

Deployment & Usage Instructions

Glass V2.1.0-alpha

Version: 2.1.0
Last Updated: 6/11/2025

Contents

1	Introduction.....	4
2	Getting Started	4
2.1	Built-with.....	4
2.2	Pre-requisite.....	4
3	Installation.....	5
3.1	On Splunk Single Instance Setup.....	5
3.1.1	Login to Splunk web interface	5
3.1.2	Install the Glass app.....	5
3.1.3	Configure the Glass app.....	7
3.2	On Splunk Cluster Setup.....	12
3.2.1	Login to Splunk Manager/Master Node web interface	12
3.2.2	Install the Glass app.....	13
3.2.3	Configure the Glass app.....	15
3.2.4	Deploy the Glass app to Peer Nodes	19
3.2.5	Deploy the Glass app to Search Head Node	22
4	Usage Instructions	22
4.1	Opening the Glass App on Splunk UI.....	22
4.2	Running “archive” command	24
4.3	Running “catalog” command	24
4.4	Running “restore” command	25
4.5	Confirming the Restored Data in Splunk.....	26
4.5.1	Steps to run the Splunk Search query to confirm the restored Data from Splunk Search:.....	26
4.5.2	Steps to confirm the restored data from the Splunk CLI:.....	27
5	Operational Notes	27
6	Splunk Configuration	28
6.1	Traditional Architecture	28
6.2	Smartstore Architecture	29
7	Troubleshooting	30
7.1	Restart Splunk instance.....	30
8	Uninstall and cleanup	30
8.1	Splunk Single Instance Setup	30

8.2	Splunk Cluster Setup	31
8.2.1	On Master and Peer Indexer Nodes	31
8.2.2	On Search Head Node.....	32
9	Acknowledgement.....	32

1 Introduction

This document contains the installation instruction and usage guide for Glass App for Splunk. *Most Economical archiving for large Splunk implementations.*

Glass is an archiving solution that is designed to work when Splunk policies in indexes.conf results in data being transferred to Frozen tier. Once the data is available in Frozen tier, Glass App can archive the data from there to a Remote storage and restore it back to Splunk when needed.

Since Glass App only works with Frozen data, it does not directly touch any indexes of Splunk and therefore does not impact any of the existing ingestion flows into Splunk. This approach means no runtime degradation to performance of currently running Splunk systems is caused by using the Glass App services.

2 Getting Started

This section provides the steps to install and configure the Glass app.

2.1 Built-with

1. Python - <https://www.python.org/>
2. Boto3 - <https://pypi.org/project/boto3/>
3. Splunk App Guidelines - <https://dev.splunk.com/enterprise/docs/developapps/createapps/appanatomy>

2.2 Pre-requisite

1. Splunk instance with indexes configured to frozen the data. Refer section [Splunk Configuration](#) for more details.
2. Python 3.x (3.7 onwards) and pip 3.x must be installed on the Splunk instance.
3. This app is supported on Splunk version 8.x, 9.x and 10.x.
4. This app is supported for Splunk on Linux Operating Systems.
5. Instance must have access to internet
 - a. To download the dependencies
 - b. And to access the external storage system for data archive
6. Splunk user with adequate roles (splunk-system-role) and permissions to invoke the Splunk REST APIs. You can use the default admin user for testing and validation.
7. SoftNAS Server to use as NFS Server cache (recommended if the Data Size is greater than 1 TB per day).
8. If SoftNAS is enabled, the NFS remote location should be mounted on the Splunk Server node in case of Standalone Setup.
9. If SoftNAS is enabled, the NFS remote location should be mounted and accessible on all the Peer nodes in case of Cluster Setup.
10. External S3 compatible storage (AWS S3 Glacier, Geyser Data, IBM Deep Archive, Spectra) to archive the data.
11. Storage system must be accessible through Splunk instance.
12. Splunk Server's server.conf should have the below properties set for stanza [httpServer]:

```
[httpServer]
crossOriginSharingPolicy = http://localhost:8000/
crossOriginSharingHeaders = Authorization, Content-Type
```

allowBasicAuth = true

13. Google Chrome or Microsoft Edge browsers to access the Glass App from UI.

3 Installation

3.1 On Splunk Single Instance Setup

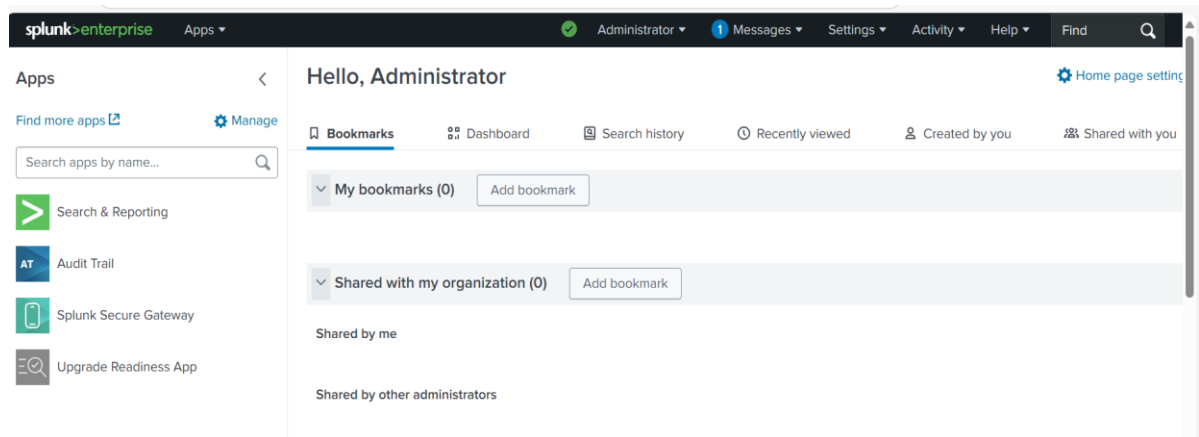
For installation, you are provided with deliverable's zip (glass_app-2.1.0.tar.gz).

