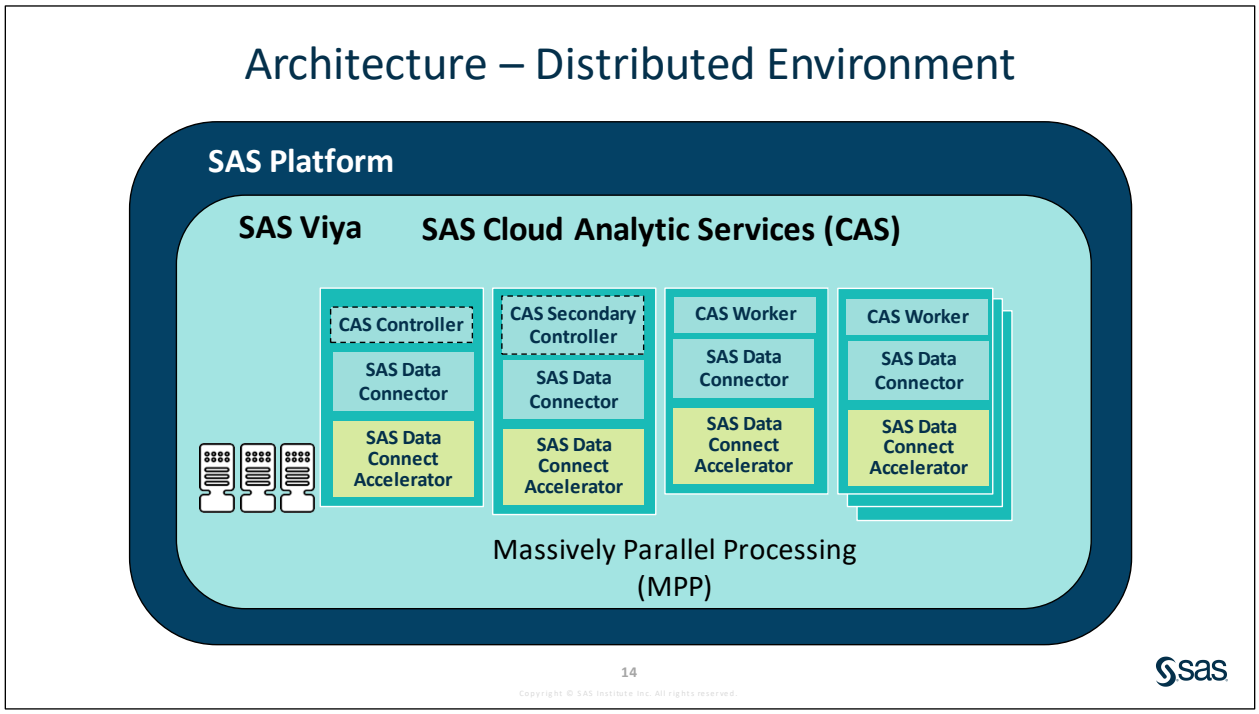


In a single-machine architecture, the CAS controller services requests and acts as a controller. The controller node performs data analysis on the rows of data that are in-memory.

A SAS Data Connector is used to configure connections to data sources such as existing SAS data, Teradata databases, and Hive data in Hadoop.

- The single machine uses the available CPUs and threads of the system to speed up data analysis.
- All the in-memory analytic features of a distributed server are available to the single-machine server.
- Single-machine servers cannot load data into memory in parallel.

CAS Server Monitor is available only in a programming only deployment.



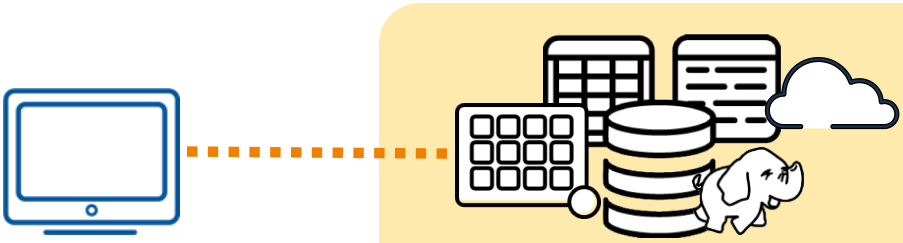
The distributed server consists of one controller, an optional backup controller, and one or more workers.

When a CAS server is running in massively parallel processing (MPP) mode, in addition to a controller, the CAS server also assigns multiple machines as CAS workers. The controller parcels out work to each worker node. The worker nodes perform coordinated parallel processing of the distributed data and generate results that are sent back to the controller. Each of the CAS nodes has a SAS Data Connector that provides connectivity to data sources. In addition, the SAS Data Connect Accelerator allows for embedded processes to run in data sources like Hadoop.

CAS has a communications layer that supports fault tolerance, so when CAS is running in an MPP configuration, it can continue processing requests even after losing connectivity to some nodes. This communication layer also enables you to remove or add nodes while the server is running. Also, if the CAS controller machine goes down, you can configure an optional backup controller in an MPP environment.

For both architectures, the server is multi-threaded for high-performance analytics.

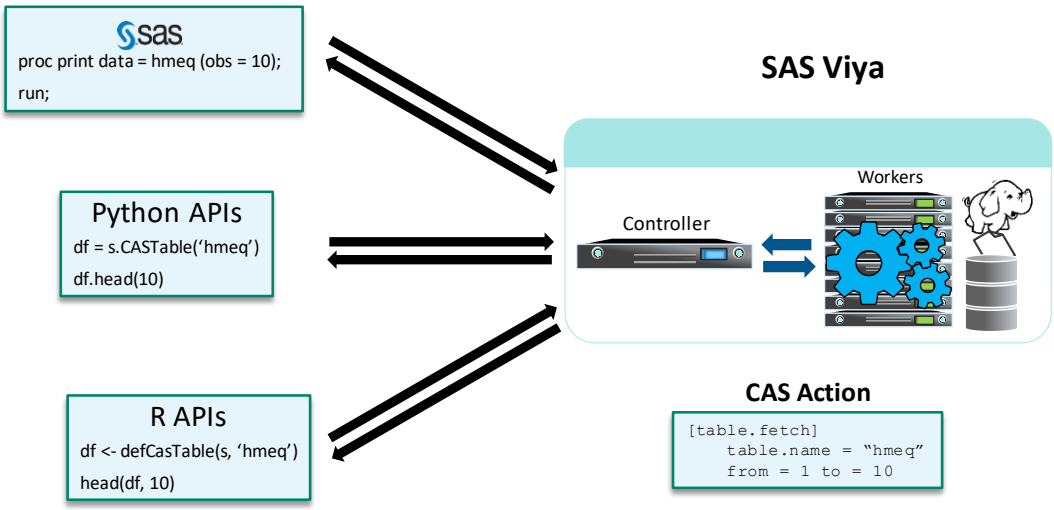
Data Sources That You Can Access with SAS Viya



- on-premises or in the cloud
- relational and unstructured
- XML, JSON, CSV, XLSX...
- SAS data sets and SASHDAT files

15

Interfaces to SAS Viya

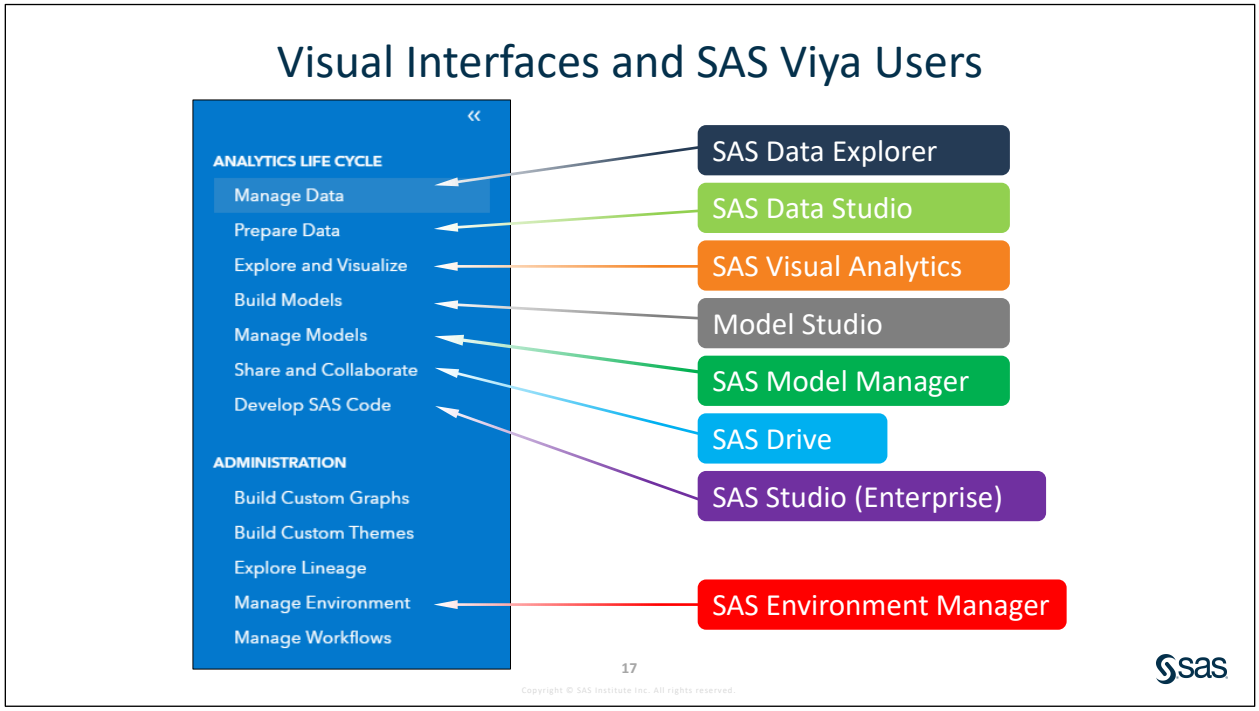


16

The Scripting Wrapper for Analytics Transfer (SWAT) enables open source software such as Python, Lua, and R to run data analysis on the CAS server. For Java, classes are provided to enable connections to the server, and other classes are provided to run data analysis.

Regardless of the language in which the API call is issued, the underlying CAS action submitted to the CAS server is the same. For example, if you wanted to print the first ten observations of your CAS table, you would use the PRINT procedure in SAS, the head method in Python, and the head function in R.

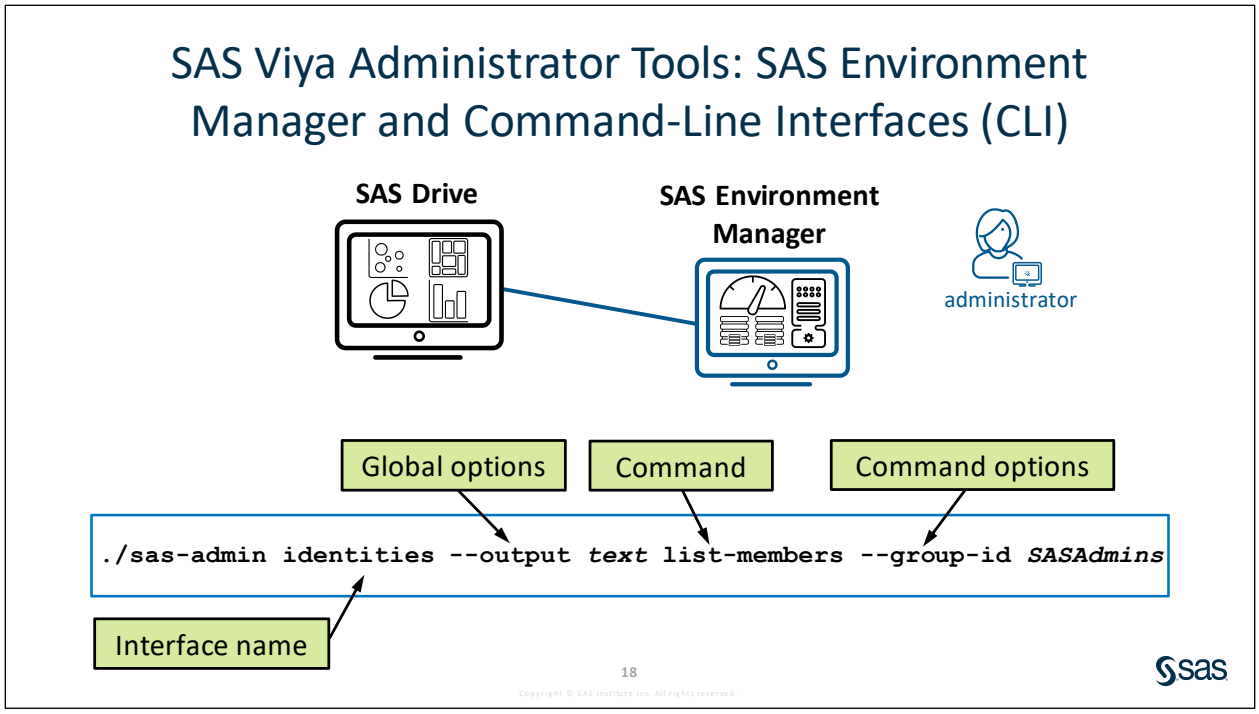
For more information about SWAT and interfaces to SAS Viya, see the Extended Learning page.



Users can access visual interfaces from SAS Drive, the hub for SAS Viya applications.

Actions	Applications
Develop SAS Code	SAS Studio (Enterprise)
Prepare Data	SAS Data Studio
Explore and Visualize Data	SAS Visual Analytics
Build Models	Model Studio
Manage Data	SAS Data Explorer
Manage Models	SAS Model Manager
Explore Lineage	SAS Lineage Viewer
Manage Environment	Environment Manager

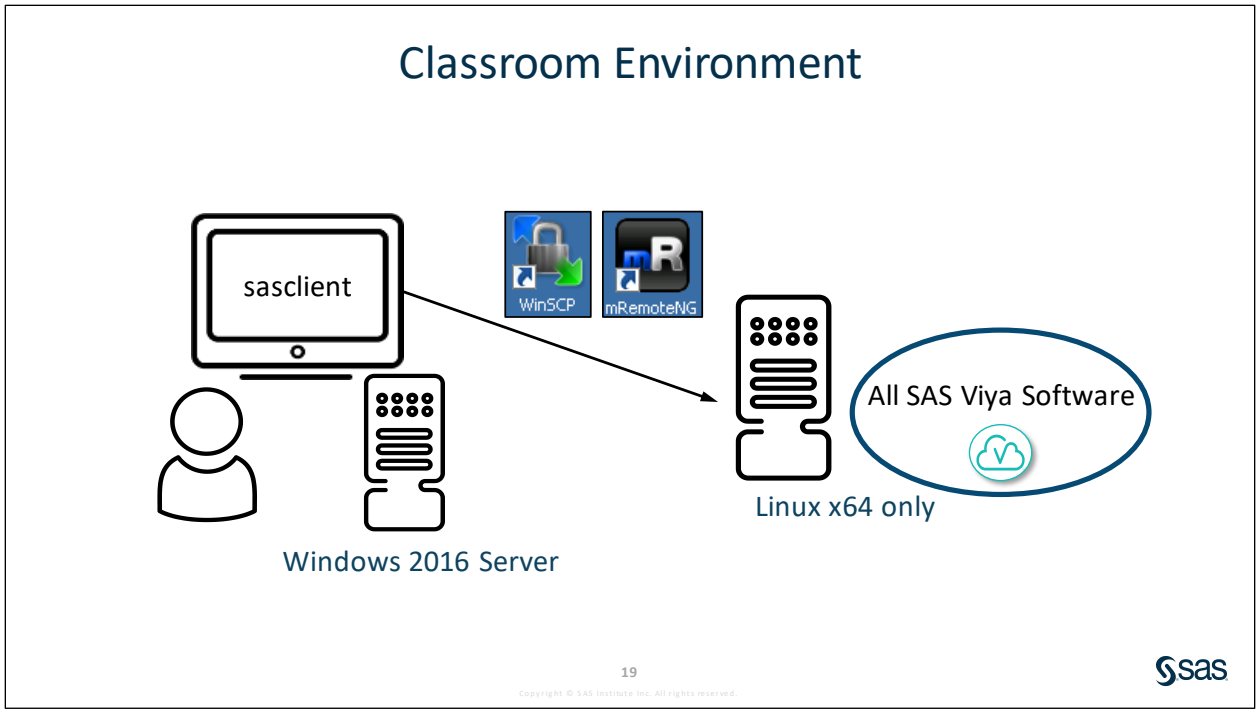
The above chart lists a few actions in SAS Drive that are used to access their respective applications. For example, selecting ***Develop SAS Code*** from SAS Drive will take you to SAS Studio (Enterprise).



Command-line interface (CLI) is a user interface to the SAS Viya REST services. You enter commands on a command line and receive a response from the system.

You can schedule scripts that use commands for nightly activities or repetitive jobs. The following activities are examples:

- From CAS, unload tables that were not accessed during the last week.
- Create a new project folder structure and apply permission rules.



For demonstrations and practices in this course, a single-machine deployment is used. The architectural view of your single-machine demonstration environment is shown above. The CAS controller, SAS products, and embedded web application server are deployed on a single machine.

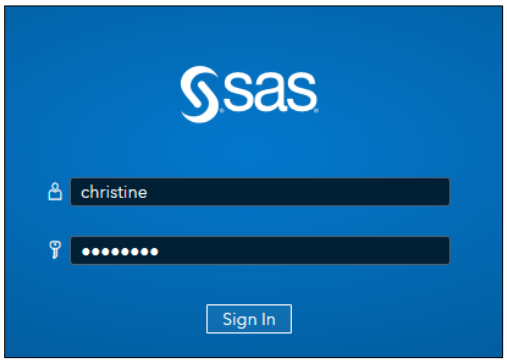
SAS Viya Administration Interfaces

This demonstration introduces SAS Environment Manager, and the Command-Line Interface (CLI) as primary tools for SAS Viya administrator to manage and monitor a SAS Viya deployment.

SAS Environment Manager

1. Open a Chrome browser and select **SAS Drive** on Bookmarks toolbar. There is a bookmark for SAS Environment Manager, but the application is also accessible through SAS Drive.

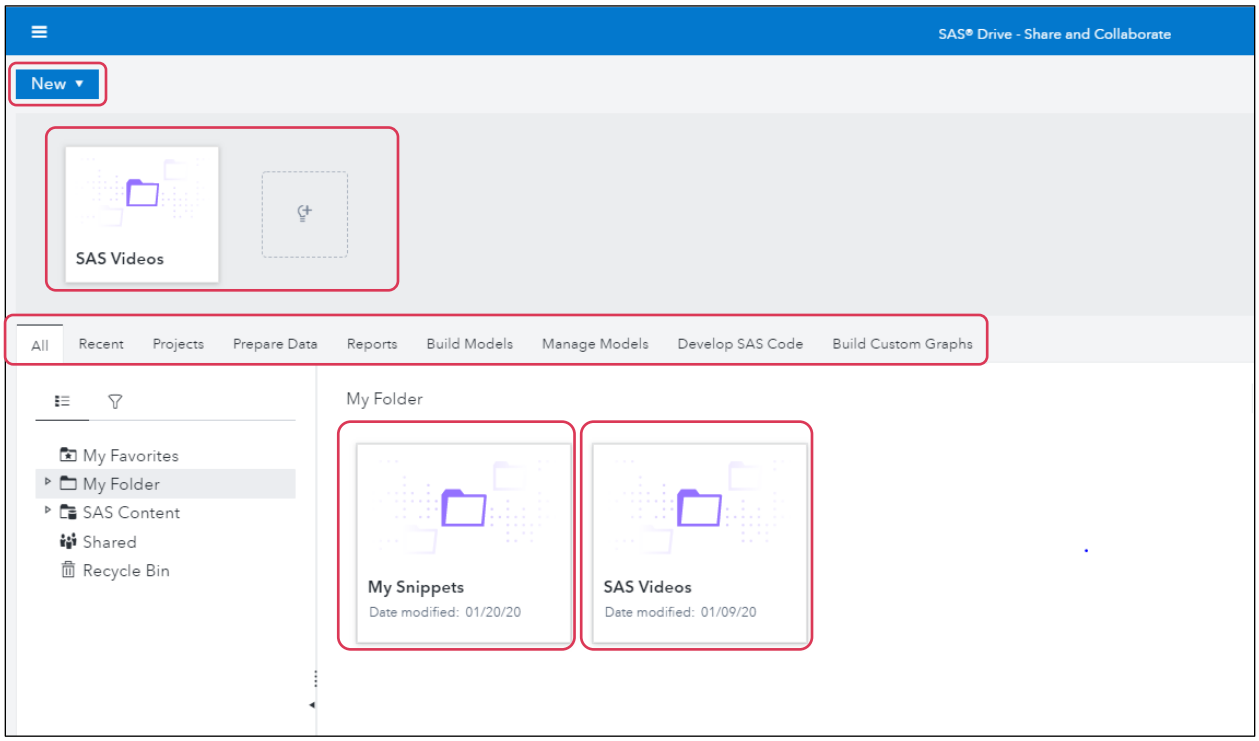
2. Sign in as the user **christine** with the password **Student1**.



3. Click **Yes** to opt in to the SASAdministrators group. Christine is a member of the SASAdministrators group, and by selecting **Yes**, her membership in this group is in effect.

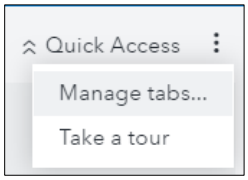
4. On the first logon, SAS Drive is the initial view of SAS Viya. It is a hub for the SAS Viya applications, and enables your users to easily view, organize, and share your content from one place. The availability of features in SAS Drive depends on the applications that have been installed, and the features and permissions that have been specified by the administrator.

There are tabs across the page and a displayed canvas for each tab, a quick access area that currently has short videos to view on a product or application, and a new item button with drop-down menu.

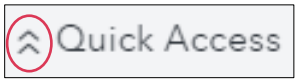


Icon	Name	Description
	Applications menu	Enables you to access other applications
	New Item button	Enables you to create new objects
	Quick Access	Area to store your most-used items
	Folders and Filter	Access your folders or filter the folder list
	Undo and Redo	Undo or redo previous actions
Recent items	Recent Items	Displays the recent objects that have been accessed
	Notifications	Displays the number of notifications that you have
Help Center	Help	Access online Help
	Menu	Enables you to manage your tabs, and take a tour
	Summary	Displays summary or detailed information about the item type, date created, date modified, with whom the item is shared, and any assigned tags
	Comments	Enables you to add comments and attachments to an item

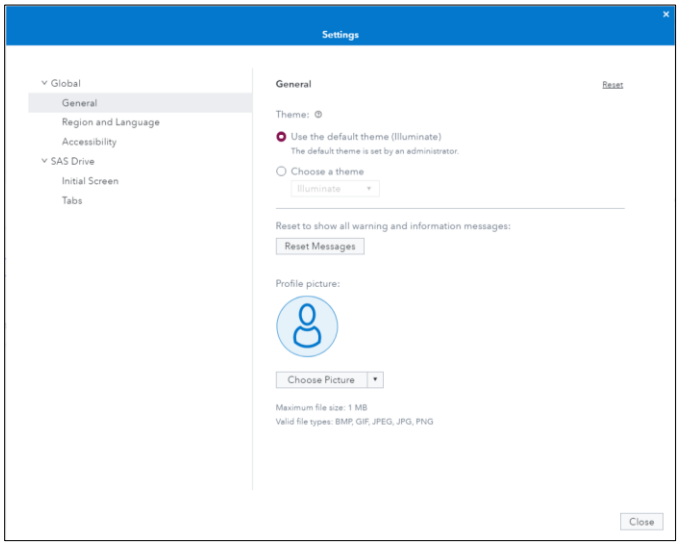
5. Click ⋮ (**Menu**) and select **Manage tabs** in the upper right corner. You can modify here the tabs that you want to be available.



6. Click ⌃⌃ in the top right corner to hide Quick Access.



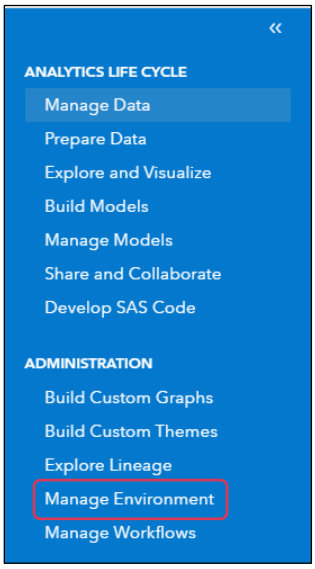
7. Click the user profile ⓒ ⇨ **Settings**. You can also manage tabs here as well, and other global settings.



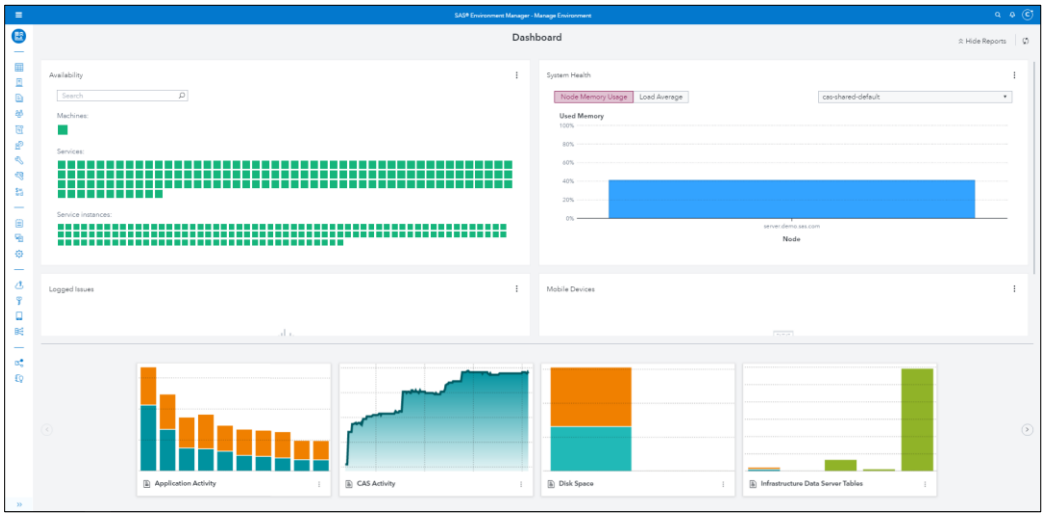
8. Click **Close** ✕.

9. To access SAS Environment Manager, click ☰ **Show application menu** in the upper left corner to view the available applications.

10. Select **Manage Environment**.



11. The dashboard provides a quick overall look of your environment's health and status. It also contains detailed views that enable you to examine and manage your environment in detail.



By default, the dashboard displays these tiles:

- *Availability* displays grids of color-coded boxes that correspond to the machines, services, and service instances in your environment.
- *System Health* displays graphs that give you a quick view of the state of the nodes (machines) in your SAS Viya cluster for the selected CAS server.

  The *Node Memory Usage* graph displays the host memory usage for each node. The *Load Average* graph displays the one-minute load average over the past five minutes for the nodes in a cluster.
- *Logged Issues* displays a time series graph of the number of ERROR and FATAL level log messages that were captured by SAS Viya log files during the previous 30 minutes.
- *Mobile Devices* displays the type of mobile device access control that is in use and the number of successful and unsuccessful logon attempts.

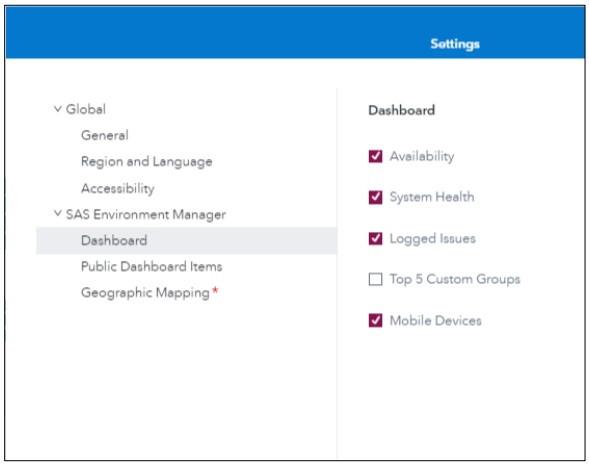
The dashboard is customizable.

12. Several management reports are provided by SAS and are available on the SAS Environment Manager Dashboard. They are accessed by clicking **Show Reports** at the top right of SAS Environment Manager.

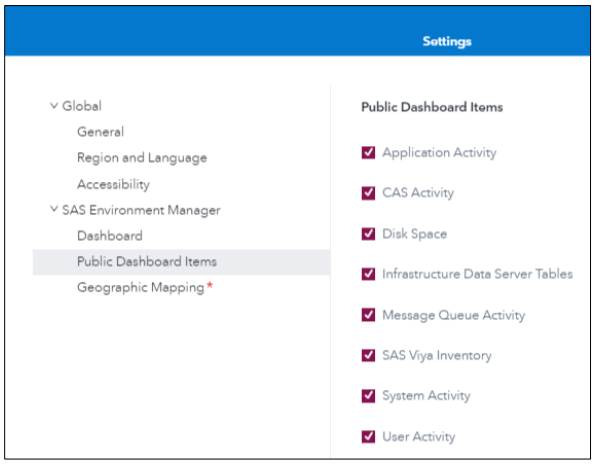
Reports are available for the following items:

- Application Activity
- CAS Activity
- Disk Space
- Infrastructure Data Server Tables
- Message Queue Activity
- System Activity
- User Activity

13. You can personalize your dashboard by selecting **Christine's Profile** ⇨ **Settings** ⇨ **Dashboard**.



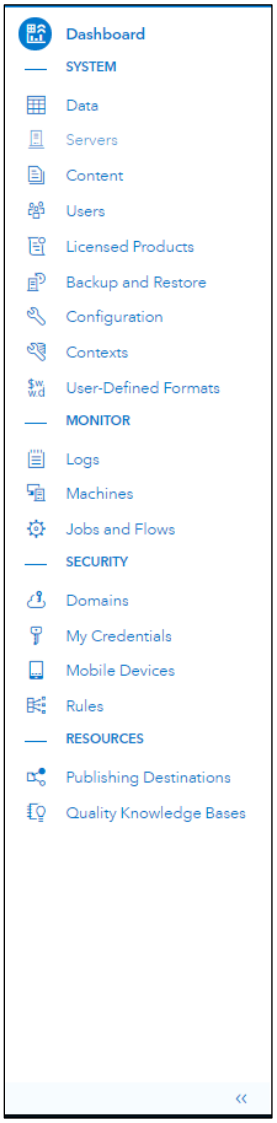
14. You choose which status reports to display on the dashboard by selecting **Public Dashboard Items**. (These reports are available to all SAS administrators.)



You can choose which reports to display on your personal dashboard, and you can add a new or modified report to **/SAS Content/<Username>/Application Data/SAS Environment Manager/Dashboard Items.**

Similarly, new or modified reports be surfaced to all users by placing the report in the folder **/SAS Content/Products/SAS Environment Manager/Dashboard Items**.

15. Because I logged on as a SAS administrator, I am able to access all pages of SAS Environment Manager from the navigation bar. You can extend the view to see not only the icons but also the page name. Click » at the bottom of the menu. Throughout class, we use these pages to manage our environment.



16. Click Content.

17. Navigate to **SAS Content ⇨ Products ⇨ SAS Environment Manager ⇨ Dashboard Items**.

Note: Subsequent logons will return you to the last location where you were working.

Application pages to manage these areas of your environment:

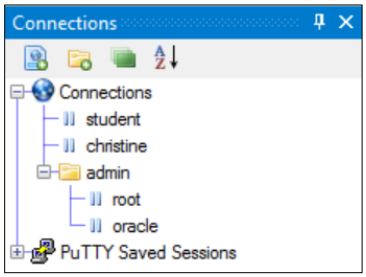
Data	CAS tables, caslibs, other data sources
Servers	Configuration and information for CAS servers and launcher servers
User content	Saved reports and data, favorites, and history
User Information	Users and groups from your directory service and SAS groups
License information	SAS licenses and expiration dates
System backups	Backups and restores of system data
Configuration	Configuration data for SAS Viya microservices
Contexts	Values such as environment variables and port ranges that are used when launching a process
User-defined formats	User-defined data formats and format libraries
Logs	Log messages from SAS applications and services
Machines	Information and metric data for the machines and services
Jobs	Monitoring of current and past jobs and schedules for jobs
Domains	Authentication domains (for storing a user ID and password), encryption domains (for storing an encryption key), and connection domains (for storing a user ID without a password)

Credentials	Personal credentials for the authenticated user across authentication and connection domains
Mobile device access	Lists that allow or prevent access to the system by specific mobile devices
Rules	Access controls and rules that control who can access resources and content in your system
Quality Knowledge Bases	Collections of files that store data and the logic that defines data quality operations such as parsing, standardization, and matching (available only if SAS Data Quality is installed)
Publishing Destinations	Destinations for publishing decisions, models, and rule sets from SAS applications (available only if SAS Model Manager, SAS Decision Manager, or Model Studio is installed)
Tenants	Information about tenants and status of tenant services (available only in a multi-tenant environment and only to provider administrators)

Command-Line Interface (CLI)

1. Open **mRemoteNG** by double-clicking the icon on the desktop.

2. Open the **christine** connection in the mRemoteNG connections list.



3. The CLI facility is found in the SAS Viya **home/bin** directory. Navigate to **/opt/sas/viya/home/bin**.

```
cd /opt/sas/viya/home/bin
```

4. You must complete the required preliminary tasks before you use the CLI.
   a. If your environment is enabled for Transport Layer Security (TLS), you must set the **SSL_CERT_FILE** environment variable to the path location of the **trustedcerts.pem** file (if using the SAS default truststore), or the path location of your organization's certificate (if using an internal truststore).

      The classroom environment is not enabled for TLS. However, let's go through the step to set SSL_CERT_FILE to the default location of the trustedcerts.pem file.

1) Issue the following command: **export SSL_CERT_FILE=/opt/sas/viya/config/etc/SASSecurityCertificateFramework/cacerts/trustedcerts.pem**.

```
export
SSL_CERT_FILE=/opt/sas/viya/config/etc/SASSecurityCertificateFramework/cacerts/trustedcerts.pem
```

b. Create at least one profile for the environment that you want to use. You can create a default (unnamed) profile or a named profile, such as **sas-admin -- profile <profilename> init** (where **<profilename>** is the name of the profile).

1) Issue the following command: **./sas-admin profile init**

```
./sas-admin profile init
```

2) Enter the configuration options:

Service Endpoint: **http://server** (https://<*host_path*>:443 is standard)

Output type (text|json|fulljson): **json**

Enable ANSI colored output (y/n)?: **n**

A message like the following is sent to indicate the successful creation of the profile:

Saved 'Default' profile to /home/christine/.sas/config.json.

c. Initiate the sign-in process by using the **sas-admin** command: **./sas-admin auth login**

The default profile is used.

```
./sas-admin auth login
```

Enter the credentials for Christine: **christine** and **Student1**

Note: By default, your authentication remains active for 12 hours. You can use the **auth logout** command to sign out.

5. Issue the following command to obtain help using the CLI:

./sas-admin help

```
./sas-admin help
```

```
NAME:
   sas-admin - SAS Administrative Command Line Interface

USAGE:
   sas-admin [global options] command [command options] [arguments...]

VERSION:
   1.1.11

COMMANDS:
   authenticate, auth, authn    Handles authentication to the target e
nvironment.
   help, h                      Shows a list of commands or help for o
ne command.
   plugins                      Manages plugins.
   profile, prof                Shows and updates options.
```

6. Use the CLI to verify the valid users of the environment:

   ./sas-admin identities –help

   Use the **list-users** option:

   ./sas-admin identities list-users

```
./sas-admin identities list-users
```

End of Demonstration

Practice

1. Exploring the SAS Environment Manager Dashboard

a. Connect to your Windows client machine.

Classroom Course	Live Web Course
Use a remote desktop connection with the IP address that is given to you by the instructor. Sign in with these credentials: User: **Student** Password: **Metadata0**	Use the URL in step 6 of the email that you received from Live Web Administration.

b. Open a Chrome browser window and select **SAS Drive** on the Bookmarks toolbar.

c. Sign in as the user **christine** with a password of **Student1**. Click **Yes** to opt in to the SASAdministrators group.

d. To access SAS Environment Manager, click the applications menu in the upper left and select **Manage Environment**.

(There is a bookmark for SAS Environment Manager if you want to go directly to the interface.)

e. Select **Show Reports** on the top right portion of the SAS Environment Manager dashboard.

f. On the Disk Space report, select the **More Options** menu and select **Open**.

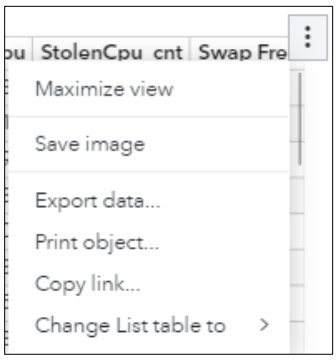
g. Select the Storage Dashboard. What is the percentage of free space on the machine?

h. Select **Manage Environment** from the side menu to return to SAS Environment Manager.

i. Open the **System Activity** Report. (Click the **More Options** icon ⇨ the three vertical black dots ⇨ **Open**.)

j. Click the **System Details** tab.

k. View your options by clicking the three vertical black dots that appear when you place your pointer in the upper right corner of the data.



l. Choose **Export data**.

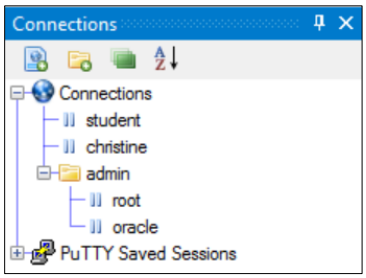
m. Keep all default columns and click **OK**.

n. This is downloaded to the Downloads directory as an MS Excel file by default. You can click **List Table – ServerT….xlsx** in the lower left corner to open the file.

2. Introducing the Administrative Command Line Interface

a. Open **mRemoteNG** by double-clicking the icon on the desktop.

b. Open the **christine** connection in the mRemoteNG connections list.



c. Navigate to **/opt/sas/viya/home/bin**.

```
cd /opt/sas/viya/home/bin
```

d. You must complete the required preliminary tasks before you use the CLI.

The classroom environment is not enabled for Transport Layer Security (TLS). However, go through the step to set SSL_CERT_FILE to the default location of the **trustedcerts.pem** file.

1) Issue the following command: **export SSL_CERT_FILE=/opt/sas/viya/config/etc/SASSecurityCertificateFramework/cacerts/trustedcerts.pem**.

```
export
SSL_CERT_FILE=/opt/sas/viya/config/etc/SASSecurityCertificateFramework/cacerts/trustedcerts.pem
```

2) Issue the following command: ./**sas-admin profile init**

```
./sas-admin profile init
```

Enter the configuration options:

Service Endpoint: **http://server** (https://<*host_path*>:443 is standard)

Output type (text|json|fulljson): **json**

Enable ANSI colored output (y/n)?: **n**

3) Initiate the sign-in process by using the **sas-admin** command: **./sas-admin auth login**

```
./sas-admin auth login
```

Enter the credentials for Christine: **christine** and **Student1**

Note: By default, your authentication remains active for 12 hours. You can use the **auth logout** command to sign out.

e. Issue the following command to obtain help using the CLI: **./sas-admin help**

```
./sas-admin help
```

f. Use the CLI to view the users and groups in your SAS Viya environment. How many users are there? Hint: Use the identities plug-in.

How many members are in the SAS Administrators group?

See the solution for command scripts.

3. (Optional) Changing the Default Expiration for the CLI Token

You can change the default expiration for all tokens issued by the system.

a. Sign in to SAS Environment Manager as **christine** and password **Student1**. Assume the SASAdministrator role.

b. Select **Configuration** area ⇨ **All services** from the **View** drop-down menu.

c. Select **SAS Logon Manager**.

d. Click **New Configuration** ⇨ **sas.logon.jwt**.

e. The default time-out for the access token is 12 hours, and it is displayed in seconds for the following attributes:

policy.accessTokenValiditySeconds

policy.global.accessTokenValiditySeconds

Change the values to **172800** for a time-out of 48 hours.

f. Click **Save**.

g. Restart the SASLogon service for the changes to be applied.

```
sudo systemctl restart sas-viya-saslogon-default
```

4. Reviewing Product License Information in SAS Environment Manager

Explore license information through SAS Environment Manager.

If you are not already in SAS Environment Manager, open SAS Drive and sign in as the user **christine** with a password of **Student1**. Click **Yes** to opt in to the SASAdministrators group, and click **Manage Environment** from the drop-down side menu.

a. Click **Licensed Products** from the left navigation menu.

Note: The Licensed Products page is an advanced interface. It is available only to SAS administrators.

b. How many products are licensed?

Hint: Look for the number in parentheses at the top of the window.

c. Examine the **Status** column by scrolling through the list.

Are any of the products expired or about to expire?

Use the table below to help determine the effective license status of each product.

For each product, the following icons depict the effective license status:
The SAS license is current.
The SAS license is due for renewal (grace period). The grace period is a predetermined range of days immediately after the license expiration date. For example, if the expiration date is 30 June, the grace period might extend 45 days: from 1 July - 14 August.
The SAS license is about to expire (warning period). The warning period is a predetermined range of days that follows the grace period. For example, if the expiration date is 30 June, the warning period might extend 56 days: from 15 August - 09 October.
The SAS license has expired. License expiration occurs immediately after the warning period ends. An expired license means that SAS does not run. For example, if the warning period ends on 09 October, SAS stops running at 12:00 a.m. on 10 October.

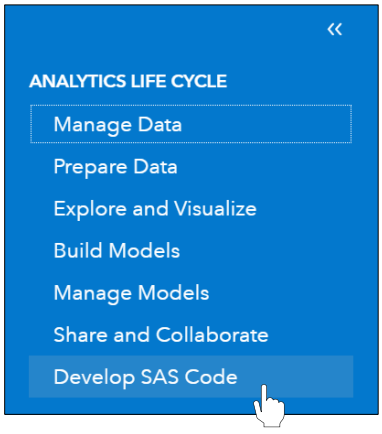
d. Examine the **Status** section of the filters on the left side of the window. Does the number next to **License is current** match the number from step **b**?

e. In the Product section of the filters, enter **Visual** in the field and click **Enter**. How many products that contain the string *Visual* are licensed?

f. Click **Reset** in the Product filter to remove **Visual**, enter **Data Connector** and click **Enter**. How many Data Connector licenses exist?

5. Viewing License information using SAS Studio

a. From SAS Environment Manager, click the applications menu in the upper left and select **Develop SAS Code**.



You can also access SAS Studio by entering the appropriate URL:
http://*server*/SASStudioV

b. Create a new SAS program, and enter the following command:

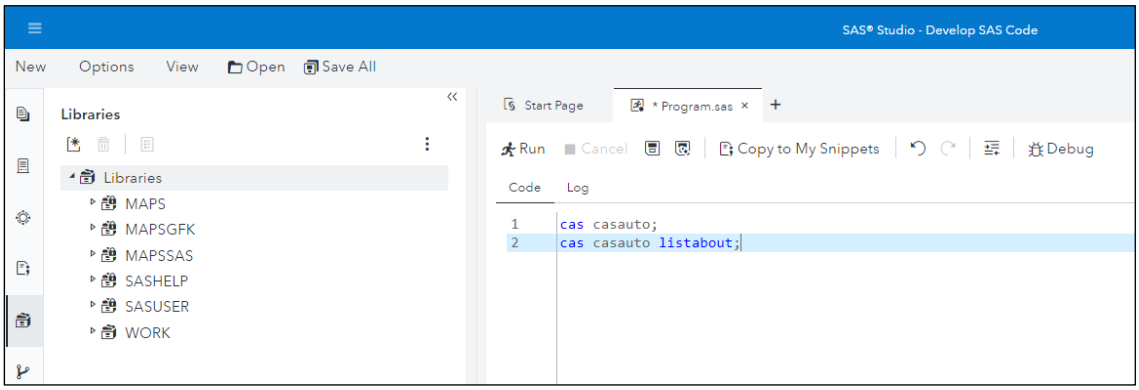
```
proc setinit; run;
```

c. Click the **Run** icon . The log displays the licensed products in this deployment.

There are various methods to get information about CAS and license information for your SAS Viya deployments.

d. Go back to the Code section, delete the PROC SETINIT code, and enter the following code:

```
cas casauto;
cas casauto listabout;
```



e. Click the **Run** icon . The log displays SAS Cloud Analytic Services license information.

6. Using the CLI to Find License Information

Use the command-line interface (CLI) to examine the SAS Viya environment license information.

a. Use the **christine** connection in the **mRemoteNG** connections list.

b. Using the Linux **cd** command, navigate to the bin directory in the SAS Viya Home directory. The sas-admin CLI "host" is found here.

```
cd /opt/sas/viya/home/bin
```

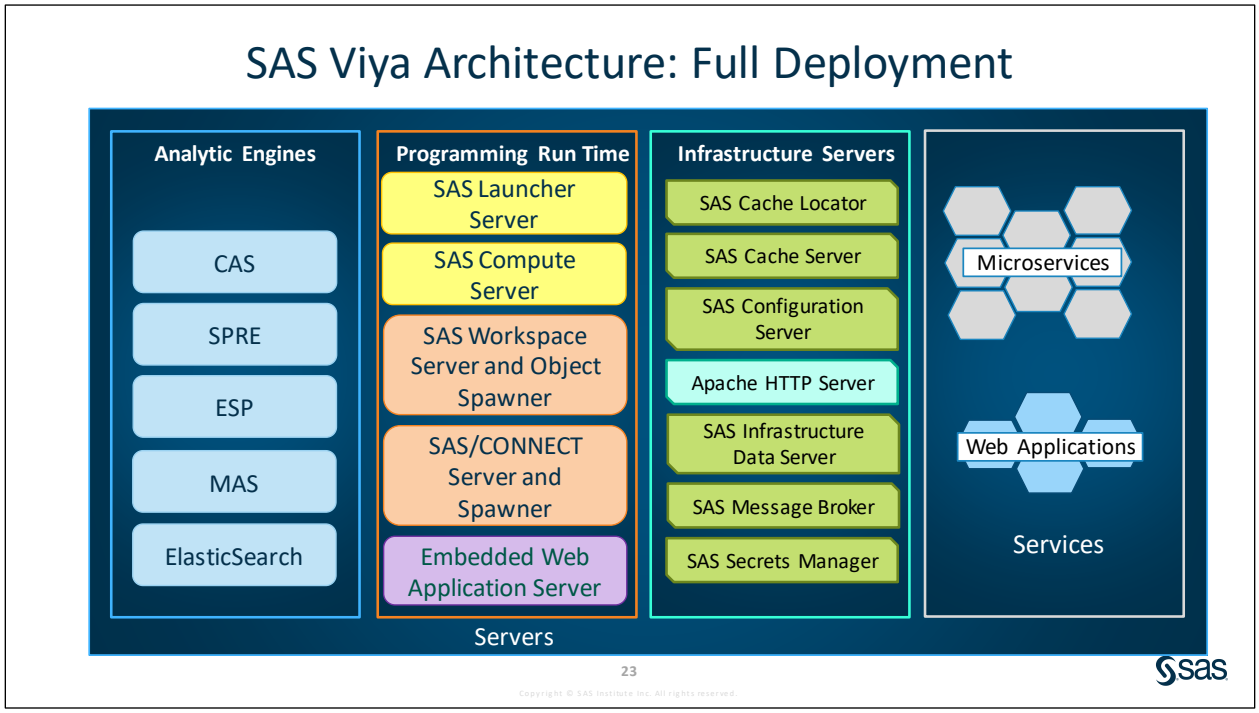
c. Issue the following command:

```
./sas-admin licenses count
```

Does the CLI output agree with the SAS Environment Manager on the number of licensed products?

End of Practices

1.2 SAS Viya Architecture

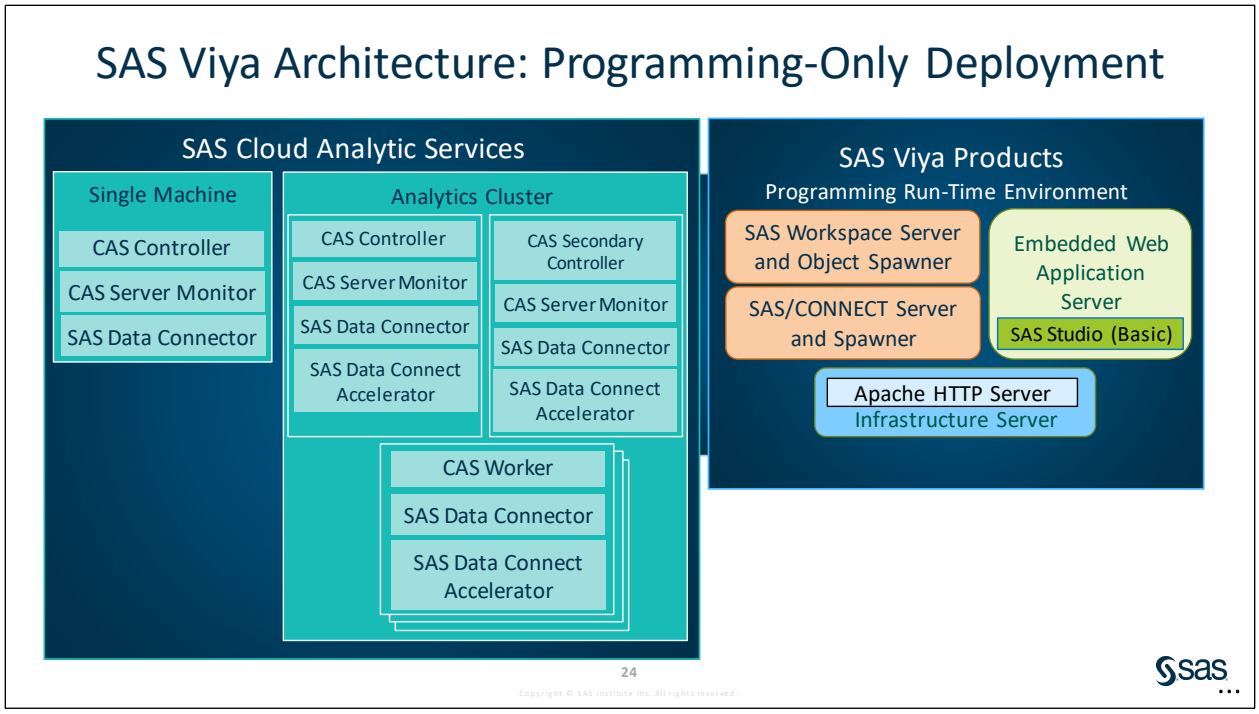


SAS Viya contains several servers and services in a full deployment and are usually distributed across multiple physical machines. This is a default type of deployment.

- SAS Cloud Analytic Services – CAS provides the run-time environment for data management and analytics. *Run-time environment* refers to the combination of hardware and software where data management and analytics occur. The server can run on a single machine or as a distributed server on multiple machines.
- Programming run-time servers – These servers provide the necessary components to enable the SAS Studio programming environment to interact with CAS.
- Infrastructure servers – These servers provide essential services to CAS such as a registry of all the services, security certificate management, a database to manage various content, inter-process message management, an HTTP server, and caching.
- Microservices – They are self-contained, lightweight pieces of software that do ***one*** thing and depend on other microservices and processes as little as possible. One or more instances of a microservice can be running. The number of sessions can change as demand changes to provide scalability.

  In a multi-machine deployment, each machine can have its own unique set of running microservices. The set of deployed microservices also depends on the set of products or SAS Solutions that are deployed.

  Because microservices can be duplicated (for high availability), some microservices might be running on more than one machine.



Note: If SAS Drive is available (http://*host*/SASDrive), you do not have a programming-only deployment.

The programming-only deployment type is a convenience for sites that choose to install and use only a subset of the software. The programming-only deployment type does not correspond to a limitation in software licensing or entitlement.

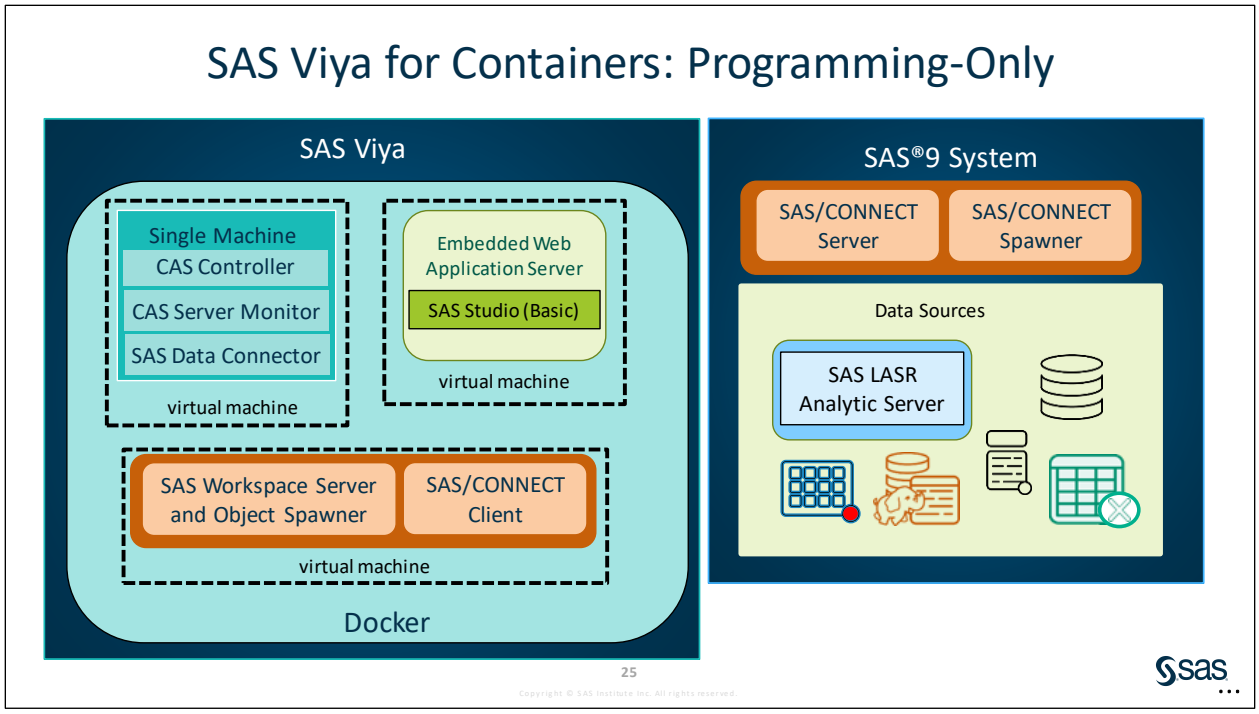
CAS Server Monitor is a web application that you use to monitor your CAS server and to perform some administration tasks in a programming-only deployment.

You must be a member of the CAS (Superuser) role in order to do the following tasks in CAS Server Monitor:

- monitor sessions
- stop the server
- add or remove nodes
- terminate sessions
- designate administrators
- set caslib permissions

The Data Administrator role can also set caslib permissions. This role is applicable only in CAS Server Monitor.

SAS Studio (Basic) is available in the programming-only deployment. The interface is used to submit traditional SAS program code to run-time servers. With SAS Studio (Basic), you access files using the file system and there is no access to SAS content.



SAS Viya for Containers includes a programming-only deployment. A programming-only deployment supports data scientists and programmers who use SAS Studio or direct programming interfaces such as Python, or REST APIs. This type of deployment excludes SAS Drive and the visual interfaces that are accessed through SAS Drive.

- The supported CAS server mode is symmetric multi-processing (SMP).
- Multiple single instances of SAS Viya can be deployed on a single host.
- Hadoop is supported but co-locating the CAS server with Hadoop is not supported.

Refer to the respective Docker or Kubernetes documentation for information about running commands.

Practice

7. Examining the SAS Viya Configuration Directory

In this practice, you examine the SAS Viya configuration directory. Use WinSCP to discover some key locations that are important to administrators in the configuration.

a. Double-click the **WinSCP** icon from the Windows desktop or Windows taskbar.

b. Double-click **sas** in the Login window.

This signs you on to a session with the user ID **sas** on the server machine where SAS Viya is installed. The current directory is **/opt/sas/viya**, which is displayed on the right side of the WinSCP window.

c. Navigate to **/opt/sas/viya/home**.

These are the directories for the SAS Viya binaries. Because this is a single-machine deployment, all SAS binaries are located here.

- An optional product, SAS Event Stream Processing, was installed on this machine.
- The SASSecurityCertificateFramework directory contains security certificate files, the key files, the trustedcerts files, and certificate chain files that are included in each of the directories for the CAS Server.

d. Navigate to **/opt/sas/viya/config/etc**.

The etc directory is where the various SAS Viya servers are configured. You can find configuration files for each server in its associated directory.

- What directory contains the CAS Server?
- What directory contains the SAS Studio web application?
- What directory contains the SAS Object Spawner?

e. Navigate to **/opt/sas/viya/config/etc/cas/default**.

f. Double-click the **casconfig.lua** file.

What is the **deployment_id** of this deployment?

Who is the default CAS Superuser?

What port does the CAS server run on?

g. Navigate to **/opt/sas/viya/config/var/log**.

The log directory is where the logs for the servers and services are located. SAS Viya uses the log4j logging protocol. Log files are organized by product in this log directory. The default system logging location of **/var/log/sas/viya** is a link to this directory.

h. Navigate to the CAS server log directory: **/opt/sas/viya/config/var/log/cas/default**

i. Click the **Changed** column to sort by date so that the most recent CAS server log file is at the top.

Double-click to view it. Most of the messages should be INFO-level messages. Are there WARN- or ERROR-level messages?

8. Using the Command-Line Interface (CLI) to Examine the Environment

a. In mRemoteNg, navigate to **/opt/sas/viya/home/bin**.

The **sas-ops** command is used to run operations infrastructure tasks that will be discussed in a later lesson. It provides information about your SAS Viya environment, including the services, the machines, and the environment.

You must be the SAS install user (sas) to run the command:

```
su sas
```

b. Enter **Student1** for the password.

c. Run the **sas-ops** command with **--help**:

```
./sas-ops --help
```

```
[sas@server bin]$ ./sas-ops --help
NAME:
  sas-ops - SAS Operations command line interface

USAGE:
  sas-ops [global options] command [arguments...]

VERSION:
  1.5.23

COMMANDS:
  alerts          Stream alerts or show the most recent alerts
  datamarts       Display data mart information
  env             Display summary of relevant environment information
  info            Display properties of the components of the deployment
  logs            Streams log events
  metrics         Streams metric events
  notifications   Streams notification events
  notify          Publish a notification message
  services        Lists services, service details, and health
  tasks           Lists tasks defined for sas-ops-agent
  validate        Performs validation of the deployment
  help            Show usage

GLOBAL OPTIONS:
  --colors-enabled    Enable color output (default true)
  --consul address    Consul agent address (http[s]://hostname:port) [$CONSUL_HTTP_ADDR]
  --debug             Enable debug logging
  --insecure          Allow connections to TLS sites without validating the server certificates
  --locale locale     Specify a locale to use (currently 'en-US')
  --token token       Consul ACL token [$CONSUL_TOKEN]
  --token-file file   Path to a file that contains a Consul ACL token [$CONSUL_TOKEN_FILE]
  --version           Display version information

COPYRIGHT:
  Copyright © 2019, SAS Institute Inc., Cary, NC, USA. All Rights Reserved.
```

d. Use the **env** command to view information for the machine.

```
./sas-ops env
```

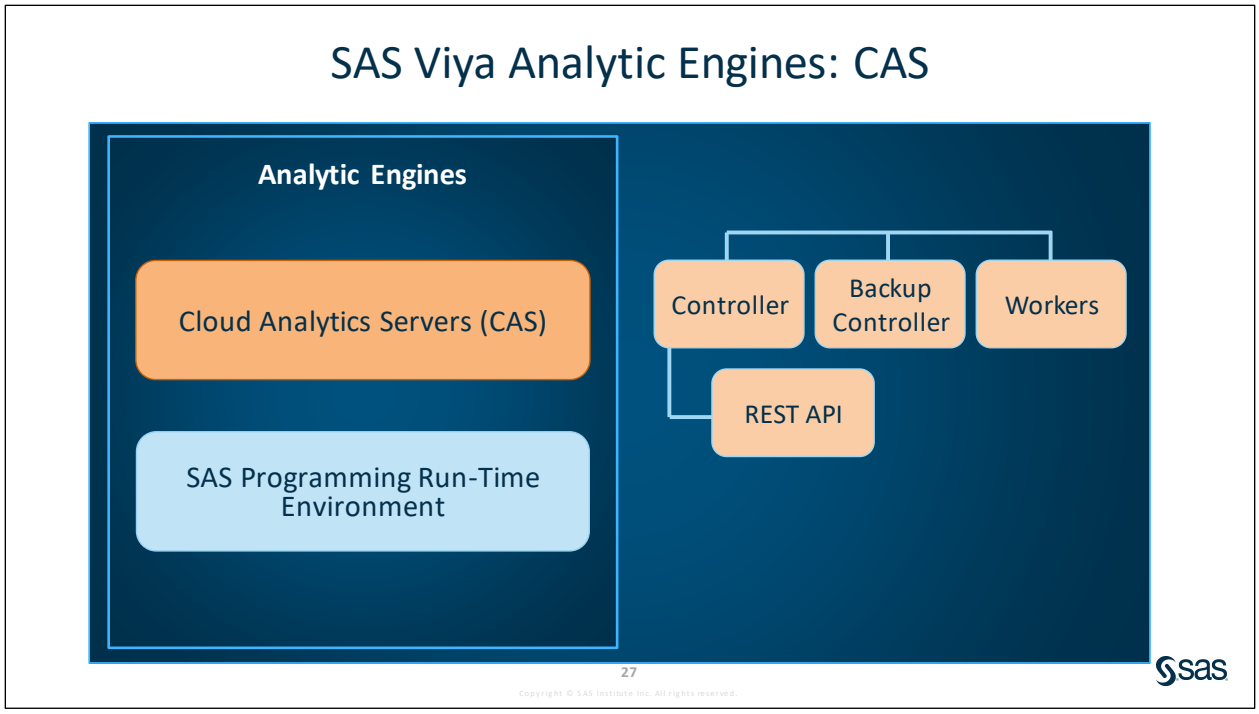
```
[sas@server bin]$ ./sas-ops env
Host Information:
  Full hostname             : server.demo.sas.com
  Short hostname            : server
  Consul node name          : server.demo.sas.com

SAS environment variables:
  CONSUL_CACERT    = /opt/sas/viya/config/etc/SASSecurityCertificateFramework/cacerts/trustedcerts.pem
  CONSUL_HTTP_ADDR = https://localhost:8501

SAS Viya Deployment:
  Site Environment ID       : 4eb436eb-9b86-404d-add8-5e9373803ce5
  Install user              : sas
  Deployment ID             : viya
  Tenant ID                 : provider
  Home directory            : /opt/sas/viya/home
  Config directory          : /opt/sas/viya/config
  Log directory             : /opt/sas/viya/config/var/log
  Temp directory            : /opt/sas/viya/config/var/tmp
  Spool directory           : /opt/sas/viya/config/var/spool
  SAS executable            : /opt/sas/spre/home/SASFoundation/bin/sas_u8
```

e. Use the **info** command to view properties of the components of the machine.

```
./sas-ops info
```

```
[sas@server bin]$ ./sas-ops info
server.demo.sas.com
   common
      architecture : amd64
      boot-time : 2020-01-21T11:32:47.000000-05:00
      hostname-long : server.demo.sas.com
      hostname-short : server
      ip-addrs : 10.242.76.211,10.242.76.211
      last-update : 2020-01-23T02:44:11.656045-05:00
      memory-total : 128668790784
      operating-system : linux
      timezone : EST
      timezone-offset : -05:00
   linux
      kernel-release : 3.10.0-957.27.2.el7.x86_64
      kernel-version : #1 SMP Mon Jul 29 17:46:05 UTC 2019
      operating-system-release : CentOS Linux release 7.6.1810 (Core)
      packages
         sas-aacomp1 : sas-aacomp1-01.20.00-20191104.231512463969.x86_64
         sas-aastatistcs1 : sas-aastatistcs1-03.21.00-20191104.231512427032.x86_64
         sas-accelmva1 : sas-accelmva1-01.20.00-20191104.231512465559.x86_64
```

End of Practices



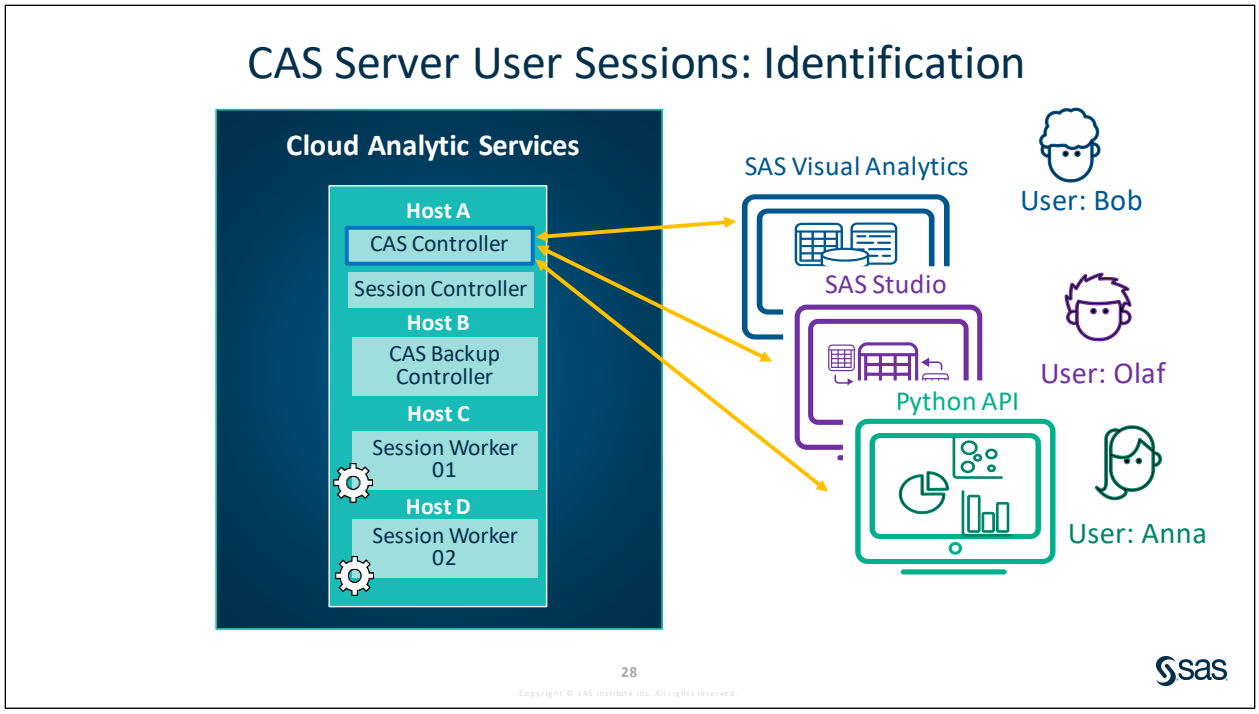
The components that process the data are the analytic engines. Different SAS Viya offerings and solutions can include one or more of these engines.

- The main analytics engine in SAS Viya is called CAS.
- SPRE is the engine that executes SAS Foundation or Base SAS code.

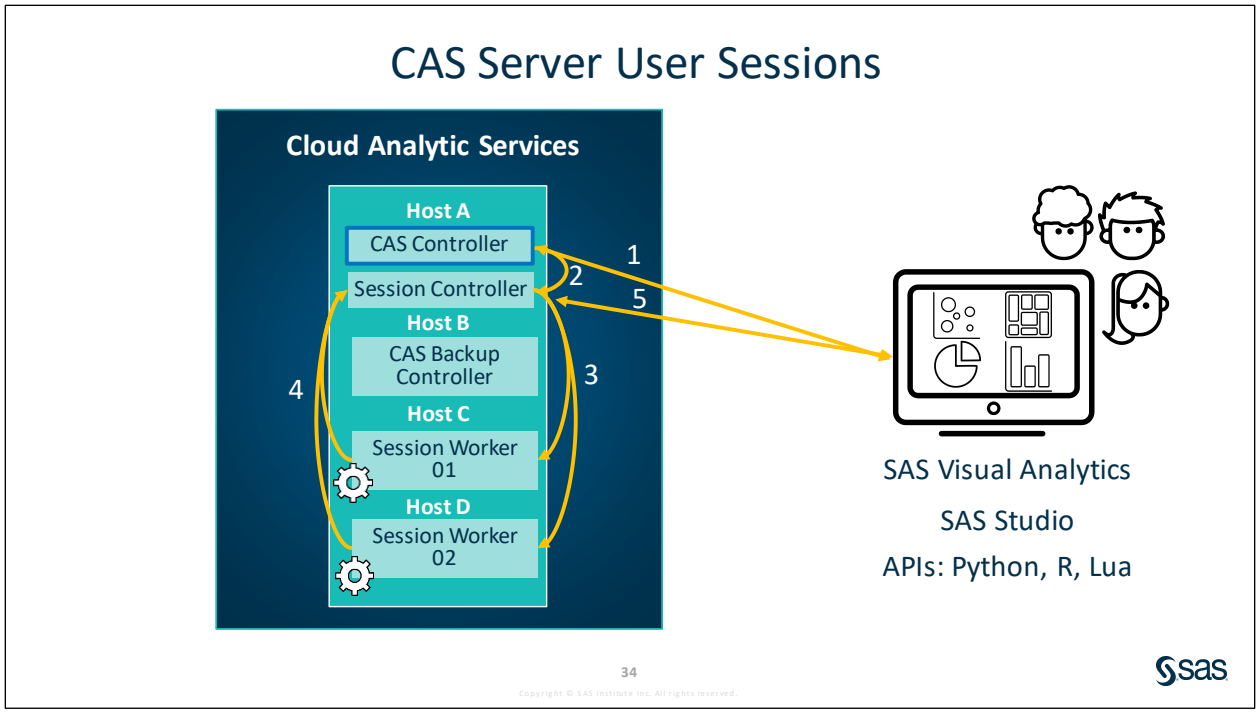
Depending on which solutions are deployed, there might be other analytic engines as well:

- SAS Event Stream Processing analyzes streaming data and takes appropriate action instantly.
- SAS Micro Analytic Service is a memory-resident, high-performance, program-execution service that can run DS2 and Python code. It is included in selected SAS solutions.
- Elastic Search is a third party, open source search and indexing engine. It is included with SAS Visual Investigator.

Analytical teams can use visual, coding, or REST interfaces to make use of these analytic engines.



When you connect to CAS, the server authenticates your user credentials before it creates the session processes. The processes that are created for your session retain your identity and use it to access resources on the server.



Step 1	User connects to CAS server with a client.
Step 2	CAS Controller starts a session controller.
Step 3	Session controller distributes data to worker nodes.
Step 4	Upon completion, results are sent back to the session controller.
Step 5	Client communicates with session controller to receive the results.

CAS Controller

For both server architectures (distributed and single-machine), one machine is assigned the controller role. When the server starts, the controller process is started. This process is sometimes referred to as the *server controller*. The controller accepts connections from clients.

CAS Backup Controller

A SAS Cloud Analytic Services (CAS) backup controller provides fault tolerance for the CAS controller. A backup controller is used only in a distributed server architecture. Deploying a backup controller is optional. CAS supports one backup controller only.

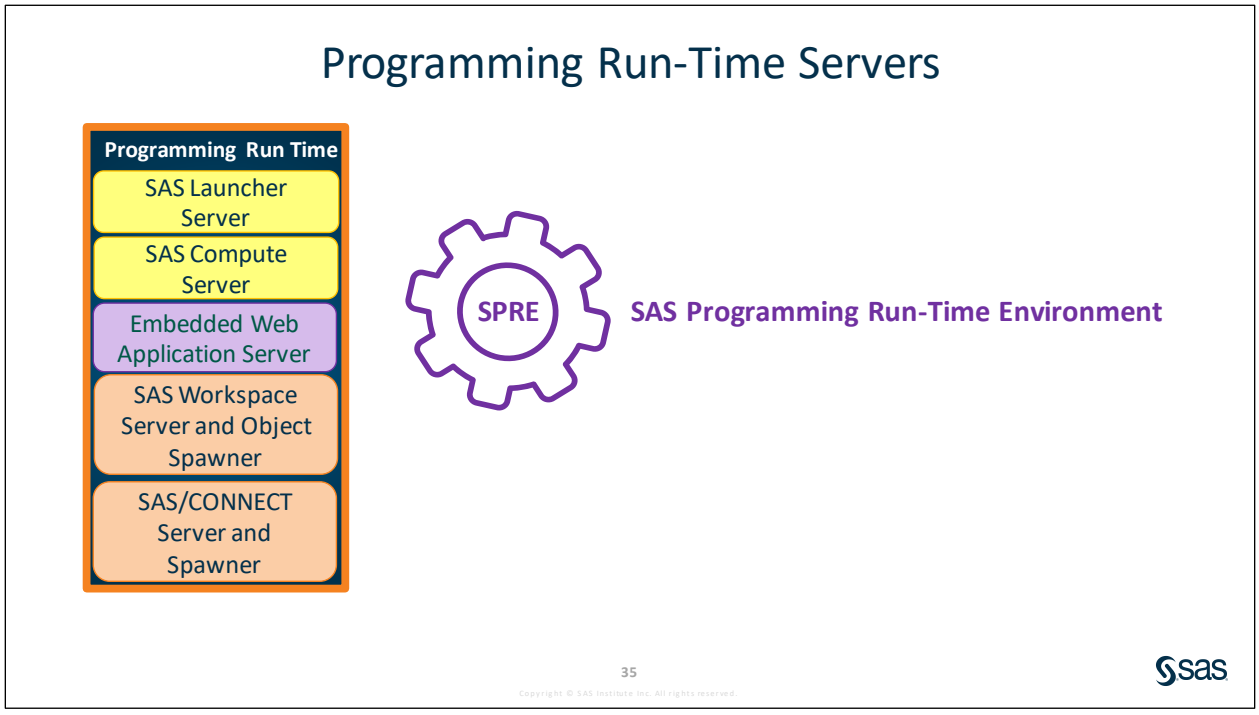
When CAS starts, the backup controller process is also started. If the controller experiences a disruption (such as a loss of network connectivity, disk full scenarios, and so on), the backup controller enables the CAS server to continue running. When the backup controller takes control of client communication, the transfer is seamless.

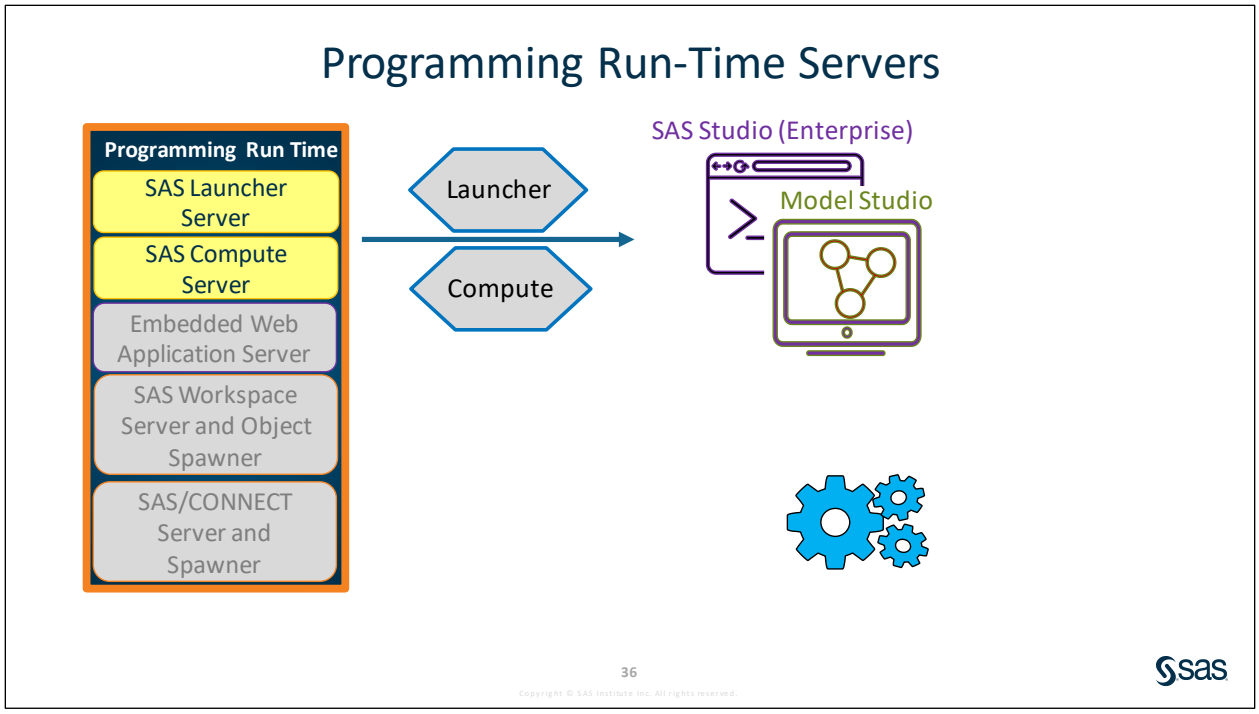
CAS Workers

When a server is running in massively parallel processing (MPP) mode, in addition to a controller, CAS also has multiple machines that are assigned the worker role. The controller parses out work to each worker node. Each worker node sends the results of its computations to the controller for aggregation and return to the client.

A server running in symmetric multiprocessing mode (SMP mode) consists of a controller only, and the server starts a session controller process only. It is the session controller process that operates on rows of data.

Fault isolation is provided for each session through the isolation of its processes from those other client sessions and those of the server itself. If a problem occurs in your session, it does not impact other clients or the server. And by default, the resources that a user creates in their session have session scope. That is, they are visible only within one's own session but not to other client sessions. Other users cannot access and modify another user's session-scope resources. Concurrent processing provides greater efficiency when processing large amounts of data, especially in distributed systems.





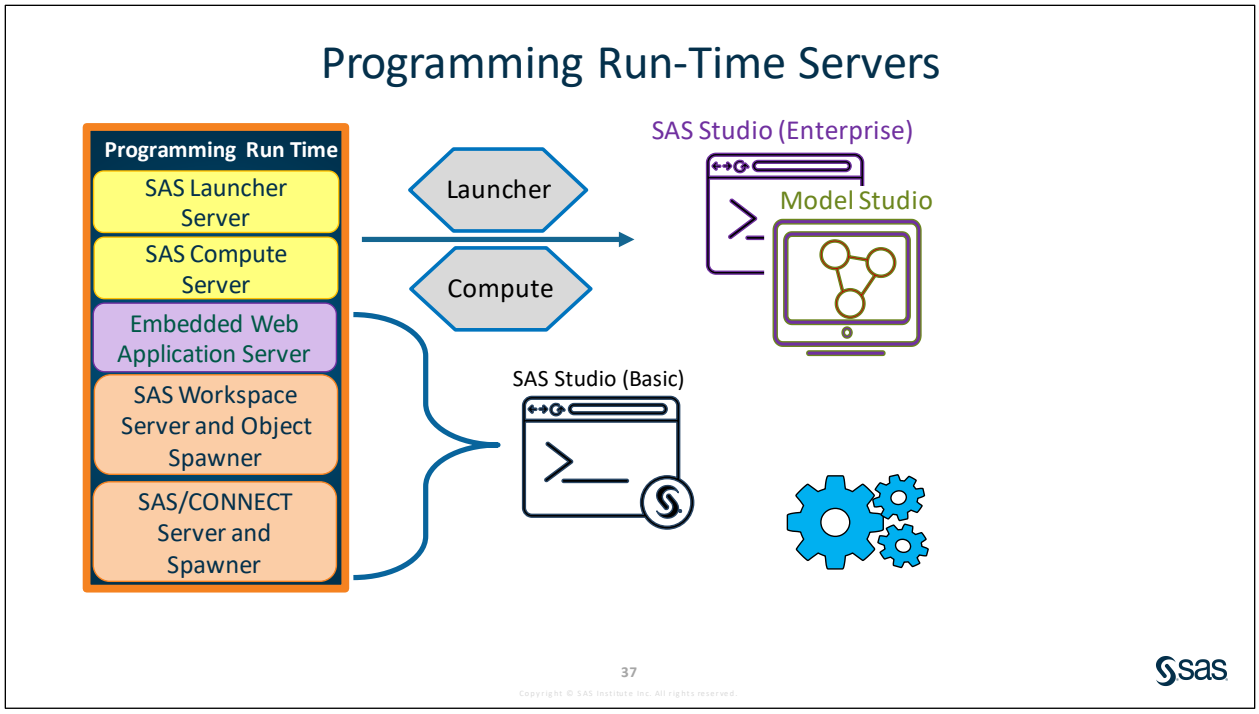
The launcher server and compute server are scalable for high availability and can be installed on multiple machines.

The SAS Launcher Server is used to start processes in a SAS Viya environment. The SAS Launcher Service is a microservice that starts processes using a launcher server and defines launcher contexts.

The SAS Compute Server is the server process that provides access to SAS Foundation in SAS Viya. The SAS Compute Service is a microservice that enables communication with a compute server, and defines compute contexts.

The Launcher/Compute server contexts provide information needed to run launcher servers and compute servers, such as environment variables, port ranges, authorized identities, SAS options, or autoexec statements.

Although the launcher and compute servers are new components that are integrated in the SAS Viya architecture, the remainder of the programming run-time environment relies on SAS®9 technologies.



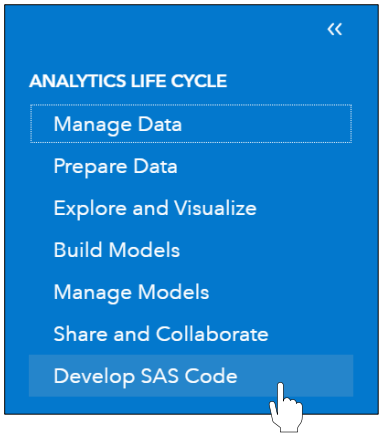
The embedded web application server is an Apache Tomcat server that hosts the SAS Studio application.

SAS/CONNECT server and spawner can be used to connect SAS Viya to legacy SAS environments.

Reviewing Configuration Files That Are Read When SAS Studio Is Used

This demonstration illustrates when the launcher server and compute server are used.

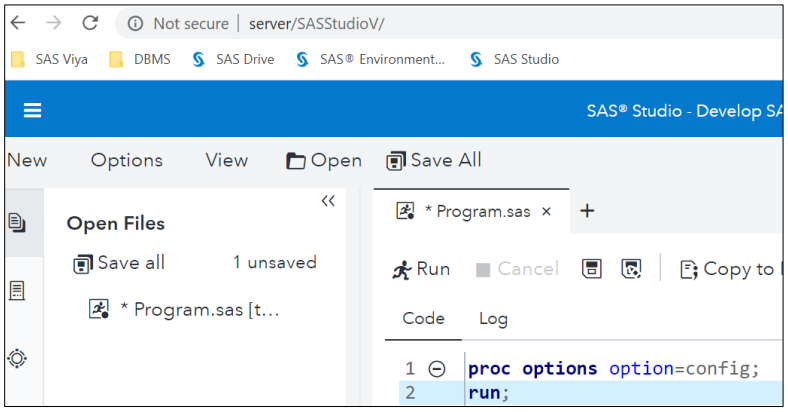
1. Log on to SAS Drive as **eric** and password **Student1**.
2. Select the applications menu ⇨ **Develop SAS Code**. Note the application name in the URL: SASStudioV. This is SAS Studio (Enterprise), which uses the launcher server and compute server for processing SAS program code.



3. Get started by clicking **New SAS Program**.

4. Enter the code shown below in the code window.

```
proc options option=config;
run;
```



5. Click **Submit**.

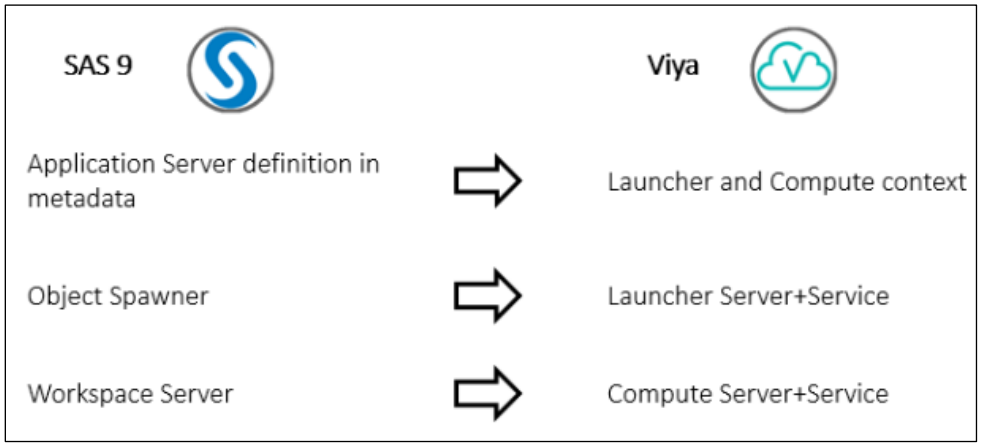
6. In the log, you see the configuration files that are read: the compute server (compsrv) and sasv9.cfg of SAS Foundation.

   The SAS Compute Server is a back-end server process that provides access to SAS Foundation in a SAS Viya environment.

```
1    %studio_hide_wrapper;
82   proc options option=config;
83   run;
    SAS (r) Proprietary Software Release V.03.05  TS1M0
 CONFIG=( /opt/sas/spre/home/SASFoundation/sasv9.cfg /opt/sas/spre/home/SASFoundation/sasv9_samples.cfg
/opt/sas/spre/home/SASFoundation/nls/u8/sasv9.cfg /opt/sas/spre/home/SASFoundation/sasv9_local.cfg
/opt/sas/viya/config/etc/compsrv/default/sasv9.cfg /opt/sas/viya/config/etc/compsrv/default/sasv9_deployment.cfg
/opt/sas/viya/config/etc/compsrv/default/sasv9_usermods.cfg )
                  Specifies the configuration file that is used when initializing or overriding the values of SAS system options.
```

   Note: The compute server is like a workspace server, but the workspace server is accessed using the proprietary IOM protocol, whereas a compute server is accessed through a compute service via a standard REST API.

   Just like the workspace server, the compute server is used to submit SAS code as jobs, query data, and access files via filerefs.



End of Demonstration

Practice

9. Creating, Viewing, and Terminating Three CAS Sessions

In this practice, you use a SAS Studio snippet to launch three CAS sessions. Use SAS Environment Manager and the CLI to terminate them. (You are repeating the demonstration.)

a. Select **SAS Drive** on the Bookmarks toolbar from Mozilla Firefox browser. (A shortcut to the browser is found on the Windows taskbar.)

b. Sign in to SAS Drive as **eric** with the **Student1** password.

c. Click **Skip setup** to continue to SAS Drive.

d. From the applications menu, select **Develop SAS Code**, which brings up SAS Studio (Enterprise).

e. Click **Snippets**  in the left pane.

f. Expand **SAS Snippets** ⇨ **SAS Viya Cloud Analytic Services**.

g. Double-click **New CAS Session** to add the code to the program window.

h. Copy the line of code and paste it twice below. Change the mySession string to **mySession1**, **mySession2**, and **mySession3**.

Code | Log

```
1   /*****************************************************************************/
2   /*  Start a session named mySession using the existing CAS server connection */
3   /*  while allowing override of caslib, timeout (in seconds), and locale     */
4   /*  defaults.                                                                */
5   /*****************************************************************************/
6
7   cas mySession1 sessopts=(caslib=casuser timeout=1800 locale="en_US");
8   cas mySession2 sessopts=(caslib=casuser timeout=1800 locale="en_US");
9   cas mySession3 sessopts=(caslib=casuser timeout=1800 locale="en_US");
10
```

i. Run the program to create the sessions by pressing the F3 key or clicking (the **Run SAS Code** icon). Check the log to confirm that there are no errors.

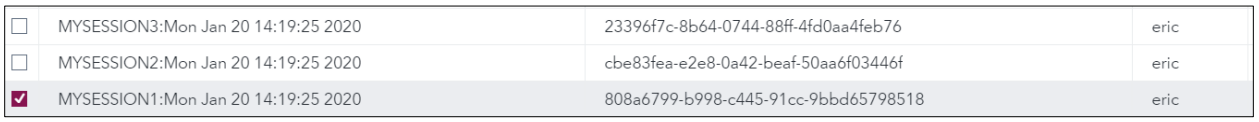
j. Open a new Chrome browser window and select **SAS Environment Manager** on the Bookmarks toolbar. (Or you might already be logged on to SAS Environment Manager as **christine**.) Sign in as the user **christine** with the password **Student1**. Assume the **SASAdministrator** role.

k. Click **Servers** on the side menu. The tasks from the **Servers** page can be performed only by SAS administrators.

l. Right-click the **cas-shared-default** server. Select **Assume the Superuser role**. A message in the window indicates that you are now in the Superuser mode.

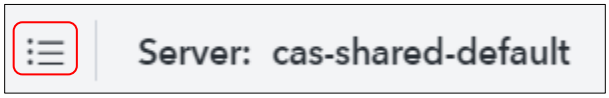
m. Right-click **cas-shared-default** again and select **Configuration**. (Alternatively, you can highlight **cas-shared-default** and click the **Configuration** icon  in the upper right.)

n. The first tab displays the list of sessions. Find **MYSESSION1**, which is owned by eric. Select the check box to the left. Click the **Terminate** icon at the top right to terminate the session.



o. Verify that you want to terminate the session.

p. Click the **Servers** menu to go back to the Servers page.



q. Use the CLI to terminate a CAS session. If an mRemoteNG session is not started, open one now as Christine.

r. Change the directory to **/opt/sas/viya/home/bin** to access **sas-admin**.

```
cd /opt/sas/viya/home/bin
```

Note: If Christine has been inactive for at least 12 hours, you will need to log back on to the CLI utility. Enter the command below and providing the user ID and password for **christine**.

```
./sas-admin auth login
Enter credentials for https://server.demo.sas.com:

Userid> christine

Password> <enter Student1>
Login succeeded. Token saved.
```

s. Obtain a list of servers. Enter the **sas-admin** command below. The value in the **Name** column is used for subsequent commands.

```
./sas-admin cas servers list
```

t. Open a list of eric's remaining sessions that are currently running on the CAS server. Enter the **sas-admin** command below. The session ID for MYSESSION2 is needed for the next step to terminate MYSESSION2.

```
./sas-admin cas sessions list -server cas-shared-default --
superuser --owner eric
```

```
[christine@server bin]$ ./sas-admin cas sessions list -server cas-shared-default --superuser --owner eric
{
    "items": [
        {
            "authenticationType": "OAuth",
            "id": "b8864392-d530-914e-9437-b1d17a3486bf",
            "name": "  Session:Tue Aug 28 11:58:37 2018",
            "owner": "eric",
            "state": "Connected",
            "transactionState": ""
        },
        {
            "authenticationType": "OAuth",
            "id": "68bf06b8-6e48-8e49-9878-1a507e4200b0",
            "name": "MYSESSION2:Tue Aug 28 12:06:31 2018",
            "owner": "eric",
            "state": "Connected",
            "transactionState": ""
        },
        {
            "authenticationType": "OAuth",
            "id": "df34bd48-b5c7-b64c-a3bc-cfe476c679ef",
            "name": "MYSESSION3:Tue Aug 28 12:06:31 2018",
            "owner": "eric",
            "state": "Connected",
            "transactionState": ""
```

Note: SAS Environment Manager was used previously to terminate MYSESSION1.

u. Terminate **MYSESSION2**. Enter the **sas-admin** command below.

```
./sas-admin cas sessions delete -server cas-shared-default --
superuser --session-id get from the previous command's output
```

v. Obtain a list of eric's remaining sessions that are currently running on the CAS server. Enter the **sas-admin** command below. Only one session remains.

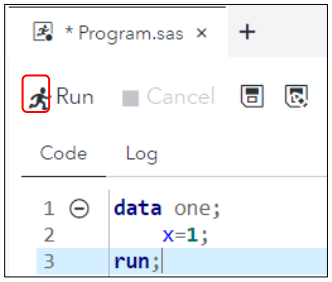
```
./sas-admin cas sessions list -server cas-shared-default --
superuser --owner eric
```

10. Viewing the Process Owned by Eric in the Operating System

a. Log on to SAS Drive as **eric** using the password **Student1**.

b. Select the applications menu ⇨ **Develop SAS Code** to launch SAS Studio.

c. Create a new SAS program and enter the code shown below on the Program.sas tab. A workspace server is launched to process the code submission.



