How to Implement SAS 9.4 on an Amazon Web Services Cloud Server Instance

Jeff Lehmann, Slalom Consulting, LLC

ABSTRACT

This paper demonstrates a tactical scenario where a SAS® 9.4 test environment is installed and configured on an Amazon Web Services (AWS) Elastic Compute Cloud (EC2) instance running Linux Red Hat version 7.1. The best practice actions to complete this SAS® 9.4 implementation are based upon successful implementation techniques as well as existing customer installations.

INTRODUCTION

The process to install SAS® 9.4 on an Amazon EC2 instance can be divided into the following steps:

1. Create an AWS EC2 instance using virtual private cloud (VPC)

2. Connect to the EC2 instance

3. Download a SAS® 9.4 software depot with SAS download manager

4. Perform SAS® 9.4 pre-installation tasks

5. Install SAS® 9.4 software with SAS Deployment Manager

6. Complete SAS® 9.4 post-installation tasks and configuration

While the majority of these installation actions are similar, even agnostic to the target operating system, the steps to complete a Windows or UNIX implementation may vary with what is proposed in this paper. Moreover, properly sizing an EC2 instance to replace an existing SAS® 9.4 data center installation is beyond the scope of this paper, as are discussions of potential issues and pitfalls to watch out for. Additionally, this paper assumes that the administrator has some familiarity with the AWS Management Console and its various networking, storage, database and security offerings.

SAS administrators and users who are interested in investigating solutions outside of the traditional data center environment will benefit from understanding this paper's installation and configuration exercise. As more enterprises using SAS® search for ways to experiment with new software, they will find that cloud service providers such as Amazon can help them reach their implementation goals at a faster pace and at a lower cost.   Alleviating the SAS® enterprise of some labor and capacity planning constraints while allowing staff to refocus on more productive or innovative uses of SAS® will lead to notably higher ROI on new SAS® software investments.

CREATE AWS EC2 INSTANCE USING A VPC

What follows is a series of steps to guide the SAS® administrator through the AWS Management Console VPC Wizard and EC2 Launch Instance interface.

1. Log into AWS Management Console and click the VPC icon. Then, click "Start VPC Wizard" and finally, click "VPC with Public and Private Subnets":

Display 1. "Select a VPC Configuration" ties in with "VPC with Public and Private Subnets" interface

Next, Specify: "IP CIDR block", "VPC Name", "Public subnet/name", "Private subnet/name", "Instance type", "Key pair name", S3 "Subnet/Policy" and then, click the "Create VPC" button.

Display 2. "Create VPC with Public and Private Subnets" details

The above step created a VPC instance ID, *vpc-466c6b23*, along with 2 subnets, a routing table, *rtb-83d137e7*, an internet gateway, *igw-362e5153*, an endpoint, *vpce-db2bcfb2*, a network ACL, *acl-0f0e096a* and most prominently, a new EC2 instance, *i-d057df79*.

2. The next step is to launch a new EC2 instance into the VPC already created. Back in the AWS Management Console, click the EC2 icon. Choose "Launch instance". Then, select "Red Hat Enterprise Linux 7.1 (HVM) - ami-12663b7a (64-bit)"

Display 3. Amazon Machine Image (AMI) selection list prompted by the EC2 Launch Instance action

*The compatible version of SAS® 9.4 for Red Hat 7.1 must be SAS 9.4 TS1M0 or later.

3. Select the following instance specifications for a SAS® test environment that will handle from 25 to 50 concurrent users and click "Next: Configure Instance Details":

Family: Compute optimized family
Type: c3.4xlarge
vCPUs: 16vCPUs
Memory: 30GB memory
Instance Storage: 2x160GB
EBS-Optimized Available: Yes
Network Performance: High

Display 4. EC2 Launch Instance Type specification page

4. In the "Configure Instance Details" screen Network field, select the newly created VPC. This will also populate the Subnet field. Then, for the Auto-assign Public IP field, select "Enable". Finally, in the Enable termination protection field, click the box to "Protect against accidental termination". Click "Next: Add Storage":

Display 5. "Configure Instance Details" details

5. Click "Next: Add Storage" and it is recommended to type in a larger size than the 10GB default. Below, 300GB was chosen to start. In any event, if required, storage can be added later without stopping the instance:

Display 6. "Add Storage" details include customizable size and volume type

3

6. Click "Next: Tag Instance" and enter in a unique key-value pair

Step 5: Tag Instance
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)	
Name	SAS 9.4 9C4VEX RHEL	⊗

Create Tag (Up to 10 tags maximum)

Display 7. "Tag Instance" useful key-value pairs can be the SAS® version, the SAS® order number or the OS

7. Click "Next: Configure Security Group" and enter in the firewall rules for your VPC. Refer to the SAS® 9.4 pre-installation checklist for ports [1] for inbound/outbound traffic instructions. NOTE: The below list of SAS ports is open only to the specified port. It is NEVER recommended to have the source be set to "Anywhere" at any port 0.0.0.0. Consider setting strict, specific IP address source origins, such as a VPN gateway IP address. Contact your network admin to confirm IP address(s).

Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ⦿ Create a **new** security group
○ Select an **existing** security group

Security group name: secgrp-SAS-9.4-Linux-RHEL
Description: secgrp-SAS-9.4-Linux-RHEL created 2015-06-10T18:44:32.918-04:00

Type	Protocol	Port Range	Source	
SSH	TCP	22	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	7980	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	21050	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	8111	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	41415	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	9380-9384	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	8581	My IP	72.28.157.179/32	⊗
HTTPS	TCP	443	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	11099	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	8811	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	7080	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	8701	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	8631	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	10651	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	7541	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	8801	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	9452	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	7551	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	5451	My IP	72.28.157.179/32	⊗
Custom TCP Rule	TCP	8591	My IP	72.28.157.179/32	⊗

Cancel   Previous   Review and Launch

Display 8. "Configure Security Group" details containing a list of firewall rules for required SAS® ports

Above, the listed ports are accessible from any source, anywhere. Select the "Review and Launch" button. The following warning message appears:

⚠ **Your instance configuration is not eligible for the free usage tier**
To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about free usage tier eligibility and usage restrictions.
Don't show me this again

Display 9. Warning message at "Review and Launch" time for the EC2 instance

Another less administratively intensive best practice would be to attach a virtual private gateway to the VPC, creating a custom route table and updating the security rules. The result would be a VPN connection between the VPC and an external corporate network. Setting up this VPN connection is beyond the scope of this paper, but the details can be found at this AWS VPC user guide web page [2].

8. Click the "Launch" button. Next, a popup requests to "Choose an existing key pair" or "create new key pair". AWS uses public-key cryptography to encrypt and a private key to decrypt login information. Together, they are known as a key pair [3]. If no key pair exists, it must be created. Below, an existing key pair was selected. Then, the "Launch Instances" button was clicked.

Select an existing key pair or create a new key pair   ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Choose an existing key pair   ⌄

Select a key pair
test1   ⌄

☑ I acknowledge that I have access to the selected private key file (test1.pem), and that without this file, I won't be able to log into my instance.

                                              Cancel   **Launch Instances**

Display 10. Key pair selection/creation screen

Launch Status

✔ **Your instances are now launching**
The following instance launches have been initiated: i-7dab20d4   View launch log

Display 11. Launch status message details

9. Select VPC off the AWS Management Console menu and then select "Internet Gateways". An internet gateway [4] allows communication between a VPC instance and the internet. Review the previously created internet gateway attached to the earlier created VPC.

☑   igw-362e5...   attached   vpc-466c6b23 (10.0.0.0/16) | vpc_S...

<

igw-362e5153

Summary	Tags

                ID: igw-362e5153   Attached VPC ID: vpc-466c6b23 (10.0.0.0/16) | vpc_SAS_9.4_9B6PXC_RHEL2
             State: attached   Attachment state: available

Display 12. Internet gateway attached to a VPC

10. The steps leading up to now created a secure connectivity method to the internet, connecting from a Private Network EC2 residing in a Public Network NAT (Network Address Translation) instance [18]. A NAT instance can be enabled to receive Internet-bound traffic from instances in a private subnet (e.g. 10.0.1.0/24), as well as SSH traffic from your network. To review the connectivity to the internet, check the Routes tab on the Route Table *rtb-83d137e7*.

☑   rtb-83d137e7   0 Subnets   Yes   vpc-466c6b23 (10.0.0.0/16) | vpc_S...

<

rtb-83d137e7

Summary	**Routes**	Subnet Associations	Route Propagation	Tags

Edit

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
pl-63a5400a (com.amazonaws.us-east-1.s3)	vpce-db2bcfb2	Active	No
0.0.0.0/0	eni-f831f7d7 / i-d057df79	Active	No

Display 13. Route table association with the internet gateway for the public subnet

11. Return to the AWS Management Console and select Elastic IP off the VPC menu. Click "Allocate New Address" and then "Yes, Allocate" to make it assignable to a VPC. Once allocated, the IP address can then be assigned back to the newly created EC2 instance ID. Elastic IP [5] addresses are very useful to provide users with a consistent IP address to use regardless of what dynamic cloud resource is implemented.

Display 14. Dialogue boxes for Elastic IP allocation and association

12. Select EC2 off the AWS Management Console and select the newly created EC2. Take note of the associated Public DNS: : **ec2-XX-XXX-XX-XXX.compute-1.amazonaws.com** (XX-XXX-XX-XXX is a mask for an IP Address. Your installation will have its own unique IP address)

CONNECT TO THE EC2 INSTANCE

Now that an AWS EC2 instance has been launched in a VPC, permitting access to the internet as well as providing external access to specified SAS® 9.4 ports, the next step is to set up client connections using ssh, FTP and VNC as well as a Firefox web browser running on the EC2 instance.

