



## Keeping your Archive Safe (and on TRAC) with SafeArchive and LOCKSS

Micah Altman <micah\_altman@alumni.brown.edu>

Jonathan Crabtree <jonathan\_crabtree@unc.edu>

Thu-Mai Christian <tlchristian@unc.edu>

Location 311

June 5, 2012 | 9:30am – 12:30pm

### Overview

---

This ½-day workshop focuses on how to protect your archival content, and how to formalize, document and audit storage policies. The workshop is appropriate for curators of content who wish to replicate their content and/or document storage policies for compliance with TRAC, Data Seal of Approval, and other archival standards. This provides hands-on practice with and example configurations for LOCKSS installation and configuration; SafeArchive installation and configuration, generating and interpreting policy reports, and TRAC documentation. At the end of the workshop the student will be able to install the SafeArchive system; use it to replicate archival content exposed through DVN, OAI-PMH or the web; and produce formal audits and reports to determine compliance with archival storage policies.

### Requirements

---

- Laptop computer with the latest version of Firefox installed
- Amazon Web Services account (please obtain an AWS account *prior* to the workshop event)

### Agenda

---

Introductions	9:30 – 9:45
Overview and Tour of the SafeArchive System	9:45 – 10:15
Hands On: Running the SafeArchive System using Amazon Web Services	10:15 – 11:00
Break	11:00 – 11:10
Hands On: Setting up the SafeArchive System	11:10 – 11:40
Hands On: Using the SafeArchive System	11:40 – 12:30

## Running the SafeArchive System Using Amazon Web Services

The SafeArchive System (SAAS) can easily be run using Amazon Web Services. While SAAS is free-to-use open source software, Amazon Web Services (AWS) charges a fee for web hosting and data storage services. For this workshop, you can expect to incur a minimal cost of less than \$5. *To avoid any additional fees, you must ensure that you terminate the service at the conclusion of the workshop.*

Amazon's Getting Started guide at <http://docs.amazonwebservices.com/AWSEC2/latest/GettingStartedGuide> may also be helpful as you set up the SAAS system using AWS.

### Launching the SafeArchive Amazon Machine Instance

The SafeArchive Installation begins in the AWS Management Console within Amazon Web Services. The instructions below provide guidance on launching and running the SafeArchive Amazon Machine Instance (AMI).

1. Launch a supported web browser such as Firefox.



2. Navigate to the Amazon Web Services homepage: <http://aws.amazon.com>. Sign in to the AWS Management console by clicking on the **My Account/Console** button and selecting **AWS Management Console**.

The screenshot shows the AWS homepage with the 'My Account / Console' dropdown menu open. A green arrow points to the 'AWS Management Console' option. The page includes a header with 'Sign Up' and 'My Account / Console' buttons, a main banner for 'Innovation. Powered by Amazon Web Services', and sections for 'Featured Events' (AWS re:Invent), 'Products & Services' (Compute, Database), and 'Recent News'.

3. Enter your e-mail address and Amazon password. If you do not have an Amazon account, you can create one for free by selecting "I am a new user."

If you have not yet signed up for AWS, a screen will appear that will instruct you through the process of signing up for AWS.

The screenshot shows the AWS 'Sign In or Create an AWS Account' page. The page has a heading 'Sign In or Create an AWS Account' and a sub-heading 'You may sign in using your existing Amazon.com account or you can create a new account by selecting "I am a new user."'. There is a text input field for 'My e-mail address is:' and two radio button options: 'I am a new user.' and 'I am a returning user and my password is:'. Below the radio buttons are a password input field, a 'Sign in using our secure server' button, and links for 'Forgot your password?' and 'Has your e-mail address changed?'. At the bottom, there is a link to 'Learn more about AWS Identity and Access Management and AWS Multi-Factor Authentication'.

4. Follow the SAAS AMI link <<https://console.aws.amazon.com/ec2/home?region=us-east-1#launchAmi=ami-e67ddc8f>> to request the SafeArchive Installation AMI. When the Request Instances Wizard dialog box appears, click on the **Continue** button.

The screenshot shows the 'Request Instances Wizard' dialog box in the AWS Management Console, specifically the 'CHOOSE AN AMI' step. The wizard has four steps: 'CHOOSE AN AMI', 'INSTANCE DETAILS', 'CREATE KEY PAIR', and 'CONFIGURE FIREWALL'. The 'CHOOSE AN AMI' step is active. Below the step indicators, there is a note: 'The bookmark that was activated refers to the AMI below. Please review...'. Under the heading 'AMI Details', the following information is displayed: Image Id: ami-62ce6f0b, Owner: 707773282281, Manifest: 707773282281/SafeArhivePreInstall, Platform: Other Linux, Architecture: i386, Root Device Type: ebs. Below this, under 'Attached Block Devices', a table shows a device named '/dev/sda1' with a volume size of 6 GB. At the bottom right of the dialog box is a 'Continue' button with a right-pointing arrow.

5. In the Instance Details step of the Request Instances Wizard, change the Instance type to "Small (m1.small, 1.7GB)." Click on the **Continue** button.

The screenshot shows the 'Request Instances Wizard' dialog box in the AWS Management Console, specifically the 'INSTANCE DETAILS' step. The wizard has four steps: 'CHOOSE AN AMI', 'INSTANCE DETAILS', 'CREATE KEY PAIR', and 'CONFIGURE FIREWALL'. The 'INSTANCE DETAILS' step is active. Below the step indicators, there is a note: 'Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.' Below this, there are two fields: 'Number of Instances:' with a value of 1, and 'Instance Type:' with a dropdown menu set to 'Small (m1.small, 1.7 GB)'. A green arrow points to this dropdown menu. Below these fields, there are two radio button options: 'Launch Instances' (selected) and 'Request Spot Instances'. Under 'Launch Instances', there is a sub-section 'Launch into:' with a radio button for 'EC2' and a dropdown for 'Availability Zone:' set to 'No Preference'. At the bottom left is a '< Back' button and at the bottom right is a 'Continue' button with a right-pointing arrow.

6. On the next screen, keep the default settings. Click on the **Continue** button.

The screenshot shows the 'Request Instances Wizard' dialog box in the AWS Management Console, specifically the 'CONFIGURE FIREWALL' step. The wizard has four steps: 'CHOOSE AN AMI', 'INSTANCE DETAILS', 'CREATE KEY PAIR', and 'CONFIGURE FIREWALL'. The 'CONFIGURE FIREWALL' step is active. Below the step indicators, there is a note: 'Here you can choose a specific kernel or RAM disk to use with your instances. You can also choose to enable CloudWatch Detailed Monitoring or enter data that will be available from your instances once they launch.' Below this, there are two dropdown menus: 'Kernel ID:' set to 'Use Default' and 'RAM Disk ID:' set to 'Use Default'. Below these, there is a 'Monitoring:' section with a checkbox 'Enable CloudWatch detailed monitoring for this instance (additional charges will apply)'. Below that is a 'User Data:' section with two radio buttons: 'as text' (selected) and 'as file', and a checkbox 'base64 encoded'. Below that is a 'Termination Protection:' section with a checkbox 'Prevention against accidental termination.' and a 'Shutdown Behavior:' dropdown set to 'Stop'. Below the 'Shutdown Behavior:' dropdown is a note: 'Choose the behavior when the instance is shutdown from within the instance.' At the bottom left is a '< Back' button and at the bottom right is a 'Continue' button with a right-pointing arrow.

7. Enter a Value for the “Name” Key, which will be used to identify your SAAS instance. Click on the **Continue** button.

**Request Instances Wizard** [Cancel]

CHOOSE AN AMI | **INSTANCE DETAILS** | CREATE KEY PAIR | CONFIGURE FIREWALL | REVIEW

Add tags to your instance to simplify the administration of your EC2 infrastructure. A form of metadata, tags consist of a case-sensitive key/value pair, are stored in the cloud and are private to your account. You can create user-friendly names that help you organize, search, and browse your resources. For example, you could define a tag with key = Name and value = WebsERVER. You can add up to 10 unique keys to each instance along with an optional value for each key. For more information, go to [Using Tags in the EC2 User Guide](#).

Key (127 characters maximum)	Value (255 characters maximum)	Remove
Name	SafeArchive	✖
		✖

Add another Tag. (Maximum of 10)

< Back [Continue]

8. The SAAS Installer has been programmed to operate without the need for a new Key Pair. Select “Proceed without a Key Pair.” Click on the **Continue** button.

**Request Instances Wizard** [Cancel]

CHOOSE AN AMI | INSTANCE DETAILS | **CREATE KEY PAIR** | CONFIGURE FIREWALL | REVIEW

Public/private key pairs allow you to securely connect to your instance after it launches. To create a key pair, enter a name and click **Create & Download your Key Pair**. You will then be prompted to save the private key to your computer. Note, you only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance.

Choose from your existing Key Pairs

Create a new Key Pair

**Proceed without a Key Pair**

I do not want a keypair installed on this instance.

**NOTE:** You will not be able to connect to this instance unless you already know the password built in to this AMI.

< Back [Continue]

9. In the Configure Firewall step of the Request Instances Wizard, select the default Security Group. Click on the **Continue** button.