3.1.1 Login to Splunk web interface

1. Access the Splunk web UI through browser and login



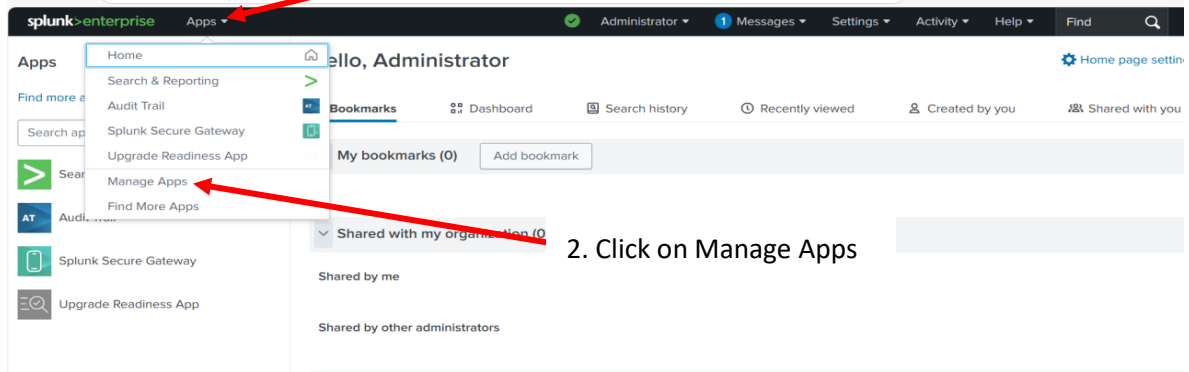
2. After successfully logging in, you will be redirected to the Splunk homepage