13. Download and configure a new ssh client connection to the instance using putty [6]. Next, download Pageant and install from the same page in order to get the most secure SSH agent functionality. First, convert your AWS .pem credentials file to a .ppk file using PuttyGen. Next, open Pageant (running as a Windows service), click the "Add Key" button and enter in the AWS Passphrase. Close the Pageant window and then configure putty as shown below and check the "Allow agent forwarding" box. As long as the matching private key for the instance is loaded into Pageant, the connection will be successful. The NAT scenario described up to now where the SAS 9.4 instance resides in a private subnet also requires setting up a reverse ssh tunnel [19].
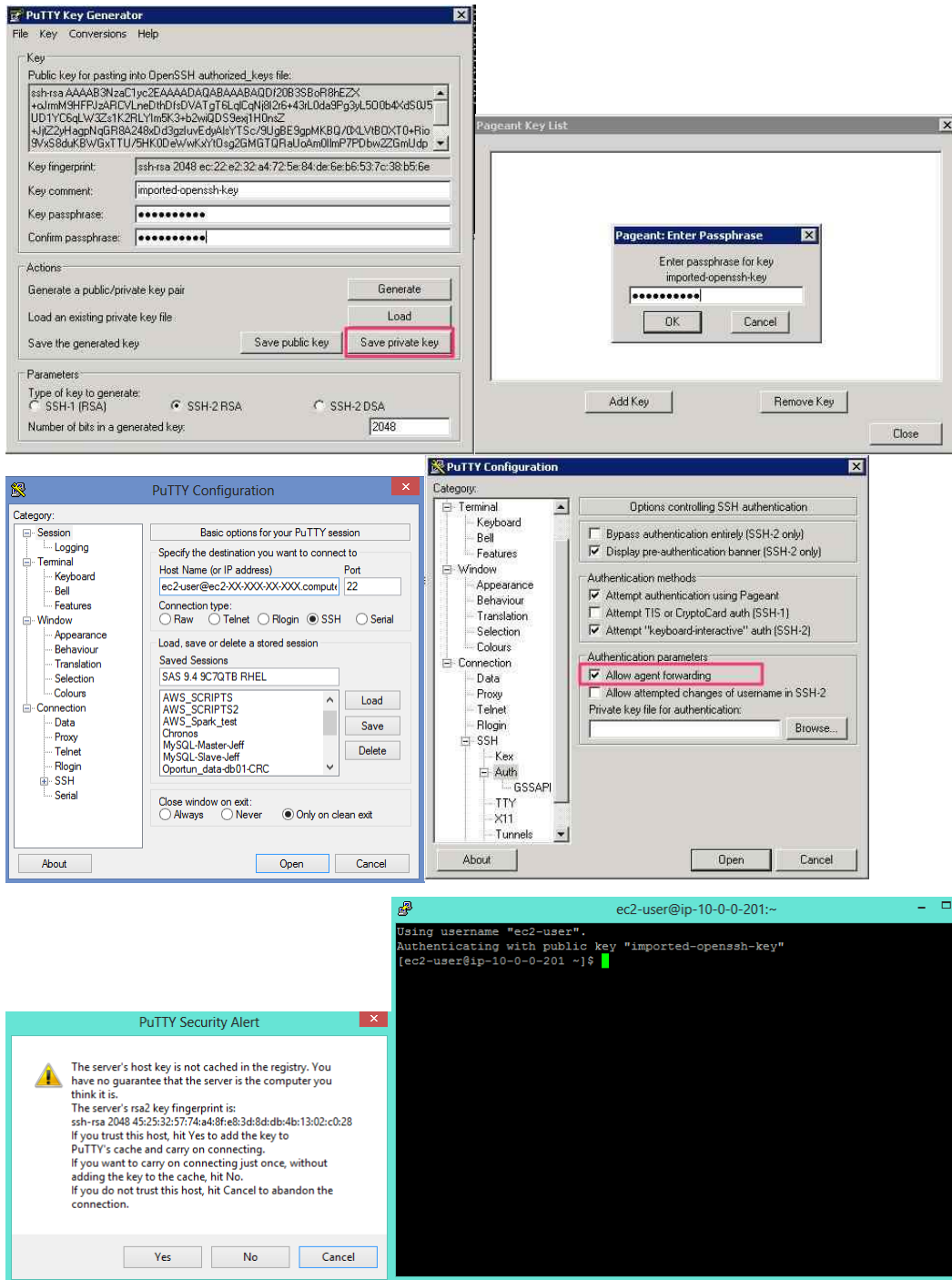
Display 15. Putty configuration details using private key file

14. Configure WinSCP [7], an FTP client, to connect to the EC2 instance in a similar way, clicking the same Allow agent forwarding" box. Click "OK" to confirm "Advanced Site Settings", "OK" to save the session site name and "Yes" to the unknown server warning:
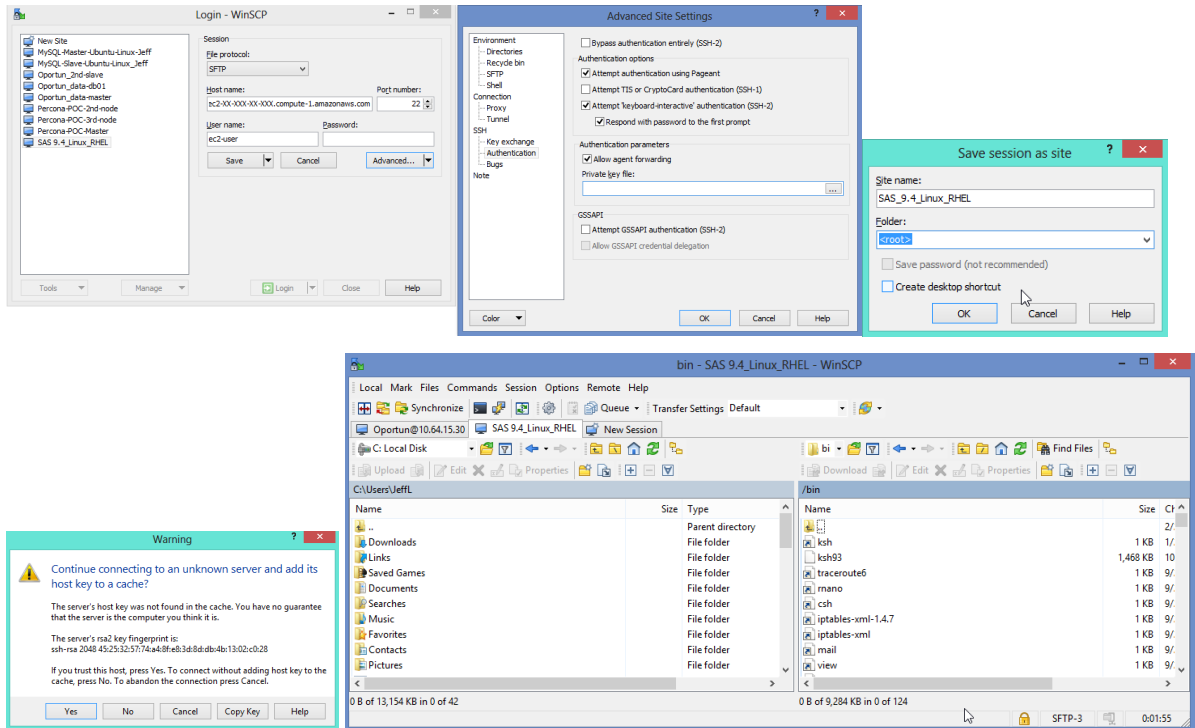
Display 16. WinSCP configuration details using private key file

15. Return to the putty session to run the Red Hat Linux OS update (It may discover no new updates):

```
[ec2-user@ip-10-0-0-201 ~]$ sudo yum install update
Loaded plugins: amazon-id, rhui-lb, security
rhui-REGION-client-config-server-6                    | 2.9 kB    00:00
rhui-REGION-client-config-server-6/primary_db         | 4.0 kB    00:00
rhui-REGION-rhel-server-releases                      | 3.7 kB    00:00
rhui-REGION-rhel-server-releases/primary_db           | 28 MB     00:00
rhui-REGION-rhel-server-releases-optional             | 3.5 kB    00:00
rhui-REGION-rhel-server-releases-optional/primary_db  | 2.8 MB    00:00
rhui-REGION-rhel-server-rh-common                     | 2.9 kB    00:00
rhui-REGION-rhel-server-rh-common/primary_db          | 33 kB     00:00
rhui-REGION-rhel-server-rhscl                         | 3.1 kB    00:00
rhui-REGION-rhel-server-rhscl/primary_db              | 584 kB    00:00
Setting up Install Process
No package update available.
Error: Nothing to do
```

16. [Install Tiger VNC Server](#) [8], on the EC2 instance. In putty, type the following commands separately:

sudo yum groupinstall "Desktop" (It will prompt: Is this ok [y/N]: **y**; At the end, it shows: Complete!)

sudo yum install pixman pixman-devel libXfont

sudo yum install tigervnc-server

vncpasswd (Set VNC Password)

8

sudo vi /etc/sysconfig/vncservers (Edit VNC configuration file: add the following 2 lines at the end)

    VNCSERVERS="1:ec2-user"

    VNCSERVERARGS[1]="-geometry 1024x768"

vncserver (Start the VNC server instance. The following lines show typical response entries)

      xauth: creating new authority file /home/ec2-user/.Xauthority

      New 'ip-10-0-0-201:1 (ec2-user)' desktop is ip-10-0-0-201:1

      Creating default startup script /home/ec2-user/.vnc/xstartup
      Starting applications specified in /home/ec2-user/.vnc/xstartup
      Log file is /home/ec2-user/.vnc/ip-10-0-0-201:1.log

17. Use the TigerVNC viewer [9] client to connect to your EC2 instance:
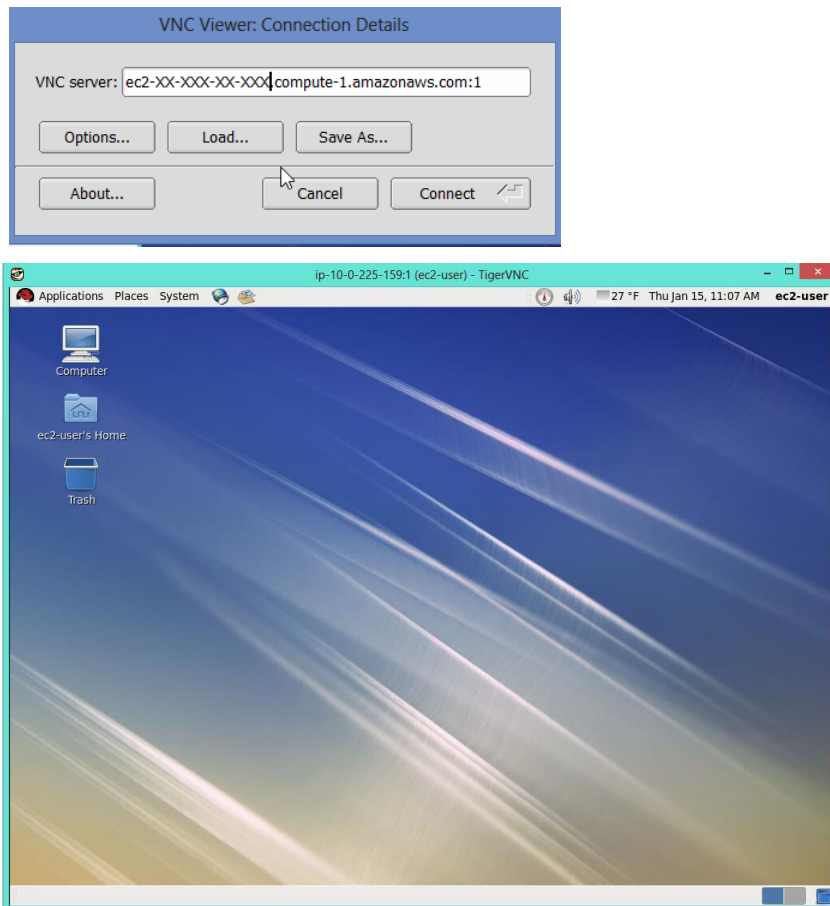
Display 17. TigerVNC Viewer's connection details and successful logon to GUI interface