**Request Instances Wizard** [Cancel]

CHOOSE AN AMI | INSTANCE DETAILS | CREATE KEY PAIR | **CONFIGURE FIREWALL** | REVIEW

Security groups determine whether a network port is open or blocked on your instances. You may use an existing security group, or we can help you create a new security group to allow access to your instances using the suggested ports below. Add additional ports now or update your security group anytime using the Security Groups page.

**Choose one or more of your existing Security Groups**

sg-414bf929 - default

(Selected groups: sg-414bf929)

Create a new Security Group

< Back [Continue]

10. Click on the **Launch** button to accept your settings and proceed.

The screenshot shows the 'Request Instances Wizard' dialog box with the 'REVIEW' step selected. The wizard contains the following configuration details:

- AMI:** Other Linux AMI ID ami-62ce6f0b (i386) [Edit AMI]
- Number of Instances:** 1
- Availability Zone:** No Preference
- Instance Type:** Small (m1.small)
- Instance Class:** On Demand [Edit Instance Details]
- Monitoring:** Disabled
- Termination Protection:** Disabled
- Tenancy:** Default
- Kernel ID:** Use Default
- Shutdown Behavior:** Stop
- RAM Disk ID:** Use Default
- User Data:** [Edit Advanced Details]
- Key Pair Name:** No Key Pair [Edit Key Pair]
- Security Group(s):** sg-414bf929 [Edit Firewall]

At the bottom of the dialog, there is a 'Back' link and a 'Launch' button.

11. The SAAS Instance request process is now complete. **Close** the Launch Instance Wizard dialogue box.

The screenshot shows the 'Launch Instance Wizard' dialog box with a green checkmark and the message: 'Your instances are now launching.' Below this, there is a note: 'Your instances may take a few minutes to launch, depending on the software you are running. Note: Usage hours on your new instance will start immediately and continue to accrue until you stop or terminate your instance.' A link is provided: '> View your instances on the Instances page'.

Below the message, there is a section titled 'Other AWS Features' with three columns of information:

- Spot Instances:** Spot Instances enable customers to lower their Amazon EC2 costs by up to 75% by bidding on unused capacity and running instances for as long as the maximum bid exceeds the current Spot Price. [Go to Amazon EC2 Spot Instances]
- Reserved Instances:** Reserved Instances provide substantial savings over On-Demand instances and ensure that the capacity you need is available to you when required. [Go to Amazon EC2 Reserved Instances]
- Suse Linux Instances:** Suse Linux instances are a proven platform with superior reliability and security and are automatically kept up to date with Novell's security patches, bug fixes and new features. [Go to Amazon EC2 running SUSE Linux]

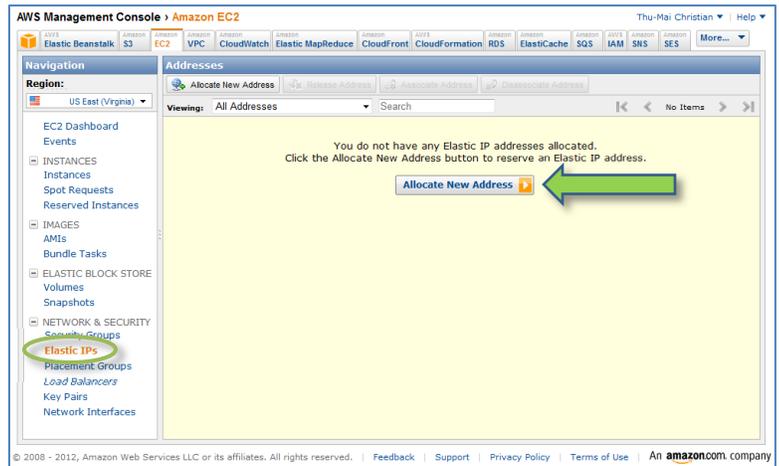
At the bottom of the dialog, there is a 'Close' button.

## Configuring and Installing the SafeArchive AMI

Once the SafeArchive AMI is running, it will need to be associated with an IP address and TCP ports must be specified prior to running the SafeArchive Installer. The instructions below provide guidance on completing these required tasks.

1. [Creating an Elastic IP](#)
2. [Setting up Security Groups](#)
3. [Running the SAAS Installer](#)

1. Your SAAS installation requires that an IP address be associated with the instance. To generate an IP address, click on the **Elastic IPs** link in the Navigation panel on the left-hand side of the screen. Click on the **Allocate New Addresses** button at the top of the Addresses panel.

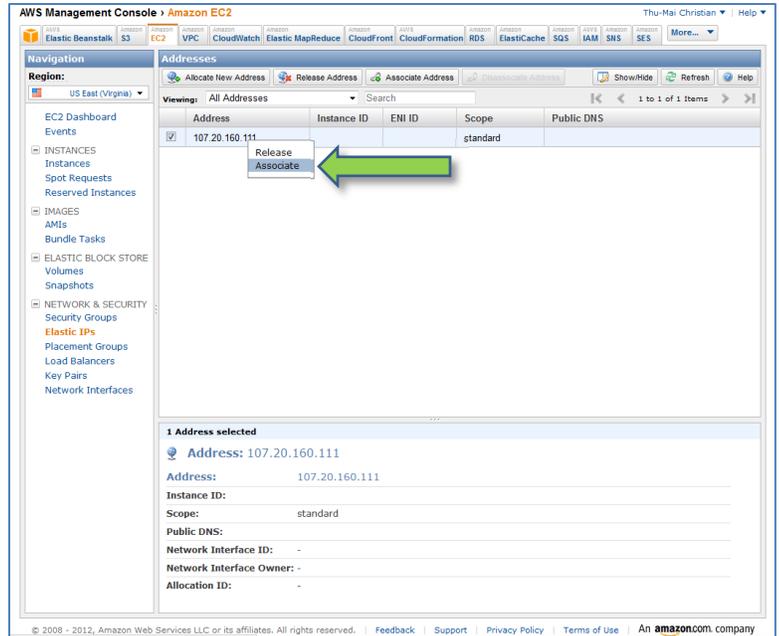


A dialogue box will appear to confirm the IP allocation action. Click on the **Yes, Allocate** button.

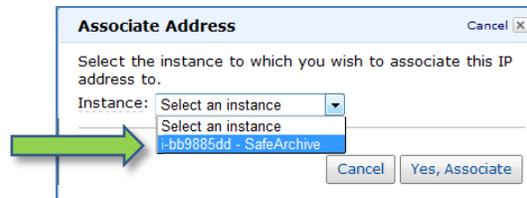


Associate your new elastic IP by right-clicking on the IP address you just generated. Select **Associate**.

Record your new Elastic IP Address here:



A dialogue box will appear, which allows you to select the instance to which the IP address will be associated. Click on the SafeArchive AMI. Click on the **Yes, Associate** button.

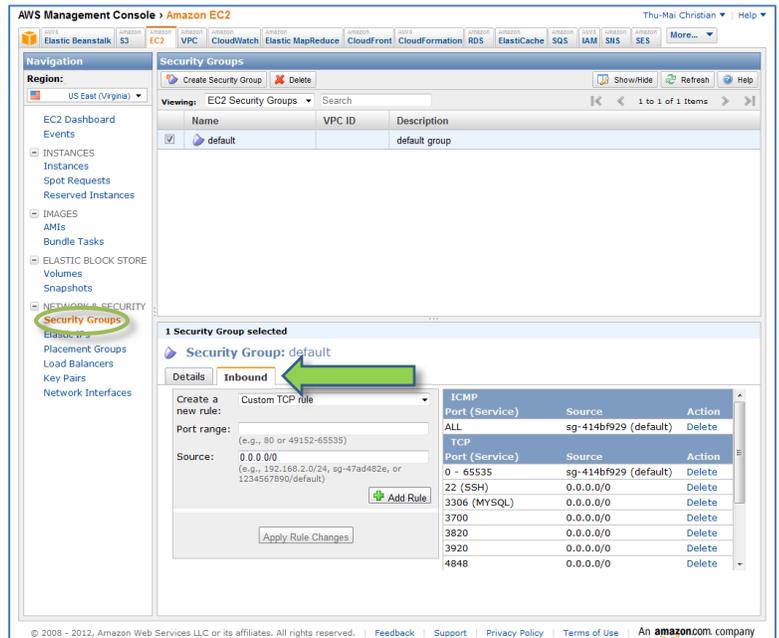


- Running SAAS requires several TCP ports to be open. To specify these ports, click on the **Security Groups** link in the Navigation panel on the left-hand side of the screen. Check the box to the left of your designated security group (the "default" security group will be used for the workshop). In the panel below, click on the **Inbound** tab. In the **Port range** field, enter the port number. Click on the **+Add Rule** button. Complete this process for each of the 8 ports listed in the box below.