3.1.2 Install the Glass app

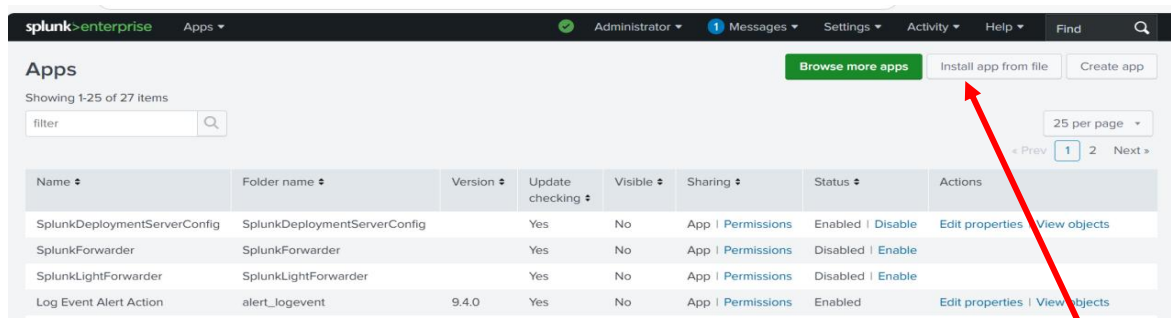
1. Go to the manage app page

1. Click on Apps



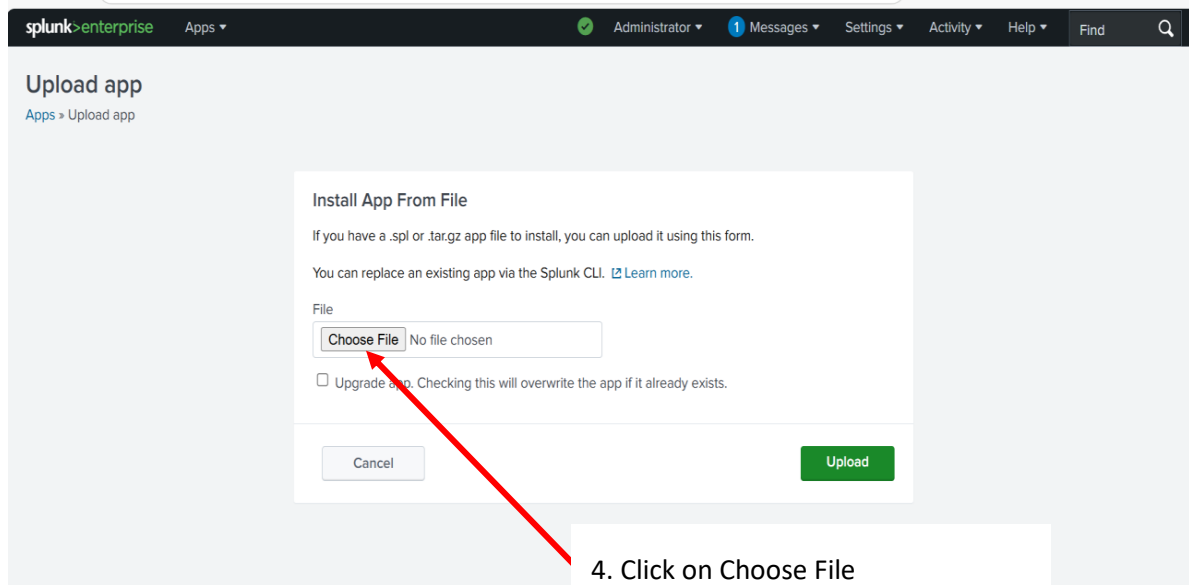
2. Click on Manage Apps

2. After clicking on Manage Apps, you will be directed to Apps page



3. Click on Install app from file

3. After clicking on Install from file, you will be directed to upload app page



4. Click on Choose File

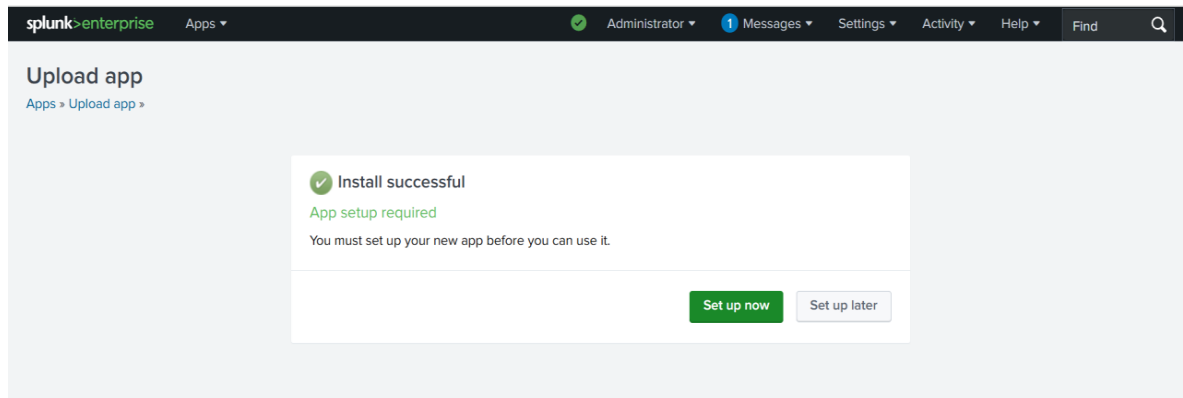
5. Select the glass_app-2.1.0.tar.gz

6. Click on upload after file selection

4. After successful upload of the Glass app, you will be redirected to the Glass App's setup page to complete the App's configuration.

If you select "Set up now" then continue with step 3 of [section 3.1.3](#) to continue with the app configuration.

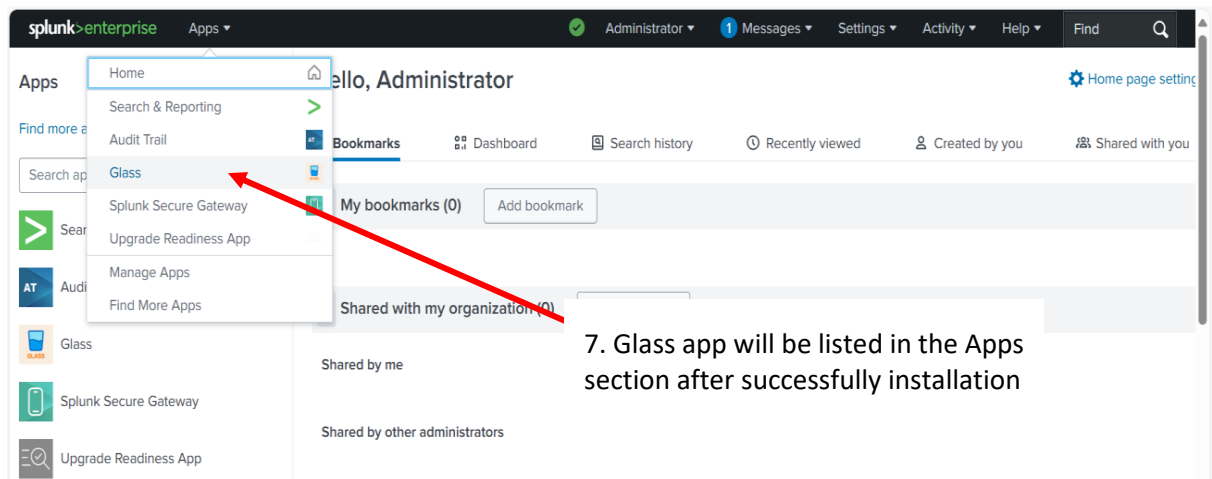
If you select "Setup Later" then refer to [section 3.1.3](#) for configuring the app later.



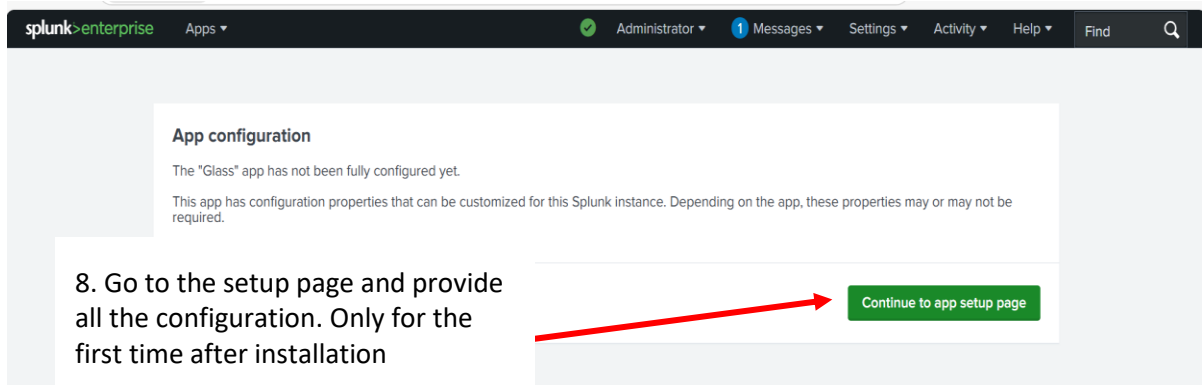
Note: - Splunk Server restart might be required after App installation to display the app icons and images properly.