18. Download and install Firefox web browser on the EC2 instance:

sudo yum install firefox

Start Firefox by clicking on the icon to the right of the System drop down menu:
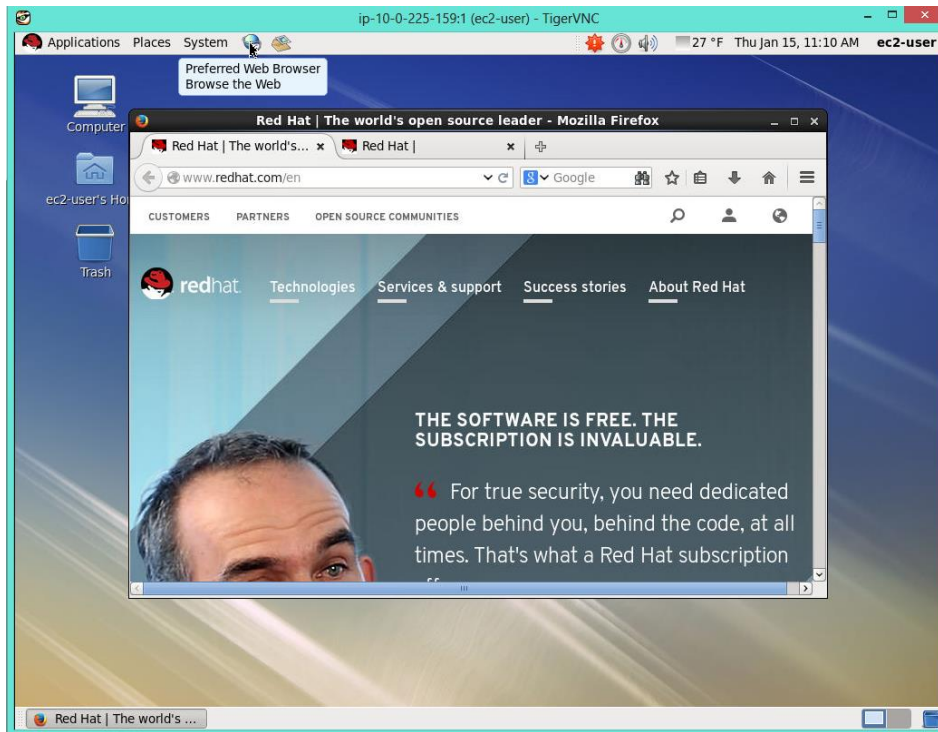
Display 18. Firefox [10] web browser launched in EC2 instance GUI interface

DOWNLOAD A SAS® 9.4 SOFTWARE DEPOT

Since there now is a GUI interface available running the Firefox web browser, a SAS software depot can be downloaded to the EC2 instance.

19. Browse to the SAS Download Manager download page [11]. Log into a SAS profile. First click on the Release 1.61 link and then click on the link for Linux for x64 and begin the download process:

		SAS Download Manager				
Platform	**Description**	**Request Download**	**Size**	**Uncompressed**	**Release Date**	
64-bit enabled AIX	SAS Download Manager	esdclient__94250__r64__xx__web__1	117MB	534MB	2014-09	
64-bit enabled Solaris	SAS Download Manager	esdclient__94250__s64__xx__web__1	88MB	534MB	2014-09	
HP-UX IPF	SAS Download Manager	esdclient__94250__h6i__xx__web__1	109MB	534MB	2014-09	
Linux for x64	SAS Download Manager	esdclient__94250__lax__xx__web__1	67MB	534MB	2014-09	
Macintosh	SAS Download Manager	esdclient__94250__mac__xx__web__1.dmg	15MB	534MB	2014-09	
Microsoft® Windows® for x64	SAS Download Manager	esdclient__94250__wx6__xx__web__1.exe	42MB	534MB	2014-09	
Solaris for x64	SAS Download Manager	esdclient__94250__sax__xx__web__1	83MB	534MB	2014-09	
Windows	SAS Download Manager	esdclient__94250__win__xx__web__1.exe	42MB	534MB	2014-09	
z/OS	SAS Download Manager	esdclient__94250__mvs__xx__web__1.zos	17MB	534MB	2014-09	

Display 19. SAS Download Manager download by platform

20. Start a terminal session. Create a new SAS software depot directory. Open up permissions on the depot directory and with the SAS download executable. Then, start SAS download manager to download SAS® 9.4 software with the commands below:.
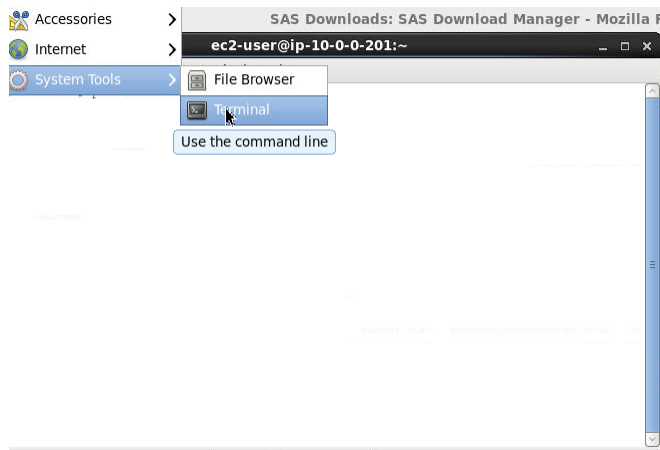
Display 20. Select System Tools drop down menu to start the "Terminal" (ssh) session

sudo mkdir /SAS_9.4_Software_Depot

sudo chmod 777 /SAS_9.4_Software_Depot

cd /home/ec2-user/Downloads

sudo chmod 777 esdclient__94250__lax__xx__web__1

./esdclient__94250__lax__xx__web__1
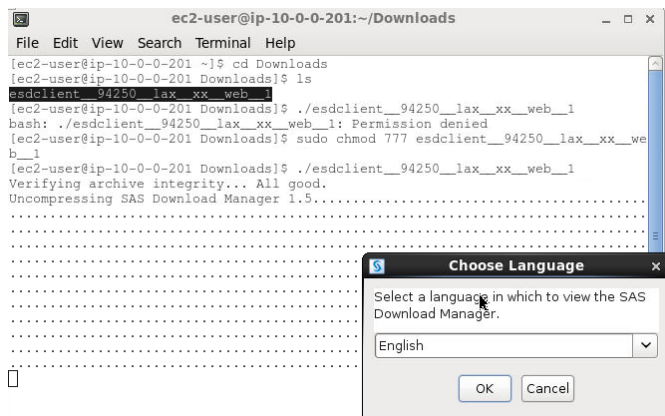
Display 21. Start SAS® Download Manager

21. After clicking OK for English on the Language prompt, obtain the SAS® 9.4 order information from the SAS orders ESD e-mail sent to the SAS site representative and type in the Order Number and SAS Installation Key on the Order Information dialogue box. Click the "Next" button and confirm the order details on the next screen. Click "Next" and opt to include the entire order or a subset. Click "Next" and select the depot directory. Click "Next" and confirm that disk space requirements are met and click "Download" to start the process. If the process is interrupted, the administrator has the opportunity to restart the download where it left off or to start again.

Display 22. The SAS Download Manager progress bar

At the end of the download process, if successful, a "Download Complete" confirmation dialogue box appears. Click "Finish".

PERFORM SAS® 9.4 PRE-INSTALLATION TASKS

In order to complete a successful deployment of SAS® 9.4, the pre-installation tasks [12] must be completed:

22. In the instance's Firefox browser, point to the following SAS® 9.4 QuickStart guide [13] URL :

    file:///SAS_9.4_Software_Depot/install_doc/9B6PXC/quickstart.html

    This web page contains useful URLs for SAS pre-installation and migration/installation/configuration documentation.

23. Run the following commands to install SAS® 9.4-required Linux packages:

    sudo yum install libXp

    sudo yum install numactl

    sudo yum install glibc

    sudo yum install compat-glibc (required [14] for SAS® 9.4to run on Linux Redhat 7.1)

24. Create the following required local users for the SAS® 9.4 installation and assign them to the new SAS user groups sas_user and sas:

    sudo groupadd sas_user

    sudo useradd sas

    sudo passwd sas

    sudo usermod -G sas_user sas

id sas (verify success of user sas creation and assignment to group sas_user)

Perform the next 5 commands again, substituting sassrv with lsfadmin, lsfuser and sasdemo)

sudo useradd sassrv

sudo passwd sassrv

sudo usermod -G sas_user sassrv

sudo usermod -g sas sassrv

id sassrv

25. Verify the install SAS software depot. Substitute the name of your software depot directory below:

sudo chmod 755 /your_software_depot_directory/*.*

sudo chmod 755 /your_software_depot_directory/hot_fix/*.xml

sudo chmod 755 /your_software_depot_directory/hot_fix/*.zip

sudo chmod 755 /your_software_depot_directory/order_data/9B6PXC/*.xml

sudo chmod 755 /your_software_depot_directory/download_data/*.xml

cd /your_software_depot_directory/utilities/depotchecker

./SASDepotCheck.sh

26. Create and provide the appropriate write access to the following directory /etc/opt/vmware/vfabric:

cd /etc/opt

sudo mkdir vmware

cd vmware

sudo mkdir vfabric

sudo chgrp -R sas /etc/opt/vmware/

sudo chown sas /etc/opt/vmware/

sudo chgrp -R sas /etc/opt/vmware/vfabric

sudo chown sas /etc/opt/vmware/vfabric

27. Increase open files limit [15] for all processes. Check **ulimit** and increase open file descriptors to **20480** and number of processes (RHEL) to **10240**:

ulimit -a

core file size   (blocks, -c) 0

data seg size   (kbytes, -d) unlimited

scheduling priority   (-e) 0

file size   (blocks, -f) unlimited

pending signals   (-i) 239355

max locked memory   (kbytes, -l) 64

max memory size   (kbytes, -m) unlimited

open files   (-n) **1024**

pipe size   (512 bytes, -p) 8

POSIX message queues   (bytes, -q) 819200

real-time priority   (-r) 0

stack size   (kbytes, -s) 10240

cpu time   (seconds, -t) unlimited

max user processes   (-u) **1024**

virtual memory   (kbytes, -v) unlimited

file locks   (-x) unlimited

sudo vi /etc/security/limits.conf (Add the following to the end of the file):

* soft nproc 10240

* hard nproc 10240

* soft nofile 20480

* hard nofile 20480

sudo vi /etc/security/limits.d/91-nofile.conf (Add the following to the end of the file):