22	3306	3700	3820
3920	4848	8080	8686

TCP ports for SAAS installation

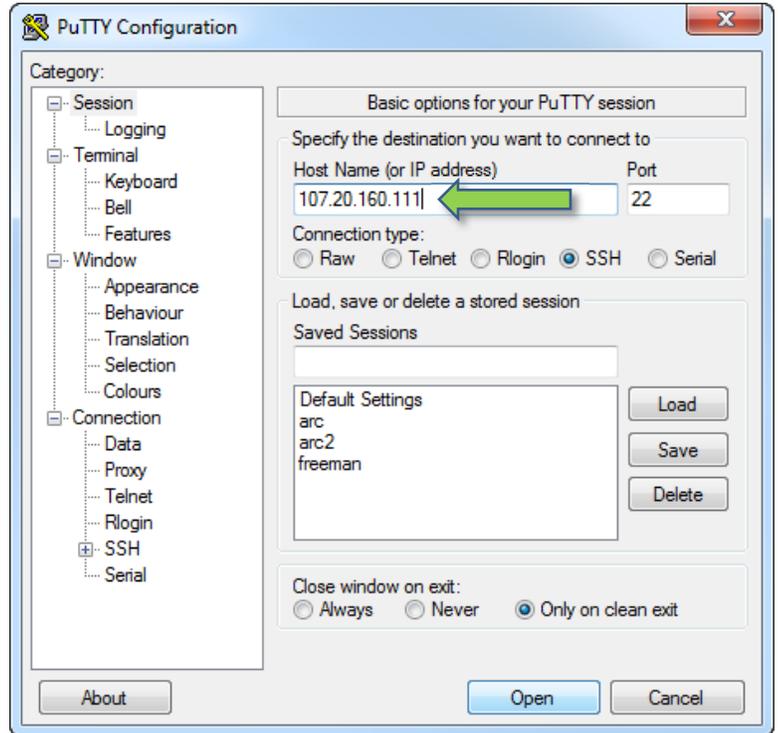
When you have added all of the ports, click on the **Apply Rule Changes** button.



3. To run the SAAS installer, open PuTTY.exe.



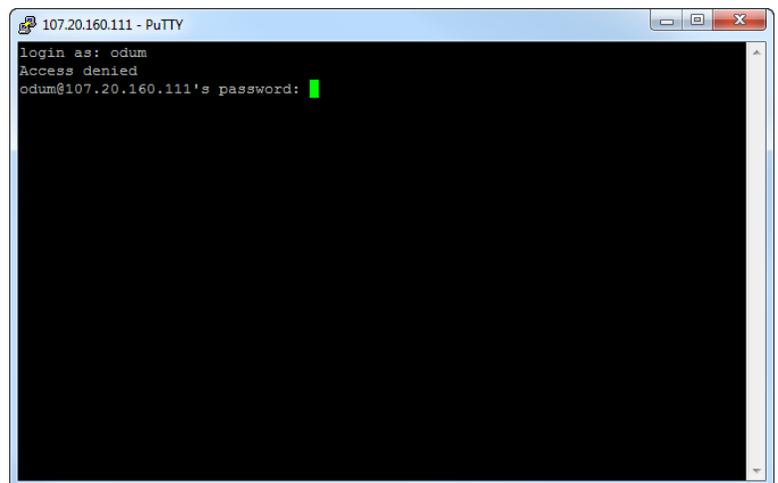
In PuTTY, enter the elastic IP address you allocated in the AWS Management Console in the Host Name (or IP address) field. Click on the **Open** button.



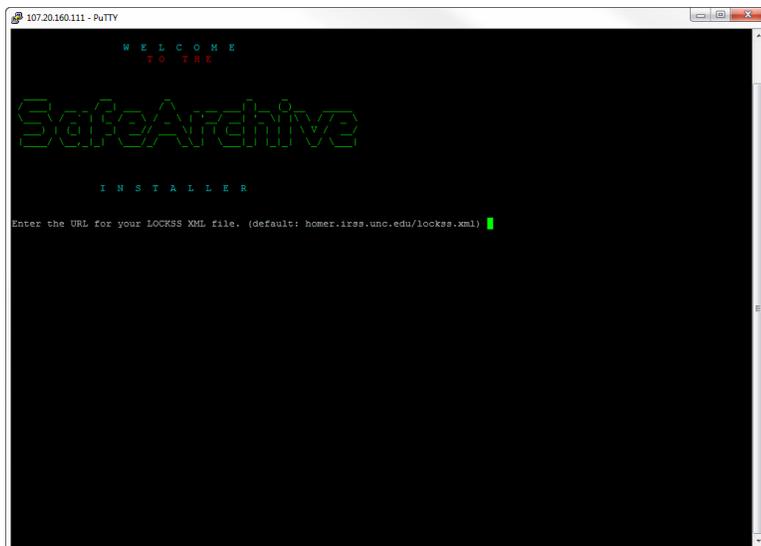
PuTTY will launch a shell script that will prompt you for a login and password. Enter the following information:

**login: odum**  
**password: odum**

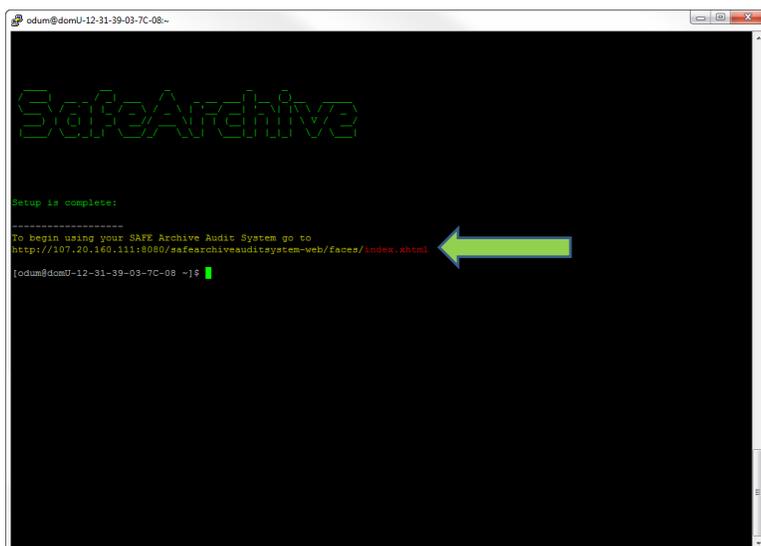
*SAAS Installer login & password*



The SafeArchive installer will prompt you for a series of inputs to configure the SafeArchive System. Default inputs are provided. To accept the default, press the enter key at the prompt.



Once the system has loaded all necessary applications and configurations, the installer will indicate that Setup is complete. A URL is provided, which links to your SafeArchive instance. Enter this URL into a Firefox browser address bar to launch the SafeArchive System.



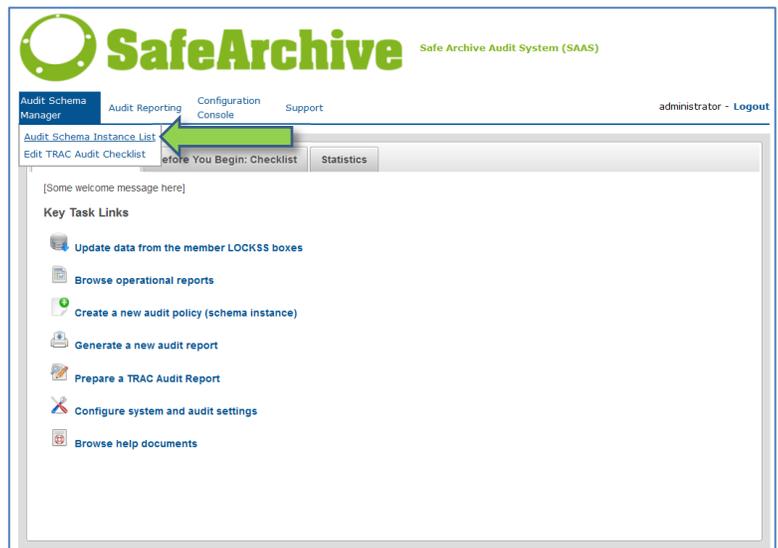
## Setting Up the SafeArchive System

This section of the workshop will enable you to complete the following tasks:

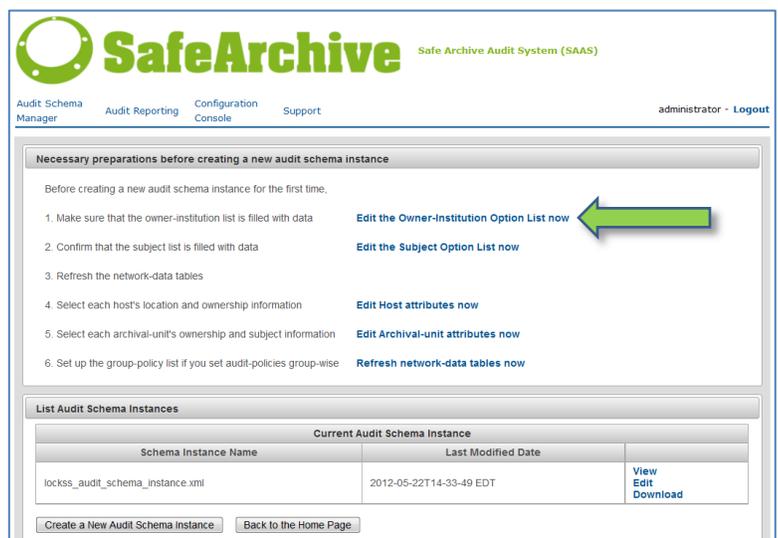
1. [Navigating to the Audit Schema Instance List page](#)
2. [Adding your owner-institution name](#)
3. [Specifying subject terms](#)
4. [Refreshing the network data status tables](#)
5. [Adding an archival unit](#)

Prior to using the SAAS, several steps must be completed. These steps include establishing your owner-institution, providing a subject list, adding hosts and archival units, editing host and archival unit information, and refreshing the network status data tables. The instructions below provide guidance on accomplishing these required tasks.