3.1.3 Configure the Glass app

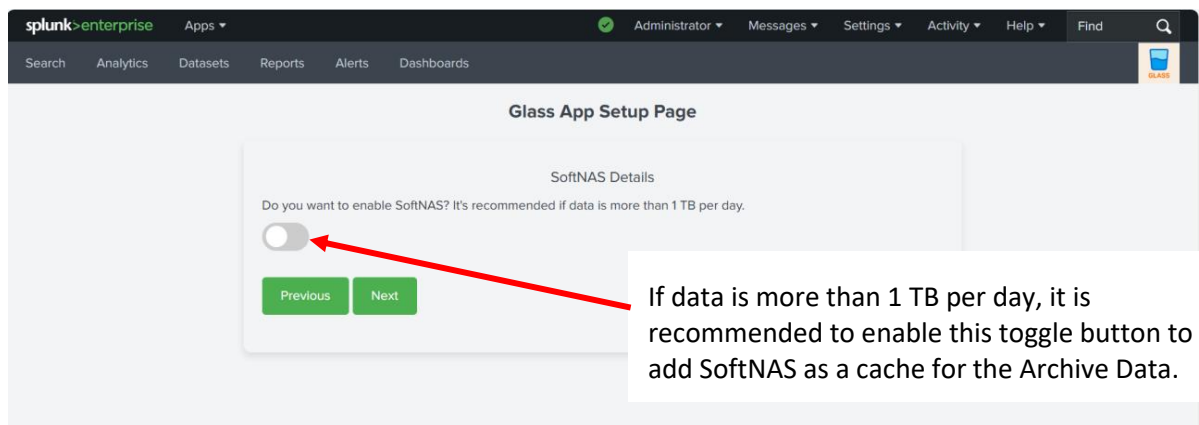
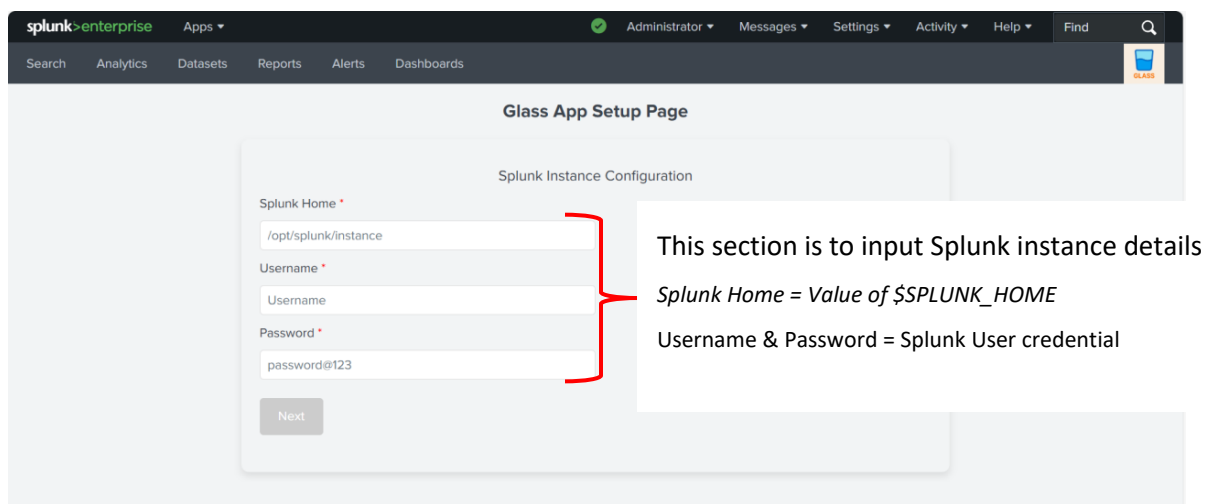
1. Login again to Splunk instance after successful restart and installation



2. Select the Glass app, you will be directed to configuration page



3. Input all the configuration details



Search Analytics Datasets Reports Alerts Dashboards

Glass App Setup Page

SoftNAS Details

Do you want to enable SoftNAS? It's recommended if data is more than 1 TB per day.

☒

Protocol

NFS

NFS Server *

nfs.example.com

NFS Remote Path *

/remote/path

NFS Local Mount Path *

/mnt/local/mount

Schedule Interval

Daily

Previous Next

This section is to input SoftNAS details

Protocol = Currently only NFS is supported

NFS Server = NFS Server IP address or Hostname

NFS Remote Path = Remote path of the NFS Storage

NFS Local Mount Path = Local path which is mounted to the NFS Remote Path

Schedule Interval = Select the duration on which the NFS scheduler will run to move Data from SoftNAS to Long Term remote store.