* - nofile 20480

sudo vi /etc/security/limits.d/90-nproc.conf (Add the following to the end of the file):

* soft nofile 20480

* hard nofile 20480

Exit out of the user session in putty, etc. to view the changes. Log back in and type the following:

[ec2-user@ip-10-0-0-98 ~]$ **ulimit -a**

core file size   (blocks, -c) 0

data seg size   (kbytes, -d) unlimited

scheduling priority   (-e) 0

file size   (blocks, -f) unlimited

pending signals   (-i) 239355

max locked memory   (kbytes, -l) 64

max memory size   (kbytes, -m) unlimited

open files   (-n) **20480**

pipe size   (512 bytes, -p) 8

POSIX message queues   (bytes, -q) 819200

real-time priority   (-r) 0

stack size   (kbytes, -s) 10240

cpu time   (seconds, -t) unlimited

max user processes   (-u) **10240**

virtual memory   (kbytes, -v) unlimited

file locks   (-x) unlimited

28. Create SAS 9.4 install home and configuration home: (e.g. **/sas_install/9.4 /sas_config/9.4**)

   sudo mkdir /sas_install

   sudo mkdir /sas_install/9.4

   sudo mkdir /sas_config

   sudo mkdir /sas_config/9.4

   sudo chgrp -R sas /sas_install

   sudo chown -R sas /sas_install

   sudo chgrp -R sas /sas_config

   sudo chown -R sas /sas_config

   sudo chmod -R 777 /sas_install

   sudo chmod -R 777 /sas_config

29. Download junit [16] and copy to the SAS install directory (e.g. /sas_install) directory using WinSCP FTP

30. Download and install C compiler and python:

   sudo yum install gcc

   sudo yum install python (python may already be installed)

   Find where python is already installed:

   sudo find . -name "python*" -print

   (e.g. /usr/lib64/python2.6, /usr/lib/python2.6, /usr/bin/python)

31. The following components are required to be installed to run ./sasbatch.sh (SAS base):

   sudo yum install ksh (Korn shell)

   sudo yum install libXp.so.6

32. In order to avoid a setuid permissions error later on in the installation process, run these commands:

   cd /sas_install/9.4/SASFoundation/9.4/utilities/bin

   sudo ./setuid.sh

INSTALL SAS® 9.4 SOFTWARE WITH SAS DEPLOYMENT MANAGER

Now that the Linux RedHat 7.1 environment has been properly prepared, SAS® 9.4 software can be installed. What follows is a series of approximate steps showing via screen prints the SAS® 9.4 Deployment Wizard installation process in its entirety. These steps vary considerably based upon the SAS® 9.4 software order and as well as on requirements for additional configuration (authentication, migration, third-party software, etc.).

33. Start the SAS® 9.4 Deployment Manager wizard and then begin and continue to process the installation:

    su sas (The SAS® 9.4 can only be installed using a sas installer id and not the root id)

    cd /SAS_9.4_Software_Depot (Switch to the SAS® 9.4 software depot directory)

    ./setup.sh -record –deploy (-record allows the wizard to capture your inputs into a response file)
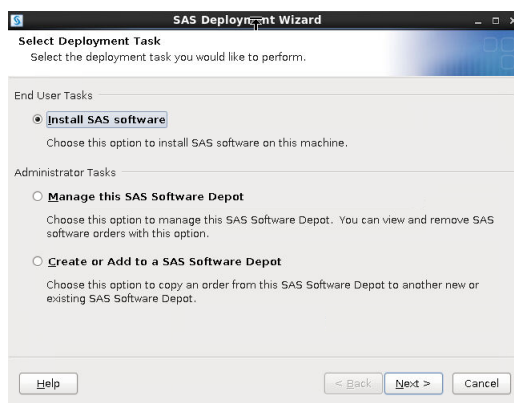
Display 23. Select SAS deployment task
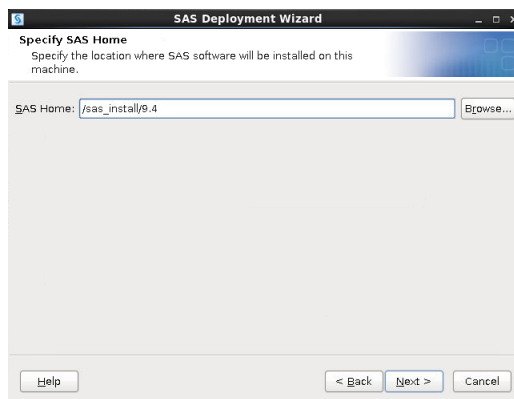
Display 24. Select SAS home directory
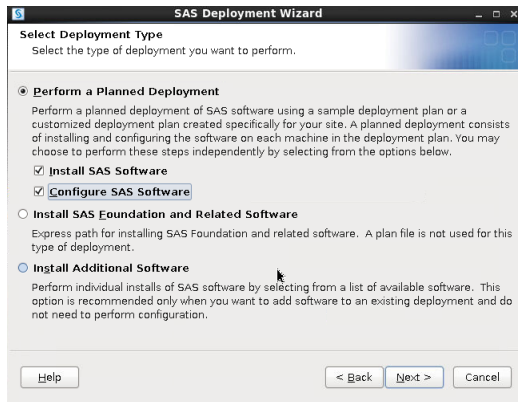
Display 25. Select SAS deployment type
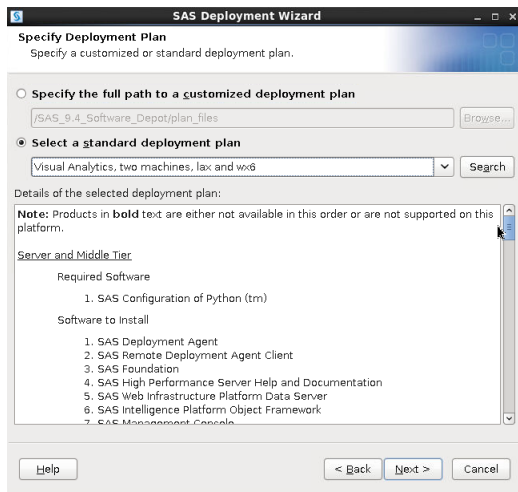
Display 26. Select SAS deployment plan
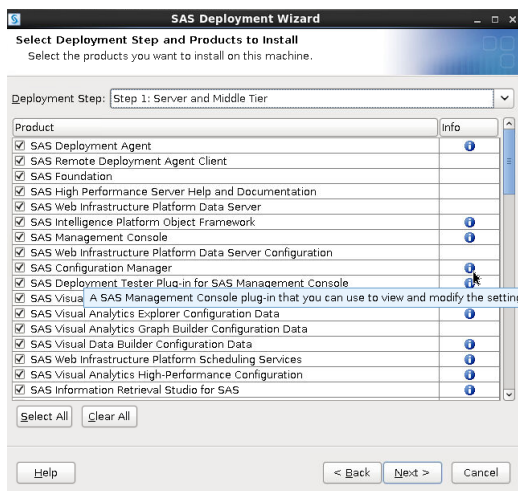
Display 27. Select SAS products to install
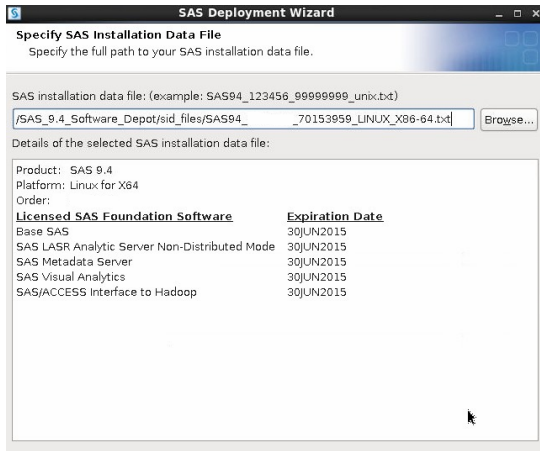
Display 28. Select SAS installation data file and take note of expiration dates
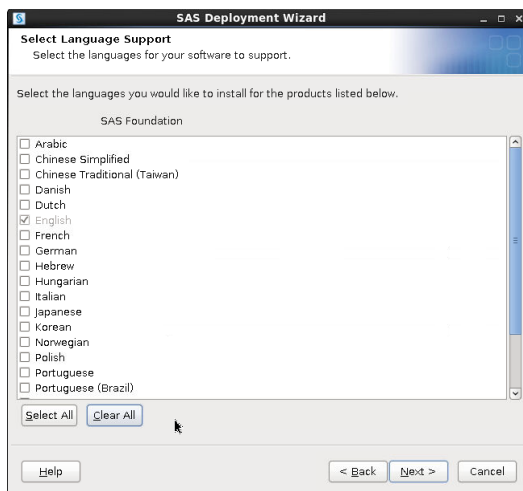
Display 29. Select SAS deployment task
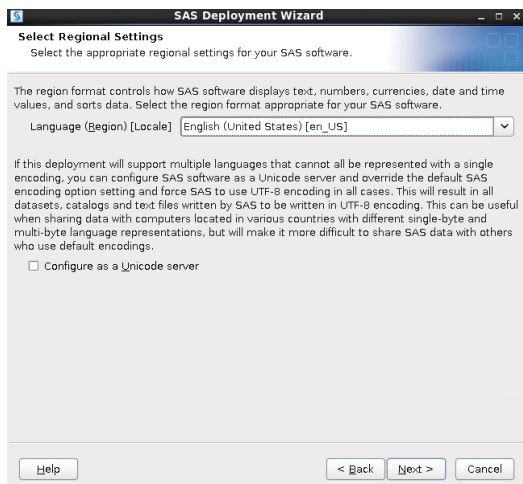
Display 30. Select Regional Settings
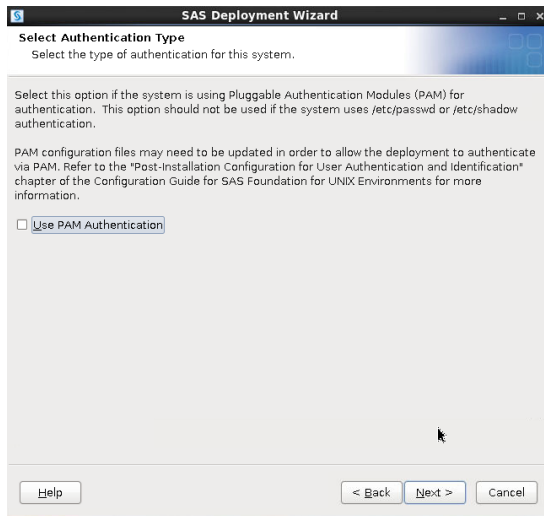
Display 31. Select Authentication Type
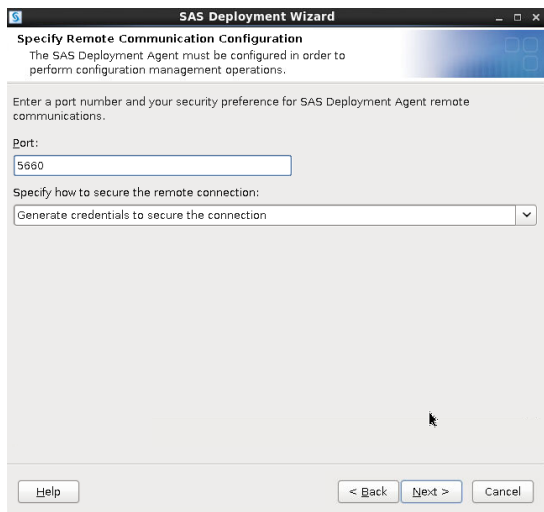
Display 32. Specify Remote Communication Configuration
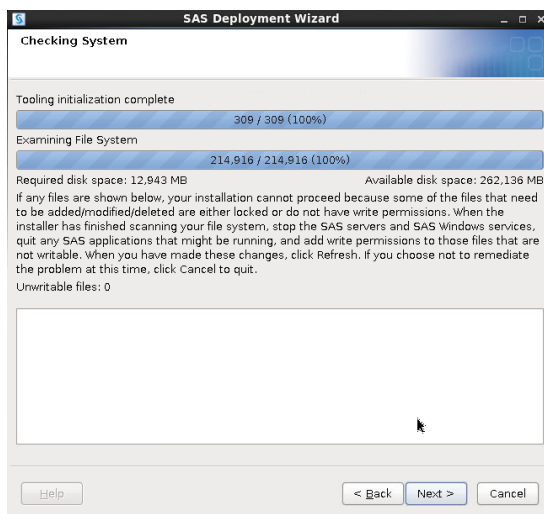
Display 33. Checking File System
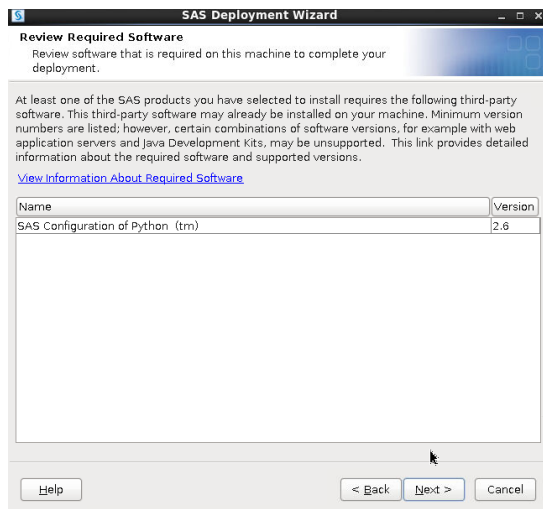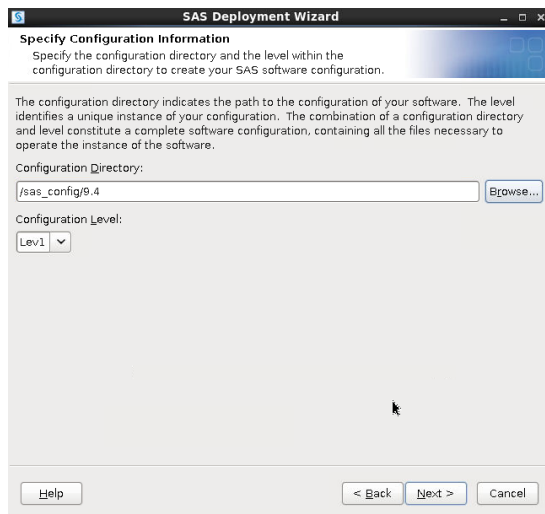
Display 34. Review Required Software
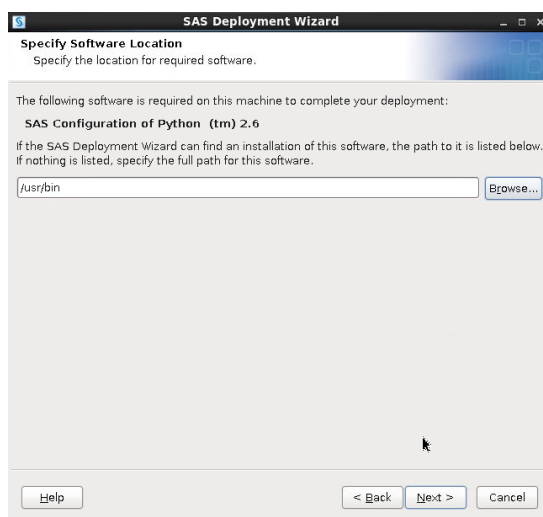
Display 35. Specify Software Location
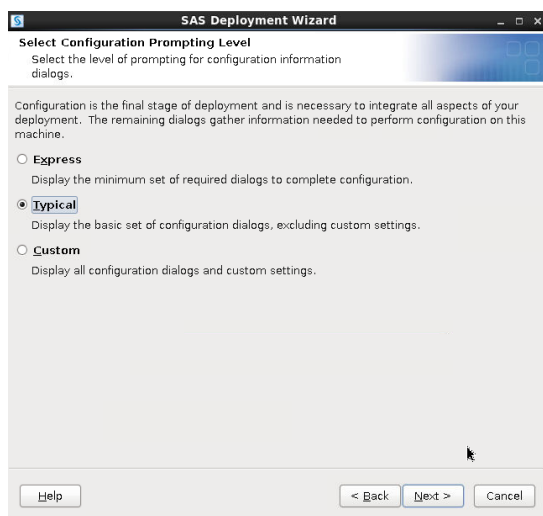
Display 36. Select Configuration Prompting Level
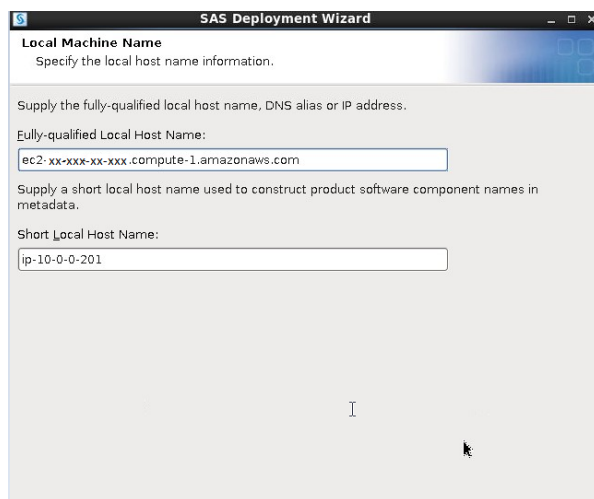
Display 37. Specify Configuration Information
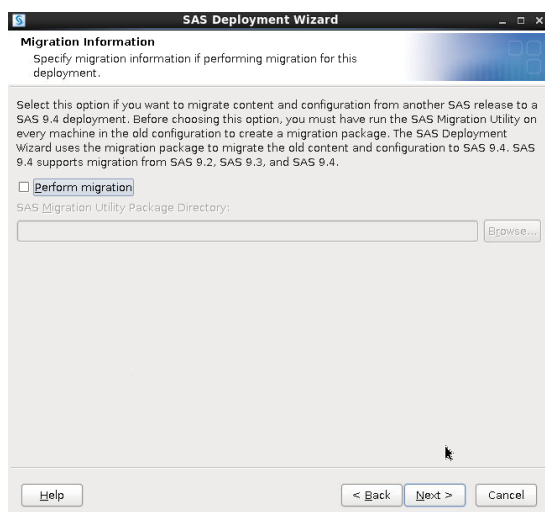
Display 38. Specify Local Host Name