Alternatively, you can copy the code snippet below and paste it into the Program.sas editor window in SAS Studio.

```
data one;
   x=1;
run;
```

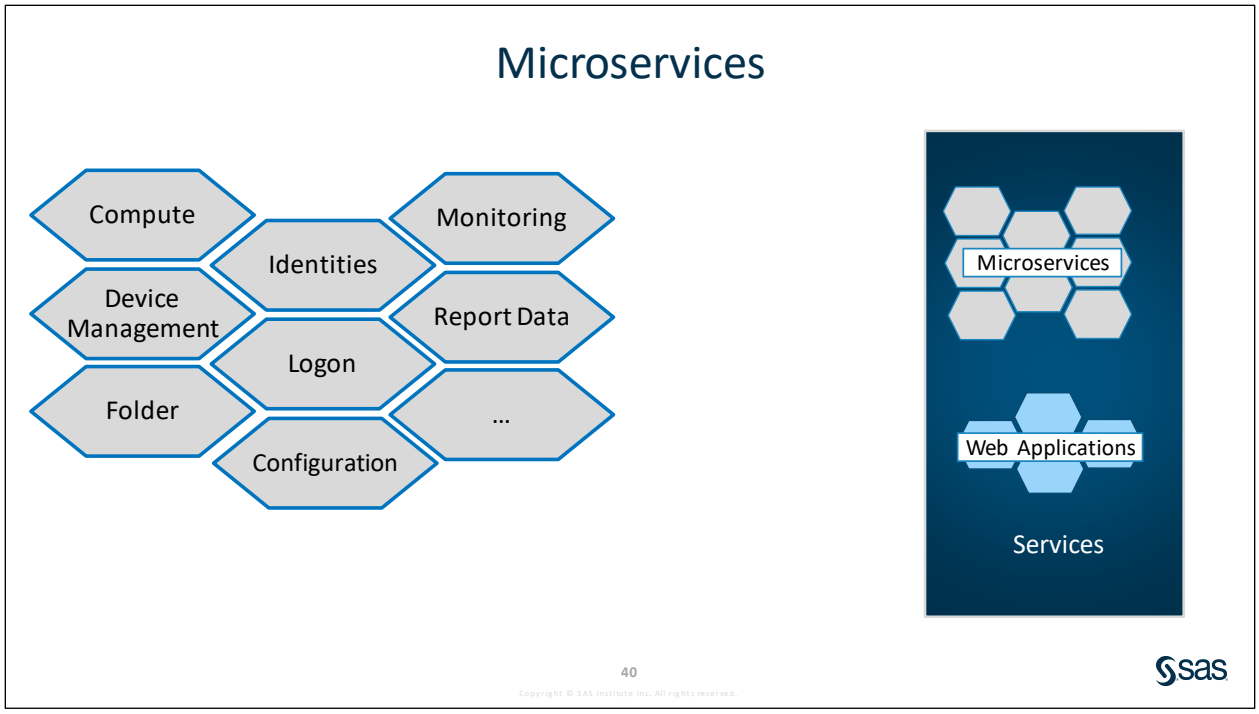
d. In mRemoteNG, search for any process owned by eric by issuing the following command:

```
ps -ef | grep eric
```

The location of the run-time server executable is **/opt/sas/spre/home/SAS Foundation**.

```
[christine@server bin]$ ps -ef | grep eric
eric      30390  40676  0 13:30 ?        00:00:00 /bin/bash -p /opt/sas/spre/home/bin/compsrv
_start.sh -serverID 04a3480d-30f7-419d-8b3f-d73125da3ab3 -context 6e131207-adbe-4af3-9f07-ea9
f305479d0
eric      30431  30390  1 13:30 ?        00:00:02 /opt/sas/spre/home/SASFoundation/utilities/
bin/compsrv -context 6e131207-adbe-4af3-9f07-ea9f305479d0 -serverID 04a3480d-30f7-419d-8b3f-d
73125da3ab3 -logconfigloc /opt/sas/viya/config/etc/compsrv/default/logconfig.xml
christi+  35786  15091  0 13:32 pts/0    00:00:00 grep --color=auto eric
```

End of Practices

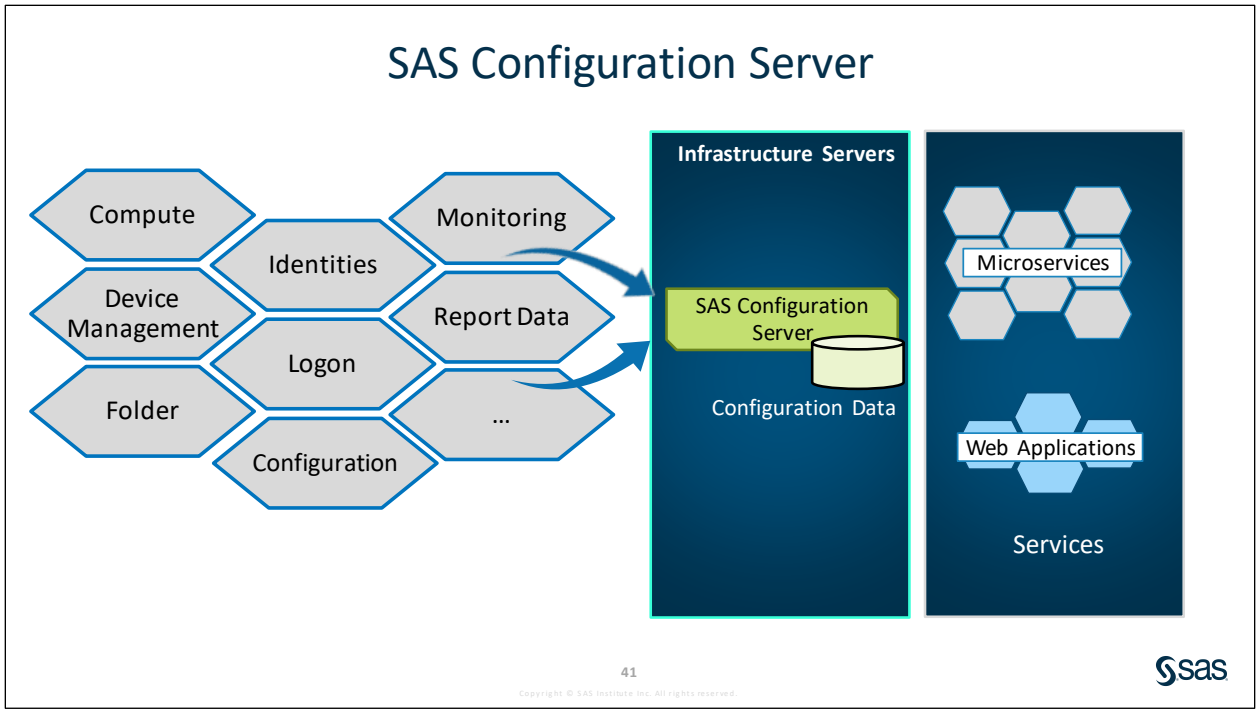


A microservice is a service that runs in its own process and communicates with a lightweight mechanism of HTTP. Microservices are self-contained and fulfill a specific role. They can be replaced independently of one another and initialize and configure themselves asynchronously. While microservices are independent of each other, they together represent a larger, cohesive architecture.

Note: "Micro" does not mean small. It refers to a single function or something that is narrow in scope.

Microservices provide a language-neutral API, which means they are accessible to developers through REST APIs.

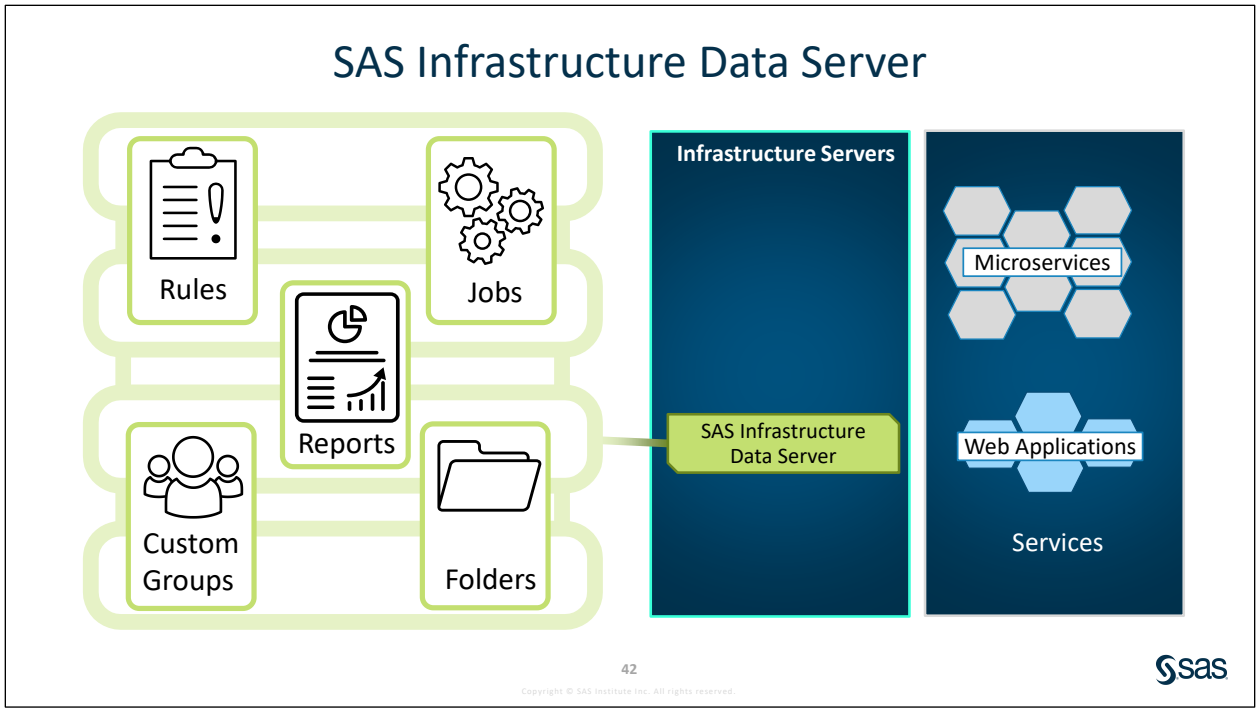
One or more instances of these processes can be running at any given time. The number of instances can change dynamically as demand changes.



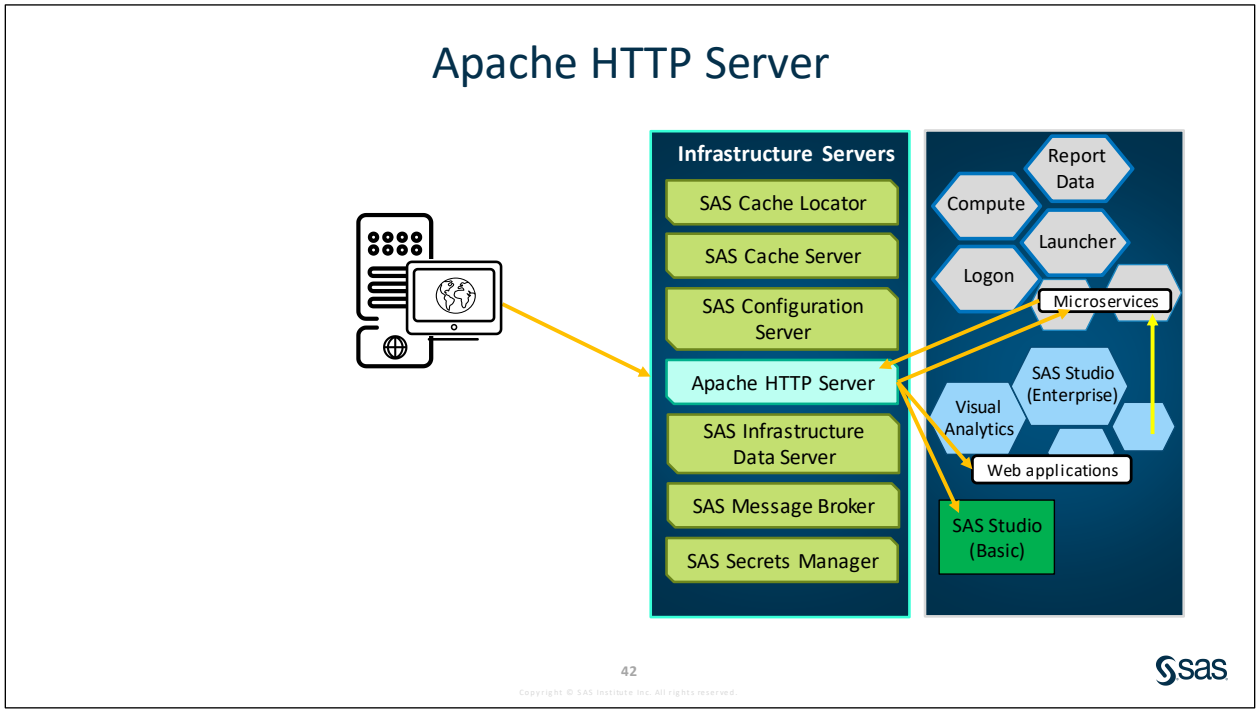
Each SAS Viya service communicates with the SAS Configuration Server for configuration information and the state of other services that it depends on. It also reports its availability to the SAS Configuration Server.

A change to configuration property values for any of the following services requires a restart of their respective services:

- SAS Cache Locator sas-viya-cachelocator-default
- SAS Cache Server sas-viya-cacheserver-default
- SAS Configuration Server sas-viya-consul-default
- SAS Message Broker sas-viya-rabbitmq-server-default
- SAS Infrastructure Data Server s**as-viya-sasdatasvrc-postgres**



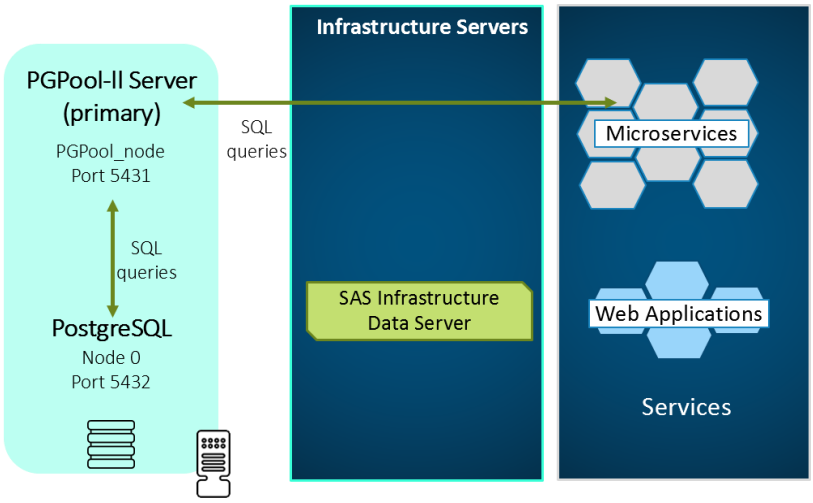
The SAS Infrastructure Data Server is used for storage by SAS middle-tier software, as well as other elements, such as folders, custom groups, authorization rules, reports, jobs, and audit records. It is also used by some SAS Solutions software, an example being Visual Investigator.



Apache HTTP Server is a web server that is used to serve static HTML content and proxy client communication to web applications and microservices. Apache proxies both external connections coming from a client such as a browser as well as internal service-to-service connections.

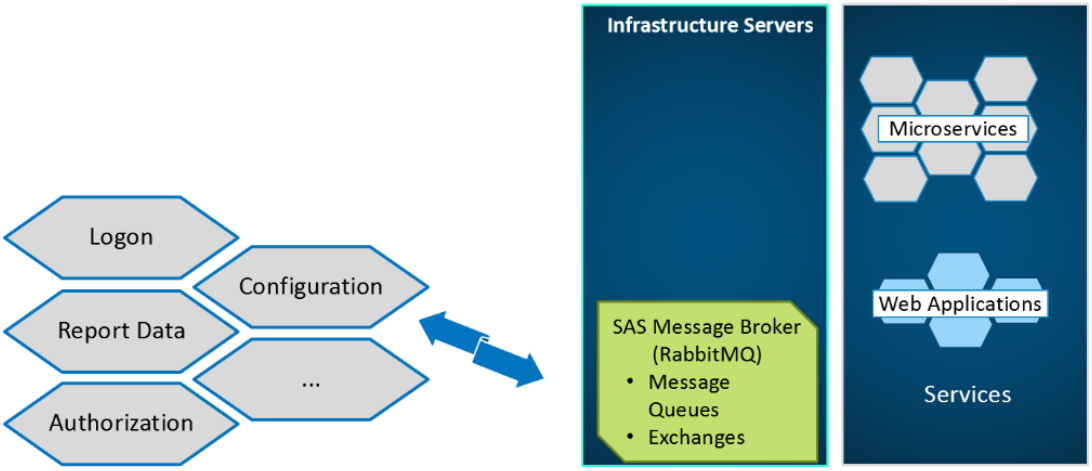
Additional Information: Other Architecture

Clustering the SAS Infrastructure Data Server



The SAS Infrastructure Data Server is based on PostgreSQL and SAS provides PGPool-II open source software that acts as proxy software. The SAS Infrastructure Data Server can be clustered to provide high availability, replication, load balancing, and connection pooling. PGPool's primary function is for clustering support and high availability.

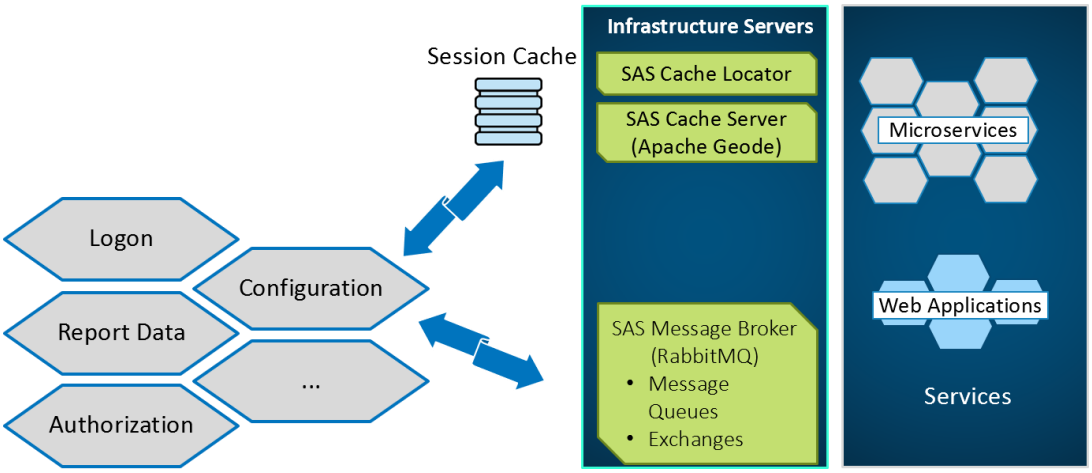
SAS Message Broker



The SAS Message Broker exchanges accept messages from publishers and route them to queues and exchanges. The exchange type controls whether messages are sent to a specific queue, to all associated queues, or only to queues that accept a particular message routing key or that match a key pattern.

SAS uses Pivotal's RabbitMQ, an AMQP-compliant message broker. The Advanced Message Queuing Protocol (AMQP) is an open standard for passing business messages between applications.

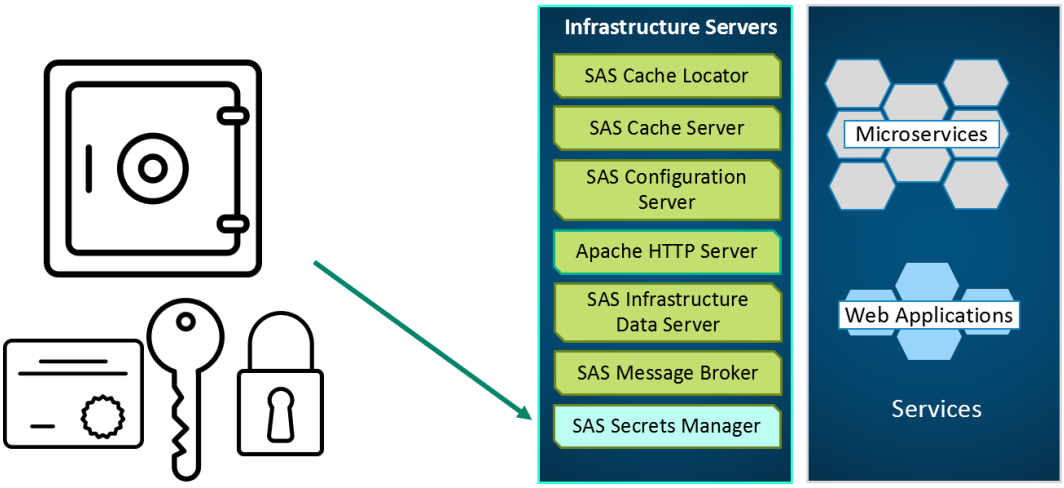
SAS Cache Locator



SAS Cache Locator and SAS Cache Server provide a distributed cache technology to microservices in SAS Viya.

The Cache Locator and Cache Server are based on the open source Apache Geode project.

SAS Secrets Manager



SAS Secrets Manager is based on HashiCorp Vault.

The SAS Secrets Manager does the following:

- Generates TLS certificates for SAS Viya servers at start-up.
- Secures storage for secrets. Microservices use secure storage so that multiple microservice instances running on the same machine do not request multiple TLS certificates.
- Encrypts and decrypts data without storing it. SAS Compute Server uses this feature when it sends a password to child processes.
- Revokes secrets. SAS Viya services use this feature when rotating security artifacts. For example, services use vault tokens to request TLS certificates).

Practice

11. Using SAS Environment Manager to Configure a Microservice

In this practice, set the time-out interval for SAS Viya web applications. The session time-out interval is the specific period of time that a web application waits before it signs off users' inactive sessions.

a. If you do not have an active SAS Environment Manager session, open a Chrome browser and select **SAS Environment Manager** on the Bookmarks toolbar. Sign in as the user **christine** with the password **Student1**. Assume the **SASAdminstrator** role.

b. Select **Configuration** from the side menu.

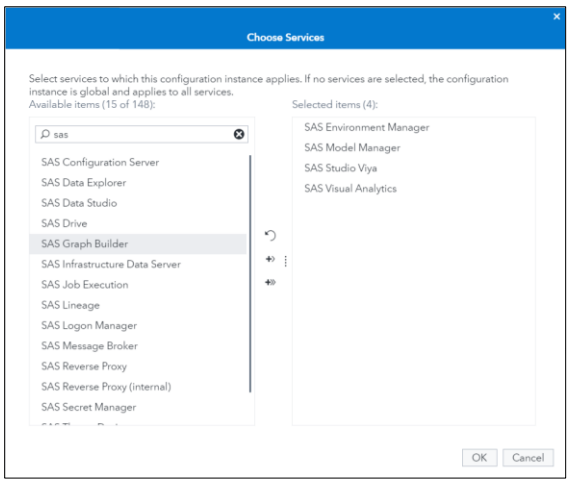
c. Click **Definitions** from the **View** drop-down menu.

d. In the list of configuration definitions, select **server**.

e. In the top right corner of the view, click **New Configuration**.

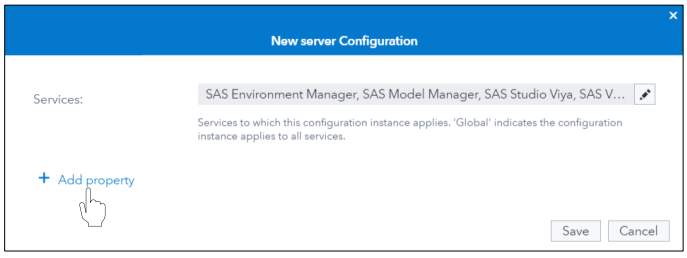
f. In the **New server Configuration** dialog box, click **Edit**.

g. In the Choose Services dialog box, filter on **sas** to see SAS Viya web applications. Move **SAS Environment Manager**, **SAS Model Manager**, **SAS Studio Viya**, and **SAS Visual Analytics** to the **Selected items** column.



h. Click **OK**.

i. In the New server Configuration dialog box, click **Add property**.



j. In the Add property dialog box, in the **Name** field, enter the following Spring server property: **session.timeout**.

k. In the **Value** field, enter the number of seconds you want the SAS Viya web applications to wait before they sign off users' inactive sessions. Enter **7200** so that two hours of inactivity will sign a user off of the application.

l. Click **Save**.

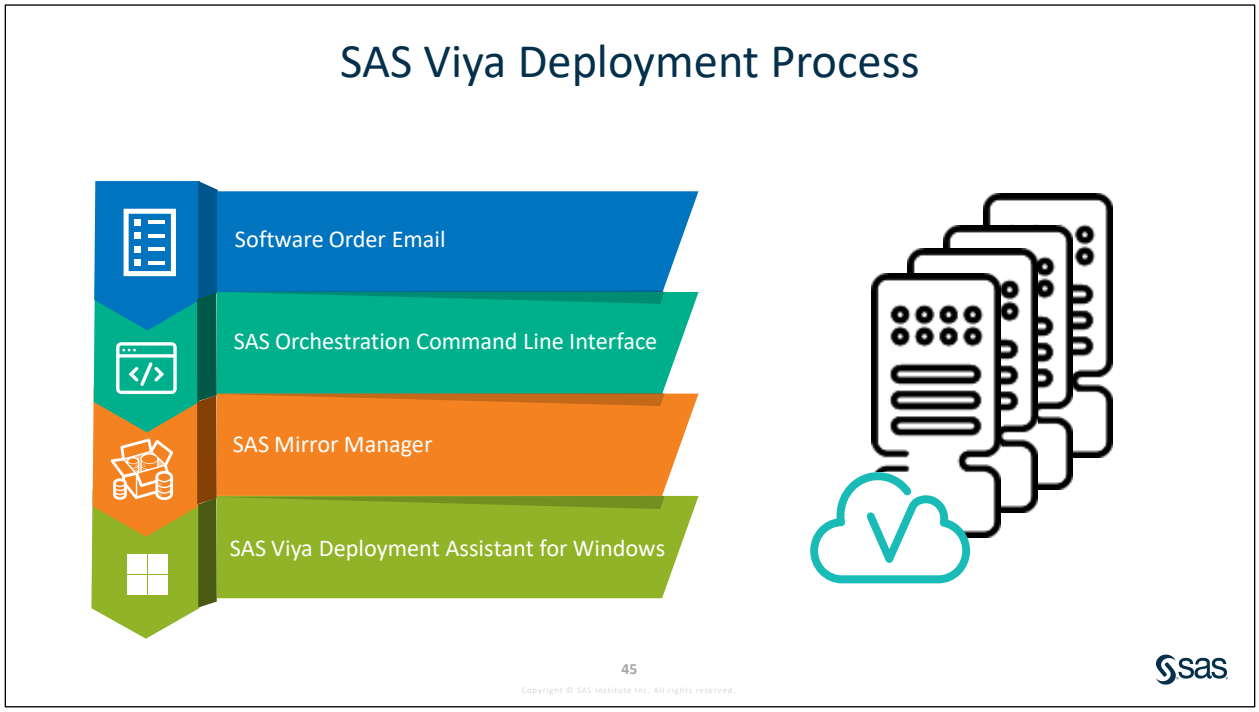
m. Click **Save**.

Your change takes effect for any new sign-ins to a SAS Viya web application.

Note: In SAS Studio (Basic), the session time-out interval is defined by the administrator with **webdms.maxSessionTimeoutInHours**.

End of Practices

1.3 Deployment Overview



SAS Viya deployments on Linux and Windows uses industry-standard deployment software.

The Software Order Email (SOE) that SAS sends to your business or organization contains a file attachment with the information specific to your order to create the deployment scripts. These deployment scripts are used to install and configure the software.

The installer downloads and runs a tool provided by SAS called the SAS Orchestration Command Line Interface, or CLI.

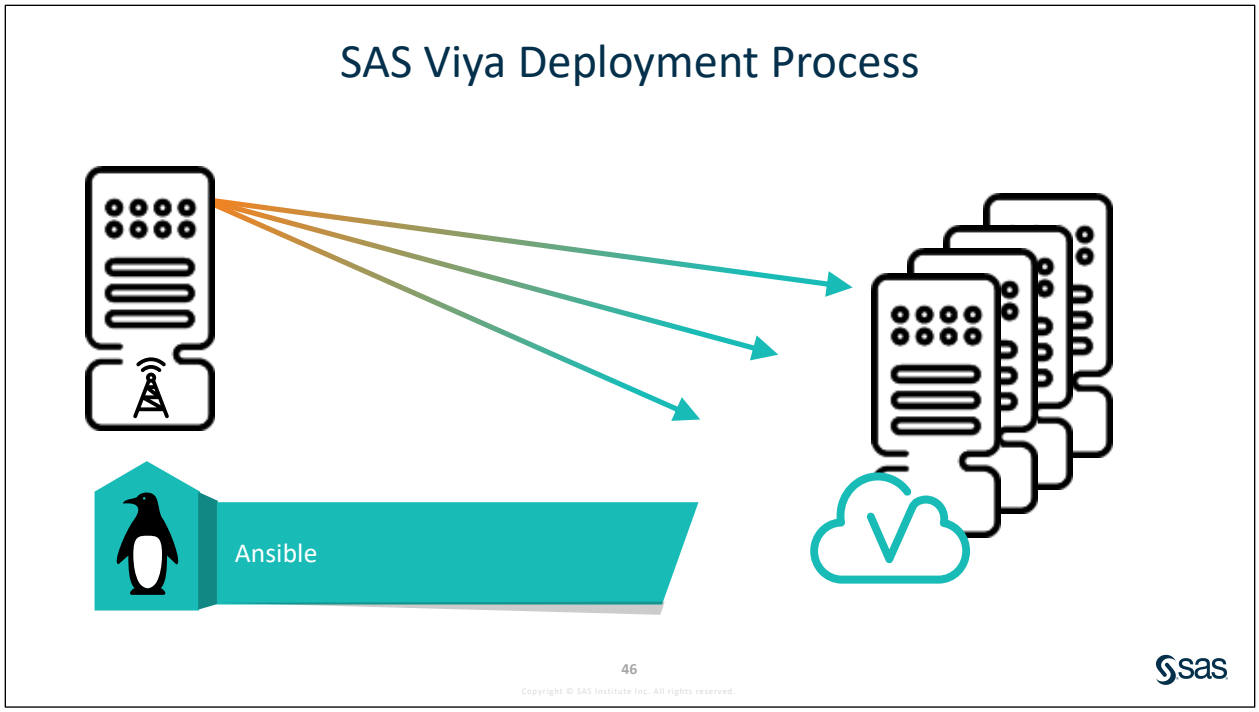
The software to which you are entitled is downloaded from repositories that are maintained by SAS, or from mirror repositories at your own site. Creating mirror repositories is an optional task that you can perform before deployment. SAS provides the SAS Mirror Manager utility to create mirror repositories.

Note: Creating mirror repositories before running the playbook is optional for deployments on Red Hat Enterprise Linux, but is required for deployments on SUSE Linux.

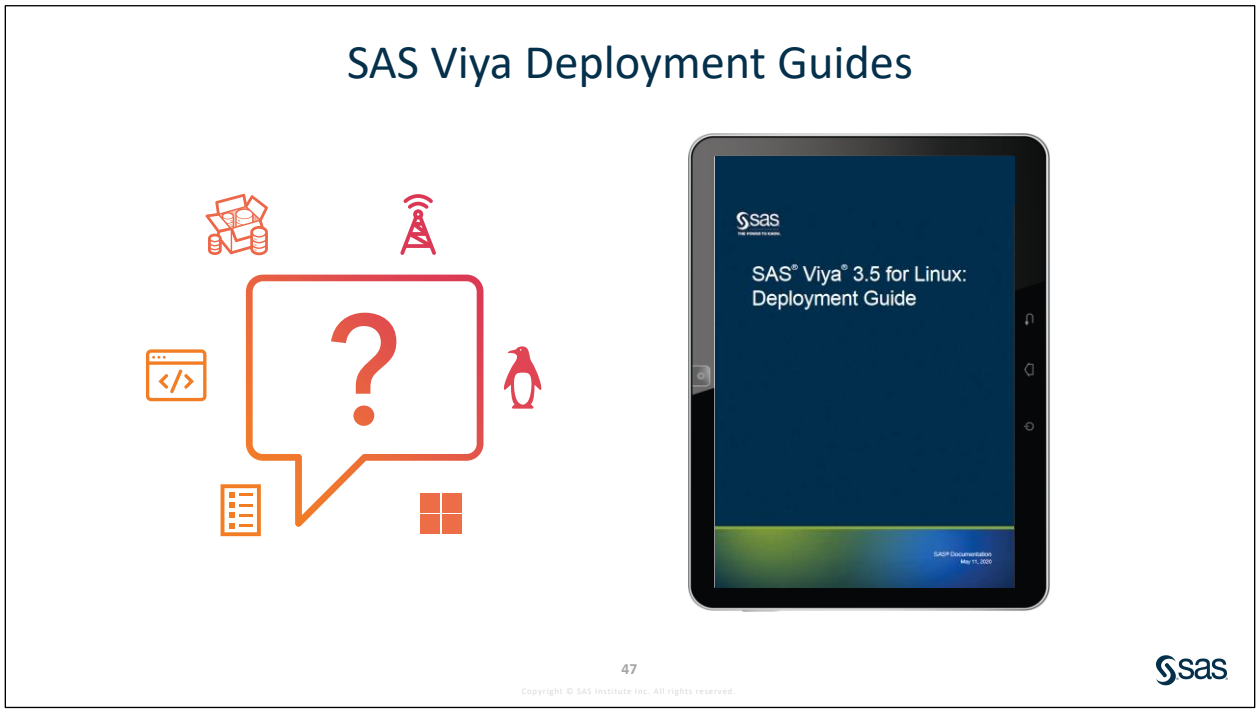
Note: For Windows deployments, SAS offers the SAS Viya Deployment Assistant to validate system settings required by SAS Viya on Windows machines.

To deploy SAS Viya software on Windows, you use PowerShell and CMD shell and the installer runs (as administrator) a **setup.bat** command that executes the deployment scripts.

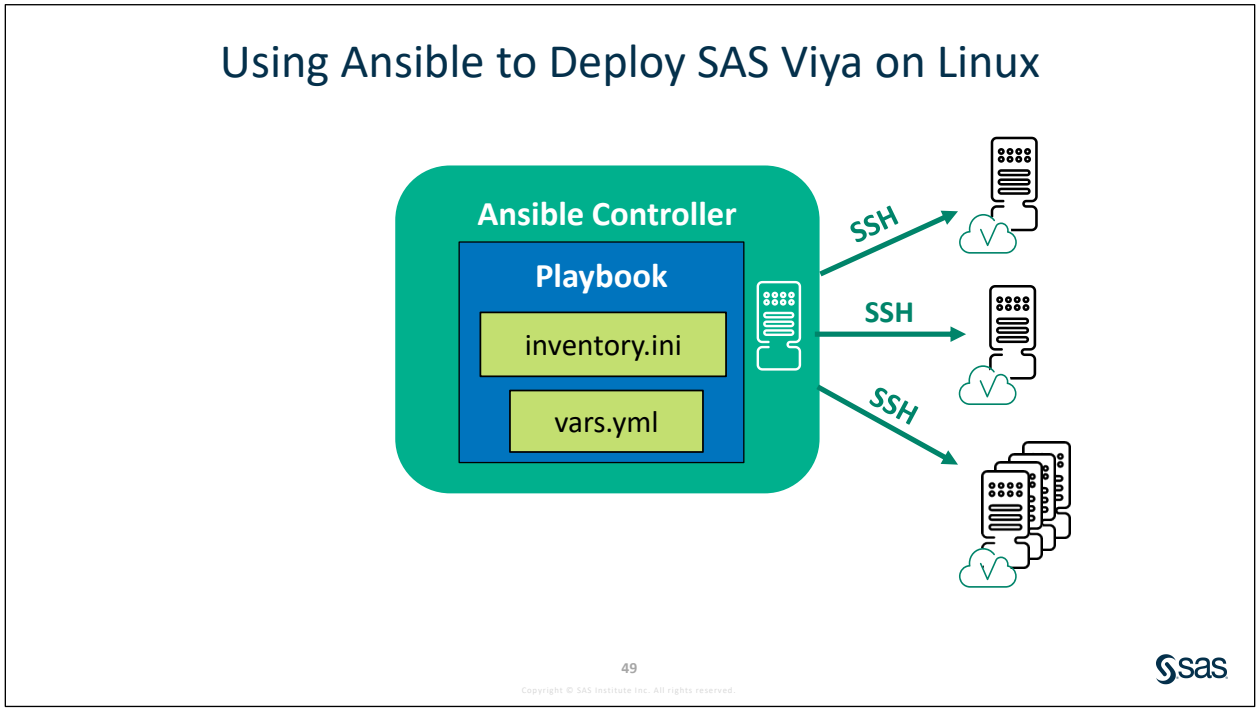
Each time you run the command, the software is securely downloaded from repositories that are maintained by SAS, or from the mirror repositories that you have created.



You use Ansible, a configuration management software tool, to deploy SAS Viya to one or multiple Linux operating system environments.

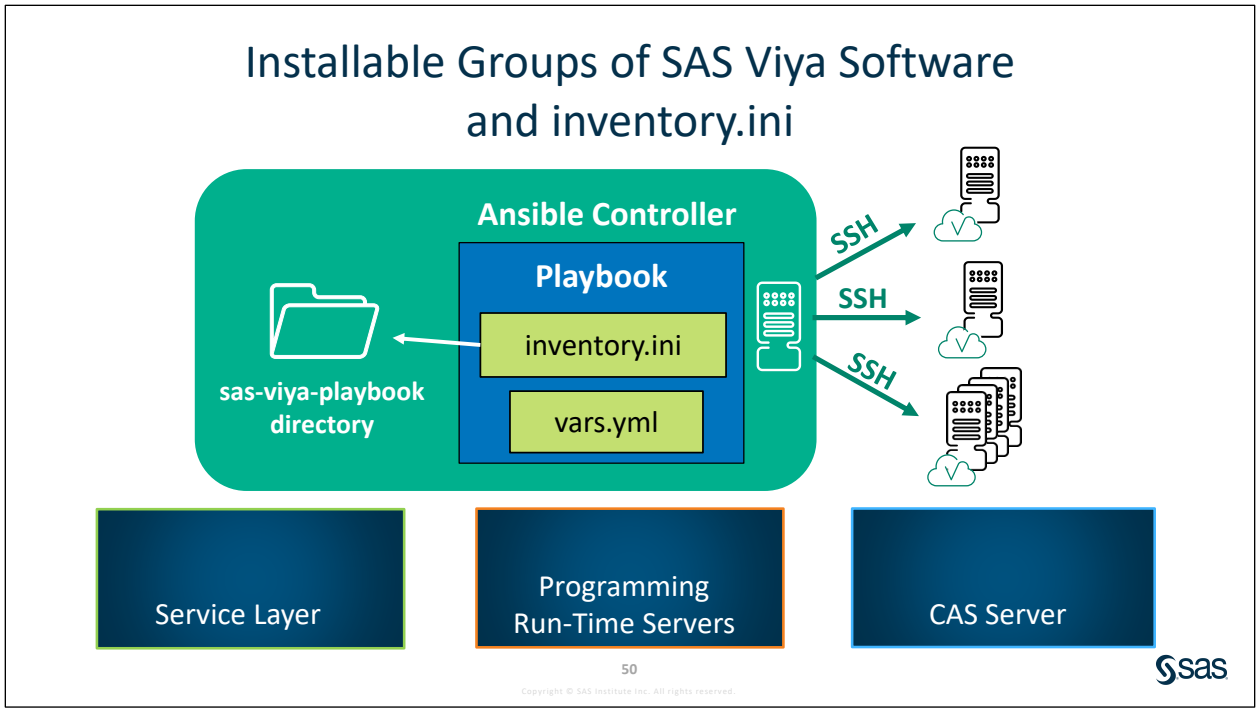


Instructions for downloading and using these tools and utilities are available in the deployment guides for your products. Your Software Order Email (SOE) contains a link to the appropriate guide. And please make sure that you have the latest as the contents of the deployment guides are subject to continual updates. If you accessed this guide directly from your SOE, you are viewing the latest guide. Otherwise, you can always access the latest release of this guide from the SAS Viya Deployment Guides site. Or, the latest deployment guides can also be accessed from SAS Viya Documentation on support.sas.com.



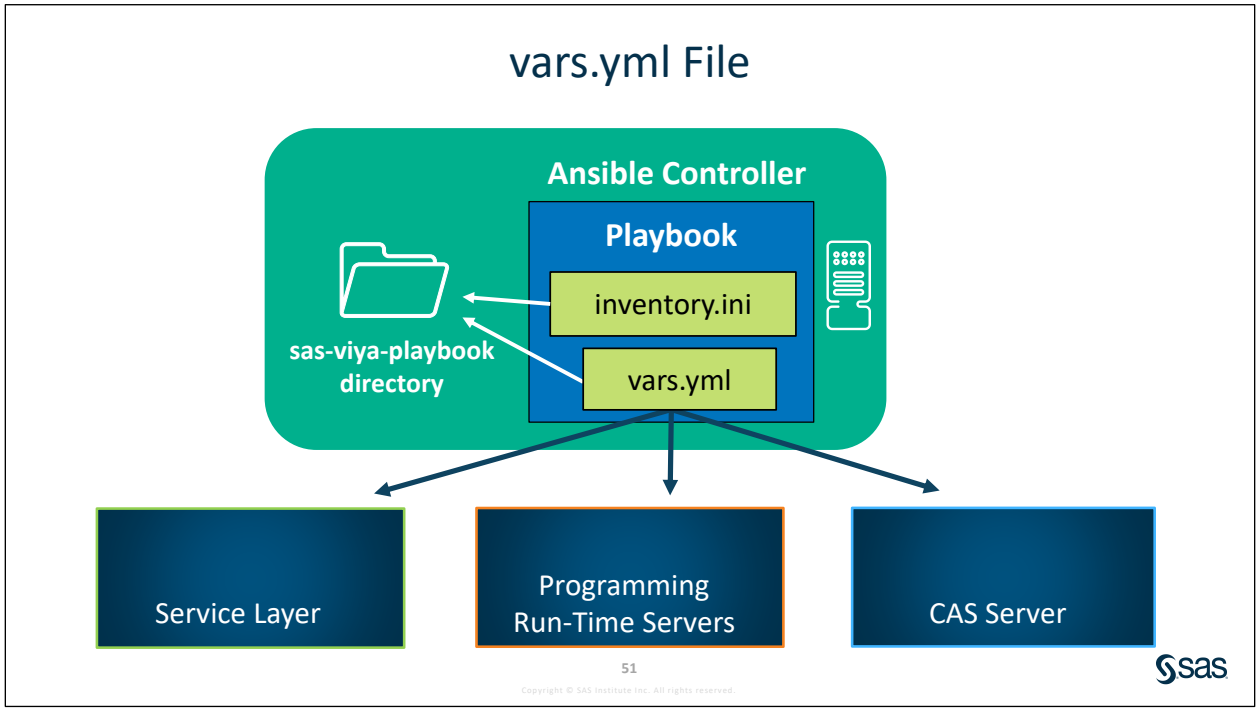
To deploy using Ansible, you customize files for your environment, and then you run a command to deploy software according to the values in those files. The set of files, known collectively as “the playbook,” provides the instructions about what software is deployed on which machines.

Note: SAS provides software as RPM packages and uses the Linux utility yum to install these packages. Ansible automates a series of yum commands to install the RPM packages on the machines that you designate.



Ansible uses an inventory file to specify the machines to be included in a deployment and the software to be installed on them. The categories of software are depicted as host groups such as the service layer, programming run-time servers, and CAS server.

Note: The **inventory.ini** file is located in the **sas-viya-playbook** directory. The **inventory.ini** file contains the specification of each machine or host on which SAS Viya software will be deployed and the host group assignment list, which is a mapping of the installable groups of software and the machines on which they will be deployed.

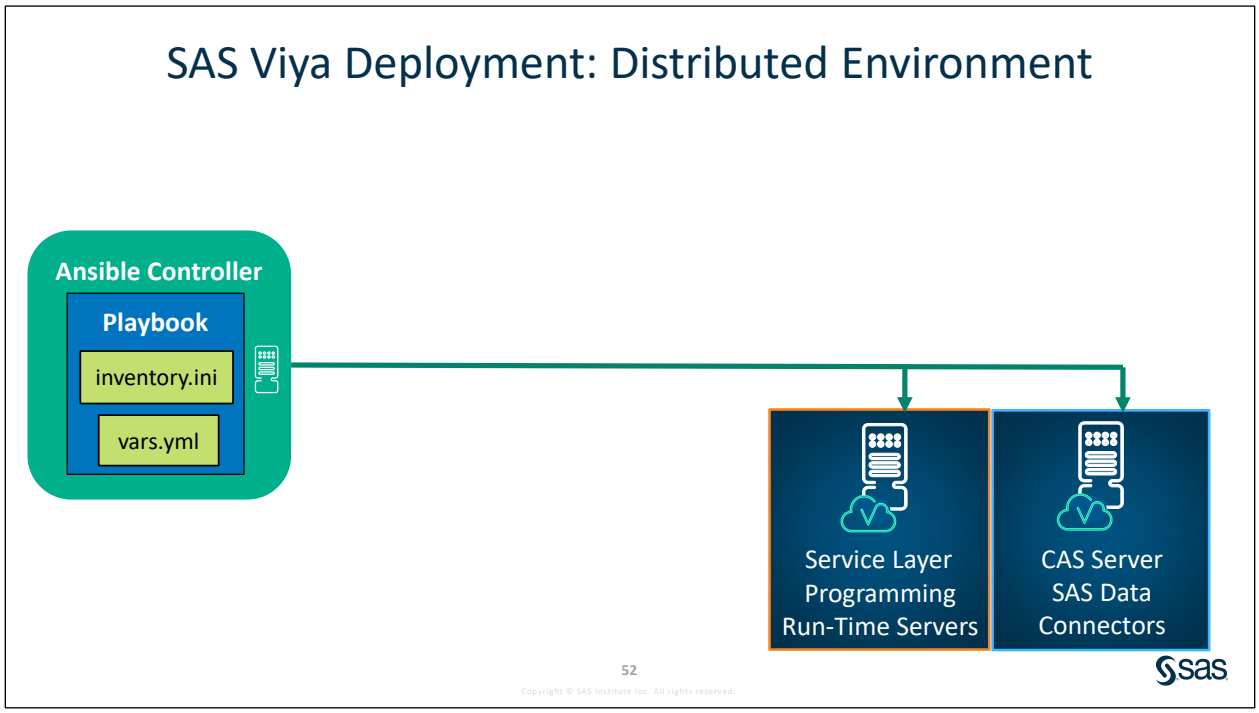


Another file that is used for deployment is the **vars.yml** file. This includes the variables that enable you to customize your deployment. For example, you edit the **vars.yml** file to configure a data connector, to manage passwordless SSH settings, and so on.

There is an optional **sitedefault.yml** file that is typically not used for the initial deployment. The **sitedefault.yml** file contains variables for more advanced implementations, such as setting up high availability PostgreSQL cluster and enabling SAS Viya to run in multi-tenancy mode.

Comparison of Deployment Tools in SAS 9.4 and SAS Viya (Linux)

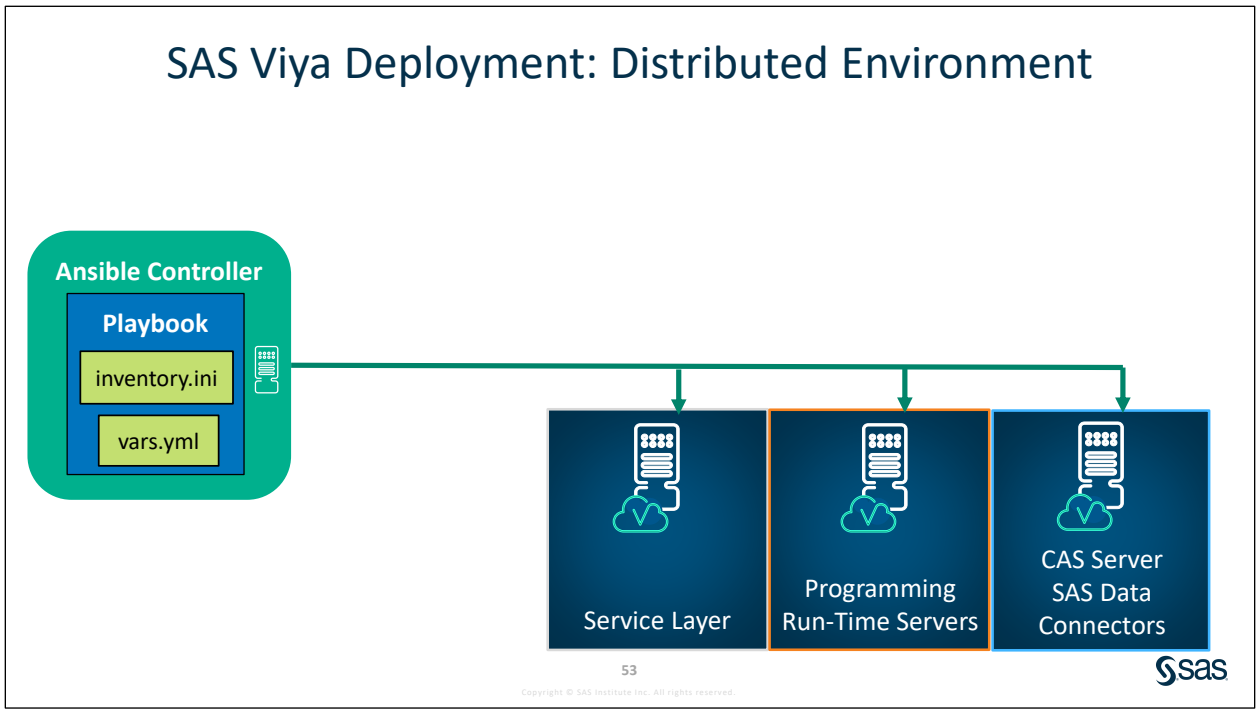
SAS 9.4	SAS Viya (Linux)
Software Order	Software Order
SAS License	SAS License
Software Depot	RPM files + Repository Mirror (optional)
SAS Download Manager	Yum
Plan.xml	Ansible Inventory file
SAS Deployment Wizard	Ansible + Ansible Playbook
Response File	vars.yml + sitedefault.yml
Hot Fix	Yum update
----	Re-run the playbook
----	Certificates



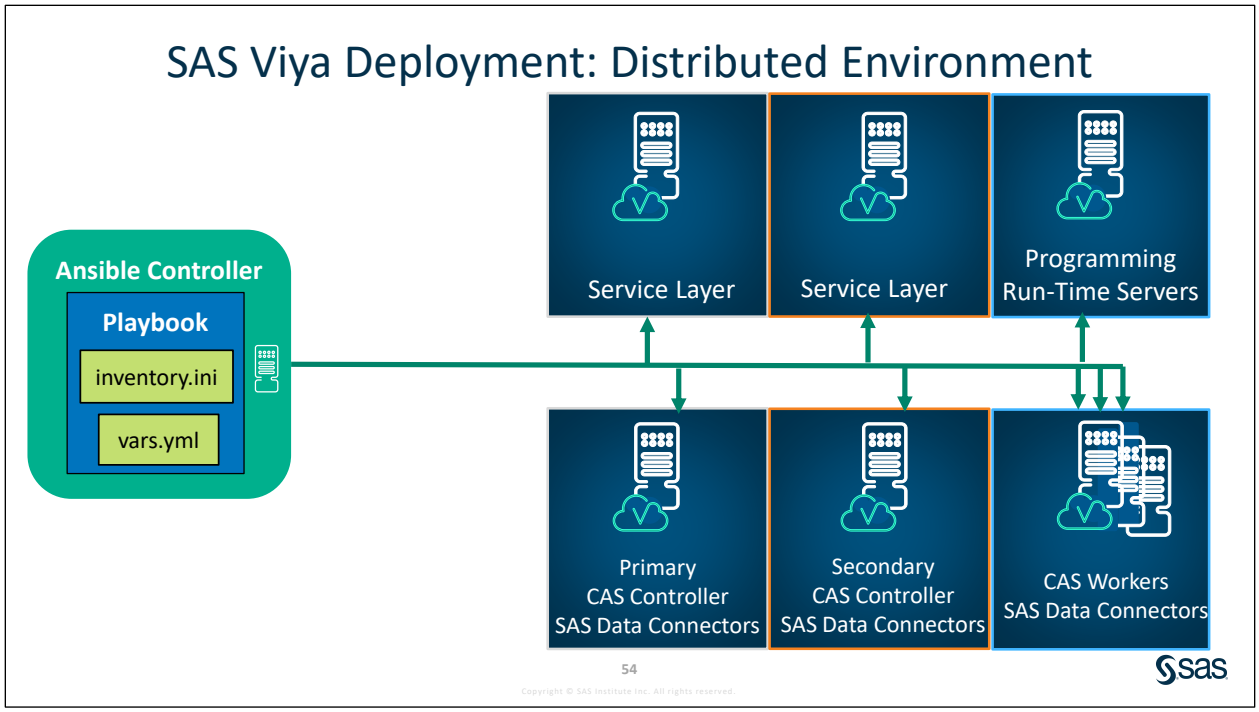
To meet the needs of different workloads, performance requirements, and optimum resource utilization, SAS Viya is flexible in working with deployments spread across multiple machines. This example shows a full deployment with single-machine CAS server and a separate machine for the service layer and the programming run-time servers.

The primary CAS controller is deployed to its own machine along with the data connectors. (You configure the data connectors for use in the vars.yml file before running the playbook.) The CAS server supports analytics and data-management processing in symmetric multiprocessing (SMP) mode.

Because a single-machine CAS server is deployed, the secondary CAS controller and the CAS workers are not deployed.



Or, you could have separate machines for the service layer and the programming run-time servers.



SAS Viya, and CAS in particular, is designed to accommodate massive scalability, which means running across many hosts, and increasing compute capacity by easily adding more CAS worker nodes. Optimal processing can be achieved through massively parallel processing or MPP mode for multiple users.

Exploring SAS Viya Deployment Files

This demonstration explores the inventory.ini and vars.yml files.

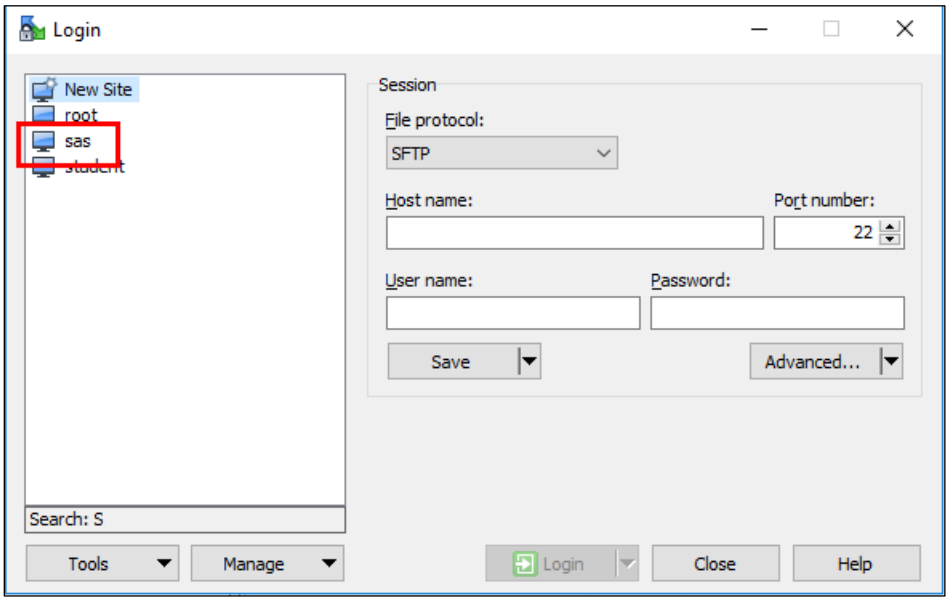
1. Connect to your Windows client machine.

Classroom Course	Live Web Course
Use a remote desktop connection with the IP address that is given to you by the instructor. Sign in with these credentials: User: **Student** Password: **Metadata0**	Use the URL in step 6 of the email that you received from Live Web Administration.

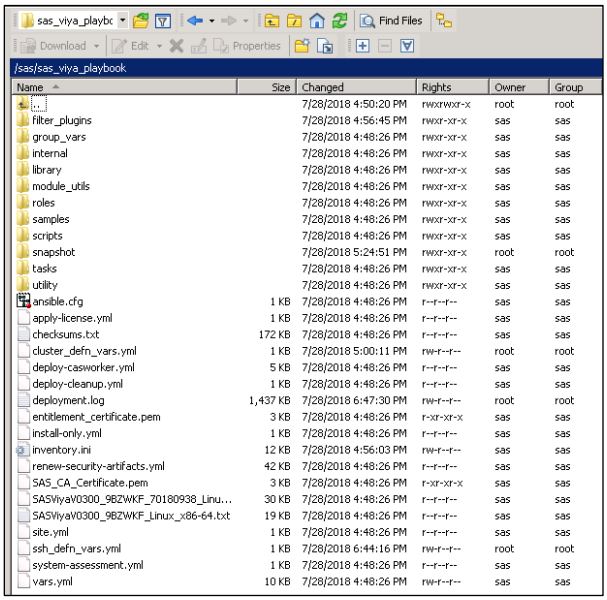
2. Double-click the **WinSCP** icon from the Windows desktop or Windows taskbar.

   Note: You can use **mRemoteNG** to view the inventory.ini and the vars.yml files.

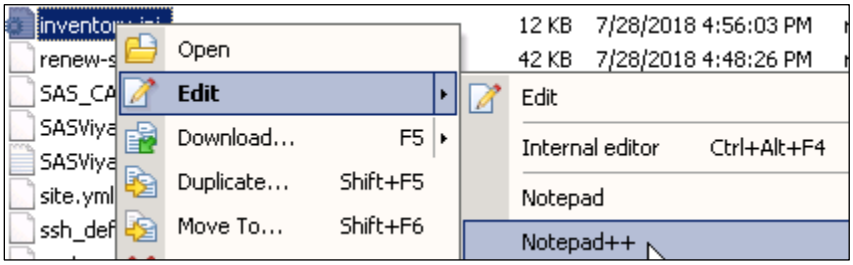
3. Select **sas** in the Login window and sign on to a session on the server machine where SAS Viya is installed.



4. Navigate to **/sas/sas_viya_playbook** on Linux, which is on the right side of the interface.



5. Right-click **inventory.ini** and select **Edit** ⇨ **Notepad++**.



6. Ansible uses an inventory file to specify the machines to be included in a deployment and the software to be installed on them.

   Each inventory file consists of a deployment target definition and a specification of each machine on which SAS Viya software will be deployed.

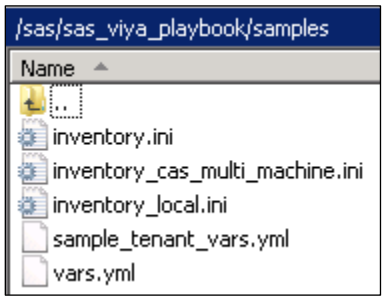
   SAS Viya software is deployed as host groups, which are identified by square brackets ([ ]) in the inventory file. Each host group is preceded by comments that describe the purpose of the software in the host group. The user specifies the machines on which a host group will be deployed by listing them under the host group name. A machine can have more than one host group deployed on it.

inventory.ini

```
deployTarget ansible_connection=local

# The AdminServices host group contains services used to support administrative tasks that have transient load.
[AdminServices]
deployTarget

# The AdvancedAnalytics host group contains services that provide advanced analytics features.
[AdvancedAnalytics]
deployTarget

# The CASServices host group contains services used to interact between the CAS server(s) and the mid-tier services.
[CASServices]
deployTarget

# The CognitiveComputingServices host group contains services for performing common text analytics tasks.
[CognitiveComputingServices]
deployTarget

# The CommandLine host group contains command line interfaces for remote interaction with services.
# It should include every host for which an administrator runs either the command-line interface (CLI)
# or the operations infrastructure. If you are using the https scheme (the default) to access SAS Viya
# Web applications and plan to onboard tenants, the first host in the CommandLine host group must be a
# host that is present in the programming, ComputeServer, or sas-casserver-* host group to successfully
# onboard multiple tenants. In all cases where the Operations host group is present, the host that is
# in the Operations host group must be included in the list of hosts for the CommandLine host group.
#
# In order for the operations infrastructure to manage audit records:
#   + Include the machine in the cas-server-primary host group for the provider or single tenant.
#   + Include the machine in the cas-server-secondary host group.
#
# For details about auditing, see the SAS Viya Administration documentation.
[CommandLine]
deployTarget

# The CommonPlanningService host group contains services to support financial and demand planning.
[CommonPlanningService]
deployTarget

# The ComputeServer host group contains the Compute Server that executes SAS code on behalf of the Compute Service.
# It supports more than one host during initial deployment for both single-tenant and multi-tenant deployments.
```

Close the file.

7. There are existing templates from the **sas_viya_playbook/samples** subdirectory. This directory contains templates for different types of deployments.



You can copy the template that you want to use, rename it inventory.ini, and place it in the **sas_viya_playbook** directory. It replaces the existing inventory.ini file.

8. Go up one level to open **vars.yml** file. The vars.yml file is similar to a response file in SAS 9.4. Scroll down to **CAS Configuration**.

```
##############################################################################
## CAS Configuration
##############################################################################

# The user that the CAS process will run under

casenv_user: cas

# The group that the CAS user belongs to

casenv_group: sas

# The following is the initial Admin user for use with CAS Server Monitor.
# This is the user you will log into CAS Server Monitor with
# in order to create global CAS libs and set access rights.
# If not set, the casenv_user will be used by default.
# If all defaults are taken, the "cas" user will not have a password
# defined for it. To have one created by the deployment process,
# review how to define a password as documented with the sas_users
# collection above.

#casenv_admin_user:


#### CAS Specific ####
# Anything in this list will end up in the cas.settings file
#CAS_SETTINGS:
   #1: ODBCHOME=ODBC home directory
   #2: ODBCINI=$ODBCHOME/odbc.ini
   #3: ORACLE_HOME=Oracle home directory
   #4: JAVA_HOME=/usr/lib/jvm/jre-1.8.0
   #5: LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib:$JAVA_HOME/lib/amd64/server:$ODBCHOME/lib

# Anything in this list will end up in the casconfig.lua file
#   The env section will create a env.VARIABLE in the file
#     Example: env.CAS_DISK_CACHE = '/tmp'
#   The cfg section will create a cas.variable in the file
#     Example: cas.port = 5570
#
# If you have defined hosts for the sas-casserver-worker then the MODE will
# automatically be set to 'mpp'. If the environment variables HADOOP_HOME and
# HADOOP_NAMENODE are set, the COLOCATION option will automatically equal 'hdfs'.
# If HADOOP_HOME and HADOOP_NAMENODE are not set, then the COLOCATION option
# will automatically equal 'none'.

CAS_CONFIGURATION:
```

```
#### CAS Specific ####
# Anything in this list will end up in the cas.settings file
#CAS_SETTINGS:
   #1: ODBCHOME=ODBC home directory
   #2: ODBCINI=$ODBCHOME/odbc.ini
   #3: ORACLE_HOME=Oracle home directory
   #4: JAVA_HOME=/usr/lib/jvm/jre-1.8.0
   #5: LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib:$JAVA_HOME/lib/amd64/server:$ODBCHOME/lib

# Anything in this list will end up in the casconfig.lua file
#   The env section will create a env.VARIABLE in the file
#     Example: env.CAS_DISK_CACHE = '/tmp'
#   The cfg section will create a cas.variable in the file
#     Example: cas.port = 5570
#
# If you have defined hosts for the sas-casserver-worker then the MODE will
# automatically be set to 'mpp'. If the environment variables HADOOP_HOME and
# HADOOP_NAMENODE are set, the COLOCATION option will automatically equal 'hdfs'.
# If HADOOP_HOME and HADOOP_NAMENODE are not set, then the COLOCATION option
# will automatically equal 'none'.

CAS_CONFIGURATION:
   env:
     #CAS_DISK_CACHE: /tmp
     #CAS_VIRTUAL_HOST: 'loadbalancer.company.com'
     #CAS_VIRTUAL_PROTO: 'https'
     #CAS_VIRTUAL_PORT: 443
   cfg:
     #gcport: 0
     #httpport: 8777
     #port: 5570
     #colocation: 'none'
     #SERVICESBASEURL: 'https://loadbalancer.company.com'
```

Note: Indention is part of the file structure, so do not remove leading white space.

End of Demonstration

Practice

12. Exploring SAS Viya Deployment Files

a. Connect to your Windows client machine.

Classroom Course	Live Web Course
Use a remote desktop connection with the IP address that is given to you by the instructor. Sign in with these credentials: User: **Student** Password: **Metadata0**	Use the URL in step 6 of the email that you received from Live Web Administration.

b. Double-click the WinSCP icon from the Windows desktop or Windows taskbar.

Note: You can use **mRemoteNG** to view the inventory.ini and the vars.yml files.

c. Double-click **sas@server** in the Login window. This signs you on to a session with the user ID sas on the server machine where SAS Viya is installed.

d. Navigate to **/workshop/LWSAVA35** to look at a sample inventory.ini file for a multi-machine deployment.

e. Right-click the **inventory_mpp.ini** file and select **Edit** ⇨ **Notepad++.**

Note: In production, the file must be named **inventory.ini** and reside in the playbook directory.

How many machines are in the SAS Viya deployment?

Which machine is the CAS controller? Hint: Find the sas-casserver-primary role.

Is this a distributed CAS environment? Hint: Look at the other CAS roles.

f. Open **/sas/sas_viya_playbook/vars.yml**.

Answer the following questions:

Who is the user that the CAS process will run under?

Who is the group that the user belongs to?

What option is set to True that then creates and sets up SSH keys for users in the sas_users group?

What is the **CAS_DISK_CACHE** set to?

Note: By default, only the **/tmp** directory is used as the cache directory. This is sufficient for demonstration purposes, but not for production use of the server. For production-use servers, set the cache to use a series of directories. The size required differs for each deployment, but can run from gigabytes to terabytes. When you specify a series of directories, each time the server needs to use disk, it uses the next path in the list. This strategy is used to distribute the load across disk volumes.

After deployment, what file will this CAS_CONFIGURATION be located in?

g. Locate **LICENSE_FILENAME** and **LICENSE_COMPOSITE_FILENAME**.

You would replace the current license file name with the corresponding new license file name. (**Note:** The JSON web token license file (.jwt) is also referred to as a *composite license*.) Then you would run the following Ansible command for the default inventory file: **ansible-playbook apply-license.yml**

13. Exploring Configuration Files

Use mRemoteng or Winscp to look at files.

a. Navigate to **/opt/sas/viya/config/etc/cas/default**.

b. Open **casconfig.lua**.

Which account is set as the default CAS superuser?

What is the starting port of the CAS server?

Changes to the options in this file are not to be made directly. Which file would you use to modify settings?

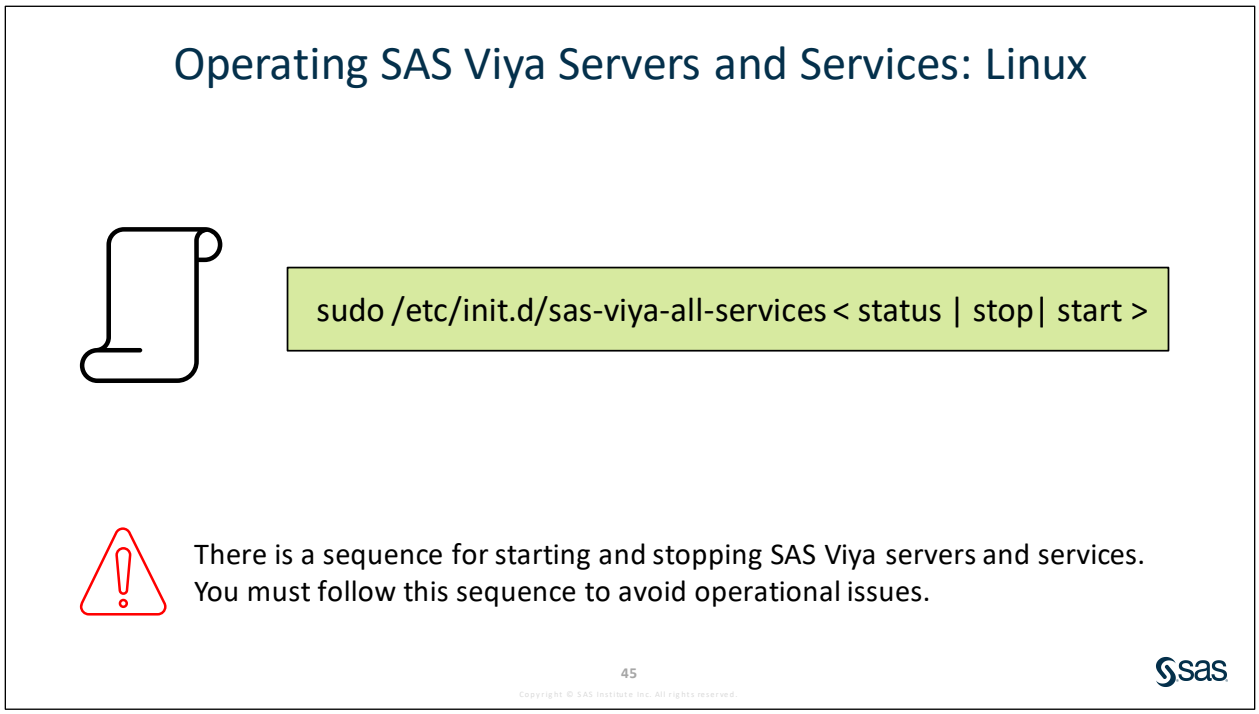
Note: For sites that use Ansible, it is recommended that you make your CAS server configuration changes to **vars.yml** and rerun Ansible to apply these changes. For more information, see “Modify the vars.yml File” in *SAS Viya for Linux: Deployment Guide.*

c. Navigate to **/opt/sas/spre/home/SASFoundation/sasv9.cfg**. Open **sasv9.cfg**.

Where is the location of the SAS Work directory?

End of Practices

1.4 Operating SAS Viya Servers and Services

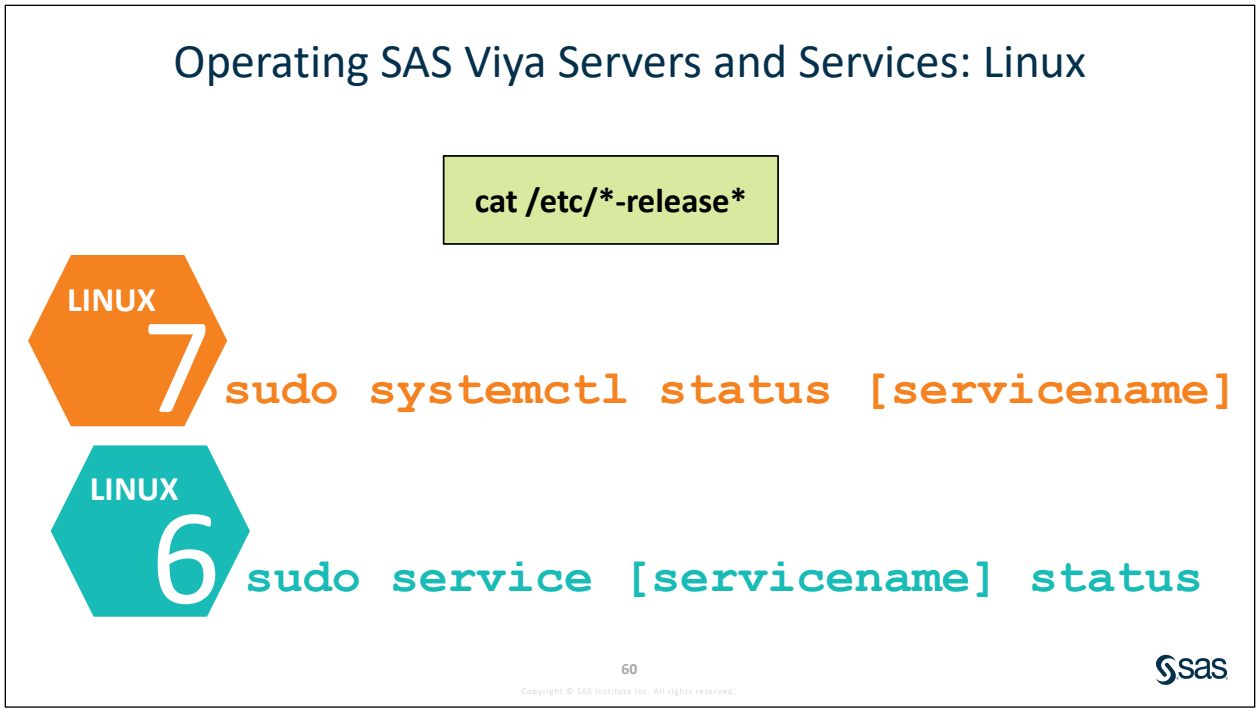


Note: **sas-viya-all-services** does not control the Apache HTTP Server. To operate the Apache HTTP Server, see “Operate” in *SAS® Viya® Administration / Infrastructure Servers*.

Note: Because the SAS Viya service start and stop sequence is so important, a best practice is to record the start and stop order of services for your site.

Individual Linux services are identified by their name and all have the following format:

sas-viya-*service-name*

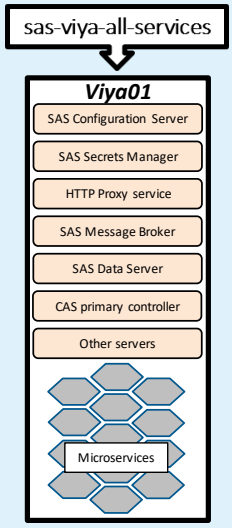


You can start, stop, restart, or display the status of a service with the **systemctl** (Linux 7) or **service** (Linux 6) command:

- sudo systemctl stop |start |restart |status sas-viya-*service-name*
- sudo service sas-viya-*service-name* stop |start |restart |status

Service Name for Server Management	
SAS Configuration Server	**sas-viya-consul-default**
SAS Secrets Manager	**sas-viya-vault-default**
SAS Infrastructure Data Server	**sas-viya-sasdatasvrc-postgres**
SAS Message Broker	**sas-viya-rabbitmq-server-default**
SAS Cache Locator	**sas-viya-cachelocator-default**
SAS Cache Server	**sas-viya-cacheserver-default**
Apache HTTP Server	**httpd** or **sas-viya-http-proxy-default**

Starting Non-distributed SAS Viya



46

There are no issues when a single host SAS Viya deployment is started using ***sas-viya-all-services***.

1.01 Activity

Determine the status of your SAS Viya servers and services.

1. Use mRemoteNG and Christine's terminal session.
2. On the command line enter: **sudo /etc/init.d/sas-viya-all-services status**
3. Verify that your SAS Viya servers and services are up.
4. From where is the status information coming?

47

Special Considerations: Distributed SAS Viya Servers and Services

The start-up and shutdown sequence on each machine is managed by the script, but the script does not span multiple hosts.

Start SAS Configuration Server agents on all CAS hosts before starting the CAS controller service.

49

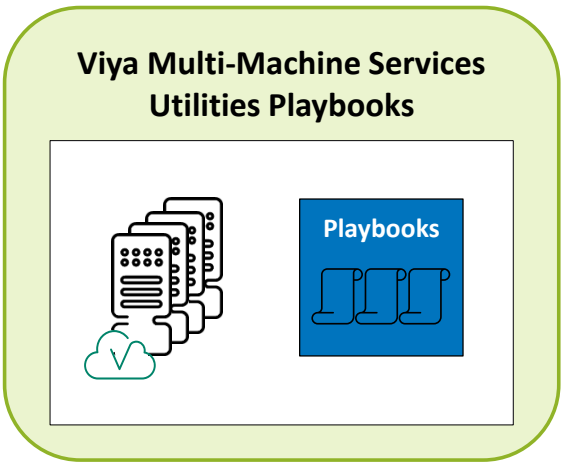
The sas-viya-cascontroller-default service starts the

- CAS Primary Controller
- CAS Secondary Controller
- CAS Worker process on all CAS Worker nodes.

The secondary CAS controller must be included during deployment. If not, it is impossible to add it after the CAS primary controller starts for the first time.

Operating SAS Viya Servers and Services: Linux

Distributed Environment

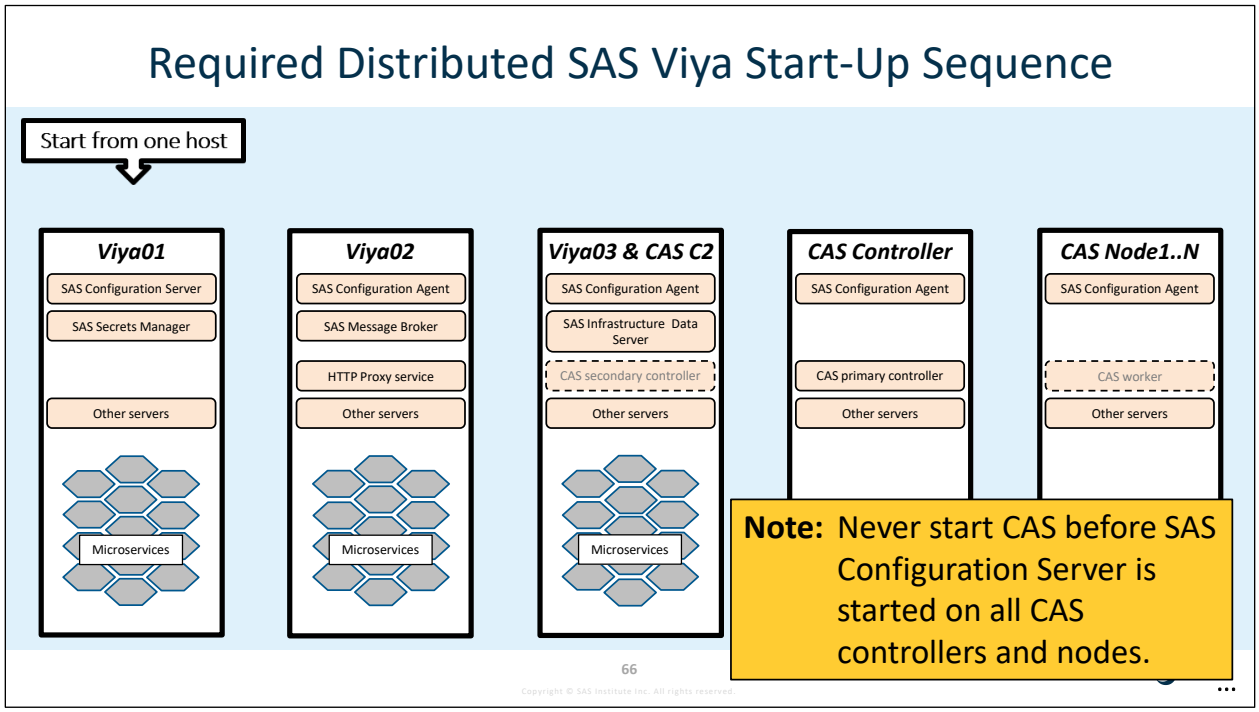


64

The SAS Viya Multi-Machine Services Utilities repository contains a set of playbooks to start or stop the SAS Viya services gracefully across the 1 - n machines that are identified in the inventory.ini file.

Note: For a single machine Windows deployment, the SAS Services Manager service is installed at deployment in the Microsoft Management Console and is used to start and stop all SAS Viya servers and services in the proper sequence. The service is configured to start automatically.

For more information, see the course extended learning page.



Services must be started in this order:

1. Primary SAS Configuration Server on the host designated in the inventory.ini file
2. Non-primary SAS Configuration Server on all others hosts
3. SAS Secrets Manager
4. SAS Message Broker
5. SAS Infrastructure Data Server service
6. HTTP Proxy service (required for the CAS server to start)
7. Other remaining services that depend on previous servers.

The SAS Configuration Server and SAS Secrets Manager must be deployed on the same host.

If SAS Secrets Manager, SAS Message Broker, and other services were deployed in high-availability mode, always start the primary service before the secondary service. This order matches the order specified in the inventory file.

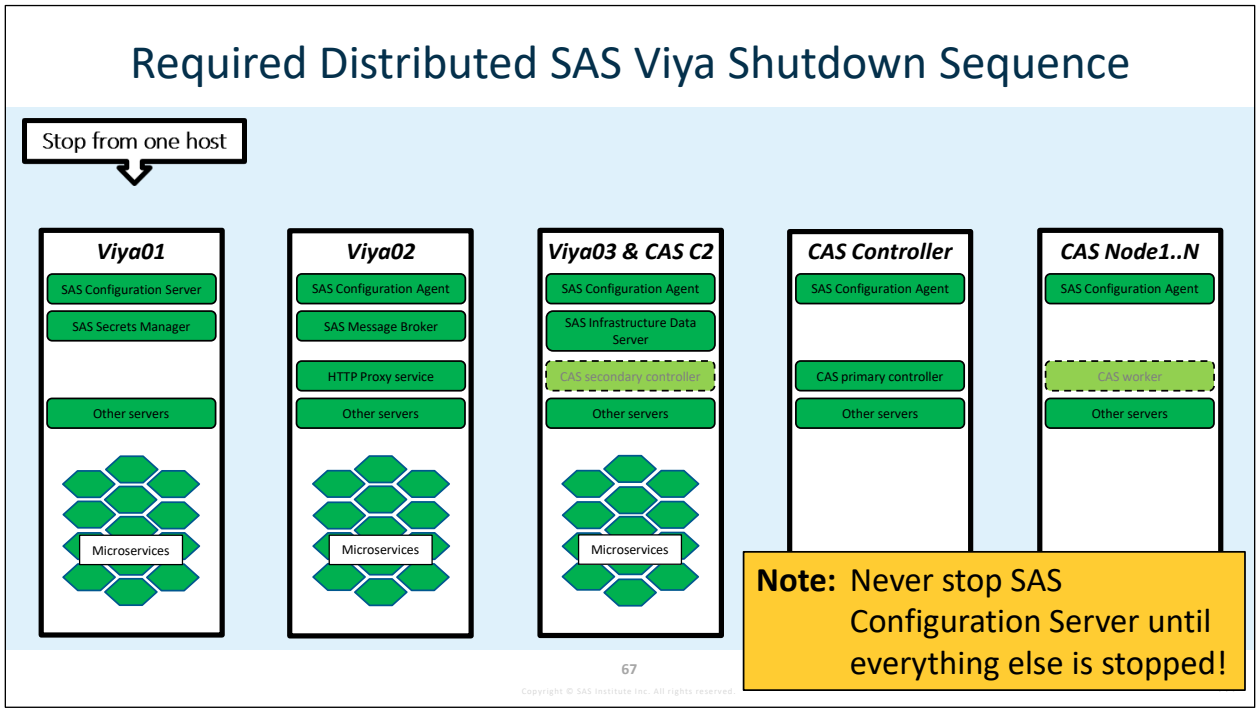
HTTP proxy service is not documented as a required service in start-up sequence, but it is required for the CAS server to start. If the HTTP proxy service is not started, the CAS server fails to start.

Below are some artifacts created at start-up. These are usually deleted when services stop gracefully. However, artifacts left over from an ungraceful shutdown might prevent services from restarting.

- Service PID files:

  A file containing the service process ID (pid) that is created at start-up and stored in a well-defined location in the file system. The PID file is used to locate the service process. They are named **sas-viya-<*serviceName*>-<*instance*>.pid** and located in **/var/run/sas**.
- Third-party software PID files are PostgreSQL:
  - node0: /opt/sas/viya/config/data/sasdatasvrc/postgres/node0/postmaster.pid
  - pgpool0: /opt/sas/viya/config/data/sasdatasvrc/postgres/pgpool0/run/pgpool.pid
  - RabbitMQ: /opt/sas/viya/config/var/run/rabbitmq-server/sas-viya-rabbitmq-server-default.pid
- Service lock files: An empty file created by a service at start-up and stored in a well-defined location in the file system. Lock files are used by the system to manage the host shutdown. They are named **sas-<*deployment*>-<*serviceName*>-<*instance*>** and located in **/run/lock/subsys/**.

If a service does not start or stop as expected, check the log for the respective service in **/opt/sas/viya/config/var/log/**.

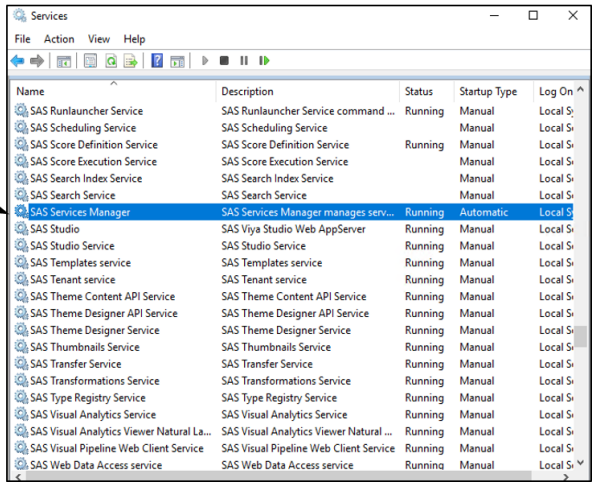


1. All servers and services on machines that do not contain SAS Configuration Servers, SAS Secret Manager, or SAS Infrastructure Data Server.
2. HTTP Proxy service
3. SAS Infrastructure Data Server
4. SAS Message Broker
5. SAS Secrets Manager
6. SAS Configuration Server agents
7. SAS Configuration Server

Additional Information: Operating SAS Viya Servers and Services on Windows

Services snap-in in Microsoft Management

SAS Services Manager



For a single machine Windows deployment, the SAS Services Manager service is installed at deployment in the Microsoft Management Console and is used to start and stop all SAS Viya servers and services in the proper sequence. The service is configured to start automatically.

Operating SAS Viya Servers and Services

This demonstration shows how to obtain status details about individual SAS Viya servers and services. SAS Viya provides scripts in **/etc/init.d** that you use to stop, start, restart, and check the status of an individual SAS Viya server and service.

How you run the individual server and service scripts depends on your operating system. You can start, stop, restart, or display the status of a service with the **systemctl** command for Red Hat Enterprise Linux 7.*x* (or an equivalent distribution) and SUSE Linux Enterprise Server 12.*x*:

- **sudo systemctl stop |start |restart |status sas-viya-*service-name***

For Red Hat Enterprise Linux 6.*x* (or an equivalent distribution), use the **service** command:

- **sudo service sas-viya-*service-name* stop |start |restart |status**

1. If an mRemoteNG session for **christine** is not started, open one now.
2. From the previous activity, you checked the status of all your servers and services with the **sas-viya-all-services** script. Unlike the individual server and services start scripts, there is only one method for running **sas-viya-all-services**.

   I will run it again to see the names of the individual scripts:

   ```
   sudo /etc/init.d/sas-viya-all-services status
   ```

   Note: Remember that services can be started or stopped only by root or using sudo privileges.

   Note: When you check the status, it is normal for certain servers and services to not display host, port, and PID information. The reason is that these servers and services are not registered with the SAS Configuration Server, including the configuration server itself.
3. Because our deployment is on CentOS7, the **systemctl** command manages individual server and service scripts. Services are identified by their name and have the following format:

   sas-viya-*service-name*

   Check the status of the backup agent with the following command:

   ```
   sudo systemctl status sas-viya-backup-agent-default
   ```
4. Stop and start the backup agent.

   ```
   sudo systemctl stop sas-viya-backup-agent-default
   ```
5. You can use SAS Environment Manager's dashboard to see the status of your services.

   (You might need to click **Return to Application** or sign back in as christine: user **christine**, password **Student1**, and **Assume the SASAdminstrator role**.)
6. The Availability tile at the top left shows Machines, Services, and Service instances as boxes. Because we are running a single node environment, only one machine is shown, and then all the running services. There could be more than one instance of that service.

   All the services should be running, as the green boxes indicate. However, after refreshing, there should be some red boxes, because we stopped the backup agent. This might take a minute to observe.
7. Go back to mRemoteNG and start the backup agent.

   ```
   sudo systemctl start sas-viya-backup-agent-default
   ```

End of Demonstration

Practice

14. Working with SAS Viya Services

In this practice, you use the **service** and **systemctl** commands to stop, start, and determine the status of SAS Viya services. SAS Environment Manager is also used to determine the status of the services.

a. If you are not logged on to the Windows client system, log on. Use the method that you used previously.

b. If an mRemoteNG session for **christine** is not started, open one now.

c. (Optional) Use the **sas-viya-all-services** service to check the status of all the SAS Viya services. (This was done in an activity already.) Enter the following command:

```
sudo service sas-viya-all-services status
```

```
[christine@server sas]$ sudo service sas-viya-all-services status
Getting service info from consul...
  Service                                      Status     Host              Port     PID
  sas-viya-consul-default                      up         N/A                N/A    5161
  sas-viya-sasdatasvrc-postgres-node0-ct-pg_hba  up       N/A                N/A    6362
  sas-viya-sasdatasvrc-postgres-node0-ct-postgresql  up   N/A                N/A    6365
  sas-viya-sasdatasvrc-postgres-pgpool0-ct-pcp  up        N/A                N/A    6359
  sas-viya-sasdatasvrc-postgres-pgpool0-ct-pgpool  up     N/A                N/A    6356
  sas-viya-sasdatasvrc-postgres-pgpool0-ct-pool_hba  up   N/A                N/A    6353
  sas-viya-vault-default                       up         10.96.16.97       8200     N/A
  sas-viya-sasdatasvrc-postgres-node0          up         N/A                N/A   12188
  sas-viya-cascontroller-default               up         N/A                N/A   15155
  sas-viya-connect-default                     up         N/A                N/A    9061
  sas-viya-httpproxy-default                   up         N/A                N/A    8752
  sas-viya-rabbitmq-server-default             up         10.96.16.97       5672    None
  sas-viya-sasdatasvrc-postgres                up         N/A                N/A   13246
                                                                                    
                                                                                    
  sas-viya-monitoring-default                  up         10.96.16.97       43825    7048
  sas-viya-projects-default                    up         10.96.16.97       38902   20381
  sas-viya-sashome-default                     up         10.96.16.97       45189   20484
  sas-viya-sasreportviewer-default             up         10.96.16.97       34477   20511
  sas-viya-sasthemedesigner-default            up         10.96.16.97       43967   30435
  sas-viya-sasvisualanalytics-default          up         10.96.16.97       43473   30447
  sas-viya-tenant-default                      up         10.96.16.97       46448   30543
  sas-viya-themecontent-default                up         10.96.16.97       45085   30614

sas-services completed in 00:00:47
```

Note: Inform the instructor if all the services are not listed.

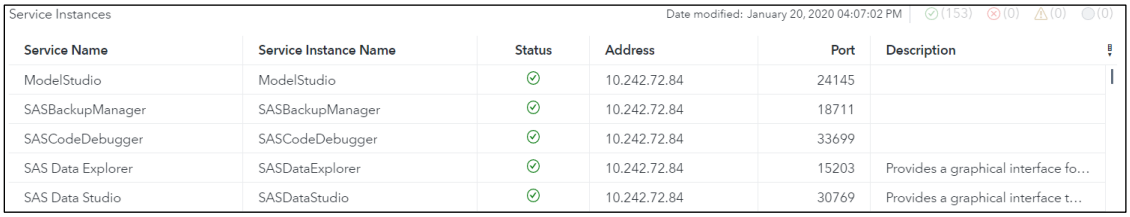
d. Use the **systemctl** command to restart a single service, **sas-viya-tenant-default**.

```
sudo systemctl restart sas-viya-tenant-default
sas-viya-tenant-default is stopped
sas-viya-tenant-default is running
```

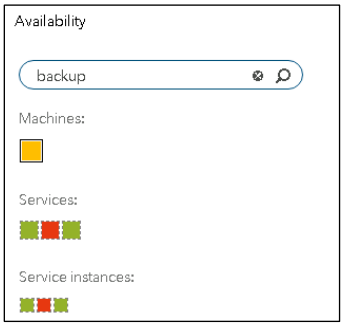
e. Another view of the services indicates the available status with SAS Environment Manager. It is on the Machines page in the Monitor section.