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Glass App Setup Page

Long Term Store Selection

Select Target Store

-- Select an option --

Previous Next

This section is to Select Long term Storage Selection

Select the long term storage from the below options in the Dropdown:

- AWS S3
- Geyser Data
- IBM Deep Archive
- Spectra

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Glass App Setup Page

AWS S3 Configuration

Bucket Name *
my_aws_s3_bucket

EndPoint URL *
https://domain/api/endpoint

Access Key Id *
Access Key

Secret Access Key *
Secret Key

SSL Certification
☐

Previous Next

This section is to provide AWS S3 bucket configuration

Bucket Name = Name of the bucket

EndPoint URL = Bucket endpoint URL

Access Key = Access Key to access the bucket

Secret Access Key = Secret Key to access the bucket

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Glass App Setup Page

Geyser Data Configuration

Bucket Name *
my_splunk_data_bucket

EndPoint URL *
https://domain/api/endpoint

Access Key Id *
Access Key

Secret Access Key *
Secret Key

SSL Certification
☐

Previous Next

This section is to provide Geyser Data bucket configuration

Bucket Name = Name of the bucket

EndPoint URL = Bucket endpoint URL

Access Key = Access Key to access the bucket

Secret Access Key = Secret Key to access the bucket

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Glass App Setup Page

IBM Deep Archive Configuration

Bucket Name *
my_ibm_bucket

EndPoint URL *
https://domain/api/endpoint

Access Key Id *
Access Key

Secret Access Key *
Secret Key

SSL Certification
☐

Previous Next

This section is to provide IBM Deep Archive bucket configuration

Bucket Name = Name of the bucket

EndPoint URL = Bucket endpoint URL

Access Key = Access Key to access the bucket

Secret Access Key = Secret Key to access the bucket

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Glass App Setup Page

Spectra Black Pearl Configuration

Bucket Name *
my_spectra_bucket

EndPoint URL *
https://domain/api/endpoint

Access Key Id *
Access Key

Secret Access Key *
Secret Key

SSL Certification
☐

Previous Next

This section is to provide Spectra Black Pearl bucket configuration

Bucket Name = Name of the bucket

EndPoint URL = Bucket endpoint URL

Access Key = Access Key to access the bucket

Secret Access Key = Secret Key to access the bucket

Glass App Setup Page

Frozen Policy

☒ Frozen Directory ☐ Frozen Script

Cluster Id *

cluster-12345

Minimum Bucket Size (in MB) *

Enter size in MB

Do you want to archive replicated buckets?

☒ Yes ☐ No

Scheduling ☒ Schedule Interval

Daily

Archive Config

Previous **Complete Setup**

This section is to provide configuration for Glass app archive script

Frozen Directory Base Path = Base path configured for Splunk coldToFrozenScript. (Only used when "Frozen Script" is selected)

Cluster Id = Unique identification for each cluster

Minimum Bucket Size = Bucket size qualified for immediate archive

Archive replicated buckets (If set to yes, replicated buckets are also archived in case of Cluster Setup, skipped otherwise)

Schedule Interval = At which archive script will be executed

9. Submit the page after providing all the details

4. Message will be shown once configuration is done successfully and you will be redirected to Glass app

3.2 On Splunk Cluster Setup

For installation, you are provided with deliverable's zip (glass_app-2.1.0.tar.gz).

3.2.1 Login to Splunk Manager/Master Node web interface

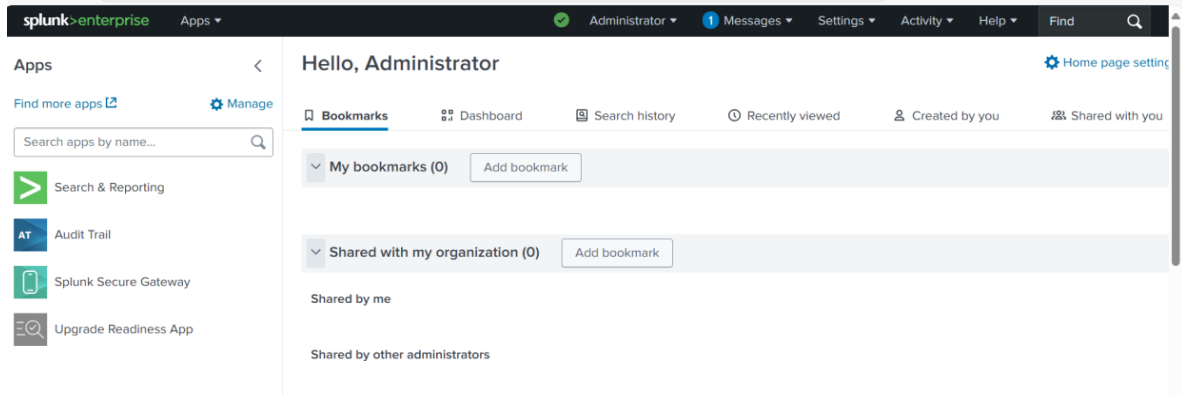
1. Access the Splunk web UI through browser and login