1. Navigate to the Audit Schema Instance List page by selecting the **Audit Schema Instance List** link in the **Audit Schema Manager** menu at the top of the screen.



2. Add your owner-institution name to the system by clicking on the **Edit the Owner-Institution Option List now** link.



In the **New owner** field, enter your owner-institution name. Click on the **Add** button. Once your institution appears in the table, enter text in the optional fields next to your Institution Name. **Click on the Save** the list button. Return to the Audit Schema Instance List page.

**SafeArchive** Safe Archive Audit System (SAAS)

Audit Schema Manager | Audit Reporting | Configuration Console | Support | administrator - Logout

**Edit the Owner-Institution List**

Institution Name	Institution Short Name	Institution code	Note	
HU-IQSS				Remove
Stanford				Remove
UNC-Odum Institute				Remove
UConn-Roper				Remove
UMich-ICPSR				Remove
required	optional	optional	optional	

**Add a new owner-institution**

To add a new owner-institution to the above table, type its name in the box below and click the Add button; and then provide or select additional information in the table and click the Save button below.

New owner: Owner Name

[Back To Audit Schema Instance List](#) [Go To System Configuration Top Page](#)

- The Subject Option List allows you to specify subject terms used to describe archival units. To edit and/or add subject terms, click on the **Edit the Subject Option List** now link on the Audit Schema Instance List page. Add a new subject by entering a term in the **New subject** field. Your term will appear in the Subject List table after you click on the **Add** button. Click on **the Save the list** button to save your updated Subject List table. Return to the Audit Schema Instance List page.

**SafeArchive** Safe Archive Audit System (SAAS)

Audit Schema Manager | Audit Reporting | Configuration Console | Support | administrator - Logout

**Edit the Subject List**

Subject	
-unclassified-	Remove
Agriculture	Remove
Archaeology, Heraldry, Biography	Remove
Bibliography, Library Science	Remove
Criminal Law	Remove
Education	Remove
Fine Arts	Remove
General Works	Remove
Geography, Anthropology, and Recreation	Remove
History: Old World and General	Remove
required	

**Add a new subject**

To add a new subject to the above table, type its name in the box below and click the Add button, and then click the Save button below.

New subject: New Subject

[Back To Audit Schema Instance List](#) [Go To System Configuration Top Page](#)

4. Refresh the network data tables. From the Audit Reporting menu option at the top of the screen, select **Detailed Network Status Data**. Click on the **Refresh Tables** button. Log out of the SAAS and log in again.

The screenshot shows the 'List Network-Status Data Tables' section of the SafeArchive SAAS interface. At the top, there is a navigation bar with 'Audit Schema Manager', 'Audit Reporting', 'Configuration Console', and 'Support'. The user is logged in as 'administrator'. Below the navigation bar, there is a table titled 'Network-Status Data Tables' with columns for 'Table Name' and 'Show Table'. The table lists several tables: lockss\_box\_table, archival\_unit\_status\_table, repository\_space\_table, au\_overview\_table, crawl\_status\_table, polls\_table, and successful\_polls\_table. Below the table, there is a 'Refresh Network-Status Data Tables' section with instructions: '1 Click the refresh button below.', '2 Wait for the refresh-completion message.', and '3 Log out and log in again.' A green arrow points to the 'Refresh Tables' button.

5. Add a new archival unit by clicking on the **Edit Archival-unit attributes now** link on the Audit Schema Instance List page. Enter the name of the archival unit in the **New AU Name** field. Click on the **Add** button.

The screenshot shows the 'Edit Archival-Unit Attributes' section of the SafeArchive SAAS interface. At the top, there is a navigation bar with 'Audit Schema Manager', 'Audit Reporting', 'Configuration Console', and 'Support'. The user is logged in as 'administrator'. Below the navigation bar, there is a table titled 'Archival-Unit Attributes' with columns for 'Archival Unit Name', 'AU Short Name', 'Owner Institution', 'Subject', 'FISMA Confidentiality', 'FISMA Integrity', 'FISMA Availability', and 'Remove'. The table lists several archival units, including ICPSR Archival U, IQSS Dataverse, and Roper's Data-PA. Below the table, there is an 'Add a new archival unit' section with instructions: 'To add a new archival unit (AU) to the above table, type its name in the box below and click the Add button; and then provide or select additional information in the table and click the Save button below.' A green arrow points to the 'New AU Name' input field.

Once the new archival unit appears in the table, you can enter an AU Short Name by entering text into the text field next to your archival unit name. You may also specify the Owner Institution, Subject, and levels of FISMA Confidentiality, Integrity, and Availability by selecting from the option in the drop down boxes next to your archival unit name. Click on the **Save the table** button to save your selections.

**SafeArchive** Safe Archive Audit System (SAAS)

Audit Schema Manager | Audit Reporting | Configuration Console | Support | administrator - Logout

### Edit Archival-Unit Attributes

Archival Unit Name	AU Short Name	Owner Institution	Subject	FISMA Confidentiality	FISMA Integrity	FISMA Availability	
ICPSR Archival U		UMich-ICF	-unclassif	low	low	low	Remove
ICPSR Archival U		UMich-ICF	-unclassif	low	low	low	Remove
ICPSR Archival U		UMich-ICF	-unclassif	low	low	low	Remove
ICPSR Archival U		UMich-ICF	-unclassif	low	low	low	Remove
ICPSR Archival U		UMich-ICF	-unclassif	low	low	low	Remove
ICPSR Archival U		UMich-ICF	-unclassif	low	low	low	Remove
ICPSR Archival U		UMich-ICF	-unclassif	low	low	low	Remove
ICPSR Archival U		UMich-ICF	-unclassif	low	low	low	Remove
ICPSR Archival U		UMich-ICF	-unclassif	low	low	low	Remove
ICPSR Archival U		UMich-ICF	-unclassif	low	low	low	Remove
IQSS Dataverse		HU-IQSS	-unclassif	low	low	low	Remove
Index of /lockss/p		HU-IQSS	-unclassif	low	low	low	Remove
Odum Dataverse		UNC-Odu	-unclassif	low	low	low	Remove
Roper's Data-PA		HU-IQSS	-unclassif	low	low	low	Remove
	required	optional	optional				

**Add a new archival unit**

To add a new archival unit (AU) to the above table, type its information in the table and click the Save button below.

New AU Name:

If the drop-down list for subjects does not include one you are looking for, click the following link to edit the list: [Edit the Subject List](#)

If the drop-down list for owner institutions does not include one you are looking for, click the following link to edit the list: [Edit the Owner-Institution List](#)

[Back To Audit Schema Instance List](#) [Go To System Configuration Top Page](#)

## Creating Preservation Policies

This section of the workshop will enable you to complete the following tasks:

1. [Establishing Network Audit Policy](#)
2. [Completing the TRAC Audit Checklist](#)

The process of creating an audit schema involves the consideration of several aspects of your PLN, hosts, and archival units. The SAAS presents several questions about each to assist with determining the audit policy appropriate for the collections in your network. The SAAS also offers a TRAC Checklist form, which stores your responses to TRAC criteria in a table. TRAC Audit reports indicate the degree to which the checklist has been completed. Follow the steps below to create network audit policy and to complete the TRAC Audit checklist.

1. From the Audit Schema Instance List page, click on the **Create a New Audit Schema Instance** button.



The screenshot displays the SafeArchive SAAS interface. At the top, the logo for SafeArchive is visible, along with the text 'Safe Archive Audit System (SAAS)'. Below the logo, there are navigation links: 'Audit Schema Manager', 'Audit Reporting Console', 'Configuration Console', and 'Support'. The user is logged in as 'administrator' and can click 'Logout'.

The main content area is divided into two sections. The first section is titled 'Necessary preparations before creating a new audit schema instance'. It contains a list of six steps, each with a corresponding link to edit or refresh data:

1. Make sure that the owner-institution list is filled with data. [Edit the Owner-institution Option List now](#)
2. Confirm that the subject list is filled with data. [Edit the Subject Option List now](#)
3. Refresh the network-data tables. [Refresh network-data tables now](#)
4. Select each host's location and ownership information. [Edit Host attributes now](#)
5. Select each archival-unit's ownership and subject information. [Edit Archival-unit attributes now](#)
6. Set up the group-policy list if you set audit-policies group-wise. [Refresh network-data tables now](#)

The second section is titled 'List Audit Schema Instances'. It contains a table with the following data:

Current Audit Schema Instance		
Schema Instance Name	Last Modified Date	
lockss_audit_schema_instance.xml	2012-05-22T14:33:49 EDT	<a href="#">View</a> <a href="#">Edit</a> <a href="#">Download</a>

Below the table is a button labeled 'Create a New Audit Schema Instance', which is highlighted by a green arrow.