If a SAS Environment Manager session is not started, open one. Sign in as **christine** with a password of **Student1**. Click **Yes** to opt in to the **SASAdministrators** group. Select the **Machines** page.

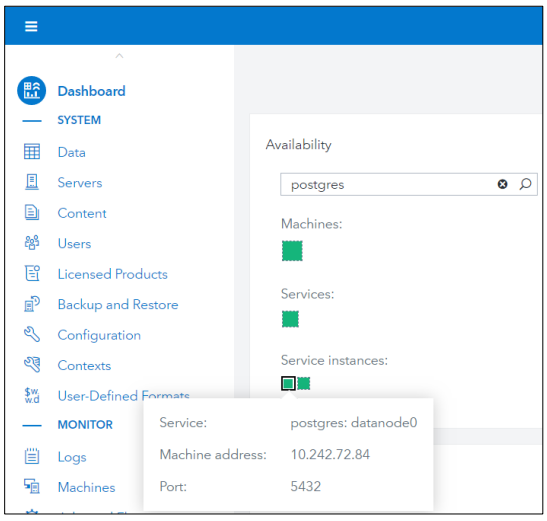
f. At the bottom of the Machine pane, there is a section with **Services Instances**. Scroll through the services. Use the scroll bar on the right side of **Services Instances** to confirm that all the services are running. There should be a green checkmark in the Status column for all the services.



g. Go back to the Dashboard page and search on **backup**. There are three backup services and three backup service instances. If you place your mouse pointer over each of the three services, you see **SAS Backup Manager**, **backup-agent**, and **Backup service**. If you place your mouse pointer over the three service instances, you see **SASBackupManager**, **backup-agent**, and **deploymentBackup**.



h. Go to the Search box and replace **backup** with **postgres**. The SAS Infrastructure Data Server is a PostgreSQL database server. In this case there is one service, the SAS Infrastructure Data Server, and two Postgres database service instances that run on different ports, 5431 and 5432.



i. Delete **postgres** from the Search box.

End of Practices

1.5 Solutions

Solutions to Practices

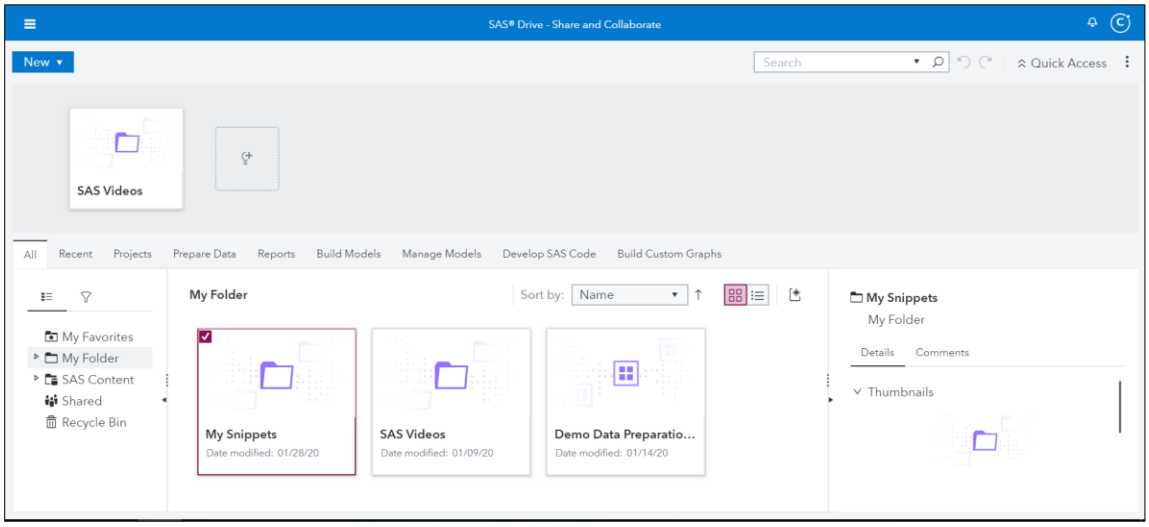
1. Exploring the SAS Environment Manager Dashboard

a. Connect to your Windows client machine.

Classroom Course	Live Web Course
Use a remote desktop connection with the IP address that is given to you by the instructor. Sign in with these credentials: User: **Student** Password: **Metadata0**	Use the URL in step 6 of the email that you received from Live Web Administration.

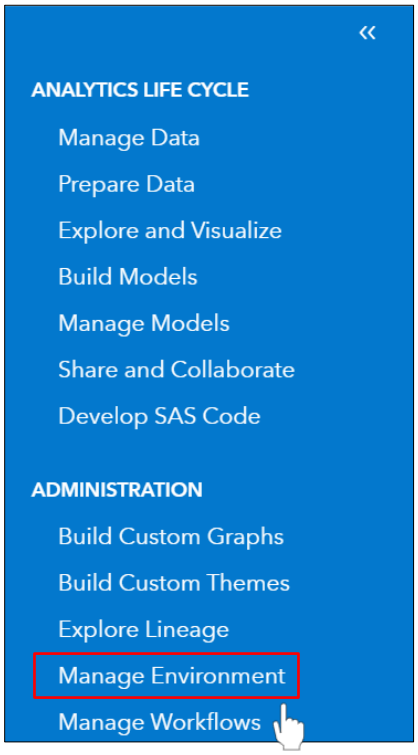
b. Open a Chrome browser window and select **SAS Drive** on the Bookmarks toolbar.

c. Sign in as the user **christine** with a password of **Student1**. Click **Yes** to opt in to the SASAdministrators group.



d. To access SAS Environment Manager, click the applications menu in the upper left and select **Manage Environment**.

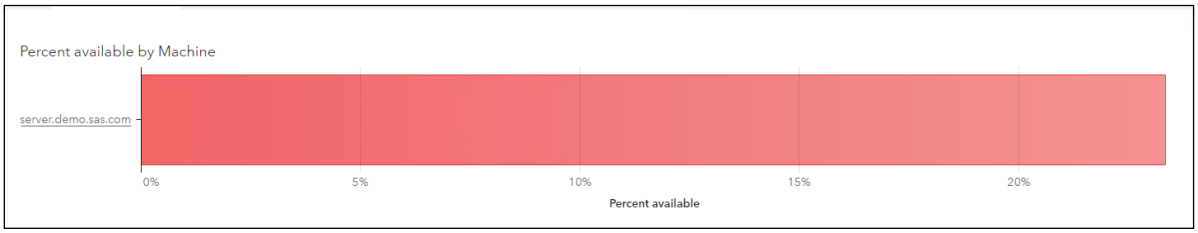
(There is a bookmark for SAS Environment Manager if you want to go directly to the interface.)



e. Select **Show Reports** on the top right portion of the SAS Environment Manager dashboard.

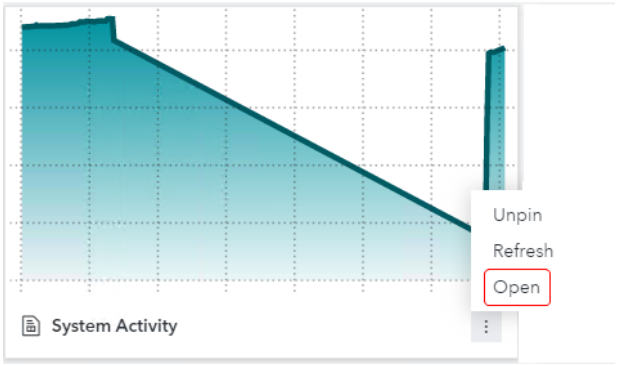
f. On the Disk Space report, select the **More Options** menu and select **Open**.

g. Select the **Storage Dashboard**. What is the percentage of free space on the machine? **23%**

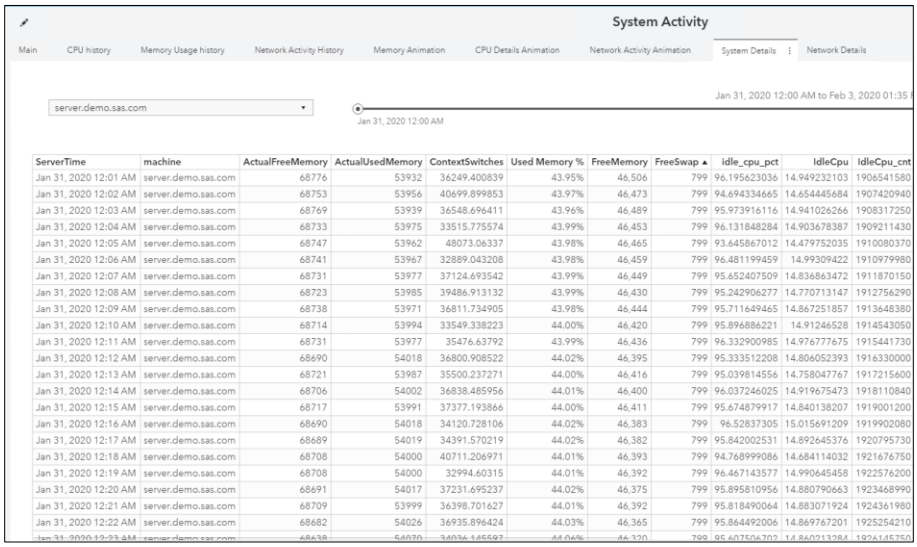


h. Select **Manage Environment** from the side menu to return to SAS Environment Manager.

i. Open the **System Activity** Report. (Click the **More Options** icon ⇨ the three vertical black dots ⇨ **Open**.)

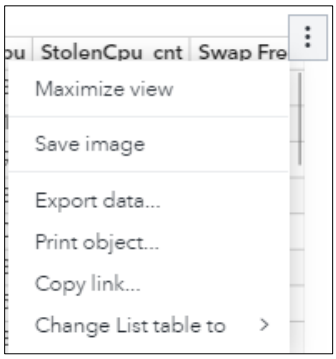


j. Click the **System Details** tab.



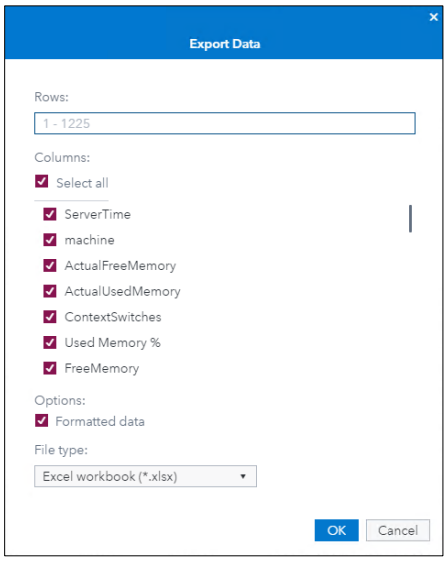
ServerTime	machine	ActualFreeMemory	ActualUsedMemory	ContextSwitches	Used Memory %	FreeMemory	FreeSwap	idle_cpu_pct	IdleCpu	IdleCpu_cnt
Jan 31, 2020 12:01 AM	server.demo.sas.com	68776	53932	36249.400839	43.95%	46,506	799	96.195623036	14.949232103	1906541580
Jan 31, 2020 12:02 AM	server.demo.sas.com	68753	53956	40699.899853	43.97%	46,473	799	94.694334665	14.654445684	1907420940
Jan 31, 2020 12:03 AM	server.demo.sas.com	68769	53939	36548.696411	43.96%	46,489	799	95.973916116	14.941026266	1908317250
Jan 31, 2020 12:04 AM	server.demo.sas.com	68733	53975	33515.775574	43.99%	46,453	799	96.131848284	14.903678387	1909211430
Jan 31, 2020 12:05 AM	server.demo.sas.com	68747	53962	48073.06337	43.98%	46,465	799	93.645867012	14.479752035	1910080370
Jan 31, 2020 12:06 AM	server.demo.sas.com	68741	53967	32889.043208	43.98%	46,459	799	96.481199459	14.99309422	1910979980
Jan 31, 2020 12:07 AM	server.demo.sas.com	68731	53977	37124.693542	43.99%	46,449	799	95.652407509	14.836863472	1911870150
Jan 31, 2020 12:08 AM	server.demo.sas.com	68723	53985	39486.913132	43.99%	46,430	799	95.242906277	14.770713147	1912756290
Jan 31, 2020 12:09 AM	server.demo.sas.com	68738	53971	36811.734905	43.98%	46,444	799	95.711649465	14.867251857	1913648380
Jan 31, 2020 12:10 AM	server.demo.sas.com	68714	53994	33549.338223	44.00%	46,420	799	95.896886221	14.91246528	1914543050
Jan 31, 2020 12:11 AM	server.demo.sas.com	68731	53977	35476.63792	43.99%	46,436	799	96.332900985	14.976777675	1915441730
Jan 31, 2020 12:12 AM	server.demo.sas.com	68690	54018	36800.908522	44.02%	46,395	799	95.333512208	14.806052393	1916330000
Jan 31, 2020 12:13 AM	server.demo.sas.com	68721	53987	35500.237271	44.00%	46,416	799	95.039814556	14.758047767	1917215600
Jan 31, 2020 12:14 AM	server.demo.sas.com	68706	54002	36838.485956	44.01%	46,400	799	96.037246025	14.919675473	1918110840
Jan 31, 2020 12:15 AM	server.demo.sas.com	68717	53991	37377.193866	44.00%	46,411	799	95.674879917	14.840138207	1919001200
Jan 31, 2020 12:16 AM	server.demo.sas.com	68690	54018	34120.728106	44.02%	46,383	799	96.52837305	15.015691209	1919902080
Jan 31, 2020 12:17 AM	server.demo.sas.com	68689	54019	34391.570219	44.02%	46,382	799	95.842002531	14.892645376	1920795730
Jan 31, 2020 12:18 AM	server.demo.sas.com	68708	54000	40711.206971	44.01%	46,393	799	94.768999086	14.684114032	1921676750
Jan 31, 2020 12:19 AM	server.demo.sas.com	68708	54000	32994.60315	44.01%	46,392	799	96.467143577	14.990645458	1922576200
Jan 31, 2020 12:20 AM	server.demo.sas.com	68691	54017	37231.695237	44.02%	46,375	799	95.895810956	14.880790663	1923468990
Jan 31, 2020 12:21 AM	server.demo.sas.com	68709	53999	36398.701627	44.01%	46,392	799	95.818490064	14.883071924	1924361980
Jan 31, 2020 12:22 AM	server.demo.sas.com	68682	54026	36935.896424	44.03%	46,365	799	95.864492006	14.869767201	1925254210

k. View your options by clicking the three vertical black dots that appear when you place your pointer in the upper right corner of the data.

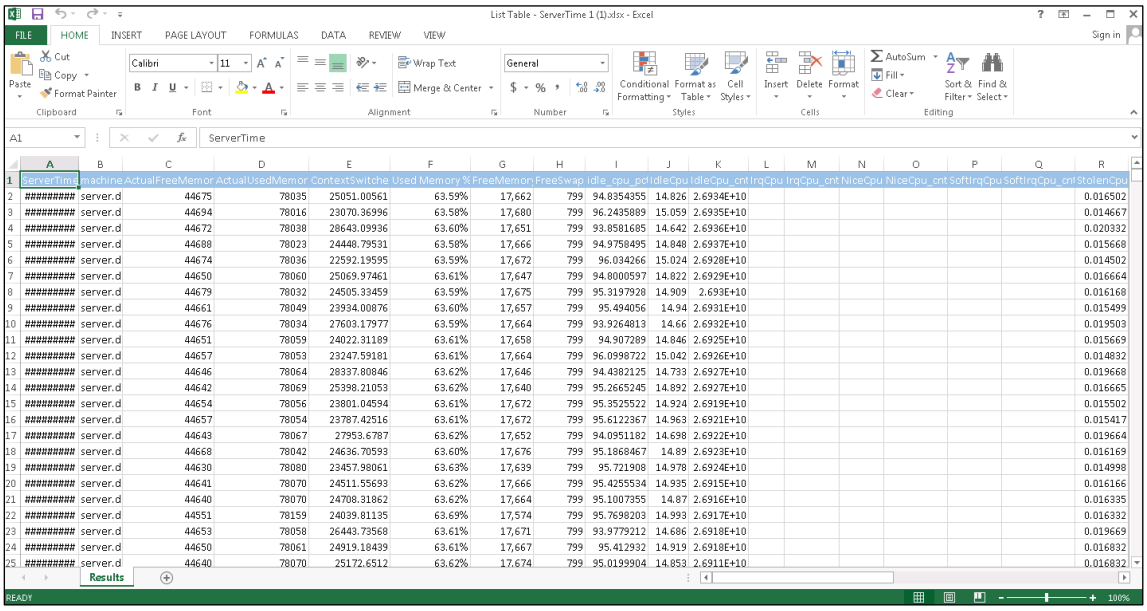


l. Choose **Export data**.

m. Keep all default columns and click **OK**.



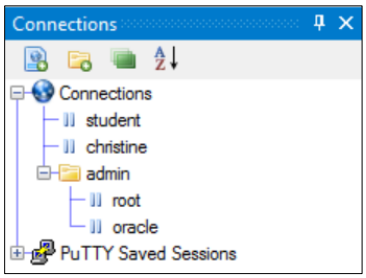
n. This is downloaded to the Downloads directory as an MS Excel file by default. You can click **List Table – ServerT….xlsx** in the lower left corner to open the file.



2. Introducing the Administrative Command Line Interface

a. Open **mRemoteNG** by double-clicking the icon on the desktop.

b. Open the **christine** connection in the mRemoteNG connections list.



c. Navigate to **/opt/sas/viya/home/bin**.

```
cd /opt/sas/viya/home/bin
```

d. You must complete the required preliminary tasks before you use the CLI.

The classroom environment is not enabled for Transport Layer Security (TLS). However, go through the step to set SSL_CERT_FILE to the default location of the trustedcerts.pem file.

1) Issue the following command: **export SSL_CERT_FILE=/opt/sas/viya/config/etc/SASSecurityCertificateFramework/cacerts/trustedcerts.pem**.

```
export
SSL_CERT_FILE=/opt/sas/viya/config/etc/SASSecurityCertifica
teFramework/cacerts/trustedcerts.pem
```

2) Issue the following command: ./**sas-admin profile init**

```
./sas-admin profile init
```

Enter the configuration options:
Service Endpoint: **http://server** (https://<*host_path*>:443 is standard)
Output type (text|json|fulljson): **json**
Enable ANSI colored output (y/n)?: **n**

```
[christine@server SASFoundation]$ cd /opt/sas/viya/home/bin
[christine@server bin]$ ./sas-admin profile init
Enter configuration options:

Service Endpoint> http://server

Output type (text|json|fulljson)> json

Enable ANSI colored output (y/n)?> n
Saved 'Default' profile to /home/christine/.sas/config.json.
```

3) Initiate the sign-in process by using the **sas-admin** command: **./sas-admin auth login**

```
./sas-admin auth login
```

Enter the credentials for Christine: **christine** and **Student1**

Note: By default, your authentication remains active for 12 hours. You can use the **auth logout** command to sign out.

```
[christine@server bin]$ ./sas-admin auth login
Enter credentials for http://server:

Userid> christine

Password>
Login succeeded. Token saved.
[christine@server bin]$
```

e. Issue the following command to obtain help using the CLI: **./sas-admin help**

```
./sas-admin help
```

```
[christine@server bin]$ ./sas-admin help
NAME:
   sas-admin - SAS Administrative Command Line Interface

USAGE:
   sas-admin [global options] command [command options] [arguments...]

VERSION:
   1.1.11

COMMANDS:
   authenticate, auth, authn    Handles authentication to the target environment.
   help, h                      Shows a list of commands or help for one command.
   plugins                      Manages plugins.
   profile, prof                Shows and updates options.

PLUGINS:
   audit
   authorization
   backup
   cas
   configuration
   devices
   folders
   fonts
   identities
   job
   launcher
   licenses
   qkbs
   reports
   restore
   tenant
   transfer
```

f. Use the CLI to view the users and groups in your SAS Viya environment. How many users are there? **29**

```
[christine@server bin]$ ./sas-admin identities
NAME:
   sas-identities

USAGE:
   sas-admin identities command [command options] [arguments...]

COMMANDS:
   add-member           Adds a new member to a group.
   create-group         Creates a new group.
   delete-group         Deletes the specified group.
   help, h              Shows a list of commands or help for one command.
   list-groups          Lists the groups that are defined in the SAS system.
   list-members         Lists the members of the group.
   list-memberships     Lists the memberships in which the entity belongs.
   list-users           Lists the users that are defined in the SAS system.
   refresh-cache        Refreshes users and groups in the internal cache.
   remove-member        Deletes the specified member from an existing group.
   show-group           Shows details about a particular group.
   show-user            Shows details about a particular user.
   update-group         Updates information about an existing group.
   whoami               Shows details about the current user
```

How many members are in the SAS Administrators group? **2**

```
./sas-admin identities list-members --group-id SASAdministrators
```

```
[christine@server bin]$ ./sas-admin identities list-members --group-id SASAdministrators
Id          Name        Type
ahmed       Ahmed       user
christine   Christine   user
```

3. Reviewing Product License Information in SAS Environment Manager

Explore license information through SAS Environment Manager.

If you are not already in SAS Environment Manager, open SAS Drive, sign in as the user **christine** with a password of **Student1**. Click **Yes** to opt in to the SASAdministrators group, and click **Manage Environment** from the drop-down side menu.

a. Click **Licensed Products** from the left navigation menu.

Note: The Licensed Products page is an advanced interface. It is available only to SAS administrators.

b. How many products are licensed? **179**

Hint: Look for the number in parentheses at the top of the window.

c. Examine the **Status** column by scrolling through the list.

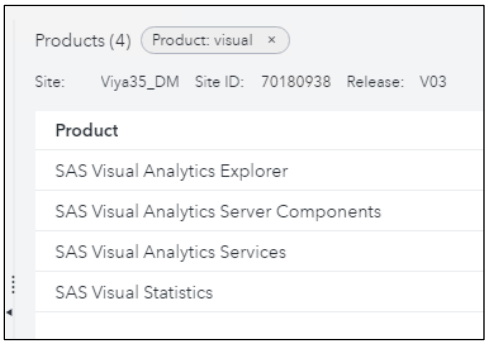
Are any of the products expired or about to expire? **No, they are all set to expire December 30, 2023.**

Use the table below to help determine the effective license status of each product.

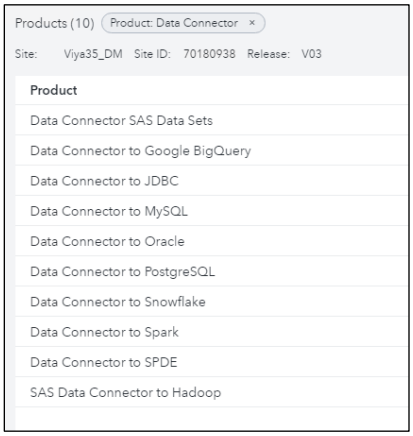
For each product, the following icons depict the effective license status:
The SAS license is current.
The SAS license is due for renewal (grace period). The grace period is a predetermined range of days immediately after the license expiration date. For example, if the expiration date is 30 June, the grace period might extend 45 days: from 1 July - 14 August.
The SAS license is about to expire (warning period). The warning period is a predetermined range of days that follows the grace period. For example, if the expiration date is 30 June, the warning period might extend 56 days: from 15 August - 09 October.
The SAS license has expired. License expiration occurs immediately after the warning period ends. An expired license means that SAS does not run. For example, if the warning period ends on 09 October, SAS stops running at 12:00 a.m. on 10 October.

d. Examine the **Status** section of the filters on the left side of the window. Does the number next to **License is current** match the number from step **b**? **Yes, the numbers are both 179.**

e. In the Product section of the filters, enter **Visual** in the field and click **Enter**. How many products that contain the string *Visual* are licensed? **Four products are licensed for *visual*.**



f. Click **Reset** in the Product filter to remove **Visual**, enter **Data Connector** and click **Enter**. How many Data Connector licenses exist? **Ten products are licensed for *Data Connector*.**

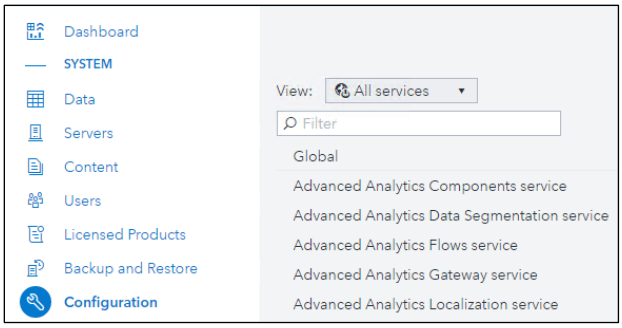


4. (Optional) Changing the Default Expiration for the CLI Token

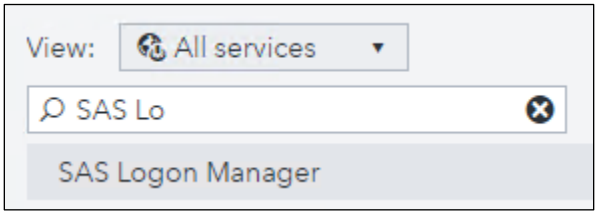
You can change the default expiration for all tokens issued by the system.

a. Sign in to SAS Environment Manager as **christine** with the password **Student1**. Assume the SASAdministrator role.

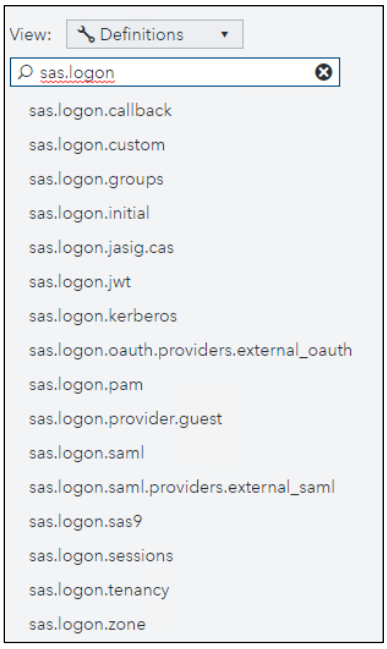
b. Select **Configuration** area ⇨ **All services** from the **View** drop-down menu.



c. Select **SAS Logon Manager**.



d. Click **New Configuration** ⇨ **sas.logon.jwt**.

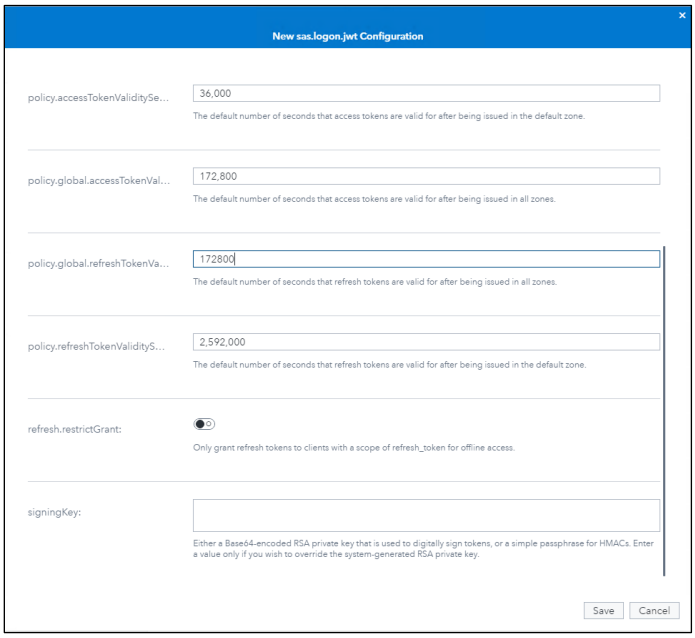


e. The default time out for the access token is 12 hours and it is displayed in seconds for the following attributes:

policy.accessTokenValiditySeconds

policy.global.accessTokenValiditySeconds

Change to values to **172800** for a time-out of 48 hours.



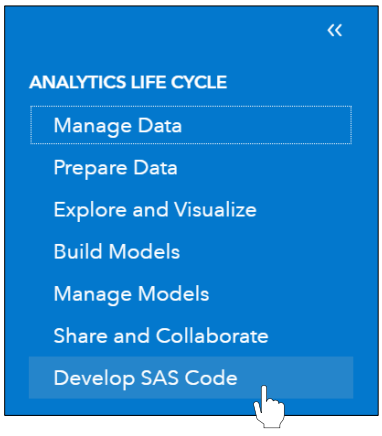
f. Click **Save**.

g. Restart the SASLogon service for the changes to be applied.

```
sudo systemctl restart sas-viya-saslogon-default
```

5. Viewing License information using SAS Studio

a. From SAS Environment Manager, click the applications menu in the upper left and select **Develop SAS Code**.



You can also access SAS Studio by entering the appropriate URL:
http://*server*/SASStudioV

b. Create a New SAS Program, and enter the following command:

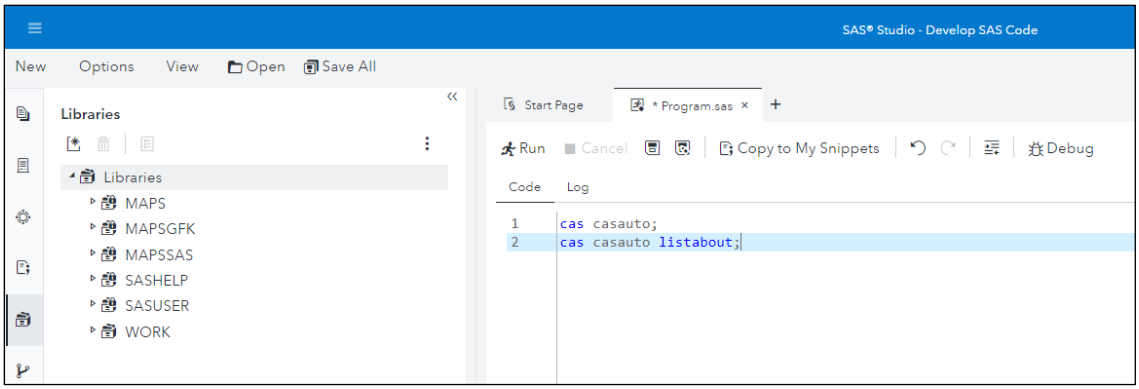
```
proc setinit; run;
```

c. Click the **Run** icon . The log displays the licensed products in this deployment.

There are various methods to get information about CAS and license information for your SAS Viya deployments.

d. Go back to the Code section, delete the PROC SETINIT code, and enter the following code:

```
cas casauto;
cas casauto listabout;
```



e. Click the **Run** icon . The log displays SAS Cloud Analytic Services license information.

6. Using the CLI to Find License Information

Use the command-line interface (CLI) to examine the SAS Viya environment license information.

a. Use the **christine** connection in the **mRemoteNG** connections list.

b. Using the Linux **cd** command, navigate to the bin directory in the SAS Viya Home directory. The sas-admin CLI "host" is found here.

```
cd /opt/sas/viya/home/bin
```

c. Issue the following command:

```
./sas-admin licenses count
```

Does the CLI output agree with the SAS Environment Manager on the number of licensed products?

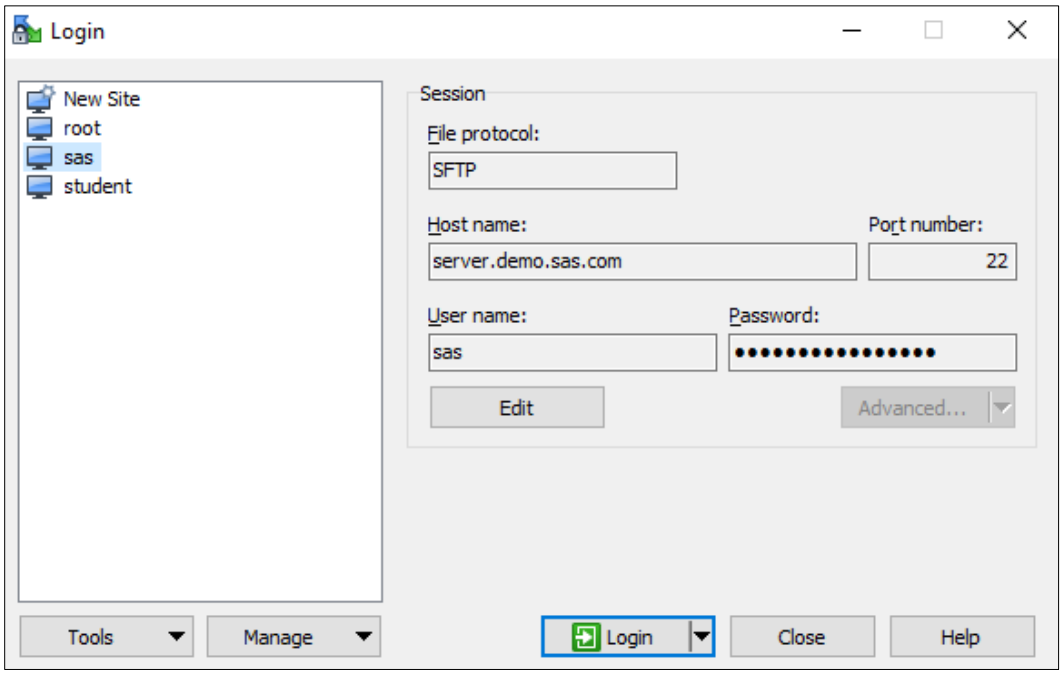
```
[student@server bin]$ ./sas-admin licenses count
There are 179 products licensed.
```

7. Examining the SAS Viya Configuration Directory

In this practice, you examine the SAS Viya configuration directory. Use WinSCP to discover some key locations that are important to administrators in the configuration.

a. Double-click the **WinSCP** icon from the Windows desktop or Windows taskbar.

b. Double-click **sas** in the Login window.



This signs you on to a session with the user ID **sas** on the server machine where SAS Viya is installed. The current directory is **/opt/sas/viya**, which is displayed on the right side of the WinSCP window.

c. Navigate to **/opt/sas/viya/home.**

These are the directories for the SAS Viya binaries. Because this is a single-machine deployment, all SAS binaries are located here.

- An optional product, SAS Event Stream Processing, was installed on this machine.
- The SASSecurityCertificateFramework directory contains security certificate files, the key files, the trustedcerts files, and certificate chain files that are included in each of the directories for the CAS Server.

d. Navigate to **/opt/sas/viya/config/etc**.

The etc directory is where the various SAS Viya servers are configured. You can find configuration files for each server in its associated directory.

- What directory contains the CAS Server? **cas**
- What directory contains the SAS Studio web application? **sasstudio**
- What directory contains the SAS Object Spawner? **spawner**
- What directory contains the Apache HTTP Web Server? **httpd**

e. Navigate to **/opt/sas/viya/config/etc/cas/default**.

f. Double-click the **casconfig.lua** file.

What is the deployment_id of this deployment? **viya**

Who is the default CAS Superuser? **cas**

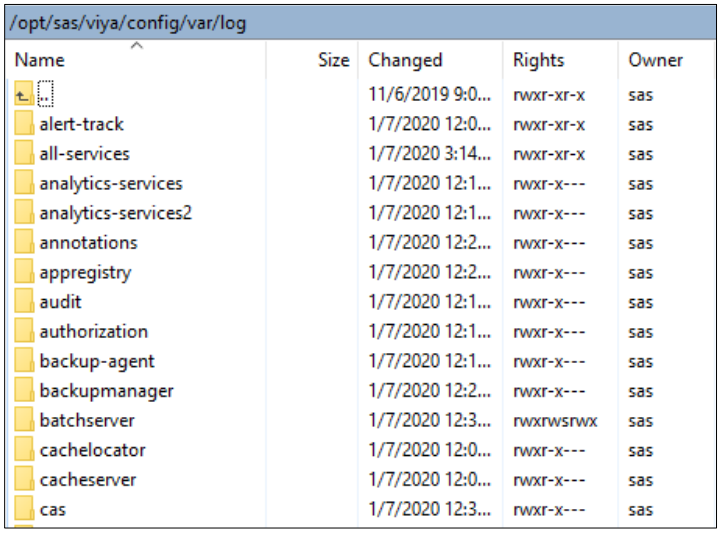
What port does the CAS server run on? **5570**

```
-- unique id for the deployment of SAS
sas_deployment_id = 'viya'

-- root path for the installation
-- Used in the default perms.xml
env.SAS_ROOT_PATH = '/opt/sas/' .. sas_deployment_id

-- For the times when the SAS_ROOT_PATH could point to a different location
--    and we still need to know the Viya location.
-- Used in the default perms.xml
env.SAS_VIYA_ROOT_PATH = '/opt/sas/' .. sas_deployment_id

-- default CAS super user used in perms.xml
env.ADMIN_USER = 'cas'

-- unique id for the deployment of CAS
current_dir = debug.getinfo(1).source:match("@?(.*/)")
deployment_instance = string.gsub(string.sub(current_dir, 1, -2), "(.*/)(.*)", "%2")
config_loc = current_dir

-- The SAS license file
env.CAS_LICENSE = config_loc .. '/sas_license.txt'

-- Define the instance_id which is used in the log configuration
env.INSTANCE_ID = deployment_instance

-- The logpath that is used by the logconfig.xml in config_loc
env.LOG_PATH = config_loc .. '../../../var/log/cas/' .. env.INSTANCE_ID
```

```
-- The logpath that is used by the EV log scraping utility
env.SAS_RESOURCE_LOG_PATH = config_loc .. '../../../var/log/cas/' .. env.INSTANCE_ID .. '_audit'

-- The location where default CAS libs are created
-- Used in the default perms.xml
env.CASDATADIR = config_loc .. '../../../data/cas/' .. env.INSTANCE_ID

-- The 'hdfsuserloc' option specifies a personal caslib to create for each
-- user at session start-up and references a HDFS path.
--  %USER - is substituted for username.
----------------------------------------------------------------------------
cas.hdfsuserloc = '/user/%USER'


-- The 'port' option determines the starting port number of the CAS server
-- This generally is always set as to avoid using an ephemeral port (read as
-- different) port with each invocation.
----------------------------------------------------------------------------
cas.port = 5570

-- The 'gcport' option determines the communicator port for the CAS server
----------------------------------------------------------------------------
cas.gcport = 0


-- The 'httpport' option will setup the internal HTTP server port for
-- Cloud Analytic Services Monitor.
-- Either a port value or a port range are accepted inputs.
----------------------------------------------------------------------------
cas.httpport = 8777
--cas.httpport = 8777-9000

-- The 'httpportmax' option allows for specifying the maximum port range
-- as a separate option.  (see 'httpport')
----------------------------------------------------------------------------
--cas.httpportmax = 9000
```

g. Navigate to **/opt/sas/viya/config/var/log**.

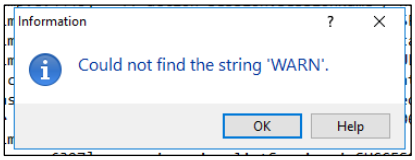
The log directory is where the logs for the servers and services are located. SAS Viya uses the log4j logging protocol. Log files are organized by product in this log directory. The default system logging location of **/var/log/sas/viya** is a link to this directory.



h. Navigate to the CAS server log directory: **/opt/sas/viya/config/var/log/cas/default**

i. Click the **Changed** column to sort by date so that the most recent CAS server log file is at the top.

Double-click to view it. Most of the messages should be INFO-level messages. Are there WARN- or ERROR-level messages? **This will depend on the status of your system!**



8. Using the Command-Line Interface (CLI) to Examine the Environment

a. In mRemoteNg, navigate to **/opt/sas/viya/home/bin**.

The **sas-ops** command is used to run operations infrastructure tasks that will be discussed in a later lesson. It provides information about your SAS Viya environment, including the services, the machines, and the environment.

You must be the SAS install user (sas) to run the command:

```
su sas
```

b. Enter **Student1** for the password.

c. Run the **sas-ops** command with **--help**:

```
./sas-ops --help
```

```
[christine@server bin]$ ./sas-ops --help

NAME:
  sas-ops - SAS Operations command line interface

USAGE:
  sas-ops [global options] command [arguments...]

VERSION:
  1.4.27

COMMANDS:
  alerts          Stream alerts or show the most recent alerts
  datamarts       Display data mart information
  env             Display summary of relevant environment information
  info            Display properties of the components of the deployment
  logs            Streams log events
  metrics         Streams metric events
  notifications   Streams notification events
  notify          Publish a notification message
  services        Lists services, service details, and health
  tasks           Lists tasks defined for sas-ops-agent
  validate        Performs validation of the deployment
  help            Show usage

GLOBAL OPTIONS:
  --colors-enabled    Enable color output (default true)
  --consul address    Consul agent address (http[s]://hostname:port) [$CONSUL_HTTP_ADDR]
  --debug             Enable debug logging
  --insecure          Allow connections to TLS sites without validating the server certificates
  --locale locale     Specify a locale to use (currently 'en-US')
  --token token       Consul ACL token [$CONSUL_TOKEN]
  --token-file file   Path to a file that contains a Consul ACL token [$CONSUL_TOKEN_FILE]
  --version           Display version information
```

d. Use the **env** command to view information for the machine.

```
./sas-ops env
```

```
[christine@server bin]$ ./sas-ops env
Host Information:
  Full hostname             : server.demo.sas.com
  Short hostname            : server
  Consul node name          : server.demo.sas.com

SAS environment variables:
  CONSUL_CACERT    = /opt/sas/viya/config/etc/SASSecurityCertificateFramework/cacerts/trustedcerts.pem
  CONSUL_HTTP_ADDR = https://localhost:8501

SAS Viya Deployment:
  Site Environment ID       :
  Install user              : sas
  Deployment ID             : viya
  Tenant ID                 : provider
  Home directory            : /opt/sas/viya/home
  Config directory          : /opt/sas/viya/config
  Log directory             : /opt/sas/viya/config/var/log
  Temp directory            : /opt/sas/viya/config/var/tmp
  Spool directory           : /opt/sas/viya/config/var/spool
  SAS executable            : /opt/sas/spre/home/SASFoundation/sas
```

e. Use the **info** command to view properties of the components of the machine.

```
./sas-ops info
```

```
[sas@server bin]$ ./sas-ops info
server.demo.sas.com
   common
      architecture : amd64
      boot-time : 2020-01-29T11:40:56.000000-05:00
      hostname-long : server.demo.sas.com
      hostname-short : server
      ip-addrs : 10.242.98.98,10.242.98.98
      last-update : 2020-01-29T11:57:13.103821-05:00
      memory-total : 128668790784
      operating-system : linux
      timezone : EST
      timezone-offset : -05:00
   linux
      kernel-release : 3.10.0-957.27.2.el7.x86_64
      kernel-version : #1 SMP Mon Jul 29 17:46:05 UTC 2019
      operating-system-release : CentOS Linux release 7.6.1810 (Core)
      packages
         sas-aacomp1 : sas-aacomp1-01.20.00-20191104.231512463969.x86_64
         sas-aastatistcs1 : sas-aastatistcs1-03.21.00-20191104.2315124270
```

9. Creating, Viewing, and Terminating Three CAS Sessions

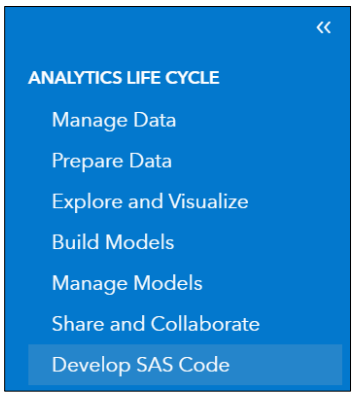
In this practice, you use a SAS Studio snippet to launch three CAS sessions. Use SAS Environment Manager and the CLI to terminate them. (You are repeating the demonstration.)

a. Click **SAS Drive** on the Bookmarks toolbar from Mozilla Firefox browser. (A shortcut to the browser is found on the Windows taskbar.)

b. Sign in to SAS Drive as **eric** with the **Student1** password.

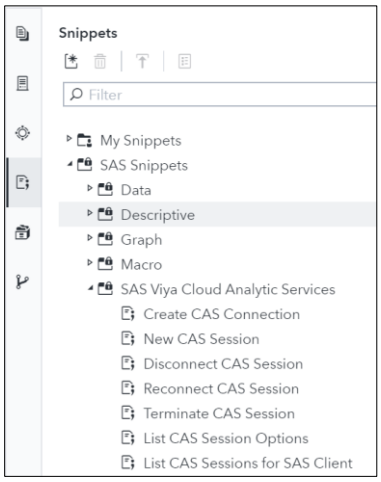
c. Click **Skip setup if** necessary to continue to SAS Drive.

d. From the applications menu, select **Develop SAS Code**, which brings up SAS Studio.

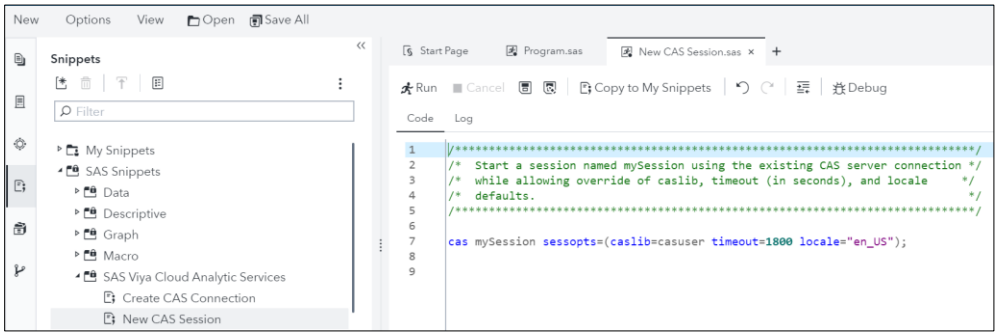


e. Click **Snippets**  in the left pane.

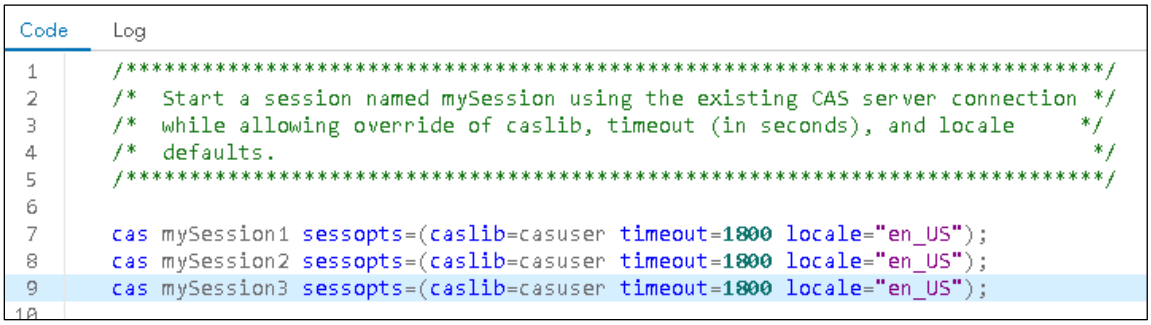
f. Expand **SAS Snippets** ⇨ **SAS Viya Cloud Analytic Services**.



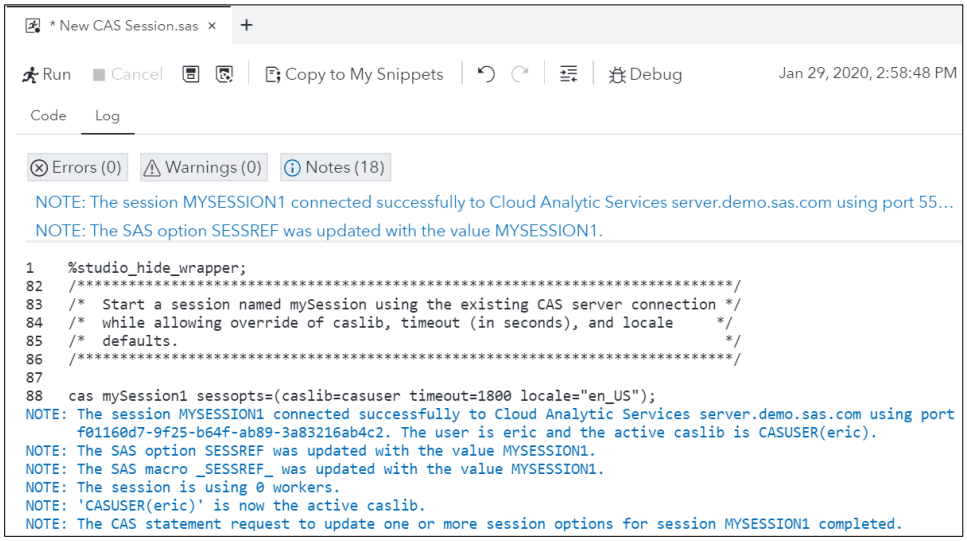
g. Double-click **New CAS Session** to add the code to the program window.



h. Copy the line of code and paste it twice below. Change the mySession string to **mySession1**, **mySession2**, and **mySession3**.

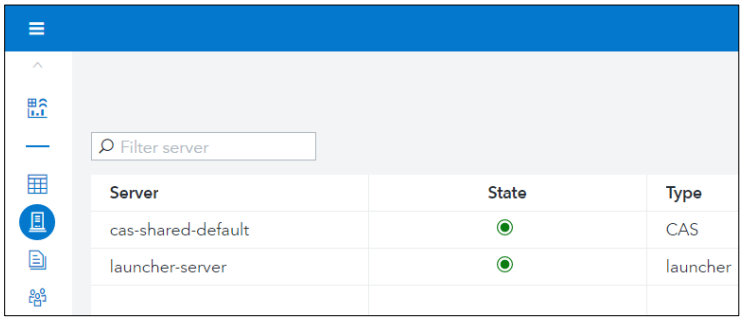


i. Run the program to create the sessions by pressing the F3 key or clicking the **Run** button. Check the log to confirm that there are no errors.

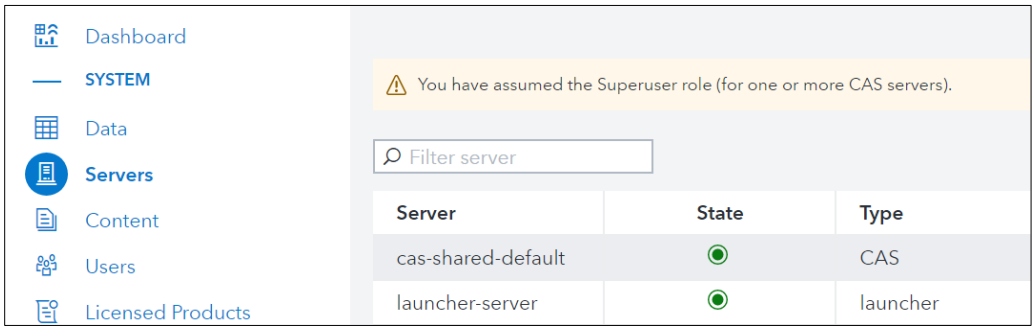


j. Open a new Chrome browser window and select **SAS Environment Manager** on the Bookmarks toolbar. (Or, you might already be logged on to SAS Environment Manager as **christine**.) Sign in as the user **christine** with the password **Student1**. Assume the **SASAdministrator** role.

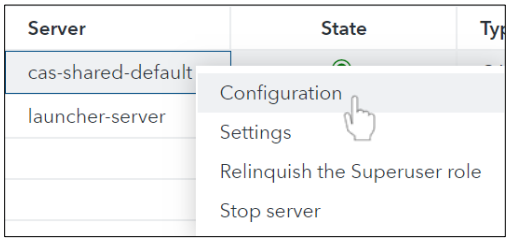
k. Click **Servers** on the side menu. The tasks from the **Servers** page can be performed only by SAS Administrators.



l. Right-click the **cas-shared-default** server. Select **Assume the Superuser role**. A message in the window indicates that you are now in the Superuser mode.

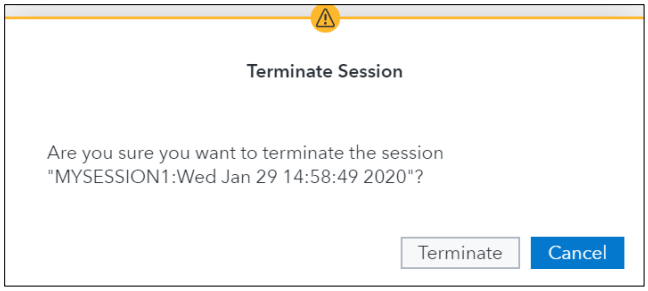


m. Right-click **cas-shared-default** again and select **Configuration**. (Alternatively, you can highlight **cas-shared-default** and click the **Configuration** icon in the upper right toolbar.)



n. The first tab displays the list of sessions. Find **MYSESSION1**, which is owned by eric. Select the check box to the left. Click the **Terminate** icon at the top right to terminate the session.

o. Verify that you want to terminate the session.



p. Click the **Servers** menu to go back to the Servers page.

q. Use the CLI to terminate a CAS session. If an mRemoteNG session for christine is not started, open one now.

r. Change the directory to **/opt/sas/viya/home/bin** to access **sas-admin**.

```
cd /opt/sas/viya/home/bin
```

Note: If Christine has been inactive for at least 12 hours, you will need to log back on to the CLI utility. Enter the command below and providing the user ID and password for **christine**.

```
./sas-admin auth login
Enter credentials for https://server.demo.sas.com:

Userid> christine

Password> <enter Student1>
Login succeeded. Token saved.
```

s. Obtain a list of servers. Enter the **sas-admin** command below. The value in the **Name** column is used for subsequent commands.

```
./sas-admin cas servers list
```

t. Open a list of eric's remaining sessions that are currently running on the CAS server. Enter the **sas-admin** command below. The session ID for MYSESSION2 is needed for the next step to terminate MYSESSION2.

```
./sas-admin cas sessions list -server cas-shared-default --
superuser --owner eric
```

```
[christine@server bin]$ ./sas-admin cas sessions list -server cas-shared-default --superuser --owner eric
{
    "items": [
        {
            "authenticationType": "OAuth",
            "id": "b8864392-d530-914e-9437-b1d17a3486bf",
            "name": "  Session:Tue Aug 28 11:58:37 2018",
            "owner": "eric",
            "state": "Connected",
            "transactionState": ""
        },
        {
            "authenticationType": "OAuth",
            "id": "68bf06b8-6e48-8e49-9878-1a507e4200b0",
            "name": "MYSESSION2:Tue Aug 28 12:06:31 2018",
            "owner": "eric",
            "state": "Connected",
            "transactionState": ""
        },
        {
            "authenticationType": "OAuth",
            "id": "df34bd48-b5c7-b64c-a3bc-cfe476c679ef",
            "name": "MYSESSION3:Tue Aug 28 12:06:31 2018",
            "owner": "eric",
            "state": "Connected",
            "transactionState": ""
```

Note: SAS Environment Manager was used previously to terminate MYSESSION1.

u. Terminate **MYSESSION2**. Enter the **sas-admin** command below.

```
./sas-admin cas sessions delete -server cas-shared-default --
superuser --session-id get from the previous command's output
```

v. Obtain a list of eric's remaining sessions that are currently running on the CAS server. Enter the **sas-admin** command below. Only one session remains.

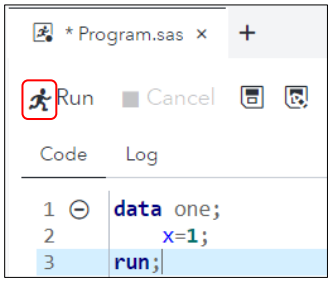
```
./sas-admin cas sessions list -server cas-shared-default --
superuser --owner eric
```

10. Viewing the Process Owned by Eric in the Operating System

a. Log on to SAS Drive as **eric** using the password **Student1**.

b. Select the applications menu ⇨ **Develop SAS Code** to launch SAS Studio.

c. Create a new SAS program and enter the code shown below on the Program.sas tab. A workspace server is launched to process the code submission.



Alternatively, you can copy the code snippet below and paste it into the Program.sas editor window in SAS Studio.

```
data one;
  x=1;
run;
```

After the code runs, a workspace server is launched.

d. In mRemoteNG and using christine's session, search for any process owned by eric by issuing the following command:

```
ps -ef | grep eric
```

The location of the run-time server executable is **/opt/sas/spre/home/SAS Foundation**.

```
[christine@server run]$ ps -ef |grep eric
eric      76374  19101  0 14:49 ?        00:00:01 /opt/sas/spre/home/SASFoundation/sasexe/sas -SA
ult/../../connectserver/default/connectserver.sh -logconfigloc ./logconfig.xml -noterminal -noxcm
rver -objectserverparms protocol=bridge spawned spp=36493 cid=0 dnsname=localhost cel=everything
eric      76525  19101  0 14:49 ?        00:00:01 /opt/sas/spre/home/SASFoundation/sasexe/sas -SA
ult/../../connectserver/default/connectserver.sh -logconfigloc ./logconfig.xml -noterminal -noxcm
rver -objectserverparms protocol=bridge spawned spp=36493 cid=1 dnsname=localhost cel=everything
christi+  85618 127617  0 14:53 pts/0    00:00:00 grep --color=auto eric
[christine@server run]$
```

11. Using SAS Environment Manager to Configure a Microservice

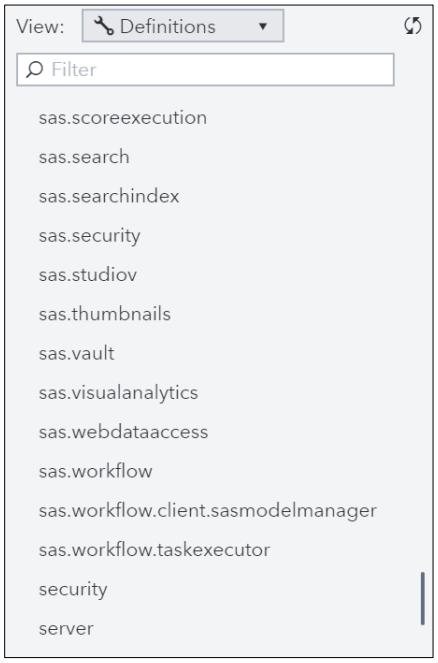
In this practice, set the time-out interval for SAS Viya web applications. The session time-out interval is the specific period of time that a web application waits before it signs off users' inactive sessions.

a. If you do not have an active SAS Environment Manager session, open a Chrome browser and select **SAS Environment Manager** on the Bookmarks toolbar. Sign in as the user **christine** with the password **Student1**. Assume the **SASAdminstrator** role.

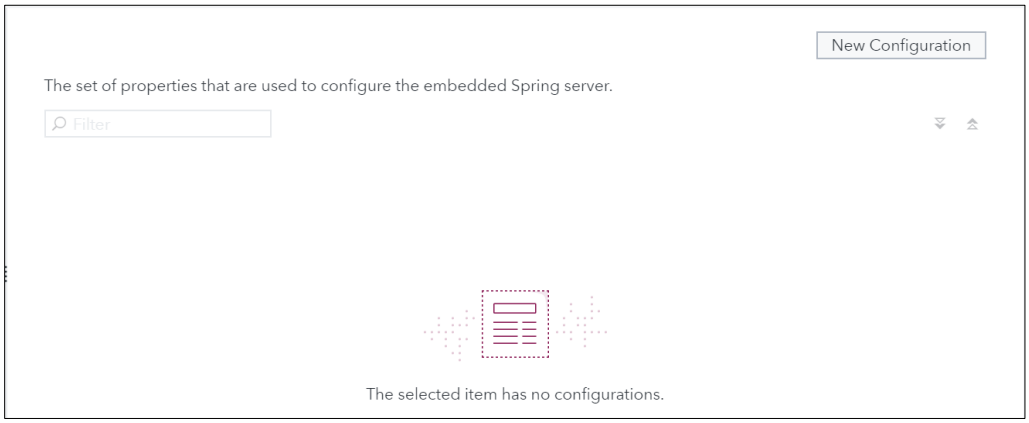
b. Select **Configuration** from the side menu.

c. Click **Definitions** from the **View** drop-down menu.

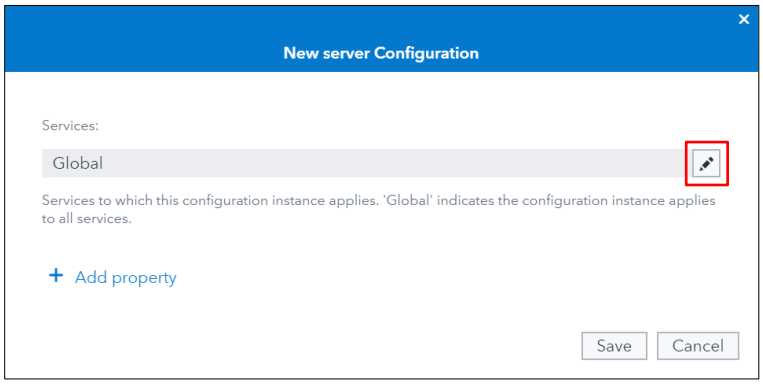
d. In the list of configuration definitions, select **server**.



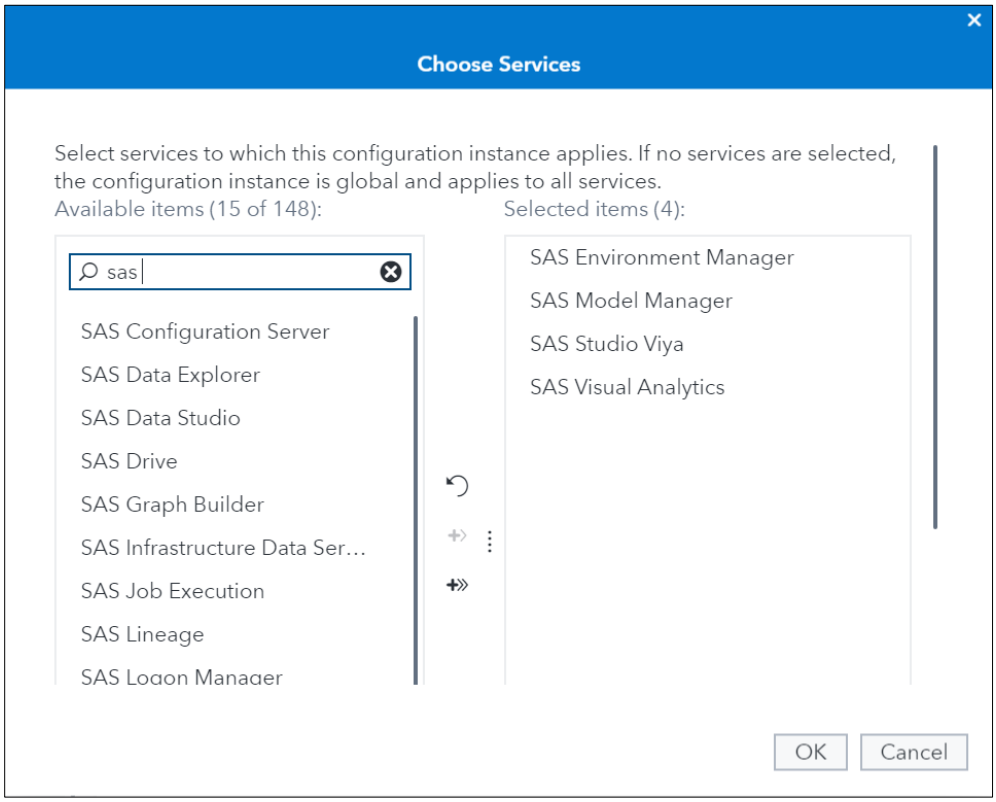
e. In the top right corner of the view, click **New Configuration**.



f. In the New server Configuration dialog box, click **Edit**.

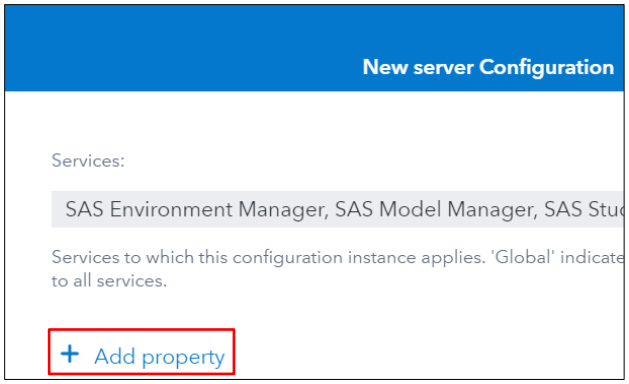


g. In the Choose Services dialog box, filter on **sas** to see SAS Viya web applications. Move **SAS Environment Manager**, **SAS Model Manager**, **SAS Studio Viya**, and **SAS Visual Analytics** to the **Selected items** column.



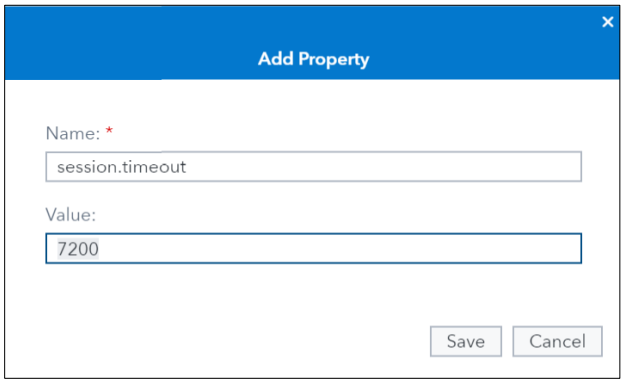
h. Click **OK**.

i. In the New server Configuration dialog box, click **Add property**.



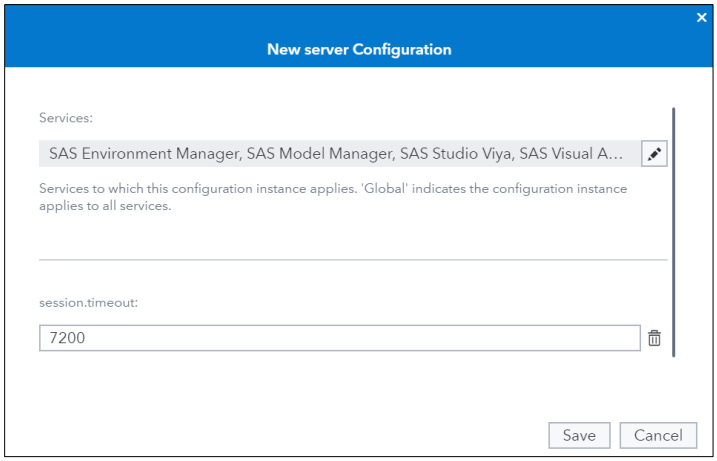
j. In the **Add property** dialog box, in the **Name** field, enter the following Spring server property: **session.timeout**.

k. In the **Value** field, enter the number of seconds you want the SAS Viya web applications to wait before they sign off users' inactive sessions. Enter **7200** so that two hours of inactivity will sign a user off of the application.



l. Click **Save**.

m. Click **Save**.



Your change takes effect for any new sign-ins to a SAS Viya web application.

Note: In SAS Studio (Basic), the session time-out interval is defined by the administrator with webdms.maxSessionTimeoutInHours.

12. Exploring SAS Viya Deployment Files

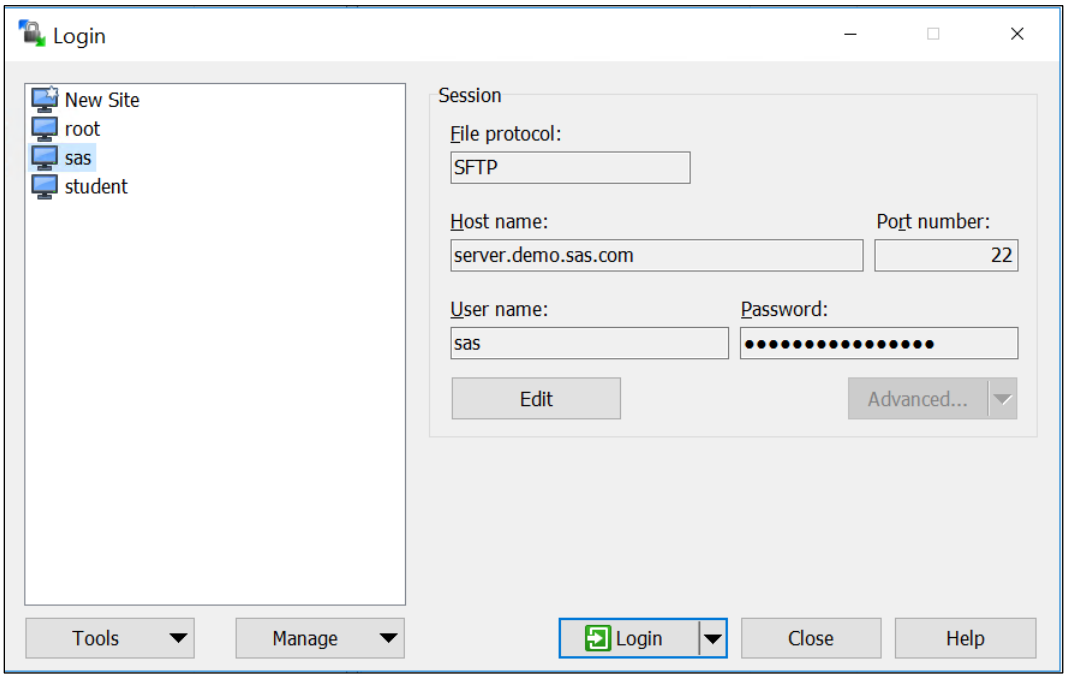
a. Connect to your Windows client machine.

Classroom Course	Live Web Course
Use a remote desktop connection with the IP address that is given to you by the instructor. Sign in with these credentials: User: **Student** Password: **Metadata0**	Use the URL in step 6 of the email that you received from Live Web Administration.

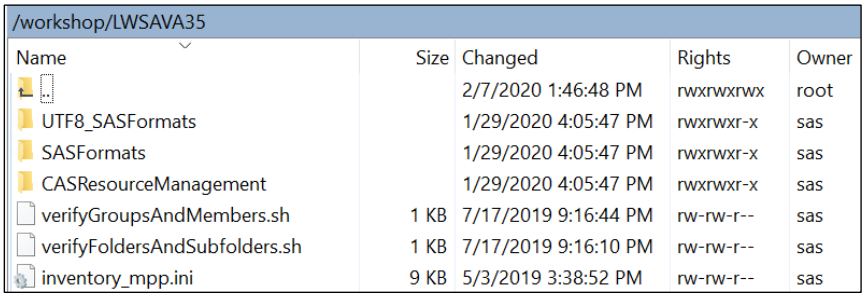
b. Double-click the WinSCP icon from the Windows desktop or Windows taskbar.

Note: You can use **mRemoteNG** to view the inventory.ini and the vars.yml files.

c. Double-click **sas@server** in the Login window. This signs you on to a session with the user ID **sas** on the server machine where SAS Viya is installed.

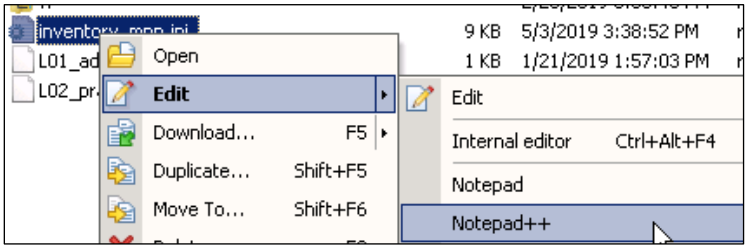


d. Navigate to **/workshop/LWSAVA35** to look at a sample inventory.ini file for a multi-machine deployment.



e. Right-click **inventory_mpp.ini** file and select **Edit** ⇨ **Notepad++**.

Note: In production, the file must be named **inventory.ini** and reside in the playbook directory.



How many machines are in the SAS Viya deployment?

6 machines

Which machine is the CAS controller? Hint: Find the sas-casserver-primary role.

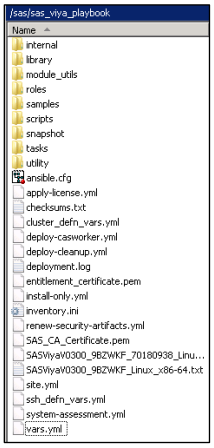
intcas01

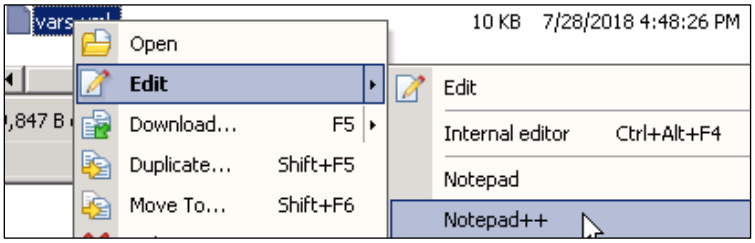
```
# The sas-casserver-primary host group contains the CAS controller node.
# The first host in the sas-casserver-primary list is used by the tenant in a single-tenant deployment or by the
# provider in a multi-tenant deployment. Only one configuration of CAS (including one primary controller and one
# secondary controller) per tenant is supported. Therefore, if you change the first host in the list, you are
# changing the primary CAS controller for a single-tenant deployment or, for multi-tenant deployments, you
# are changing the primary CAS controller for the provider. Any additional hosts in the sas-casserver-primary
# list are used in a multi-tenant environment. The configuration for those additional hosts (primary controller,
# secondary controller, or worker) are determined by the tenant-vars.yml file.
# For more information about the tenant-vars.yml file, see the SAS Viya Administration documentation.
[sas-casserver-primary]
intcas01
```

Is this a distributed CAS environment? Hint: Look at the other Cas roles.

Yes

f. Open **/sas/sas_viya_playbook/vars.yml**.





Answer the following questions:

Who is the user that the CAS process will run under?

cas

Who is the group that the user belongs to?

sas

```
##############################################################################
## CAS Configuration
##############################################################################

# The user that the CAS process will run under

casenv_user: cas

# The group that the CAS user belongs to

casenv_group: sas
```

What option is set to true that then creates and sets up SSH keys for users in the sas_users group?

setup_sas_users

```
# When set to true will try and create any user in the sas_users group below.
# This will also create and setup ssh keys for that user across all hosts
# default is true
setup_sas_users: true
```

What is the **CAS_DISK_CACHE** set to?

/tmp

Note: By default, only the **/tmp** directory is used as the cache directory. This is sufficient for demonstration purposes, but not for production use of the server. For production-use server, set the cache to use a series of directories. The size required differs for each deployment, but can run from gigabytes to terabytes. When you specify a series of directories, each time the server needs to use disk, it uses the next path in the list. This strategy is used to distribute the load across disk volumes.

After deployment, what file will this CAS_CONFIGURATION be located in?

casconfig.lua

```
# Anything in this list will end up in the casconfig.lua file
#   The env section will create a env.VARIABLE in the file
#     Example: env.CAS_DISK_CACHE = '/tmp'
#   The cfg section will create a cas.variable in the file
#     Example: cas.port = 5570
#
# If you have defined hosts for the sas-casserver-worker then the MODE will
# automatically be set to 'mpp'. If the environment variables HADOOP_HOME and
# HADOOP_NAMENODE are set, the COLOCATION option will automatically equal 'hdfs'.
# If HADOOP_HOME and HADOOP_NAMENODE are not set, then the COLOCATION option
# will automatically equal 'none'.

CAS_CONFIGURATION:
   env:
     #CAS_DISK_CACHE: /tmp
     #CAS_VIRTUAL_HOST: 'loadbalancer.company.com'
     #CAS_VIRTUAL_PROTO: 'https'
     #CAS_VIRTUAL_PORT: 443
```

g. Locate **LICENSE_FILENAME** and **LICENSE_COMPOSITE_FILENAME**.

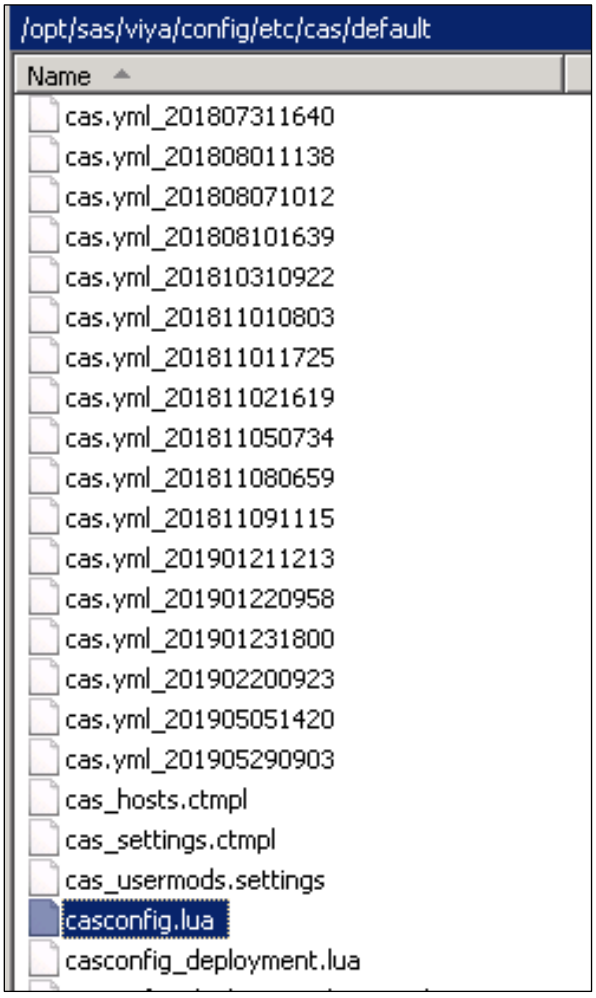
```
# The name of the license file on the Ansible machine.
LICENSE_FILENAME: "SASViyaV0300_9BZWKF_Linux_x86-64.txt"

# The name of the composite license file on the Ansible machine.
# If both files are present, the playbook will use the
# composite license file.
LICENSE_COMPOSITE_FILENAME: "SASViyaV0300_9BZWKF_70180938_Linux_x86-64.jwt"
```

You would replace the current license file name with the corresponding new license file name. (**Note:** The JSON web token license file (.jwt) is also referred to as a *composite license*.) Then you would run the following Ansible command for the default inventory file: **ansible-playbook apply-license.yml**

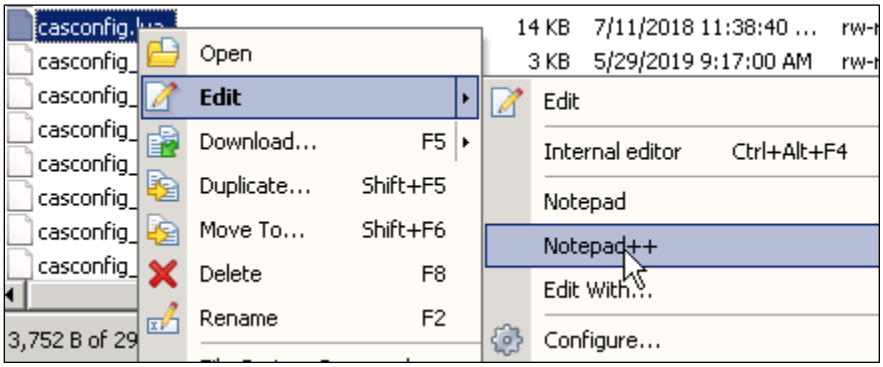
13. Exploring Configuration Files

Use mRemoteng or Winscp to look at files.

a. Navigate to **/opt/sas/viya/config/etc/cas/default**.



b. Open **casconfig.lua**.



Which account is set as the default CAS superuser?

cas

What is the starting port of the CAS server?

5570

Changes to the options in this file are not to be made directly. Which file would you use to modify settings?

casconfig_usermods.lua

Note: For sites that use Ansible, it is recommended that you make your CAS server configuration changes to **vars.yml** and rerun Ansible to apply these changes. For more information, see “Modify the vars.yml File” in *SAS Viya for Linux: Deployment Guide.*

c. Navigate to **/opt/sas/spre/home/SASFoundation/sasv9.cfg.** Open **sasv9.cfg.**

Where is the location of the SAS Work directory?

/tmp

14. Working with SAS Viya Services

In In this practice, you use the **service** and **systemctl** commands to stop, start, and determine the status of SAS Viya services. SAS Environment Manager is also used to determine the status of the services.

a. If you are not logged on to the Windows client system, log on. Use the method that you used previously.

b. If an mRemoteNG session for **christine** is not started, open one now.

c. (Optional) Use the **sas-viya-all-services** service to check the status of all the SAS Viya services. (This was done in an activity already.) Enter the following command:

```
sudo service sas-viya-all-services status
```

```
[christine@server sas]$ sudo service sas-viya-all-services status
Getting service info from consul...
  Service                                        Status     Host              Port     PID
  sas-viya-consul-default                        up         N/A                N/A    5161
  sas-viya-sasdatasvrc-postgres-node0-ct-pg_hba  up         N/A                N/A    6362
  sas-viya-sasdatasvrc-postgres-node0-ct-postgresql up      N/A                N/A    6365
  sas-viya-sasdatasvrc-postgres-pgpool0-ct-pcp   up         N/A                N/A    6359
  sas-viya-sasdatasvrc-postgres-pgpool0-ct-pgpool up        N/A                N/A    6356
  sas-viya-sasdatasvrc-postgres-pgpool0-ct-pool_hba up      N/A                N/A    6353
  sas-viya-vault-default                         up         10.96.16.97       8200    N/A
  sas-viya-sasdatasvrc-postgres-node0            up         N/A                N/A   12188
  sas-viya-cascontroller-default                 up         N/A                N/A   15155
  sas-viya-connect-default                       up         N/A                N/A    9061
  sas-viya-httpproxy-default                     up         N/A                N/A    8752
  sas-viya-rabbitmq-server-default               up         10.96.16.97       5672    None
  sas-viya-sasdatasvrc-postgres                  up         N/A                N/A   13246
                                                                                    
                                                                                    
  sas-viya-monitoring-default                    up         10.96.16.97       43825    7048
  sas-viya-projects-default                      up         10.96.16.97       38902   20381
  sas-viya-sashome-default                       up         10.96.16.97       45189   20484
  sas-viya-sasreportviewer-default               up         10.96.16.97       34477   20511
  sas-viya-sasthemedesigner-default              up         10.96.16.97       43967   30435
  sas-viya-sasvisualanalytics-default            up         10.96.16.97       43473   30447
  sas-viya-tenant-default                        up         10.96.16.97       46448   30543
  sas-viya-themecontent-default                  up         10.96.16.97       45085   30614

sas-services completed in 00:00:47
```

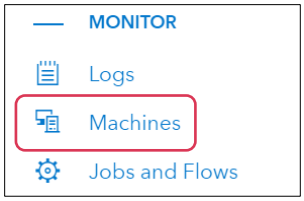
Note: Inform the instructor if all the services are not listed.

d. Use the **systemctl** command to restart a single service, **sas-viya-tenant-default**.

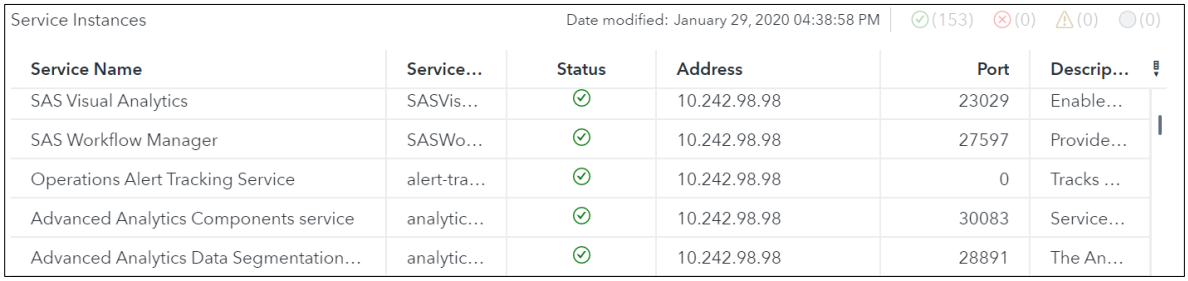
```
sudo systemctl restart sas-viya-tenant-default
sas-viya-tenant-default is stopped
sas-viya-tenant-default is running
```

e. Another view of the services indicates the available status with SAS Environment Manager. It is in the Machines side menu option in the Monitor section.

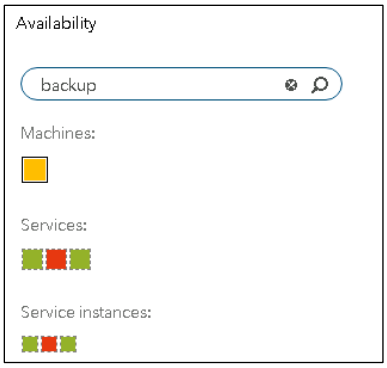
If a SAS Environment Manager session is not started, open one. Sign in as **christine** with a password of **Student1**. Click **Yes** to opt in to the **SASAdministrators** group. Select the **Machines** page.



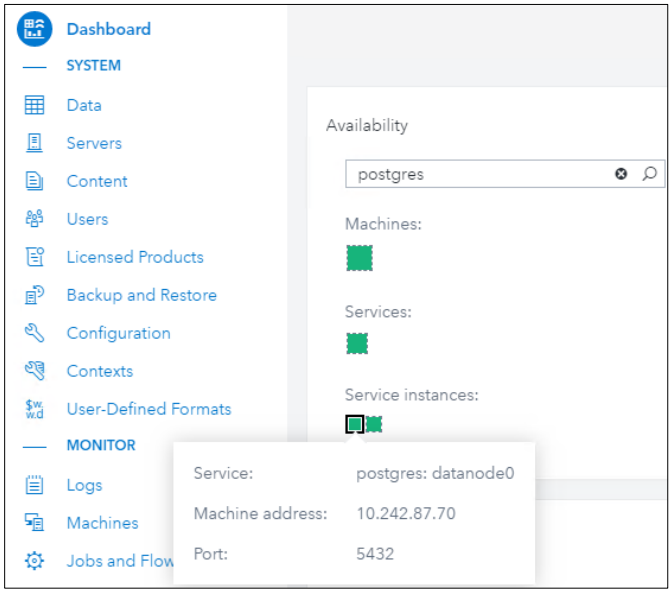
f. At the bottom of the Machine pane, there is a section with **Services Instances**. Scroll through the services. Use the scroll bar on the right side of **Services Instances** to confirm that all the services are running. There should be a green checkmark in the Status column for all the services.



g. Go back to the **Dashboard** page and search on **backup**. There are three backup services and three backup service instances. If you place your mouse pointer over each of the three services, you see **SAS Backup Manager**, **backup-agent**, and **Backup service**. If you place your mouse pointer over the three Service instances, you see **SASBackupManager**, **backup-agent**, and **deploymentBackup**.



h. Go to the Search box and replace **backup**. Enter **postgres**. The SAS Infrastructure Data Server is a PostgreSQL database server. In this case there is one service, the SAS Infrastructure Data Server, and two Postgres database service instances that run on different ports, 5431 and 5432.



i. Delete **postgres** from the Search box.

End of Solutions

Solutions to Activities and Questions

1.01 Activity – Correct Answer

Determine the status of your SAS Viya servers and services.

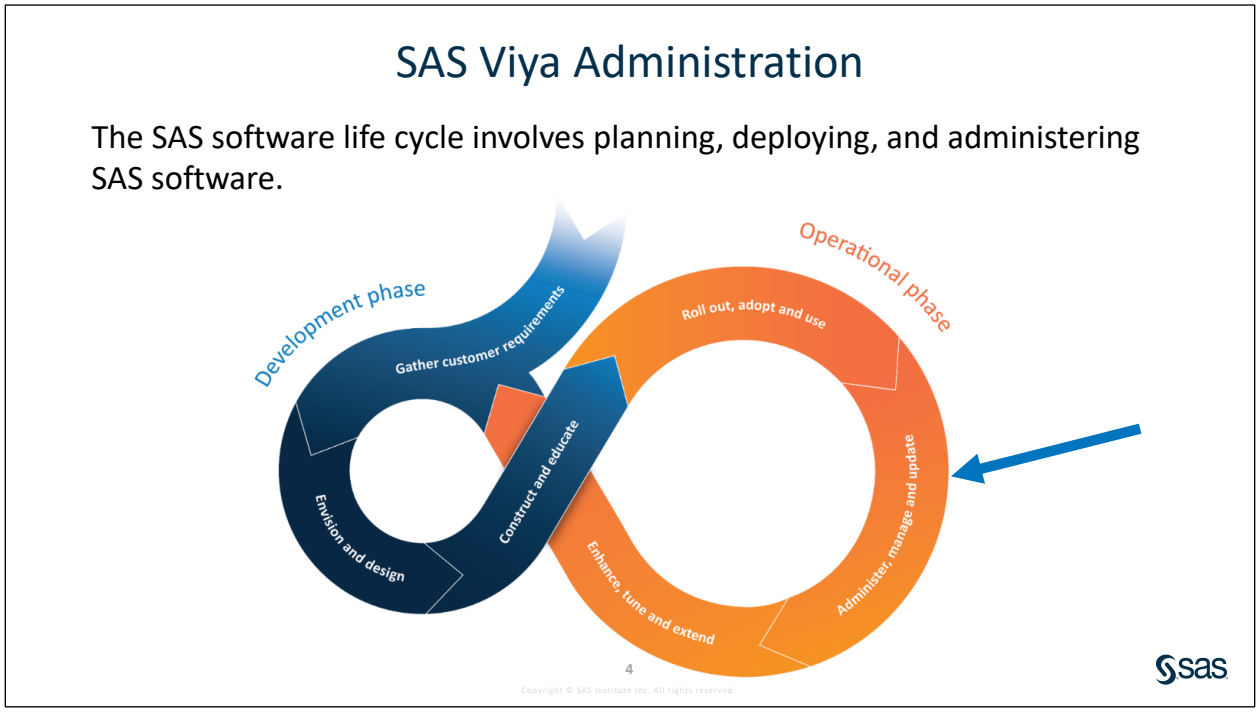
1. Use mRemoteNG and Christine's terminal session.
2. On the command line enter: **sudo /etc/init.d/sas-viya-all-services status**
3. Verify that your SAS Viya servers and services are up.
4. From where is the status information coming? **Configuration Server**

```
[christine@server sas_viya_playbook]$ sudo /etc/init.d/sas-viya-all-services status
Getting service info from consul...
  Service                                        Status     Host              Port     PID
  sas-viya-consul-default                        up         N/A                N/A   11593
  sas-viya-vault-default                         up         10.242.81.49      8200   12408
  sas-viya-sasdatasvrc-postgres-node0-ct-pg_hba  up         N/A                N/A   13650
  sas-viya-sasdatasvrc-postgres-node0-ct-postgresql up      N/A                N/A   13503
  sas-viya-sasdatasvrc-postgres-pgpool0-ct-pcp   up         N/A                N/A   13491
  sas-viya-sasdatasvrc-postgres-pgpool0-ct-pgpool up        N/A                N/A   13506
```

48

Lesson 2 Administration Tasks

2.1 Administration Tasks



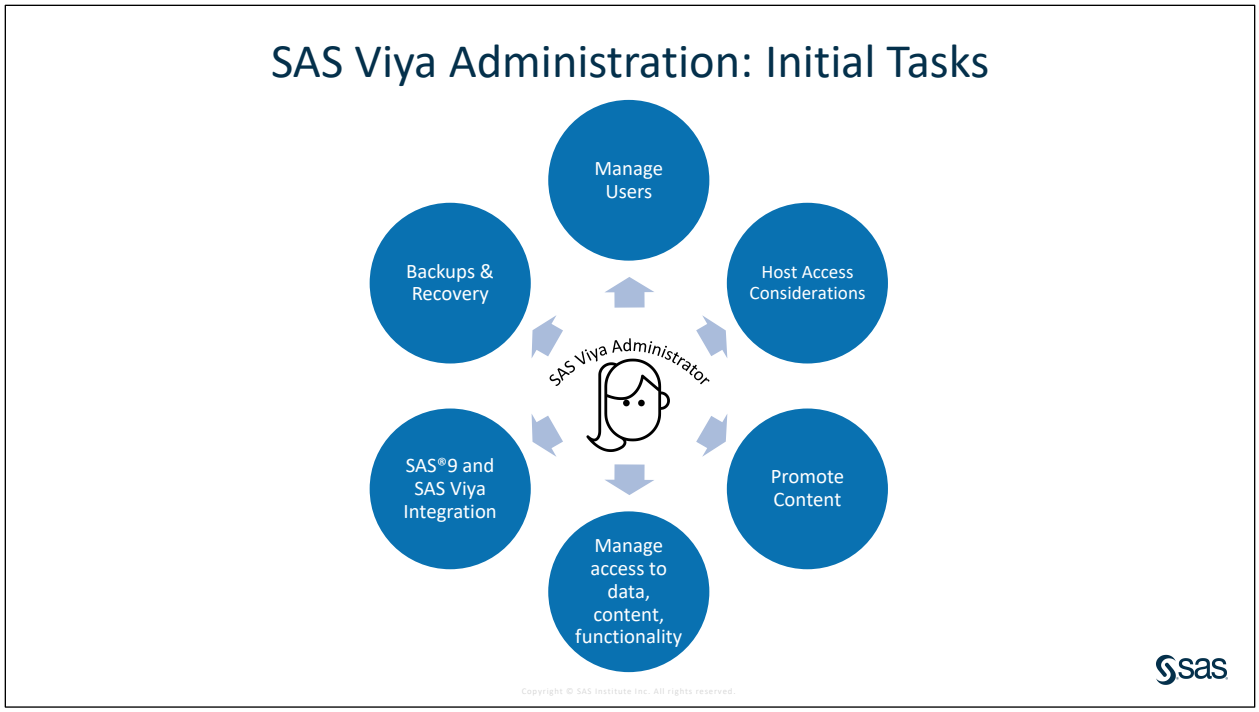
The SAS administrator might be responsible for planning, designing, deploying, monitoring, and maintaining a SAS environment, whether it is in the cloud or in a data center.