Display 39. Migration Information
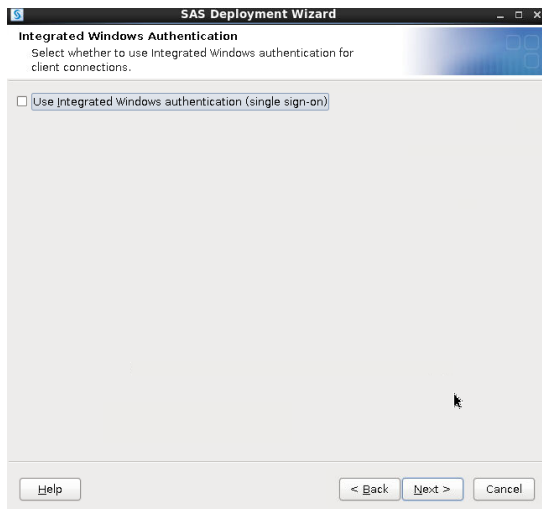
Display 40. Integrated Windows Authentication
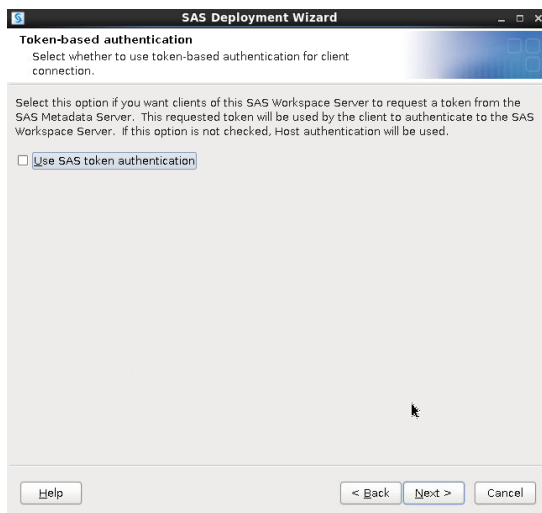
Display 41. Integrated Windows Authentication
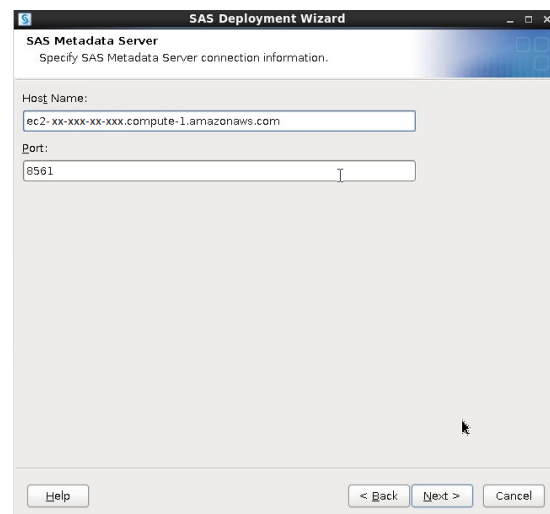
Display 42. SAS Metadata Server details
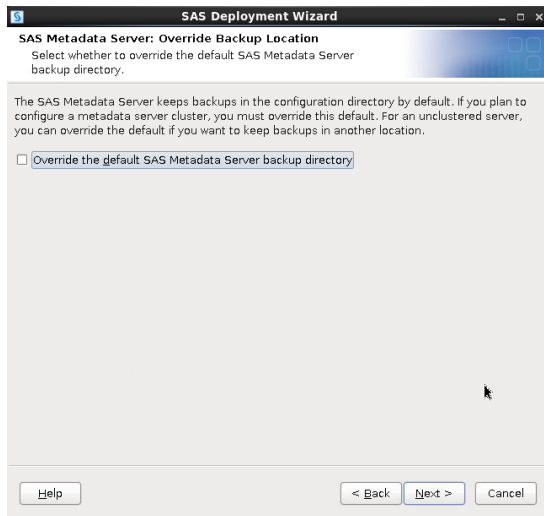
Display 43. SAS Metadata Server: Override Backup Location
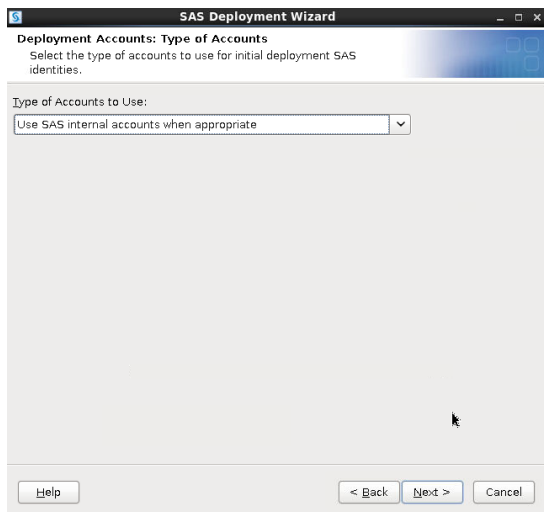
Display 44. Deployment Accounts: Type of Accounts
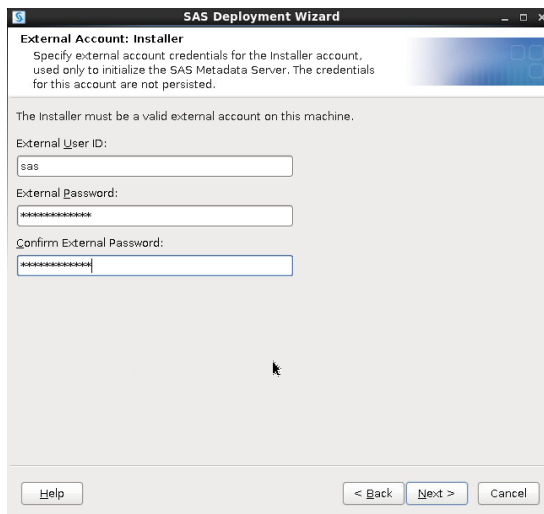
Display 45. External Account: Installer
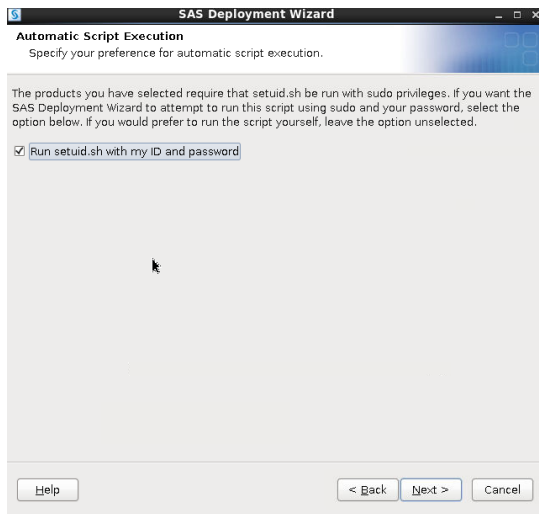
Display 46. Automatic Script Execution
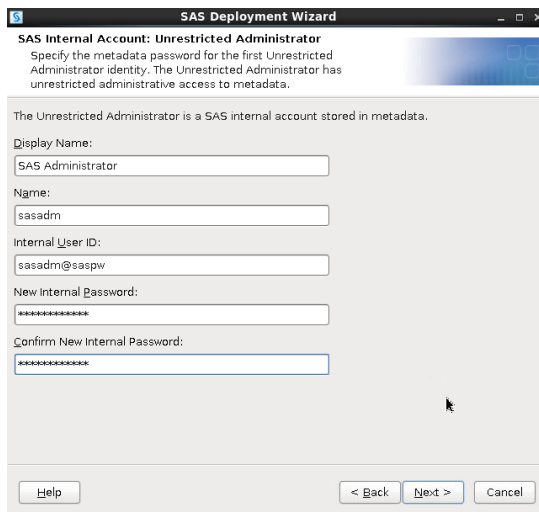
Display 47. SAS Internal Account: Unrestricted Administrator
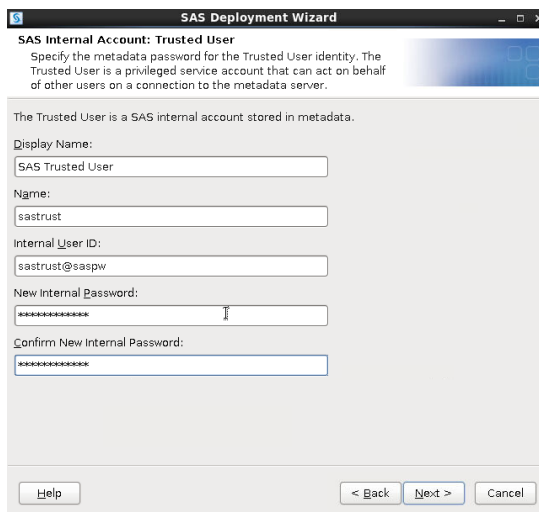
Display 48. SAS Internal Account: Trusted User
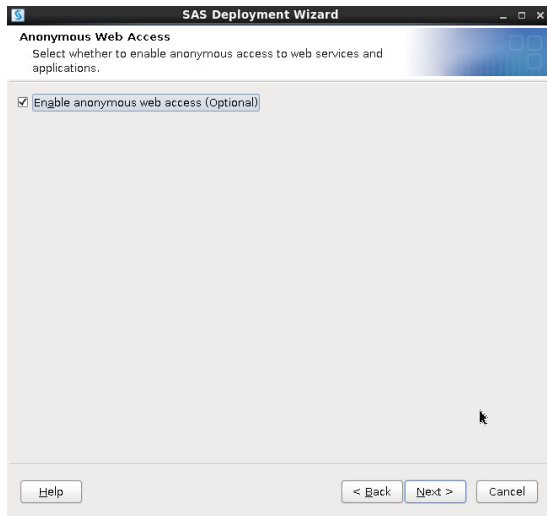
Display 49. Anonymous Web Access
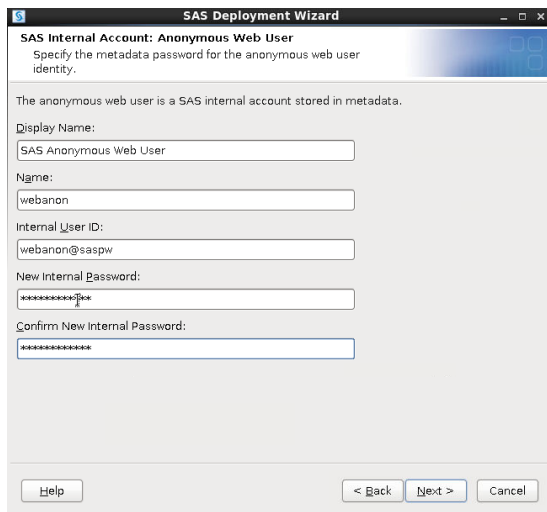
Display 50. SAS Internal Account: Anonymous Web Access
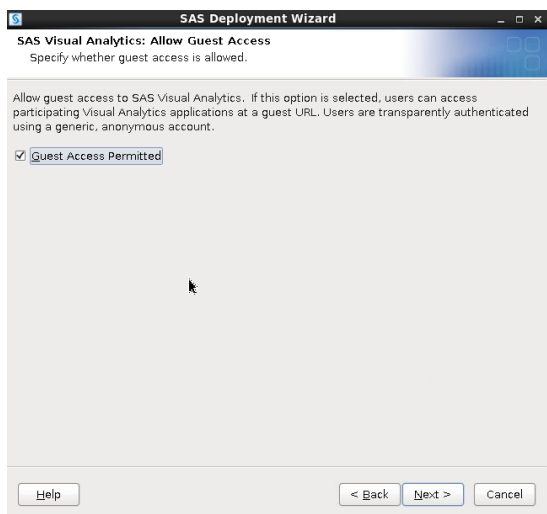
Display 51. SAS Visual Analytics: Allow Guest Access