The Create Audit Schema Instance page contains a series of questions about your network. Each input field corresponds to a question that asks about a specific aspect of your audit policy. Enter your responses to each question in the appropriate fields. Click on the **Save the Audit Schema Instance** button to save your new audit schema.


Safe Archive Audit System (SAAS)

Audit Schema Manager
Audit Reporting
Configuration Console
Support
administrator - Logout

---

### Create Audit Schema Instance

**About the PLN**

Question 1: What is the name of the private LOCKSS network (PLN) that you would like the SAFE system to audit?

Question 2: What is the email address of the PLN administrator?

**About PLN member Hosts**

Question 3: How much storage disk space do you wish to commit on each server for the SAFE system to use (in gigabytes)?

<input type="checkbox"/>	host Name	host Ip Address	Repository Capacity (Gb)	Space Committed (Gb)	Geographic Location
<input checked="" type="checkbox"/>	lockss-3.ropercenter.uconn.edu	137.99.36.160	1740.8	1740	Connecticut
<input checked="" type="checkbox"/>	lockss.hmdc.harvard.edu	140.247.115.220	39.0	30	Massachusetts
<input checked="" type="checkbox"/>	lockss-0.icpsr.umich.edu	141.211.146.29	120.0	120	Michigan
<input checked="" type="checkbox"/>	lockss-1.icpsr.umich.edu	141.211.146.62	1843.2	1843	Michigan
<input checked="" type="checkbox"/>	lockss-2.icpsr.umich.edu	141.211.146.63	1843.2	1843	Michigan
<input checked="" type="checkbox"/>	fong.jss.unc.edu	152.2.32.205	9113.6	9113	North Carolina
<input checked="" type="checkbox"/>	haar.jss.unc.edu	152.2.32.207	9113.6	9113	North Carolina

The above table shows discovered servers only. To add a missing server or update a host's attributes, click the following link:  
[Edit the Host List](#)

**About Archival Units**

Note: Before preservation content can be audited, it must be placed on a Host as an Archival unit or AU. If your content is not listed below in an AU, click the following link to add it to a LOCKSS host:  
[Edit the Host List](#)

Question 4: The following AUs have been found on the specified hosts. Please check the archival units you would like to audit and answer the following questions in respective columns of the table below:

4.1 How frequently should this archival unit AU be re-crawled (in days)? Re-crawling adds new content to the AUs as changes occur keeping your preservation copies current this is the Update Frequency.

4.2 What is the maximum size that you expect this archival unit AU to be (in gigabytes)? The default value is the current size. Please add your growth expectations. This is your storage required.

Question 5a: How many preservation copies of each collection do you want to maintain? This will be the Number of Replicates.

Question 5b: How many regions do you want to maintain a replica of a collection? This will be the value of Geographic Redundancy.

Question 6: Archival Units AUs will be tested on a regular basis for problems to ensure your content is not corrupt. What is the maximum time you would allow between these verifications, in days? This is your Verification Frequency.

Question 7: What is the maximum amount of time that the preservation system should take to ingest/crawl your content (in days)? LOCKSS uses crawling to add your content to an AU. The maximum number of days this should take is your Update Duration.

The following table lists major PLN-bound parameters:

PLN-bound Parameter	Current Value	Related Questions
Crawling Cycle	14 days	Q4.1, Q6, Q7
Quorum	5	Q5, Q5a
Member Hosts	7	Q5, Q5a
Max. Regions	7	Q5a

<input type="checkbox"/>	Archival Unit Name	Update Frequency	Storage Required (Gb)	Number of Replicates	Geographic Redundancy	Verification Frequency	Update Duration
<input checked="" type="checkbox"/>	ICPSR Archival Unit (14999)	7	67	3	2	21	21
<input checked="" type="checkbox"/>	ICPSR Archival Unit (10000-)	7	123	3	2	21	21
<input checked="" type="checkbox"/>	ICPSR Archival Unit (15810-15819)	7	6	3	2	21	21
<input checked="" type="checkbox"/>	ICPSR Archival Unit (18220-18229)	7	6	3	2	21	21
<input checked="" type="checkbox"/>	ICPSR Archival Unit (13530-13539)	7	5	3	2	21	21
<input checked="" type="checkbox"/>	ICPSR Archival Unit (18540-18549)	7	6	3	2	21	21
<input checked="" type="checkbox"/>	ICPSR Archival Unit (18550-18559)	7	6	3	2	21	21
<input checked="" type="checkbox"/>	ICPSR Archival Unit (13560-13569)	7	28	3	2	21	21
<input checked="" type="checkbox"/>	ICPSR Archival Unit (5000-9999)	7	66	3	2	21	21
<input checked="" type="checkbox"/>	Index of lockss/plugins	7	1	3	2	21	21
<input checked="" type="checkbox"/>	IQSS Dataverse	7	96	3	2	21	21
<input checked="" type="checkbox"/>	Odum Dataverse	7	62	3	2	21	21
<input checked="" type="checkbox"/>	Roper's Data-PASS subset	7	2	3	2	21	21

To update or correct an AU's subject or ownership information, click the following link:  
[Edit the Archival-Unit List](#)

**About Audit Reporting**

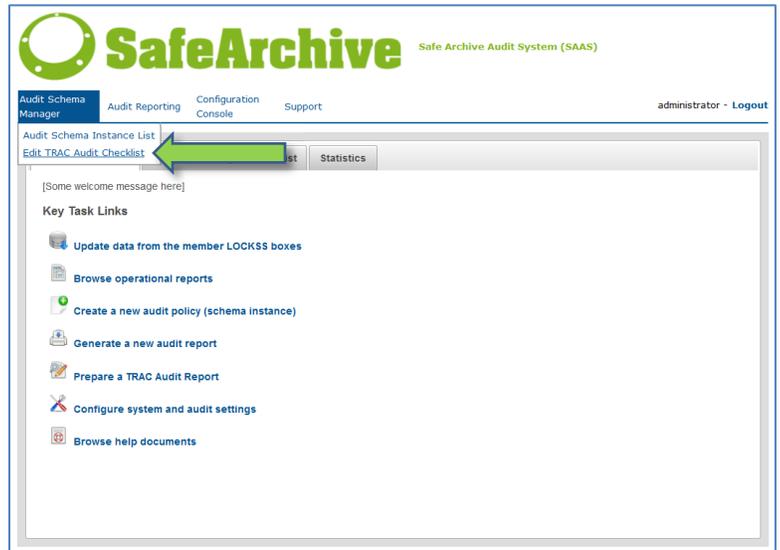
Question 8: How often should audit reports of the LOCKSS network be generated (in days)?

Daily  
 Weekly: Sunday  
 Biweekly: 14th/last days  
 Monthly: last day  
 Bimonthly: Feb, Apr, Jun, Aug, Oct, Dec  
 Quarterly: Mar, Jun, Sep, Dec  
 Biannual: Jun, Dec  
 Annual: Dec

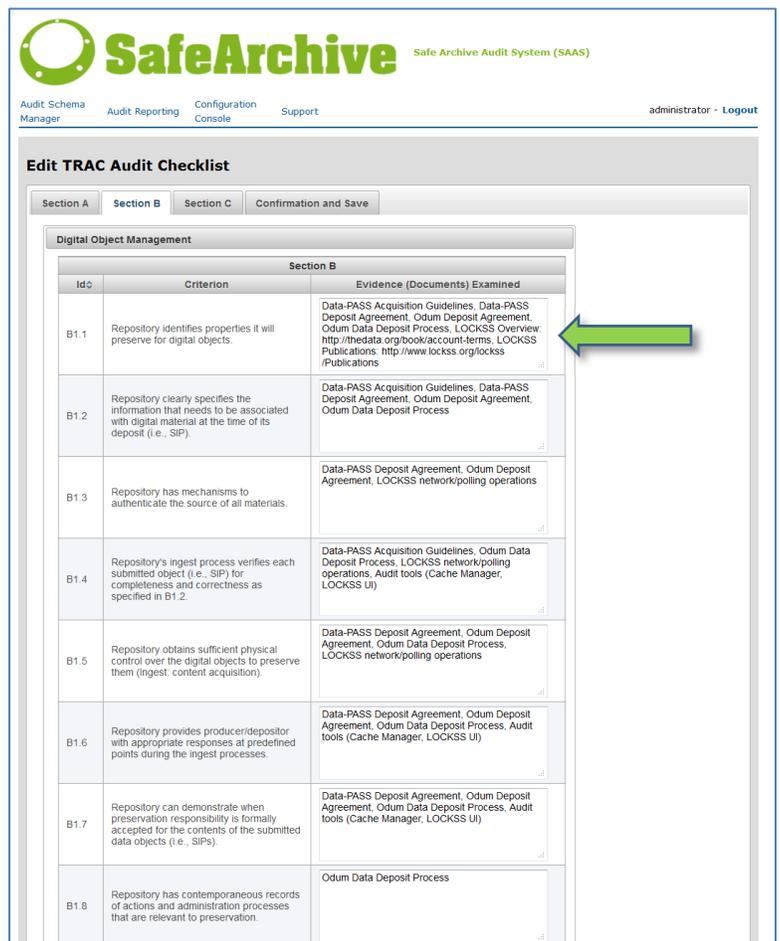
Question 9: The completed audit report will be stored for future review, but it will also be sent to an archivist. Please give an email address that LOCKSS network audit reports should be sent.