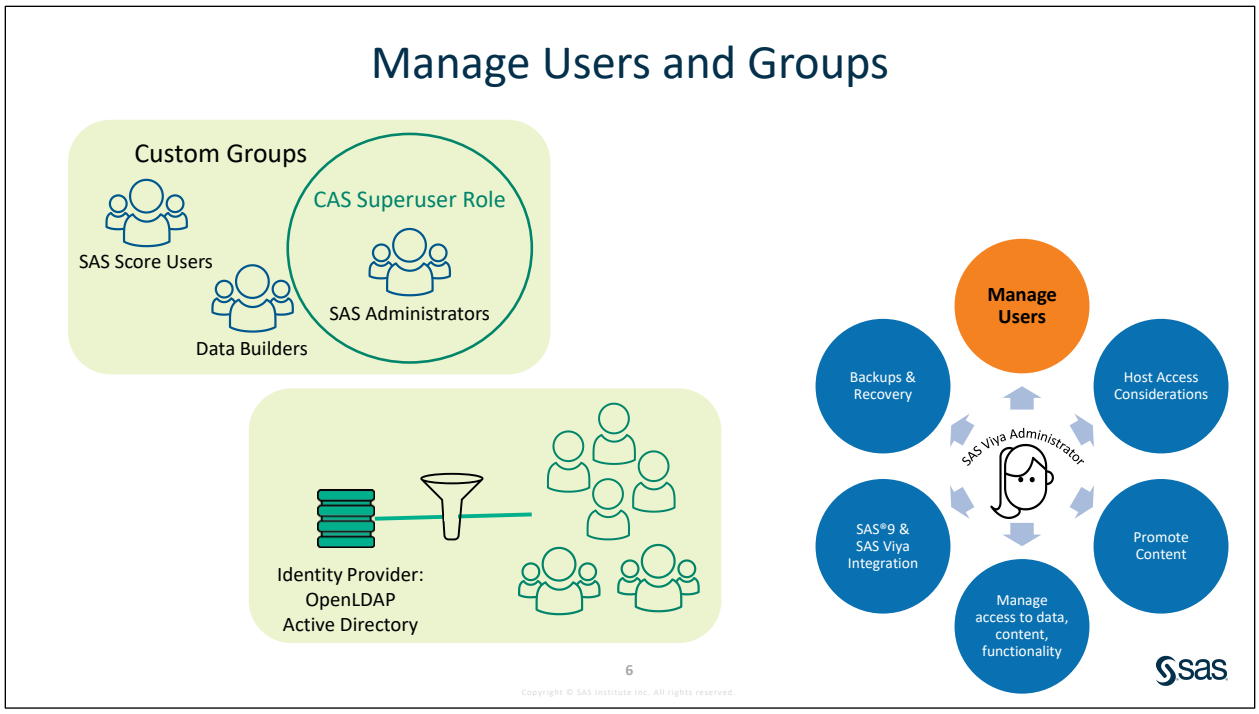
During the *development* phase, the following events occur:

- A customer's requirements are gathered to understand how the features and behaviors of SAS can support the objectives of the organization.
- A design is created with the detailed requirements of the business and IT stakeholders regarding security, scalability, availability, integration with third-party technology, installation specifications, monitoring and auditing, configuration management, disaster management, and performance.
- A plan to build and test the SAS Platform is performed. With pre-installation, the infrastructure is prepared for SAS software. SAS software is installed, configured, and validated.

During the *operational* phase, the following events occur:

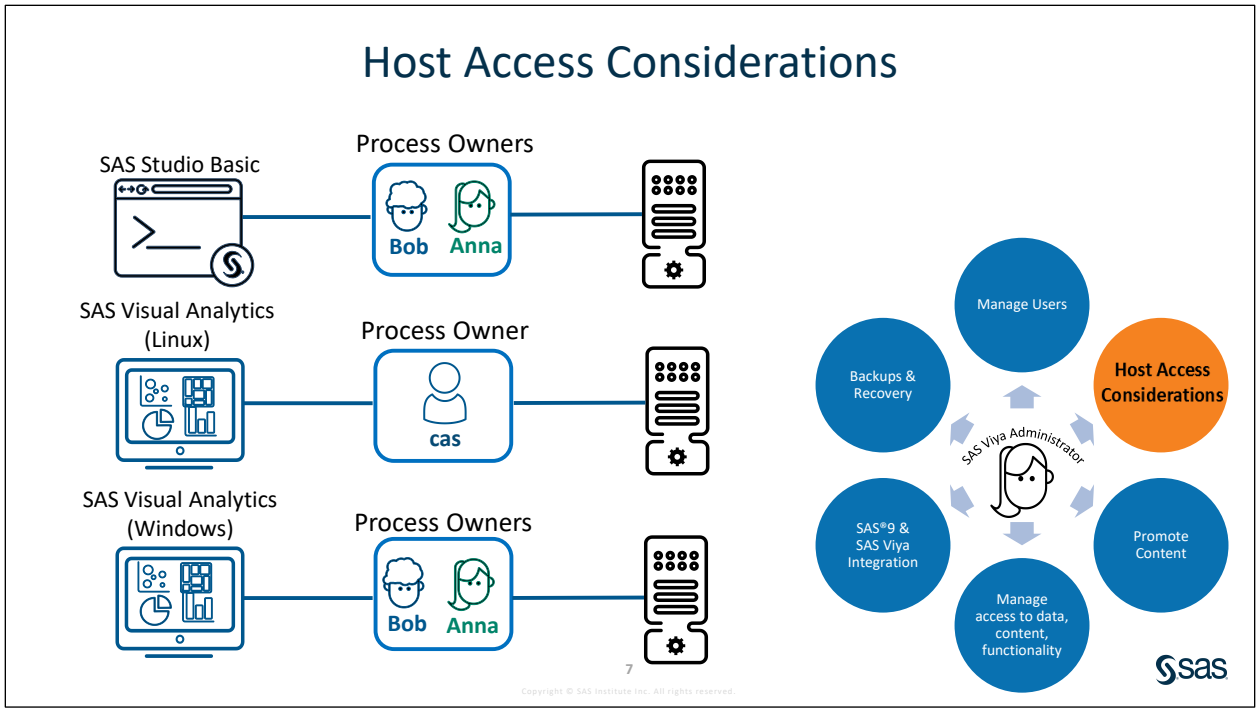
- Activities are performed to educate end users and SAS administrators. These include training and identifying efficient SAS administration practices.
- The SAS administrators perform tasks to keep the system healthy and available for the SAS users.
- Business analytics services are continued by tuning performance, adding SAS products, or additional tenants, for example.



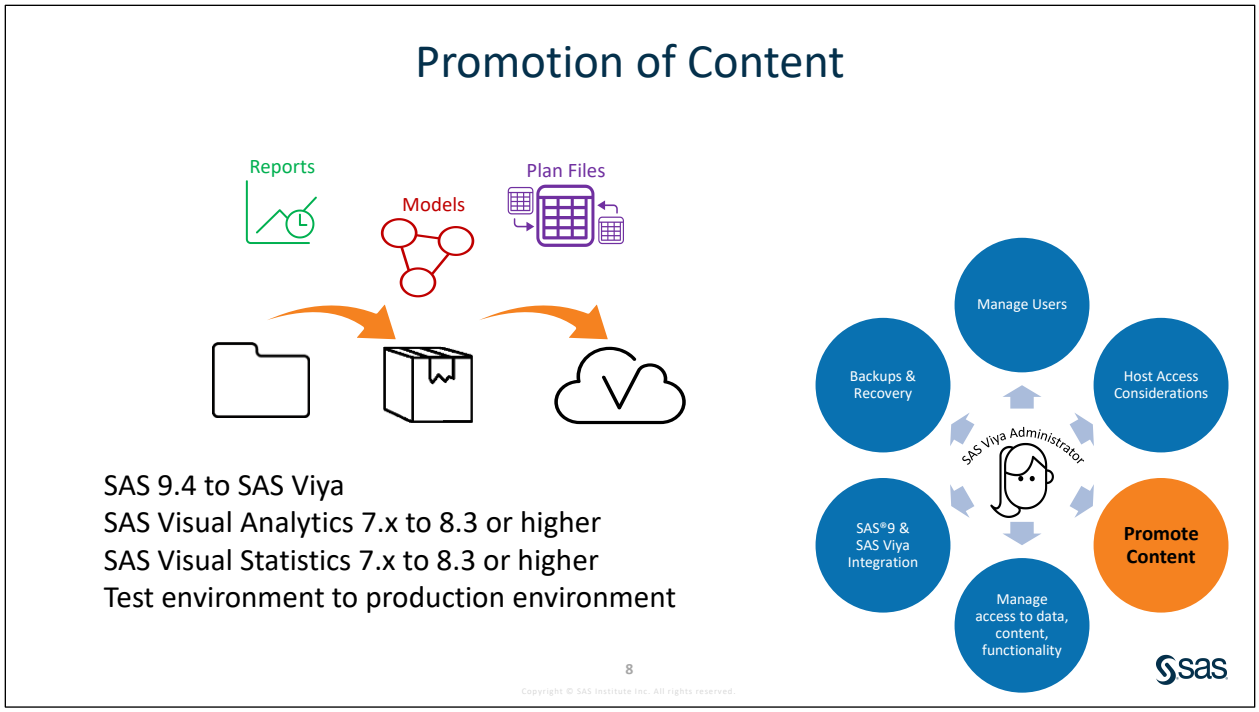


User and group identities are stored and managed by your organization's identity provider.

A SAS Viya deployment also has predefined custom groups and CAS roles. These custom groups provide an easy way for you to give user groups access to the appropriate data, content, and functionality. You can also use the groups that are retrieved from your LDAP directory server for access to necessary resources.

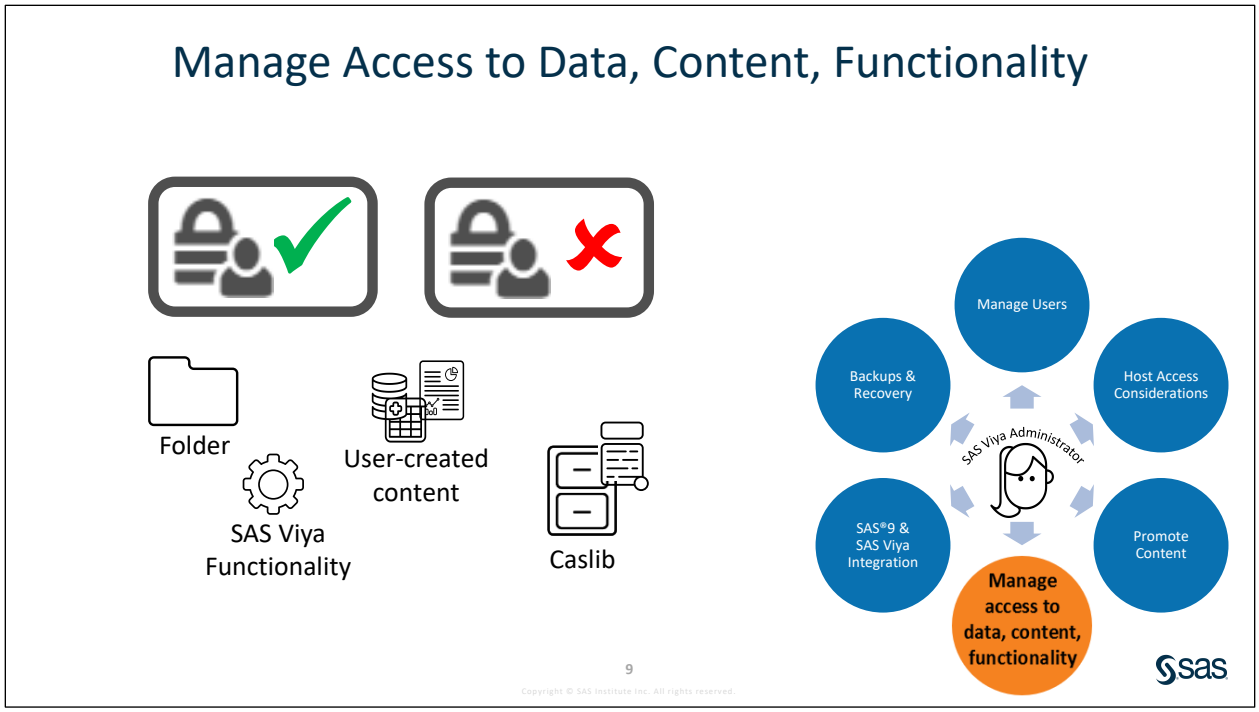


The account under which a CAS server process runs must have appropriate host-layer access to target directories and files. For users who access CAS from a programming interface, such as SAS Studio, all host access from CAS is under each user's individual identity. For these users, you must mirror CAS layer access distinctions in the host layer. For users who access CAS from a visual interface such as SAS Visual Analytics or SAS Environment Manager, all host access from CAS is under a shared identity. These users need CAS layer access to data, but they do not need host access to data. Only the shared identity needs host access to data.



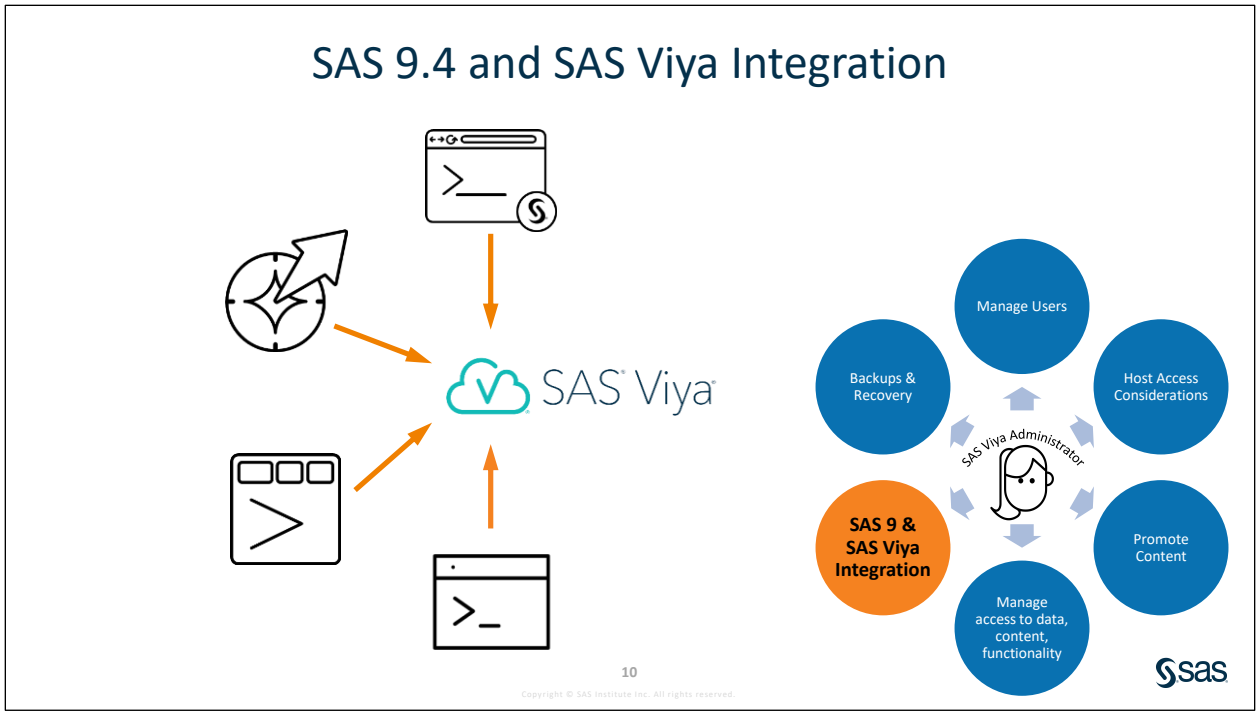
Any content from previous versions of SAS Viya or a SAS 9.4 environment will need to be made available in your current SAS Viya environment. *Promotion* is this process of making resources that exist in one environment and made available in another environment. Examples are folders, reports, explorations, data plans, or statistical models.

The promotion process has two phases, to export resources from the source environment and then import resources to the target environment.



You will need to implement a security model within your SAS Viya environment, which will determine users' access to data, content, and functionality.

The SAS Viya authorization layer consists of two systems. One is CAS authorization system, which manages caslibs, CAS tables and columns, and CAS action sets and actions. The other is the general authorization system, which secures SAS Viya folders and their content, such as reports or data plans. It also controls access to functionality, such as applications, features and services.

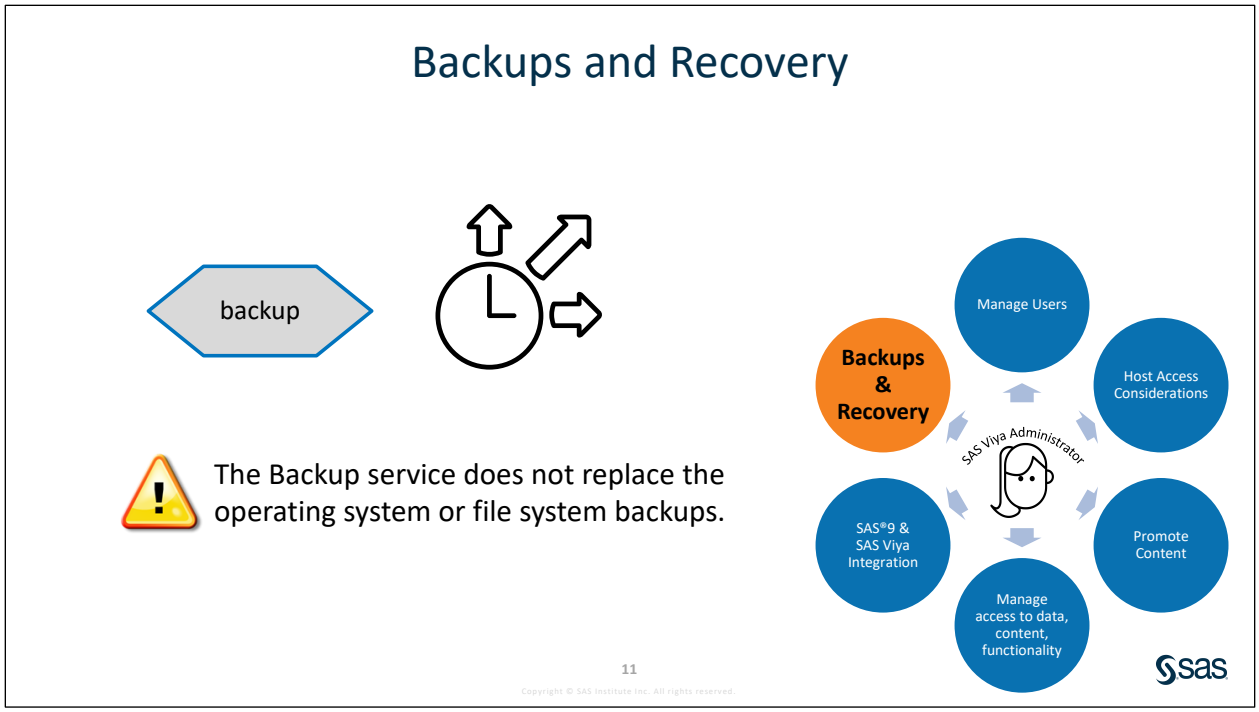


You can access SAS Viya 3.5 from any of the SAS®9 coding clients, including SAS Studio, SAS Enterprise Guide, SAS windowing environment, and batch or command-line code submission.

Prior to SAS 9.4M5, all SAS 9.4 clients leverage the SAS/CONNECT bridge to interact directly with SAS Cloud Analytic Services. SAS/CONNECT is used to initialize a SAS Foundation session within the SAS Viya environment, and this SAS Foundation session connects to SAS Cloud Analytic Services. SAS/CONNECT in SAS Viya leverages the operating system to authenticate the end-users.

With SAS 9.4M5, SAS/CONNECT is no longer needed, although it still can be leveraged.

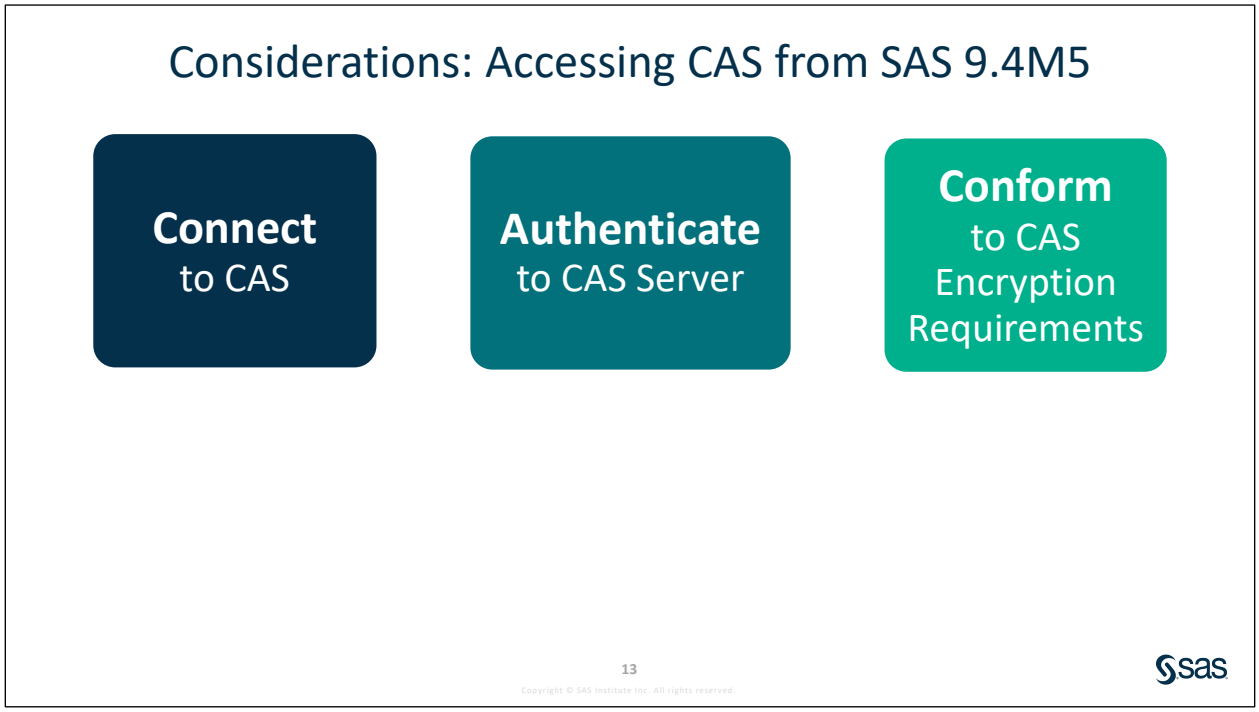
All releases of SAS can use SAS/CONNECT as a bridge to SAS Viya. See the Extended Learning page for more information.

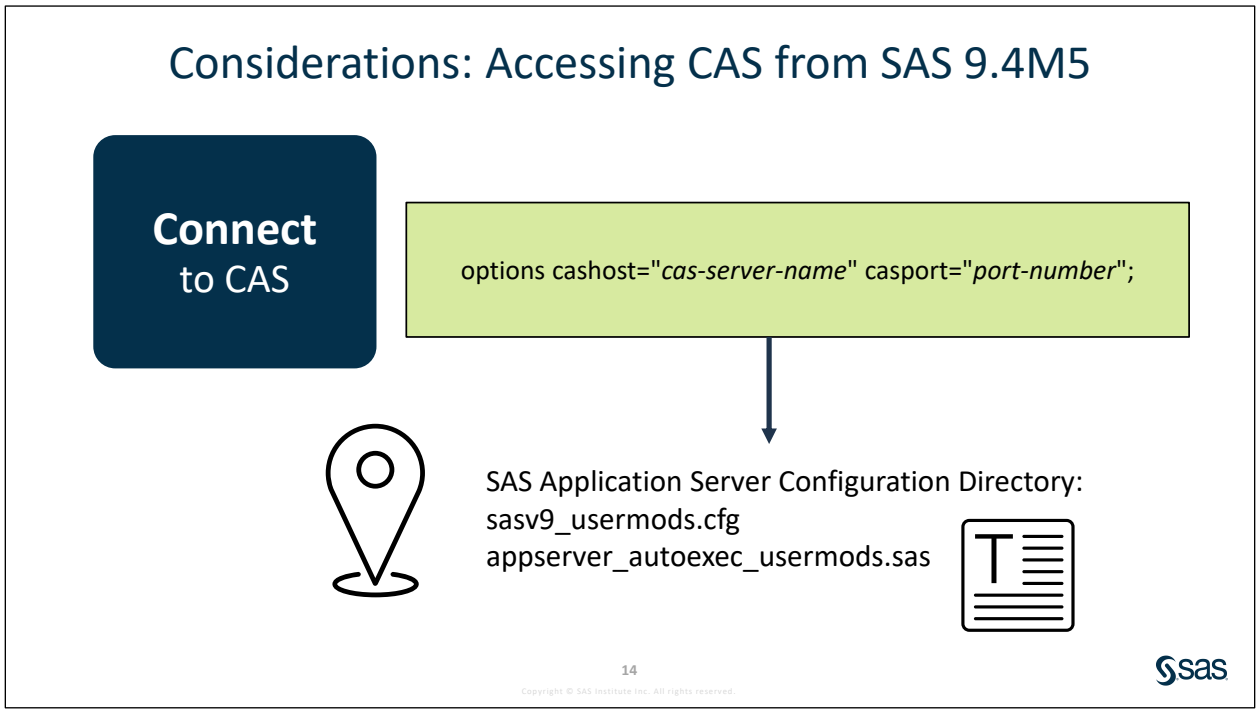


The Backup service is provided as a way to synchronize the backup and, if necessary, restore content and configuration information.

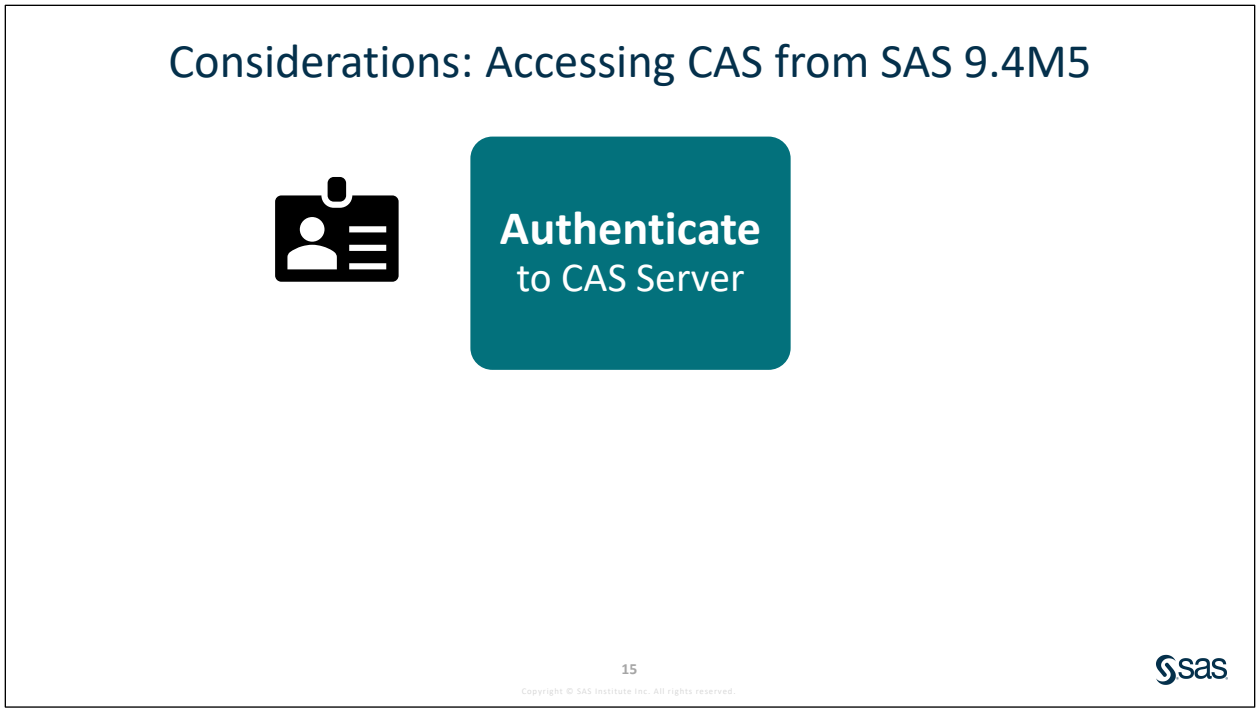
Run the Backup service as part of a regularly scheduled backup process.

2.2 Accessing CAS from SAS 9.4

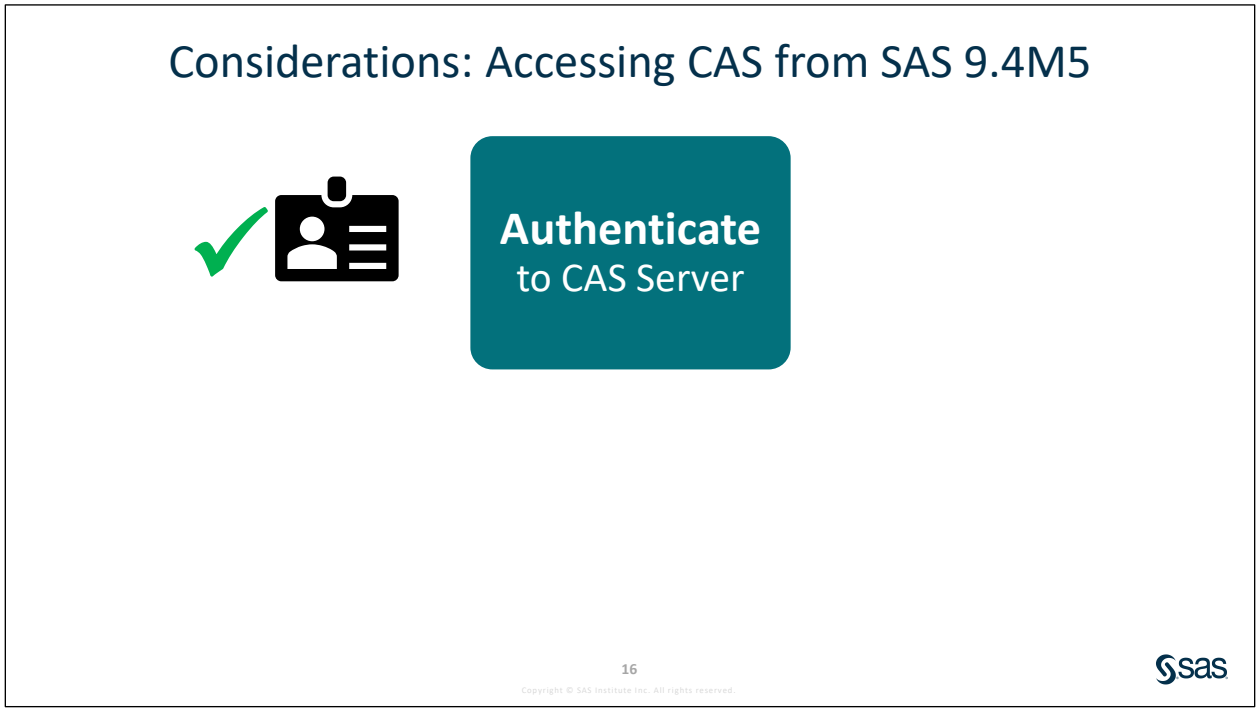




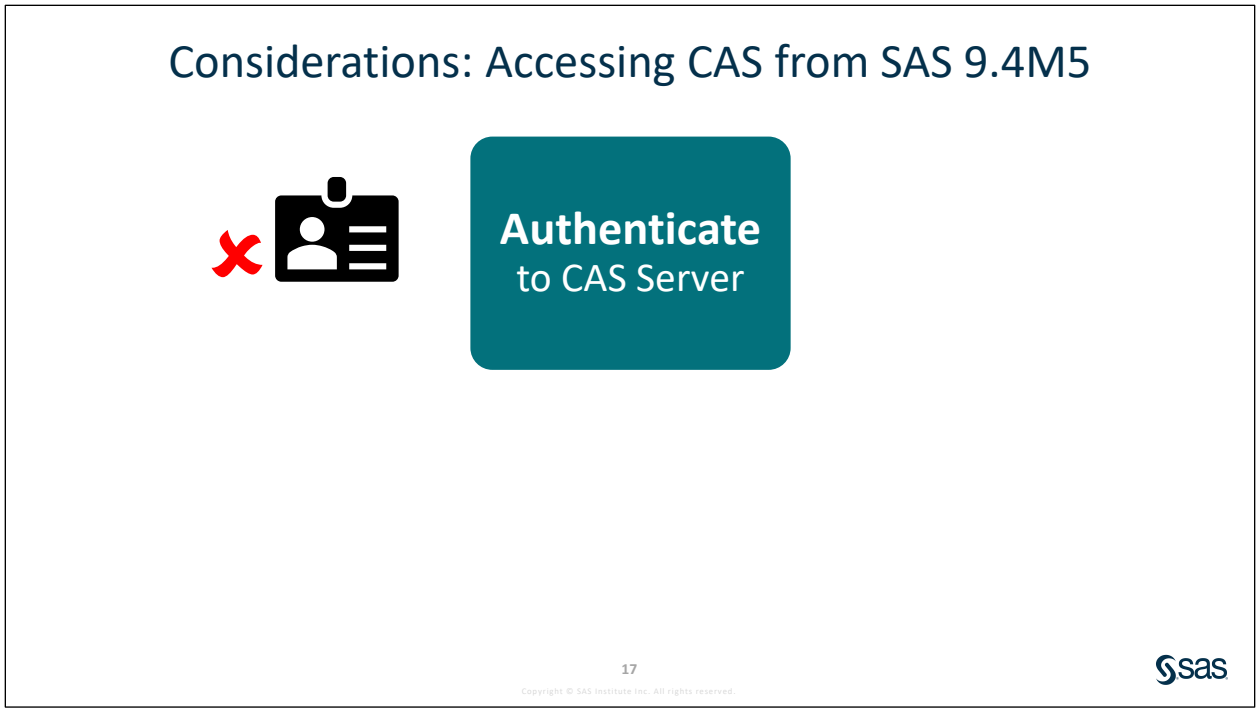
A SAS 9.4M5 client session needs to find CAS. Users can write an OPTIONS statement with the location of the CAS server and the port that the server is listening on. Or you can make the information available by adding the information to your SAS®9 server start-up files.



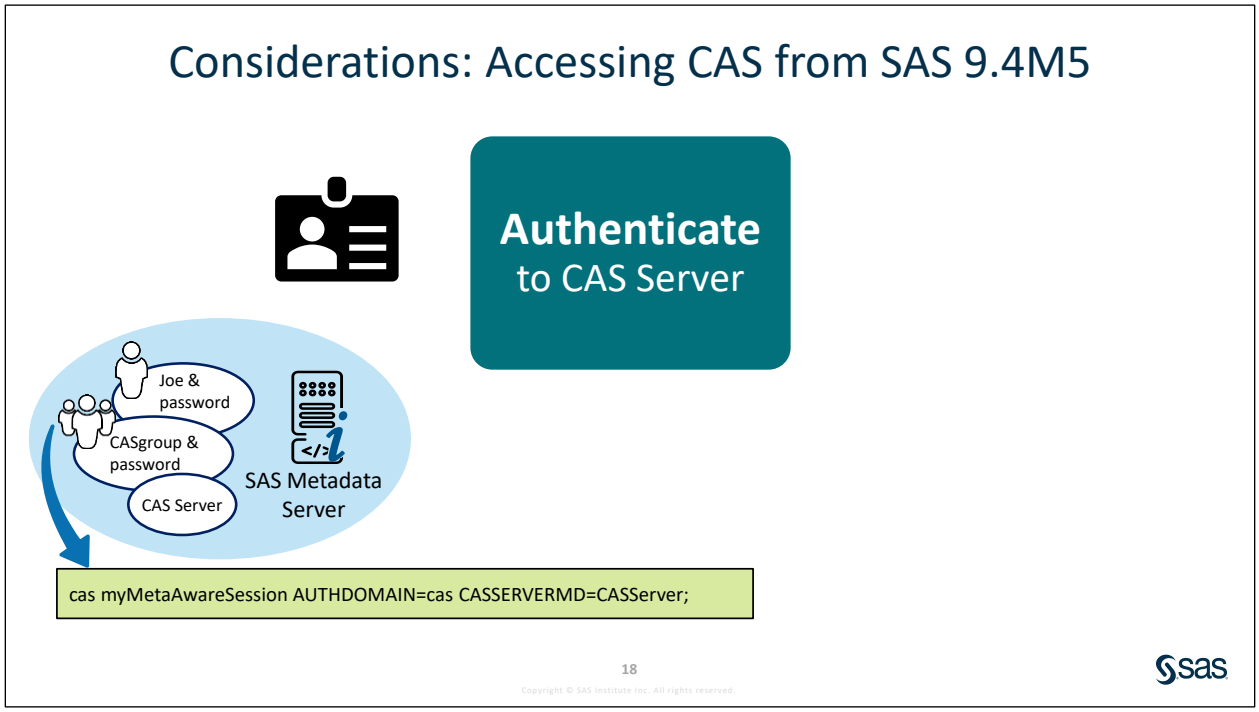
The SAS 9.4M5 client session needs to authenticate to CAS. When the SAS 9.4M5 session uses a user name and password to authenticate to CAS, it will use cached credentials from the initialization of the SAS 9.4M5 session.



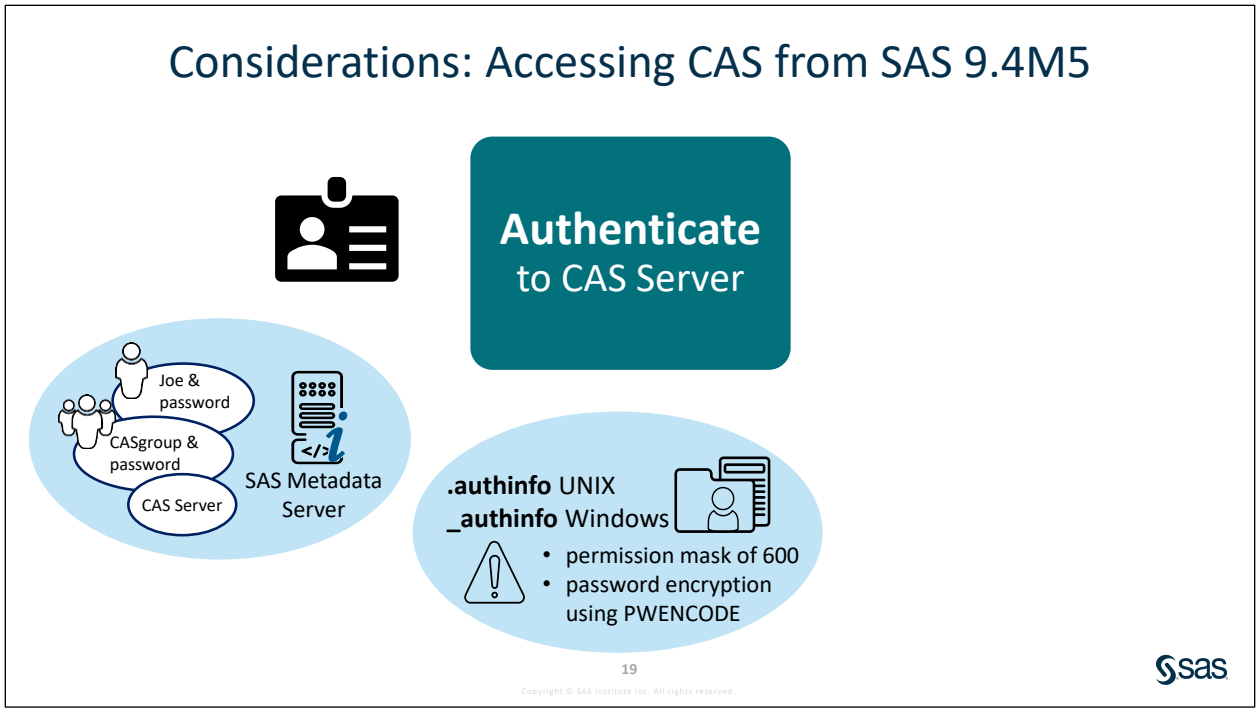
If that user exists with the same password in SAS 9.4 and SAS Viya authentication providers, then the connection to CAS is easily established under that identity and nothing more needs to be done.



If the credentials that are cached from the initialization of the SAS 9.4M5 session will not authenticate to the CAS server because the user does not exist in the authentication provider for SAS Viya and CAS, then you have a couple of options for storing the user name and password that will authenticate to CAS.



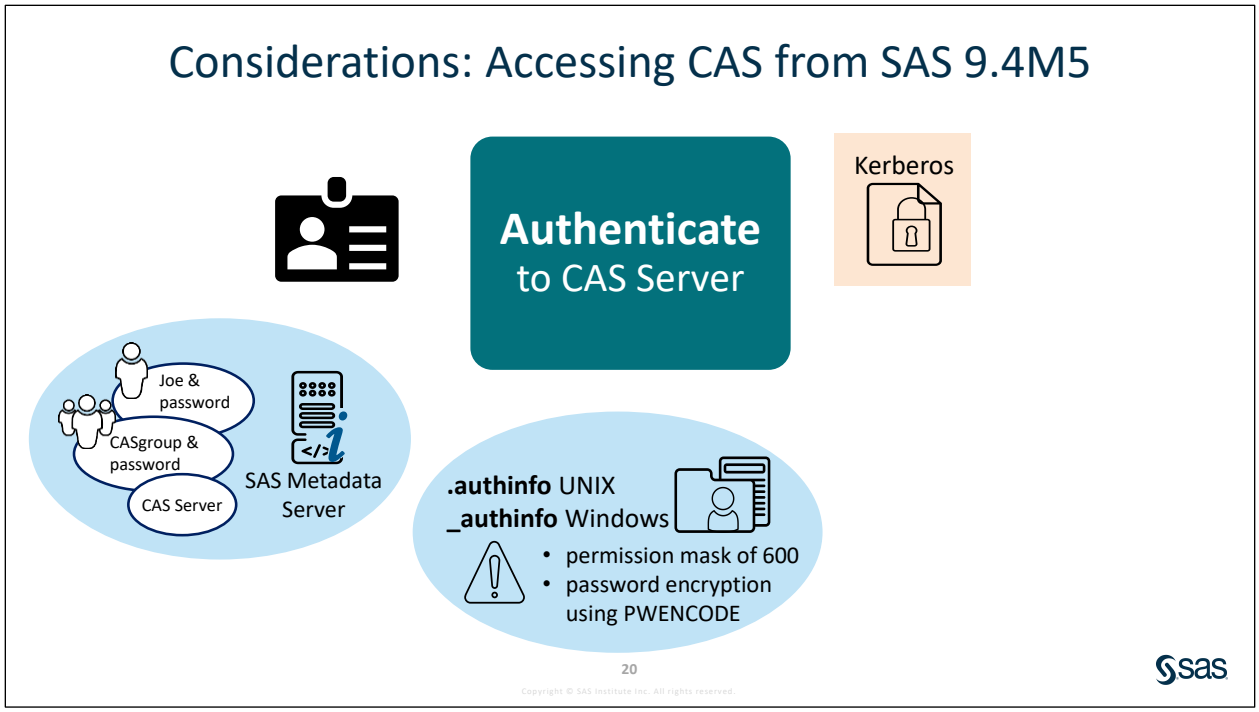
You can store server connection and CAS credentials in the SAS Metadata Server. Users need to include the **casservermd** option in the CAS statement to point to the CAS server definition in metadata.



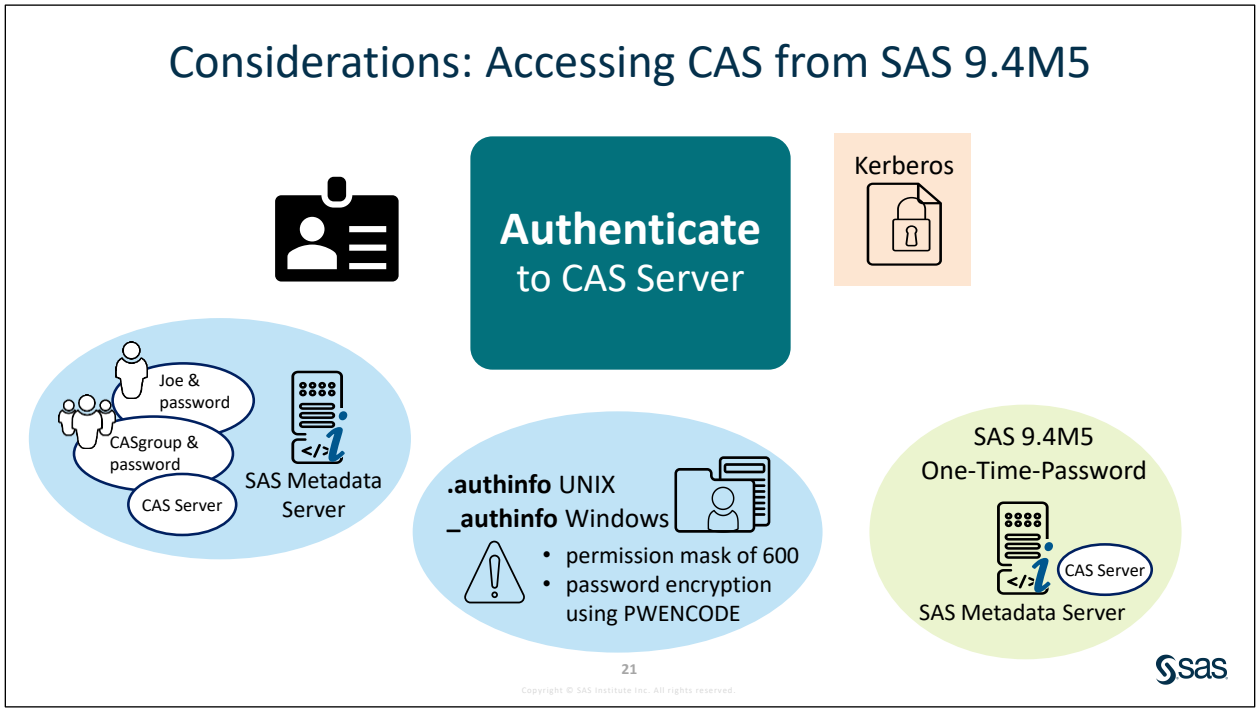
If you do not have a metadata aware SAS session, such as a batch session, then it is possible to connect to CAS by specifying user credentials in an authinfo file. An authinfo file contains credentials that can include one or more user IDs, passwords, host names, and port numbers to authenticate to multiple servers and spawners, and most importantly, the CAS servers.

Note: SAS Studio does not use the authinfo file by default. To use the authinfo file in SAS Studio, you must specify either the AUTHINFO= SAS system option or the AUTHINFO= CAS statement option.

Note: The authentication of the SAS 9.4M5 session to SAS Cloud Analytic Services is separate to any configuration of SAS Viya Logon Manager, because the SAS 9.4M5 session directly connects to SAS Cloud Analytic Services. However, SAS Viya Logon Manager is still involved. SAS Cloud Analytic Services in a full deployment will still connect to SAS Viya Logon Manager to obtain an internal OAuth token during the start-up. This will be with the credentials provided to SAS Cloud Analytic Services by the SAS 9.4M5 session.



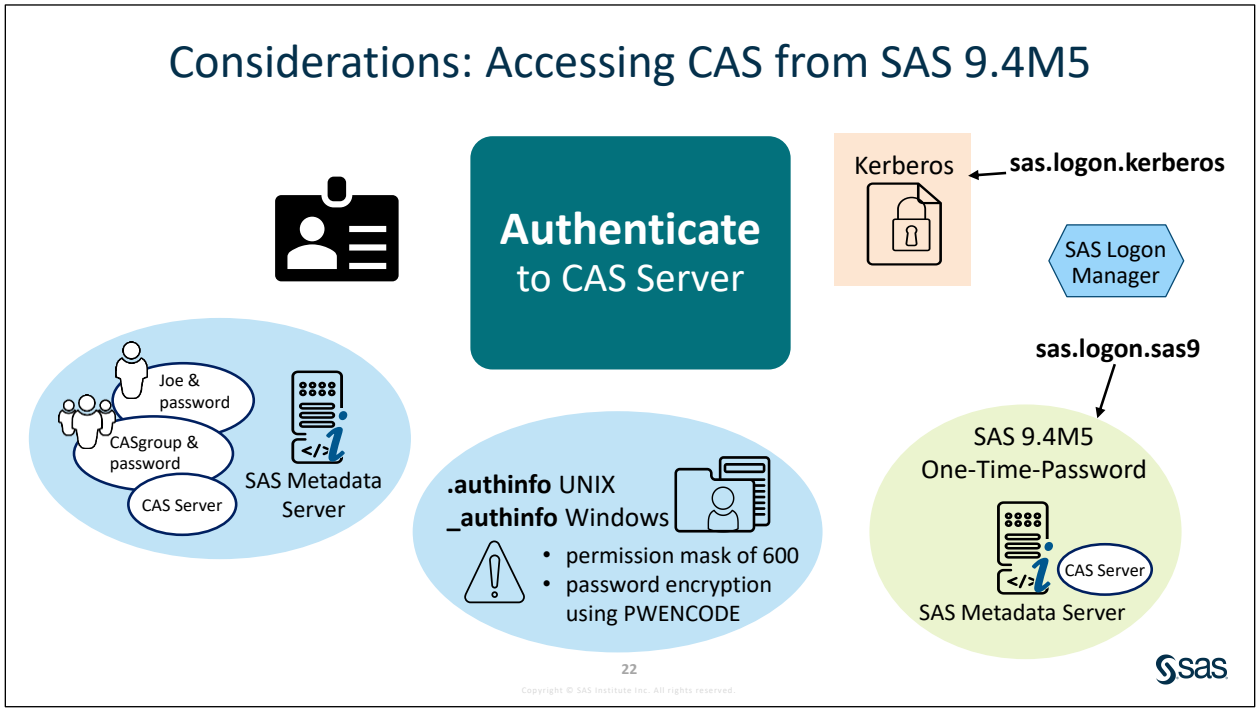
If your SAS Viya environment is configured to use Kerberos authentication, the cached credentials or credentials retrieved from metadata or from the authinfo file can be used for seamless access. If your 9.4 environment is also configured for Kerberos, kerborized connections throughout will be used for seamless access.



You also have the option to connect to CAS through a SAS 9.4 session that is using server launch credentials, such as sassrv. The SAS 9.4 session is not running as the end user and does not have access to the end-user credentials. However, you can still connect to CAS by configuring one-time passwords generated by SAS Metadata Server.

You create a CAS server definition using the AUTHDOMAIN= argument.

```
cas myMetaAwareSession AUTHDOMAIN=CAS CASSERVERMD=CASServer;
```



The SAS Viya Logon Manager needs to be configured for Kerberos and one-time-password authentication. For Kerberos to work correctly, the SAS Viya Logon Manager must be configured for Kerberos authentication. The configuration property that must be configured is **sas.logon.kerberos**.

In order for one-time-passwords to be validated, SAS Viya Logon Manager must be configured with details of the SAS 9.4M5 middle-tier. The configuration property that must be configured is **sas.logon.sas9**.

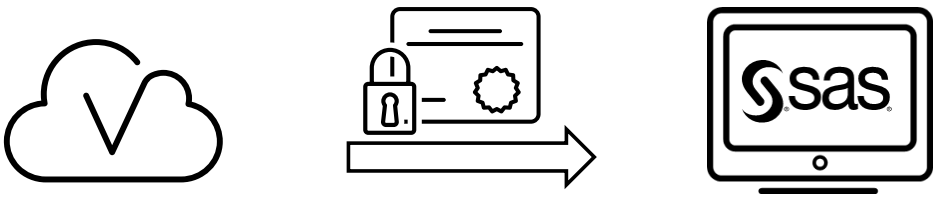
2.01 Activity

1. Sign in to SAS Environment Manager as **christine** and password **Student1**.
2. Select **Configuration** page from the side menu.
3. Change the View drop-down menu to **Definitions**.
4. Filter on **sas9** or scroll to **sas.logon.sas9**.
5. Highlight **sas.logon.sas9** and click **New Configuration**.
6. What property values should be modified?
7. Click **Cancel**.

23

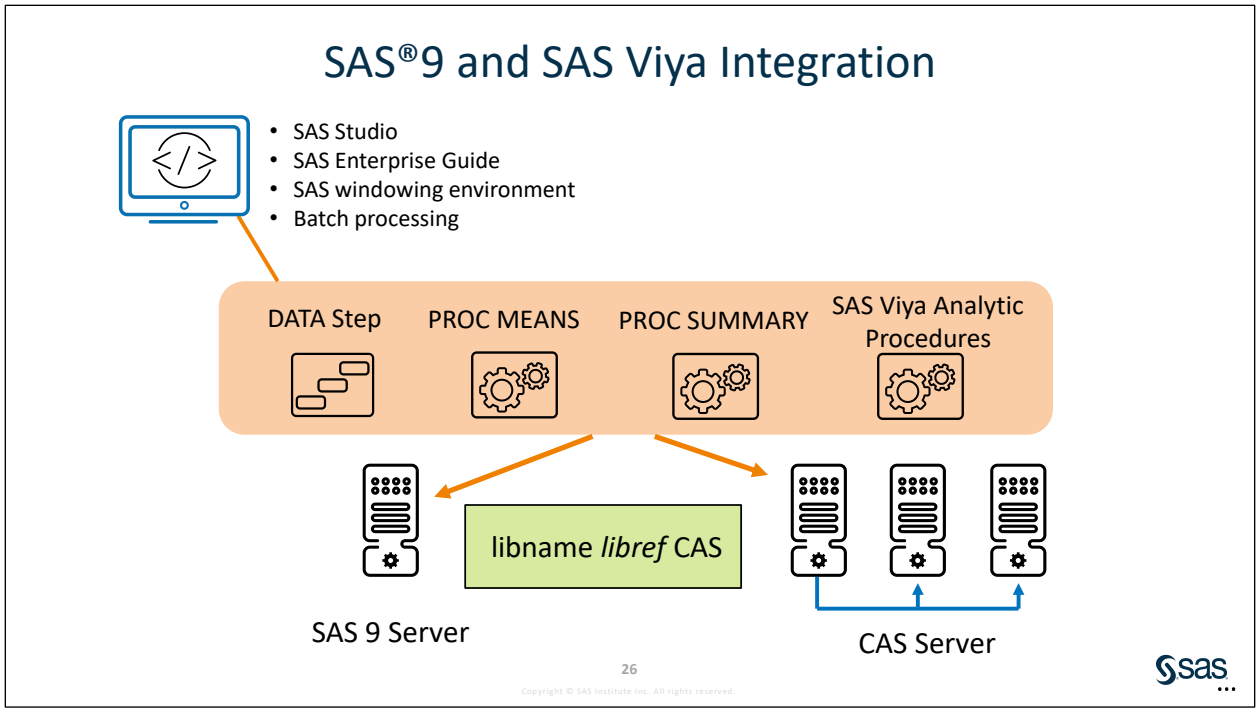
Considerations: Accessing CAS from a SAS 9.4 Client

Conform to CAS Encryption Requirements



25

If a SAS 9.4M5 client session does not meet the encryption standards of the CAS server, you need to make the appropriate certificates available. From the SAS Viya deployment, two certificates need to be made available to the SAS 9.4 client: the CA certificate that was used to sign the certificate that the CAS server is using, and the CA certificate that was used to sign the certificate that the Apache HTTP Server is using in order to interact with REST and Python. See Configure SAS 9.4 Clients to Work with SAS Viya on the Extended Learning page for more information.



After the connection and authentication to the CAS server is in place, the CAS LIBNAME engine provides Read and Write access to CAS tables from SAS. When the CAS LIBNAME engine is used by procedures, CAS table data is transferred between the SAS session and the CAS server as needed.

In addition to your users writing program code to access and load data into CAS, they can access SAS®9 data through the visual applications of SAS Viya that are accessed through SAS Drive.

SAS 9.4M5 and above provides integration with CAS through the Query Builder task and Upload to CAS task in SAS Enterprise Guide. You must define a CAS server definition in metadata and define a CAS LIBNAME in metadata. More information and further reading is maintained in SAS Documentation and on the Extended Learning page for this course.

Practice

1. Configuring a SAS 9 Client to Work with SAS Viya

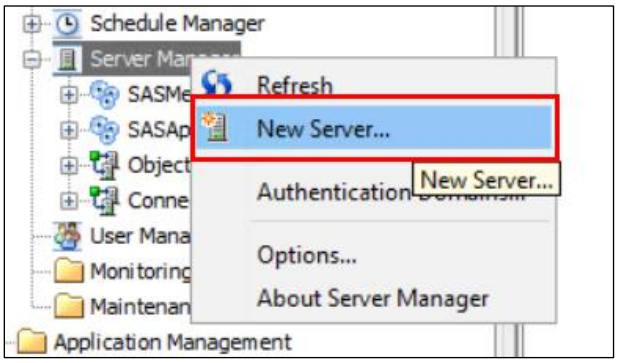
In this practice, you connect to SAS Viya from SAS 9. You will define a metadata server object for the CAS server, and store authentication information in users' metadata identities. Then you will test the connection using SAS Enterprise Guide.

Note: In a production environment, there are security certificates that are required to communicate between SAS 9 and SAS Viya. See the Extended Learning page for more information.

a. Open SAS Management Console on the Windows Server. It can be found on the Windows Start menu.

b. Using the metadata administrator, **sasadm@saspw**, with the password of **Student1**, expand Server Manager.

c. To create a metadata server to hold connection information for the CAS server, right-click on Server Manager and select **New Server**.



d. Scroll down the tree structure to locate the **SAS Servers** folder. Choose the server type: **SAS Cloud Analytics Services Server** and click **Next**.

e. Give the server a meaningful name, such as ***casapp***, and click **Next**.

f. You can fill in optional additional information at the server properties wizard screen, such as Major version number (3) and Minor version number (5). Leave the **Associated Machine** field as the default of **client.demo.sas.com**. Click **Next**.

g. At the SAS Cloud Analytics Services Information fields, enter the CAS server name and port information for the CAS host.

Server	**server.demo.sas.com**
Port	**5570**

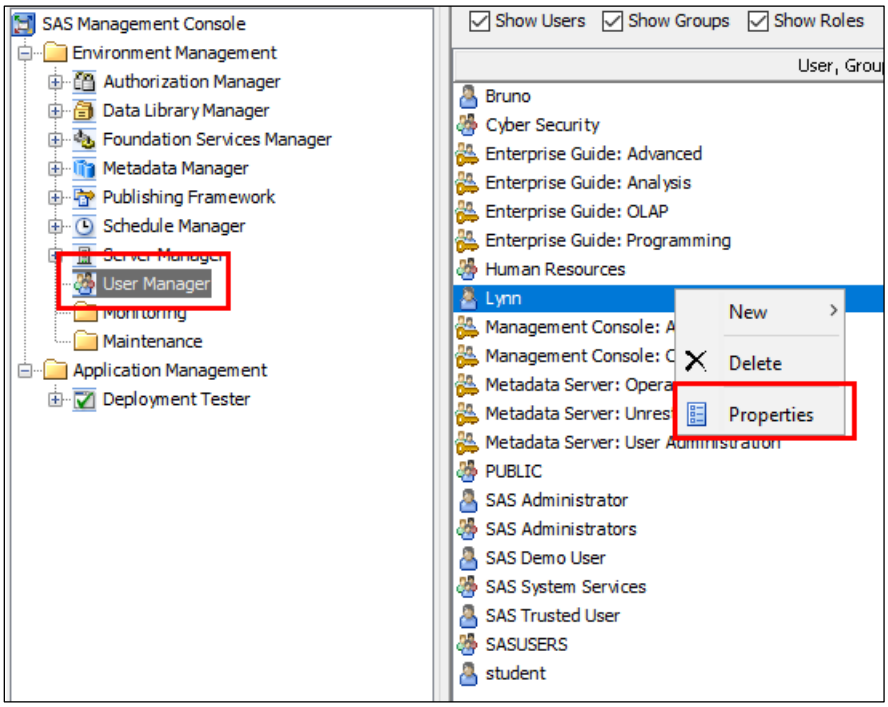
h. In the Authentication Information prompt, define a new Authentication Domain to store user authentication information for when they attempt to connect to this server. Click the **New** button to the right of **Authentication Domain: DefaultAuth**.

i. In the **New Authentication Domain** dialog box, give the Authentication Domain a meaningful name, such as ***casauth***, and click **OK**.

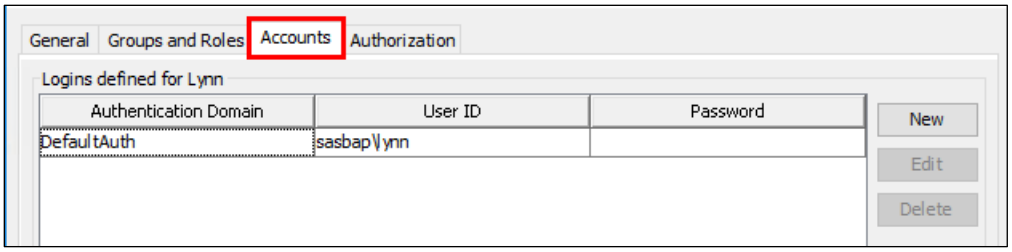
j. The new **casauth** authentication domain should automatically be selected. Click **Next**.

k. Review the new server information and click **Finish**.

l. For this practice, you need to store credential information so that users can authenticate with the CAS Server. Still in SAS Management Console, highlight the **User Manager** plug-in, and right-click the **Lynn** user to open their **Properties** window.



m. Click the user's **Accounts** tab to access the logins defined for their metadata identity.



n. Define a login for the CAS Server by clicking the **New** button.

o. In the New Login Properties dialog box, enter the user ID and password for the SAS Viya identity for this user. Be sure to select the newly defined **casauth** Authentication domain to pair these credentials with server connection information.

User ID	**lynn**
Password	**Student1**
Authentication Domain	**casauth**

Note: lynn's user ID is case-sensitive.

p. There should now be two logins defined. Click **OK**.

q. Verify the connection. Launch SAS Enterprise Guide from the **Start** menu.

r. Open the program **L02P1_egToCAS.sas** from the Recent Items list or at the path: **D:\Workshop\SAVI35**

s. This program code connects to CAS and lists detailed CAS Session and CAS services information to the log. You do need to define the **AUTHDOMAIN=** and **CASSERVERMD=** options to match the newly created authentication domain and SAS Cloud Analytics Services Server metadata object.

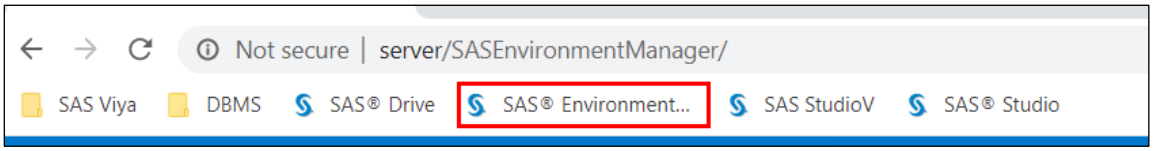
AUTHDOMAIN=	**casauth**
CASSERVERMD=	**casapp**

Note: If you named the Authentication domain or the SAS Cloud Analytics Services Server metadata object differently, enter those names here instead.

t. Run the program.

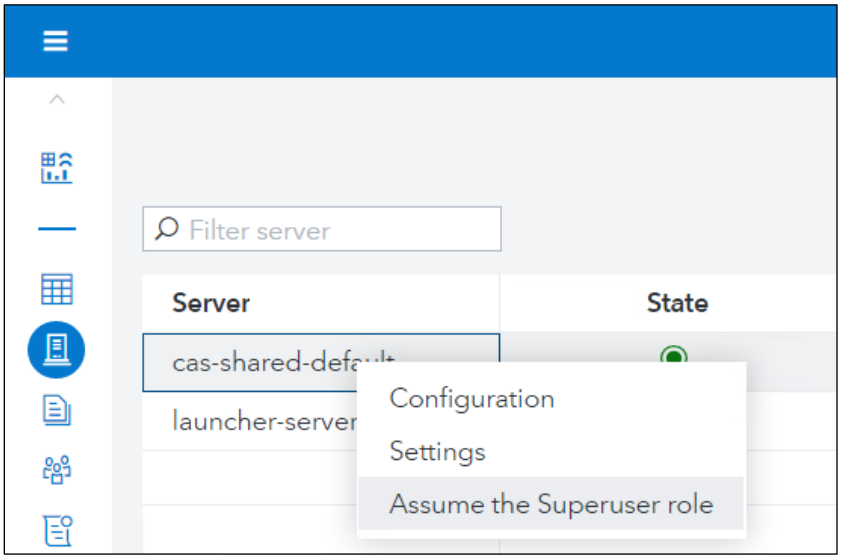
u. Check the SAS Enterprise Guide log to verify successfully credentials obtained from the SAS 9 metadata server, successful connection to SAS Viya Cloud Analytic Services, and successful authentication of Lynn.

v. Open a web browser and from the favorites bar, launch SAS Environment Manager.



w. As **christine**, opt into the SASAdministrators assumable group.

x. Proceed to the Servers page and assume the superuser role of the **cas-shared-default** server in order to check current sessions.



y. Right-click **cas-shared-default** for a second time and click **Configuration** to view connected sessions.

z. Is lynn connected?

aa. To disconnect the session, either run the commented-out cas statement with the terminate option in SAS Enterprise Guide, or just close SAS Enterprise Guide.

bb. Then relinquish the Superuser role on cas-shared-default and sign out of SAS Environment Manager.

2. (Optional) Creating an Authinfo File

In this practice, you create an authinfo file. The format of an authinfo file is based on the .netrc file specification that is used for FTP login. In addition to the .netrc file standards, the authinfo specification allows for putting commands in the file, as well as using quoted strings for passwords. The quoted strings allow for spaces within passwords and user IDs.

a. Create an **authinfo** file in Christine's home directory:

```
touch ~/.authinfo
```

b. Check permissions on the newly created file.

```
ls -al ~/.authinfo
```

c. Restrict access to everyone but Christine.

```
chmod 600 ~/.authinfo
```

d. Verify permissions.

```
ls -al ~/.authinfo
```

```
[christine@server ~]$ chmod 600 ~/.authinfo
[christine@server ~]$ ls -al ~/.authinfo
-rw-------. 1 christine users 0 Nov  1 14:31 /home/christine/.authinfo
```

e. Add credential definitions to the **authinfo** file.

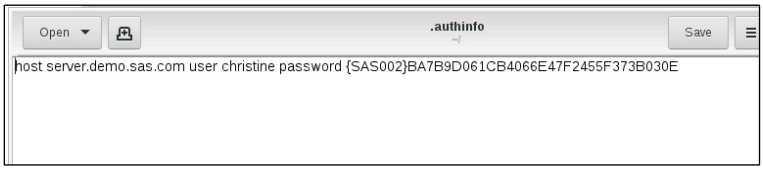
1) Use the PWENCODE procedure in SAS Studio to encode your password to store in the authinfo file.

```
proc pwencode in="Student1";
run;
```

2) From the log, copy the encrypted string of the password.

```
1          OPTIONS NONOTES NOSTIMER NOSOURCE NOSYNTAXCHECK;
72
73         proc pwencode in=XXXXXXXXXX;
74         run;

{SAS002}BA7B9D061CB4066E47F2455F373B030E
```

3) Edit the **authinfo** file using gedit in mRemoteNG. Or, use WinSCP.



4) Save the **authinfo** file.

Notes:

- SAS Studio does not use the authinfo file by default. To use the authinfo file in SAS Studio, you must specify either the AUTHINFO= SAS system option or the AUTHINFO= CAS statement option.
- It is possible to have multiple credential definitions in the authinfo file to access multiple systems.

The format of the credential entry is as follows:

- Generic credential to authenticate to host: default user *user ID* password *userpassword*

  Example: default user myuser ID password Myp4ssw0rd
- Credential to authenticate to a specific host: host *host name* user *user ID* password *userpassword*

  Example:
  - host my.cas.server user sasadm password {sas002}BA7B9D061CB4066E4…
  - host my.cas.server user sastest1 password {sas002}BA7B9D061CB4066E4…
  - host my.cas.server user sastest2 password {sas002}BA7B9D061CB4066E4…
- Credential to authenticate to a specific host on a specific port*:* host *host name* port: *port number* user *user ID* password *userpassword*
- To store authinfo file in another location:

  If you want to store the authinfo file somewhere other than the user's home directory, you need to use the AUTHINFO= option.

```
Options cashost="sasserver.demo.sas.com" casport=5570
authinfo="location";
Cas mycassession user=shrile;
```

  Or set an environment variable CAS_AUTH_METHOD to authinfo:

```
Options set=CAS_AUTH_METHOD_authinfo;
Options cashost="sasserver.demo.sas.com" casport=5570;

Cas myCASsession;
```

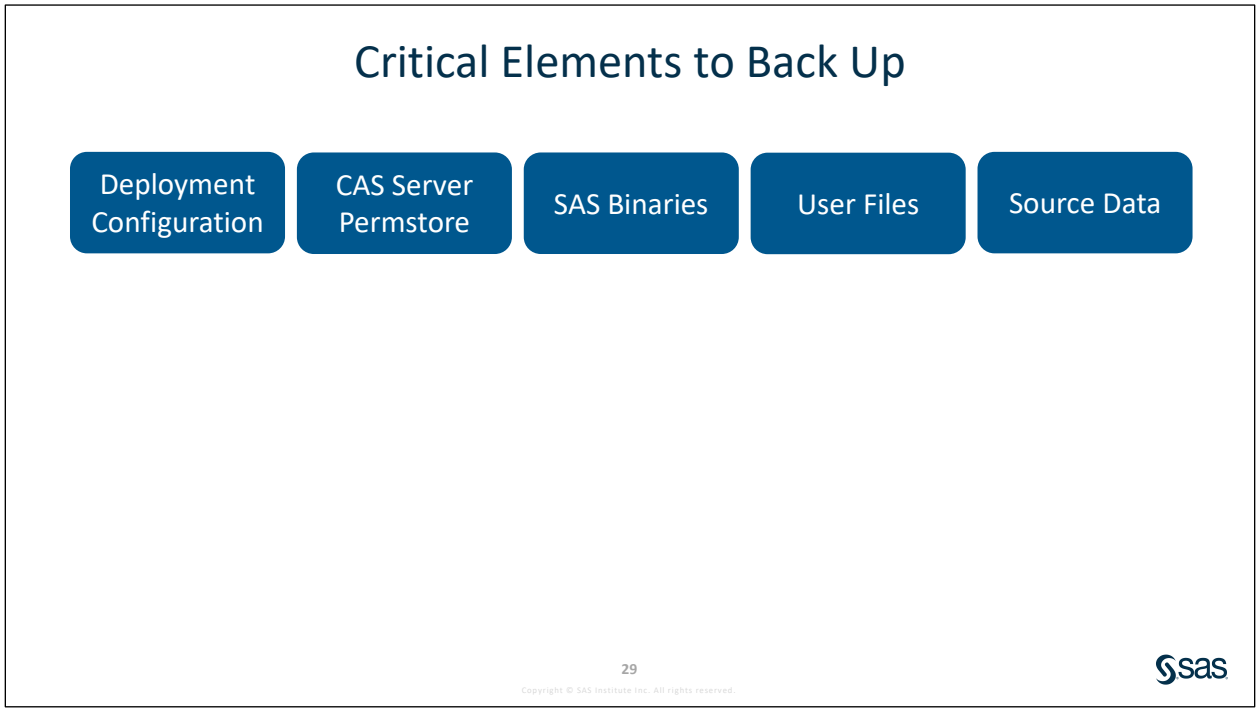
- For debugging purposes, there is a DEBUG option that will yield helpful diagnostics when the connection is failing.

```
options set=CASCLIENTDEBUG=1;
```

- If a SAS product uses an authinfo file, it does so based on the following precedence:
  1. Product-specific options
  2. The AUTHINFO= SAS system option
  3. The AUTHINFO environment variable
  4. The NETRC environment variable

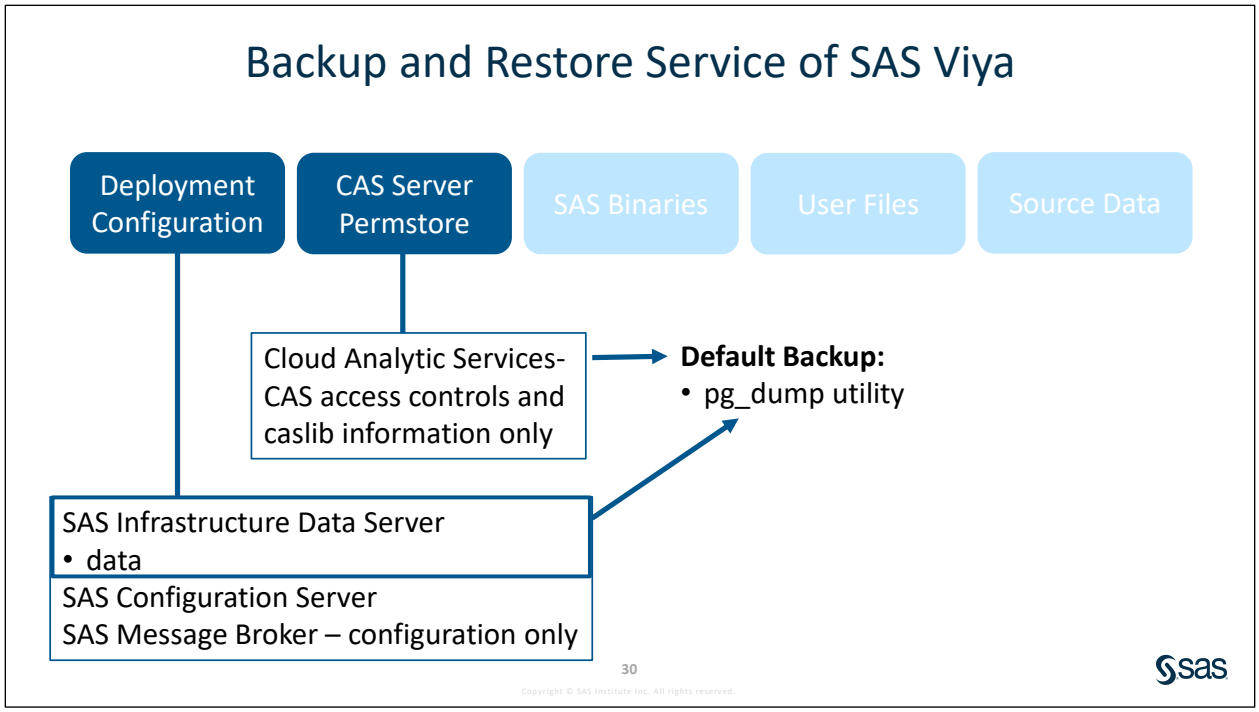
End of Practices

2.3 Backup and Recovery

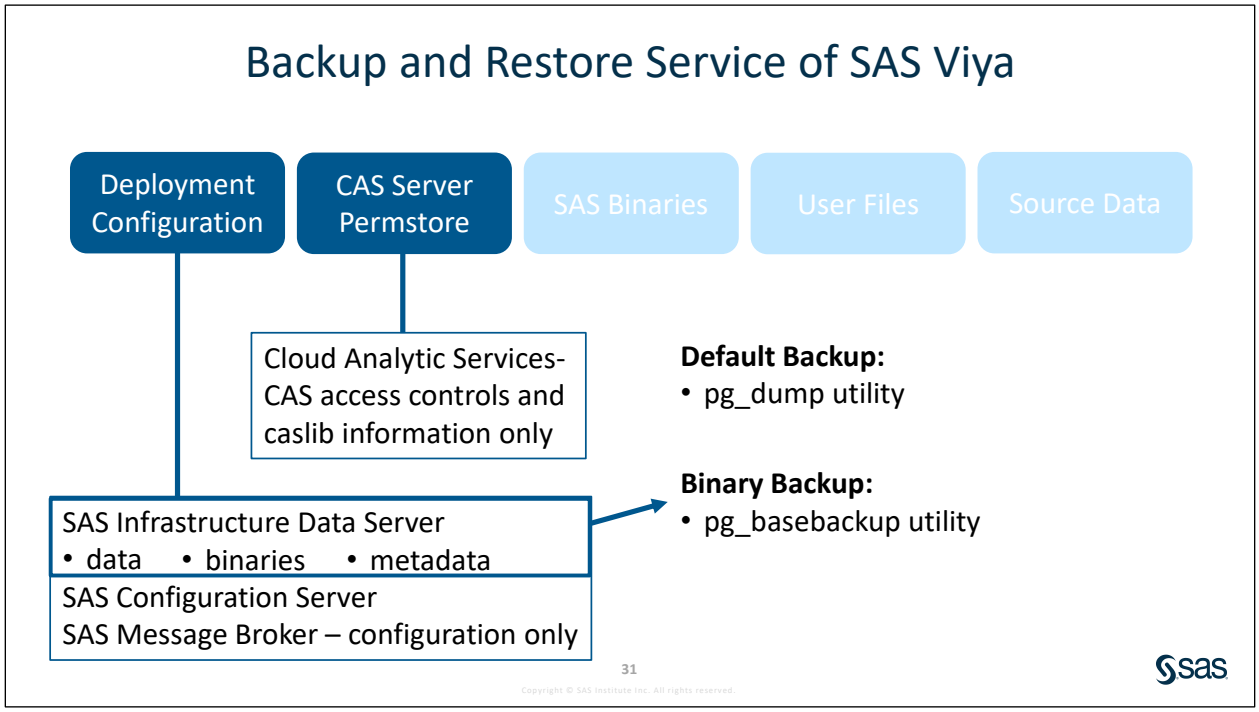


The critical components that need to be backed up include:

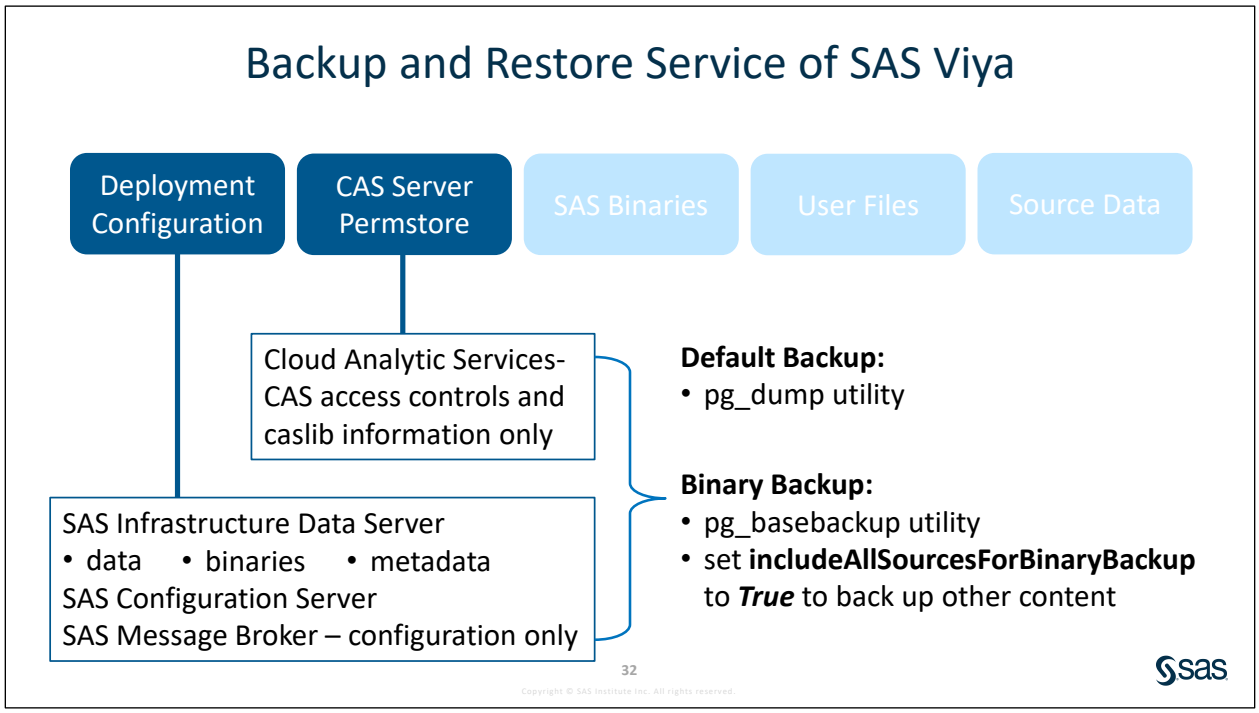
- SAS binaries
- deployment configuration
- CAS server permstore, which is where global caslibs are persisted
- user files
- source data.



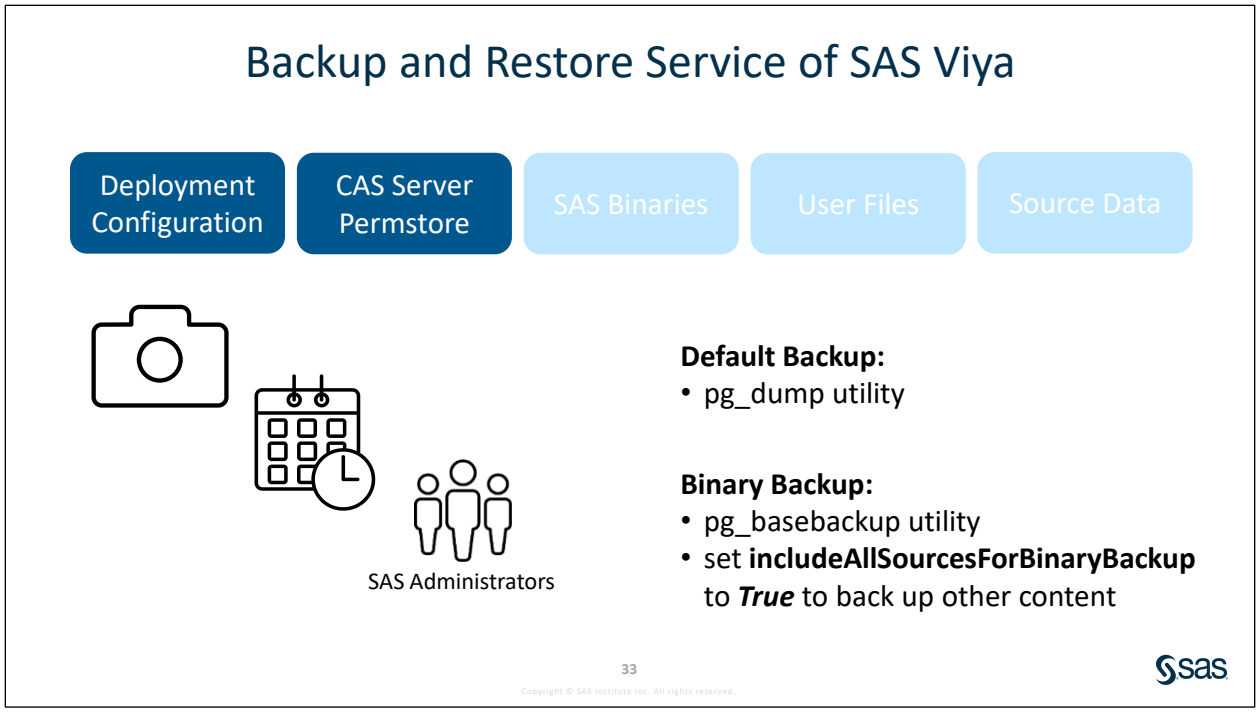
The backup function of SAS Viya offers two backup types. The Default backup uses the pg_dump utility to back up the content of the SAS Infrastructure Data Server. The Default backup also includes SAS Configuration Server, the configuration of the SAS Message Broker, and the CAS server Permstore, where CAS access controls and global caslibs are stored.



The other type is a Binary backup, which uses the pg_basebackup utility to back up the content of the SAS Infrastructure Data Server and it includes the data, the binaries of the PostgreSQL database, and the metadata (or system catalogs), such as user information, roles, and permissions. The Default backup back ups only the data.



If you set includeAllSourcesForBinaryBackup to True while initiating the backup, the binary backup will take the backup of remaining data sources (the SAS Configuration Server, SAS Message Broker, and SAS Server Permstore). This can be done through the Backup Manager in SAS Environment Manager.

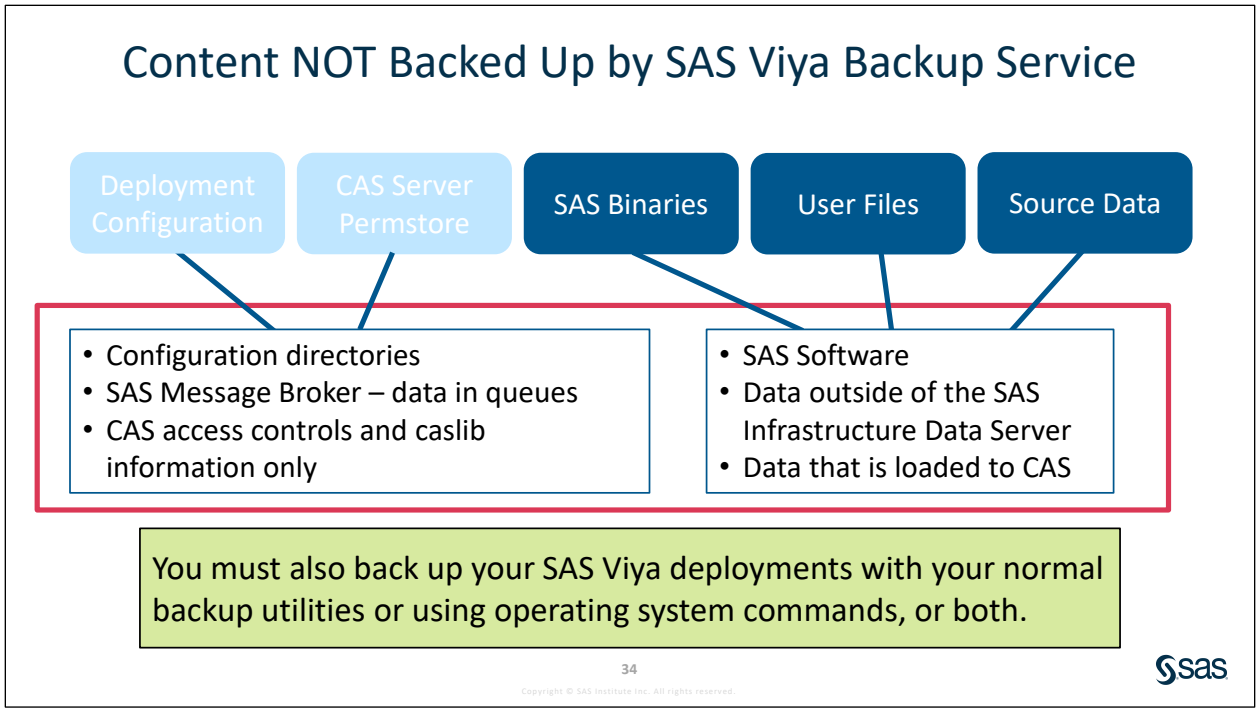


These backups work as a snapshot tool, which allows rollback to a previous state for an environment that is healthy (like saving progress in a computer game).

They are scheduled by default, but the time and frequency can be modified on the Jobs page of SAS Environment Manager.

On a standard deployment, only the members of the SAS Administrators group can perform the backup and restore operations, through SAS Environment Manager or the CLI.

On a multi-tenant deployment, a provider administrator can perform the backup and restore operations for all tenants, and a tenant administrator can perform the backup and restore operations for that tenant. On a multi-tenant deployment, the provider administrator and the tenant administrator must be the members of the SAS Administrators group.



The Backup Service does not protect all critical elements in your SAS Viya deployment!

Note: Most of the files that are located in the /opt/sas/viya/config/ directory structure are not included in the deploymentBackup policy, such as log files, services configuration files, and the Operations Infrastructure data mart.

What Needs to be Backed Up on Each Host

Type	SAS Viya Machines	CAS Controller	CAS Workers
SAS Binaries	✓	✓	✓
Deployment Configuration	✓	✓	✓
CAS Server Permstore		✓	
Source Data	Possible	Possible	
User Files	✓	Possible	

Some source data can be stored against the SAS Viya machine or the CAS controller machine, or both. Also, a shared drive, containing the data, could be accessible from these two machines.

Users can save some files against the CAS controller machine.

Recommended SAS Viya Deployment Backup Process

1. Schedule routine backup utility to run during downtime.
2. Stop the SAS Services.
3. Use your third-party backup utility on each machine to do a complete backup of your SAS Viya deployment.
4. Restart the SAS Services.
5. Move the backup files from all machines to a shared vault location.
6. Generate a backup log.

In a distributed environment, an orchestration tool such as Ansible or Puppet can be used to manage the process.

35

Best Practices for Taking Backups

- Use the system tools to perform a full backup of the entire SAS Viya environment.
- Use the Backup and Restore tools to perform backups of the content and configuration between full backups.
- Perform a backup before and after major changes, such as installing software updates, changes to topology, modifications to SAS Viya configuration, before and after changes to authorization (permissions), and creating, altering, or dropping global caslibs.
- Backups should be scheduled at non-peak hours.
- Back up your backups. Old backups are purged after the retention period.

36

Restoring SAS Viya Content and Configuration

A restore using the Backup Manager or CLI restores content to the following destinations:

- SAS Configuration Server
- SAS Message Broker
- SAS Infrastructure Data Server

Pre-restore validations should be done before performing a restore using a given backup. It includes the following validation checks:

- Does the provided backup exist?
- Is the backup completed?
- Is the backup purged?
- If PostgreSQL is being restored using the default type of backup, does the list of databases in the backup match the list of databases currently present in PostgreSQL?
- If the restore is using the binary type of backup, is the *includeAllSourcesForBinaryBackup* property set to true?

Use the ***default backup restore*** when the data is lost in the database, or when the PostgreSQL metadata is not significantly changed. Do not use default backup restore if the SAS Infrastructure Data Server is unresponsive.

- Always use the default backup to restore to an alternate host.
- Use the ***binary backup restore*** when any change happens to the database content and metadata.
- The SAS Infrastructure Data Server (that is, PostgreSQl) portion of a binary backup must be restored manually. You can use the restore operation for other restore after this is done.

Note: The restore of the CAS Server Access Controls and caslib information is a secondary operation and is not performed as part of the restores begun by the Backup Manager or the CLI.