Display 52. External Account: SAS Spawned Servers Account

Display 53. Deployment Account: First User

Display 54. External Account: First User

Display 55. Server Encryption

Display 56. Estimated System Size

Display 57. E-mail Server details

Display 58. E-mail Addresses

Display 59. SAS Object Spawner port selection

Display 60. SAS Object Spawner port bank
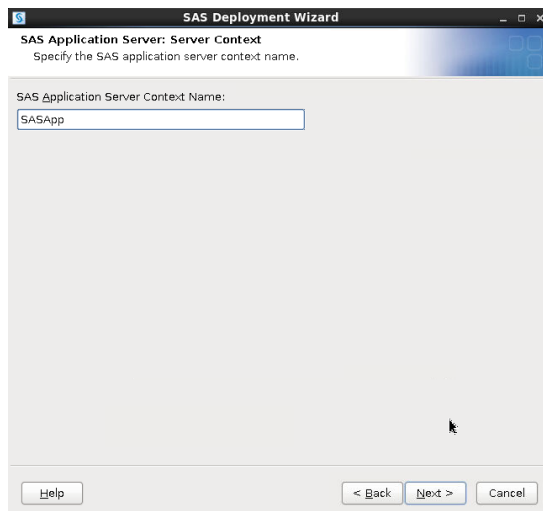
Display 61. SAS Application Server: Server Context
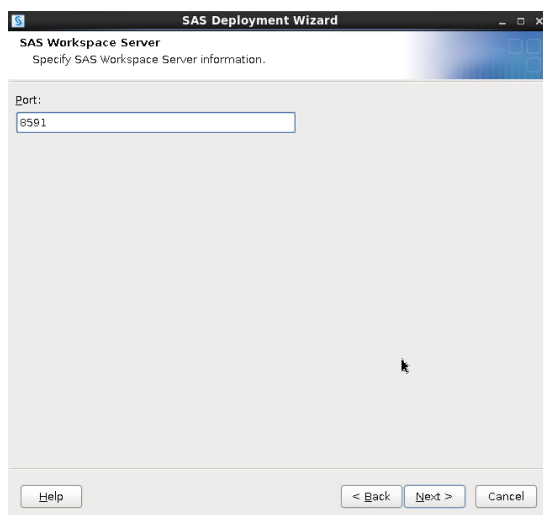
Display 62. SAS Workspace Server port
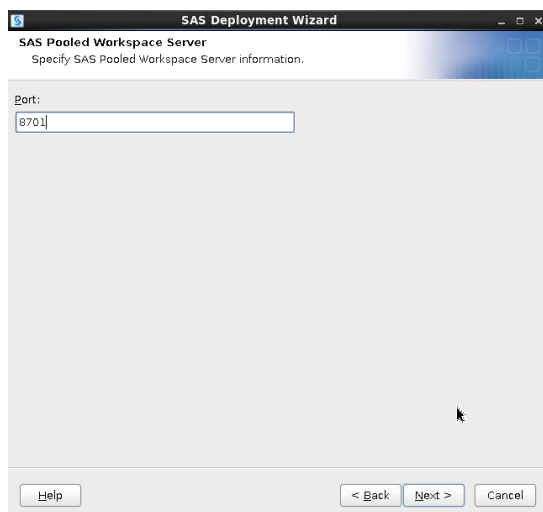
Display 63. SAS Pooled Workspace Server port