[Save this Audit Schema Instance](#)
[Back To Audit Schema Instance List](#)

- To generate a TRAC Audit report, you must first complete the TRAC Audit Checklist. To do this, click on the **Edit TRAC Audit Checklist** link in the Audit Schema Manager menu option



A table will display that includes tables for each of three sections of the checklist. Enter the evidence in the field that addresses each of the TRAC criterion. Click on the section tabs to fill in information for all three sections.



When you have entered data into each of the fields, click on the **Confirmation and Save** tab and click on the **Save the TRAC audit checklist** button.

The screenshot displays the SafeArchive web application interface. At the top left is the SafeArchive logo, and to its right is the text "Safe Archive Audit System (SAAS)". Below the logo are navigation links: "Audit Schema Manager", "Audit Reporting", "Configuration Console", and "Support". In the top right corner, the user is identified as "administrator - Logout". The main content area is titled "Edit TRAC Audit Checklist" and contains four tabs: "Section A", "Section B", "Section C", and "Confirmation and Save". The "Confirmation and Save" tab is active. Within this tab, there are three buttons: "Save the TRAC audit checklist" (highlighted with a green arrow), "Reset the TRAC Checklist", and a link "Back to the Home Page".

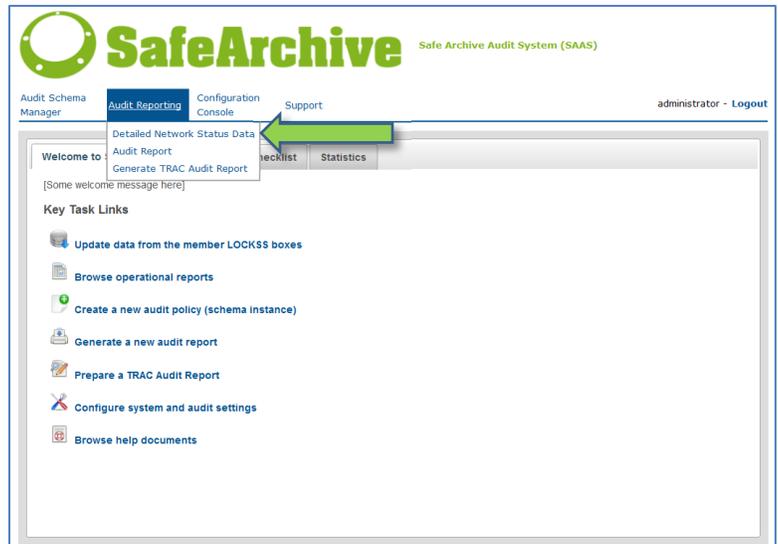
## Using the SafeArchive System

This section will enable you to complete the following tasks:

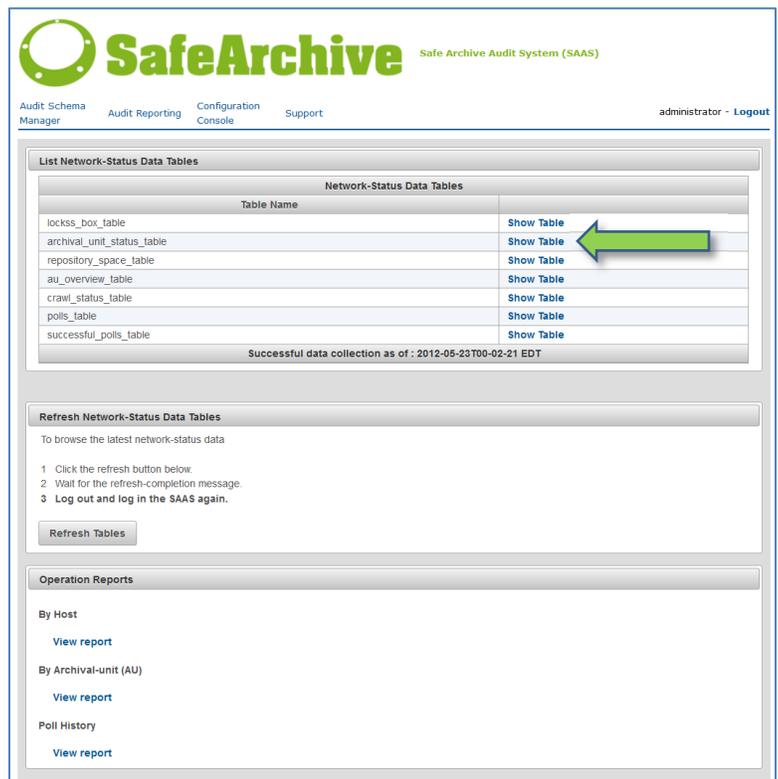
1. [Viewing detailed network status data](#)
2. [Generating operational reports](#)
3. [Generating network audit reports](#)
4. [Generating TRAC audit reports](#)

Once the SafeArchive System has been set up, you may view detailed network status data tables, generate audit and operational reports, and generate TRAC-audit reports. The instructions below provide guidance on accomplishing these reporting tasks.

1. From the main menu bar, navigate to the **Detailed Network Status Data** link in the **Audit Reporting** menu option.



To view detailed status data tables, click on the **Show Table** link next to the table you wish to view.



A table containing the network status data will appear. Clicking on the arrow buttons in the far left column will toggle a sub-table containing more detailed network table for the individual network host or archival unit.



The screenshot shows the 'Archival-Unit Overview Table' with the following data:

PinAuid	AuName	AuSizeMax	AuNReplicas	AuNVerifiedReplicas	LastSPollEnd	LastSCrawlEnd	CrawlDuration
12	Odum Dataserve	62,757.0	7	4	2012-05-22T00-37-10 EDT	2012-05-22T15-21-29 EDT	0d 0 0 0.001
11	IQSS Dataserve	97,961.0	6	5	2012-05-21T19-52-07 EDT	2012-05-22T12-27-39 EDT	0d 0 0 0.009
1	ICPSR Archival Unit (1-4999)	68,050.0	5	4	2012-05-21T02-40-24 EDT	2012-05-22T17-28-09 EDT	0d 0 0 0.001

Below the table is a detailed view for PinAuid 1:

```

PinAuid: 1
Auid: edu\harvard\j\dvn\lockss\plugin\DVNOAPlugin&base_url=http%3A%2F%2Fstaging%2Eicpsr%2Eumich%2Eedu&base_url2=http%3A%2F%2Fstaging%2Eicpsr%2Eumich%2Eedu%2Fbankmanifest%2Entm%3FICPSR&oa_request_url=http%3A%2F%2Fstaging%2Eicpsr%2Eumich%2Eedu%2Fbankmanifest%2Entm%3FICPSR&oa_spec=icpsr-safe-1-4999
AuName: ICPSR Archival Unit (1-4999)
AuSizeMax: 71355232362
DiskUsageMax(MB): 7.37499152384E10
AuNReplicas: 5
AuNVerifiedReplicas: 4
LastSPollEnd: 2012-05-21T02-40-24 EDT
LastSCrawlEnd: 2012-05-22T17-28-09 EDT
CrawlDuration: 0d 0 0 0.001
PollId: aeATUyC1qq3cPk5eLdsFvDcEgow=
  
```

At the bottom of the table, there are navigation arrows and a page indicator showing '1' of '2' pages.

- To generate printer-friendly operational reports via BIRT Report Viewer, return to the Detailed Network Status Data page. In the "Operation Reports" section at the lower part of the screen, click on the **View report** link either By Host or By Archival-unit (AU) as desired.

The screenshot shows the 'List Network-Status Data Tables' section with the following table:

Table Name	Show Table
lockss_box_table	Show Table
archival_unit_status_table	Show Table
repository_space_table	Show Table
au_overview_table	Show Table
crawl_status_table	Show Table
polls_table	Show Table
successful_polls_table	Show Table

Below this table, it says "Successful data collection as of : 2012-05-30T00-03-14 EDT".

The 'Refresh Network-Status Data Tables' section contains the following instructions:

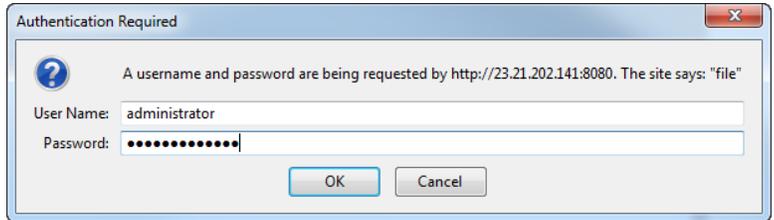
- Click the refresh button below.
- Wait for the refresh-completion message.
- Log out and log in the SAAS again.