A partial set of services and servers must be running to perform a restore:

- SAS Backup Server – sas-viya-deploymentBackup-default
- SAS Backup Agent – sas-viya-backup-agent-default
- SAS Configuration Server – sas-viya-consul-default
- SAS Configuration Service – sas-viya-configuration-default
- SAS Message Broker – sas-viya-rabbitmq-server-default
- SAS Infrastructure Data Server – sas-viya-sasdatasvrc-postgres*
- SAS Identities service – sas-viya-identities-default
- SAS Logon Manager – sas-viya-saslogon-default
- Apache HTTP Server – sas-viya-httpproxy-default
- SAS Cache Locator service – sas-viya-cachelocator-default
- SAS Authorization service – sas-viya-authorization-default
- SAS CAS Controller – sas-viya-cascontroller-default
- CAS Management Service – sas-viya-cas-management-default
- SAS Secrets Manager – sas-viya-vault-default

Recommended Recovery Process

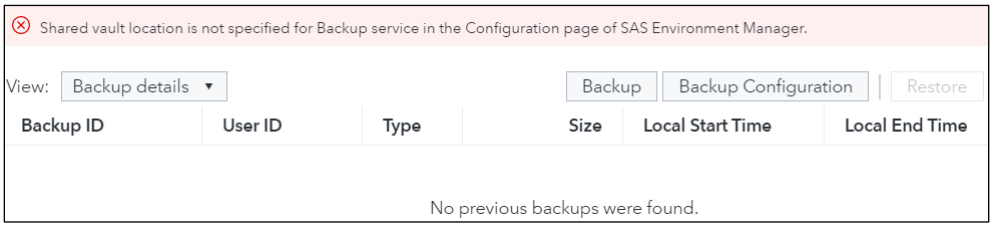
1. Choose a backup.
2. Stop the SAS Services.
3. Restore the required content on each machine from the selected backup files.
4. Start the SAS Services.
5. Generate a restore log.

In a distributed environment, an orchestration tool such as Ansible or Puppet can be used to manage the process.

Using the Backup Manager in SAS Environment Manager

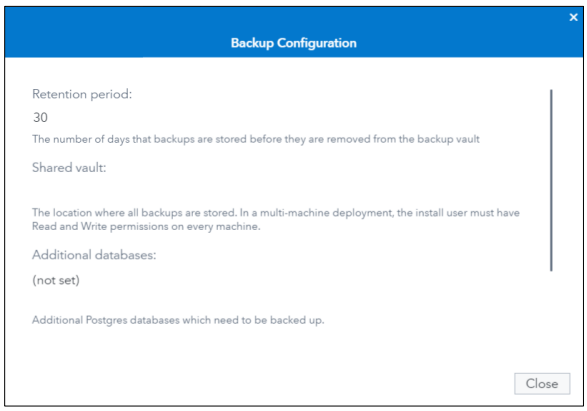
1. If you do not have an active SAS Environment Manager session, open a Chrome browser and select **SAS Environment Manager** on the Bookmarks toolbar. Sign in as the user **christine** with the password **Student1**. Assume the **SASAdminstrator** role.
2. Click **Backup and Restore** on the side menu.

3. You need to specify a vault location before a backup can be run.



4. Click the **Backup Configuration** button.

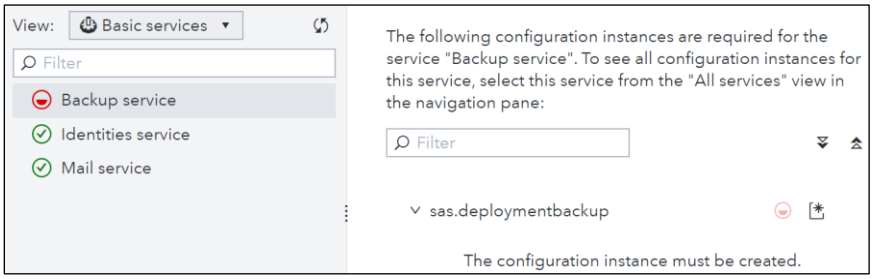
The retention period is set to 30 days, by default, but the **Shared Vault** value is not set. You can modify these values from the Configuration page.



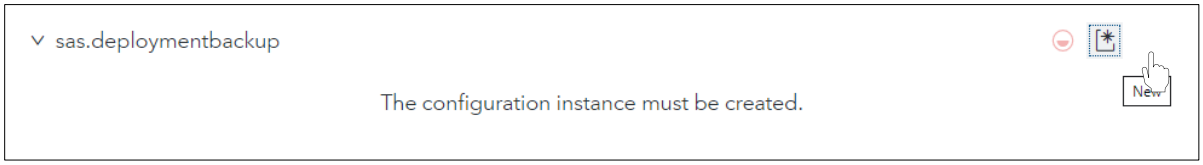
5. Click **Close**.
6. Click **Configuration** from the side menu.

7. Click **Backup service**. The shared vault is any network location where the backup files are moved to, from the local vault on each machine in your SAS Viya deployment. (The location of the local vault is set to *SAS-configuration-directory*/**backup** on Linux and Windows by default automatically by the backup service.)

   Specify a unique vault location for every SAS Viya deployment.

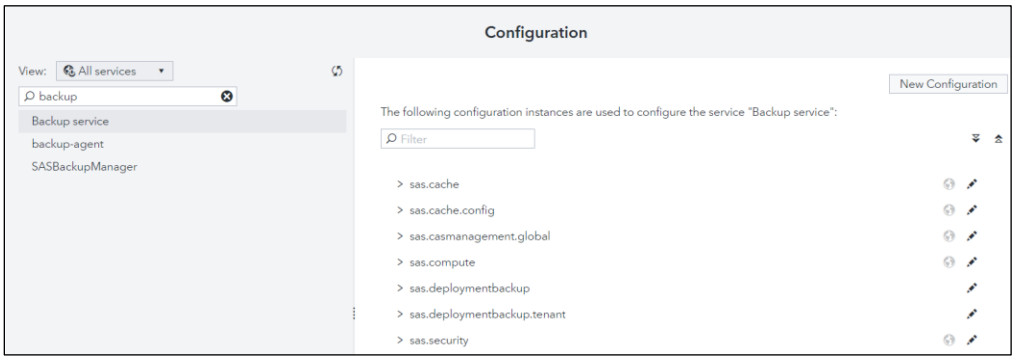


8. Click **New**.

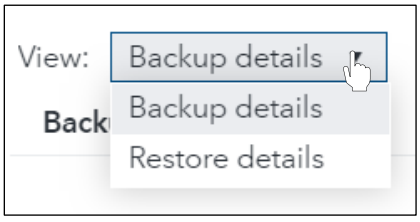


9. Scroll in the sas.deploymentbackup Configuration window until you find **sharedVault** and enter **/sasViyaBackups** in the field. Click **Save**.

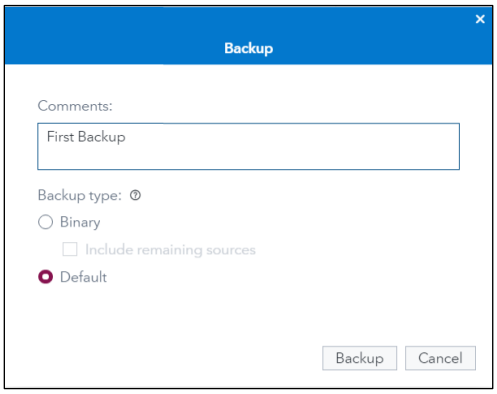
   The **sas.deploymentbackup** window is now configured.



10. Go to the Backup and Restore page to view details and properties of backups. You can view the backup or restore details by using the **View** drop-down menu.

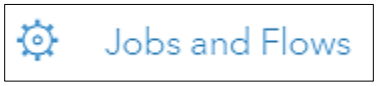


11. Click **Backup**. Write a comment. Keep the Default backup type checked.

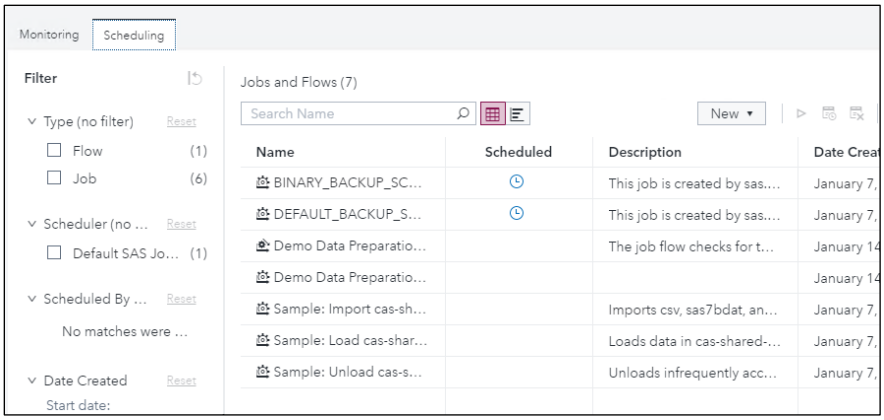


The Binary backup also backs up the system catalogs of the PostgreSQL database and the data whereas the default backup backs up data only.

12. While the backup is running, click **Jobs and Flows** from the side menu.

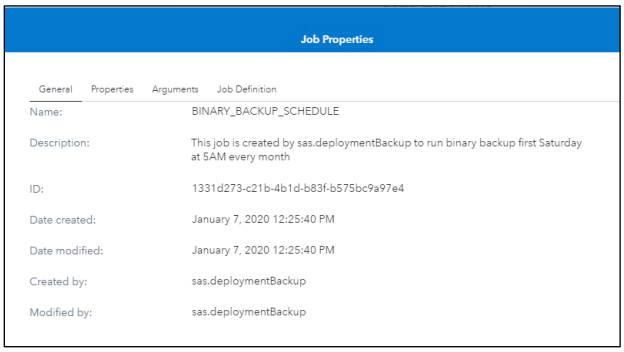


13. Click the **Scheduling** tab.



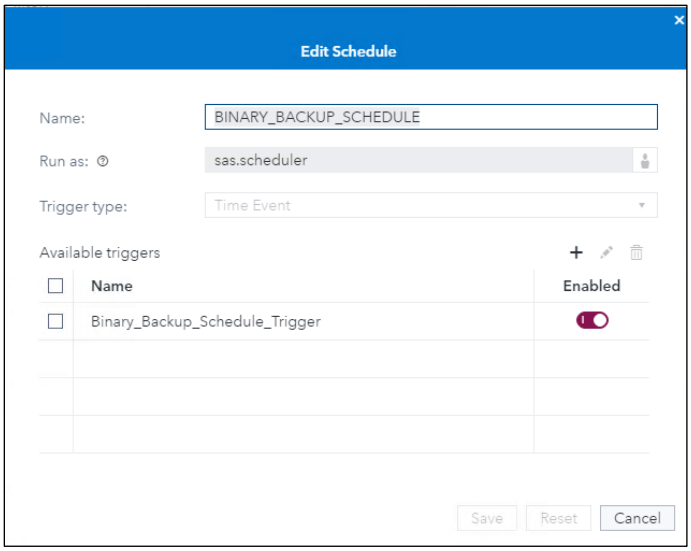
Note: If **DEFAULT_BACKUP_SCHEDULE** does not exist, restart the sas-viya-deploymentBackup service and check again.

14. Highlight **BINARY_BACKUP_SCHEDULE**. Click **Properties**  . The job is scheduled to run the binary backup the first Saturday at 5:00 am every month. A best practice is to set the *retentionPeriod* value such that you always have at least the last three to four backups available at any point in time. The retention period is 30 days, but that is modifiable.

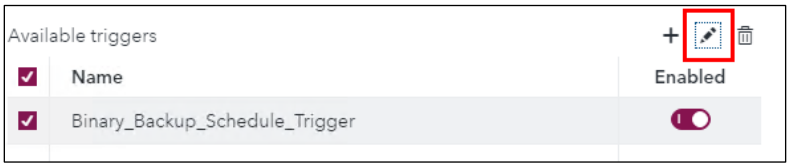


15. Click **Close**.

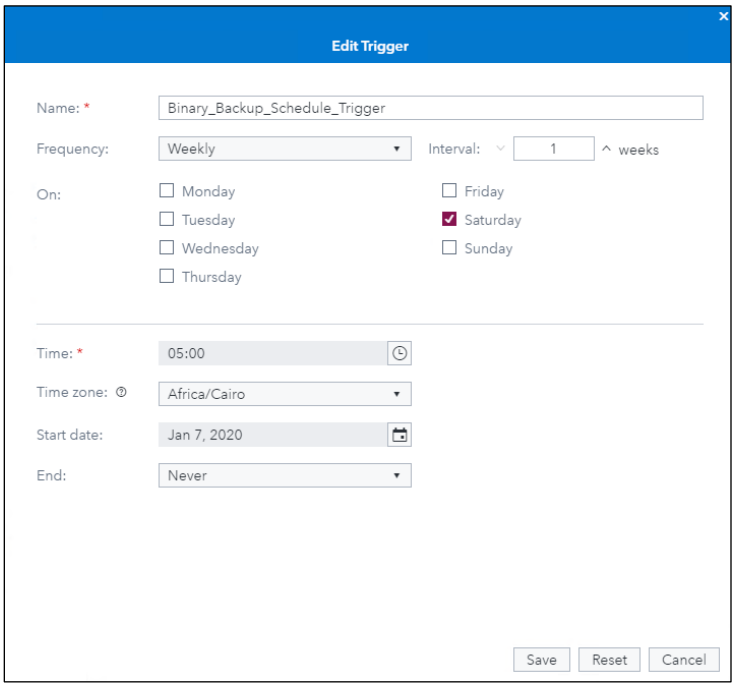
16. Click **Edit Schedule**.



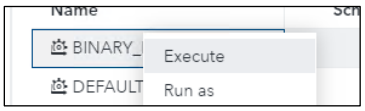
17. Check the box next to the current available trigger and select **Edit Trigger**.



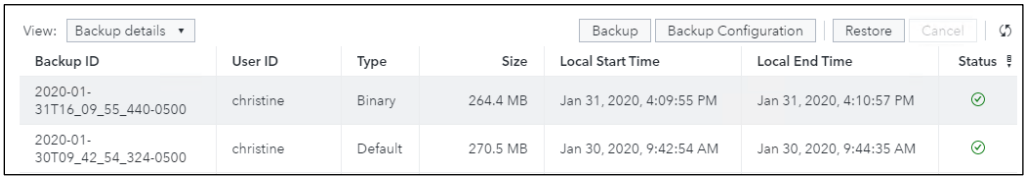
18. Change **Frequency** to **Weekly** and check **Saturday**. You would want to change the frequency or retention of backups to follow the best practice of keeping at least four backups. (By default, one binary backup would be kept and four default backups.)



19. Click **Save** to close the Edit Trigger window**.**
20. Click **Save** to close the Edit Schedule window**.**
21. Right-click the scheduled binary backup and select **Execute**.



22. Go back to the **Backup and restore** page. Click **refresh**. Both backups are displayed.



Note: The following services must be running in order to run the backup schedule:

Name on Linux	Name on Windows
sas-viya-identities-default	SAS Identities Service
sas-viya-scheduler-default	SAS Scheduling Service
sas-viya-jobdefinitions-default	SAS Job Definitions Service
sas-viya-jobexecution-default	SAS Job Execution Service
sas-viya-restexecutionprovider-default	SAS REST Execution Provider Service

23. Open a **mRemoteNG** session for **christine**.
24. Navigate to **/opt/sas/viya/home/bin** to access **sas-admin**.

```
cd /opt/sas/viya/home/bin
```

25. Log on to the CLI utility if needed.

```
./sas-admin auth login
Enter credentials for https://server:

Userid> christine

Password> <enter Student1>
Login succeeded. Token saved.
```

26. The backup and restore CLI backs up and restores the same content as the Backup Manager in SAS Environment Manager. Three backup CLI commands are specific to the backup service: start (start an ad hoc backup), list (list all backups), and show (show backup details).

    (The restore CLI can start a restore, list all restores, and show restore details.)

    Issue the following command:

```
./sas-admin backup start -h
```

```
[christine@server ~]$ /opt/sas/viya/home/bin/sas-admin backup start --h
NAME:
   sas-admin backup start - Starts a backup.

USAGE:
   sas-admin backup start [command options] [arguments...]

OPTIONS:
   --backup-type, -t "default"                  Specifies the type of backup to be taken. The default value is as follows:
"default". The valid values for the "backup-type" option are as follows: "default", "binary"
   --comments, -c "default comment"             Specifies free text comments that are associated with this backup operation
. The default value is as follows: "default comment"
   --configuration-id, -n "default"             Specifies the ID of a backup configuration to be used for a backup operatio
n. For now, only the default configuration is supported. The default value is as follows: "default"
   --include-all-sources-for-binary-backup, -i  Specifies whether to include other sources in the backup when the "backup-t
ype" option is specified as "binary". If the "true" value is specified, then all sources are included. The default value is
 as follows: "false"
   --provider-only, -p                          Specifies to start the backup of the provider tenant only on a multi-tenant
 deployment.
   --slug, -s "default slug"                    Specifies the name that is given to a backup operation. The default value i
s as follows: "default slug"
   --tenants                                    Specifies a list of tenants to be backed up on a multi-tenant deployment. T
he list of tenants must be separated by comma. Only a provider administrator can specify the list when the provider-only fl
ag is not specified.
   --version, -v "2"                            Specifies the version of the media type. The default value is 1.
```

End of Demonstration

Practice

In these practices, you perform the following tasks:

- Set the Shared Vault value for the backup artifacts.
- Use the Backup Manager in SAS Environment Manager to create a backup.
- Use the CLI to retrieve the backup details.

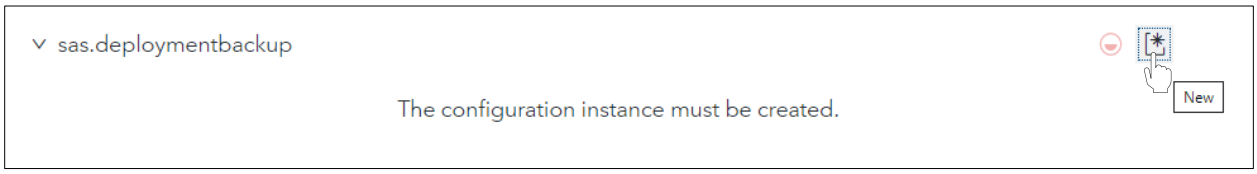
3. Configuring the Shared Vault with SAS Environment Manager

a. If you do not have an active SAS Environment Manager session, open a Chrome browser and select **SAS Environment Manager** on the Bookmarks toolbar. Sign in as the user **christine** with the password **Student1**. Assume the **SASAdministrator** role.

b. Click **Configuration** on the side menu.

c. Click **Backup service**. The icon indicates that the backup configuration is not yet created. The shared vault location needs to be entered. The shared vault is any network location to preserve the backups from all tiers. The backup files are moved from local vault to shared vault. It is referred to as sharedVault in the SAS Environment Manager user interface.

d. Click **New**.



e. Scroll in the sas.deploymentbackup Configuration window until you find **shareVault** and enter **/sasViyaBackups** in the field. Click **Save** when it is complete.

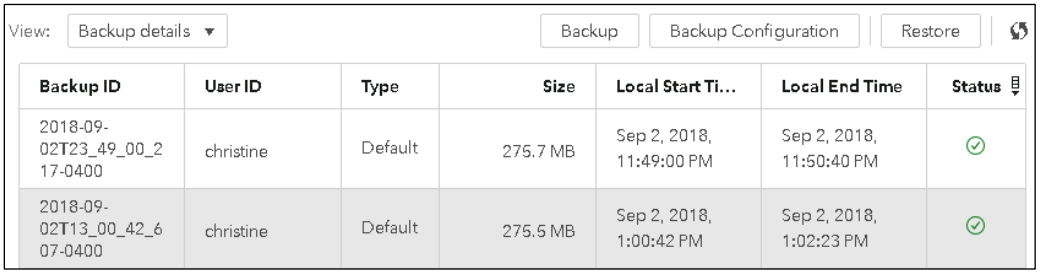
4. Performing a Backup with Backup Manager in SAS Environment Manager

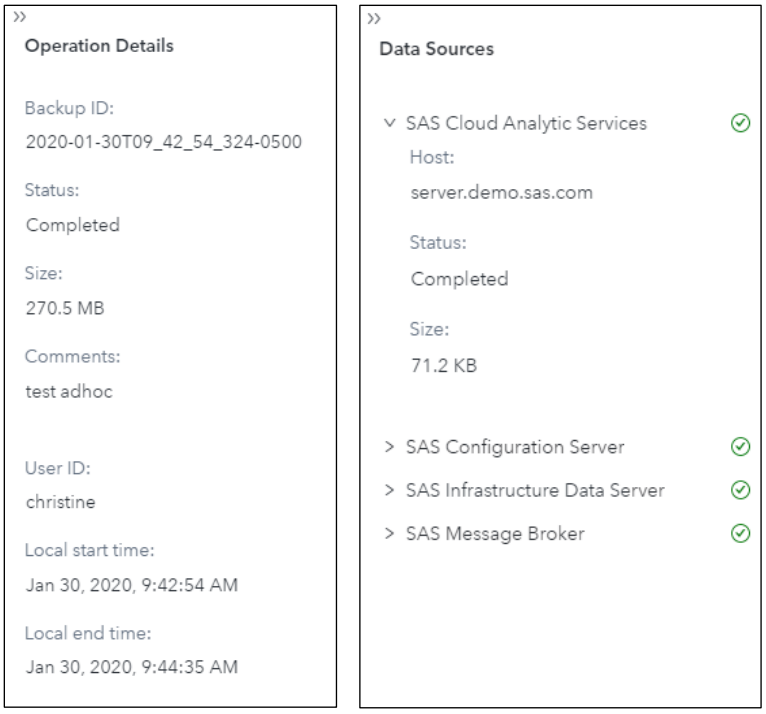
a. Select **Backup and Restore** page from the side menu. Click the **Backup** button to start a backup.

b. Enter **My first Viya Backup** in the **Comments** field. Under Backup type, verify that the **Default** radio button is selected. Start the backup by clicking the **Backup** button.

c. When the backup is complete, click **Close** on the window that appears.

d. Click the backup name in the first column. Examine the backup details and the data sources on the right side of the window.





5. Using a Backup CLI to View the Backup

a. If an mRemoteNG session for christine is not started, open one now.

b. Change the directory to **/opt/sas/viya/home/bin** to access **sas-admin**.

```
cd /opt/sas/viya/home/bin
```

c. Log on to the CLI utility. (You need to do this step only if you have not used the CLI in the past 12 hours.) Supply the credentials for Christine: **christine** and **Student1**.

```
./sas-admin auth login
```

d. Open a list of your backups. The value in the **Name** column is used for subsequent commands.

```
./sas-admin backup list
```

e. Use the SHOW option on the backup plug-in to obtain more details from the backup.

```
./sas-admin backup show --id <BackupID from the list command>
```

End of Practices

2.4 Managing Your SAS Viya Software

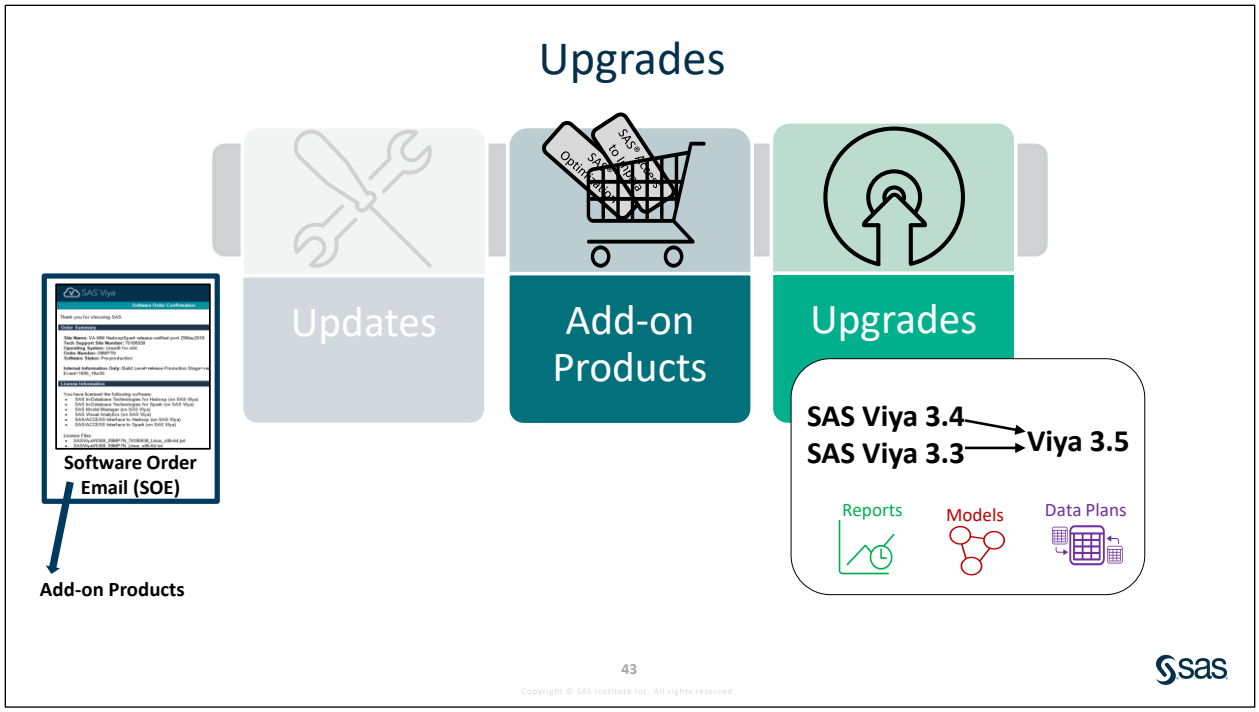
When hot fixes are released for a version of SAS Viya, you can apply these hot fixes to update the software. These updates are intended to be compatible with existing configuration, content, and data of your SAS Viya version and do not require a new software order.

There is an exception to SAS Viya 3.4 release 19week21. You ***do*** need a new Software Order Email.

An add-on product is new software that is added to your deployment and requires a new software order. Adding new software to your deployment will also update your currently deployed software.

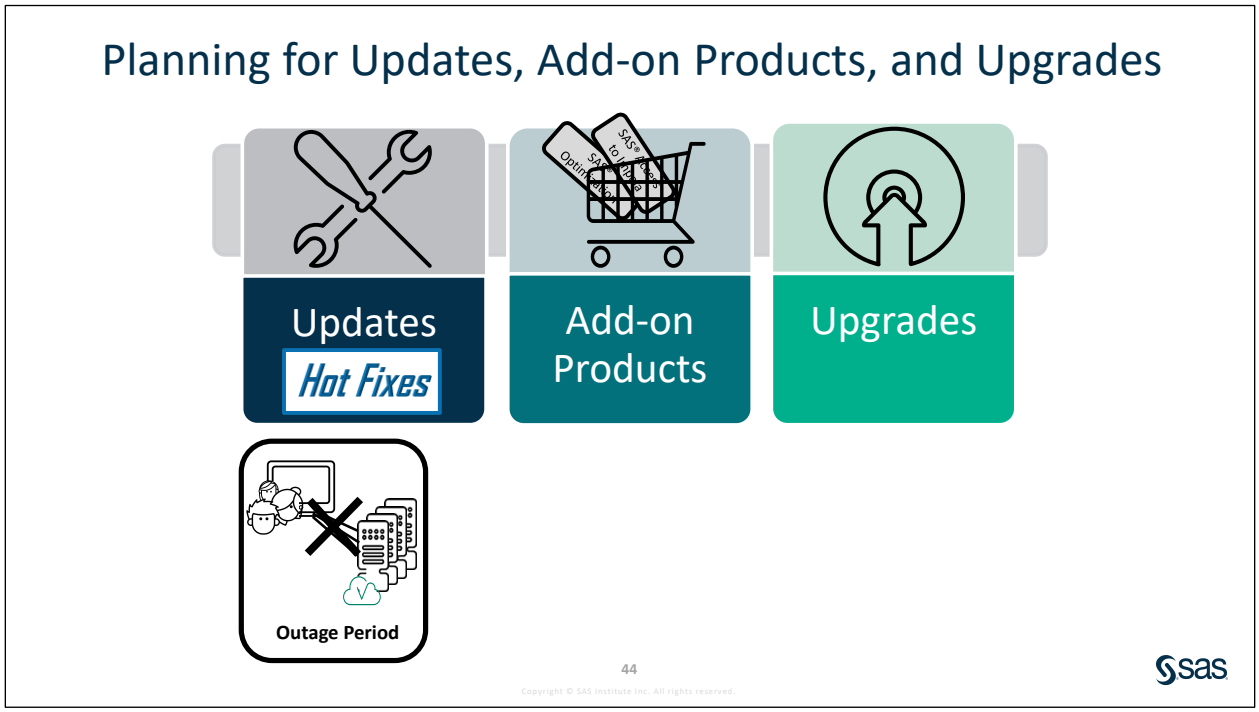
Here are some common scenarios for adding SAS Viya software to your existing deployment:

- Add new software from your initial SAS Viya order.
- You ordered software and did not install all of it.

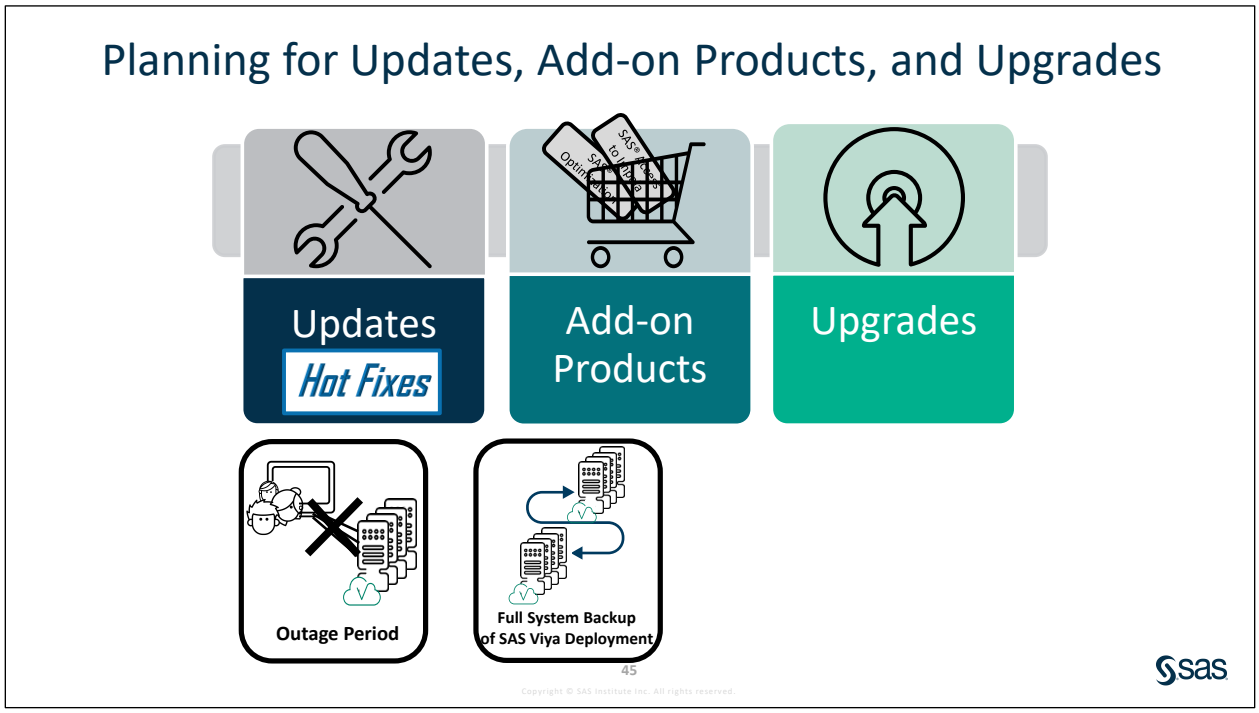


An upgrade adds significant feature changes or improvements to your deployed software, such as upgrading from one version of SAS Viya to a newer version. An upgrade is designed to maintain all content created in the previous version of SAS Viya, so reports, data plans, or models will be preserved.

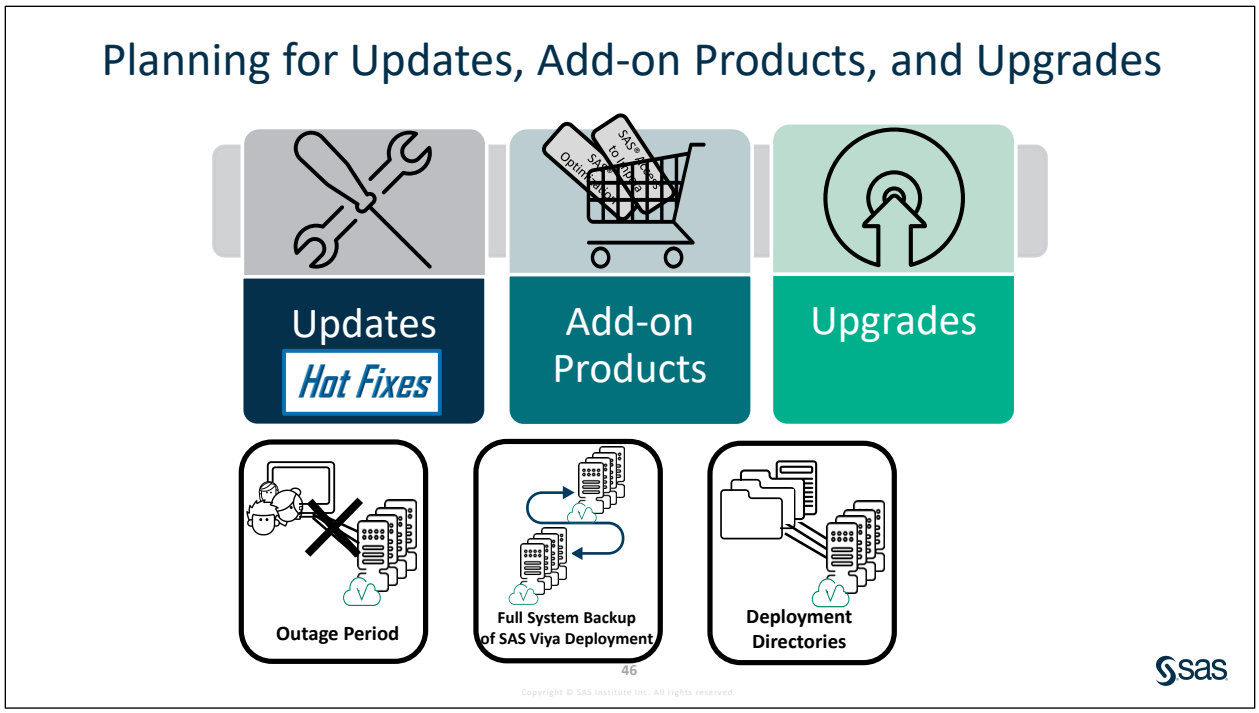
The process is similar to adding products. You will need a new software order, and any add-on products present in the order will be installed as part of the upgrade process.



Regardless of whether you are applying hot fixes, adding products, or upgrading to a newer version, SAS Viya software requires an outage period because some SAS Viya services are stopped and restarted automatically during the update process.



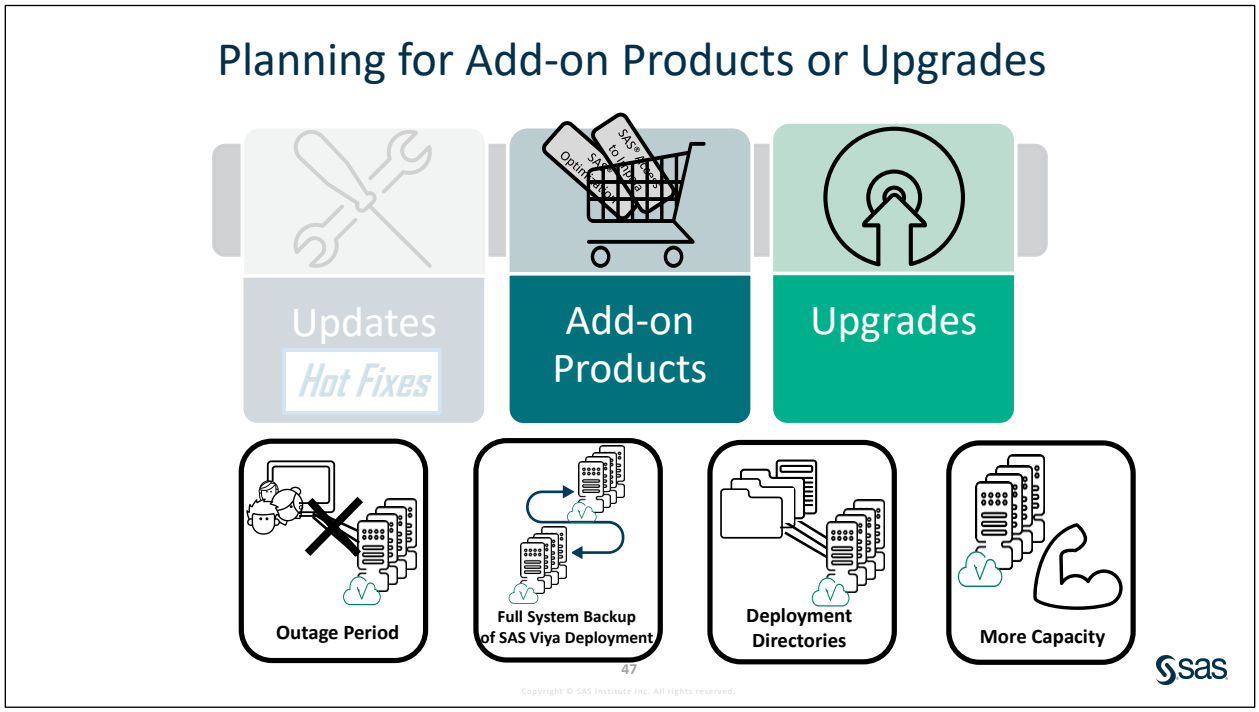
Make sure to do a full system backup of your deployment prior to making any changes! A good backup is critical as there is no rollback from an upgrade, failed or not.



You will need the location of the directory on each machine where you stored deployment and maintenance files. And if you have added any CAS servers to your initial deployment, you must update those CAS servers as well as each machine in your initial deployment.

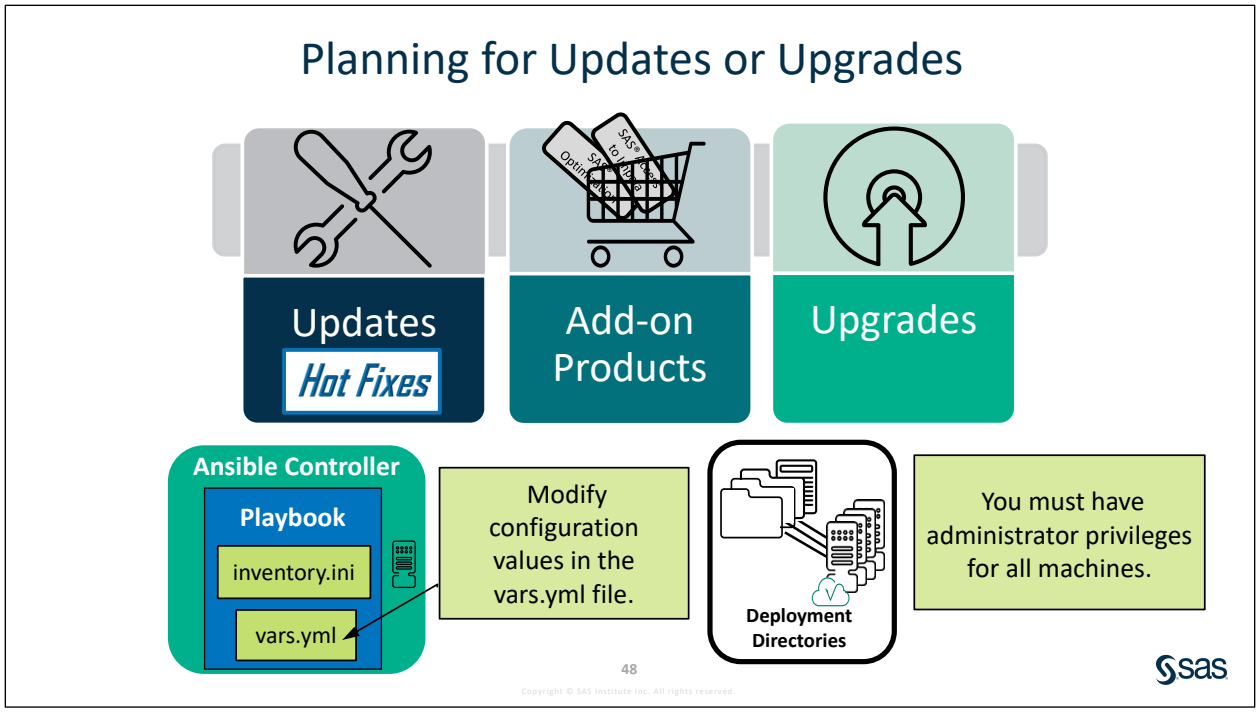
Note: The process is the same regardless of whether the deployment is single-tenant or multi-tenant.

Note: An upgrade will most likely require changes to the deployed software's configuration.



You might need to expand your environment's capacity before installing an add-on product, because it is added to your currently deployed software, and you might need more resources than what was originally required.

Also, before an upgrade, make sure all the system requirements for the new version of the software are met. System requirements do change between releases.



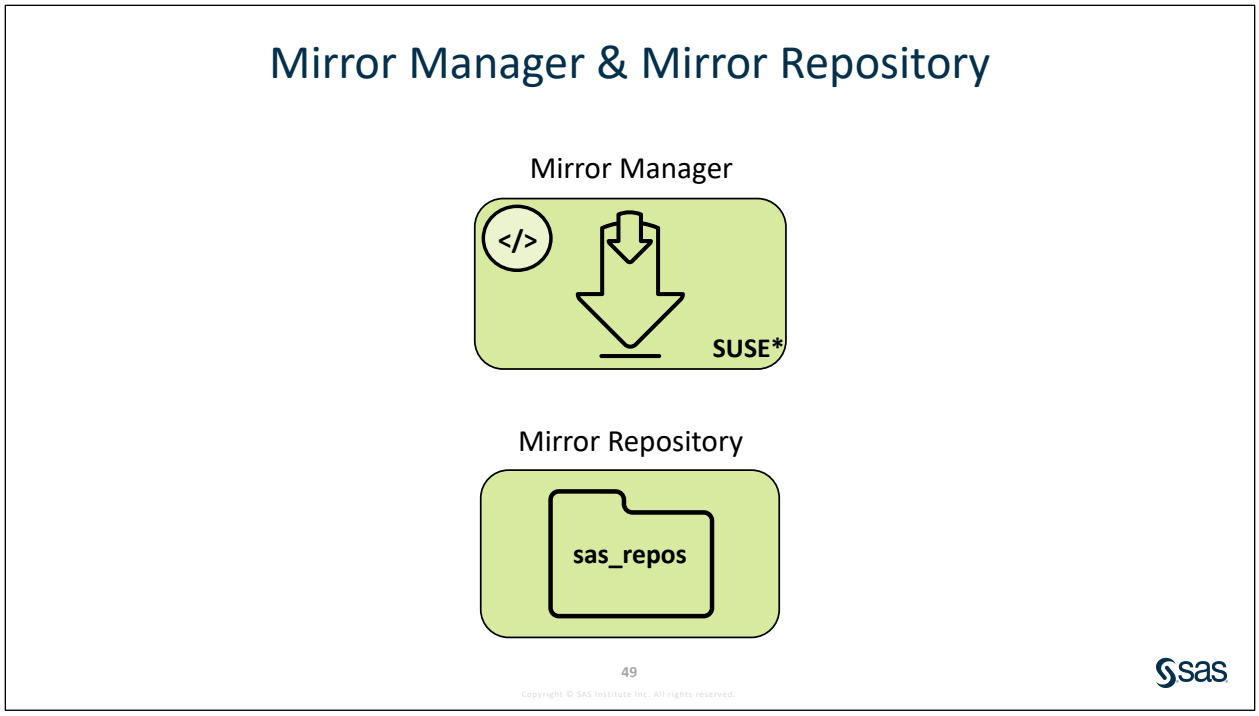
You perform the updates and upgrades with the same command that was used to install SAS Viya, and the same playbook. If you used an Ansible playbook for your initial installation, you should update with Ansible.

Running the playbook updates all software to the latest version (no partial updates). To perform the update process, you must have administrator privileges and sudo access for the machines.

Note: If you want to update your deployment from programming-only to full, you can use only Ansible.

Note: You will need to download the current version of the SAS orchestration CLI to generate a new Ansible playbook for your deployment, and then run the new Ansible playbook.

Note: The update process preserves any user-modified configuration values in the vars.yml file, but changes made to other files in the deployment might be lost. Therefore, SAS recommends that you make changes to vars.yml when possible in order to avoid any loss of customizations that you made to other files.



SAS Mirror Manager is a command-line utility for synchronizing a collection of SAS software repositories. Its primary use is to create and manage repositories for software deployment. The SAS Mirror Manager downloads the software that you ordered and creates a mirror repository. The mirror repository represents the same version of the packages in your SAS Viya deployment, and by default the repositories are placed in the sas_repos directory in the installation user's home directory.

Note: A mirror repository is required for all SAS Viya deployments on SUSE Linux. For other platforms, it is optional.

Pre-update and Post-update Reports

Before and after a planned update, administrators should run reports on installed products on each host of the SAS Viya system. One example is to use the **sas-ops info** command from a single host.

1. Enter the following command as the sas or installer user:

```
/opt/sas/viya/home/bin/sas-ops info >
/workshop/LWSAVA35/beforeViyaUpdate.txt
```

Note: These commands would be run after an update to verify the updated environment.

```
/opt/sas/viya/home/bin/sas-ops info > /tmp/afterViyaUpdate.txt

diff -U 1000 /tmp/beforeViyaUpdate.txt /tmp/afterViyaUpdate.txt
```

Update Process

1 Generate reports from your current SAS Viya deployment.

This step is required to obtain information about the current version of SAS Viya packages deployed in your environment.

Note: You can generate several reports (step 1 and 4):

- using rpm and yum commands on each machine in your SAS Viya deployment before and after the update process.
- using Ansible, which will generate all reports (before, after, and compare/differences). The process generates reports on each SAS Viya machine in your deployment and then centralizes all reports on the Ansible controller machine to produce the compare/differences report.
- using sas-ops info report (above demonstration).

2 (Optional) Update your SAS Viya mirror.

If you are using a mirrored repository, you need to re-synchronize the mirror prior to performing the update. The re-synchronizing makes the new software available to the mirrored repository so that it can be installed in the environment.

3 Update your SAS Viya deployment.

- Update with **Ansible**. To update the software and apply the hot fixes, use the **ansible** command that was used to deploy the software.
- Update with **yum**. Note that you can use yum to update your software only if your deployment is on Red Hat Enterprise Linux or an equivalent distribution.
- Update with **Zypper**. Note you can use zipper to update your software only if your deployment is on SUSE Linux or an equivalent distribution.

4 Generate reports from your updated SAS Viya deployment.

This step is required to obtain information about the current version of SAS Viya packages deployed in your environment ***after*** your update.

5 Compare reports.

You will be able to compare before and after update reports to see what changed in your SAS Viya deployment.

End of Demonstration

Practice

6. Mirror Repository Difference

The mirror repository represents the same version of the packages in your SAS Viya deployment. The SAS Hosted repository is dynamic and will always be updated with the latest versions of the packages. It is important to run a report to determine the differences between your mirror repository and the SAS Hosted repository.

a. Use the **sas** connection in MRemoteNG.

b. Navigate to **/sas**.

```
cd /sas
```

c. Run the following command (command is written on one line):

```
./mirrormgr mirror diff --deployment-data
/sas/Full/SAS_Viya_deployment_data.zip --path /sas/Full --
latest --platform x64-redhat-linux-6 | grep -v "suse" >
newpackages.txt
```

Note: This command filters out SUSE packages that are not relevant to our environment and places the output in a new file named **newpackages.txt**.

d. Use WinSCP or MRemoteNG with gedit or vi to view the newly created file located in the **/sas** directory.

7. (Required) Remove Audit Data

In Lesson 6, you will learn about System and Audit Reports, and the SAS Viya operations infrastructure. This required activity resets the audit data, allowing the data to rebuild in preparation for the later lesson.

a. Use the **sas** or **christine** connection in MRemoteNG.

b. Navigate to /workshop/LWSAVA35.

```
cd /workshop/LWSAVA35
```

c. Run the removeaudit.sh script to reset audit data.

```
./removeaudit.sh
```

d. The script contains the commands to remove two files, which are rebuilt over the course of class:

```
[sas@server formats]$ cd /opt/sas/viya/config/var/cache/auditcli/
[sas@server auditcli]$ ll
total 39344
-rw-r--r--. 1 sas sas 40280615 Jun 12 15:54 audit.csv
-rw-r--r--. 1 sas sas      161 Jun 12 15:54 AuditLastRecordFile56791d72cc67.json
[sas@server auditcli]$ rm -rf audit.csv
[sas@server auditcli]$ rm -rf AuditLastRecordFile56791d72cc67.json
[sas@server auditcli]$ ll
total 0
```

End of Practices

2.5 Solutions

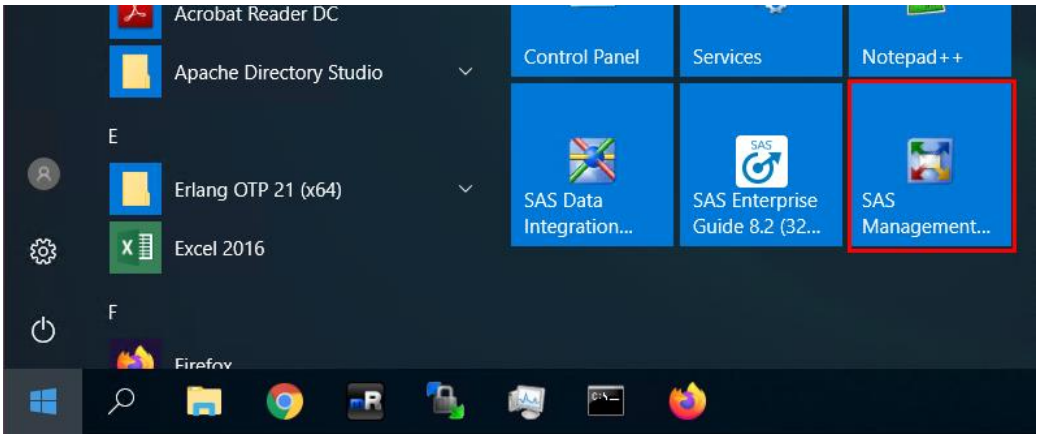
Solutions to Practices

1. Configuring a SAS 9 Client to Work with SAS Viya

In this practice, you connect to SAS Viya from SAS 9. You will define a metadata server object for the CAS server, and store authentication information in users' metadata identities. Then you will test the connection using SAS Enterprise Guide.

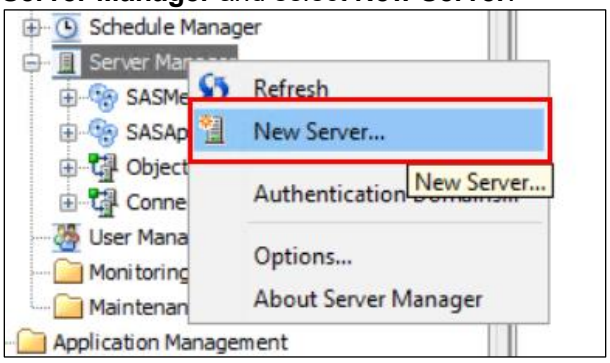
Note: In a production environment, there are security certificates that are required to communicate between SAS 9 and SAS Viya. See the Extended Learning page for more information.

a. Open SAS Management Console on the Windows server. It can be found on the Windows Start menu.

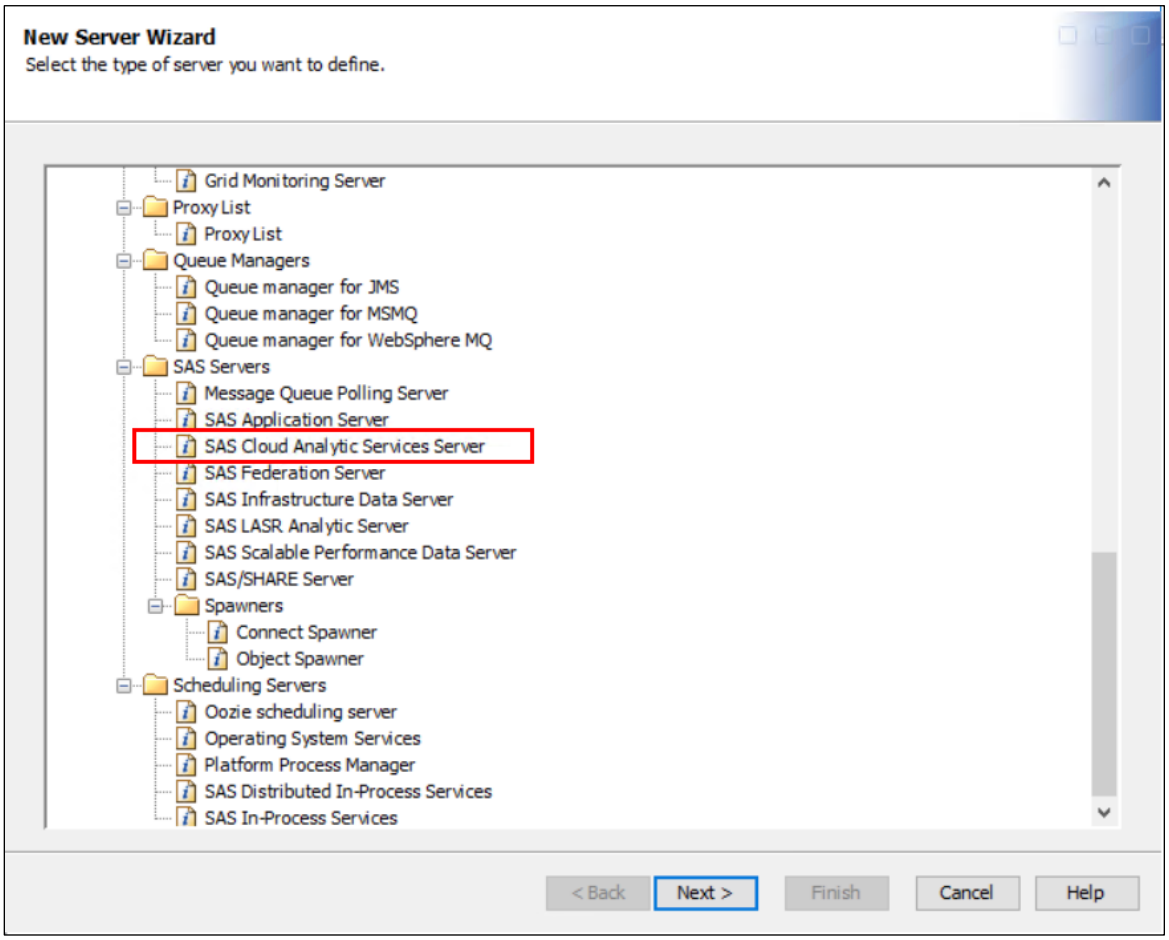


b. Using the metadata administrator, **sasadm@saspw**, with the password of **Student1**, expand Server Manager.

c. To create a metadata server to hold connection information for the CAS server, right-click on **Server Manager** and select **New Server**.

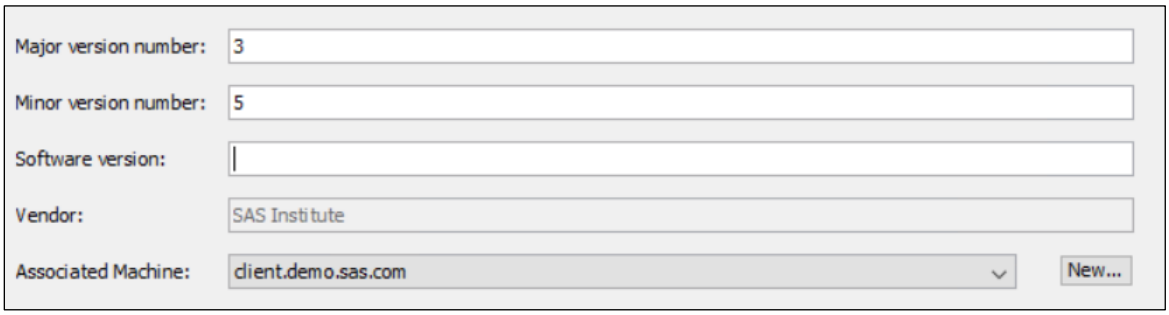


d. Scroll down the tree structure to locate the **SAS Servers** folder. Choose the server type: **SAS Cloud Analytics Services Server** and click **Next**.



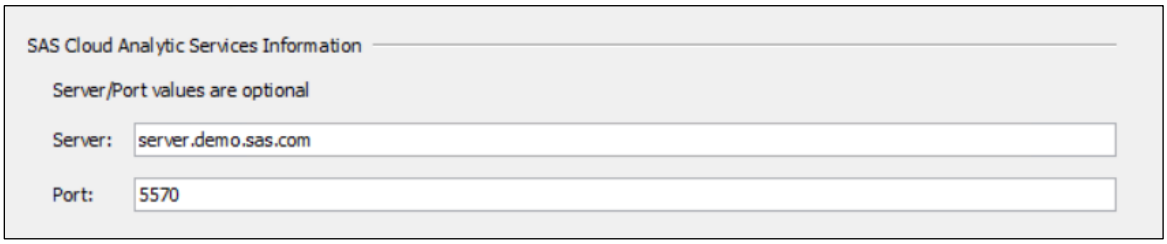
e. Give the server a meaningful name, such as ***casapp***, and click **Next**.

f. You can fill in optional additional information at the server properties wizard screen, such as Major version number (3) and Minor version number (5). Leave the **Associated Machine** field as the default of **client.demo.sas.com**. Click **Next**.

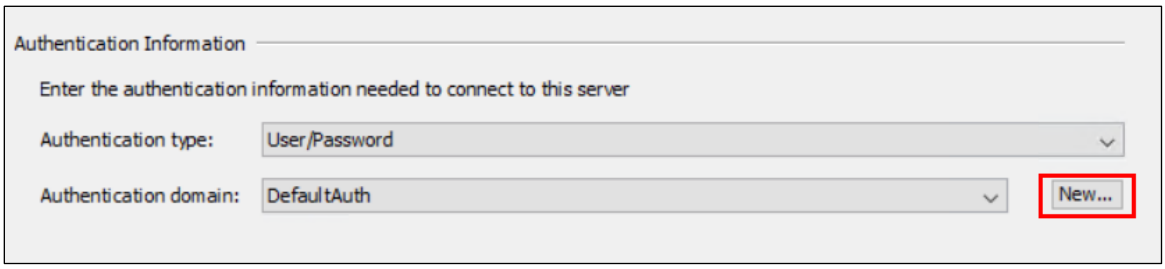


g. At the SAS Cloud Analytics Services Information fields, enter the CAS server name and port information for the CAS host.

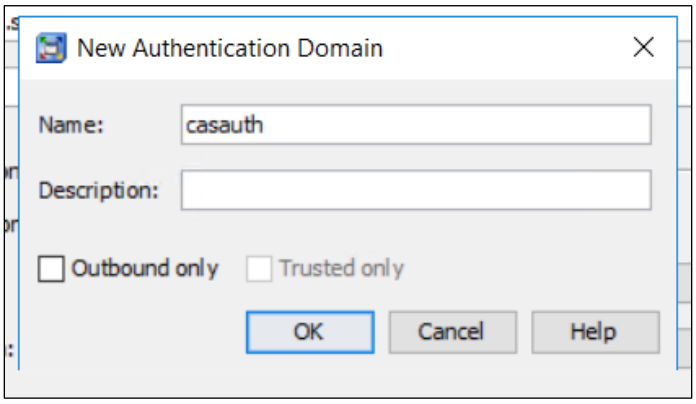
Server	**server.demo.sas.com**
Port	**5570**



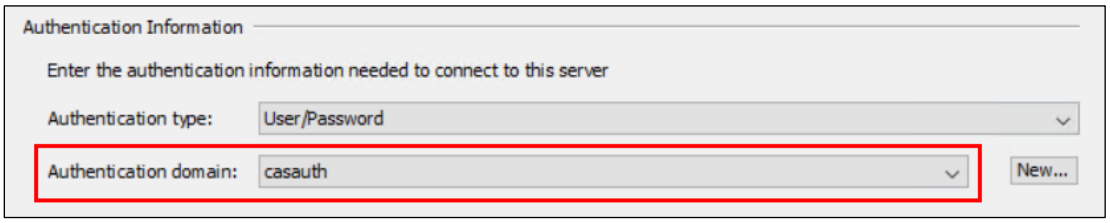
h. In the Authentication Information prompt, define a new Authentication Domain to store user authentication information for when they attempt to connect to this server. Click the **New** button to the right of **Authentication Domain: DefaultAuth**.



i. In the **New Authentication Domain** dialog box, give the Authentication Domain a meaningful name, such as ***casauth***, and click **OK**.

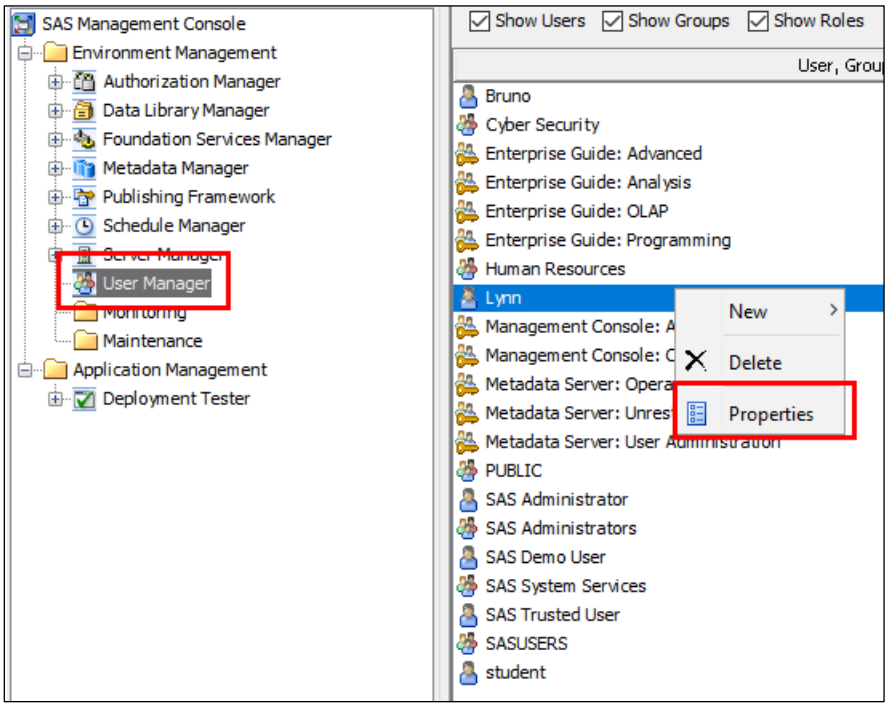


j. The new **casauth** authentication domain should automatically be selected. Click **Next**.

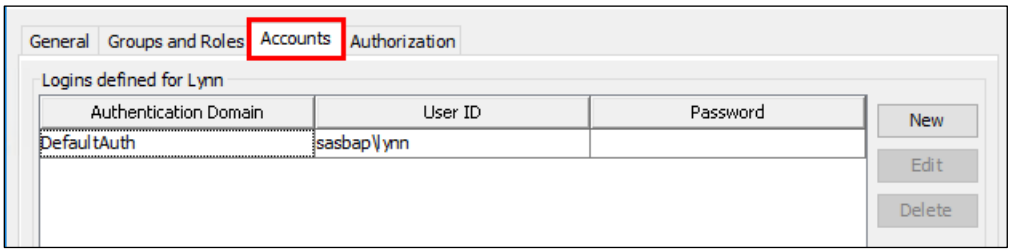


k. Review the new server information and click **Finish**.

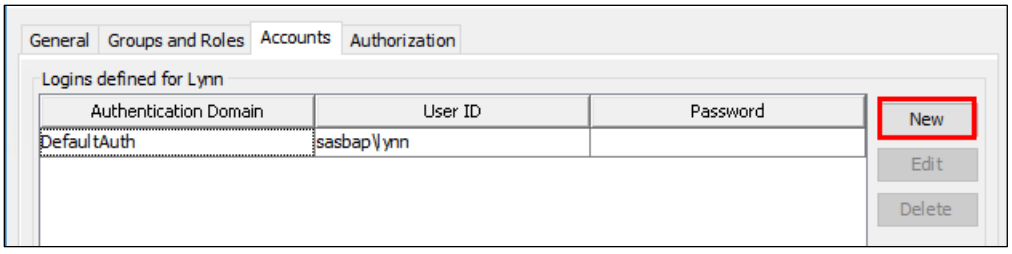
l. For this practice, you need to store credential information so that users can authenticate with the CAS Server. Still in SAS Management Console, highlight the **User Manager** plug-in, and right-click the **Lynn** user to open their **Properties** window.



m. Click the user's **Accounts** tab to access the logins defined for their metadata identity.



n. Define a login for the CAS server by clicking the **New** button.

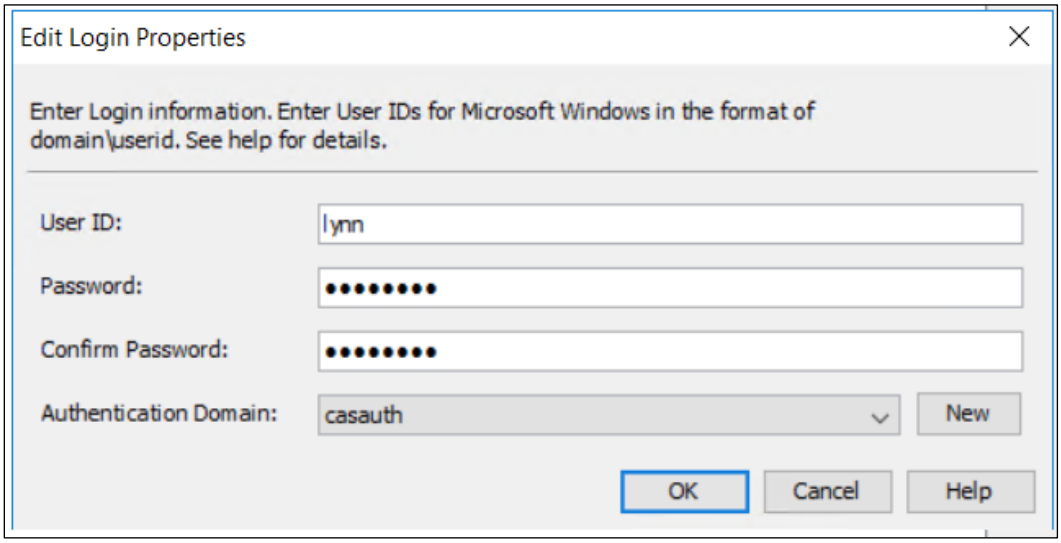


o. In the New Login Properties dialog box, enter the user ID and password for the SAS Viya identity for this user. For the purposes of this practice, **lynn** will be the user. Be sure to select the newly defined **casauth** Authentication domain to pair these credentials with server connection information.

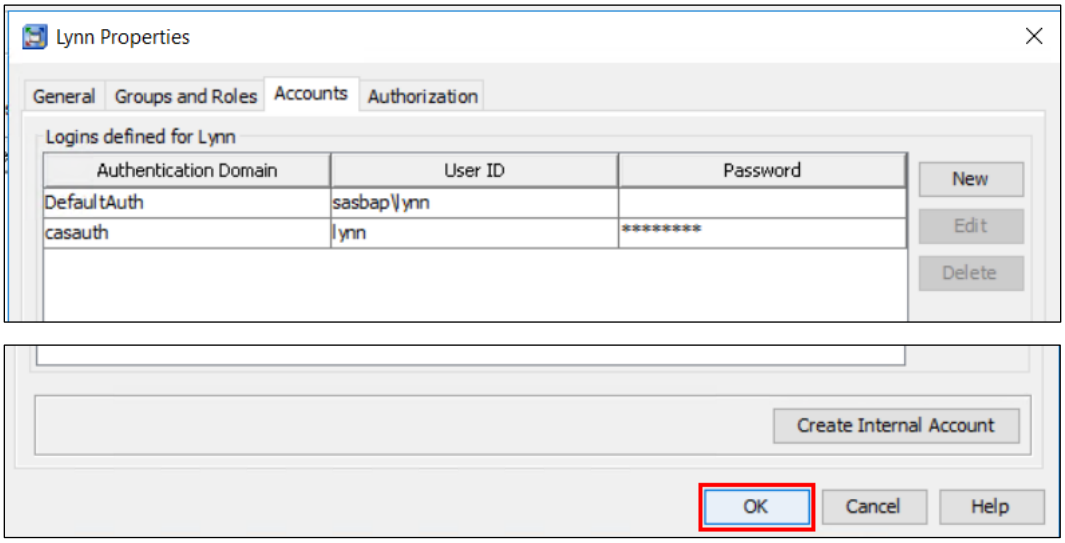
User ID	**lynn**

Password	**Student1**
Authentication Domain	**casauth**

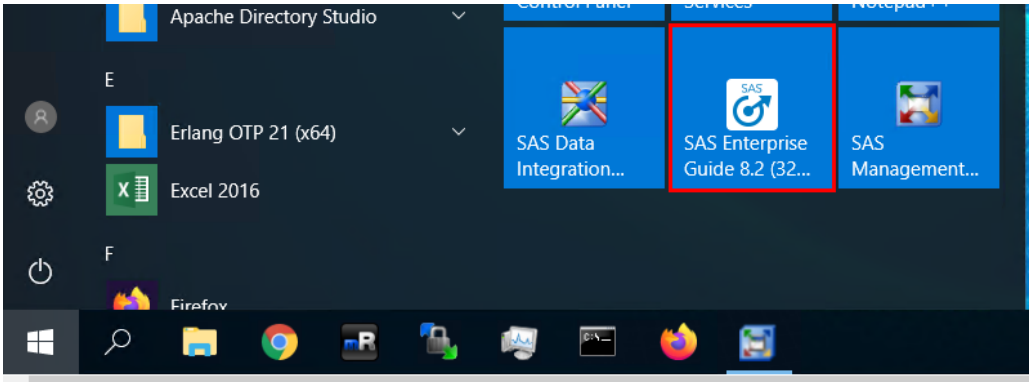
Note: lynn's user ID is case-sensitive.



p. There should now be two logins defined. Click **OK**.



q. Verify the connection. Launch SAS Enterprise Guide from the **Start** menu.



r. Open the program **L02P1_egToCAS.sas** from the Recent Items list or at the path: **D:\Workshop\SAVI35**

s. This program code connects to CAS and lists detailed CAS session and CAS services information to the log. You do need to define the **AUTHDOMAIN=** and **CASSERVERMD=** options to match the newly created authentication domain and SAS Cloud Analytics Services Server metadata object.

AUTHDOMAIN=	**casauth**
CASSERVERMD=	**casapp**

Note: If you named the Authentication domain or the SAS Cloud Analytics Services server metadata object differently, enter those names here instead.

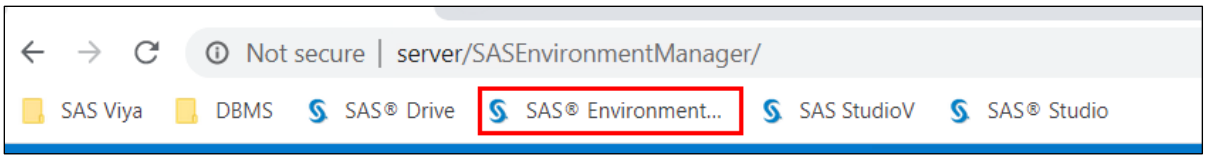
```
Code
 1
 2  cas CASAUTO AUTHDOMAIN=casauth  CASSERVERMD=casapp ;
 3
 4  caslib _all_ assign;
 5
 6 proc cas;
 7    session CASAUTO;
 8
 9  cas _all_ list;
10  cas CASAUTO listabout;
11
12  run;
13  quit;
14
15  cas CASAUTO terminate;
```

t. Run the program.

u. Check the SAS Enterprise Guide log to verify successful credentials obtained from the SAS 9.4 metadata server, successful connection to SAS Viya Cloud Analytic Services, and successful authentication of Lynn.

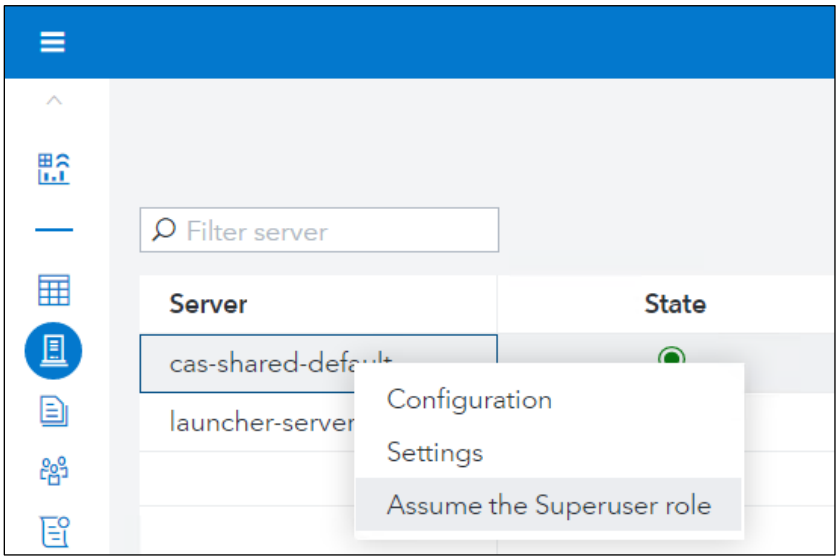
```
29         cas CASAUTO AUTHDOMAIN=casauth  CASSERVERMD=casapp ;
NOTE: Credential obtained from SAS metadata server.
NOTE: The session CASAUTO connected successfully to Cloud Analytic Services server.demo.sas.com using p
      c99fba7e-7b1a-b748-bace-a65a727bad54. The user is lynn and the active caslib is CASUSER(lynn).
NOTE: The SAS option SESSREF was updated with the value CASAUTO.
NOTE: The SAS macro _SESSREF_ was updated with the value CASAUTO.
NOTE: The session is using 0 workers.
30
31         caslib _all_ assign;
NOTE: A SAS Library associated with a caslib can only reference library member names that conform to SA
NOTE: CASLIB CASUSER(lynn) for session CASAUTO will be mapped to SAS Library CASUSER.
NOTE: CASLIB DIDP for session CASAUTO will be mapped to SAS Library DIDP.
NOTE: CASLIB Formats for session CASAUTO will be mapped to SAS Library FORMATS.
NOTE: CASLIB ModelPerformanceData for session CASAUTO will not be mapped to SAS Library ModelPerformanc
      not valid for use as a libref.
NOTE: CASLIB Models for session CASAUTO will be mapped to SAS Library MODELS.
NOTE: CASLIB Public for session CASAUTO will be mapped to SAS Library PUBLIC.
NOTE: CASLIB Samples for session CASAUTO will be mapped to SAS Library SAMPLES.
```

v. Open a web browser and from the favorites bar, launch SAS Environment Manager.



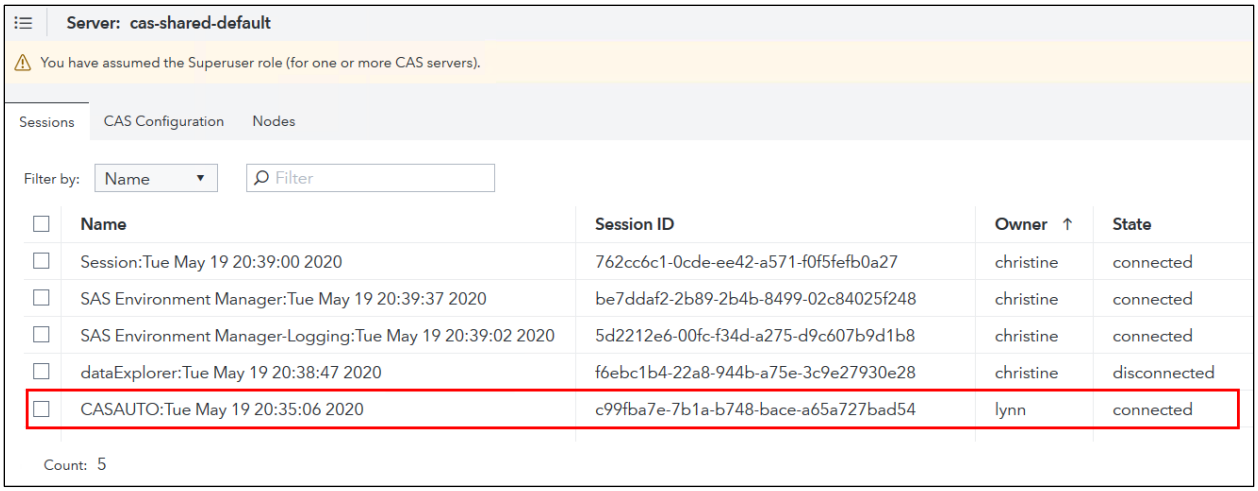
w. As **christine**, opt into the SASAdministrators assumable group.

x. Proceed to the Servers page and assume the superuser role of the **cas-shared-default** server in order to check current sessions.



y. Right-click **cas-shared-default** for a second time and click **Configuration** to view connected sessions.

z. Is lynn connected? **Yes**



aa. To disconnect the session, either run the commented-out CAS statement with the terminate option in SAS Enterprise Guide, or just close SAS Enterprise Guide.

bb. Then relinquish the Superuser role on cas-shared-default and sign out of SAS Environment Manager.

2. **(Optional) Creating an Authinfo File**

In this practice, you create an authinfo file. The format of an authinfo file is based on the .netrc file specification that is used for FTP login. In addition to the .netrc file standards, the authinfo specification allows for putting commands in the file, as well as using quoted strings for passwords. The quoted strings allow for spaces within passwords and user IDs.

a. Create an **authinfo** file in Christine's home directory:

```
touch ~/.authinfo
```

```
[christine@server LWSAVI34]$ cd ~
[christine@server ~]$ touch ~/.authinfo
```

b. Check permissions on the newly created file.

```
ls -al ~/.authinfo
```

```
[christine@server ~]$ ls -al ~/.authinfo
-rw-r--r--. 1 christine users 0 Nov  1 14:31 /home/christine/.authinfo
```

c. Restrict access to everyone but Christine.

```
chmod 600 ~/.authinfo
```

d. Verify permissions.

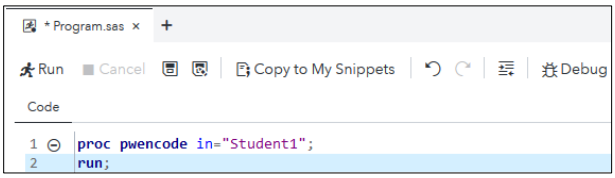
```
ls -al ~/.authinfo
```

```
[christine@server ~]$ chmod 600 ~/.authinfo
[christine@server ~]$ ls -al ~/.authinfo
-rw-------. 1 christine users 0 Nov  1 14:31 /home/christine/.authinfo
```

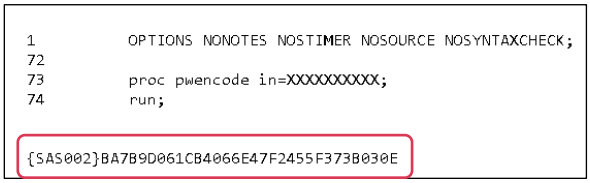
e. Add credential definitions to the **authinfo** file.

1) Use PWENCODE procedure in SAS Studio to encode your password to store in the authinfo file.

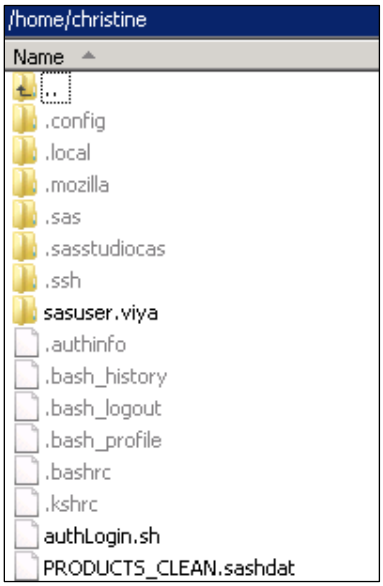
```
proc pwencode in="Student1";
run;
```

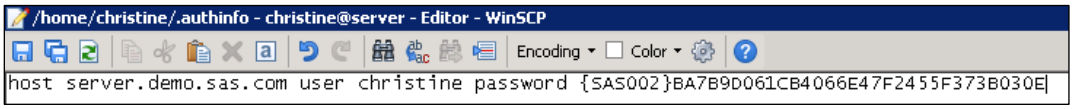


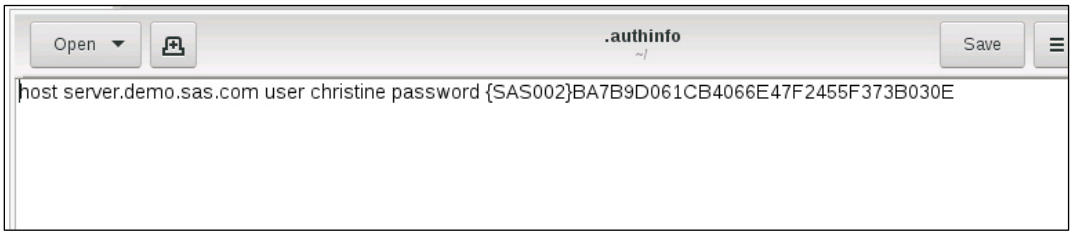
2) From the log, copy the encrypted string of the password.



3) Edit the **authinfo** file using gedit in mRemoteNG. Or, use WinSCP.







4) Save the **authinfo** file.

Notes:

- SAS Studio does not use the authinfo file by default. To use the authinfo file in SAS Studio, you must specify either the AUTHINFO= SAS system option or the AUTHINFO= CAS statement option.
- It is possible to have multiple credential definitions in the authinfo file to access multiple systems.

The format of the credential entry is as follows:

- Generic credential to authenticate to host: default user *user ID* password *userpassword*

  Example: default user myuser ID password Myp4ssw0rd
- Credential to authenticate to a specific host: host *host name* user *user ID* password *userpassword*

  Example:
  - host my.cas.server user sasadm password {sas002}BA7B9D061CB4066E4…
  - host my.cas.server user sastest1 password {sas002}BA7B9D061CB4066E4…
  - host my.cas.server user sastest2 password {sas002}BA7B9D061CB4066E4…
- Credential to authenticate to a specific host on a specific port*:* host *host name* port: *port number* user *user ID* password *userpassword*

- If you want to store the authinfo file somewhere other than the user's home directory, you need to use the AUTHINFO= option. (This also ensures that SAS Studio will use the authinfo file, which overrides the default connect behavior with USER= CAS Connect option.)

```
Options cashost="sasserver.demo.sas.com" casport=5570
authinfo="location";
Cas mycassession user=shrile;
```

  Or set an environment variable CAS_AUTH_METHOD to authinfo:

```
Options set=CAS_AUTH_METHOD_authinfo;
Options cashost="sasserver.demo.sas.com" casport=5570;

Cas myCASsession;
```

- For debugging purposes, there is a DEBUG option that will yield helpful diagnostics when the connection is failing.

```
options set=CASCLIENTDEBUG=1;
```

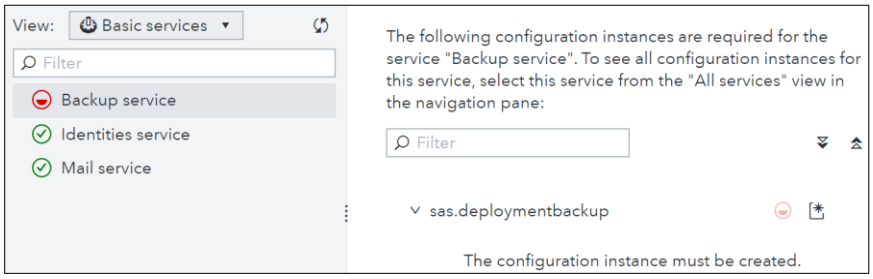
- If a SAS product uses an authinfo file, it does so based on the following precedence:
  1. Product-specific options.
  2. The AUTHINFO= SAS system option.
  3. The AUTHINFO environment variable.
  4. The NETRC environment variable.

3. Configuring the Shared Vault with SAS Environment Manager

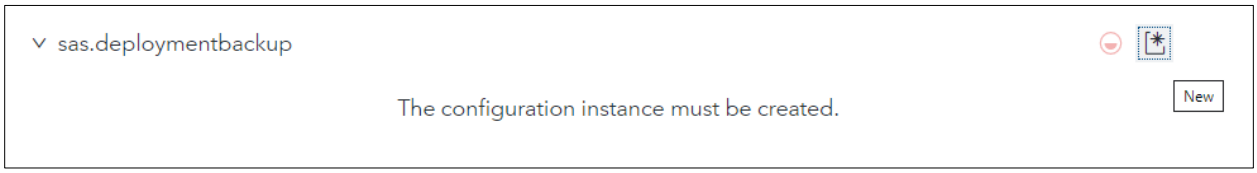
a. If you do not have an active SAS Environment Manager session, open a Chrome browser and select **SAS Environment Manager** on the Bookmarks toolbar. Sign in as the user **christine** with the password **Student1**. Assume the **SASAdministrator** role.

b. Click **Configuration** on the side menu.

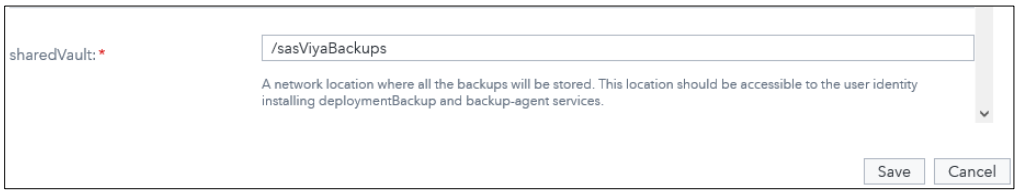
c. Click **Backup service**. The icon indicates that the backup configuration is not yet created. The shared vault location needs to be entered. The shared vault is any network location to preserve the backups from all tiers. The backup files are moved from local vault to shared vault. It is referred to as sharedVault in the SAS Environment Manager user interface.



d. Click **New**.

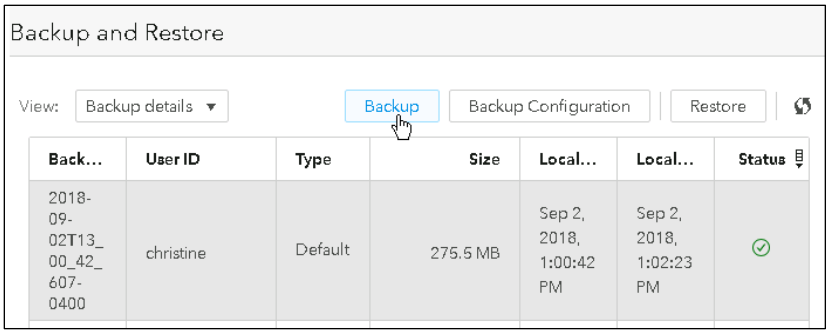


e. Scroll in the sas.deploymentbackup Configuration window until you find **shareVault** and enter **/sasViyaBackups** in the field. Click **Save** when it is complete.

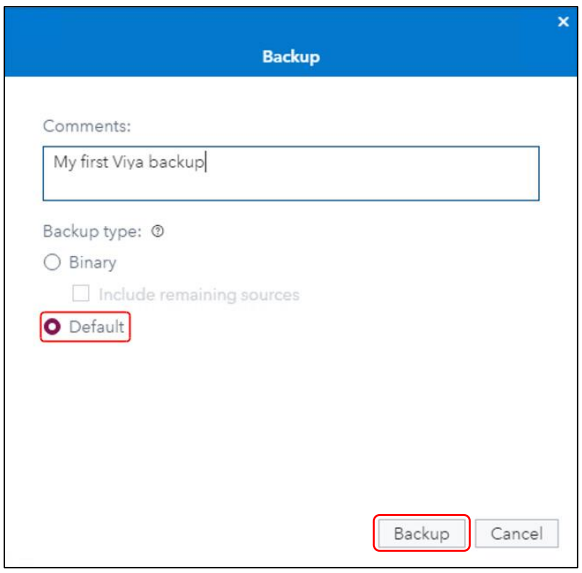


4. **Performing a Backup with Backup Manager in SAS Environment Manager**

a. Select **Backup and Restore** page from the side menu. Click the **Backup** button to start a backup.

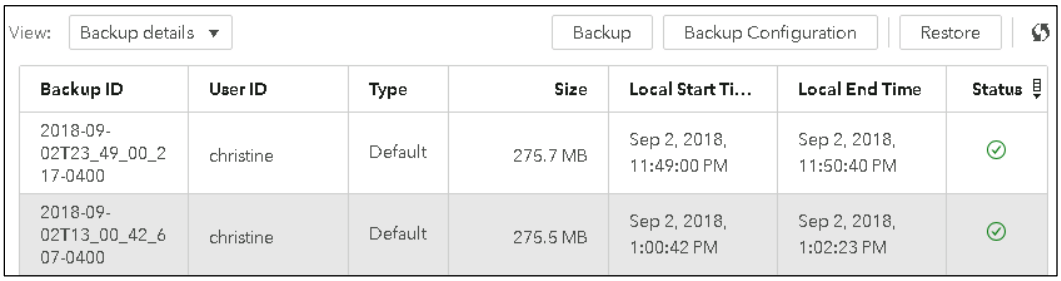


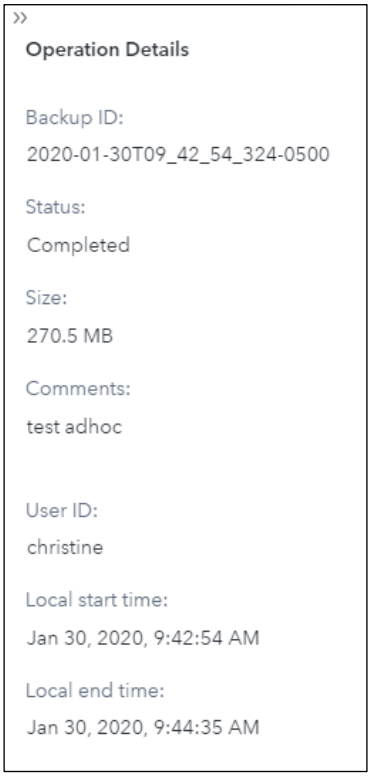
b. Enter **My first Viya Backup** in the **Comments** field. Under Backup type, verify that the **Default** radio button is selected. Start the backup by clicking the **Backup** button.

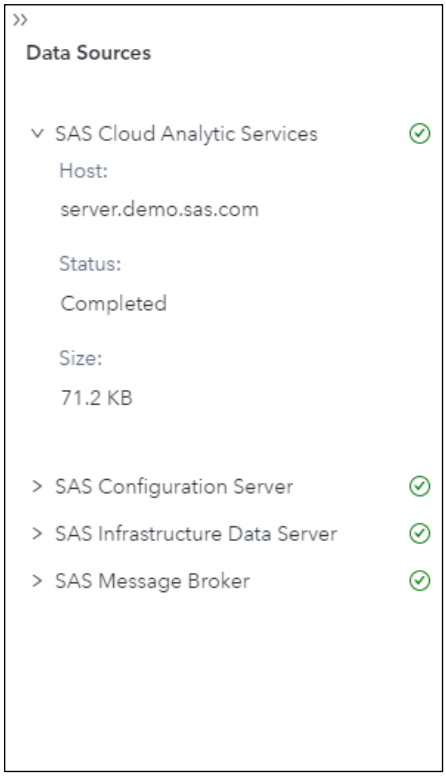


c. When the backup is complete, click **Close** on the window that appears.

d. Click the backup name in the first column. Examine the backup details and the data sources on the right side of the window.