splunk>enterprise

Username Password **Sign In**

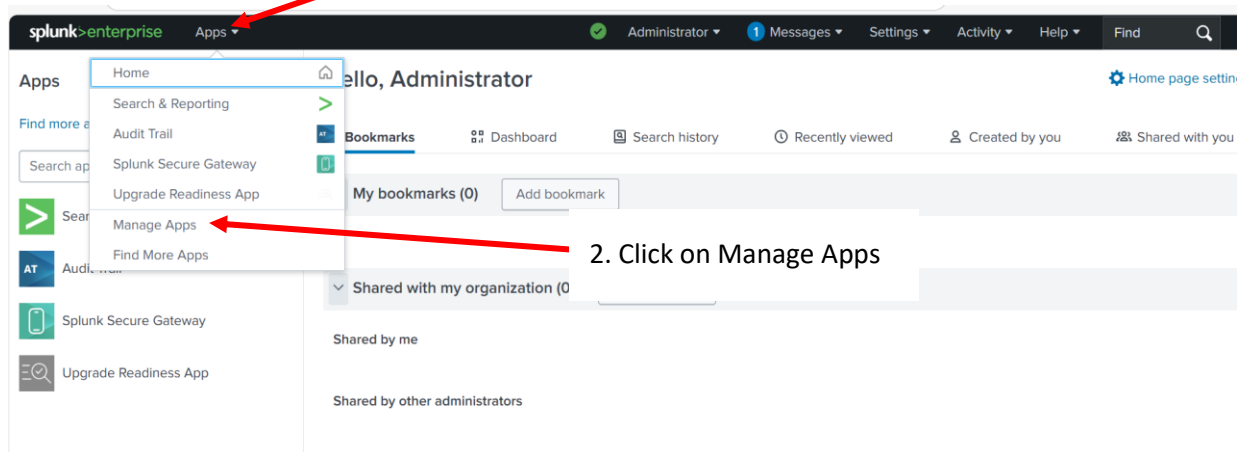
First time signing in?