There is a 'Refresh Tables' button.

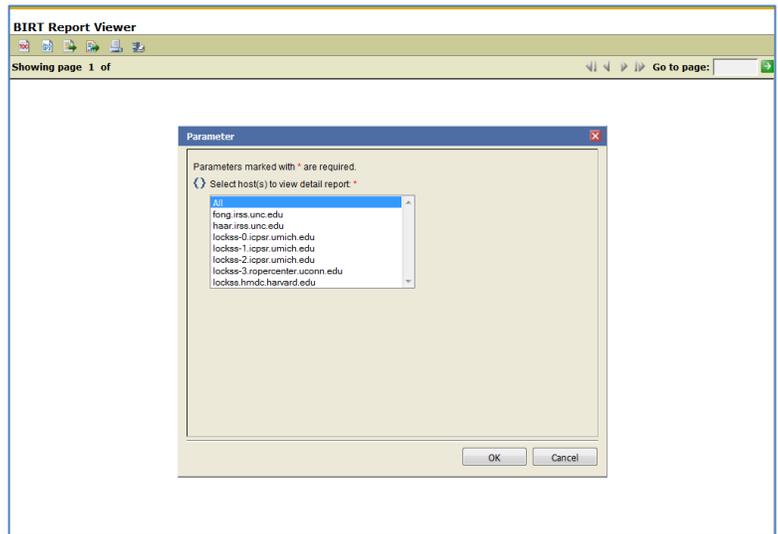
The 'Operation Reports' section has three sub-sections:

- By Host**: View report
- By Archival-unit (AU)**: View report (indicated by a green arrow)
- Poll History**: View report

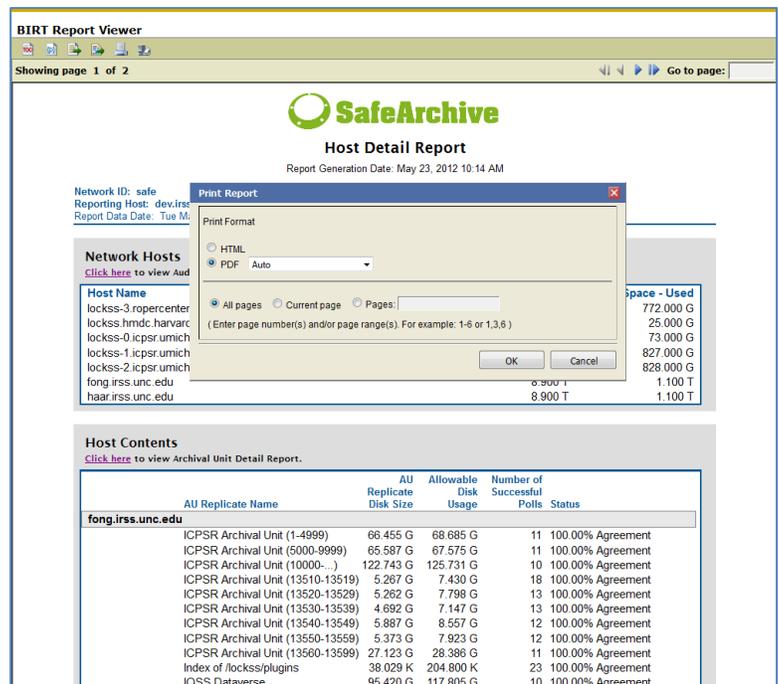
A dialogue box will appear that will prompt you to enter a User Name and Password. Enter the same user name and password used to access the SAAS. Click on the **OK** button.



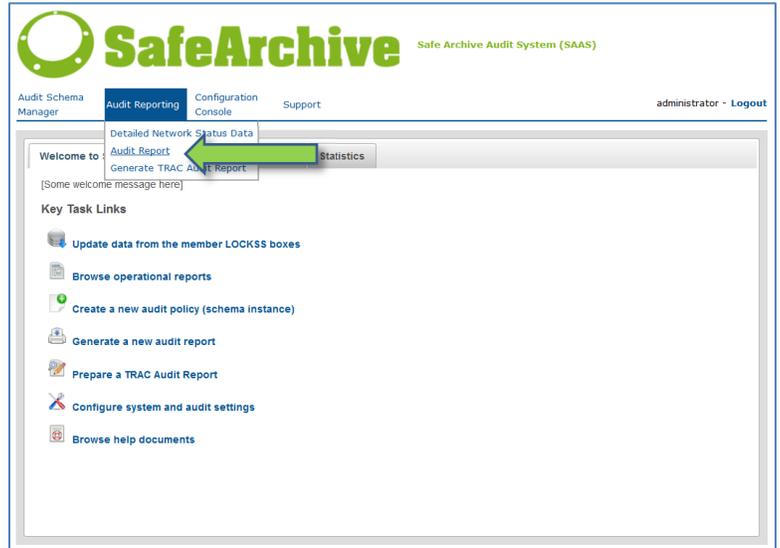
The BIRT Report Viewer will open a dialogue box requesting selection of the host/archival unit to be included in the report. Make your selection(s) and click on the **OK** button.



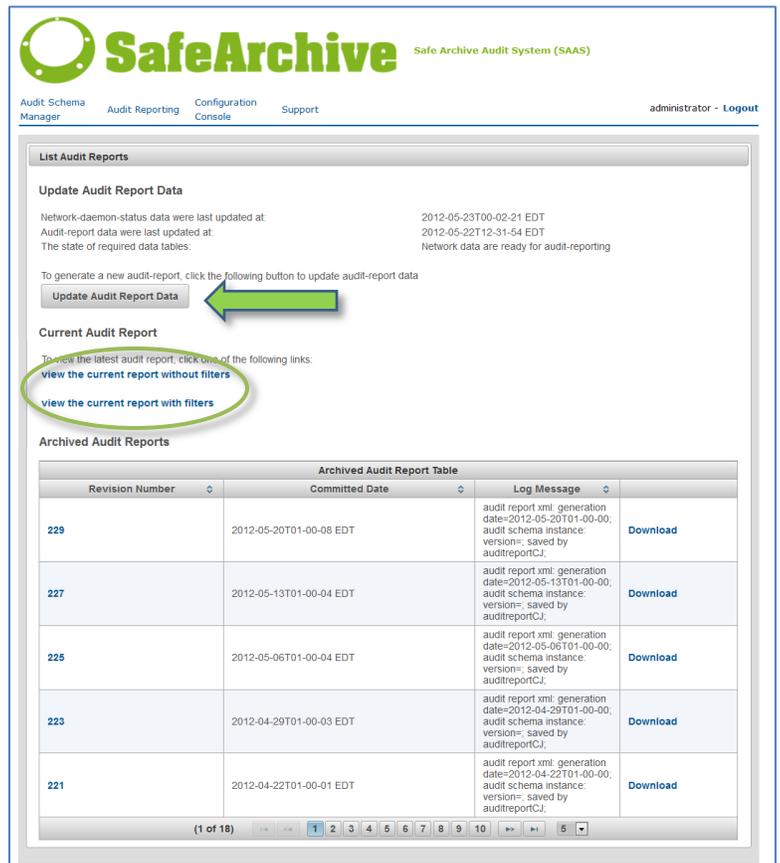
To print the report, click on the printer icon on the main menu bar at the top of the screen. A dialogue box will prompt you to select the print format and identify which pages of the report you wish to print. Click on the **OK** button to generate a printer-friendly version of the report.



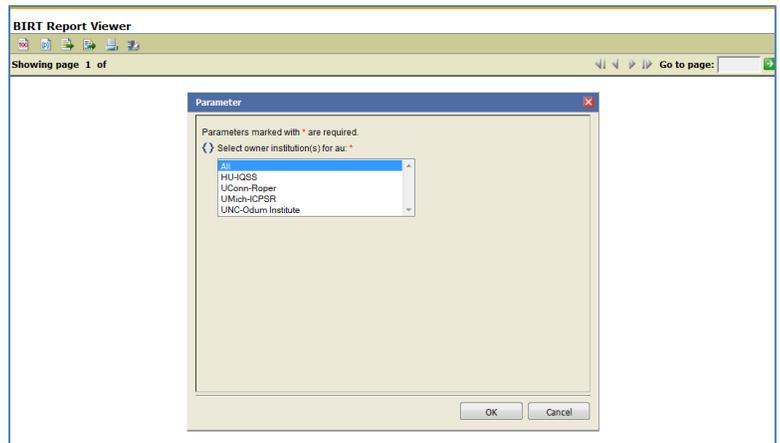
- To generate an audit report, navigate to the **Audit Report** page in the Audit Reporting menu option at the main SAAS menu bar.



Click on the **Update Audit Report Data** button to fetch the most current network data. By clicking on the view the **current report without filters** link, the system will launch the BIRT report viewer displaying an audit report with details of the entire network.



The **current report with filters** link displays the archival units and hosts owned by a specific institution based on your selection in the Parameter dialogue box.



The BIRT Audit Report Summary provides audit results of the preservation network with pass/fail indicators. The Archival Unit Summary and Host Summary sections provide details of policy compliance or noncompliance for each individual archival unit and host.