5. Using a Backup CLI to View the Backup

a. If an mRemoteNG session for christine is not started, open one now.

b. Change the directory to **/opt/sas/viya/home/bin** to access **sas-admin**.

```
cd /opt/sas/viya/home/bin
```

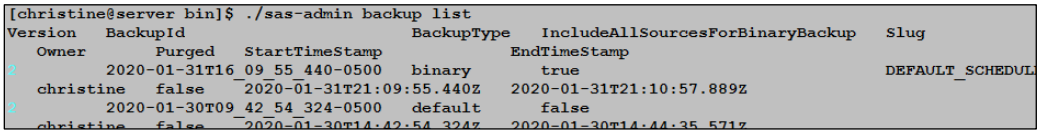
c. Log on to the CLI utility. (You need to do this step only if you have not used the CLI in the past 12 hours.) Supply the credentials for Christine: **christine** and **Student1**.

```
./sas-admin auth login
```

```
[christine@server bin]$ ./sas-admin auth login
Enter credentials for http://server:

Userid> christine

Password>
Login succeeded. Token saved.
```

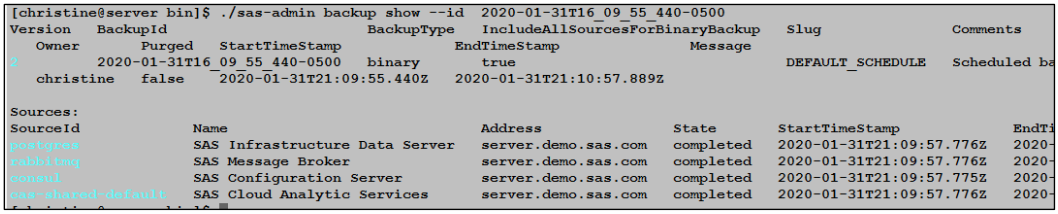
d. Open a list of your backups. The value in the **Name** column is used for subsequent commands.

```
./sas-admin backup list
```



e. Use the SHOW option on the backup plug-in to obtain more details from the backup.

```
./sas-admin backup show --id <BackupID from the list command>
```



6. Mirror Repository Difference

The mirror repository represents the same version of the packages in your SAS Viya deployment. The SAS Hosted repository is dynamic and will always be updated with the latest versions of the packages. It is important to run a report to determine the differences between your mirror repository and the SAS Hosted repository.

a. Use the **sas** connection in MRemoteNG.

b. Navigate to **/sas**.

```
cd /sas
```

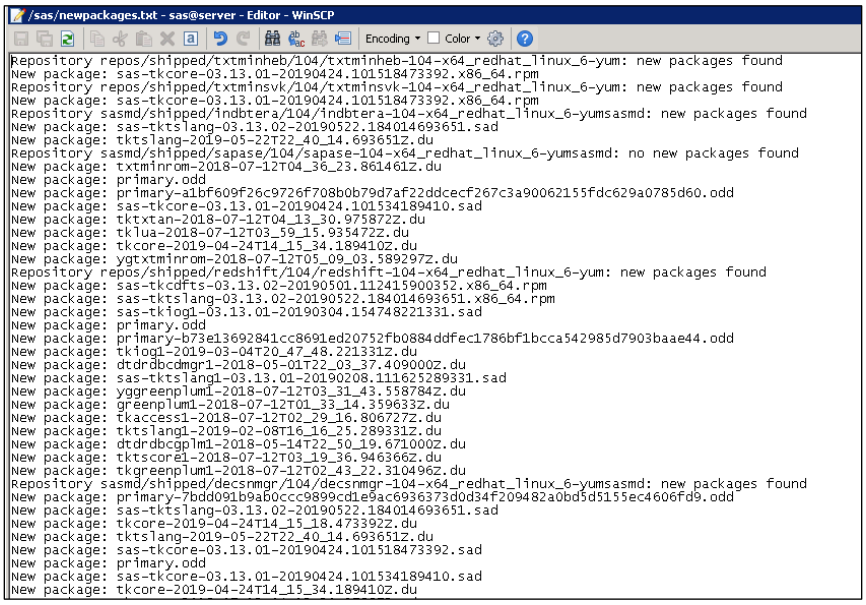
c. Run the following command (command is written on one line):

```
./mirrormgr mirror diff --deployment-data
/sas/Full/SAS_Viya_deployment_data.zip --path /sas/Full --
latest --platform x64-redhat-linux-6 | grep -v "suse" >
newpackages.txt
```

Note: This command filters out SUSE packages that are not relevant to our environment and places the output in a new file named **newpackages.txt**.

```
[sas@server sas]$ ./mirrormgr mirror diff --deployment-data /sas/Full/SAS_Viya_deployment_data.zip -
-path /sas/Full --latest --platform x64-redhat-linux-6 | grep -v "suse sad" > newpackages.txt
Starting diff process
Diffing 1/298 repos/shipped/connect/100/connect-100-x64_suse_linux_12-yum
Diffing 2/298 repos/shipped/connect/104/connect-104-x64_redhat_linux_6-yum
Diffing 3/298 repos/shipped/db2/100/db2-100-x64_suse_linux_12-yum
Diffing 4/298 repos/shipped/db2/104/db2-104-x64_redhat_linux_6-yum
Diffing 5/298 repos/shipped/decsnmgr/100/decsnmgr-100-x64_suse_linux_12-yum
Diffing 6/298 repos/shipped/decsnmgr/104/decsnmgr-104-x64_redhat_linux_6-yum
```

d. Use WinSCP or MRemoteNG with gedit or vi to view the newly created file located in the **/sas** directory.



7. (Required) Remove Audit Data

In Lesson 6, you will learn about System and Audit Reports, and the SAS Viya operations infrastructure. This required activity resets the audit data, allowing the data to rebuild in preparation for the later lesson.

a. Use the **sas** or **christine** connection in MRemoteNG.

b. Navigate to /workshop/SAVA35.

```
cd /workshop/SAVA35
```

c. Run the removeaudit.sh script to reset audit data.

```
sh removeaudit.sh
```

d. The script contains the commands to remove two files, which are rebuilt over the course of class:

```
[sas@server formats]$ cd /opt/sas/viya/config/var/cache/auditcli/
[sas@server auditcli]$ ll
total 39344
-rw-r--r--. 1 sas sas 40280615 Jun 12 15:54 audit.csv
-rw-r--r--. 1 sas sas      161 Jun 12 15:54 AuditLastRecordFile56791d72cc67.json
[sas@server auditcli]$ rm -rf audit.csv
[sas@server auditcli]$ rm -rf AuditLastRecordFile56791d72cc67.json
[sas@server auditcli]$ ll
total 0
```

End of Solutions

Solutions to Activities and Questions

2.01 Activity – Correct Answer

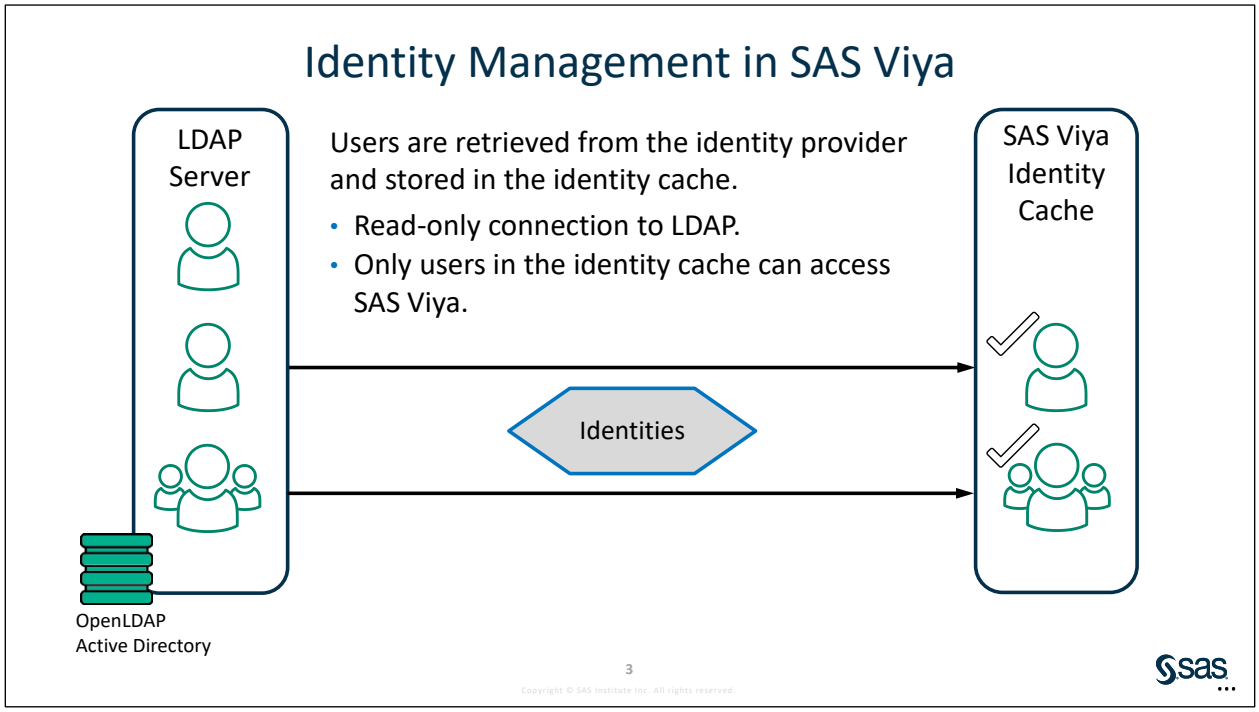
1. Sign in to SAS Environment Manager as **christine** and password **Student1**.
2. Select **Configuration** page from the side menu.
3. Change the View drop-down menu to **Definitions**.
4. Filter on **sas9** or scroll to **sas.logon.sas9**.
5. Highlight **sas.logon.sas9** and click **New Configuration**.
6. What property values should be modified?
7. Click **Cancel**.

enabled: (enable sign-ins using SAS 9 credentials)
sas9LogonUrl: (the URL of the SAS 9 Logon Manager)
single.signOn.enabled: (redirect to SAS 9 for single sign-on)
viyaLogonUrl: (the URL of the SAS Viya Logon Manager)

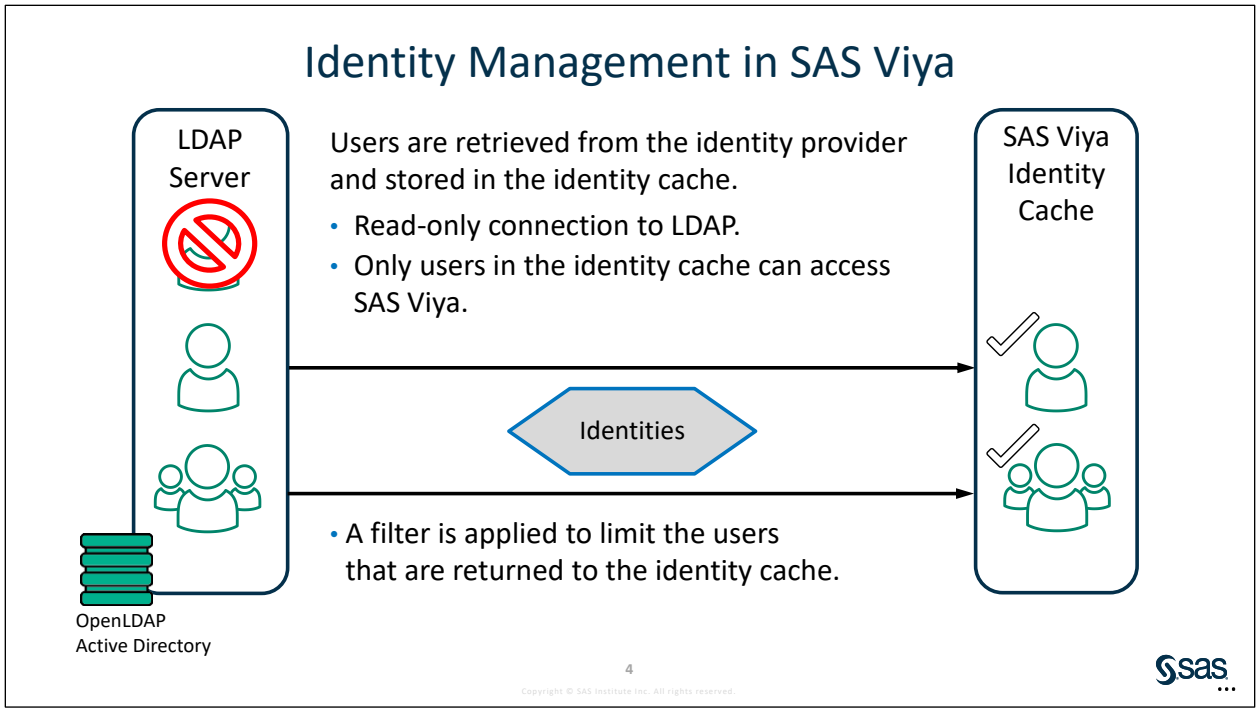
24

Lesson 3 User Management Tasks

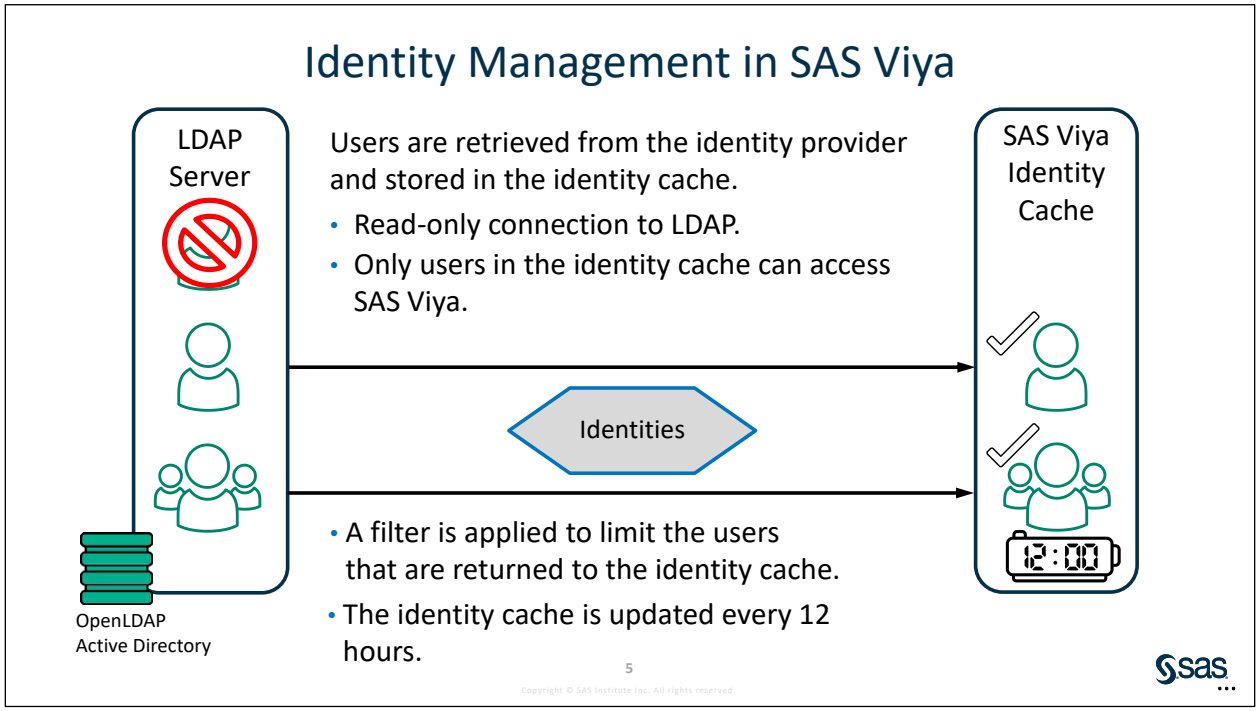
3.1 Identity Management



SAS Viya supports identity providers that are based on Lightweight Directory Access Protocol (LDAP). LDAP is a protocol that is used to access directory servers.



You would not want to include non-identity related resources such as computers or mailing lists. This will also improve performance and reduce memory requirements.



Note: Do not set cache.cacheRefreshInterval below 20 minutes. Doing so might have a significant impact on your overall system, especially on the LDAP and SAS Infrastructure Data servers.

Note: A change to a mapped attribute in the LDAP server does not trigger refreshing the identity cache.

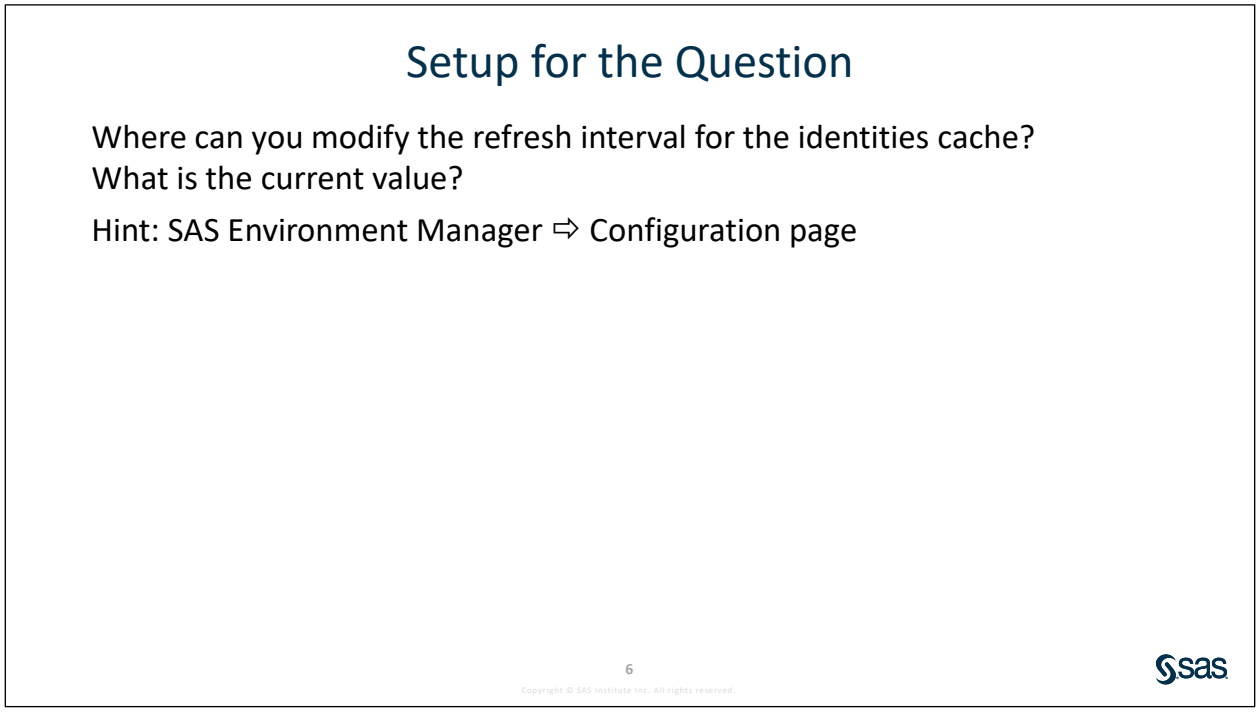
Use the following conventions to specify the unit of time for the refresh interval:

- d – refers to days (for example, 6d)
- h – refers to hours (for example, 6h)
- m – refers to minutes (for example, 6m)
- s – refers to seconds (for example, 6s)
- ms – refers to milliseconds (for example, 6ms)

Programming-only Environment

SAS identity management is not used in a programming-only deployment. In such deployments, your operating system user management is used. In a programming-only environment, the following conditions exist:

- An LDAP server is ***not*** required.
- Users and groups are read from the configured authentication provider.
- CAS users require a host account and Home directory.
- CAS roles govern access to CAS administrative functionality.
- No custom groups are present.
- One authorization system is used: CAS for caslibs, tables, columns, and actions.
- Only a user name and password are supported for authentication.
- Authentication is generally done via pluggable authentication modules (PAM).



3.01 Multiple Choice Question

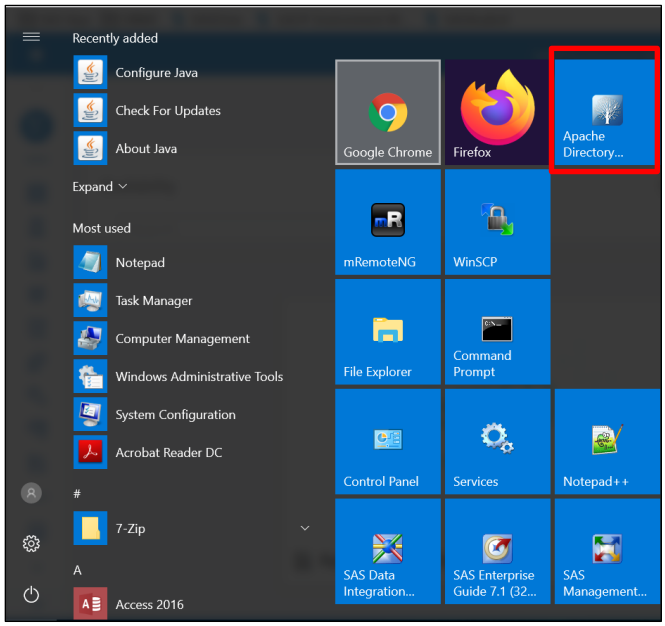
Where can you modify the refresh interval for the identities cache?

a. Credentials service
b. Mail service
c. Identities service
d. Cache Server service

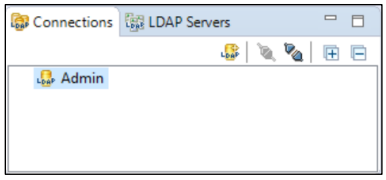
Examining the Identities Service in SAS Environment Manager

This demonstration illustrates how to change the configuration properties of the Identities service in SAS Environment Manager. The imported groups are also examined. The groups in SAS Environment Manager are compared to the groups in the OpenLDAP server by using the Apache Directory Studio utility.

1. From the Start menu, select **Apache Directory Studio**.

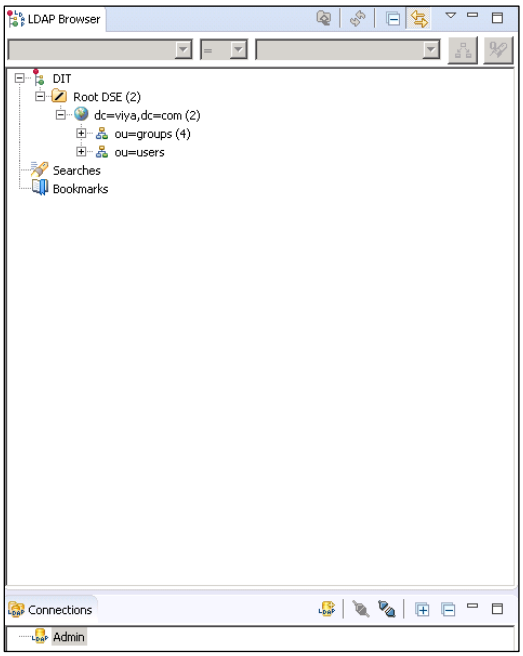


2. Double-click the **Admin** connection on the Connections tile to connect to the OpenLDAP server.



3. Expand the LDAP tree **Root DSE** ⇨ **dc=viya, dc=com** to show the users and groups defined in the LDAP server.

   LDAP is a lightweight protocol for accessing directory servers. A directory server is a hierarchical object-oriented database. LDAP directories are organized in a tree manner.



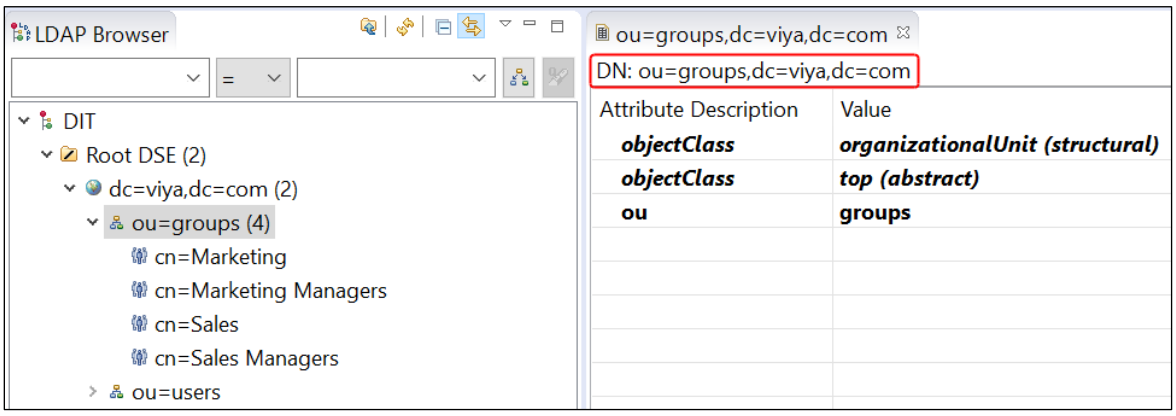
4. Select the groups node of the tree and note that the DN is **ou=groups,dc=viya,dc=com**.

   Every entry in a directory has a unique identifier, called the ***Distinguished Name (DN)***. The distinguished name is the full path to the object in the directory tree. The directory entries contain a set of attributes. An attribute has a name, and one or more values.

   dc is the domain component. You will often see examples of LDAP structures that use DNS (domain name systems) names for the domain component, such as dc=sas,dc=com. This is not required, but because DNS itself often implies organizational boundaries, it usually makes sense to use the existing naming structure.

   In this example, the domain component is dc=viya,dc=com.

   The next level down is organizational unit (ou). An organizational unit is a grouping or collection of entries. Organizational units can contain additional organizational units.



   Note: The distinguished name is the path to the object from the lowest to highest.

5. Select the users node of the tree and note that the DN is **ou=users ,dc=viya,dc=com**.

   DN: ou=users,dc=viya,dc=com

6. Expand **ou=users**.

7. Click **eric**. The attribute value pairs are the details of the entry. For example:

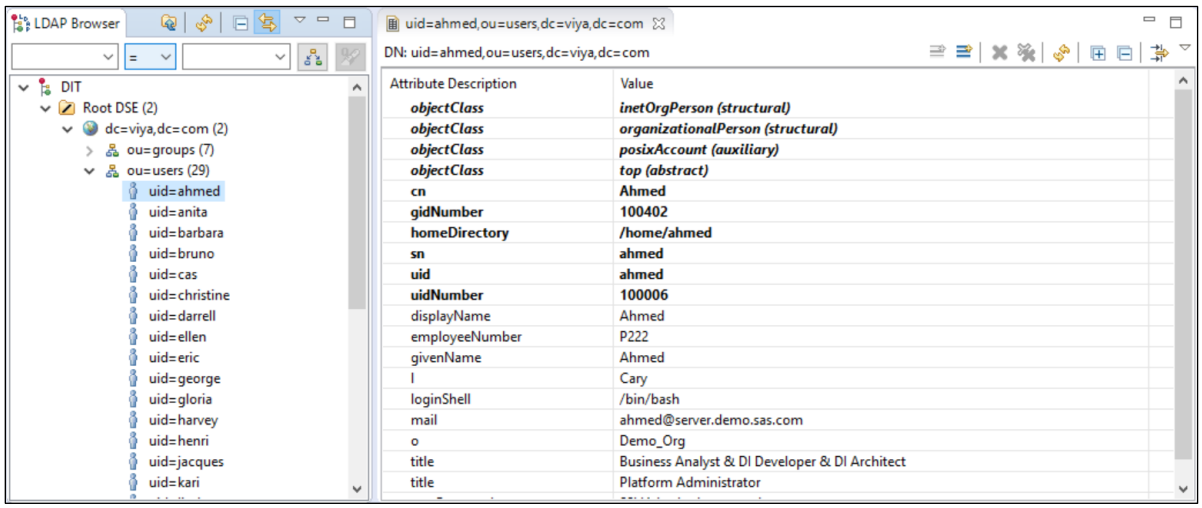
   uid (user ID)

   cn (common name)

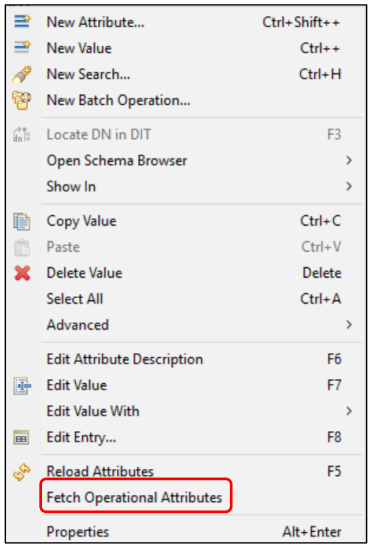
   displayName (name to display)

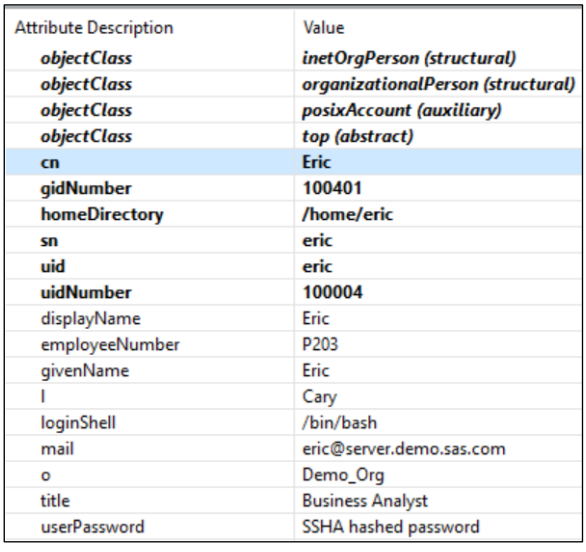
   L (location)

   Every entry has at least one **objectClass** attribute and often more than one. The **objectClass** provides the rules for the object including required and allowed attributes. For example, the **inetOrgPerson** object class specifies attributes about people who are part of an organization, including items such as uid, name, employeenumber, and so on.

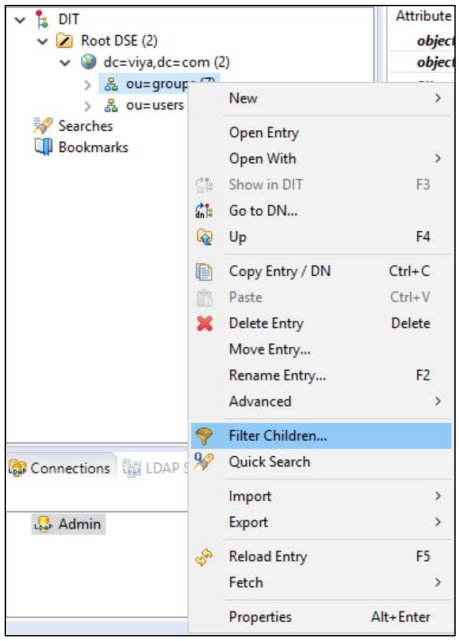


8. Right-click in the attribute list and select **FetchOperationalAttributes** to see group membership information.





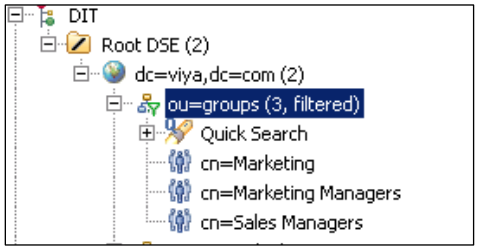
9. Right-click the **ou=groups** entry and select **Filter Children** from the drop-down list.



10. Enter the query:

```
(&(objectClass=groupOfNames)(!(name=Sales)))
```

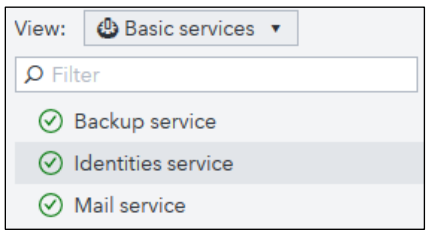
The filters return the groups that should be returned to the application. (Sales is not present.)



11. Go to SAS Environment Manager. (Open a Google Chrome browser window and sign in to SAS Environment Manager as **christine** with a password of **Student1**. Opt in to the **SASAdministrators** assumable role.)

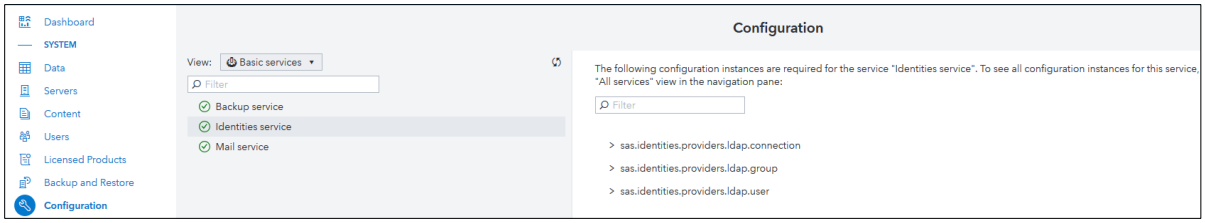
12. Select **Configuration** from the side menu.

13. Highlight **Identities service** in the Basic services list. The **Identities service** retrieves information about identities (users or groups) from your identity provider.



There are three configuration instances for the Identities service that contain the information needed to integrate SAS Viya and LDAP: **connection**, **group**, and **user**. These are expanded by default.

(It can be configured post-deployment by logging in as the sasboot user, or during deployment using the optional **sitedefault.yml** located here: **/sas/sas_viya_playbook/roles/consul/files**.)



The following information is required:

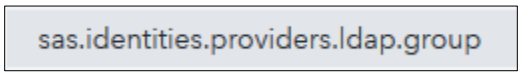
Connection information	For the LDAP server.
Attributes in LDAP	To map to the identity service configuration.
baseDN	Path at which to start the search for users and groups. Every entry in an LDAP directory has a unique identifier, called the distinguished name (DN). The distinguished name is the full path to the object in the directory tree. For example, the distinguished name of christine is uid=christine, ou=users, ou=??, dc=???, dc=com. The distinguished name is the path to the object from lowest to highest.
LDAP query	Filter the users and groups returned.

14. Explore the **sas.identities.providers.ldap.connection** configuration instance. This holds the LDAP connection information.

The **host**, **password**, **port**, and **userDN** properties are used to connect to the LDAP server for identity retrieval.

Note: We have a value of 'none' for userDN because anonymous bind is enabled. This means Read-Only operations are performed using an anonymous (unauthenticated) context.

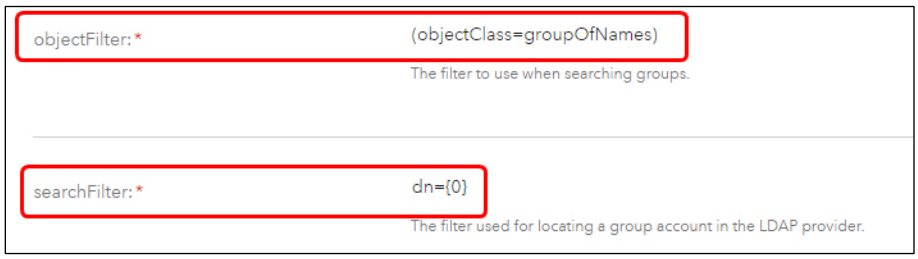
15. Explore the **sas.identities.providers.ldap.group** configuration instance. This holds the LDAP group information.



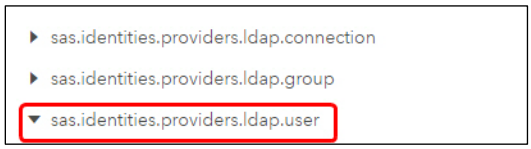
Notice the **baseDN** and **objectFilter** of the configuration instances. There is no subsetting here, as we are bringing in all the groups from our ldap server.

To limit identities returned use the **objectFilter** attribute.

Group filter limits objects returned to those that have an **objectClass** of **groupOfNames**.

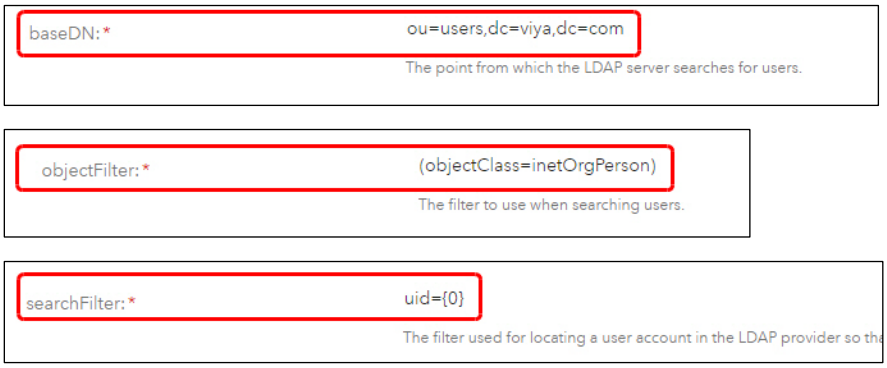


16. Explore the **sas.identities.providers.ldap.user** configuration instance. This holds the LDAP user information.



Notice the **baseDN**, **objectFilter**, and **searchFilter** properties of the group configuration instance.

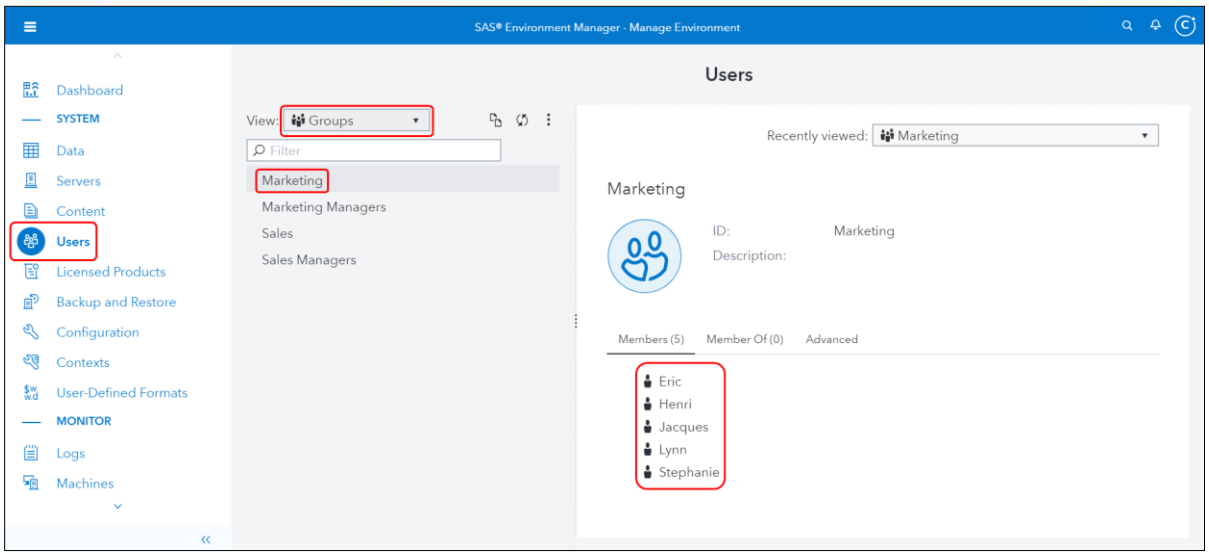
The ***objectfilter*** limits objects returned to those that have **an objectClass** of **inetOrgPerson**.



Some examples of filters:

- Region equals EAST and employeeID not blank **(&(region=EAST) (employeeID=*))**
- Objectclass groupofnames and name not equal to SASLDAP **(&(objectClass=groupOfNames)(!(name=SASLDAP)))**
- Objectclass inetOrgPerson and organization equal to Orion Star **(&(objectClass=inetOrgPerson)(o=Orion Star))**

17. Navigate to the **Users** page from the side menu. Change the view to **Groups**. Because we did not filter on groups, all four are present, the same in the LDAP server. Select the **Marketing** group. The same group members can be seen here.



End of Demonstration

Practice

1. Inspecting the Identities Service

The basic properties of the Identities service were examined in the demonstration. Additional properties are available for the Identities service by viewing **All services** in the Configuration application.

a. Sign in to SAS Environment Manager as **christine** with the password **Student1**. Opt in to the **SASAdministrators** assumable group.

b. Select **Configuration** from the side menu. Select the **Identities service**. Collapse all the configuration instances.

c. Expand the **sas.identities.providers.ldap.group** configuration instance.

Is there a filter configured on groups being brought into the SAS Viya cache?

2. Comparing the Imported Identities with the LDAP Server

The identities were imported from the local OpenLDAP server. This practice uses SAS Environment and Apache Directory Studio to compare the two lists of identities.

a. On the SAS Environment Manager side menu, select **Users**. Select **Users** from the **View** drop-down list.

b. From the Windows Start menu, launch the **Apache Directory Studio** application.

c. Double-click the **Admin** connection on the Connections tile to connect to the OpenLDAP server. Expand the directory tree until all 29 users are visible.

d. Are the two lists the same? Is there a user who is named **abbott** in either list?

3. Adding a User to the LDAP Server and Refreshing the Identity Cache

The identity cache is not updated when changes are made to the content in the identity provider. The content is updated at the next scheduled refresh. (The default is every 12 hours.) It can also be updated by the following:

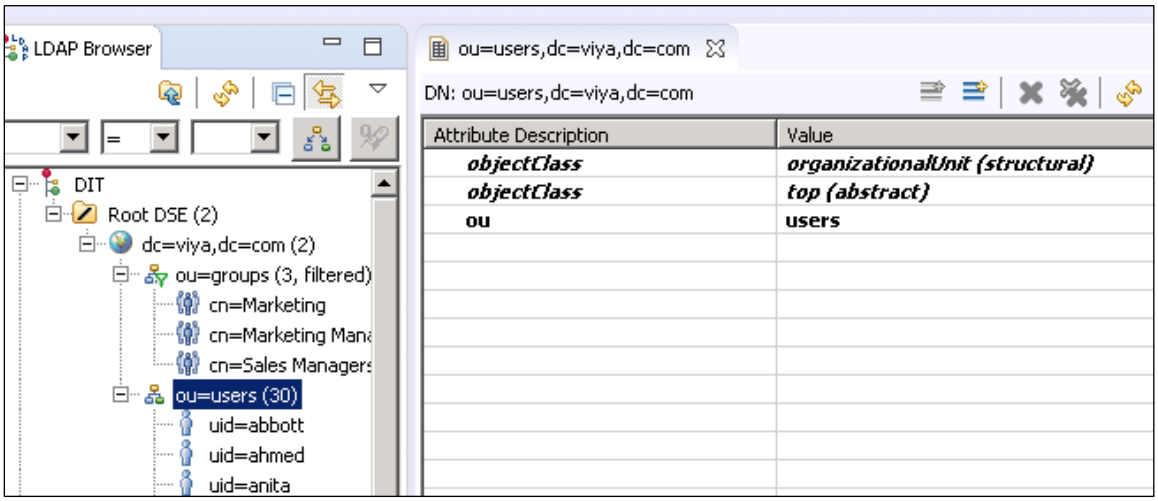
- using the Reload Identities option on the Users page of SAS Environment Manager
- CLI Identities plug-in refresh-cache option
- restarting the Identities service

In this practice, a new user is added to the OpenLDAP server using Apache Directory Studio. Identities are reloaded, and the identities are checked in SAS Environment Manager to confirm the import of the new user.

a. Right-click the **ou=users** tree in Apache Directory Studio. Select **Import** ⇨ **LDIF Import**.

b. Use the navigation window to go to **D:\Workshop\SAVI35\abbott.ldif**. Click **Open**. Click **Finish** in the LDIF Import window to import the LDIF file.

c. Examine the list of users under the **ou=users** tree. Verify that the user **abbott** was added to the OpenLDAP server.



d. Select **Users** from the side menu in SAS Environment Manager and verify that **abbott** is not listed.

e. Click the **More Options** icon ⋮ to the right of the **View** drop-down menu and select **Reload Identities**.

f. Take note of the warning. Click **Yes**.

Note: Other options for refreshing the cache to retrieve new users and groups:

CLI command:

```
/opt/sas/viya/home/bin/sas-admin identities refresh-cache
```

Restart the identity service:

```
sudo systemctl restart sas-viya-identities-default
```

g. Click **Refresh** ↻. Abbott is now able to use the SAS Viya system.

4. **Using the CLI to List the Users**

a. As **christine** in an mRemoteNG session, enter the command shown below.

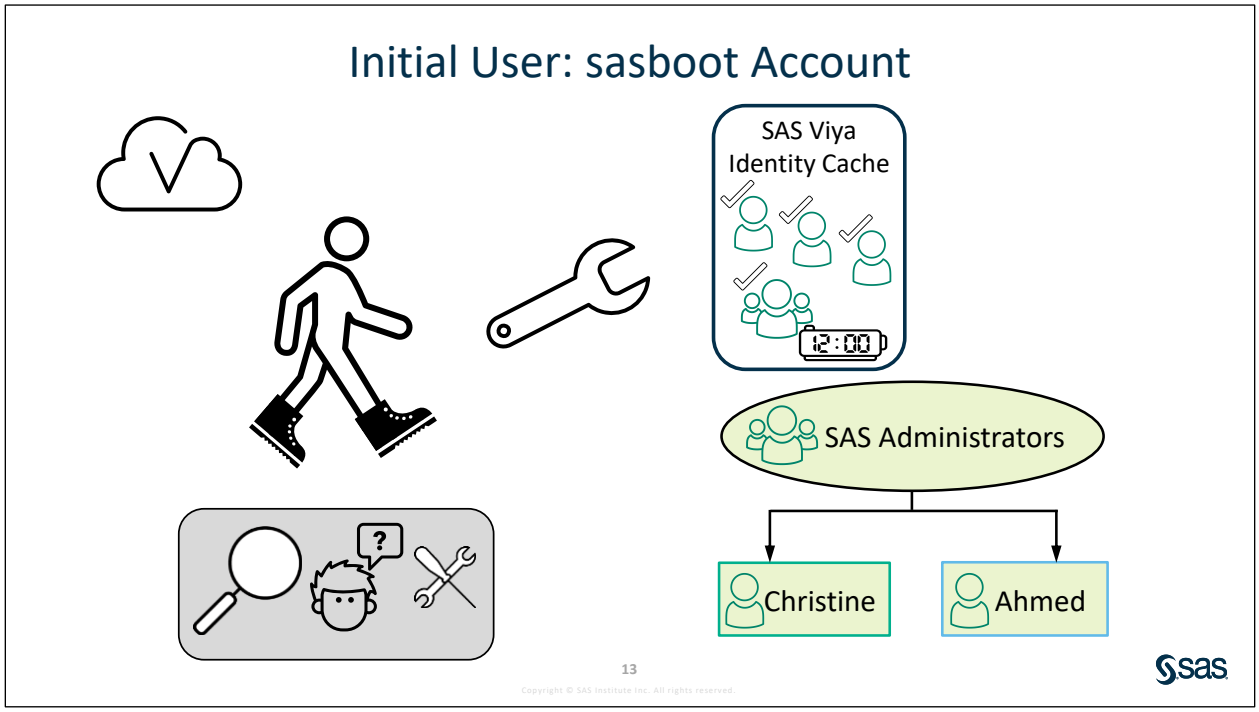
```
/opt/sas/viya/home/bin/sas-admin --output text identities list-users
```

Note: You might need to run **/opt/sas/viya/home/bin/sas-admin auth login** if your token expired.

b. Is this the same list as in SAS Environment Manager?

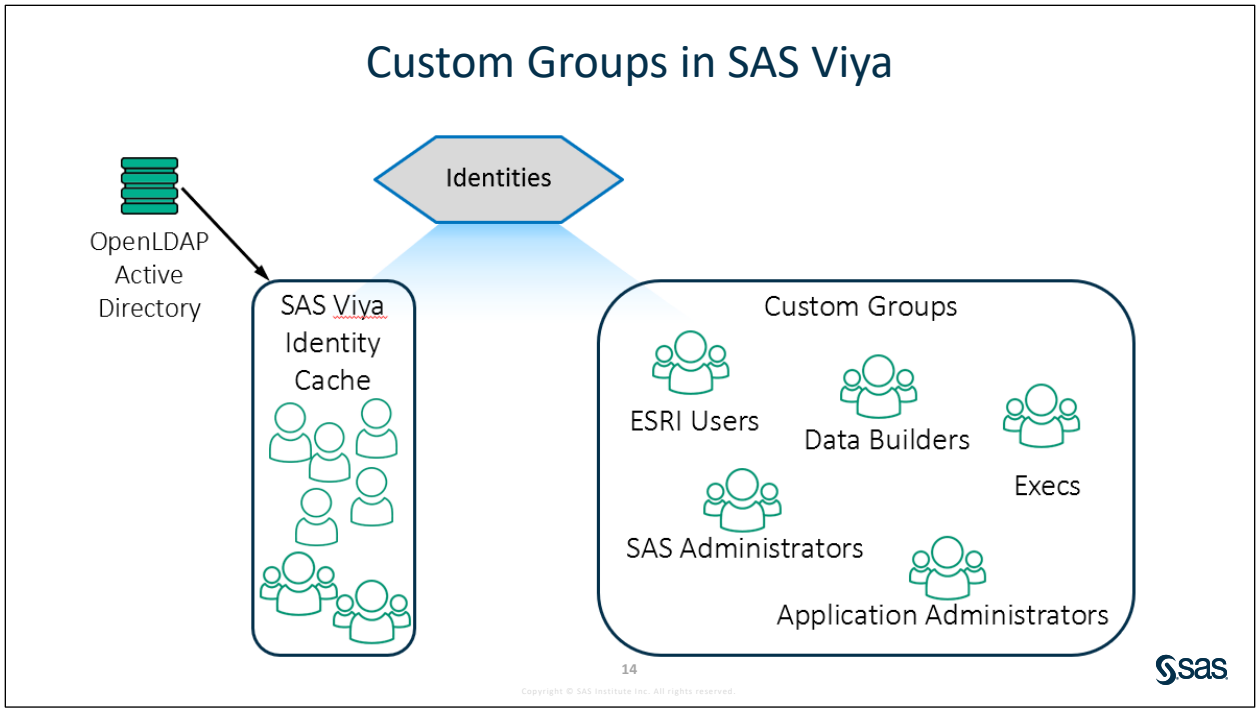
End of Practices

3.2 Exploring Users and Groups



By default, the password for the account is expired. However, each time the SASLogon service is started, a new URL is written to the service's log, which enables the password to be reset if necessary. The URL remains active for 24 hours. (For security purposes, the URL also expires after you enter it in a browser, even if the password is not reset.)

After you have set up the identity provider connection and the first administrative users, the sasboot account is generally used only if the connection to the identity provider fails. After performing the initial tasks, you should change the password, and then for additional security, you can disable the password reset feature. This prevents password reset links from being written to the log each time the SASLogon service is started.



Note: When you create new groups, first try to work with an LDAP administrator to define the groups in the identity provider. Additional custom groups should be created only as a final alternative. They are persisted in the SAS Infrastructure Data Server.

Note: Custom groups do not apply to a programming-only deployment. A programming-only deployment uses host-level accounts and also has a Home directory on the host.

Practice

5. Examining the Behavior of SAS Viya when the Logon Service Is Not Running

This practice determines the status of the logon service. You stop the service, and the symptom of it being stopped is demonstrated. You must restart the service and verify that it is working.

a. Sign out of all SAS Environment Manager and SAS Studio sessions. Close the Chrome and Firefox browser windows.

b. Open **mRemoteNG** and the **christine** connection.

c. At the Linux command prompt, enter the command below to determine the status of the logon service.

```
systemctl status sas-viya-saslogon-default
```

Note: You do not need root privileges to access the status of a service. It ***is*** required as shown below in the **stop** and **start** actions. Christine uses sudo to act like root to execute the service command to perform the stop and start. The root ID could also be used.

d. Enter the command to stop the logon service.

```
sudo systemctl stop sas-viya-saslogon-default
```

e. Click the **Chrome** icon on the taskbar. Try to access SAS Drive or SAS Environment Manager. Was it successful?

f. Close the Chrome browser window.

g. At the Linux command prompt, enter the command below to start the logon service.

```
sudo systemctl start sas-viya-saslogon-default
```

h. Wait for the service to start and sign in again. Was it successful?

Note: It might take some time before you can successfully sign in to SAS Home.

6. Resetting the Password for sasboot

This practice demonstrates how the sasboot ID's password is reset. This is necessary when logon or other authentication and authorization issues occur.

a. Double-click the **WinSCP** shortcut on the Windows desktop. Verify that the **root@server** connection is selected. Click the **Login** button.

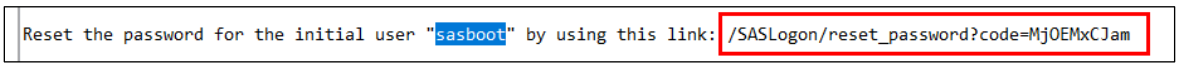
b. On the right side of the WinSCP window, navigate to **/var/log/sas/viya/saslogon/default**.

Note: **/var/log/sas/viya** is a link that resolves to **/opt/sas/viya/config/var/log**

c. Look at the timestamps in the file names. The most recent log file should be at the bottom. If it is not, select the **Changed** column to sort the files based on their previous updates.

d. Double-click the most recent log file to open it in an editor.

Click the Ctrl key and F key simultaneously to begin a search. Enter **sasboot** to find the link that is needed to reset the password. Use this link to construct a complete URL.



Alternatively, use the root session in mRemoteNg and use the **grep** command to search on **sasboot**:

```
grep 'sasboot' /var/log/sas/viya/saslogon/default/sas-
saslogon_date-and-time-stamp.log
```

e. Open a new browser window. Use **http://server** and the link in the log to create a valid URL to sign in and reset the sasboot password:

http://server/SASLogon/reset_password?code=<*code_from_log_file*>

Note: The SASLogon address is case sensitive.

f. Change the password to **Student2**. Confirm the new password and then click **Change Password**.

g. Log on to SAS Environment Manager as **sasboot** with the new password of **Student2**. Opt in to the **SASAdministrators** assumable group.

Note: If the URL has expired, it can be refreshed by restarting the SASLogon service:

```
sudo systemctl restart sas-viya-saslogon-default
```

Then go to the log and obtain the new URL. The URL expires 24 hours after the SASLogon service restarts. For security purposes, the URL that is specified in a browser or in a text editor also expires, even if the password is not reset. After you reset the password, SAS Environment Manager automatically opens in your browser. Opt in to all of the assumable groups so that you have the permissions to perform subsequent tasks.

(Optional) For additional security, you can then disable the password reset feature. This prevents password reset links from being written to the log each time the SASLogon service is started.

Make sure you document the password!

h. Select **Configuration** from the side menu.

i. Select **Definitions** from the drop-down list.

j. In the left pane, select **sas.logon.initial**. Then click **New Configuration** at the top of the right pane.

k. Set **reset.enabled** to **off**.

l. Click **Save**.

m. Restart the SASLogon service.

```
sudo systemctl restart sas-viya-saslogon-default
```

n. Sign out of the sasboot session.

7. Using the CLI to Create a New Custom Group and Adding Users to the Group

a. As **christine** in an mRemoteNG session, enter the command below to create the Finance group.

```
/opt/sas/viya/home/bin/sas-admin identities create-group --
name Finance --id Finance
```

Note: If your token expired, you might need to run the following command:

```
/opt/sas/viya/home/bin/sas-admin auth login
```

b. To add Lynn, Kari, and Marty to the newly created Finance group and verify their membership in the Finance group, run the following command:

```
/opt/sas/viya/home/bin/sas-admin identities add-member --
group-id Finance --user-member-id Lynn
```

```
/opt/sas/viya/home/bin/sas-admin identities add-member --
group-id Finance --user-member-id Kari
```

```
/opt/sas/viya/home/bin/sas-admin identities add-member --
group-id Finance --user-member-id Marty
```

```
/opt/sas/viya/home/bin/sas-admin identities list-members --
group-id Finance
```

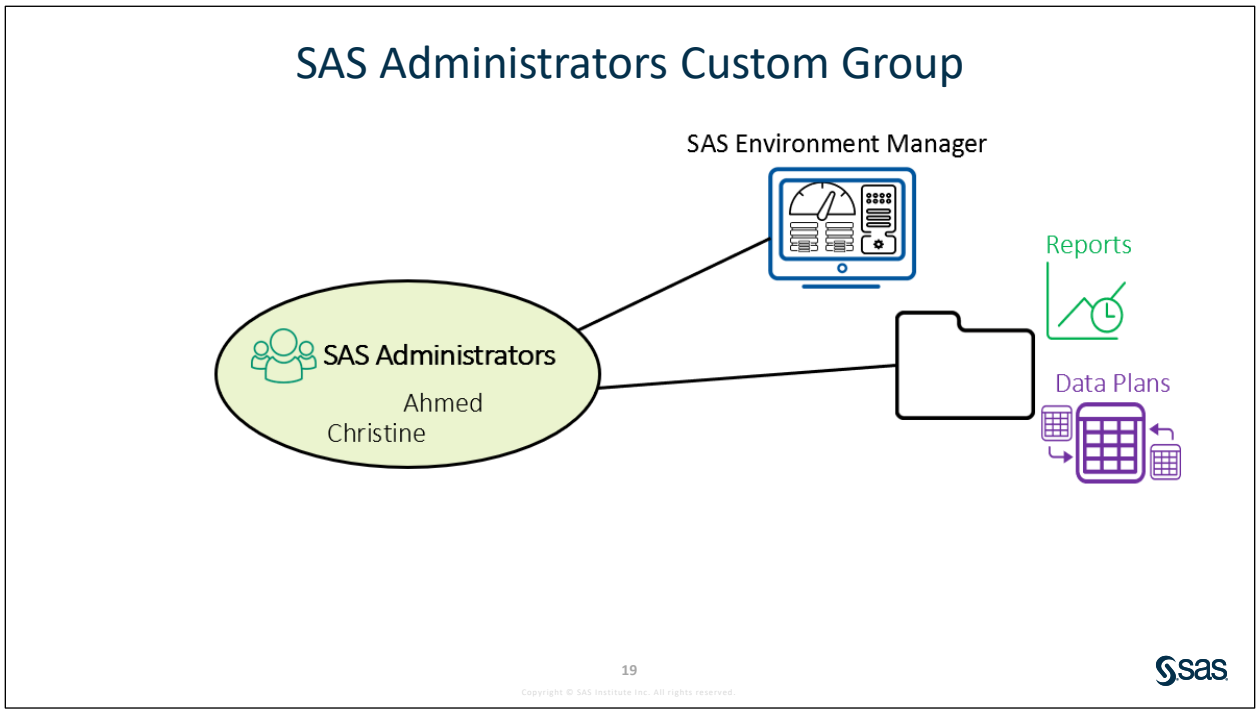
c. Log on to SAS Environment Manager as **christine** with the password **Student1** to verify that the custom group was added, along with the three users.

Note: There is a CLI script to add access controls on Finance caslib:

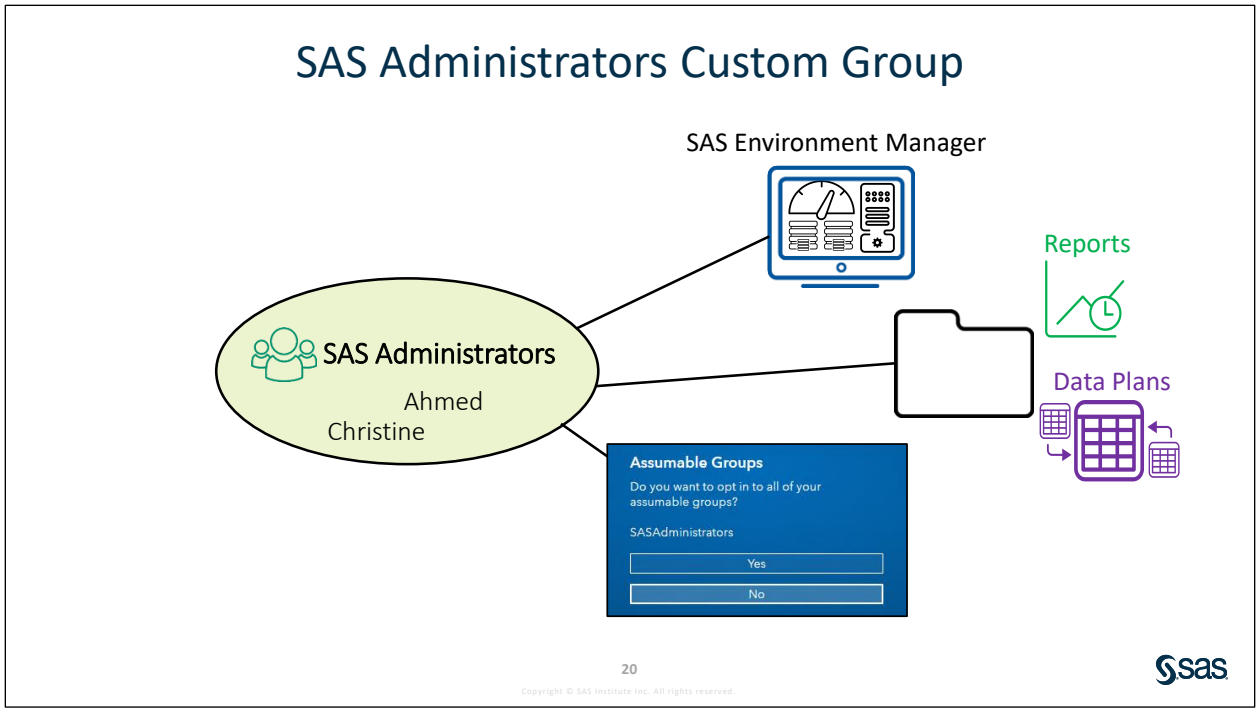
```
/workshop/LWSAVI35/scripts/L04/practice07_addFinanceGroup.sh
```

End of Practices

3.3 Exploring Administrative Groups and Roles

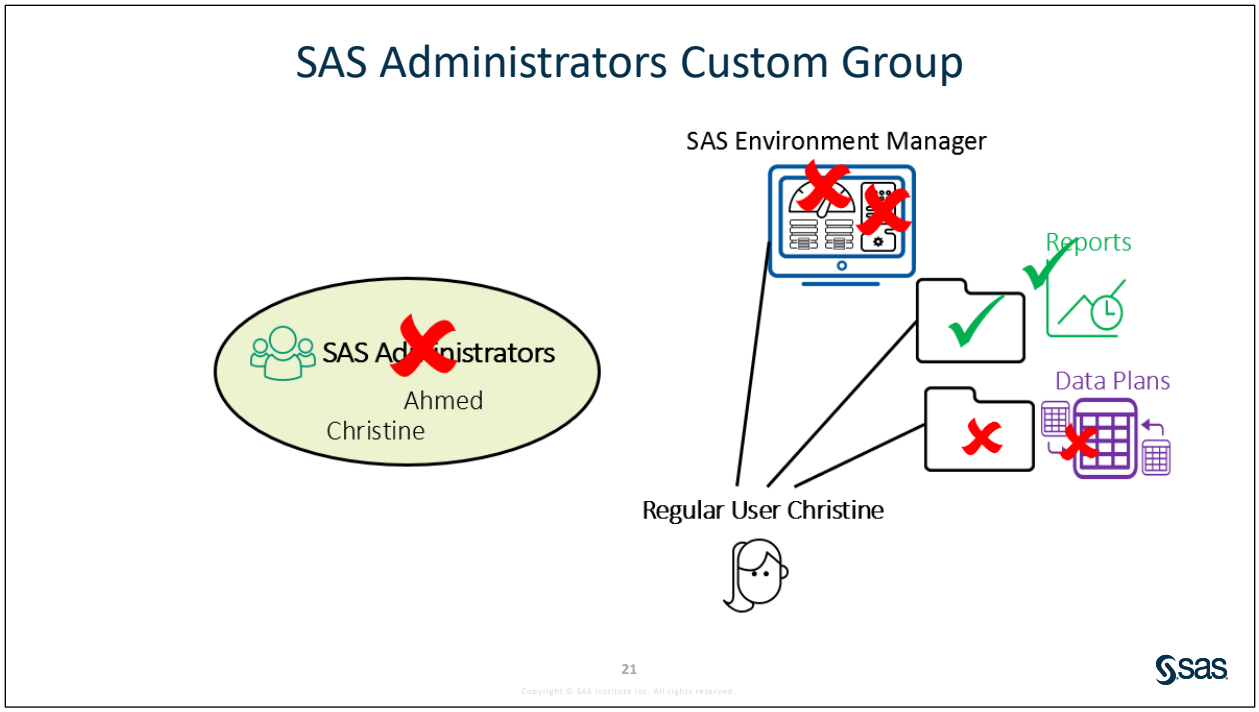


The SAS Administrators custom group has access to all tasks in SAS Environment Manager, and all folders and all objects that the folders contain (for example, data plans and reports).

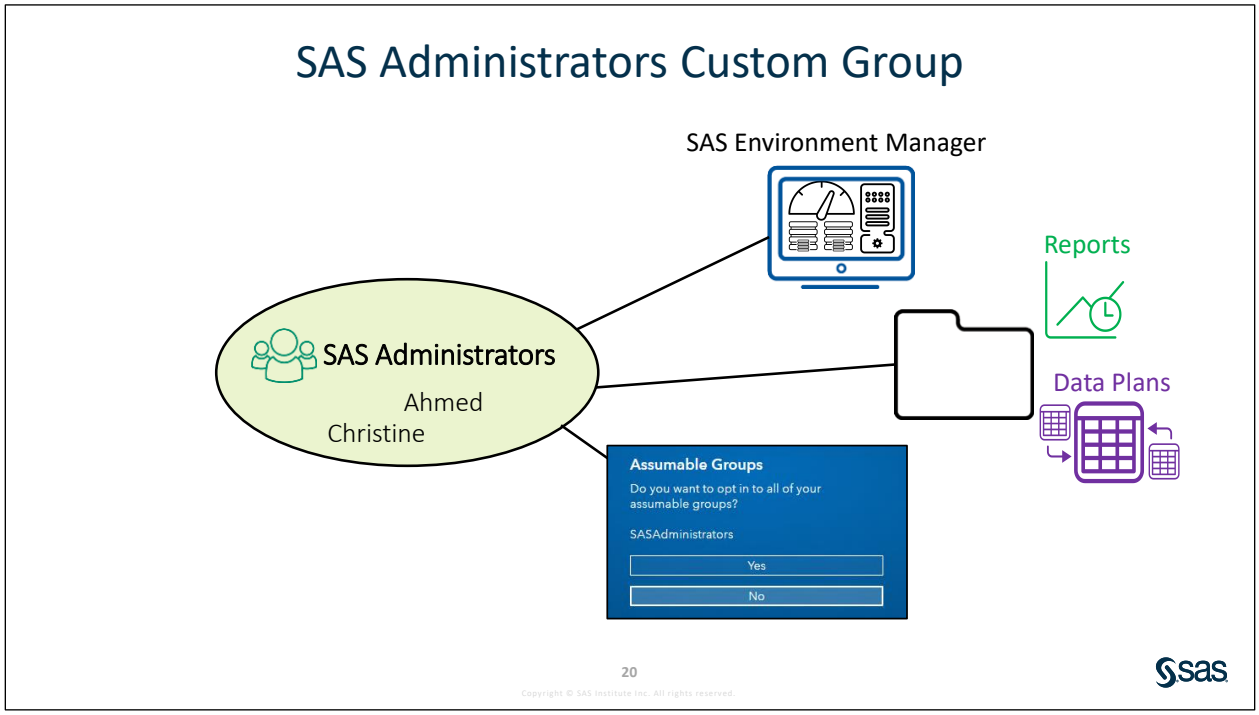


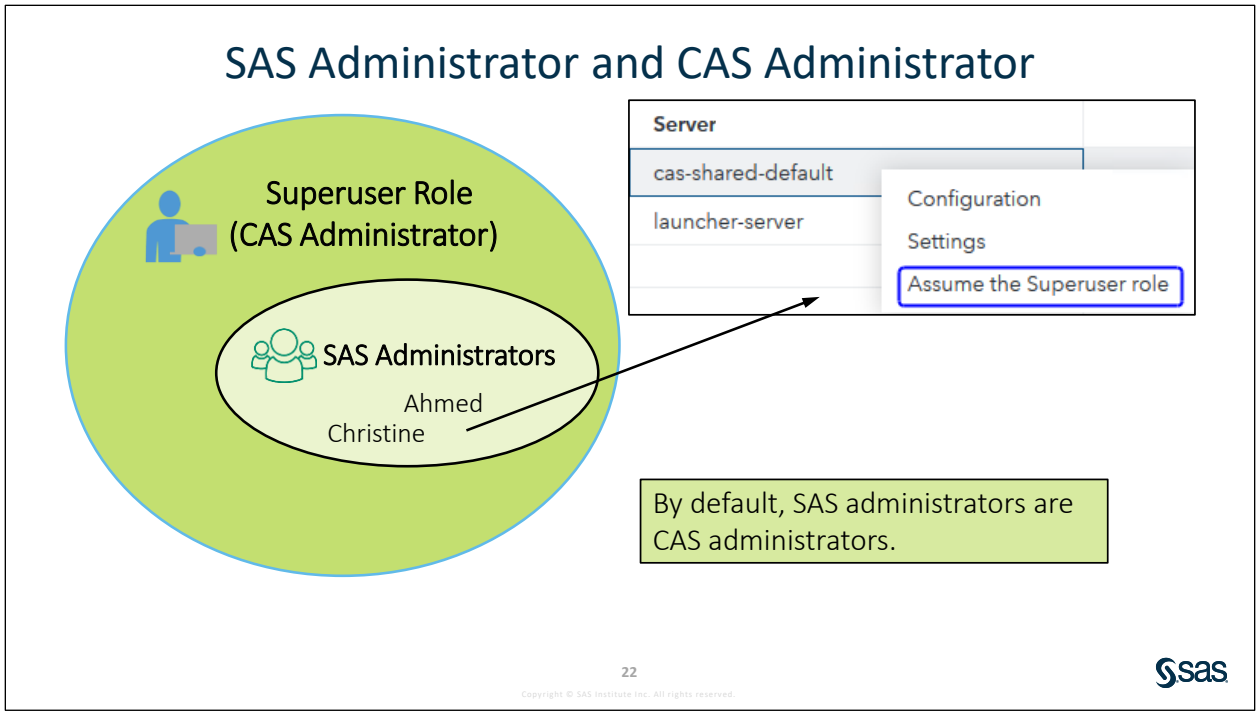
SAS Administrators custom group is an ***assumable*** group. When a user in this group signs on to SAS Viya, a prompt appears regarding opting in to their assumable groups. A list of assumable groups to which the user belongs appears below the prompt.

If the user selects Yes, the user gets the extra permissions that are associated with the assumable groups.

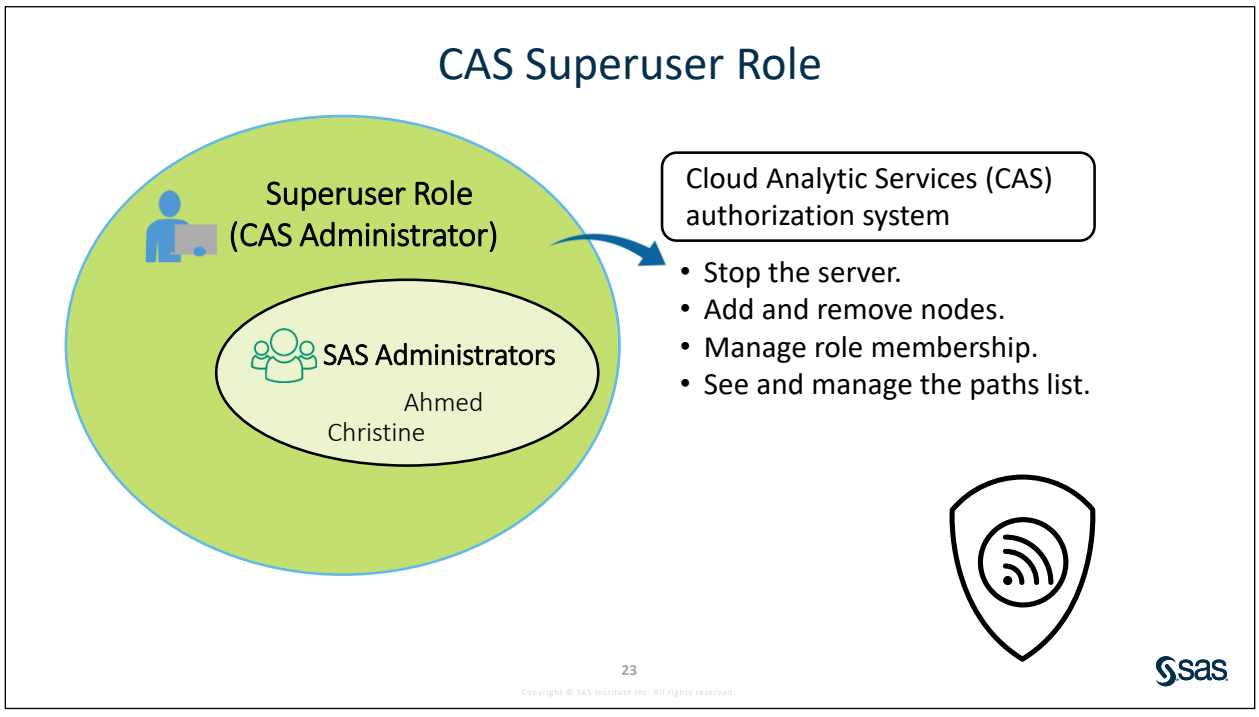


If the user selects No, the user does not get the extra permissions. The selection remains in effect until the user signs out. As a best practice, users should select Yes only when they need to perform tasks that require the extra permissions.

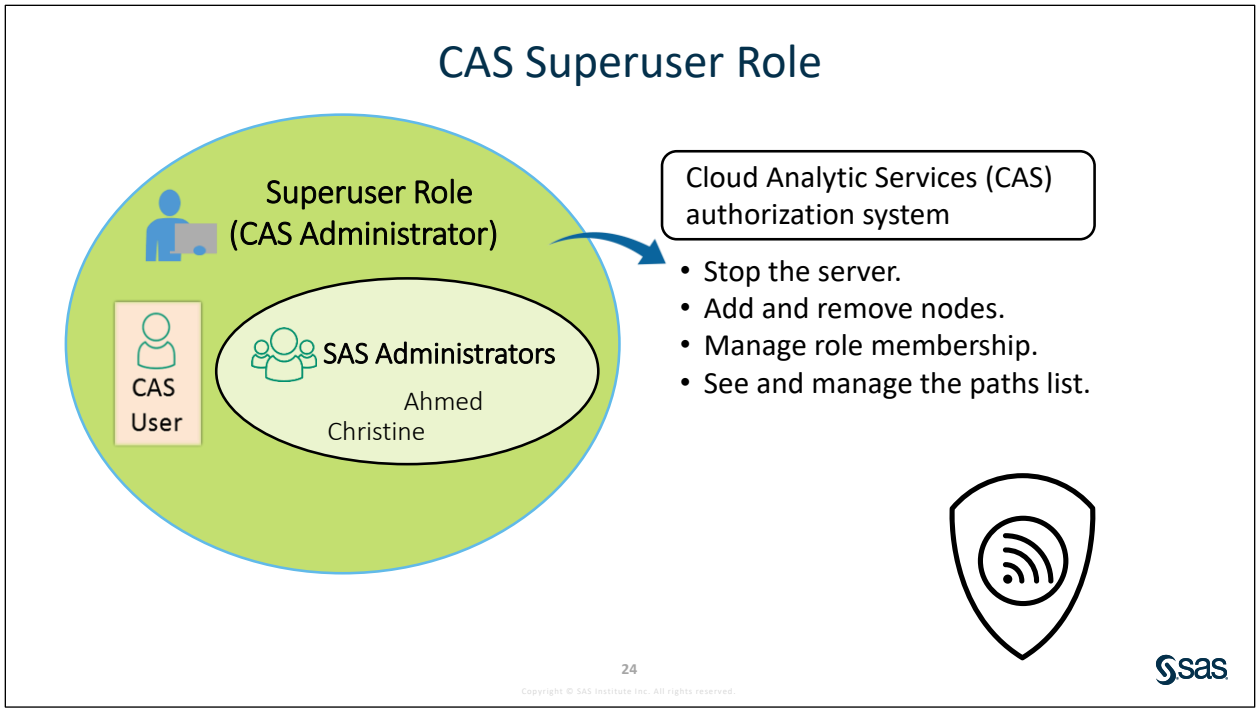




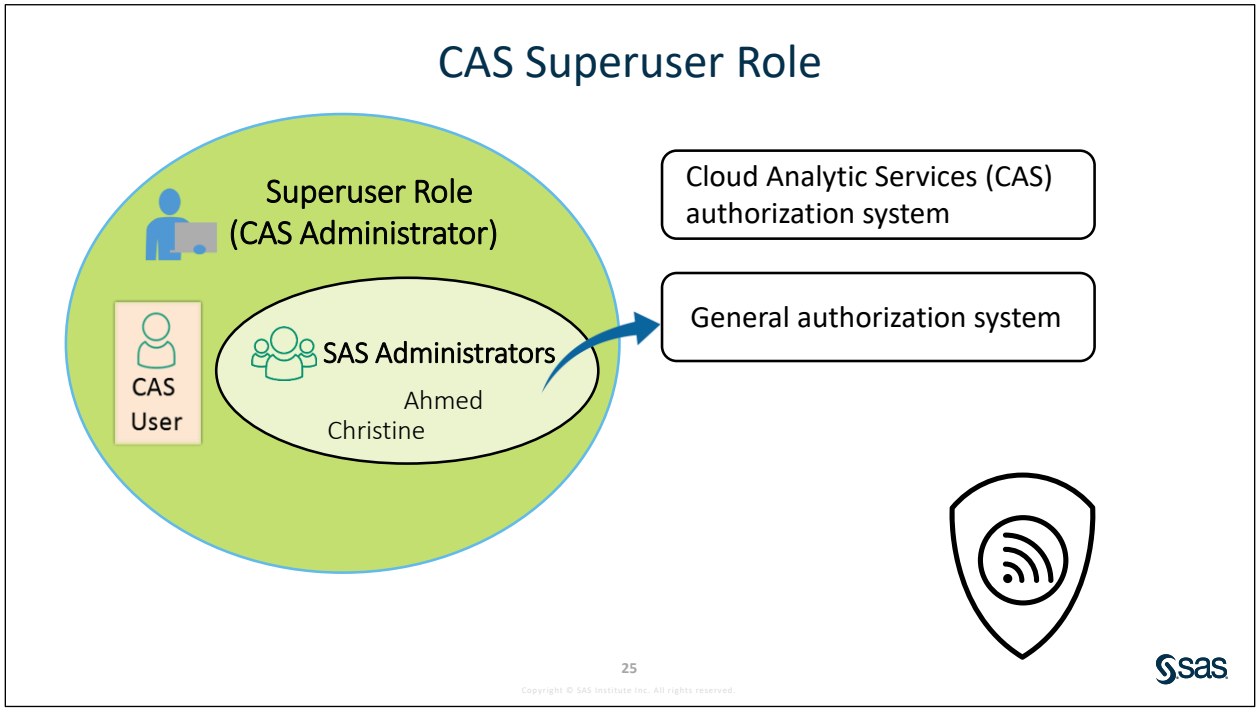
Members of the SAS Administrators can assume the CAS Superuser role. By default, the SAS Administrators custom group is a member of the CAS Administrator role.



CAS roles determine the level of administrative access for the CAS server and caslib administration and authorization tasks. This pertains to the CAS authorization system, one of two systems that make up the SAS Viya authorization layer. Superusers are exempt from permissions regarding access to CAS. Only a superuser can stop the server, add and remove nodes, manage role membership, and see and manage the paths list.



The account that starts a CAS server is an implicit member of the CAS Superuser role.



The SAS Administrators custom group provides access throughout the general authorization system, the other system that makes up the SAS Viya authorization layer. A predefined rule grants all permissions throughout the general authorization system to the SAS Administrators group. However, the SAS Administrators group is not unrestricted or exempt from authorization requirements.

Practice

8. Adding a User to the CAS Superuser Role

In this practice, you add Lynn to the Superuser role. The membership is validated after she is added.

a. Sign in to SAS Environment Manager as **lynn** with the password **Student1**. (Lynn has no assumable groups. Specifically, she is not in the SAS Administrator group.)

If this is your first time in the class logging in as **lynn**, a welcome message will appear. Select **Skip setup**.

b. Can Lynn see all the actions from the side menu that Christine can see, when Christine assumes her membership to the SAS Administrator group?

c. Select **Servers** ⇨ right-click **cas-shared-default** ⇨ **Settings**. Lynn cannot assume the Superuser role.

d. Click **Lynn** and select **Sign Out**.

e. Sign back on as **christine** with the password **Student1** and opt in to assumable groups.

f. Add Lynn to the Superuser role.

1) Select **Servers** ⇨ right-click **cas-shared-default** ⇨ **Assume the Superuser role**.
2) Right-click **cas-shared-default** ⇨ **Settings**.
3) Click **Superuser Role Membership**.
4) Add **Lynn** using the edit button.
5) Move **Lynn** to **Selected Identities** using the arrow between the two lists.

g. Sign out as **Christine** and sign back on as **lynn** with the password **Student1**, and verify that the **Assume the Superuser role** option is available. Do you see more actions on the side menu in SAS Environment Manager because of your CAS Superuser role?

9. Adding Identities to the Data Builders and Application Administrators Custom Groups

In this practice, you add Lynn to the Application Administrators custom group. Then you add the Finance group to the Data Builders custom group. (Lynn is a member of the Finance group.)

a. Sign in as **christine** with the password **Student1**. In the Assumable Groups window, click **Yes**

b. Add Lynn to the Application Administrators custom group. Members of Application Administrators can access selected administrative functions within applications.

1) Select **Users** from the side menu.
2) Highlight **Application Administrators** from **View** ⇨ **Custom groups**.
3) Click **Edit** icon to the right of Members area.
4) Move **Lynn** to the **Selected Identities**. Click **OK**.

c. Add the Finance custom group to Data Builders custom group. (The Finance group was created through the CLI in the previous practice.)

1) Highlight **Data Builders** from **View** ⇨ **Custom groups**.
2) Click **Edit** icon to the right of the Members area.

3) Move the **Finance** custom group to **Selected Identities**. Click **OK**.

d. To see the functionality that is granted to Application Administrators and Data Builders, select **Rules** from the side menu.

e. Filter on Application Administrators to bring up only rules that pertain to this custom group.

1) Select **Choose Identities** under the **Principal** section from the **Rules Filter** side.

2) Select **Custom groups** from the **Filter by** drop-down menu and move **Application Administrators** to the **Selected Identities**. Click **OK**.

3) Check the **Application Administrators** box and click **Apply** to apply the filter that will display rules with this group as the principal.

f. You can right-click a rule and select **Properties** to see a description of what this rule allows Application Administrators to do. For example, right-click **SASVisualAnalytics_capabilities/shareDataView** and select **Properties**.

g. Application Administrators can share a data view in SAS Visual Analytics. Click **Close**.

h. Filter on **Data Builders** in the Filter window.

1) Select **Choose Identities** under the Principal section from the Rules Filter side.

2) Select **Custom groups** from the **Filter by** drop-down menu and move **Data Builders** to the **Selected Identities**. Remove **Application Administrators**. Click **OK**.

3) Check the **Data Builders** box and click **Apply** to apply the filter that will display rules with this group as the principal.

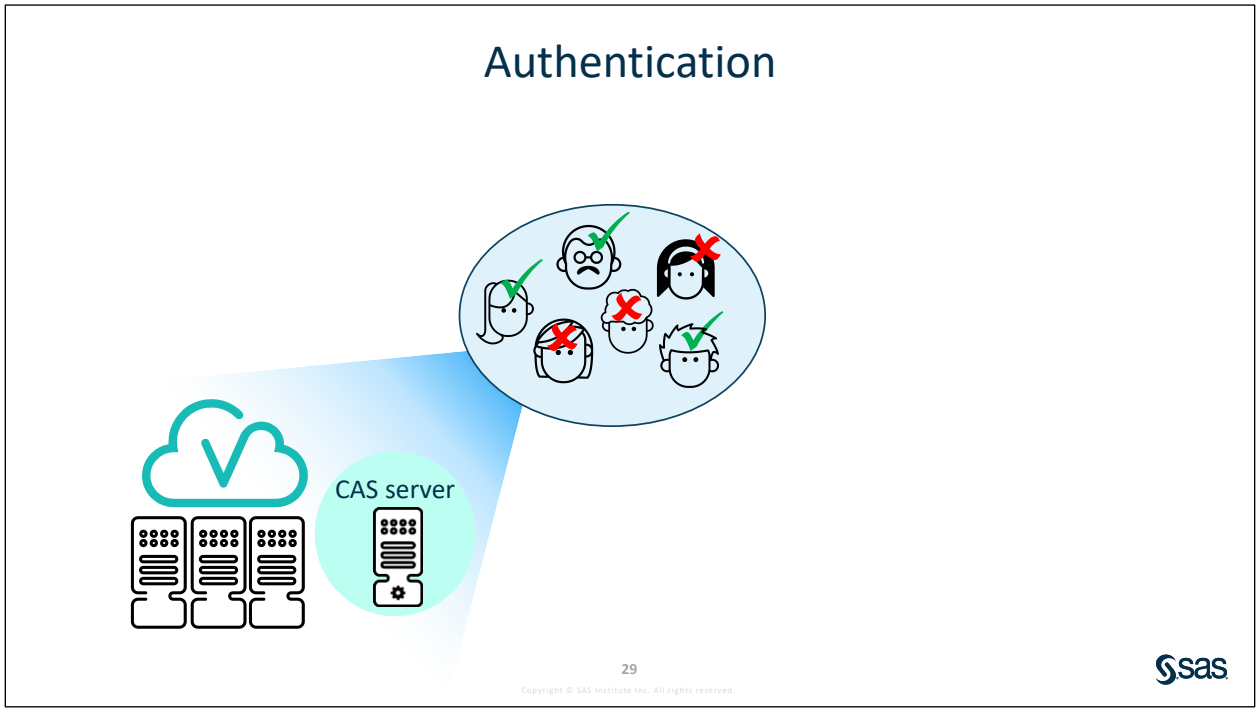
i. Right-click **/SASDataStudio/**** and select **Properties**.

j. Members of the Data Builders custom group can access SAS Data Studio, the visual interface that is included with SAS Data Preparation.

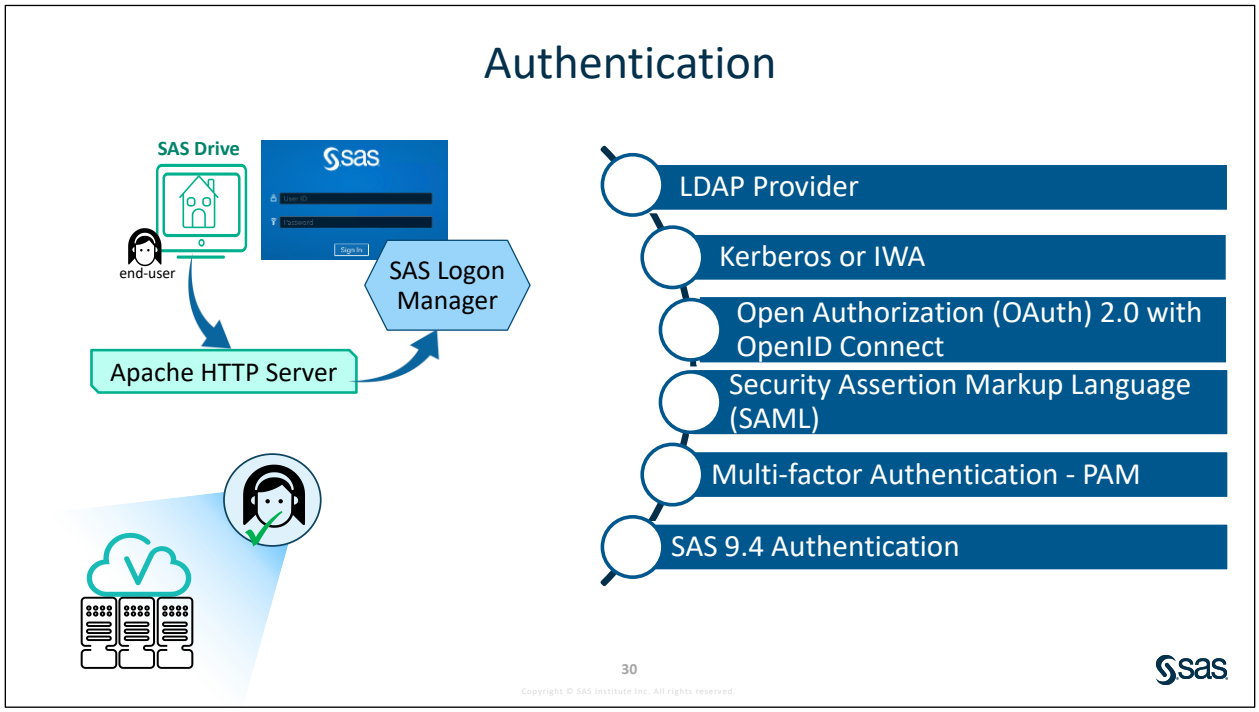
Note: Rules are discussed in the next lesson.

End of Practices

3.4 Authentication



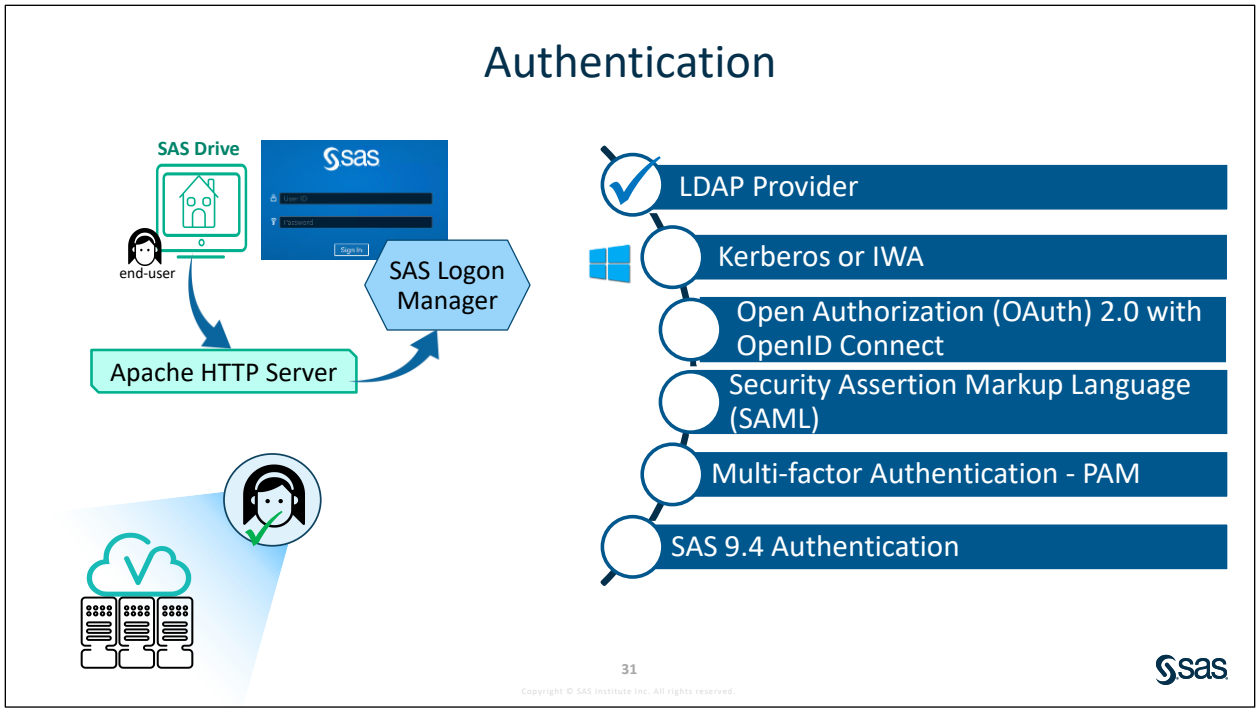
Authentication is the process of verifying the identity of a user that is attempting to log on to or access software or a server.



In a full deployment, the SAS Logon Manager web application provides the authentication services for visual interfaces. It is accessed via the Apache HTTP Server.

SAS Viya supports six authentication mechanisms.