2. After successfully logging in, you will be directed to the Splunk homepage

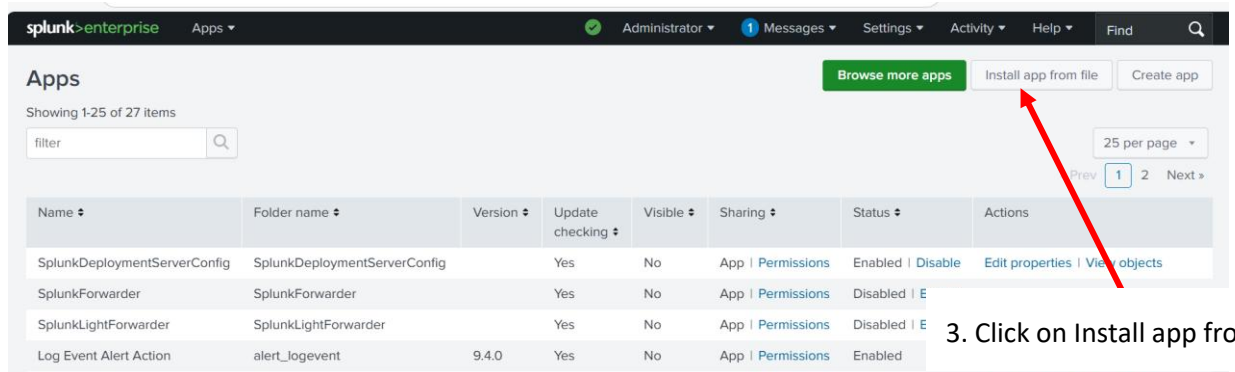


3.2.2 Install the Glass app

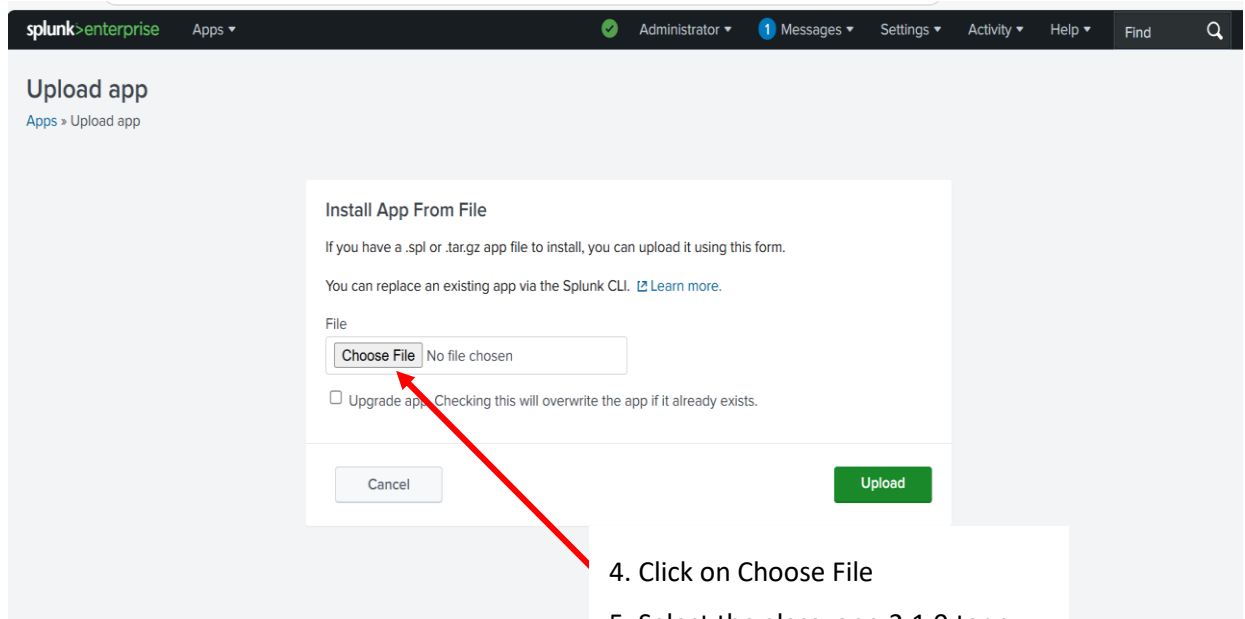
1. Go to the manage app page



2. After clicking on Manage Apps, you will be directed to Apps page



3. After clicking on Install from file, you will be directed to upload app page

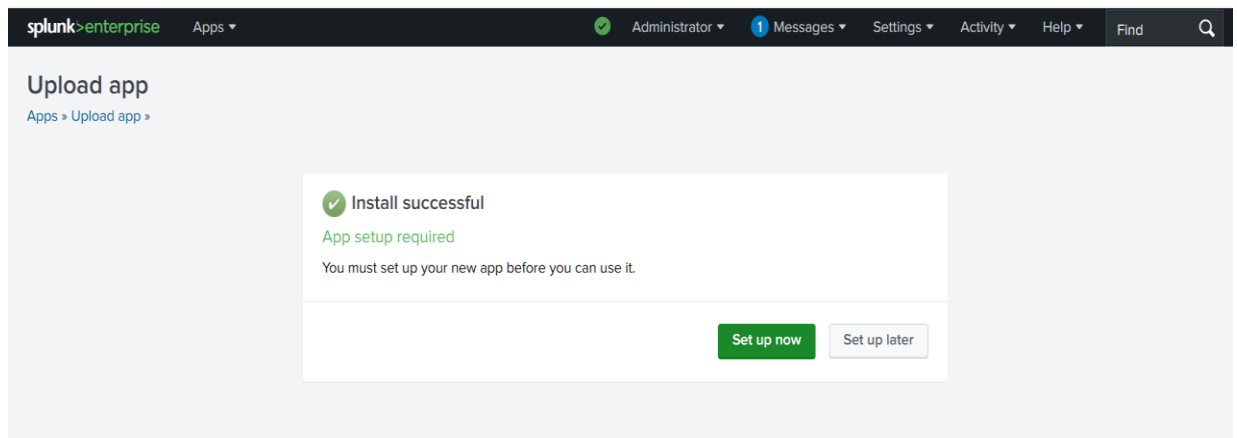


4. Click on Choose File

5. Select the glass_app-2.1.0.tar.gz

6. Click on upload after file selection

4. After successful upload of the Glass app, you will be redirected to the Glass App's setup page to complete the App's configuration. Click on "Set up now" and continue with step 3 of [section 3.2.3](#). If you select "Setup Later" then refer to [section 3.2.3](#) for configuring the app later.

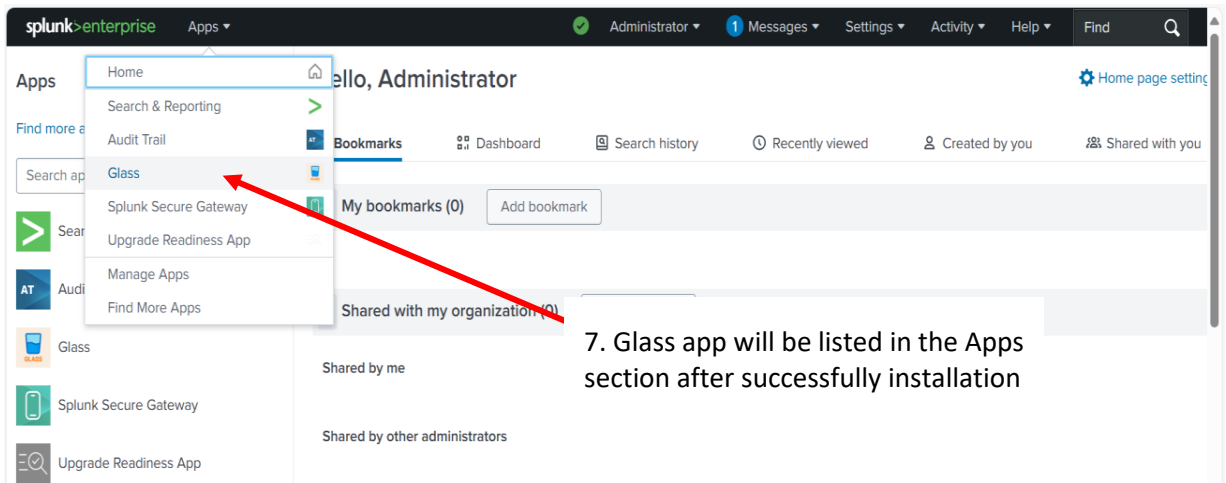


Note: - Splunk Server restart might be required after App installation to display the app icons and images properly.

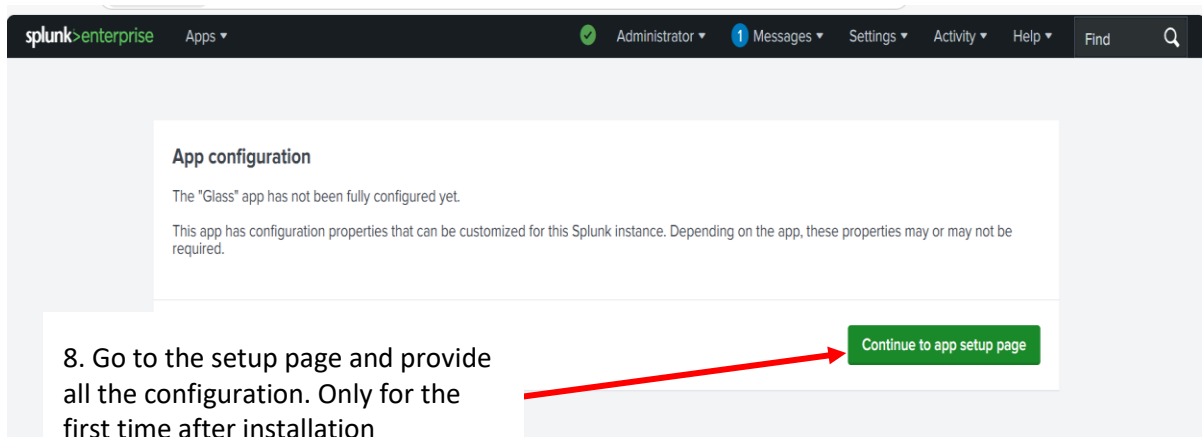
3.2.3 Configure the Glass app

Note: In case of Splunk Cluster, configuration added on the setup page should be same on Peer nodes as well as Search Head Nodes.