Display 64. SAS Stored Process Server port

Display 65. SAS Stored Process Server: MultiBridge Connections

Display 66. SAS Web Infrastructure Platform Data Server details

Display 67. SAS Data Step Batch Server

Display 68. Operating System Services Scheduling Server

Display 69. SAS Deployment Tester Server details

Display 70. SAS Web Server: Automated or Manual Configuration Op
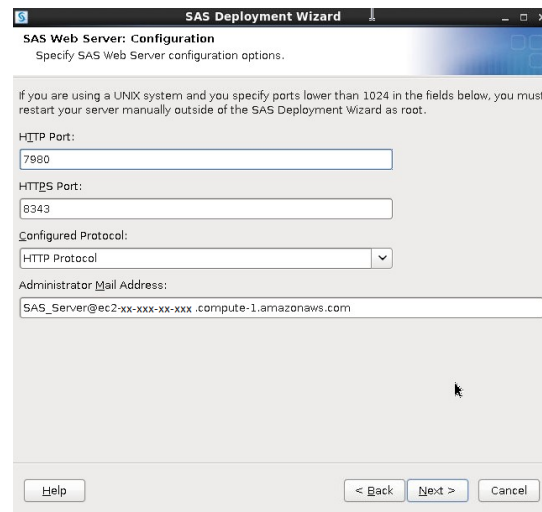
Display 71. SAS Web Server: Configuration
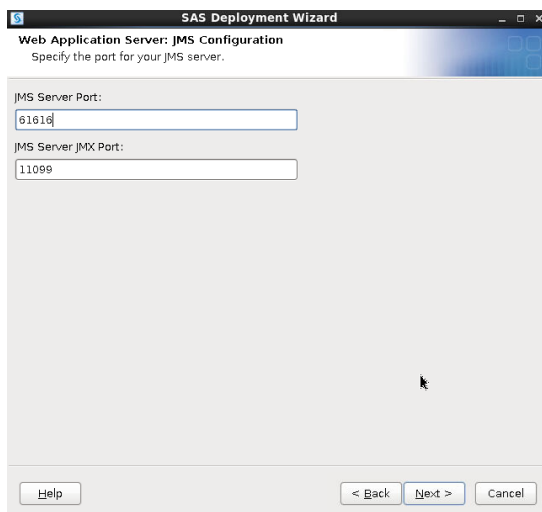
Display 72. SAS Web Application Server: JMS Configuration

Display 73. SAS Web Application Server: Cache Locator Configuration

Display 74. SAS Web Application Server: Server Configuration

Display 75. SAS Web Application Server: Server Ports
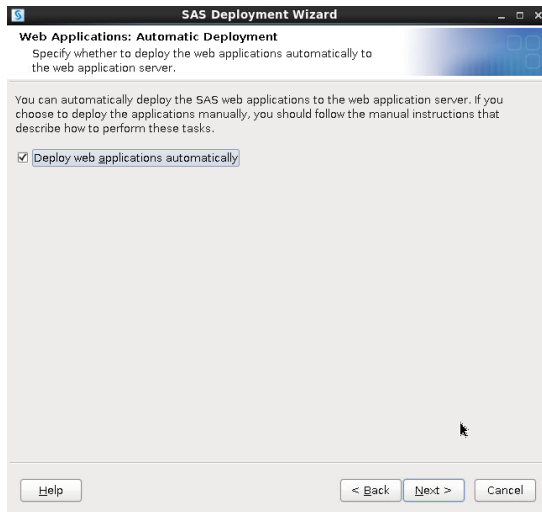
Display 76. SAS Web Application Server: Automatic Deployment
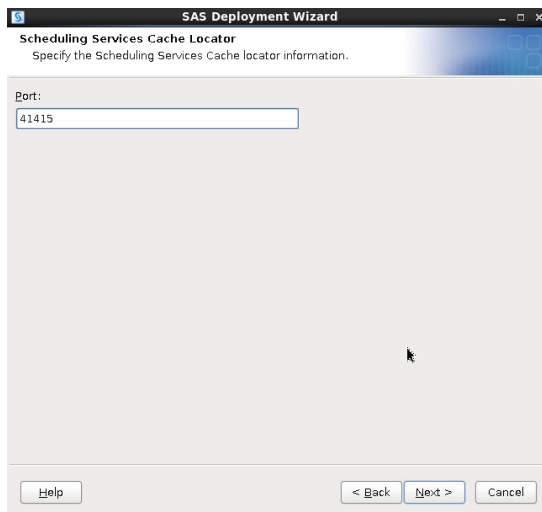
Display 77. Scheduling Services Cache Locator
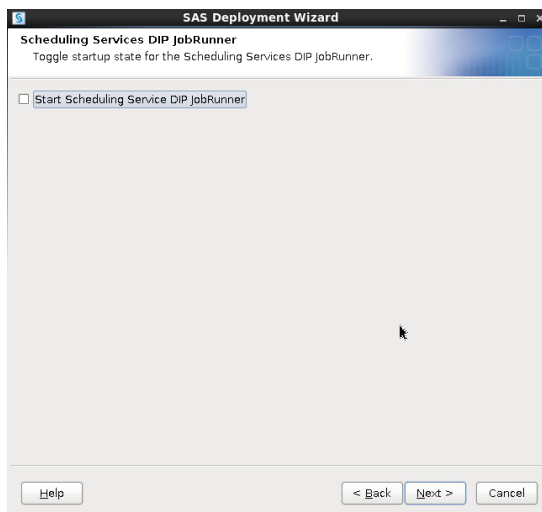
Display 78. Scheduling Services DIP JobRunner

Display 79. Web Application Themes

Display 80. IP Multicast Version

Display 81. IP Multicast details

Display 82. SAS Content Server: Repository Directory

Display 83. SAS Web Infrastructure Platform Database: JDBC Properties
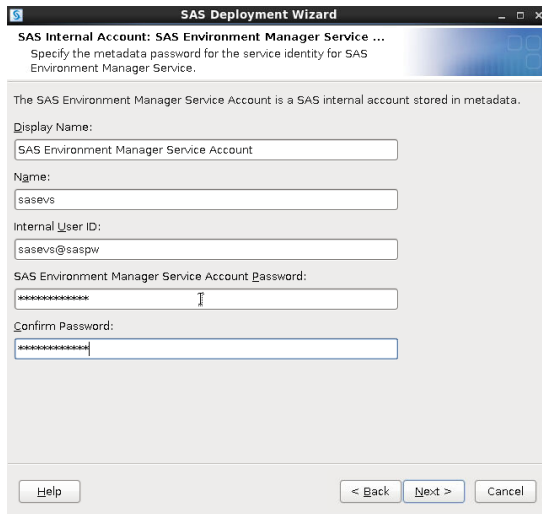
Display 84. SAS Environment Manager: Administration Database ID