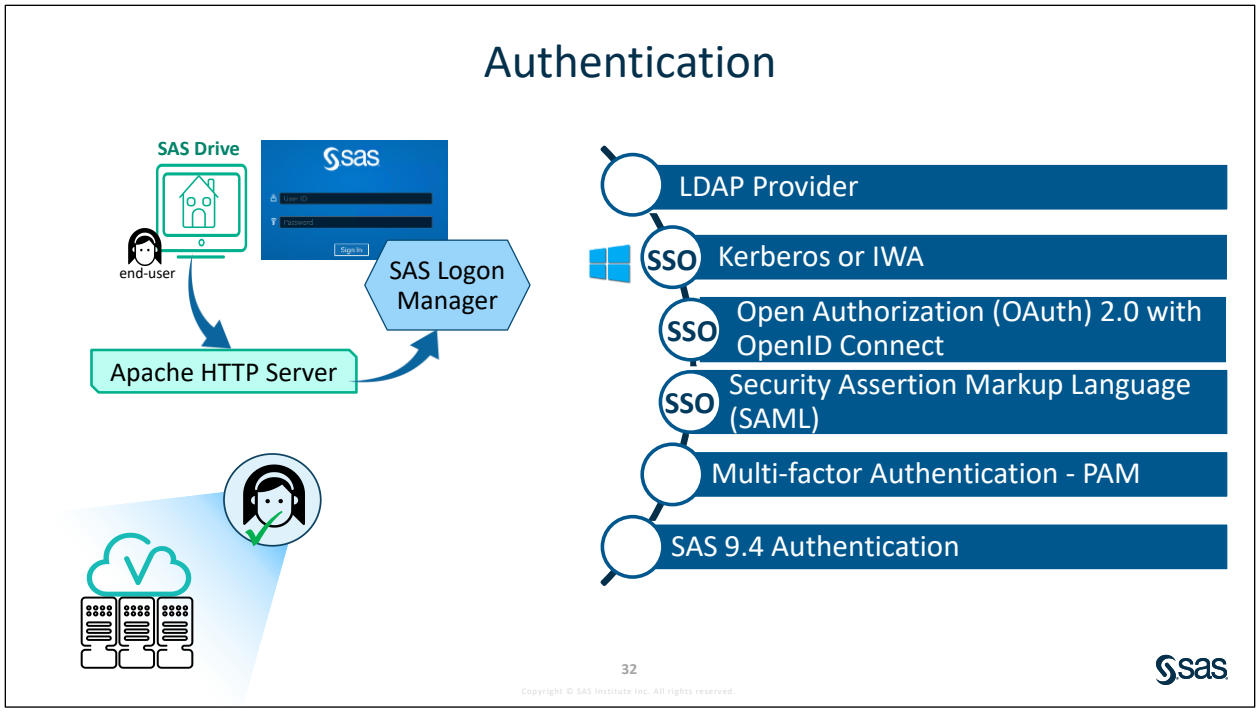
The security architecture used by SAS Logon Manager is built around Open Authorization (OAuth) and OpenID Connect.



The default authentication mechanism that is configured is your LDAP provider.

Authentication support is also available for Kerberos or Integrated Windows Authentication (IWA). This means that the user is not supplying credentials but instead tickets are passed over the network.

For Windows deployments, Kerberos or Active Directory is the only supported authentication mechanism for visual interfaces and configuration of the middle tier environment.

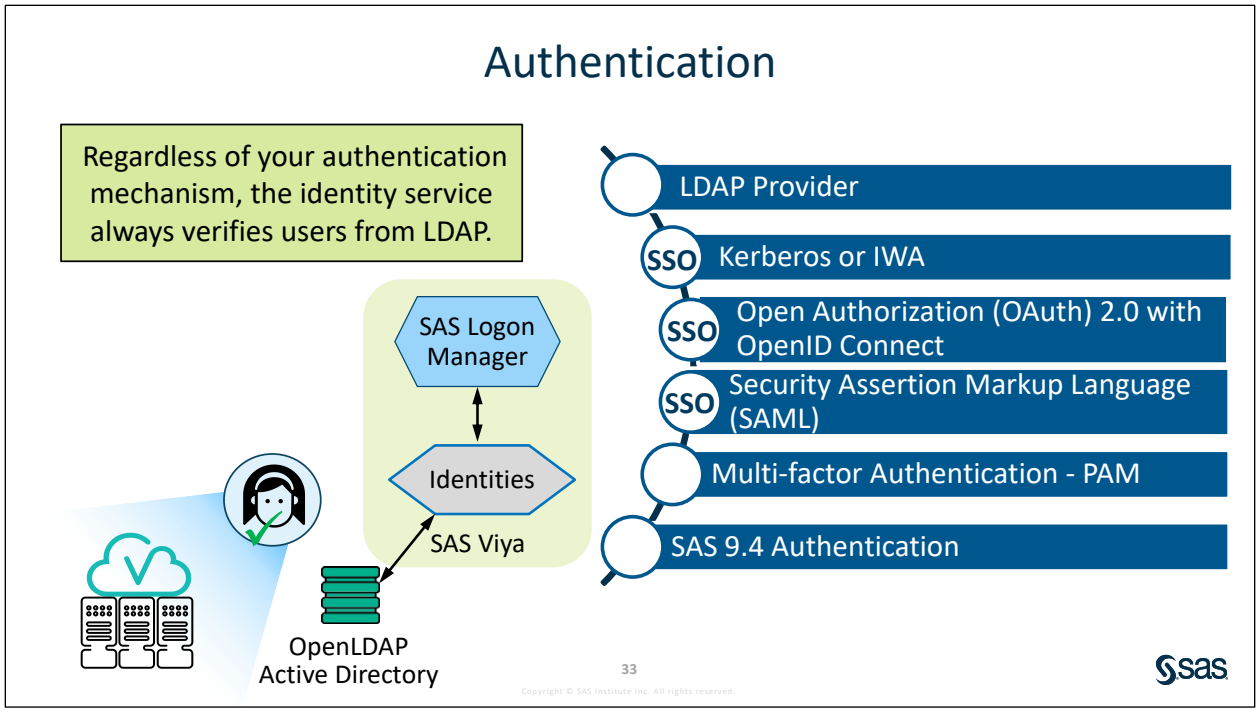


Other single sign on mechanisms that are supported are OAuth with OpenID connect and SAML (Security Assertion Markup Language) identity provider.

Multi-factor authentication is an option that has been available since SAS Viya 3.3 and requires the configuration of PAM, or pluggable authentication module. The SAS Logon Manager uses the operating system PAM stack.

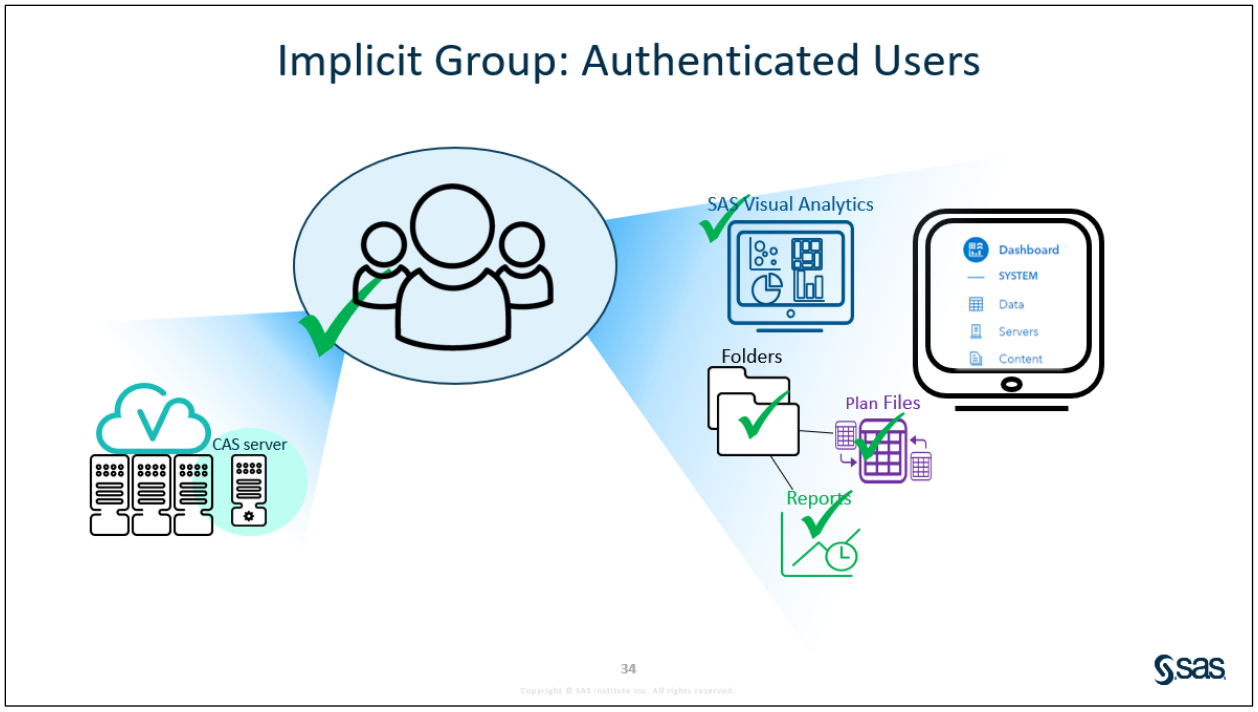
SAS Viya also supports the use of an existing SAS 9.4 environment, and this can be any release of SAS 9.4.

Note: For a programming-only and full deployment, host authentication is supported on both Linux and Windows systems. On Linux systems, you can configure the host to use only pluggable authentication modules (PAM).

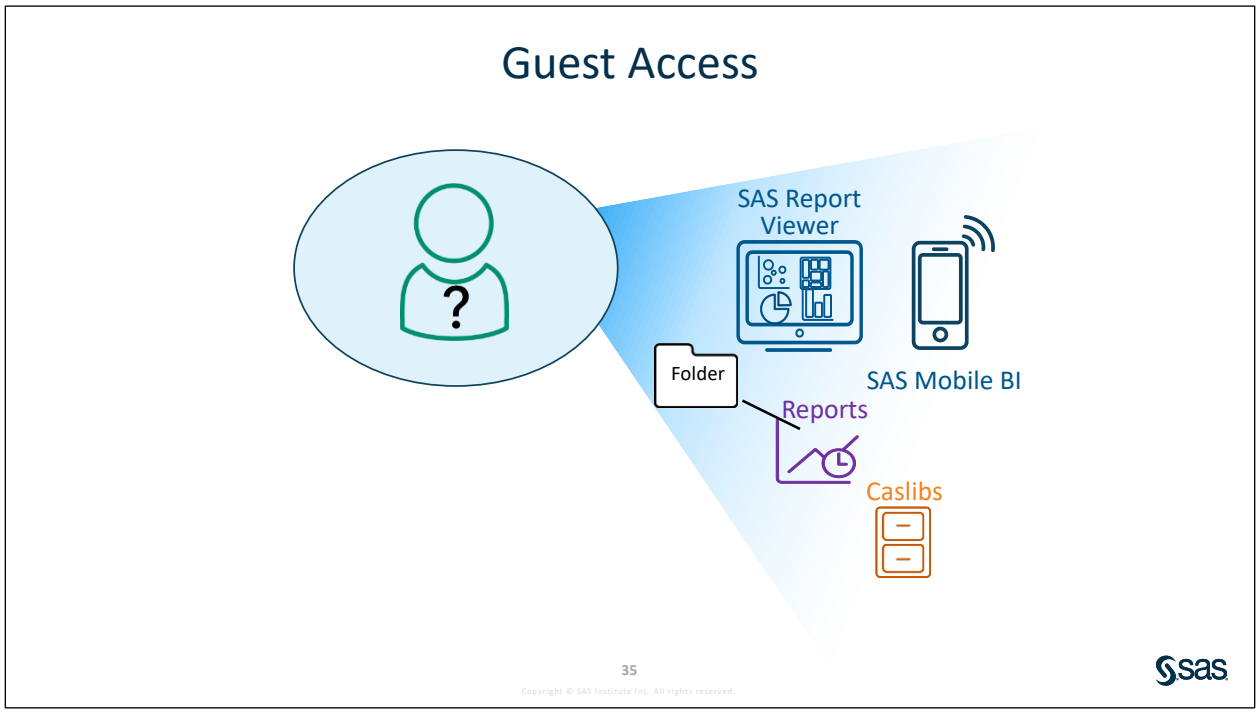


The following table lists the key services that are used in authentication in SAS Viya:

Service Name	Description
SAS Logon Manager	Provides and end-user interface for authentication and internal authentication to other services. • Enables single sign-on within the SAS Viya environment between services. • Enables single sign-on to the SAS Viya environment through configuration of third-party software.
Identities service	Provides the user and group information to other services. Reads user and group information from the LDAP provider.
Authorization service	Provides authorization information to other services.
Launcher service	Provides the connection and authentication to the SAS Launcher Server. Resolves the credentials that are used when authenticating to the SAS Launcher Server.
SAS Cloud Analytics Services	Authenticates end users launching CAS sessions by way of the SAS Cloud Analytics Services controller.
SAS 9.4	Supports several mechanisms for coupling authentication with SAS 9.4.
SAS Studio (Basic)	Leverages the SAS Object Spawner to authenticate users accessing SAS Studio (Basic).

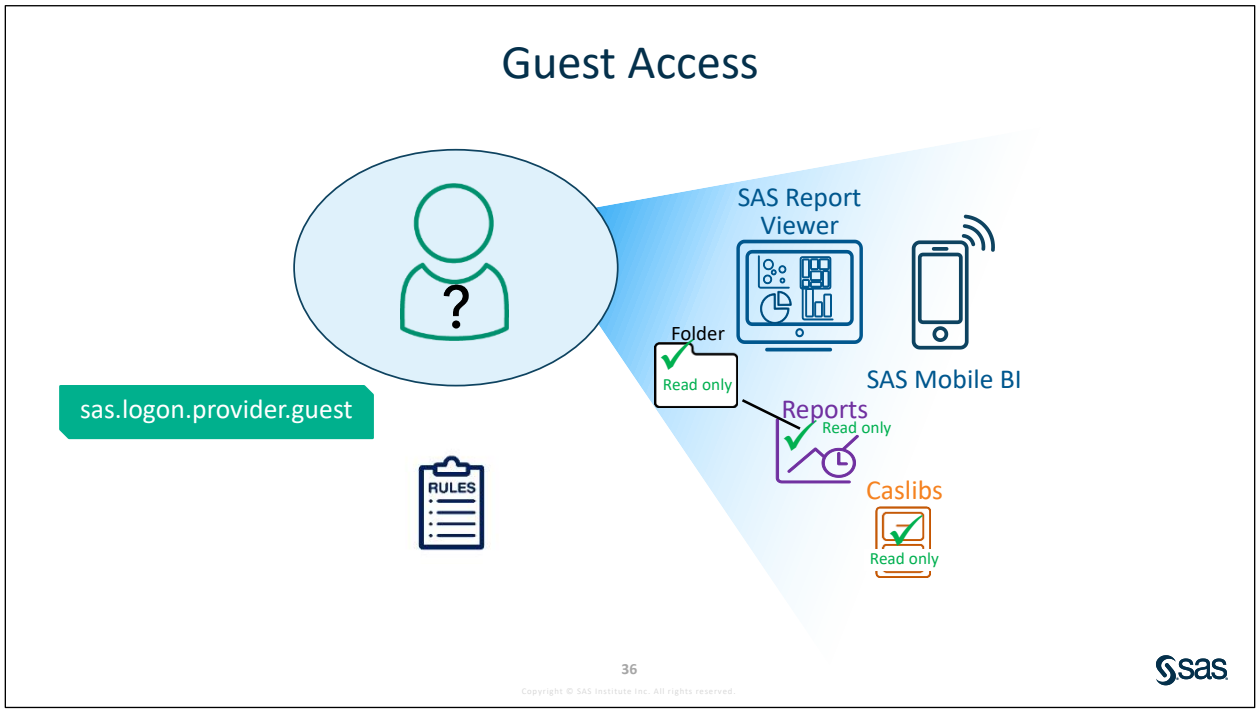


The *Authenticated Users* group is an implicit group to which all users who can authenticate to the system belong. The members of this group are in the identity cache. All authenticated users can initially access the Dashboard, Data, and Content pages in SAS Environment Manager; the group can access SAS Visual Analytics and perform operations on folders and on the objects that the folders contain (subject to permissions).



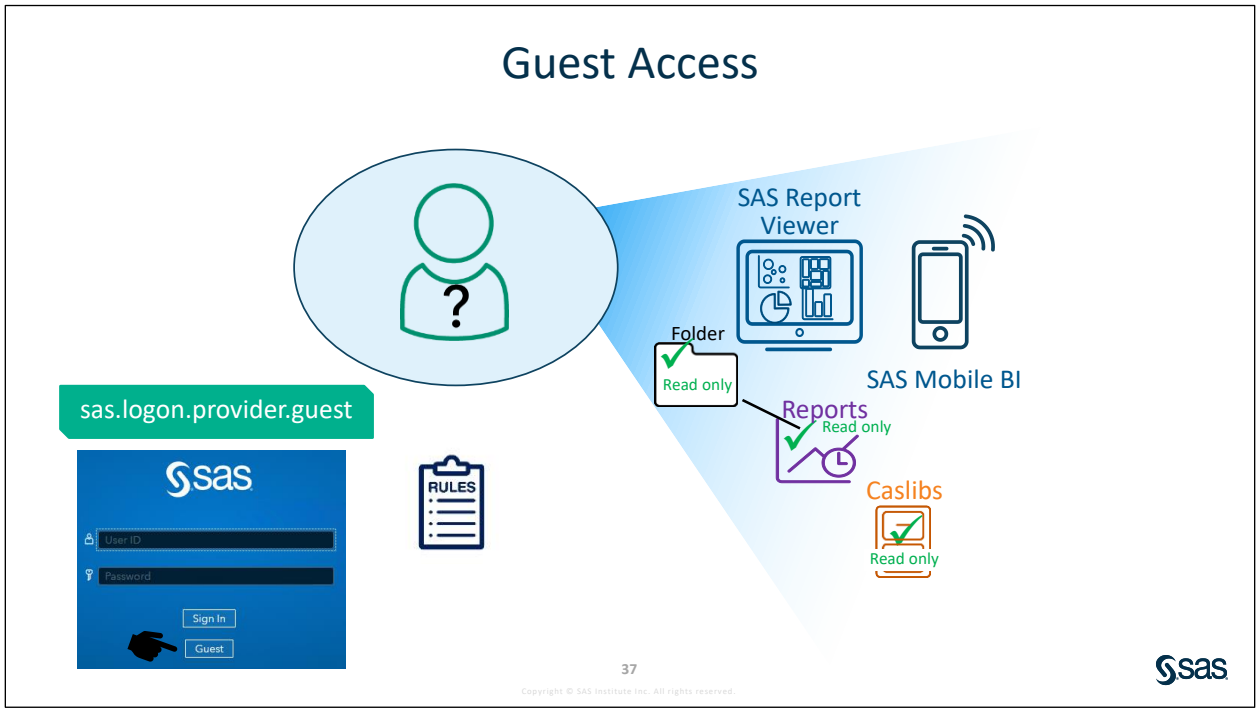
If there are reports that need to be viewed by users that cannot be authenticated to SAS Viya, *guest access* is an optional feature that provides anonymous Read-Only access to a subset of resources.

With guest access, you can view reports in the SAS Report Viewer and the SAS Visual Analytics Apps.



Guest access is enabled by setting the **sas.logon.provider.guest** configuration property, using Environment Manager.

Be sure to add access controls that provide Read access to caslibs, folders, and reports that should be accessible to guest users.



After guest access is enabled, a guest login button will be available in SAS Report Viewer and SAS Visual Analytics Apps.

Note: An implicit group called **Everyone** includes all authenticated users and guest users.

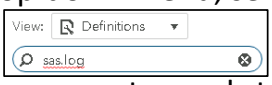
3.02 Activity

1. In SAS Environment Manager, select **Content** from the side menu.
2. Right-click the **Public** folder ⇨ **View authorization**. Who are the Principals listed? (A *principal* is a user or group to which a rule is assigned.) Click **Close**.
3. Select **Rules** from the side menu. How many implicit Principals (or identities) are there?
4. Is **Guest Access** enabled? Hint: Apply a filter with **Guest** checked.

39

3.03 Activity

1. In SAS Environment Manager, select **Configuration** from the side menu.
2. From the **View** drop-down menu, select **Definitions**.
3. Search **sas.log**.

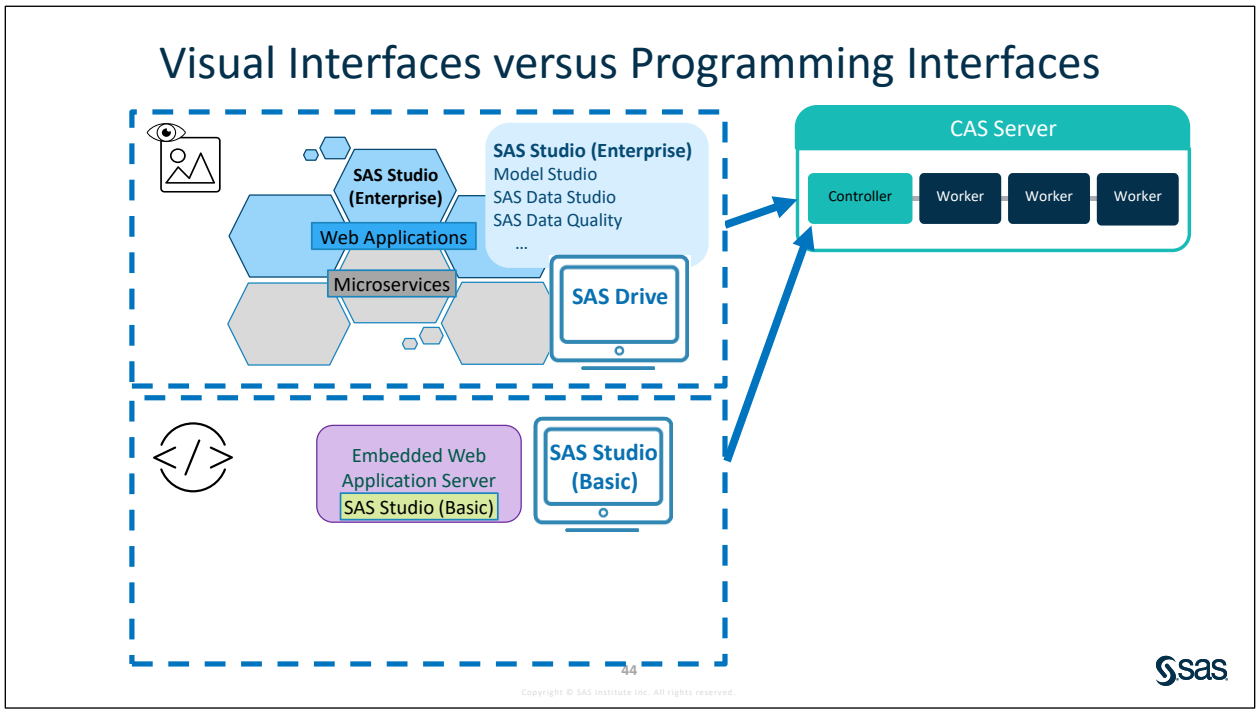


4. What configuration property needs to be configured to enable guest access?
5. What service needs to be restarted when configuring properties pertaining to authentication mechanisms?

   Hint: Highlight **sas.logon.kerberos**

41

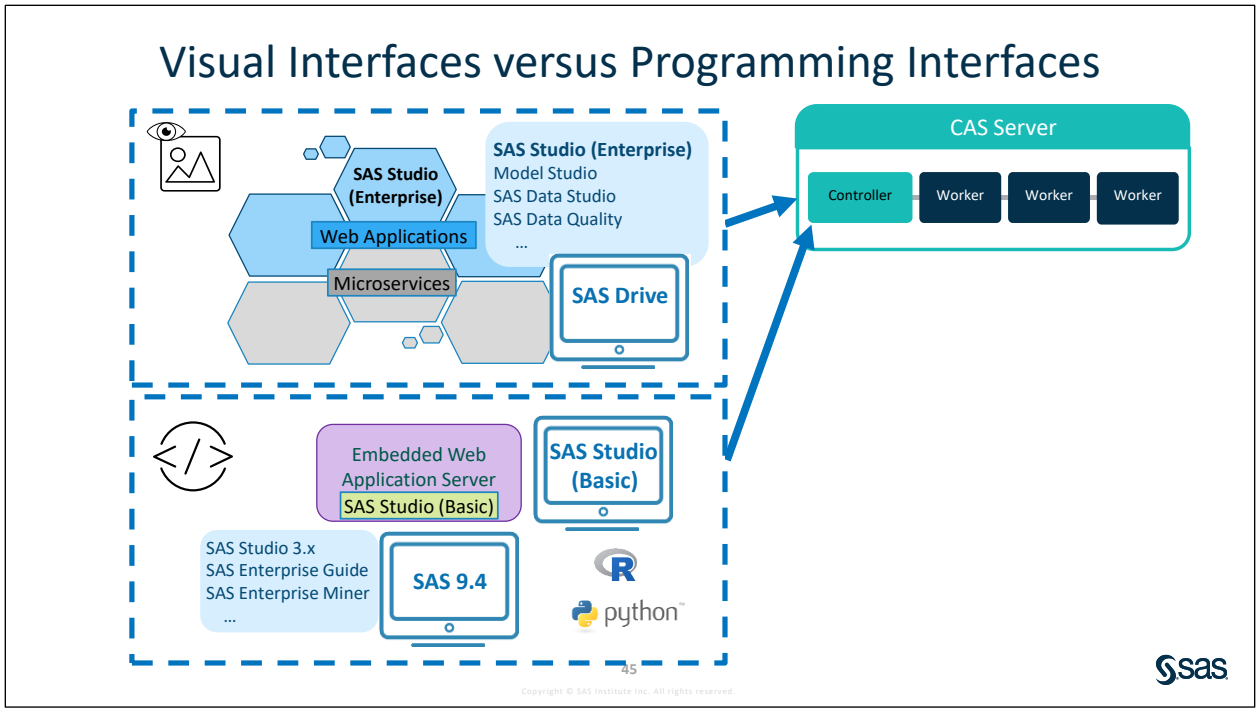
3.5 Exploring Authentication to Processing Servers



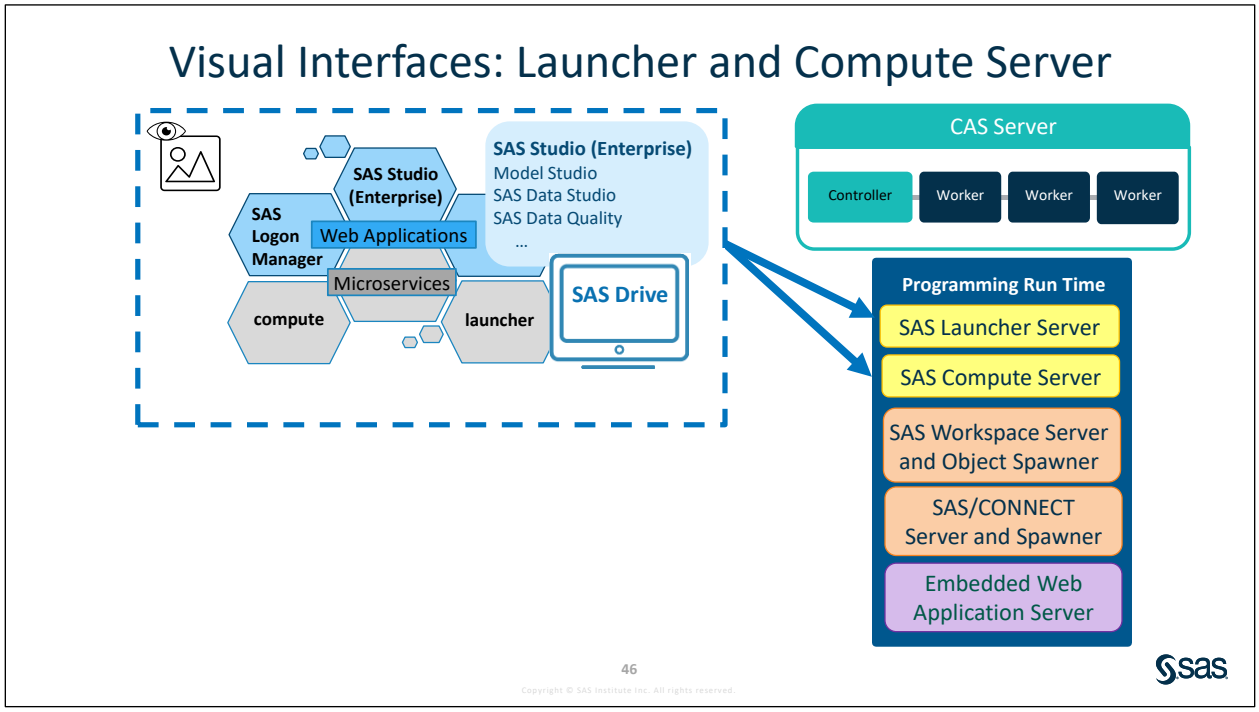
SAS Viya includes two releases of SAS Studio: SAS Studio (Basic) and SAS Studio (Enterprise). SAS Studio (Enterprise) is the new, microservices-based version and integrates with other SAS Viya visual interfaces, all of which can be accessed through SAS Drive.

SAS Studio (Basic) is the traditional version that has been available since the first release of SAS Viya and has an embedded web application that does not rely on external services. This is referred to as a *programming interface*. If you have a programming-only environment, you will have only SAS Studio (Basic), because microservices and web applications are not included.

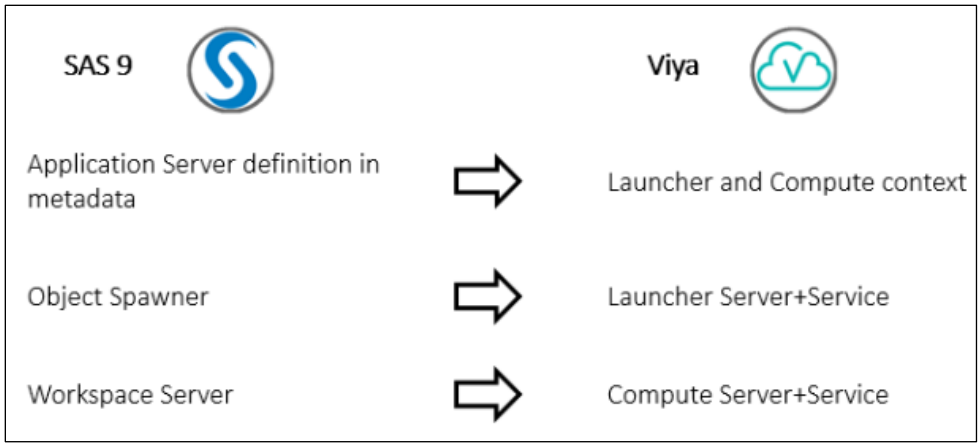
Code submission from either version of SAS Studio can occur on the CAS server.



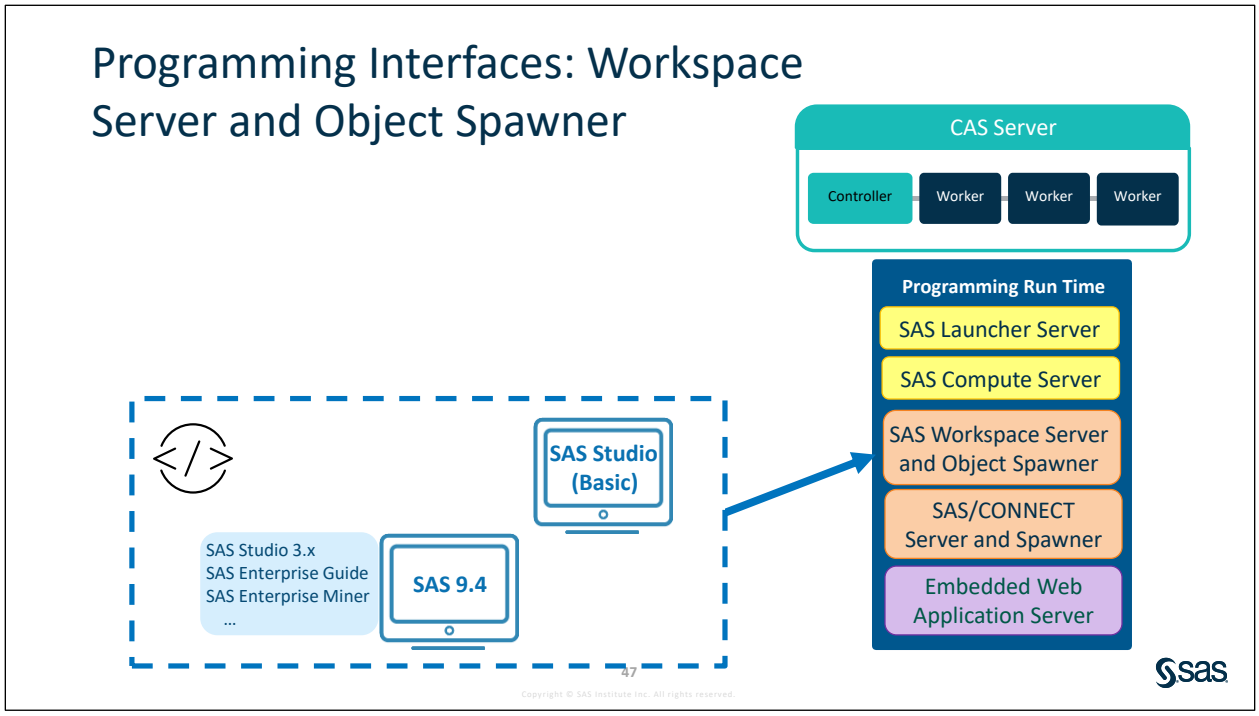
Programming interfaces also include Python, R, or Java interfaces that access SAS Cloud Analytic Services. And, you can directly connect to CAS from SAS Foundation in SAS 9.4, so another interface to consider is the SAS 9.4 client.



With SAS Studio (Enterprise), any processing that is not on the CAS server will use the Launcher Server and Compute Server. The communication happens using the HTTP(S) protocol through REST interfaces. Clients do not directly talk to the back-end servers, as the communication is handled by the compute and launcher microservices on the front end. The compute service enables clients to submit SAS programs in the form of jobs for processing.

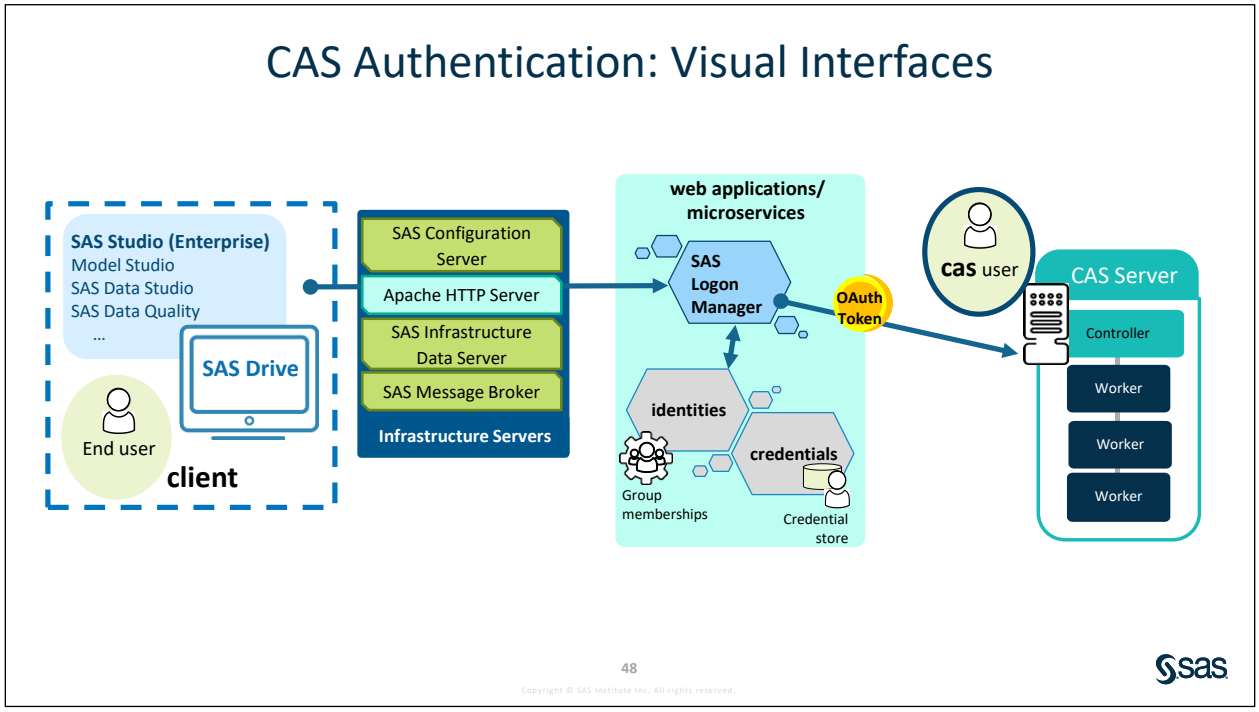


A compute server is like a workspace server, but a workspace server is accessed using the proprietary IOM protocol, and a compute server is accessed through the compute service via a standard REST API. A compute server instance uses the SAS Foundation executable provided by SPRE (/opt/sas/spre/home/SASFoundation). Just like the workspace server, the compute server is used to submit SAS code as jobs, query data, and access files via filerefs.



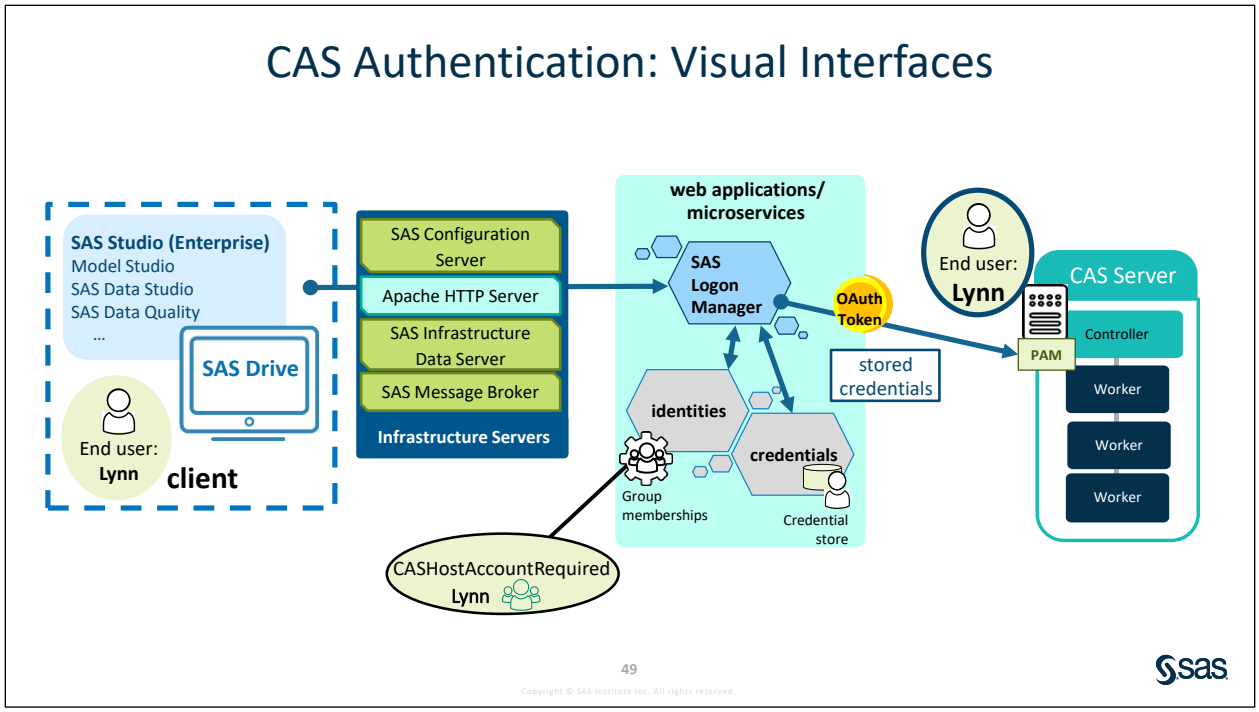
SAS Studio (Basic) and other programming interfaces use the SAS Workspace Server and Object Spawner to process jobs and tasks with the SAS language. The SAS Object Spawner creates a process for each client connection. SAS Workspace Servers are initialized by the SAS Object Spawner. An object spawner runs on the same machine as the workspace server, listens for requests, and launches the servers as necessary.

Note: SAS/CONNECT enables you to use SAS Viya functionality and processing power for users of SAS 9.4 in earlier versions of SAS Viya.



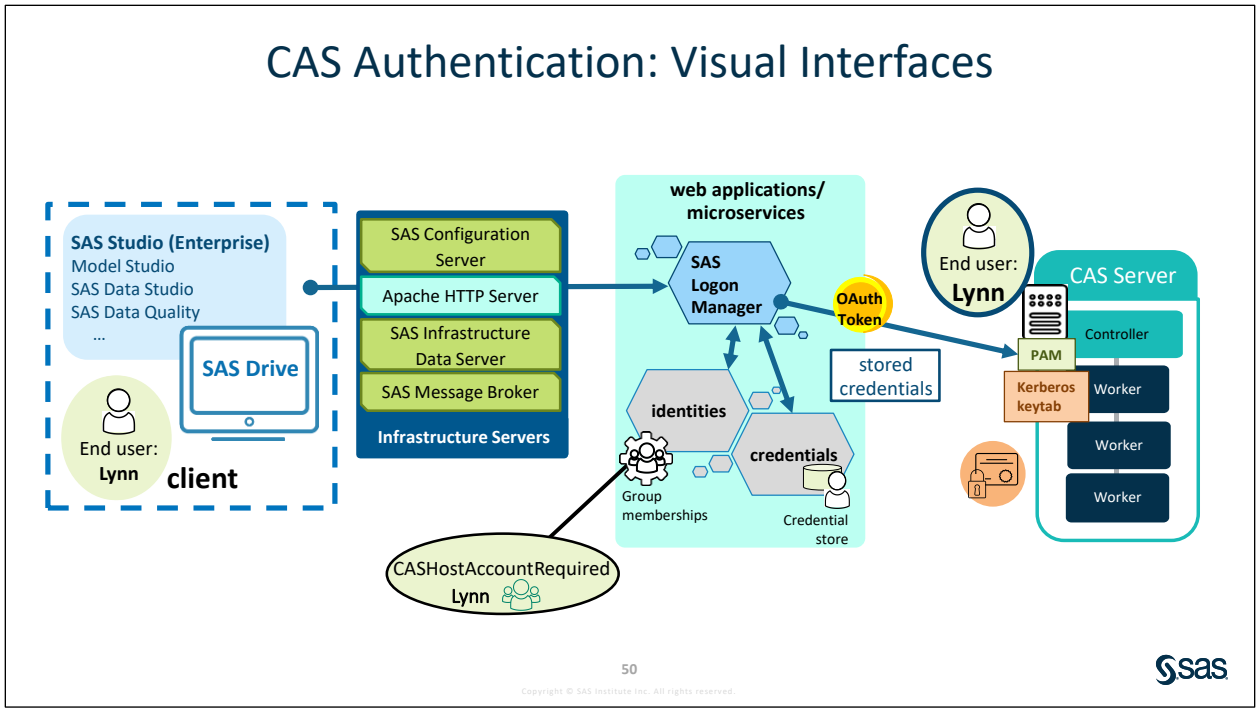
CAS authentication from visual interfaces, such as SAS Studio (Enterprise), occurs when the client requests a CAS session. Initial authentication has already taken place. The end user is authenticated with their internal OAuth token, and a CAS session will be launched using the service account CAS. The internal OAuth token is constructed by the Logon Manager and requires the end-users group information, which is provided by the identities microservice (The group information includes both LDAP and custom groups and is included in the claims in the OAuth token.)

This is without membership to the CASHostAccountRequired custom group.



If the end user is a member of the CASHostAccountRequired custom group, that means we want the CAS session to run as the end user. User names and passwords are stored in the credentials microservice. If credentials have been made available to the end user, either individually or through a group membership, these can be used to launch the CAS session. These credentials will be used with the PAM configuration for CAS to authenticate to the operating System.

(If credentials are not available, then CAS is able to just launch the process as the end user identified by the user name in the internal OAuth token. The name from the OAuth token must be valid on the operating system for this to succeed.)



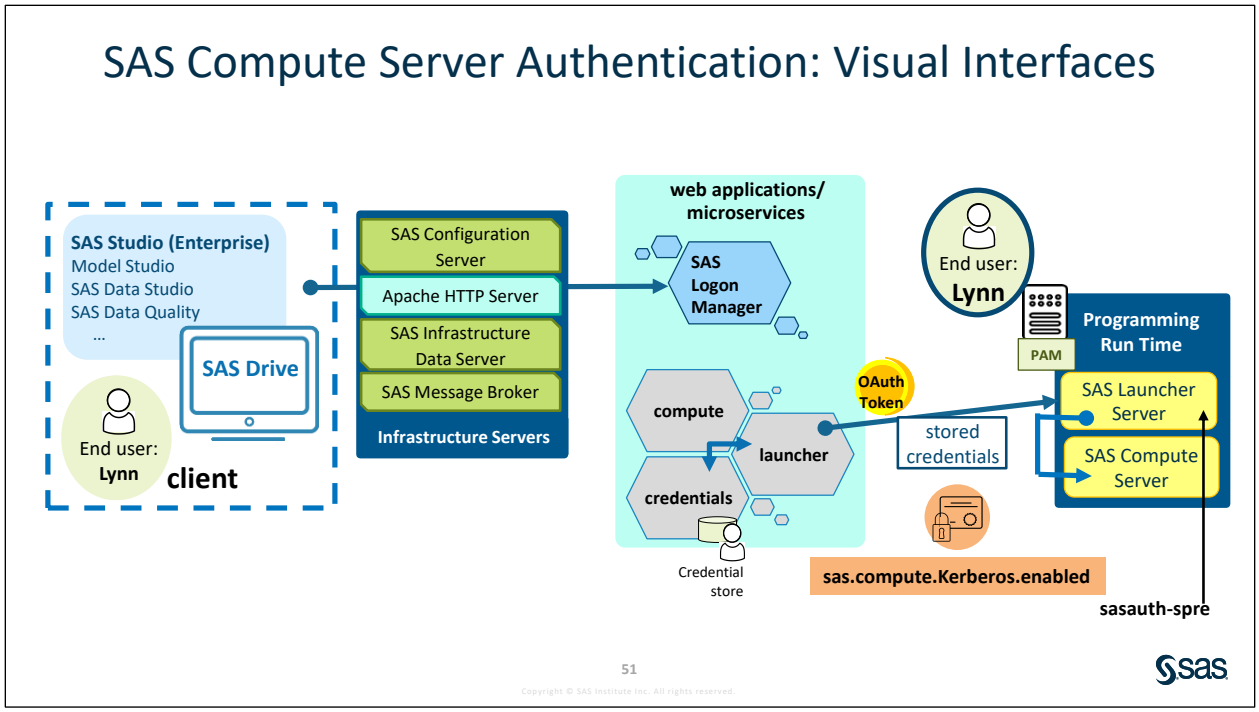
If the Kerberos-enabled configuration setting is present and set to true, then delegated Kerberos authentication will be attempted.

The CAS client in the web application is responsible for retrieving the delegated Kerberos credentials stored by SAS Logon Manager. The security rules ensure that only the end user who owns the Kerberos credentials can retrieve them.

The delegated credentials are used to request a Service Ticket for connecting to SAS Cloud Analytic Services. The CAS Controller is provided with a Kerberos keytab, that is used to validate the presented Service Ticket. If this is successful, the CAS session is launched as the end user and their Kerberos credentials are made available to the session.

However, the Kerberos credentials stored by SAS Logon Manager can expire or otherwise be invalid. If these cannot be used to authenticate the end user to SAS Cloud Analytic Services, an alternative is needed. As before, if a username and password have been stored for the end user, these can be used to authenticate.

Finally, if Kerberos is not successful and no username and password are stored, the CAS controller is able to directly launch the session as the end user, because it is running on Linux. This takes the username from the internal OAuth token. This username must be valid on the operating system.

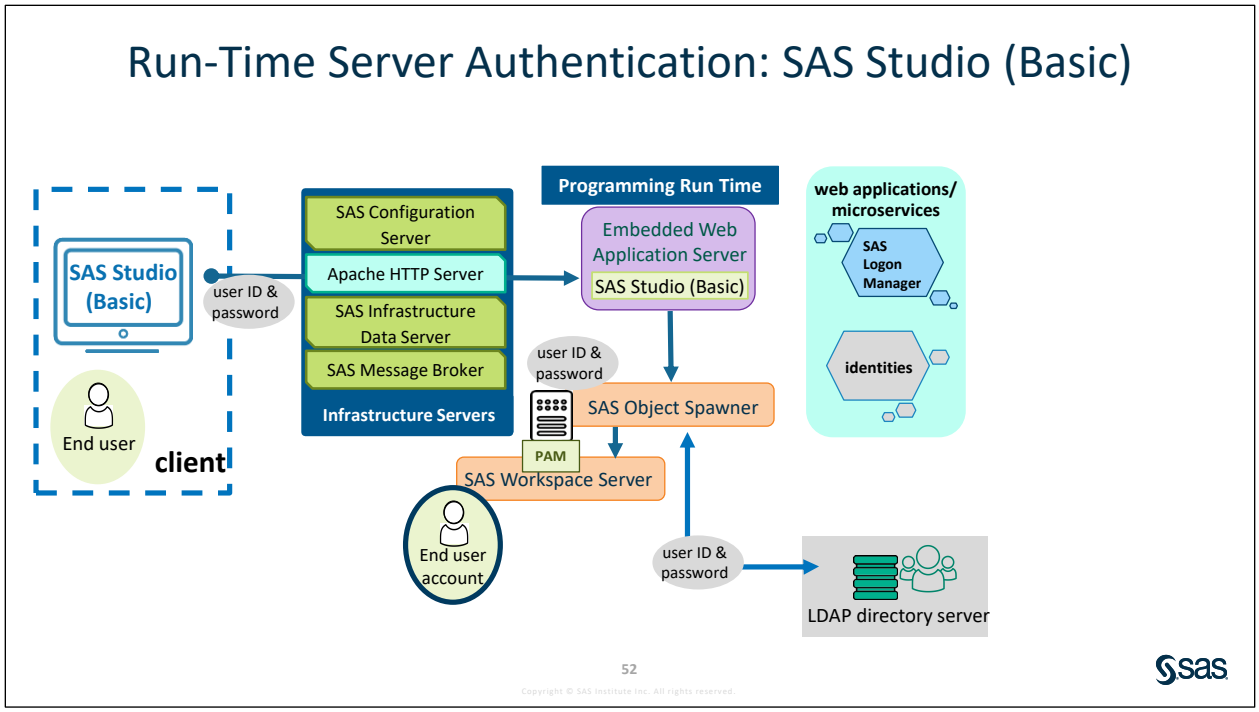


The SAS Compute Server always attempts to launch a server under the user ID of the requesting user, unlike SAS Cloud Analytic Services. Therefore, there is nothing equivalent to the **CASHostAccountRequired** group for the SAS Compute Server. The SAS Launcher microservice is performing all of the checks and the actual authentication to the SAS Launcher Server. The SAS Launcher Server starts the SAS Compute Server session after successful authentication.

A single configuration option, **sas.compute.kerberos.enabled**, is used to enable Kerberos authentication. This option is shared with SAS Cloud Analytic Services, so enabling Kerberos for one enables Kerberos for the other.

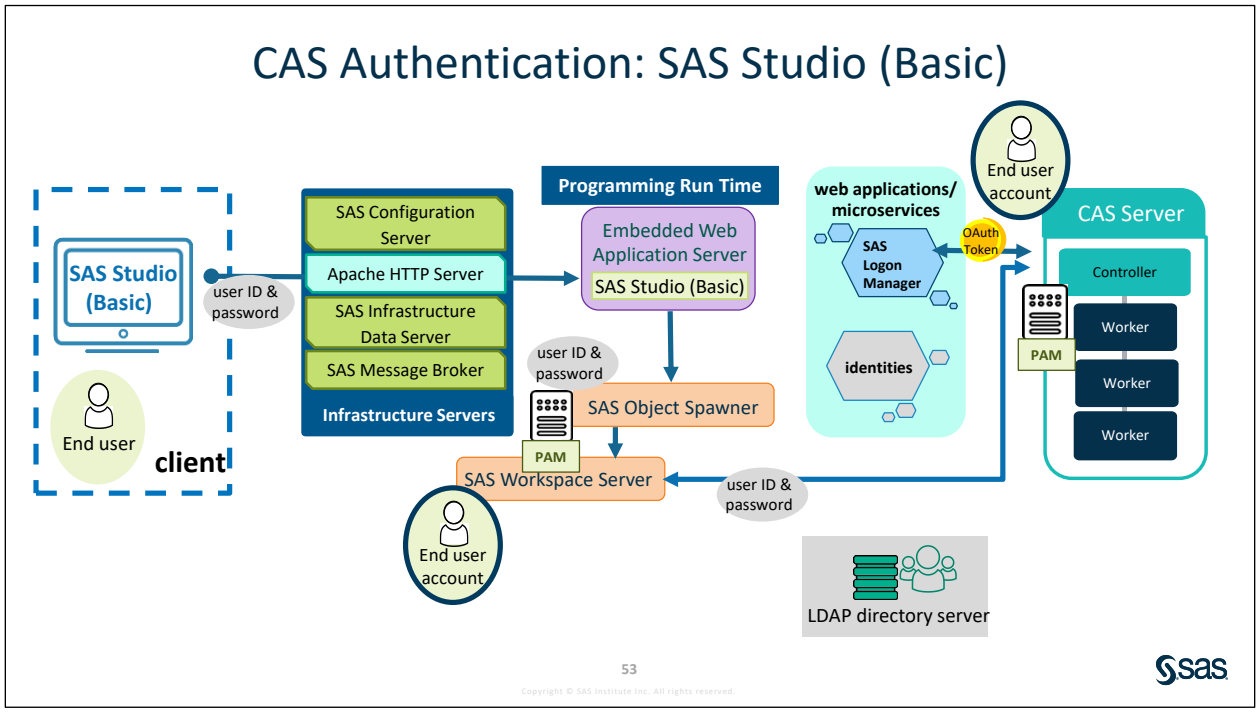
If Kerberos is not configured, a similar route is taken with the SAS Launcher microservice attempting to retrieve a username and password from the credentials microservice. If a username and password are stored for the end user, this will be leveraged by the SAS Launcher microservice to connect to the SAS Launcher Server. The SAS Launcher Server uses the **sasauth-spre** PAM configuration to validate the credentials and launch the SAS Compute Server.

If a stored username and password are not available, the SAS Launcher microservice uses the internal OAuth token to connect to the SAS Launcher Server. The SAS Launcher Server then launches the SAS Compute Server session for the end user using the username from the internal OAuth token. So, the username from the internal OAuth token must be valid on the operating system.



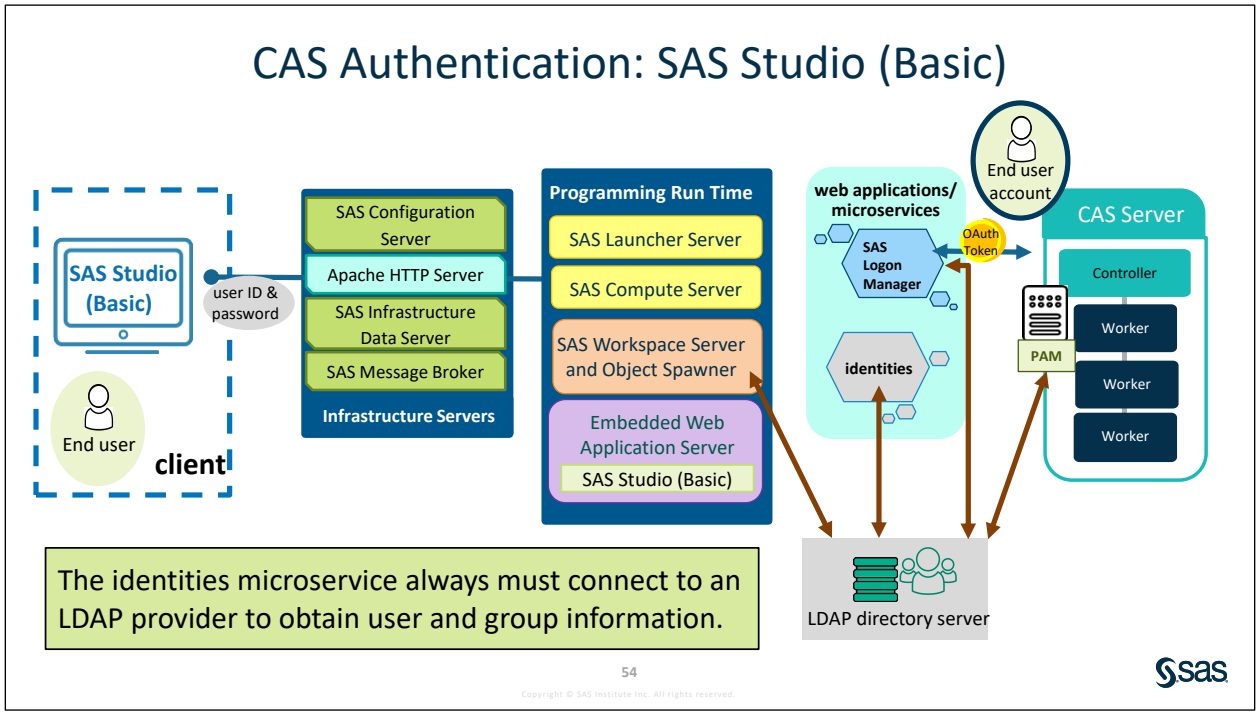
SAS Studio (Basic), the programming interface, is not integrated with the SAS Logon Manager.

The username and password entered into SAS Studio (Basic) are not passed to the SAS Logon Manager to authenticate. Instead, the SAS Object Spawner uses the PAM configuration on the host to validate the username and password. This could be a local account on the host or, depending on the PAM configuration, an account in an LDAP Provider. This authentication is sufficient to start the SAS Workspace Server where the code entered in SAS Studio (Basic) will be run.



When the SAS Workspace Server connects to the SAS Cloud Analytic Services environment, it uses the username and password that were used to start the SAS Workspace Server. The CAS Controller uses its own PAM configuration to validate the end-user's credentials and launch the session process running as the end-user.

Because SAS Cloud Analytic Services is integrated into the visual components of SAS Viya, the CAS Controller uses the username and password from the SAS Workspace Server to obtain an internal OAuth token from the SAS Logon Manager. This means that the username and password must be valid in the provider configured for the SAS Logon Manager. If this is not the case, CAS will not be able to obtain an OAuth token and the session launch will fail.



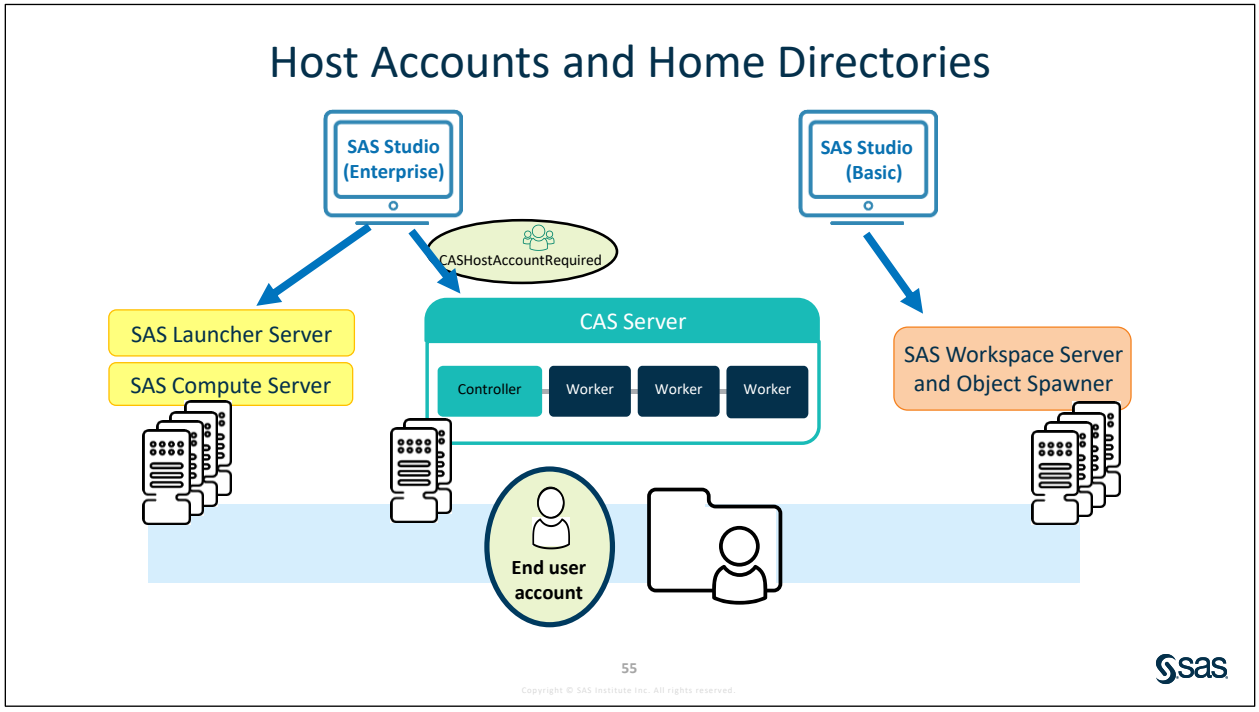
All three components, PAM for CAS (cas), PAM for SAS Studio (Basic) (sasauth-spre*), and SAS Logon Manager, should use the same LDAP provider. If these three components are not sending the username and password entered in SAS Studio (Basic) to the same place, you are likely to see errors when trying to connect. Also, the identities microservice always must connect to an LDAP provider to obtain user and group information.

SAS Studio (Basic)	SAS Studio (Basic) uses host authentication such as Pluggable Authentication Modules (PAM) and Integrated Windows Authentication (IWA) to authenticate users.
SAS Studio (Enterprise)	SAS Studio (Enterprise) authentication fully integrates with the features provided by SAS Logon Manager, and provides more authentication possibilities, such as the following: LDAP provider: standard user name and password form. Kerberos or Integrated Windows Authentication (IWA): single sign-on from the client host to the visual interfaces. Security Assertion Markup Language (SAML) provider: single sign-on from third-party provider.

OAuth and OpenID connect provider: single sign-on from third-party provider.

Pluggable Authentication Modules (PAM): multi-factor authentication via third-party tools.

SAS 9.4: single sign-on from SAS 9.4.



Whenever the process is running under the end user, host accounts and home directories will be needed on the machines where

- the Compute server is installed
- the CAS controller is installed if the CASHostAccountRequired custom group is used
- SAS Workspace Server and Object Spawner are installed.

Note:

When you modify the membership of the CASHostAccountRequired group, this can affect where data resides regarding host directories.

If a user has previously created SASHDAT files and is then added to the CASHostAccountRequired custom group, the user can continue to work with data in memory. However, if certain triggering events occur, such as a CAS server restart, the same user can no longer see the SASHDAT files because the location of these files is different for members of this group. Users in this situation should copy the SASHDAT files from the default location to the host CAS user path.

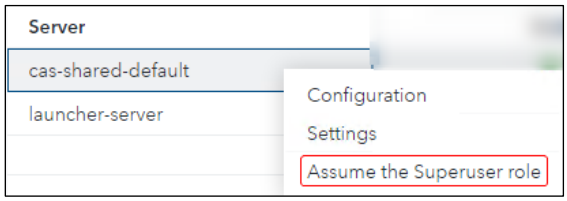
- The original default location is /opt/sas/viya/config/data/cas/default/casuserlibraries/*username* where *username* is the user's host account.
- The host CAS user location is ~/casuser/, where the ~ represents the user's home directory.

Viewing CAS Sessions before Adding a User to the CASHostAccountRequired Custom Group

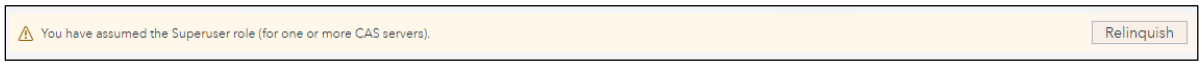
This demonstration illustrates the default behavior in which CAS sessions are run using the **CAS** account when sessions are created through visual interfaces.

1. Open a browser such as Google Chrome, and log in to Environment Manager as Christine.
2. Select **Servers** from the side menu in SAS Environment Manager.
3. Check the current sessions to confirm that there are no sessions owned by Lynn.

   Right-click **cas-shared-default** and click **Assume the Superuser Role**.

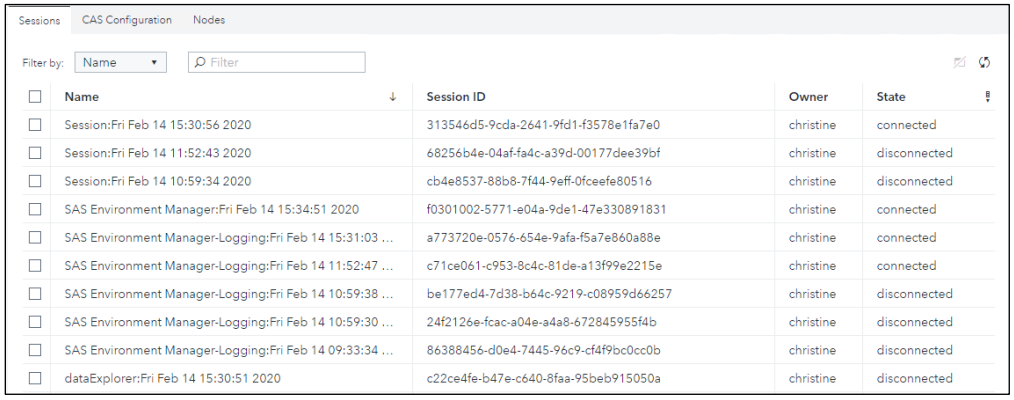


   Notice the message about assuming the Superuser role above the list of servers.

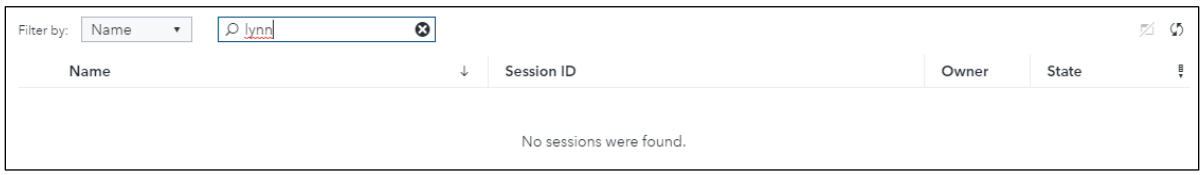


4. Double-click **cas-shared-default** from the servers list to bring up sessions. (You can also right-click and select **Configuration**.)

   There are no sessions owned by Lynn in the list of owners. (It is okay to see some disconnected sessions.)



   You can also filter by owner **lynn** on this screen.



5. In mRemoteNG, enter the following command to check Lynn's sessions:

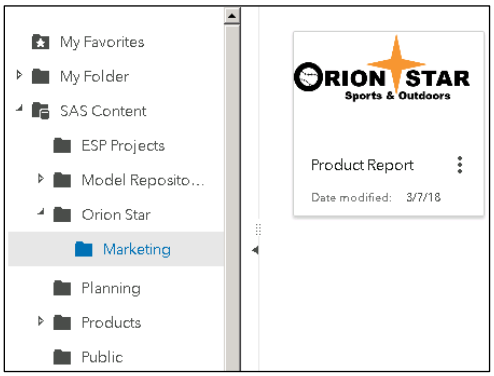
```
/opt/sas/viya/home/bin/sas-admin cas sessions list --owner lynn
--superuser --server cas-shared-default
```

```
[christine@server bin]$ /opt/sas/viya/home/bin/sas-admin cas sessions list --owner lynn --superus
No sessions are available that match the specified filters.
```

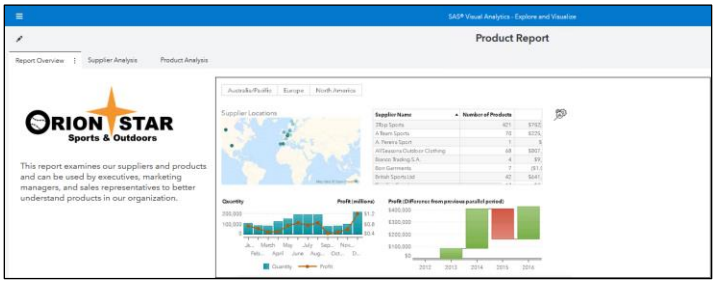
6. In a separate browser, log on to SAS Drive as **lynn** with the password **Student1**.

   If this is the first time logging on as Lynn, you might see the Welcome window. Click **Skip Setup**.

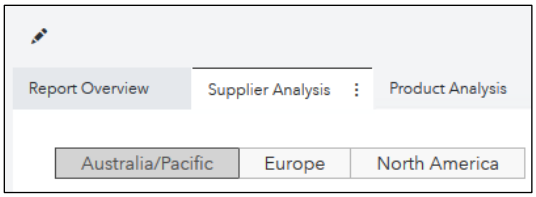
7. Expand **SAS Content** ⇨ **Orion Star** ⇨ **Marketing**.



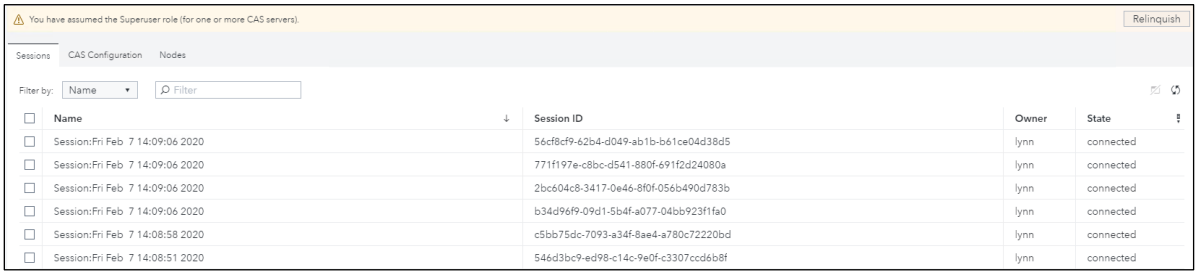
8. Double-click **Product Report** to open it.



9. Click the **Supplier Analysis** tab.



10. Go back to the other browser, running SAS Environment Manager as Christine. Refresh the session list. Notice that Lynn now has CAS sessions.



11. In nRemoteNG, enter the following command to check Lynn's sessions:

```
/opt/sas/viya/home/bin/sas-admin cas sessions list --owner lynn
--superuser --server cas-shared-default
```

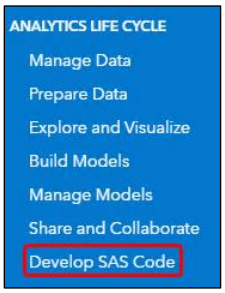
```
[christine@server /]$ /opt/sas/viya/home/bin/sas-admin cas sessions list --owner lynn --superuser --server cas-shared-d
efault
{
    "items": [
        {
            "authenticationType": "OAuth",
            "id": "546d3bc9-ed98-c14c-9e0f-c3307ccd6b8f",
            "name": "  Session:Fri Feb  7 14:08:51 2020",
            "owner": "lynn",
            "state": "Connected",
            "transactionState": ""
        },
        {
            "authenticationType": "OAuth",
            "id": "c5bb75dc-7093-a34f-8ae4-a780c72220bd",
            "name": "  Session:Fri Feb  7 14:08:58 2020",
            "owner": "lynn",
            "state": "Connected",
            "transactionState": ""
        },
```

12. Enter the following command to see whether Lynn is the owner of the CAS processes in the OS:

```
ps -elf |grep session
```

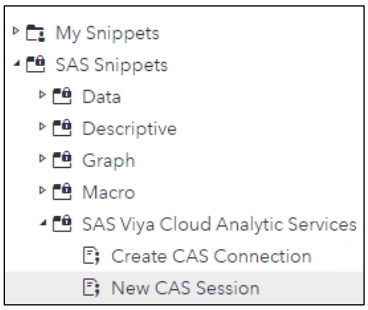
```
[christine@server bin]$ ps -elf |grep session
4 S cas       30291  18203  0  80   0 - 397962 futex_ 06:16 ?       00:00:01 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17675
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       31141  18203  0  80   0 - 255637 futex_ 06:16 ?       00:00:00 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17683
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       31516  18203  0  80   0 - 360478 futex_ 06:16 ?       00:00:02 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17686
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       31608  18203  0  80   0 - 433015 futex_ 06:16 ?       00:00:01 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17688
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       52870  18203  0  80   0 - 247427 futex_ Nov02 ?       00:01:04 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 18 -rc
ntroller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       64843  18203  0  80   0 - 333743 futex_ 06:28 ?       00:00:00 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17964
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       71859  18203  0  80   0 - 246393 futex_ 06:31 ?       00:00:00 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17994
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       71954  18203  2  80   0 - 639259 futex_ 06:31 ?       00:00:15 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17998
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
0 S christi+  95850  44376  0  80   0 - 28177 pipe_w 06:42 pts/0    00:00:00 grep --color=auto session
```

13. Go back to Firefox, where Lynn is still logged in. From the applications menu, select **Develop SAS Code**. This brings up SAS Studio.

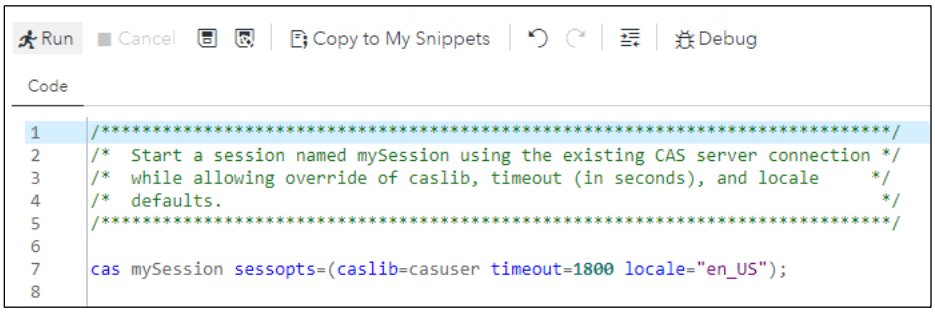


14. Click the **Snippets** icon on the left

15. Expand **SAS Snippets** ⇨ **SAS Viya Cloud Analytic Services**. Double-click **New CAS Session** to bring the code into the Program Editor.

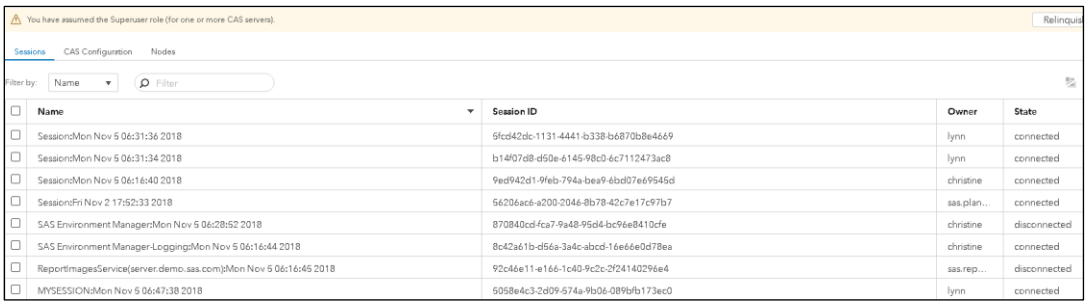


16. Click **Run**  to submit the code.



17. Check the log for errors.

18. Go back to Christine's Environment Manager session and refresh the session list. Lynn has a new session because she is using SAS Studio, a code development environment.



19. In nRemoteNG, enter the following command to check Lynn's sessions:

```
/opt/sas/viya/home/bin/sas-admin cas sessions list --owner lynn
--superuser --server cas-shared-default
```

```
[christine@server bin]$ /opt/sas/viya/home/bin/sas-admin cas sessions list --owner lynn --super
{
    "items": [
        {
            "authenticationType": "OAuth",
            "id": "b7270bbe-ccd8-8648-98a0-c4efde2a8ac2",
            "name": "MYSESSION:Fri Nov  2 11:34:15 2018",
            "owner": "lynn",
            "state": "Connected",
            "transactionState": ""
        }
    ],
    "name": "sessions",
    "version": 2
}
```

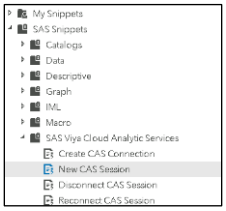
20. Enter the following command to see whether Lynn is the owner of the CAS processes in the OS:

```
ps -elf |grep session
```

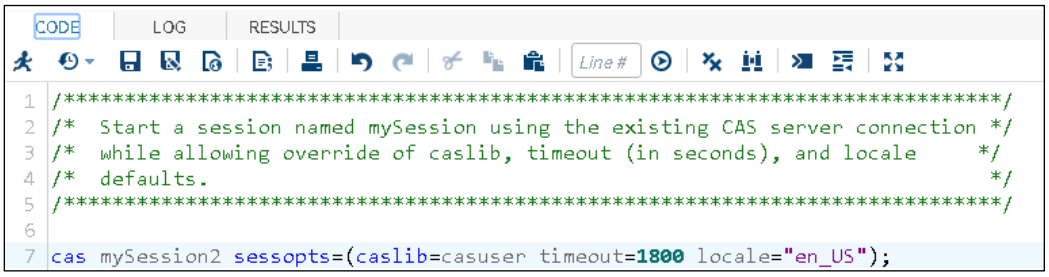
```
[christine@server bin]$ ps -elf |grep session
4 S cas       30291  18203  0  80   0 - 397962 futex_ 06:16 ?       00:00:01 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17675
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       31141  18203  0  80   0 - 255637 futex_ 06:16 ?       00:00:00 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17683
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       31516  18203  0  80   0 - 360478 futex_ 06:16 ?       00:00:02 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17686
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       31608  18203  0  80   0 - 433015 futex_ 06:16 ?       00:00:01 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17688
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       52870  18203  0  80   0 - 247427 futex_ Nov02 ?       00:01:04 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 18 -ro
ntroller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       64843  18203  0  80   0 - 333743 futex_ 06:28 ?       00:00:00 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17964
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       71859  18203  0  80   0 - 246393 futex_ 06:31 ?       00:00:00 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17994
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       71954  18203  2  80   0 - 639259 futex_ 06:31 ?       00:00:15 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session 17998
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
0 S christi+  95850  44376  0  80   0 - 28177 pipe_w 06:42 pts/0    00:00:00 grep --color=auto session
```

There is no process owned by Lynn.

21. Open **SAS Studio (Basic)** in Lynn's browser.
22. Sign in as **lynn** using the password **Student1**.
23. Expand **SAS Snippets** ⇨ **SAS Viya Cloud Analytic Services**. Double-click **New CAS Session** to bring the code into the Program Editor.



24. Change **MySession** to **Mysession2** and click the running person to submit the code.



25. Check the log for errors.

26. In nRemoteNG, enter the following command to check Lynn's sessions:

```
/opt/sas/viya/home/bin/sas-admin cas sessions list --owner lynn
--superuser --server cas-shared-default
```


```
shared-default
{
    "items": [
        {
            "authenticationType": "OAuth",
            "id": "0b221a37-bb14-8c43-afaa-4bf57815e819",
            "name": "dataExplorer:Mon Mar  9 14:44:01 2020",
            "owner": "lynn",
            "state": "Connected",
            "transactionState": ""
        },
        {
            "authenticationType": "OAuth",
            "id": "83f00a72-a7e4-8546-af39-cc2323e5df22",
            "name": "MYSESSION:Mon Mar  9 14:44:45 2020",
            "owner": "lynn",
            "state": "Connected",
            "transactionState": ""
        },
        {
            "authenticationType": "OAuth/External PAM",
            "id": "e86baaa1-c8f0-3a4c-a6e2-bd7716658a53",
            "name": "MYSESSION:Mon Mar  9 14:54:44 2020",
            "owner": "lynn",
            "state": "Connected",
            "transactionState": ""
        },
        {
            "authenticationType": "OAuth/External PAM",
            "id": "02db2884-bf85-d746-889d-37711fc51250",
            "name": "MYSESSION2:Mon Mar  9 14:54:54 2020",
            "owner": "lynn",
            "state": "Connected",
            "transactionState": ""
        },
        {
            "authenticationType": "OAuth",
            "id": "7dea37ca-7219-e541-8419-74ac8e8c5061",
            "name": "SAS Environment Manager:Mon Mar  9 14:44:06 2020",
            "owner": "lynn",
            "state": "Connected",
            "transactionState": ""
        }
    ],
    "name": "sessions",
    "version": 2
}
```

27. Enter the following command to see whether Lynn is the owner of the CAS processes in the OS:

```
ps -elf |grep session
```

```
[christine@server LWSAVI35]$ ps -elf |grep session
4 S cas       38888  34516  0  80   0 - 486682 futex_ 12:55 ?       00:00:02 /opt/sas/viya/home/SASFoundation/u
d 34518 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       40021  34516  0  80   0 - 248435 futex_ 12:56 ?       00:00:02 /opt/sas/viya/home/SASFoundation/u
d 34518 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       40584  34516  0  80   0 - 377974 futex_ 12:56 ?       00:00:02 /opt/sas/viya/home/SASFoundation/u
d 34518 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       51527  34516  0  80   0 - 316958 futex_ 14:44 ?       00:00:00 /opt/sas/viya/home/SASFoundation/u
d 34518 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       51859  34516  0  80   0 - 241965 futex_ 14:44 ?       00:00:00 /opt/sas/viya/home/SASFoundation/u
d 34518 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       54165  34516  0  80   0 - 238000 futex_ 14:44 ?       00:00:00 /opt/sas/viya/home/SASFoundation/u
d 34518 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       57498  34516  0  80   0 - 245743 futex_ 14:46 ?       00:00:00 /opt/sas/viya/home/SASFoundation/u
d 34518 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S lynn      80270  34516  0  80   0 - 237492 futex_ 14:54 ?       00:00:00 /opt/sas/viya/home/SASFoundation/u
d 34518 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S lynn      80424  34516  0  80   0 - 237493 futex_ 14:54 ?       00:00:00 /opt/sas/viya/home/SASFoundation/u
d 34518 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
0 S christi+  84719  49842  0  80   0 - 28179 pipe_w 14:56 pts/0    00:00:00 grep --color=auto session
```

When using SAS Studio (Basic), the CAS controller starts the process as lynn.

Note: To use SAS Studio (Basic), a user must have a host account and Home directory wherever the CAS controller is running.

In the practices, you will create the **CASHostAccountRequired** custom group. Members of this group automatically run their CAS sessions under their own host account.

End of Demonstration

Practice

10. Creating a CASHostAccountRequired Custom Group

By default, CAS sessions use the **CAS** account when using visual interfaces, such as SAS Visual Analytics. Files generated in such a session are saved in a folder belonging to the **CAS** account, but in a directory path that includes the user's ID.

By default, CAS sessions are run by the individual user when using a programming interface, such as SAS Studio (Basic). Files generated in such a session are saved in the user's Home directory.

If you prefer users to launch CAS sessions under their own accounts to cause their files to be saved to their UNIX directories, create and populate a custom group with the ID **CASHostAccountRequired**. When members of the **CASHostAccountRequired** group launch a CAS session, that session runs under that user's host account, and the generated files are created in the user's Home directory. Members of this group ***must*** have host accounts.

In this practice, you create the **CASHostAccountRequired** custom group.

a. The users of the Marketing group need to be verified as existing on the server with a Home directory. Use the CLI or SAS Environment Manager to see who is in the Marketing group.

SAS Environment Manager

Select **Users** from the side menu ⇨ **Groups** from the drop-down menu ⇨ highlight **Marketing**.

CLI

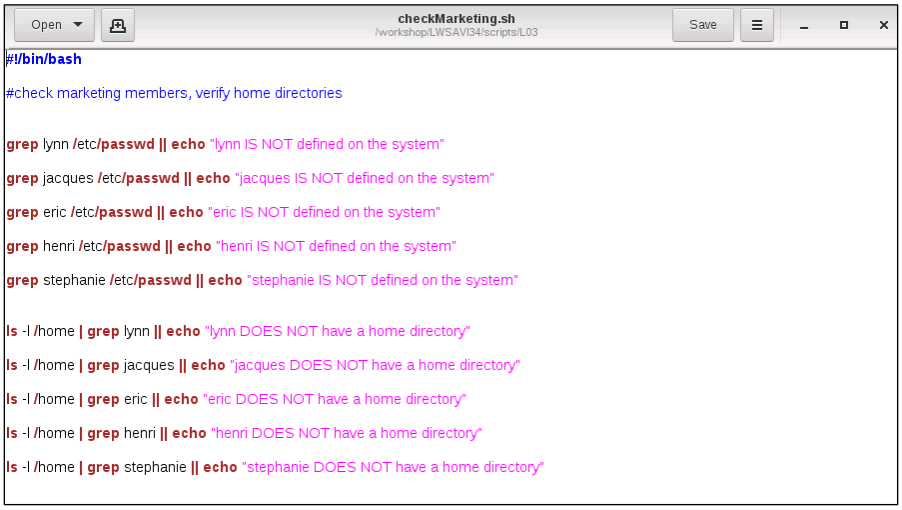
Use **christine**'s connection in mRemoteNg and run the following command:

```
/opt/sas/viya/home/bin/sas-admin identities list-members --
group-id Marketing
```

b. Run the following script to verify that Marketing group members have host accounts and home directories:

```
/workshop/LWSAVA35/checkMarketing.sh
```

Contents of **checkMarketing.sh**

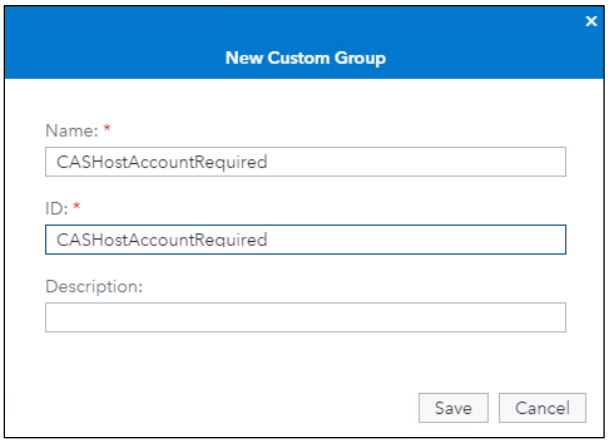


c. In SAS Environment Manager, select **Users** from the side menu. Select **Custom groups** from the **View** drop-down list.

   (If not already logged on, sign into SAS Environment Manager as **christine** with the password **Student1**. Opt in to the **SASAdministrators** assumable group.)

d. Select **New custom group**.

e. Enter **CASHostAccountRequired** in the **Name** and **ID** fields. Add a description if you want. Click **Save**.



f. Verify that the **Members (0)** tab is active. Click the **Edit** icon to the right.

g. Select the **Marketing** group and click the right arrow to move the group from the **Available** list box to the **Selected** list box. (You will need to change the **Filter by** value to **Groups**.)

h. Click **OK** to save the changes. You should see the members of the Marketing group under members section in the **CASHostAccountRequired** custom group.

11. Viewing CAS Sessions after CASHostAccountRequired Custom Group Is Created

a. Select the **Servers** area.

b. Check the current sessions to confirm that there are no sessions owned by Lynn.

   1) Right-click **cas-shared-default** and select **Assume the Superuser Role**.

      Notice the message about assuming the Superuser role above the list of servers.

   2) Double-click **cas-shared-default** from the servers list to bring up sessions. (You can also right-click and select **Configuration**.)

      There should not be any sessions owned by Lynn in the list of owners. (It is okay to see some disconnected sessions.)

      You can also filter by owner **lynn** on this screen.

c. In mRemoteNG, enter the following command to check Lynn's sessions:

```
/opt/sas/viya/home/bin/sas-admin cas sessions list --owner
lynn --superuser --server cas-shared-default
```

d. In a Firefox browser, log on to SAS Drive as **lynn** with the password **Student1**.

   If this is the first time logging on as Lynn, you might see the Welcome window. Click **Skip Setup**.

e. Open a report from SAS Drive.

1) Expand **SAS Content** ⇨ **Orion Star** ⇨ **Marketing**.
2) Double-click **Product Report** to open it.
3) Click the **Supplier Analysis** tab.

f. Go back to SAS Environment Manager and refresh the Sessions list from the toolbar in the upper right. Lynn now has CAS sessions.

g. In nRemoteNG, enter the following command to check Lynn's sessions:

```
/opt/sas/viya/home/bin/sas-admin cas sessions list --owner
lynn --superuser --server cas-shared-default
```

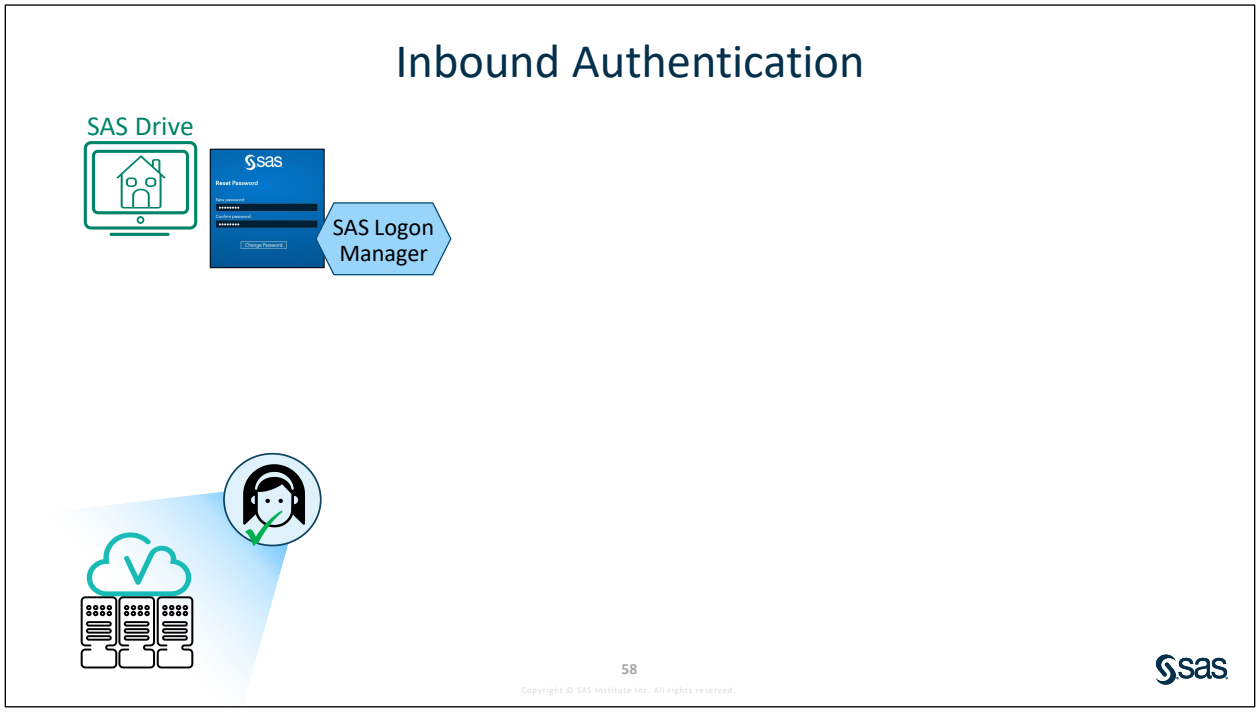
h. Enter the following command to see whether Lynn is the owner of the CAS processes on the host machine:

```
ps -elf | grep session
```

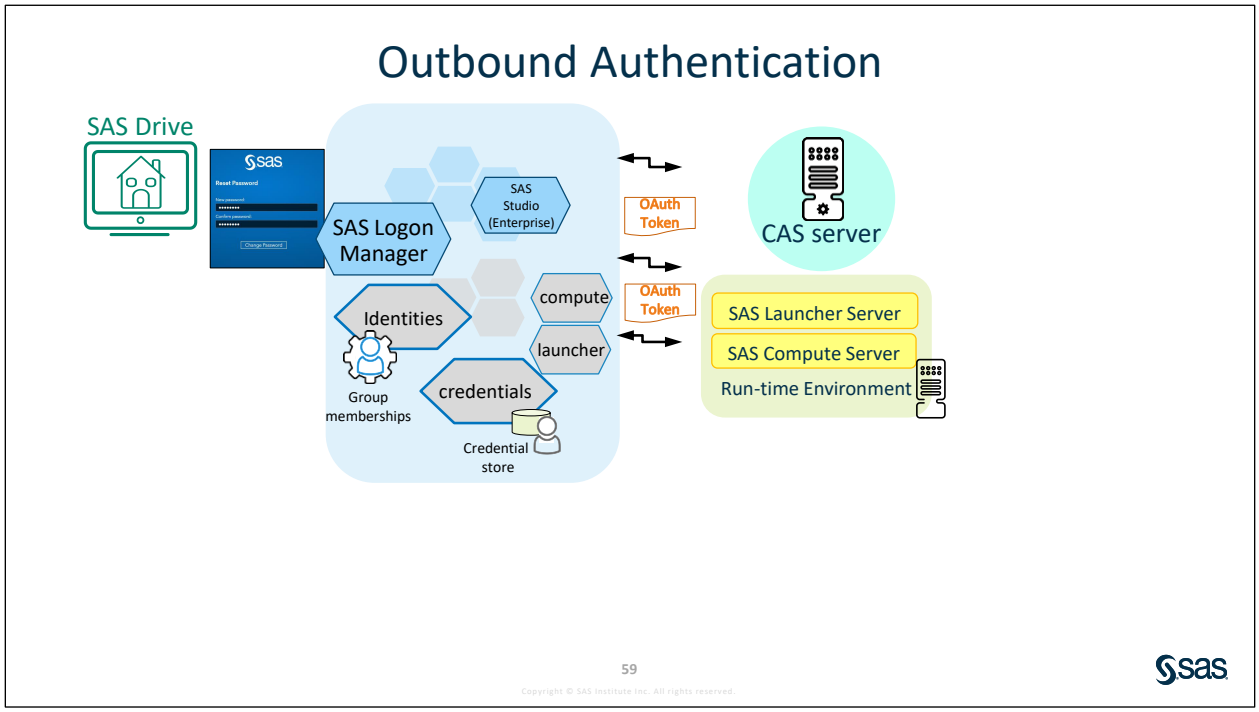
Because Lynn is in the **CASHostAccountRequired** custom group, her CAS session process is run by her ID instead of the CAS user in the operating system.