**SafeArchive**  
**Audit Summary Report**  
 Report Generation Date: May 23, 2012 11:44 AM

Network ID: safe  
 Reporting Host: dev.irss.unc.edu  
 Audit Data Date: Tue May 22 2012 12:31:54 GMT-0400 (EDT)

**Preservation Network Summary**

Mean Up Time for LOCKSS Hosts	65d:7h:24m:34s
Number of Hosts in the PLN	7
Number of Hosts NOT Reporting	0
Number of Unique AUs in the PLN	13
Total Number of AU Replicates	72
Number of AUs NOT Policy Compliant	1
Total Disk Space in the PLN	23.256 T
Total Disk Space in Use	4.666 T
Total Disk Space Free	18.589 T
Number of Hosts NOT Meeting Storage Commitments	0

**Archival Unit (AU) Summary** [UNC-Odum Institute]

[Click here](#) to view Archival Unit Detail Report.

**AU Disk Size (estimated):**

AU Name	Policy	Actual	Audit Result	Notes
Odum Dataverse	62.000 G	61.286 G	Pass	-

**Number of Verified AU Replicates:**

AU Name	Policy	Actual	Audit Result	Notes
Odum Dataverse	3	5	Pass	-

**Number of Verified AU Regions:**

AU Name	Policy	Actual	Audit Result	Notes
Odum Dataverse	2	3	Pass	-

**Days since Last Completed Crawl:**

AU Name	Policy	Actual	Audit Result	Notes
Odum Dataverse	7	0d:23h:34m:20s	Pass	-

**Crawl Duration:**

AU Name	Policy	Actual	Audit Result	Notes
Odum Dataverse	21	0d:0h:0m:0s	Pass	-

**Days since Last Successful Poll:**

AU Name	Policy	Actual	Audit Result	Notes
Odum Dataverse	21	0d:13h:4m:38s	Pass	-

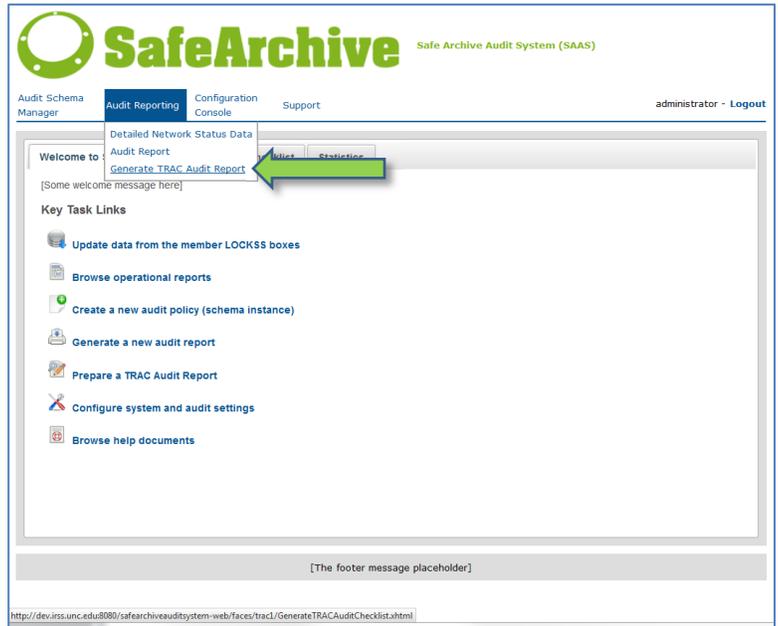
**LOCKSS Host Summary** [UNC-Odum Institute]

[Click here](#) to view Host Detail Report.

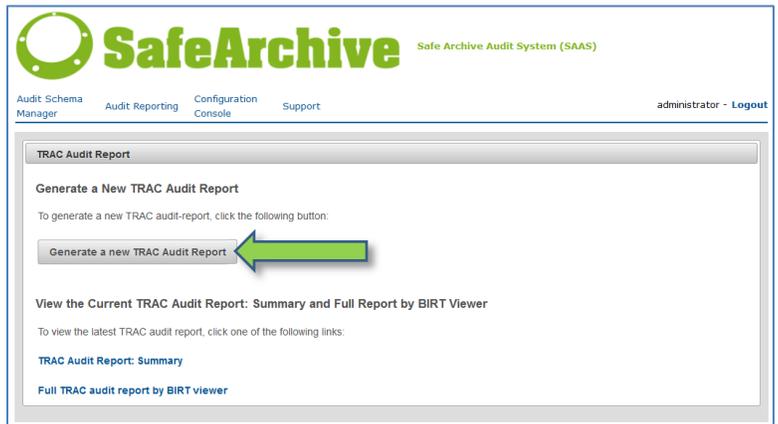
**Committed Disk Space:**

Host Name	Policy	Actual	Audit Result	Notes
fong.irss.unc.edu	8.899 T	8.900 T	Pass	-
haar.irss.unc.edu	8.899 T	8.900 T	Pass	-

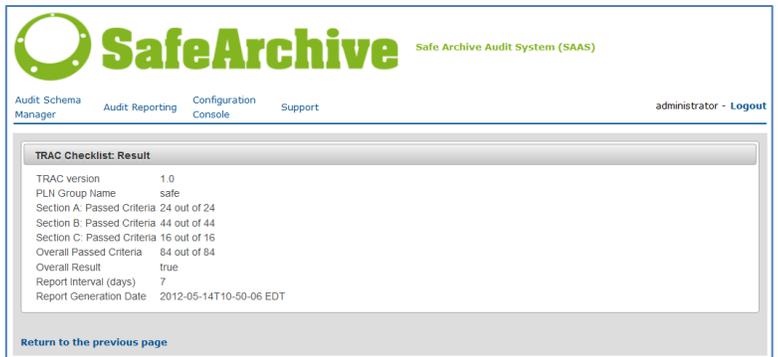
- To view TRAC audit information, click on the **Generate TRAC Audit Report** link in the Audit Reporting menu option at the main SAAS menu.



After clicking on the **Generate a new TRAC Audit Report** button, click on either the **TRAC Audit Report Summary** or **Full TRAC audit report by BIRT viewer** link.



The TRAC Audit Report Summary link provides the completion status of the TRAC checklist. "Passed" status is given if text has been input into the TRAC checklist.



A printable BIRT report can also be generated by clicking on the **Full TRAC audit report by BIRT** viewer link on the **Generate TRAC Audit Report** page. This report not only displays the summary, but also it displays the TRAC checklist entries.

BIRT Report Viewer

Showing page 1 of 2

Go to page:



**Trusted Repositories Audit & Certification (TRAC) Report**  
May 23, 2012 12:29 PM

**TRAC Audit Summary**

PLN Group Name: safe  
TRAC version: 1.0  
TRAC Report data generation date: Mon May 14 10:50:06 EDT 2012

**Complete**

[Section A: 24 out of 24 entered](#)  
[Section B: 44 out of 44 entered](#)  
[Section C: 16 out of 16 entered](#)

**TRAC Audit Checklist**

**Section A** **Complete**

A1.1 Repository has a mission statement that reflects a commitment to the long-term retention of, management of, and access to digital information.  
**Data-PASS About Page:** <http://www.icpsr.umich.edu/icpsrweb/DATAPASS/about.jsp#overview>, **Data-PASS Articles of Collaboration:** <http://www.icpsr.umich.edu/files/DATAPASS/pdf/collaboration.pdf>

A1.2 Repository has an appropriate, formal succession plan, contingency plans, and/or escrow arrangements in place in case the repository ceases to operate or the governing or funding institution substantially changes its scope.  
**Data-PASS Articles of Collaboration**

A2.1 Repository has identified and established the duties that it needs to perform and has appointed staff with adequate skills and experience to fulfill these duties.  
**Data-PASS Articles of Collaboration, Odum Staff Page and Bios**

A2.2 Repository has the appropriate number of staff to support all functions and services.  
**Data-PASS Publications and Presentations:** <http://www.icpsr.umich.edu/icpsrweb/DATAPASS/presentations.jsp>, **partner's Staff Pages**

A2.3 Repository has an active professional development program in place that provides staff with skills and expertise development opportunities.  
**Data-PASS Publications and Presentations, Odum Internal Courses**

A3.1 Repository has defined its designated community(ies) and associated knowledge base(s) and has publicly accessible definitions and policies in place to dictate how its preservation service requirements will be met.  
**Data-PASS Articles of Collaboration, Data-PASS Confidentiality (pg. 6-7):** <http://www.icpsr.umich.edu/files/DATAPASS/pdf/confidentiality.pdf>, **Odum Mission Statement**

A3.2 Repository has procedures and policies in place, and mechanisms for their review, update, and development as the repository grows and as technology and community practice evolve.  
**Data-PASS committee meetings, Odum Interwiki, Data-PASS Best Practices:** <http://www.icpsr.umich.edu/icpsrweb/DATAPASS/best-practices.jsp>

**NOTE:** To avoid additional charges, remember to TERMINATE YOUR INSTANCE! To do this, return to your AWS Management Console. Click on the **Instances** link in the main navigation menu at the left-hand side of the screen. Right-click on the SafeArchive instance. Click on **Terminate**.