Display 85. SAS Internal Account: SAS Environment Manager Service

Display 86. SAS Environment Manager: Configuration

Display 87. SAS Environment Manager: Database Configuration

Display 88. SAS Environment Manager Agent Configuration

Display 89. SAS Flex Application Themes

Display 90. SAS Visual Analytics High-Performance Configuration details

Display 91. SAS Visual Analytics Public Data Provider

Display 92. SAS Visual Analytics Data Library Information

Display 93. SAS Visual Analytics Autoload Location

39

Display 94. SAS Information Retrieval Studio

Display 95. Search Interface to SAS Content Feeder Configuration

Display 96. SAS Internal Account: Search Interface to SAS Content

Display 97. SAS Visual Analytics Administration: SAS LASR Analytic Server

Display 98. SAS Visual Analytics Services Database Credentials

Display 99. SAS Visual Analytics Transport Service: Mobile Whitelist
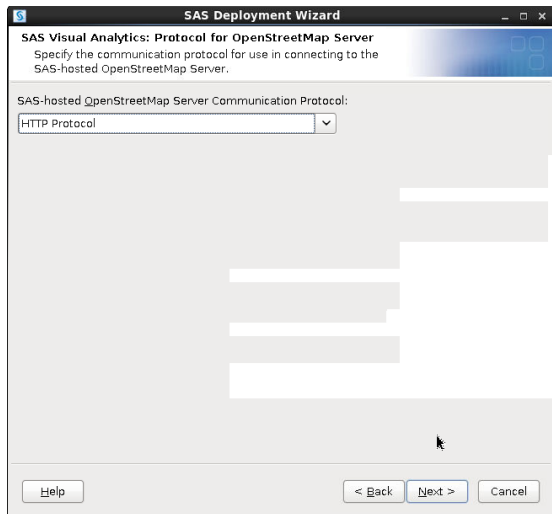
Display 100. SAS Visual Analytics: Protocol for OpenStreetMap Server
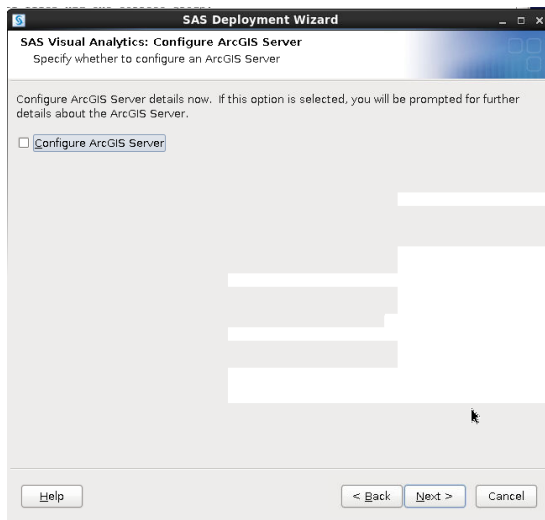
Display 101. SAS Visual Analytics: Configure ArcGIS Server
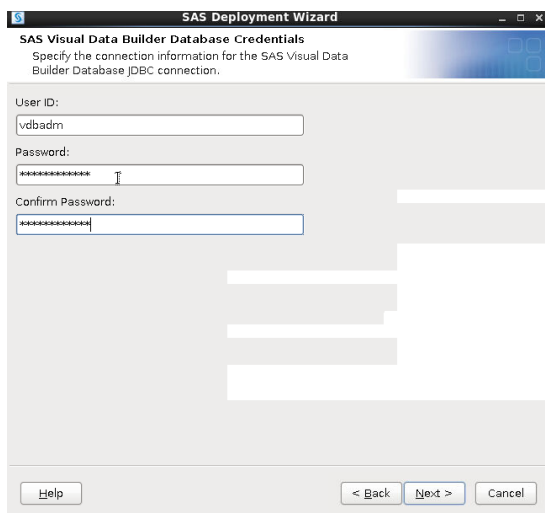
Display 102. SAS Visual Data Builder Database Credentials
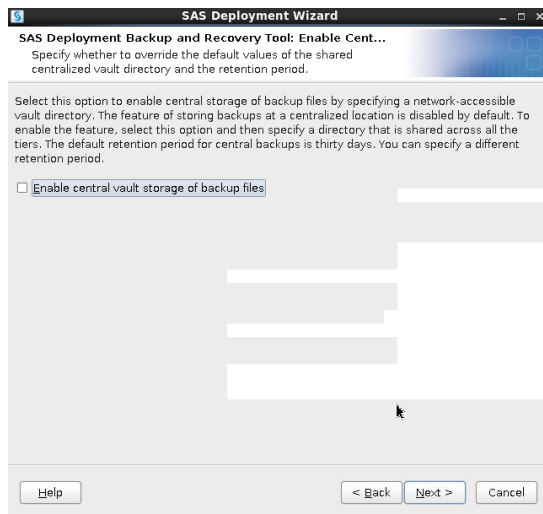
Display 103. SAS Deployment Backup and Recovery Tool: Enable Storage
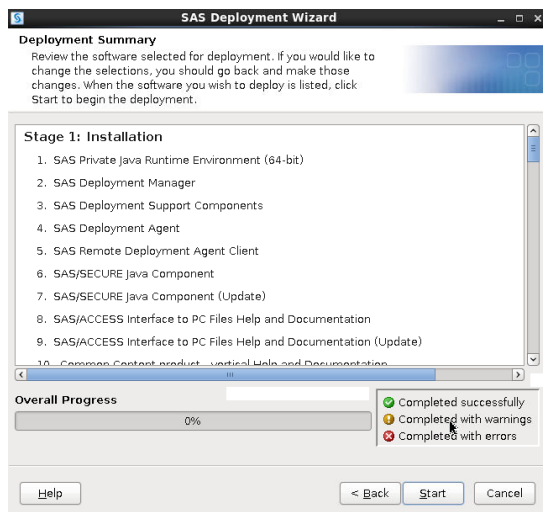
Display 104. Deployment Summary
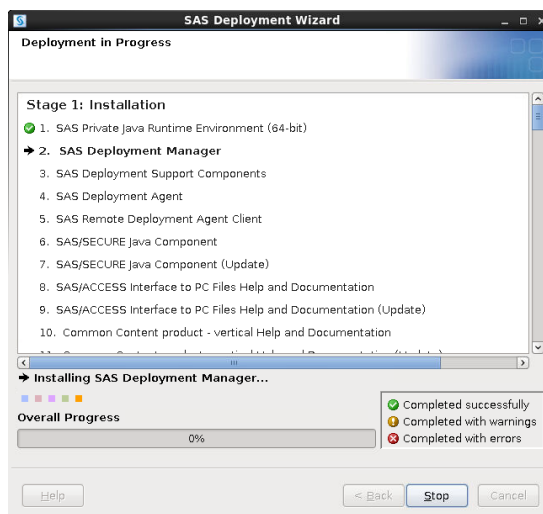
Display 105. Deployment in Progress (Installation steps occur in Stage 1)
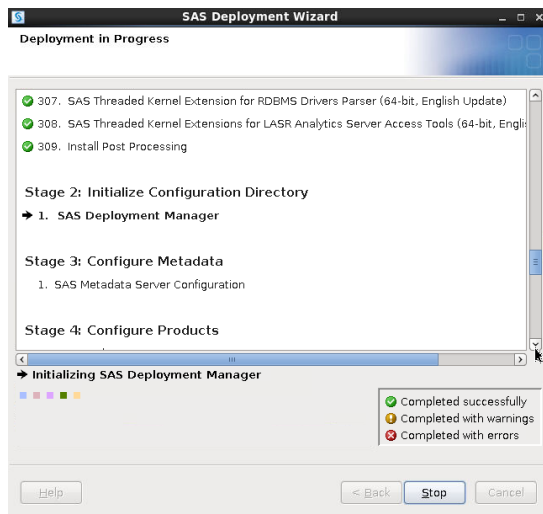
Display 106. Deployment in Progress (Configuration steps at Stage 2)

COMPLETE SAS® 9.4 POST-INSTALLATION TASKS AND CONFIGURATION

The last remaining to do items to complete the SAS installation have to do with both efficiencies as well as practical items such as how to connect to a few of the SAS® 9.4 software clients.

34. Complete all the tasks and validations that are required in *instructions.html*, which is produced at the end of SAS® 9.4 deployment wizard installation/configuration process. Also, maintain a copy in your records of *DeploymentSummary.html*.

35. Review the following logs in the directory, $HOME/.SASAppData/SASDeploymentWizard/9.4:

    SDW.log, SDW_<date>.log, sdwprefs.txt

36. Create a home directory for each user to store SAS data and programs. For example, create a directory named /users and add a sub-directory for all users individually. Provide appropriate read/write permissions for each user.

37. Change the temp file WORK location for SAS users logged onto SAS clients from its default /tmp location to another chosen directory location. Create that new directory and provide appropriate permissions for SAS software to write to that directory. Add a new line at the bottom of the sasv9.cfg file in /*sas_config_directory*/Lev1/SASApp:

    -work /*temp_files_work_dir*

40. Set appropriate SAS option settings [17] for the following:

    MEMSIZE, SORTSIZE, BUFFSIZE, IBUFFSIZE, UBUFFSIZE, SGIO, WORKTERM, WORKINIT

    These settings can be effected in the sasv9.cfg in /*sas_config_directory*/Lev1/SASMeta/MetadataServer

    The sub-optimal default for MEMSIZE, for example, is MAX. (max memory setting is not efficient)

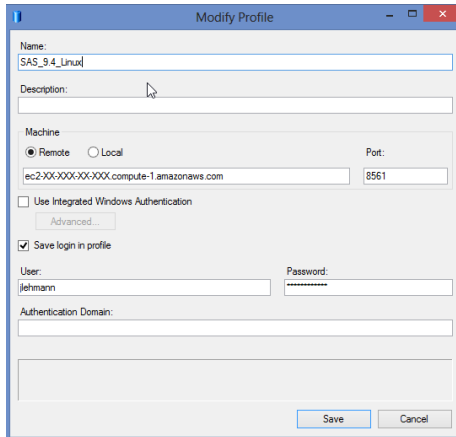41. Install and configure SAS® 9.4 clients on your laptop. Here is a sample configuration setup for SAS®
    Enterprise Guide 7.1:

    Name: **SAS9.4_Linux**   Port: **8561**

    Machine: **ec2-XX-XXX-XX-XXX.compute-1.amazonaws.com**

    (XX-XXX-XX-XXX is a mask for an IP Address. Your installation will have its own IP address)

Display 107. SAS® Enterprise Guide 7.1 client profile configuration

CONCLUSION

SAS administrators now have an additional, low-cost method to deploy a new test environment. The
AWS method of deployment allows for quick, autonomous implementation of SAS® 9.4 by an informed
SAS administrator. This paper's tactical, step-by-step perspective will hopefully be a helpful guide in
setting up an AWS cloud instance of SAS® 9.4 for those looking beyond an enterprise data center's
offerings.

REFERENCES

[1] "SAS® 9.4 Pre-installation Checklist for Ports." Available at:

http://support.sas.com/documentation/cdl/en/biig/63852/HTML/default/viewer.htm#n02027intelplatform00install.htm

[2] "Amazon Web Services Virtual Private Cloud User Guide." Available at:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

[3] "Amazon EC2 Key Pairs." Available at:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html

[4] "Internet Gateways." Available at:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html

[5] "Elastic IP Addresses (EIP)." Available at:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

[6] "PuTTY Download Page" Available at:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

[7] "WinSCP Downloads Page" Available at:

http://winscp.net/eng/download.php

[8] "Configuring VNC Server Access on a Redhat Linux" Available at:

http://linuxconfig.org/configuring-vnc-server-access-on-a-redhat-linux

[9] "TigerVNC 1.4.3" Available at:

https://github.com/TigerVNC/tigervnc/releases

[10] "Firefox-Free Download" Available at:

https://www.mozilla.org/en-US/firefox/new/?utm_source=firefox-com&utm_medium=referral

[11] "SAS Download Manager" Available at:

http://support.sas.com/downloads/package.htm?pid=1583

[12] "Pre-Installation Steps for the SAS® 9.4 Middle Tier" Available at:

http://support.sas.com/resources/thirdpartysupport/v94/appservers/preinstall.html

[13] "QuickStart Guide: SAS® 9.4 Planned Deployments using Electronic Software Delivery" Available at:

http://support.sas.com/documentation/installcenter/en/ikqsgplanesd/66210/PDF/default/quickstart.pdf

[14] "Installation Note 53997: Red Hat Enterprise Linux 7 is supported for SAS® 9.4 with restrictions" Available at:

http://support.sas.com/kb/53/997.html

[15] "How can I increase open files limit for all processes?" Available at:

http://unix.stackexchange.com/questions/8945/how-can-i-increase-open-files-limit-for-all-processes

[16] "SAS® 9.4 Support for Additional Software Products" Available at:

http://support.sas.com/resources/thirdpartysupport/v94/othersw.html

[17] "SAS® INSTALLATIONS: SO YOU WANT TO INSTALL SAS®?" Available at:

http://support.sas.com/resources/papers/proceedings14/1262-2014.pdf

[18] "AWS NAT Instance Basics" Available at:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html

 [19] "Set Up SSH Tunneling on a Linux / Unix / BSD Server To Bypass NAT" Available at:

http://www.cyberciti.biz/faq/set-up-ssh-tunneling-on-a-linux-unix-bsd-server-to-bypass-nat/

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Name:	Jeff Lehmann
Enterprise:	Slalom Consulting
E-mail:	jeffl@slalom.com

Twitter: @jefflehmann