End of Practices

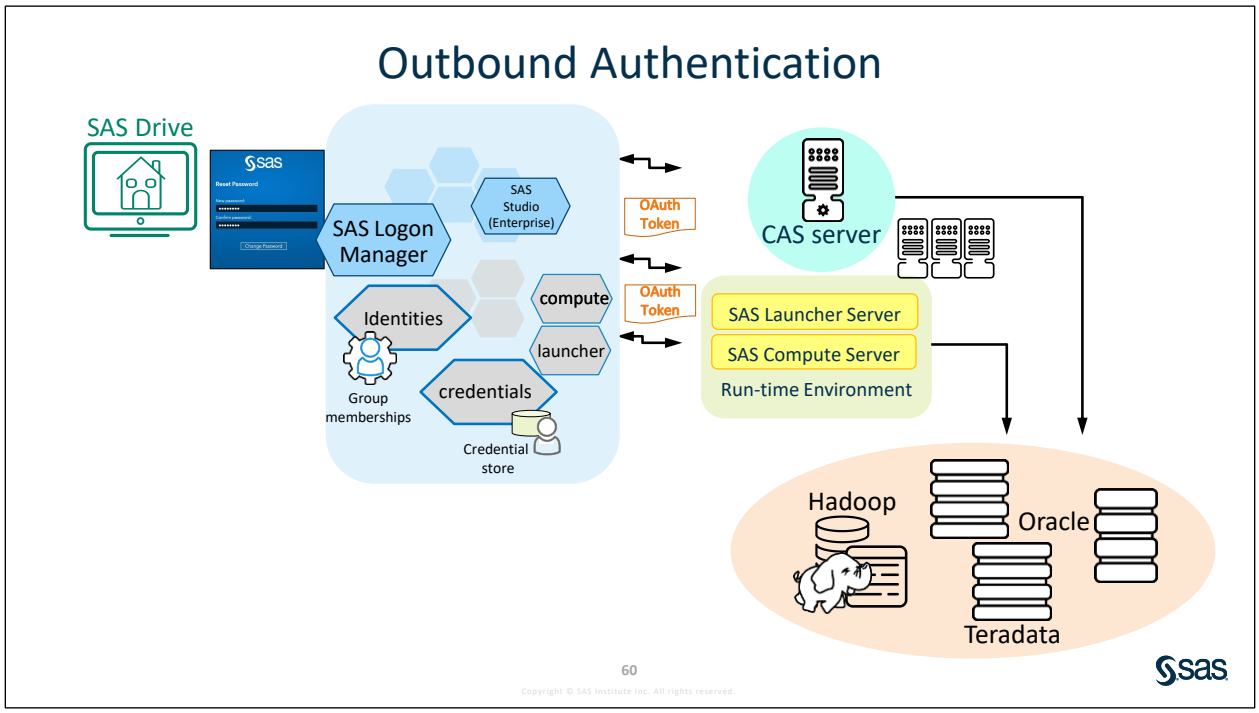
3.6 Managing External Credentials



Inbound authentication is the initial authentication to the environment.

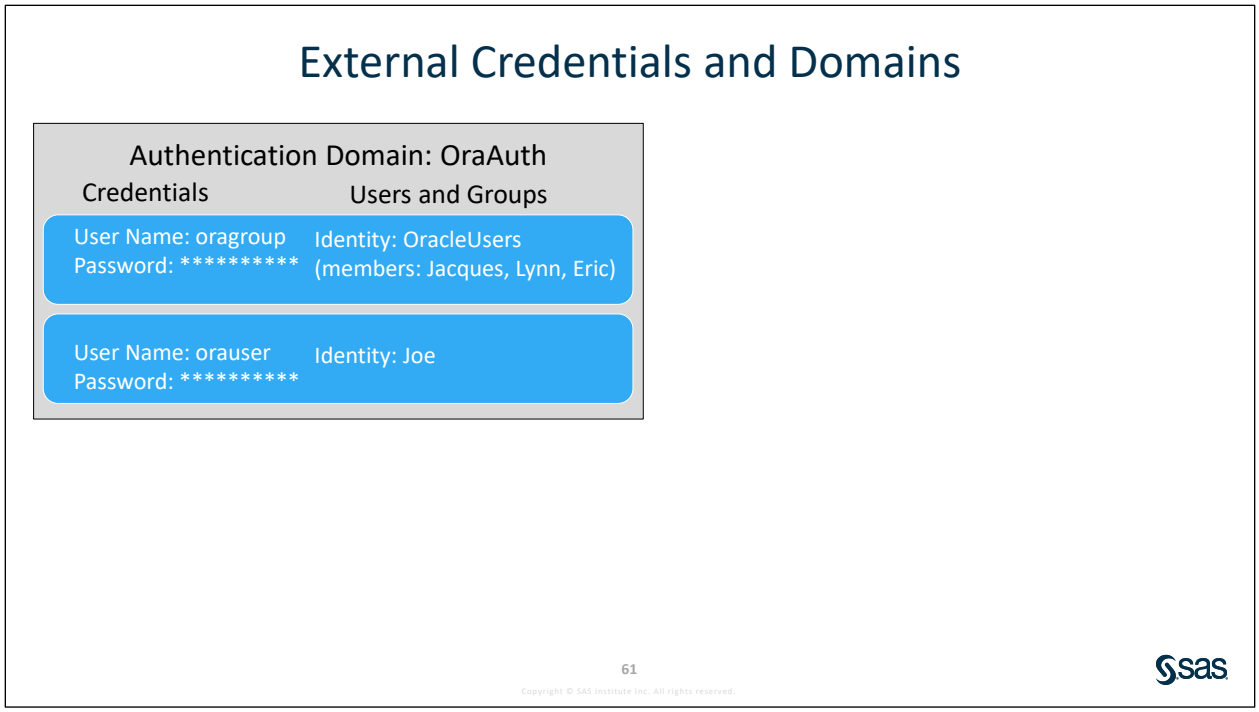


Outbound authentication refers to the authentication of the SAS process to a downstream process. The inbound authentication provides an internal OAuth token with group membership information in the OAuth token. Underneath the covers, outbound authentication is occurring to CAS and the SAS Compute Server through the launcher service seamlessly.



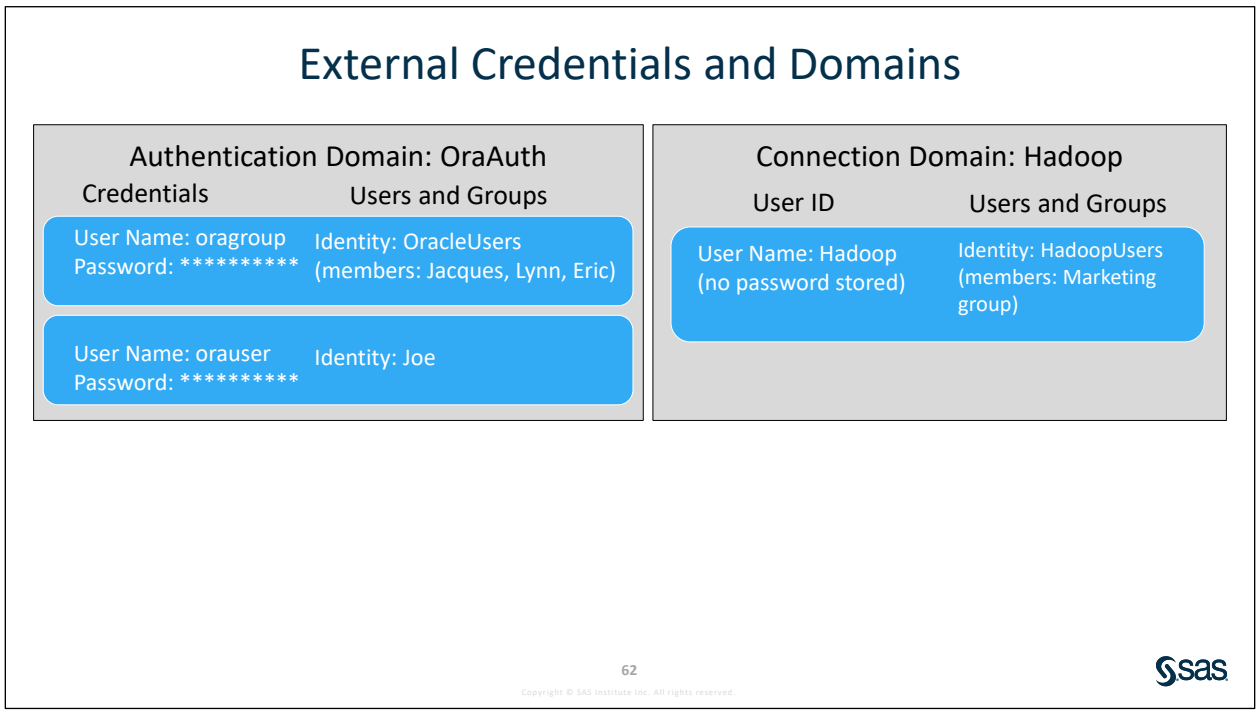
Users on SAS Viya systems might need different credentials for accessing secured Hadoop environments or third-party database servers than what they use for authenticating to SAS Viya.

SAS Viya must be able to use those credentials in order to access data sources seamlessly.

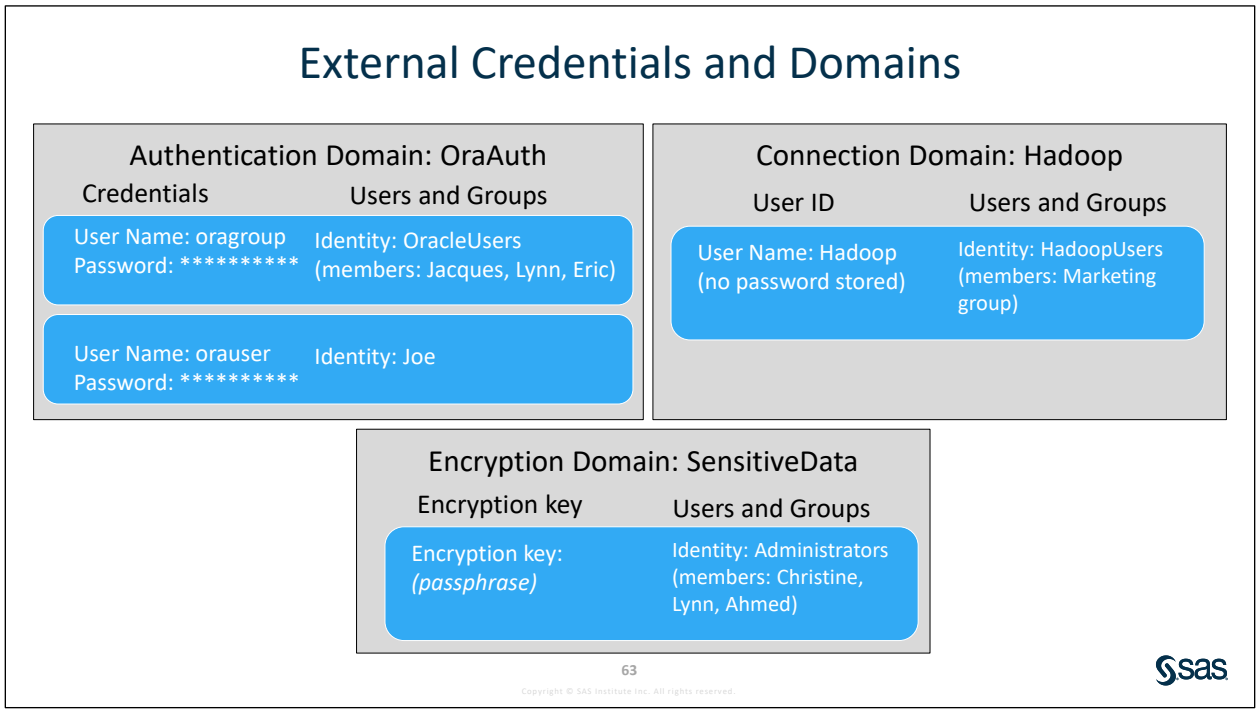


Domains are used to store both the credentials and the identities that are allowed to use them to access an external data source. There are three domain types.

An authentication domain makes a set of credentials available to a set of users so that SAS Viya can seamlessly access an external source, such as an Oracle database. You store both the credentials required to access external data sources and the identities that are allowed to use those credentials in a domain. A user can access the credentials either directly with their user ID or indirectly as a member of a group that is defined as an identity.



A connection domain is used when the external source has been set up to require a user ID but no password. For example, a third-party database like Hadoop might be configured with accounts for authentication that do not require a password.



An encryption domain is used to store an encryption key that is required to read data at rest in a path assigned to a caslib. The identities assigned to this encryption domain have access to the key. When you create a path-based caslib, you can choose to enable encryption. Then you select an encryption domain to assign an encryption key. Tables imported to this caslib are now encrypted. (If the path contains preexisting tables, those tables are not encrypted.)

Creating an authentication domain leverages the Credentials microservice. The Credentials microservice uses the SAS Infrastructure Data Server (PostgreSQL) as the backing store. The Credentials microservice uses AES-GCM encryption with a random key (per deployment key). The password and salt used as inputs to the AES-GCM key are stored in the SAS Configuration Server key or value store. If, at the start-up of the Credentials microservice, those keys or values do not exist, they are generated randomly. The authorization rules that are defined in SAS Environment Manager control who can access the credentials that are stored by the Credentials microservice.

Practice

12. Modifying External Credentials in SAS Environment Manager

Users can manage their external credential information in SAS Environment Manager. The **My Credentials** page allows them to add, remove, and change these credentials used to access external resources.

a. Sign in to SAS Environment Manager as **Christine** with the password **Student1**.

b. From the side menu, select the **My Credentials** page.

c. View the Credential Properties of sasworkshop, the account used by christine to connect to the EsriAuth Domain.

d. After reviewing the Credential Properties, close the page.

e. Edit the stored Credential information for **sasworkshop** to store the password **Student2** so that christine can connect to the EsriAuth Domain.

f. Save your changes.

Note: The **My Credentials** page and the SAS Logon Manager screen cannot change the password used to authenticate to SAS Viya. Those credentials are managed and verified at the Authentication Provider level, which is typically LDAP.

End of Practices

3.7 Solutions

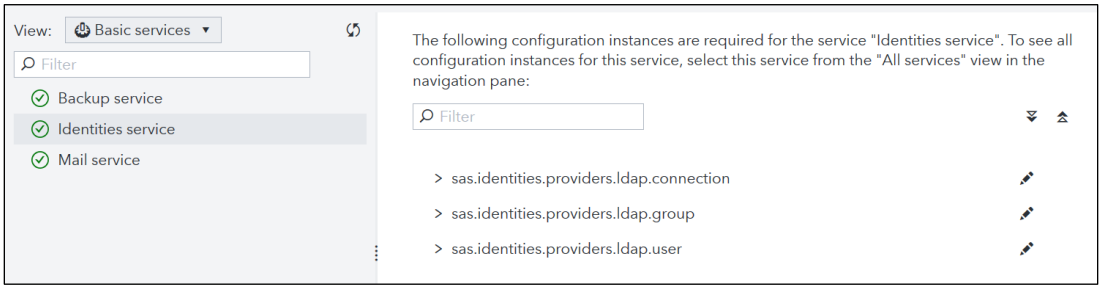
Solutions to Practices

1. Inspecting the Identities Service

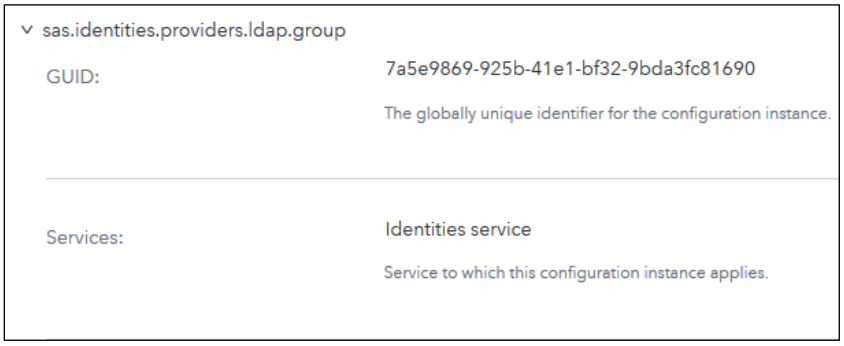
The basic properties of the Identities service were examined in the demo. Additional properties are available for the Identities service by viewing **All services** in the Configuration application.

a. Sign in to SAS Environment Manager as **christine** with the password **Student1**. Opt in to the **SASAdministrators** assumable group.

b. Select **Configuration** from the side menu. Select the **Identities service**. Collapse all the configuration instances.

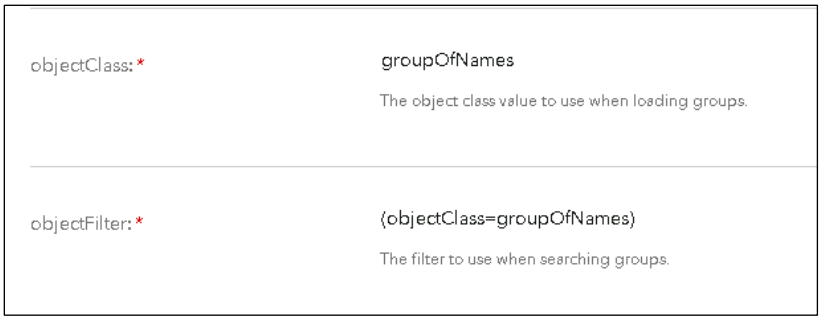


c. Expand the **sas.identities.providers.ldap.group** configuration instance.



Is there a filter configured on groups being brought into the SAS Viya cache?

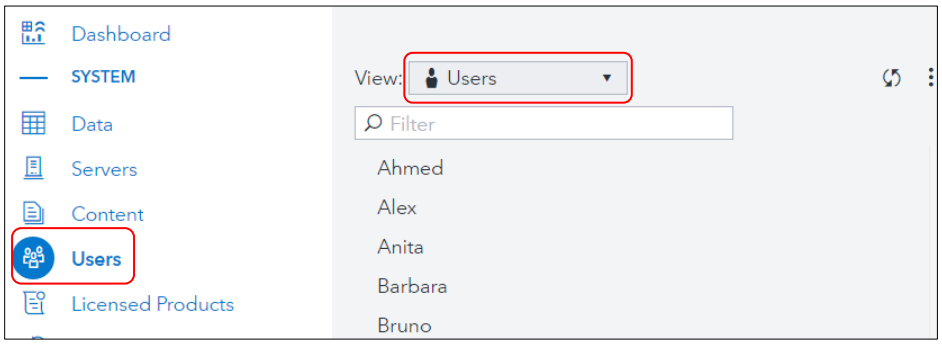
No



2. Comparing the Imported Identities with the LDAP Server

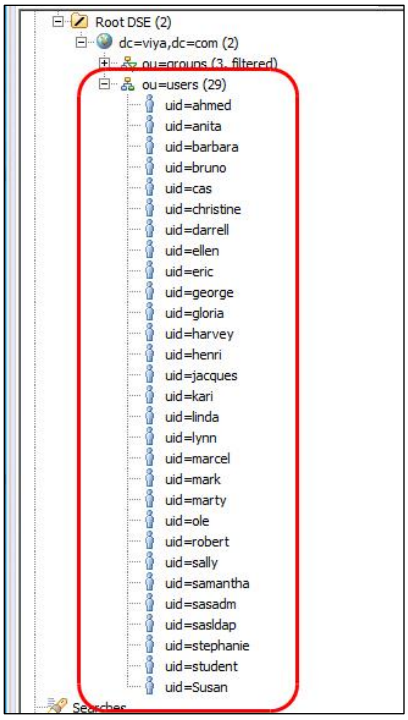
The identities were imported from the local OpenLDAP server. This practice uses SAS Environment and Apache Directory Studio to compare the two lists of identities.

a. On the SAS Environment Manager side menu, select **Users**. Select **Users** from the **View** drop-down list.



b. From the Windows Start menu, launch the **Apache Directory Studio** application.

c. Double-click the **Admin** connection on the Connections tile to connect to the OpenLDAP server. Expand the directory tree until all 29 users are visible.



d. Are the two lists the same? **Yes** Is there a user who is named **abbott** in either list? **No**

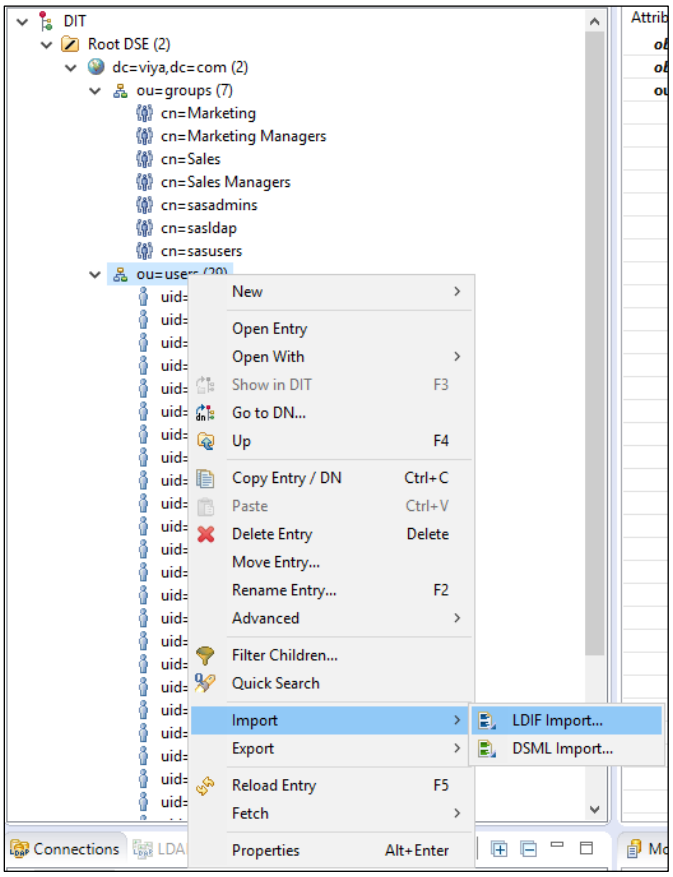
3. **Adding a User to the LDAP Server and Refreshing the Identity Cache**

The identity cache is not updated when changes are made to the content in the identity provider. The content is updated at the next scheduled refresh. (The default is every 12 hours.) It can also be updated by the following:

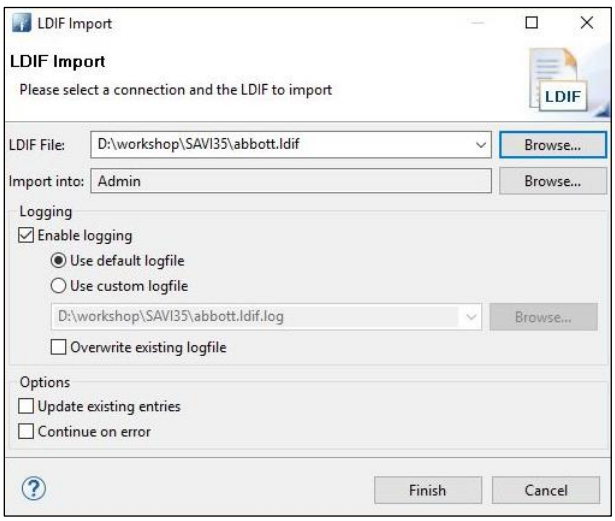
- using the Reload Identities option on the Users page of SAS Environment Manager
- CLI Identities plug-in refresh-cache option
- restarting the Identities service

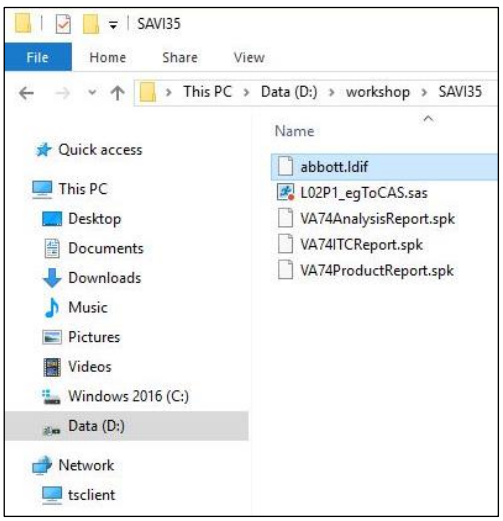
In this practice, a new user is added to the OpenLDAP server using Apache Directory Studio. Identities are reloaded, and the identities are checked in SAS Environment Manager to confirm the import of the new user.

a. Right-click the **ou=users** tree in Apache Directory Studio. Select **Import** ⇨ **LDIF Import**.

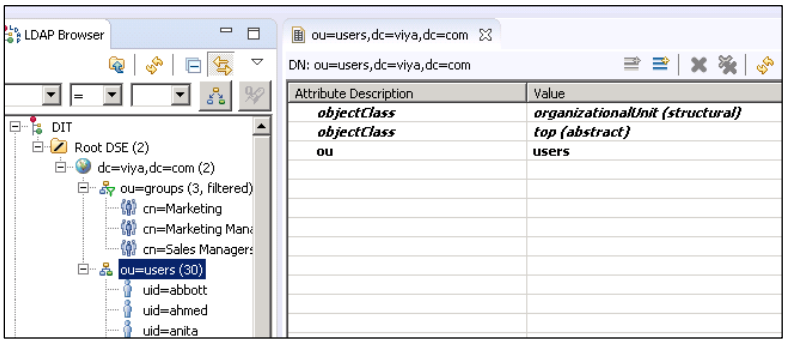


b. Use the navigation window to go to **D:\Workshop\SAVI35\abbott.ldif**. Click **Open**. Click **Finish** in the LDIF Import window to import the LDIF file.

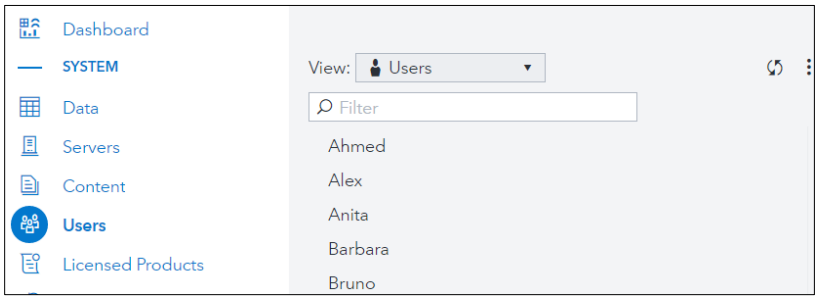




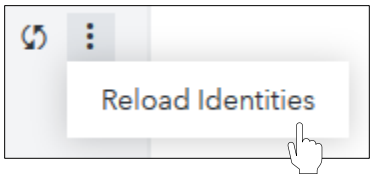
c. Examine the list of users under the **ou=users** tree. Verify that the user **abbott** was added to the OpenLDAP server.



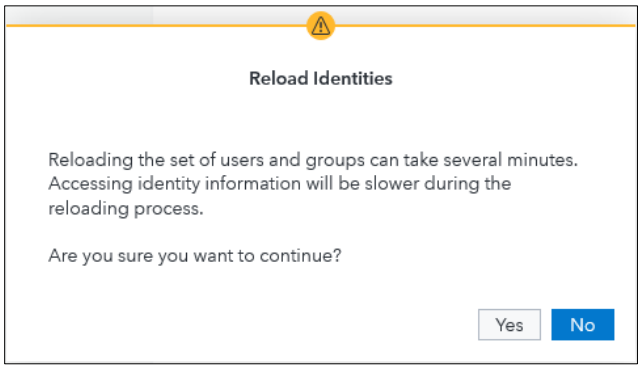
d. Select **Users** from the side menu in SAS Environment Manager and verify that **abbott** is not listed.



e. Click the **More Options** icon  to the right of **View** drop-down menu and select **Reload Identities**.



f. Take note of the warning. Click **Yes**.



Note: You can also refresh the cache to retrieve new users and groups:

- Use CLI: sas-admin identities refresh-cache
- Restart the identity service: service sas-viya-identities-default restart

```
sudo systemctl restart sas-viya-identities-default
```

g. Click **Refresh** . Abbott is now able to use the SAS Viya system.

4. Using the CLI to List the Users

a. As **christine** in an mRemoteNG session, enter the command shown below.

```
/opt/sas/viya/home/bin/sas-admin --output text identities list-users
```

Note: You might need to run **/opt/sas/viya/home/bin/sas-admin auth login** if your token expired.

```
[christine@server bin]$ ./sas-admin --output text identities list-users
Id          Name        Description   State
Susan       Susan       <nil>         active
abbott      Abbott      <nil>         active
ahmed       Ahmed       <nil>         active
anita       Anita       <nil>         active
barbara     Barbara     <nil>         active
bruno       Bruno       <nil>         active
cas         cas         <nil>         active
christine   Christine   <nil>         active
darrell     Darrell     <nil>         active
```

b. Is this the same list as in SAS Environment Manager? **Yes**

5. Examining the Behavior of SAS Viya when the Logon Service Is Not Running

This practice determines the status of the logon service. You stop the service, and the symptom of it being stopped is demonstrated. You must restart the service and verify that it is working.

a. Sign out of all SAS Environment Manager and SAS Studio sessions. Close the Chrome and Firefox browser windows.

b. Open **mRemoteNG** and the **christine** connection.

c. At the Linux command prompt, enter the command below to determine the status of the logon service.

```
sudo systemctl status sas-viya-saslogon-default
```

Note: You do not need root privileges to access the status of a service. It ***is*** required as shown below in the **stop** and **start** actions. Christine uses sudo to act like root to execute the service command to perform the stop and start. The root ID could also be used.

```
[christine@server bin]$ sudo systemctl status sas-viya-saslogon-default
● sas-viya-saslogon-default.service - LSB: start and stop sas-saslogon service
   Loaded: loaded (/etc/rc.d/init.d/sas-viya-saslogon-default; bad; vendor preset: disabled)
   Active: active (running) since Thu 2020-01-30 10:07:27 EST; 42min ago
```

d. Enter the command to stop the logon service.

```
sudo systemctl stop sas-viya-saslogon-default
```

```
[christine@server bin]$ sudo systemctl stop sas-viya-saslogon-default
[christine@server bin]$ sudo systemctl status sas-viya-saslogon-default
● sas-viya-saslogon-default.service - LSB: start and stop sas-saslogon service
   Loaded: loaded (/etc/rc.d/init.d/sas-viya-saslogon-default; bad; vendor preset: disabled)
   Active: inactive (dead)
```

e. Click the **Chrome** icon on the taskbar. Try to access SAS Drive or SAS Environment Manager. Was it successful?

f. Close the Chrome browser window.

g. At the Linux command prompt, enter the command below to start the logon service.

```
sudo systemctl start sas-viya-saslogon-default
```

```
[christine@server bin]$ sudo systemctl start sas-viya-saslogon-default
[christine@server bin]$ sudo systemctl status sas-viya-saslogon-default
● sas-viya-saslogon-default.service - LSB: start and stop sas-saslogon service
   Loaded: loaded (/etc/rc.d/init.d/sas-viya-saslogon-default; bad; vendor preset: disabled)
   Active: active (running) since Thu 2020-01-30 10:52:59 EST; 1s ago
```

h. Wait for the service to start and sign in again. Was it successful?

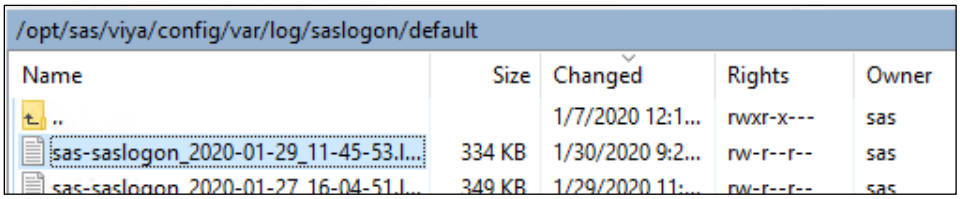
Note: It might take some time before you can successfully sign in to SAS Home.

6. Resetting the Password for sasboot

This practice demonstrates how the sasboot ID's password is reset. This is necessary when logon or other authentication and authorization issues occur.

a. Double-click the **WinSCP** shortcut on the Windows desktop. Verify that the **root@server** connection is selected. Click the **Login** button.

b. On the right side of the WinSCP window, navigate to **/var/log/sas/viya/saslogon/default**.

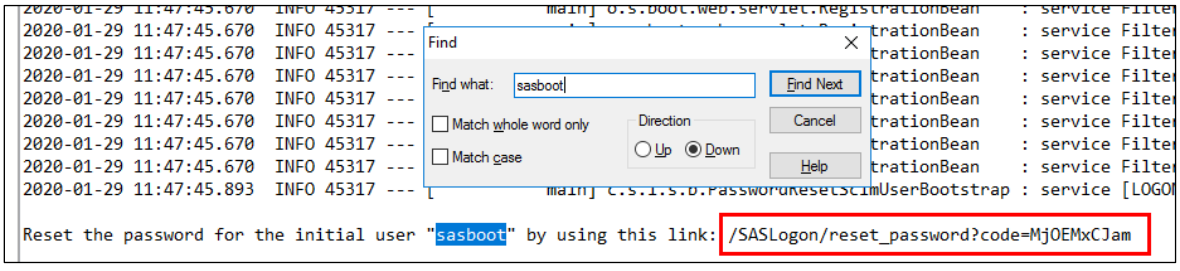


Note: **/var/log/sas/viya** is a link that resolves to **/opt/sas/viya/config/var/log**

c. Look at the timestamps in the file names. The most recent log file should be at the bottom. If it is not, select the **Changed** column to sort the files based on their previous updates.

d. Double-click the most recent log file to open it in an editor.

Click the Ctrl key and the F key simultaneously to begin a search. Enter **sasboot** to find the link that is needed to reset the password. Use this link to construct a complete URL.

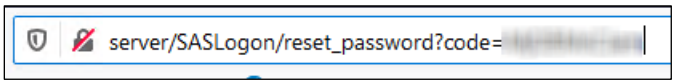


Alternatively, use the root session in mRemoteNg and use the **grep** command to search on **sasboot**:

```
grep 'sasboot' /var/log/sas/viya/saslogon/default/sas-saslogon_date-and-time-stamp.log
```

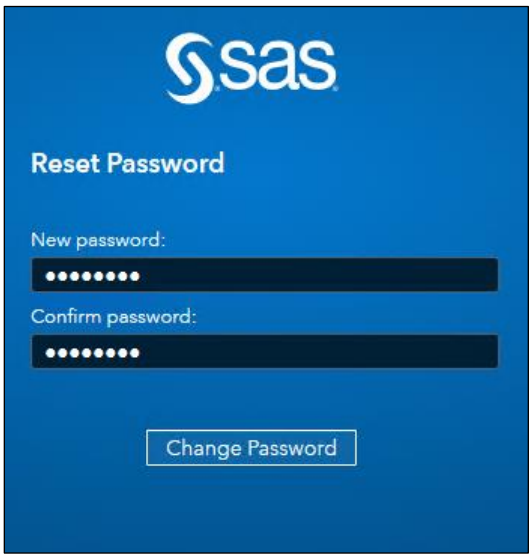
e. Open a new browser window. Use **http://server** and the link in the log to create a valid URL to sign in and reset the sasboot password:

http://server/SASLogon/reset_password?code=<*code_from_log_file*>



Note: The SASLogon address is case sensitive.

f. Change the password to **Student2**. Confirm the new password and then click **Change Password**.



g. Log on to SAS Environment Manager as **sasboot** with the new password of **Student2**. Opt in to the **SASAdministrators** assumable group.

Note: If the URL has expired, it can be refreshed by restarting the SASLogon service:

```
sudo systemctl restart sas-viya-saslogon-default
```

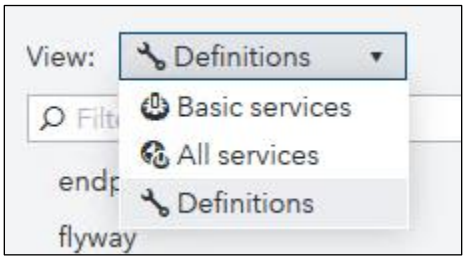
Then go to the log and obtain the new URL. The URL expires 24 hours after the SASLogon service restarts. For security purposes, the URL that is specified in a browser or in a text editor also expires, even if the password is not reset. After you reset the password, SAS Environment Manager automatically opens in your browser. Opt in to all of the assumable groups so that you have the permissions to perform subsequent tasks.

(Optional) For additional security, you can then disable the password reset feature. This prevents password reset links from being written to the log each time the SASLogon service is started.

Make sure you document the password!

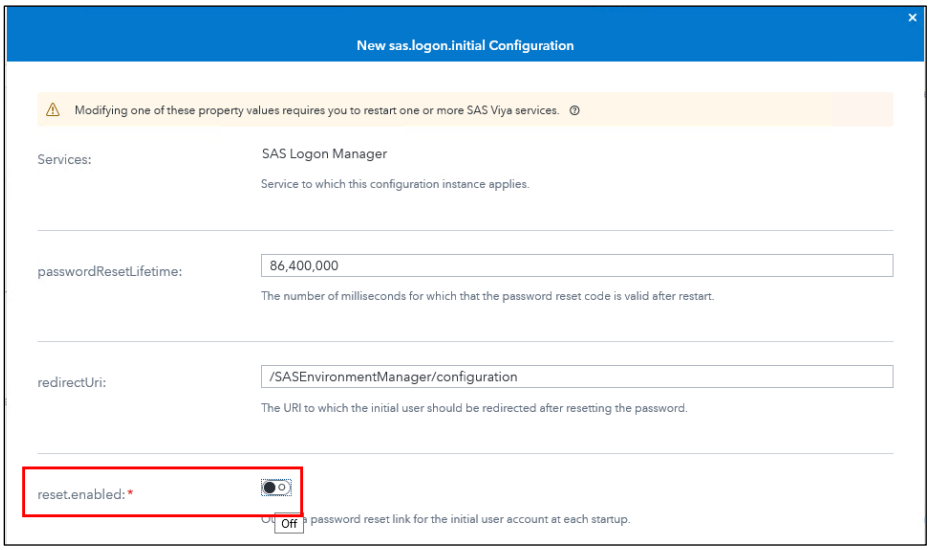
h. Select **Configuration** from the side menu.

i. Select **Definitions** from the drop-down list.



j. In the left pane, select **sas.logon.initial**. Then click **New Configuration** at the top of the right pane.

k. Set **reset.enabled** to **off**.



l. Click **Save**.

m. Restart the SASLogon service.

```
sudo systemctl restart sas-viya-saslogon-default
```

n. Sign out of the sasboot session.

7. Using the CLI to Create a New Custom Group and Adding Users to the Group

a. As **christine** in an mRemoteNG session, enter the commands below to create the Finance group.

```
cd /opt/sas/viya/home/bin
./sas-admin identities create-group --name Finance --id Finance
```

```
[christine@server bin]$ ./sas-admin identities create-group --name Finance --id Finance
{
    "description": "",
    "id": "Finance",
    "name": "Finance",
    "state": "active"
}
The group was created successfully.
```

Note: If your token expired, you might need to run the following command:

```
/opt/sas/viya/home/bin/sas-admin auth login
```

b. To add Lynn, Kari, and Marty to the newly created Finance group and verify their membership in the Finance group, run the following command:

```
/opt/sas/viya/home/bin/sas-admin identities add-member --
group-id Finance --user-member-id Lynn
```

```
/opt/sas/viya/home/bin/sas-admin identities add-member --
group-id Finance --user-member-id Kari
```

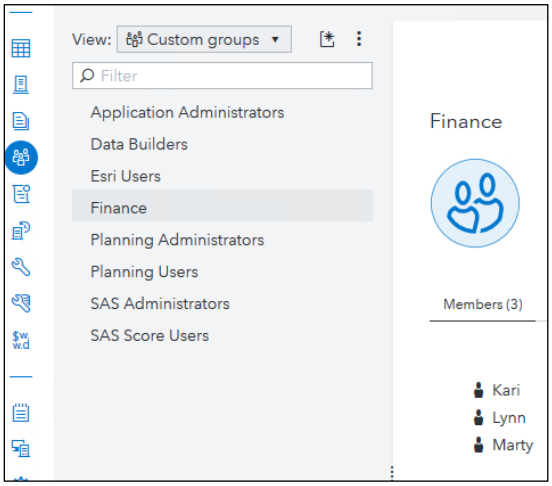
```
/opt/sas/viya/home/bin/sas-admin identities add-member --
group-id Finance --user-member-id Marty
```

```
[christine@server bin]$ /opt/sas/viya/h
{
    "description": "",
    "id": "Finance",
    "name": "Finance",
    "state": "active"
}
The group was created successfully.
[christine@server bin]$ /opt/sas/viya/h
Lynn has been added to group Finance
[christine@server bin]$ /opt/sas/viya/h
Kari has been added to group Finance
[christine@server bin]$ /opt/sas/viya/h
y
Marty has been added to group Finance
```

```
/opt/sas/viya/home/bin/sas-admin identities list-members --
group-id Finance
```

```
[christine@server bin]$ /opt/sas/viya/home/bin/sas-admin identities list-
members --group-id Finance
{
    "items": [
        {
            "id": "kari",
            "name": "Kari",
            "type": "user"
        },
        {
            "id": "lynn",
            "name": "Lynn",
            "type": "user"
        },
        {
            "id": "marty",
            "name": "Marty",
            "type": "user"
        }
    ]
```

c. Log on to SAS Environment Manager as **christine** with the password **Student1** to verify that the custom group was added, along with the three users.



Note: There is a CLI script to add access controls on Finance caslib:

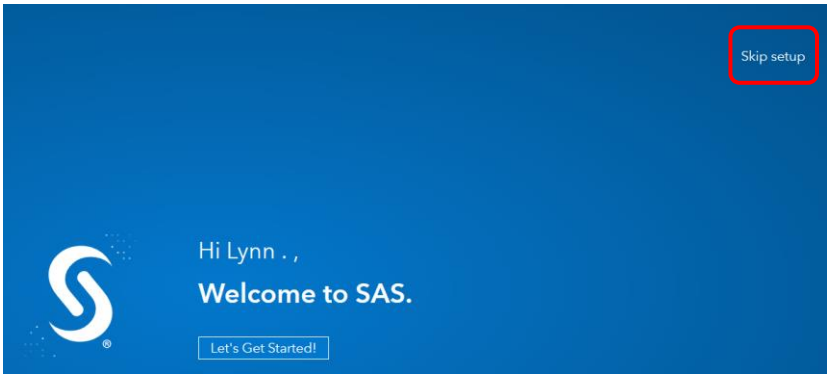
```
/workshop/LWSAVI35/scripts/L04/practice07_addFinanceGroup.sh
```

8. Adding a User to the CAS Superuser Role

In this practice, you add Lynn to the Superuser role. The membership is validated after she is added.

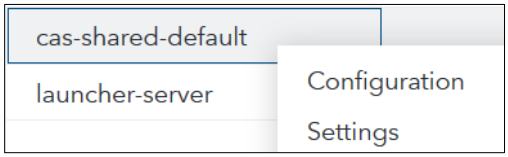
a. Sign in to SAS Environment Manager as **lynn** with the password **Student1**. (Lynn has no assumable groups. Specifically, she is not in the SAS Administrator group.)

If this is your first time in the class logging in as **lynn**, a welcome message will appear. Select **Skip setup**.

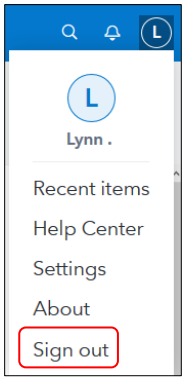


b. Can Lynn see all the actions from the side menu that Christine can see, when Christine assumes her membership to the SAS Administrator group? **No**. **But she does see the same actions that Christine sees when she does not assume her membership to the SAS Administrator group.**

c. Select **Servers** ⇨ right-click **cas-shared-default** ⇨ **Settings**. Lynn cannot assume the Superuser role.



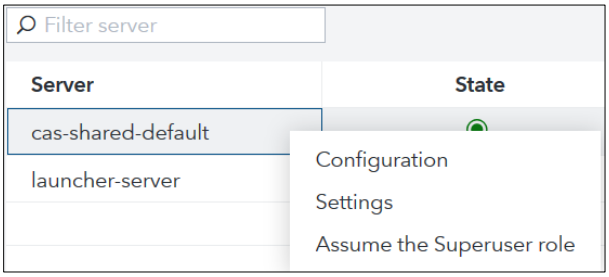
d. Click **Lynn** and select **Sign Out**.



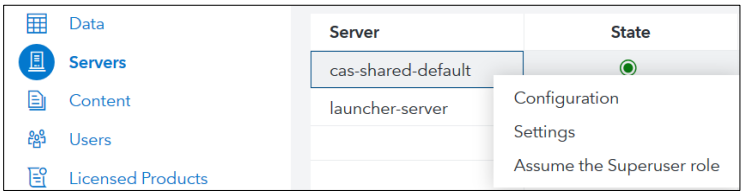
e. Sign back on as **christine** with the password **Student1** and opt in to assumable groups.

f. Add Lynn to the Superuser role.

1) Select **Servers** ⇨ right-click **cas-shared-default** ⇨ **Assume the Superuser role**.

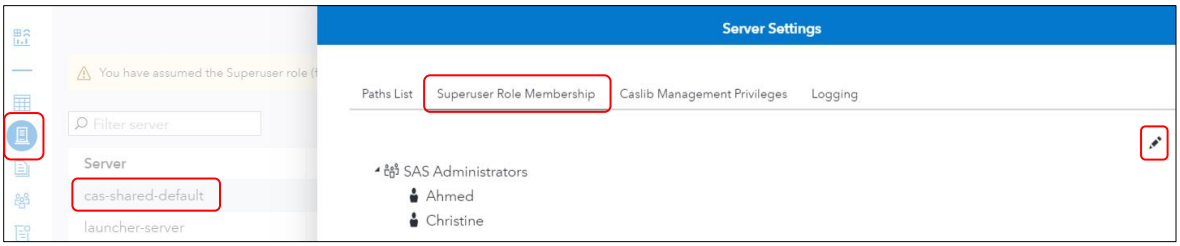


2) Right-click **cas-shared-default** ⇨ **Settings**.

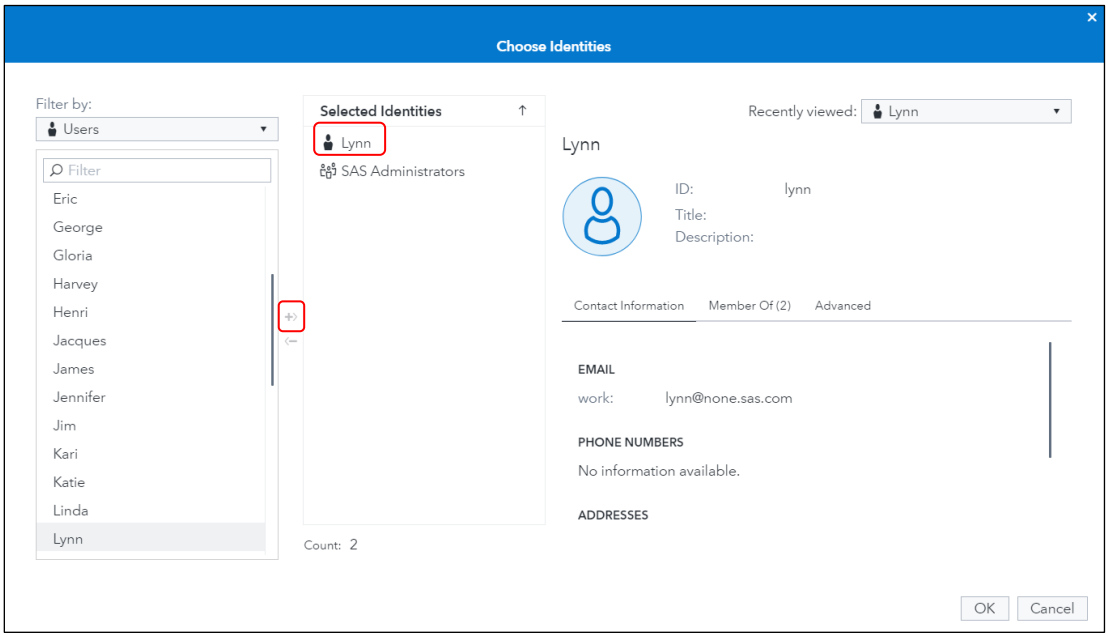


3) Click **Superuser Role Membership**.

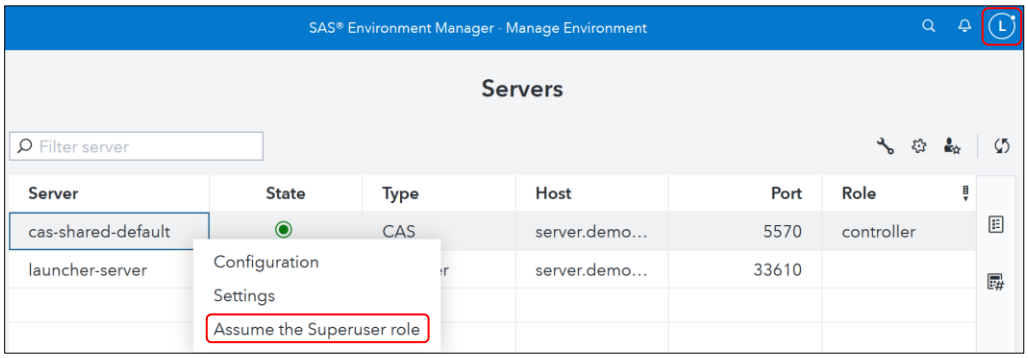
4) Add **Lynn** using the edit button.



5) Move **Lynn** to **Selected Identities** using the arrow between the two lists.



g. Sign out as **Christine** and sign back on as **lynn** with password **Student1**, and verify that the **Assume the Superuser role** option is available. Do you see more actions on the side menu in SAS Environment Manager because of your CAS Superuser role? **No. The CAS Superuser role controls management of the CAS server. Lynn is not in the SAS Administrators custom group, which would give her all the functionality of SAS Environment Manager.**



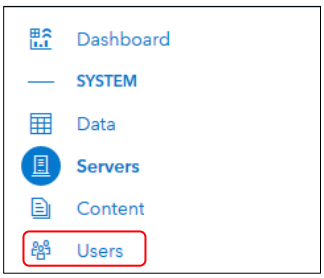
9. Adding Identities to the Data Builders and Application Administrators Custom Groups

In this practice, you add Lynn to the Application Administrators custom group. Then you add the Finance group to the Data Builders custom group. (Lynn is a member of the Finance group.)

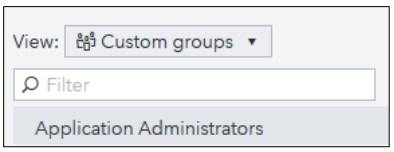
a. Sign in as **christine** with the password **Student1**. In the Assumable Groups window, click **Yes**

b. Add Lynn to the Application Administrators custom group. Members of Application Administrators can access selected administrative functions within applications.

1) Select **Users** from the side menu.

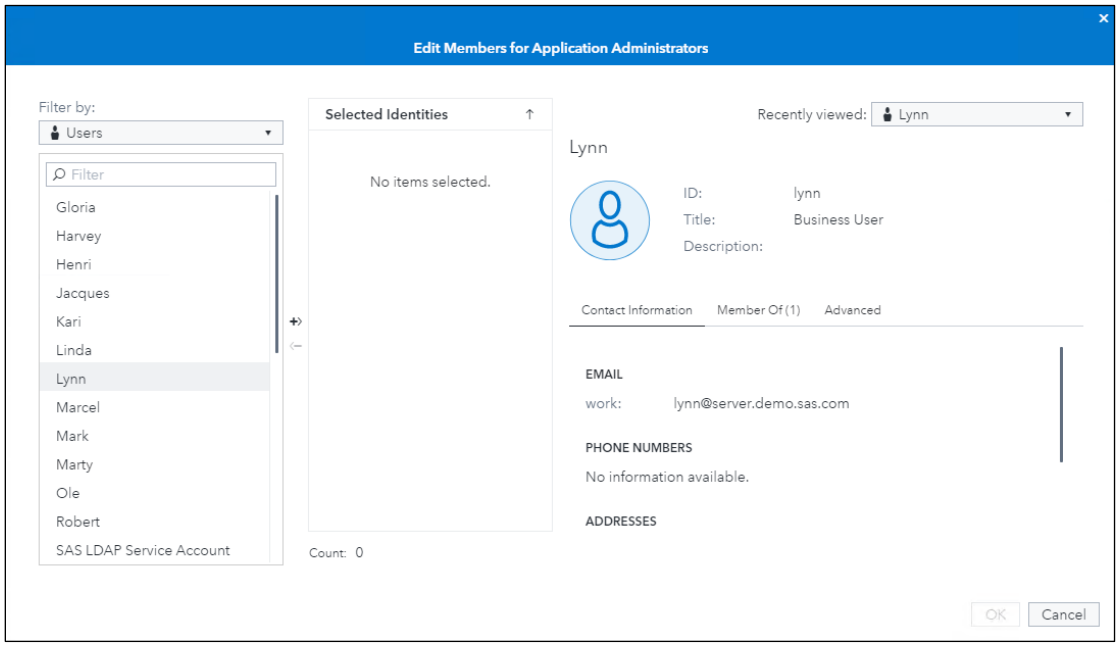


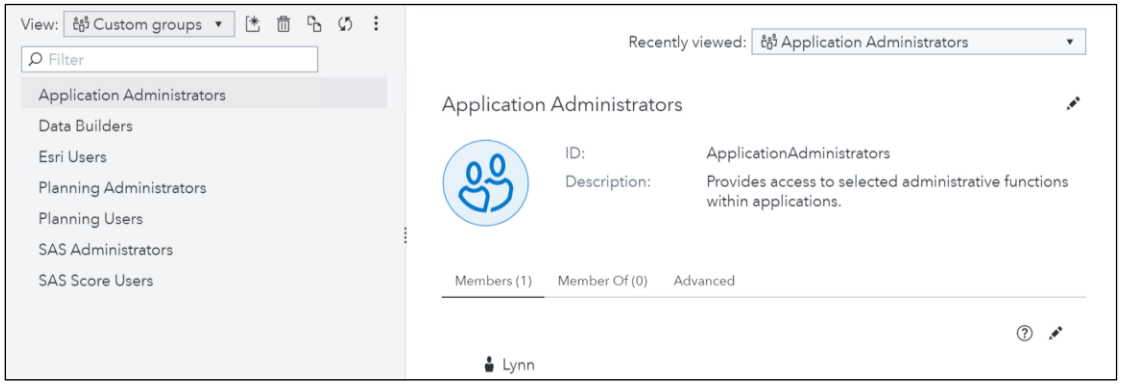
2) Highlight **Application Administrators** from **View** ⇨ **Custom groups**.



3) Click **Edit** icon to the right of Members area.

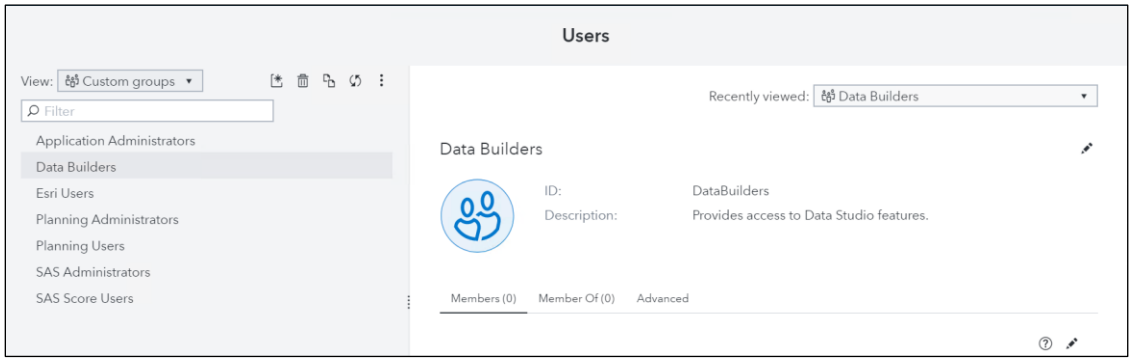
4) Move **Lynn** to the **Selected Identities**. Click **OK**.





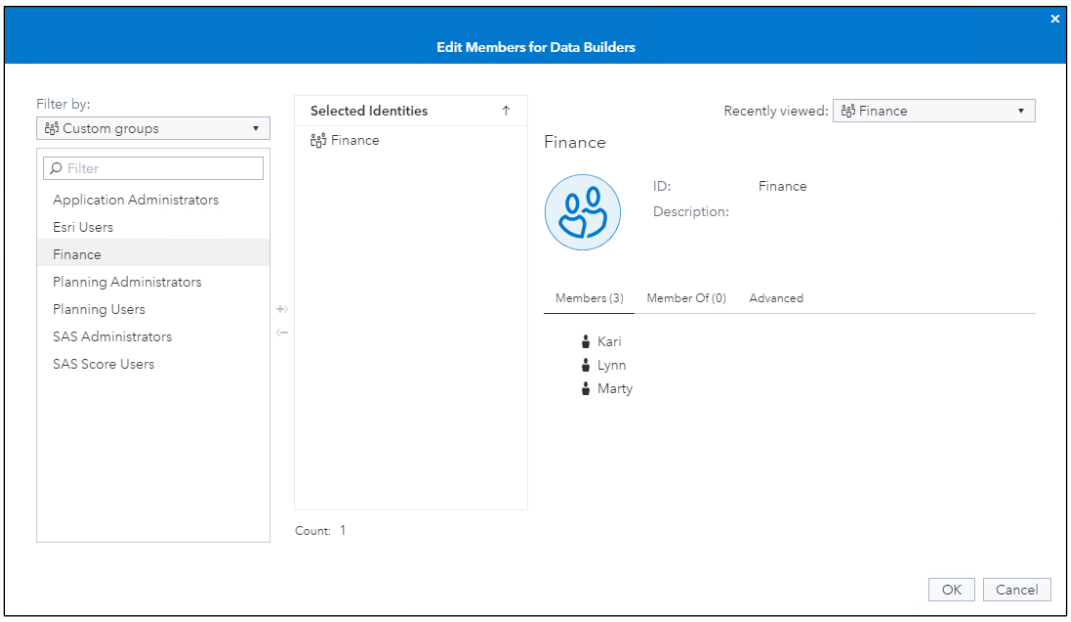
c. Add Finance custom group to Data Builders custom group. (The Finance group was created through the CLI in the previous practice.)

1) Highlight **Data Builders** from **View** ⇨ **Custom groups**.

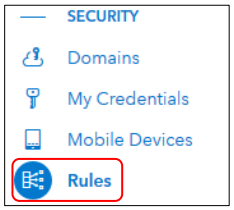


2) Click the **Edit** icon to the right of the Members area.

3) Move the **Finance** custom group to the **Selected Identities**. Click **OK**.

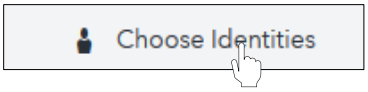


d. To see the functionality that is granted to Application Administrators and Data Builders, select **Rules** from the side menu.

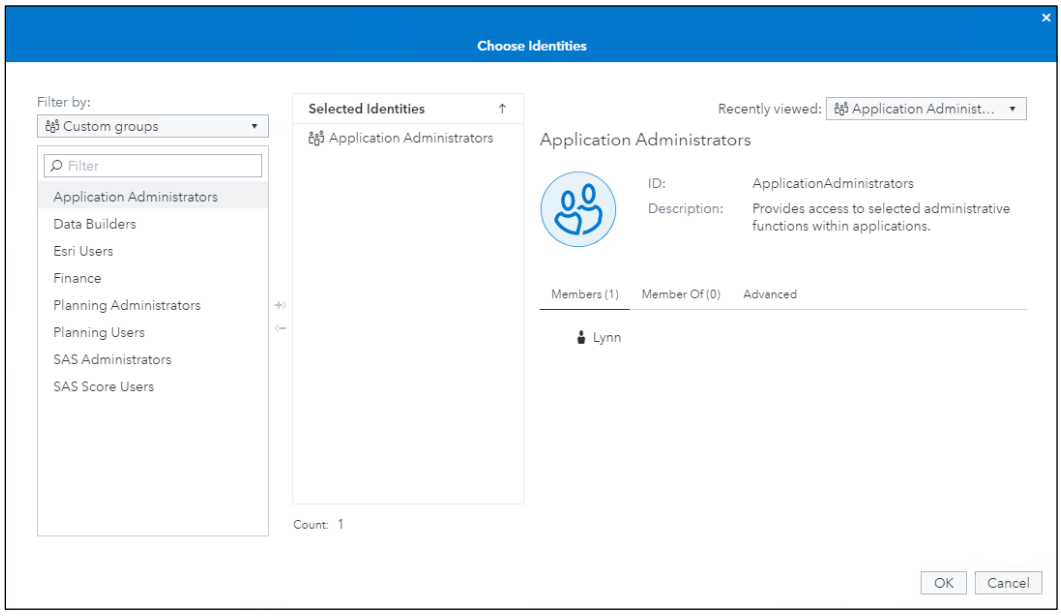


e. Filter on Application Administrators to bring up only rules that pertain to this custom group.

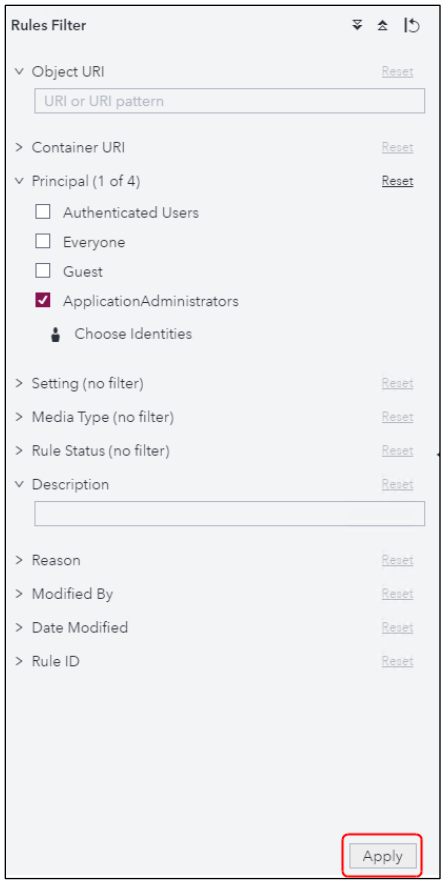
1) Click **Choose Identities** under the **Principal** section from the **Rules Filter** side.



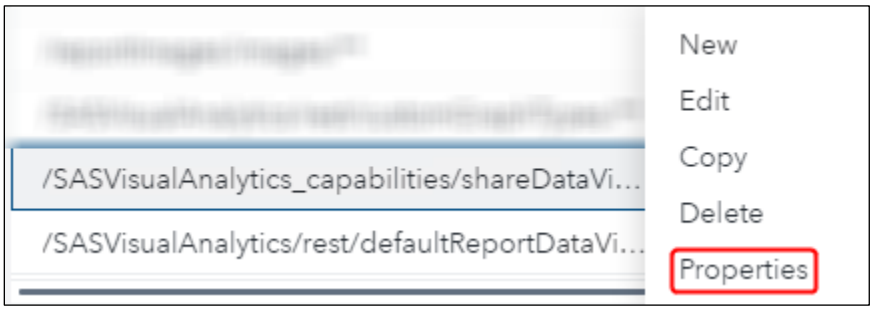
2) Select **Custom groups** from the **Filter by** drop-down menu and move **Application Administrators** to the **Selected Identities**. Click **OK**.



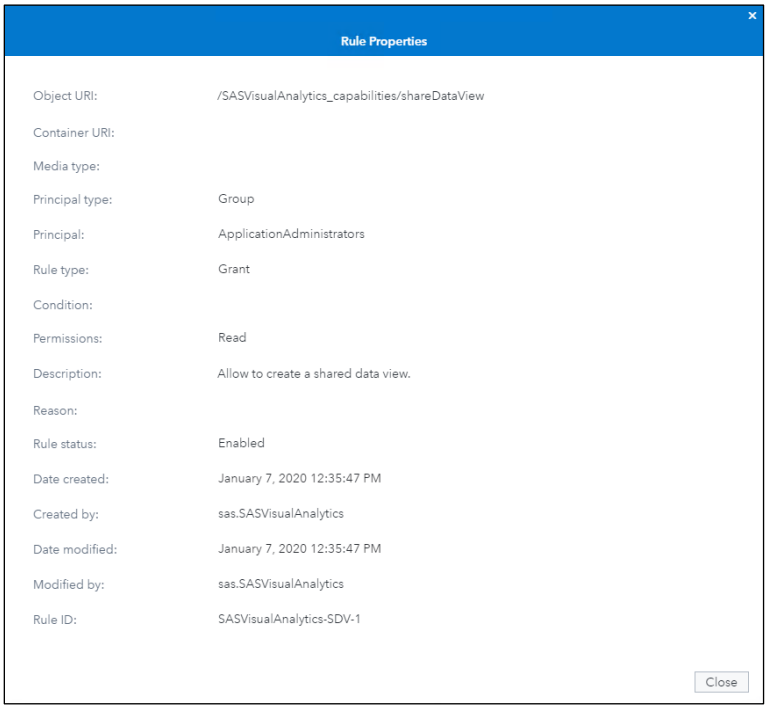
3) Check the **Application Administrators** box and click **Apply** to apply the filter that will display rules with this group as the principal.



f. You can right-click a rule and select **Properties** to see a description of what this rule allows Application Administrators to do. For example, right-click **SASVisualAnalytics_capabilities/shareDataView** and select **Properties**.

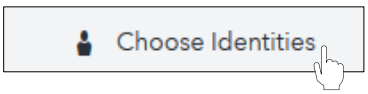


g. Application Administrators can share a data view in SAS Visual Analytics. Click **Close**.

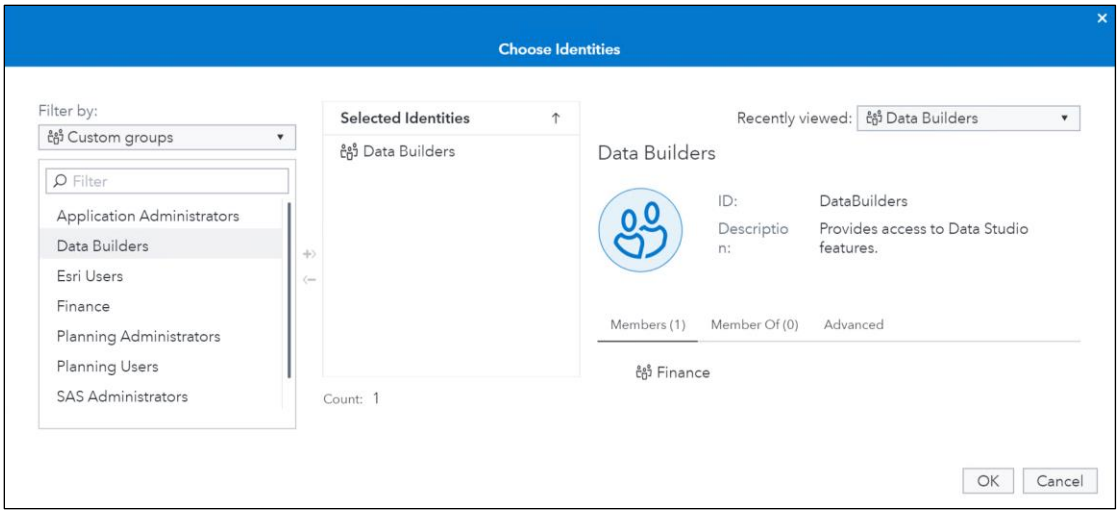


h. Filter on **Data Builders** in the Filter window.

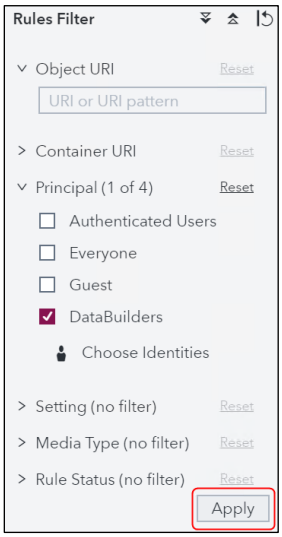
1) Select **Choose Identities** under the Principal section from the Rules Filter side.



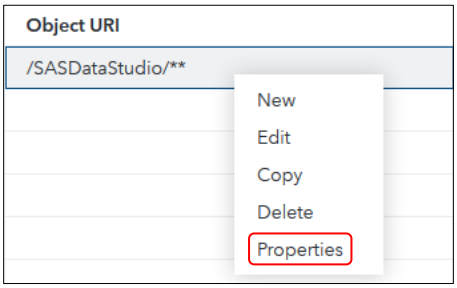
2) Select **Custom groups** from the **Filter by** drop-down menu and move **Data Builders** to the **Selected Identities**. Remove **Application Administrators**. Click **OK**.



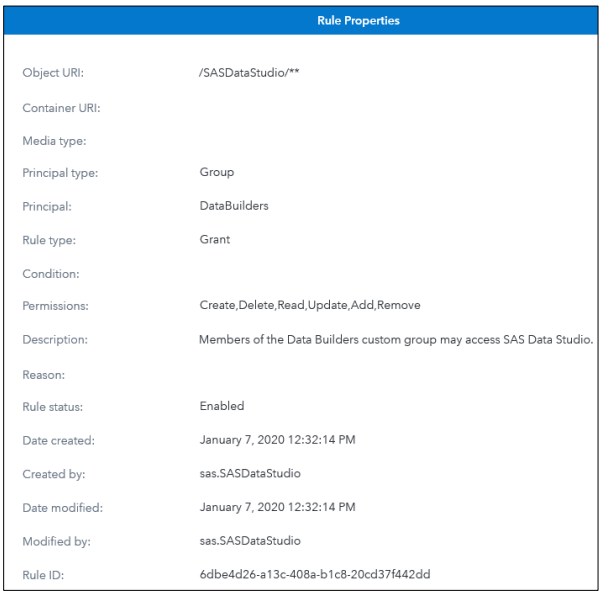
3) Check the **Data Builders** box and click **Apply** to apply the filter that will display rules with this group as the principal.



i. Right-click **/SASDataStudio/**** and select **Properties**.



j. Members of the Data Builders custom group can access SAS Data Studio, the visual interface that is included with SAS Data Preparation.



Rule Properties

Object URI:	/SASDataStudio/**
Container URI:	
Media type:	
Principal type:	Group
Principal:	DataBuilders
Rule type:	Grant
Condition:	
Permissions:	Create,Delete,Read,Update,Add,Remove
Description:	Members of the Data Builders custom group may access SAS Data Studio.
Reason:	
Rule status:	Enabled
Date created:	January 7, 2020 12:32:14 PM
Created by:	sas.SASDataStudio
Date modified:	January 7, 2020 12:32:14 PM
Modified by:	sas.SASDataStudio
Rule ID:	6dbe4d26-a13c-408a-b1c8-20cd37f442dd

Note: Rules are discussed in the next lesson.

10. Creating a CASHostAccountRequired Custom Group

By default, CAS sessions use the **CAS** account when using visual interfaces, such as SAS Visual Analytics. Files generated in such a session are saved in a folder belonging to the **CAS** account, but in a directory path that includes the user's ID.

By default, CAS sessions are run by the individual user when using a programming interface, such as SAS Studio (Basic). Files generated in such a session are saved in the user's Home directory.

If you prefer users to launch CAS sessions under their own accounts to cause their files to be saved to their UNIX directories, create and populate a custom group with the ID **CASHostAccountRequired**. When members of the **CASHostAccountRequired** group launch a CAS session, that session runs under that user's host account, and the generated files are created in the user's Home directory. Members of this group ***must*** have host accounts.

In this practice, you create the **CASHostAccountRequired** custom group.

a. The users of the Marketing group need to be verified as existing on the server with a Home directory. Use the CLI or SAS Environment Manager to see who is in the Marketing group.

SAS Environment Manager

Select **Users** from the side menu ⇨ **Groups** from the drop-down menu ⇨ highlight **Marketing**.

CLI

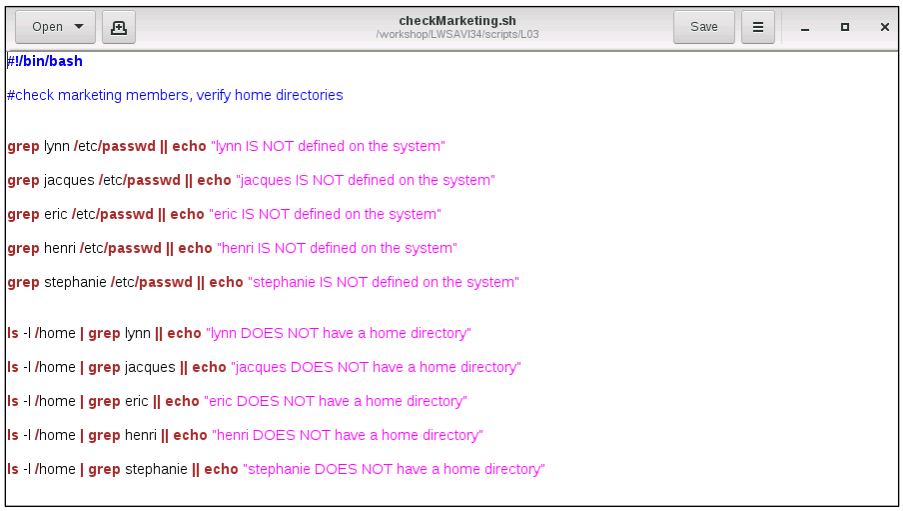
Use **christine**'s connection in mRemoteNg and run the following command:

```
/opt/sas/viya/home/bin/sas-admin identities list-members --
group-id Marketing
```

b. Run the following script to verify that Marketing group members have host accounts and home directories:

```
/workshop/LWSAVA35/checkMarketing.sh
```

Contents of **checkMarketing.sh**:

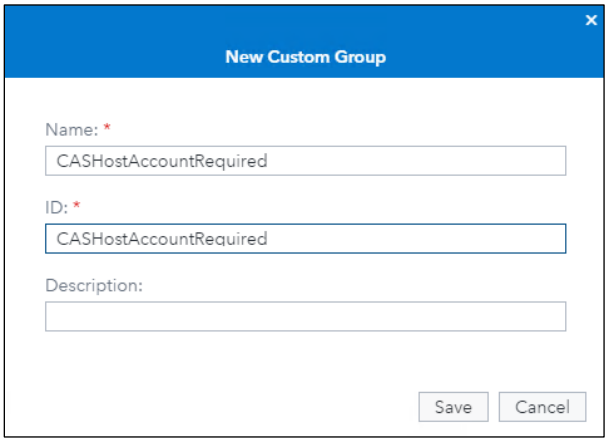


c. In SAS Environment Manager, select **Users** from the side menu. Select **Custom groups** from the **View** drop-down list.

(If not already logged on, sign in to SAS Environment Manager as **christine** with the password **Student1**. Opt in to the **SASAdministrators** assumable group.)

d. Select **New custom group**.

e. Enter **CASHostAccountRequired** in the **Name** and **ID** fields. Add a description if you want. Click **Save**.



f. Verify that the **Members (0)** tab is active. Click the **Edit** icon to the right.

g. Select the **Marketing** group and click the right arrow to move the group from the **Available** list box to the **Selected** list box. (You will need to change the **Filter by** value to **Groups**.)

h. Click **OK** to save the changes. You should see the members of the Marketing group under members section in the **CASHostAccountRequired** custom group.

11. Viewing CAS Sessions after CASHostAccountRequired Custom Group Is Created

a. Select the **Servers** area.

b. Check the current sessions to confirm that there are no sessions owned by Lynn.

1) Right-click **cas-shared-default** and select **Assume the Superuser Role**.

Notice the message about assuming the Superuser role above the list of servers.

2) Double-click **cas-shared-default** from the servers list to bring up sessions. (You can also right-click and select **Configuration**.)

There should not be any sessions owned by Lynn in the list of owners. (It is okay to see some disconnected sessions.)

You can also filter by owner **lynn** on this screen.

c. In mRemoteNG, enter the following command to check Lynn's sessions:

```
/opt/sas/viya/home/bin/sas-admin cas sessions list --owner
lynn --superuser --server cas-shared-default
```

d. In a Firefox browser, log on to SAS Drive as **lynn** with the password **Student1**.

If this is the first time logging on as Lynn, you might see the Welcome window. Click **Skip Setup**.

e. Open a report from SAS Drive.

1) Expand **SAS Content** ⇨ **Orion Star** ⇨ **Marketing**.

2) Double-click **Product Report** to open it.

3) Click the **Supplier Analysis** tab.

f. Go back to SAS Environment Manager and refresh the Sessions list from the toolbar in the upper right. Lynn now has CAS sessions.

g. In nRemoteNG, enter the following command to check Lynn's sessions:

```
/opt/sas/viya/home/bin/sas-admin cas sessions list --owner
lynn --superuser --server cas-shared-default
```

```
[christine@server L03]$ /opt/sas/viya/home/bin/sas-admin cas sessions list --owner lynn --superuser --server cas-shared-default
{
    "items": [
        {
            "authenticationType": "OAuth",
            "id": "3d655c7f-67be-e14b-84cb-ebaa097a3426",
            "name": "  Session:Mon Nov  5 08:57:55 2018",
            "owner": "lynn",
            "state": "Connected",
            "transactionState": ""
        },
        {
            "authenticationType": "OAuth",
            "id": "f813d6a6-de98-c145-9a24-e834d5552848",
            "name": "  Session:Mon Nov  5 08:57:55 2018",
            "owner": "lynn",
            "state": "Connected",
            "transactionState": ""
        }
```

h. Enter the following command to see whether Lynn is the owner of the CAS processes on the host machine:

```
ps -elf |grep session
```

```
[christine@server L03]$ ps -elf |grep session
4 S cas       31141  18203  0  80   0 - 258198 futex_ 06:16 ?       00:00:03 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       31516  18203  0  80   0 - 363039 futex_ 06:16 ?       00:00:05 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       52870  18203  0  80   0 - 266372 futex_ Nov02 ?       00:01:07 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session
ntroller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       69783  18203  0  80   0 - 427929 futex_ 08:38 ?       00:00:01 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       70237  18203  0  80   0 - 274646 futex_ 08:38 ?       00:00:00 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       70346  18203  0  80   0 - 435569 futex_ 08:38 ?       00:00:01 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas       70660  18203  0  80   0 - 363158 futex_ 08:38 ?       00:00:02 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S lynn     116864  18203  0  80   0 - 246393 futex_ 08:57 ?       00:00:00 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S lynn     116923  18203  3  80   0 - 620881 futex_ 08:57 ?       00:00:08 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
4 S cas      118210  18203  0  80   0 - 238165 futex_ 08:58 ?       00:00:00 /opt/sas/viya/home/SASFoundation/utilities/bin/cas session
 controller -id 0 -loghost 127.0.0.1 -keyfile - -controlpid 18205 -port 5570 -cfgpath /opt/sas/viya/config/etc/cas/default
0 S christi+ 124223  44376  0  80   0 - 28177 pipe_w 09:01 pts/0    00:00:00 grep --color=auto session
```

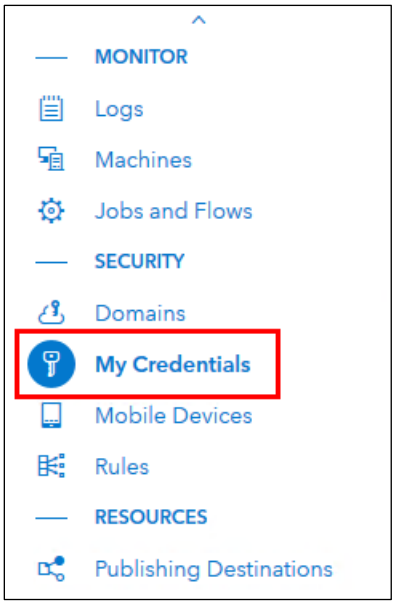
Because Lynn is in the **CASHostAccountRequired** custom group, her CAS session process is run by her ID instead of the CAS user in the operating system.

12. Modifying External Credentials in SAS Environment Manager

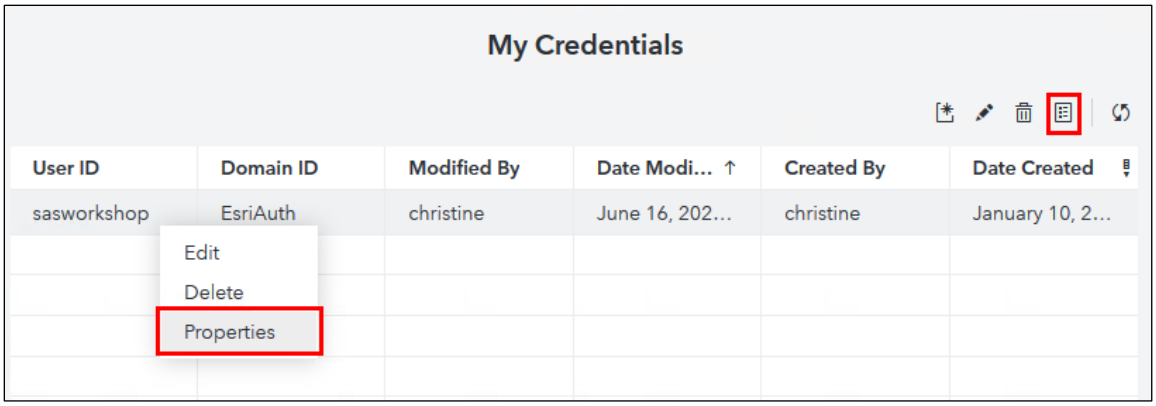
Users may manage their external credential information in SAS Environment Manager. The **My Credentials** page allows them to add, remove, and change these credentials used to access external resources.

a. Sign in to SAS Environment Manager as **Christine** with the password **Student1**.

b. From the side menu, select the **My Credentials** page.

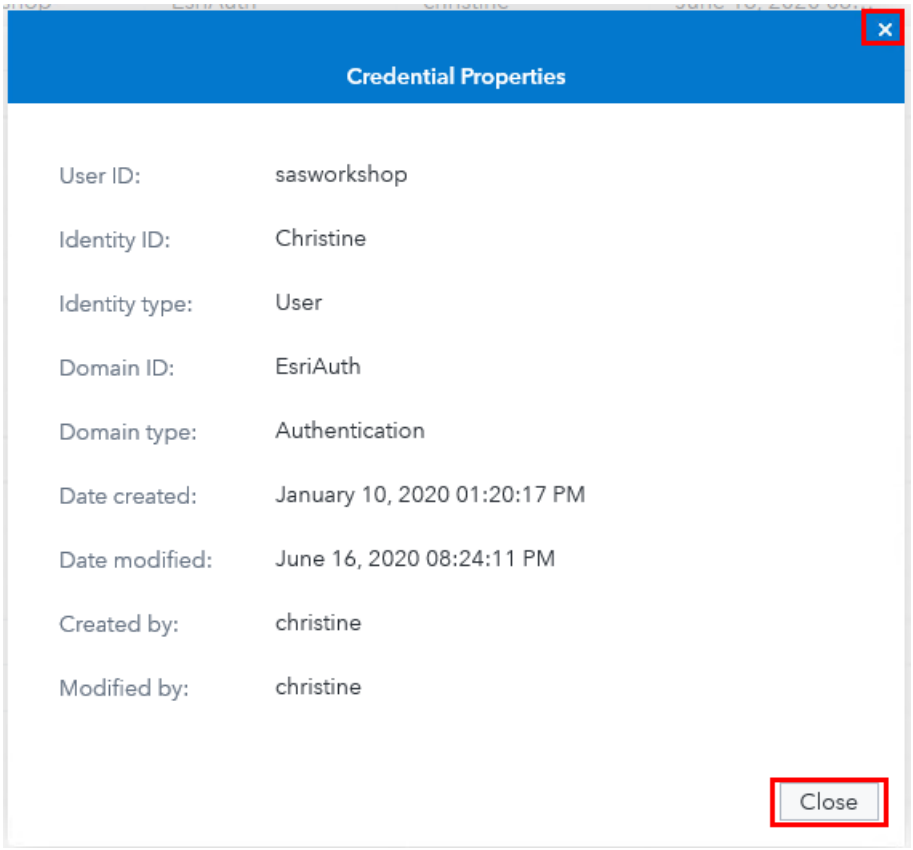


c. View the Credential Properties of sasworkshop, the account used by christine to connect to the EsriAuth Domain.



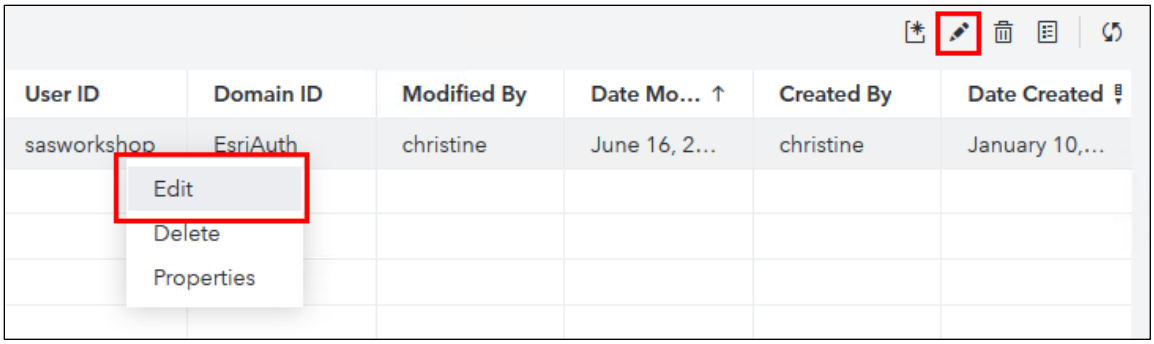
- Right-click on **sasworkshop** and select **Properties**.
- Or click the **Properties** button while **sasworkshop** is highlighted.

d. After reviewing the Credential Properties, close the page.

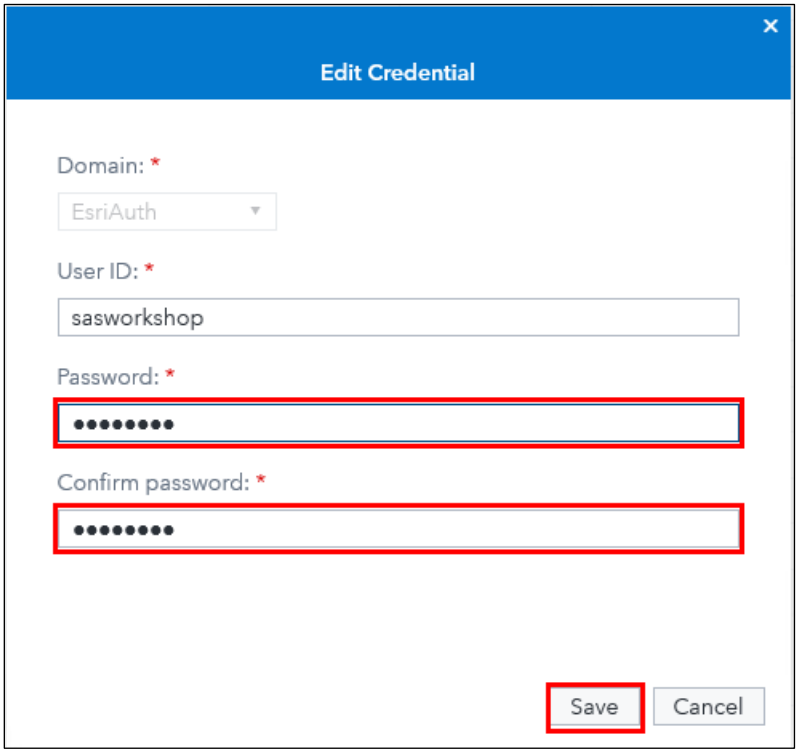


- Click **Close**.
- Or click the X in the upper right corner.

e. Edit the stored Credential information for **sasworkshop** to store the password **Student2** so that christine can connect to the EsriAuth Domain.



- Right-click **sasworkshop**.
- Or click the **Properties** button while **sasworkshop** is highlighted.



- Enter **Student2** in the **Password** and **Confirm Password** fields.

f. Save your changes.

End of Solutions

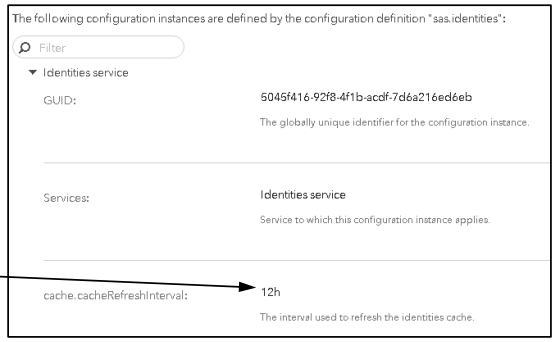
Solutions to Activities and Questions

3.01 Multiple Choice Question – Correct Answer

Where can you modify the refresh interval for the identities cache?

a. Credentials service
b. Mail service
c. Identities service
d. Cache Server service

SAS Environment Manager ⇨ Configuration page ⇨ View ⇨ All Services ⇨ identities service ⇨ sas.identities instance



The cache interval can be adjusted. The default is 12 hours.

8

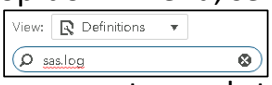
3.02 Activity – Correct Answer

1. In SAS Environment Manager, select **Content** from the side menu.
2. Right-click the **Public** folder ⇨ **View authorization**. Who are the Principals listed? (A *principal* is a user or group to which a rule is assigned.) Click **Close**.
   Authenticated Users, SAS Administrators, Christine
3. Select **Rules** from the side menu. How many implicit Principals (or identities) are there?
   Three – Authenticated Users, Everyone, Guest
4. Is **Guest Access** enabled? Hint: Apply a filter with **Guest** checked.
   No

40

3.03 Activity – Correct Answer

1. In SAS Environment Manager, select **Configuration** from the side menu.
2. From the **View** drop-down menu, select **Definitions**.
3. Search **sas.log**.



4. What configuration property needs to be configured to enable guest access?
   sas.logon.provider.guest
5. What service needs to be restarted when configuring properties pertaining to authentication mechanisms?

   Hint: Highlight **sas.logon.Kerberos**
   SAS Logon Manager