1. Login again to Splunk instance after successful restart and installation



2. Select the Glass app, you will be directed to configuration page



3. Input all the configuration details

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Glass App Setup Page

Splunk Instance Configuration

Splunk Home *

/opt/splunk/instance

Username *

Username

Password *

password@123

Next

This section is to input Splunk instance details
Splunk Home = Value of \$SPLUNK_HOME
Username & Password = Splunk User credential

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Glass App Setup Page

SoftNAS Details

Do you want to enable SoftNAS? It's recommended if data is more than 1 TB per day.

☐

Previous Next

If data is more than 1 TB per day, it is recommended to enable this toggle button to add SoftNAS as a cache for the Archive Data.

Search Analytics Datasets Reports Alerts Dashboards

Glass App Setup Page

SoftNAS Details

Do you want to enable SoftNAS? It's recommended if data is more than 1 TB per day.

☒

Protocol

NFS

NFS Server *

nfs.example.com

NFS Remote Path *

/remote/path

NFS Local Mount Path *

/mnt/local/mount

Schedule Interval

Daily

Previous Next

This section is to input SoftNAS details
Protocol = Currently only NFS is supported
NFS Server = NFS Server IP address or Hostname
NFS Remote Path = Remote path of the NFS Storage
NFS Local Mount Path = Local path which is mounted to the NFS Remote Path
Schedule Interval = Select the duration on which the NFS scheduler will run to move Data from SoftNAS to Long Term remote store.

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Glass App Setup Page

Long Term Store Selection

Select Target Store

-- Select an option --

Previous Next

This section is to Select Long term Storage Selection

Select the long term storage from the below options in the Dropdown:

- AWS S3
- Geyser Data
- IBM Deep Archive
- Spectra

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Glass App Setup Page

AWS S3 Configuration

Bucket Name *

my_aws_s3_bucket

EndPoint URL *

https://domain/api/endpoint

Access Key Id *

Access Key

Secret Access Key *

Secret Key

SSL Certification

Previous Next

This section is to provide AWS S3 bucket configuration

Bucket Name = Name of the bucket

EndPoint URL = Bucket endpoint URL

Access Key = Access Key to access the bucket

Secret Access Key = Secret Key to access the bucket

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Glass App Setup Page

Geyser Data Configuration

Bucket Name *
my_splunk_data_bucket

EndPoint URL *
https://domain/api/endpoint

Access Key Id *
Access Key

Secret Access Key *
Secret Key

SSL Certification
☐

Previous Next

This section is to provide Geyser Data bucket configuration

Bucket Name = Name of the bucket

EndPoint URL = Bucket endpoint URL

Access Key = Access Key to access the bucket

Secret Access Key = Secret Key to access the bucket

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Glass App Setup Page

IBM Deep Archive Configuration

Bucket Name *
my_ibm_bucket

EndPoint URL *
https://domain/api/endpoint

Access Key Id *
Access Key

Secret Access Key *
Secret Key

SSL Certification
☐

Previous Next

This section is to provide IBM Deep Archive bucket configuration

Bucket Name = Name of the bucket

EndPoint URL = Bucket endpoint URL

Access Key = Access Key to access the bucket

Secret Access Key = Secret Key to access the bucket

Glass App Setup Page

Spectra Black Pearl Configuration

Bucket Name *

my_spectra_bucket

EndPoint URL *

https://domain/api/endpoint

Access Key Id *

Access Key

Secret Access Key *

Secret Key

SSL Certification

☐

Previous Next

This section is to provide Spectra Black Pearl bucket configuration

Bucket Name = Name of the bucket

EndPoint URL = Bucket endpoint URL

Access Key = Access Key to access the bucket

Secret Access Key = Secret Key to access the bucket

Glass App Setup Page

Archive Configuration

Frozen Policy

☒ Frozen Directory ☐ Frozen Script

Cluster Id *

cluster-12345

Minimum Bucket Size (in MB) *

Enter size in MB

Do you want to archive replicated buckets?

☒ Yes ☐ No

Scheduling

☒ Schedule Interval

Daily

Previous Complete Setup

This section is to provide configuration for Glass app archive script

Frozen Directory Base Path = Base path configured for Splunk coldToFrozenScript. (Only used when "Frozen Script" is selected)

Cluster Id = Unique identification for each cluster

Minimum Bucket Size = Bucket size qualified for immediate archive

Archive replicated buckets (If set to yes, replicated buckets are also archived in case of Cluster Setup, skipped otherwise)

Schedule Interval = At which archive script will be executed

9. Submit the page after providing all the details

4. Message will be shown once configuration is done successfully and you will be redirected to Glass app

3.2.4 Deploy the Glass app to Peer Nodes

1. Go to the Splunk CLI of the Manager/Master node.

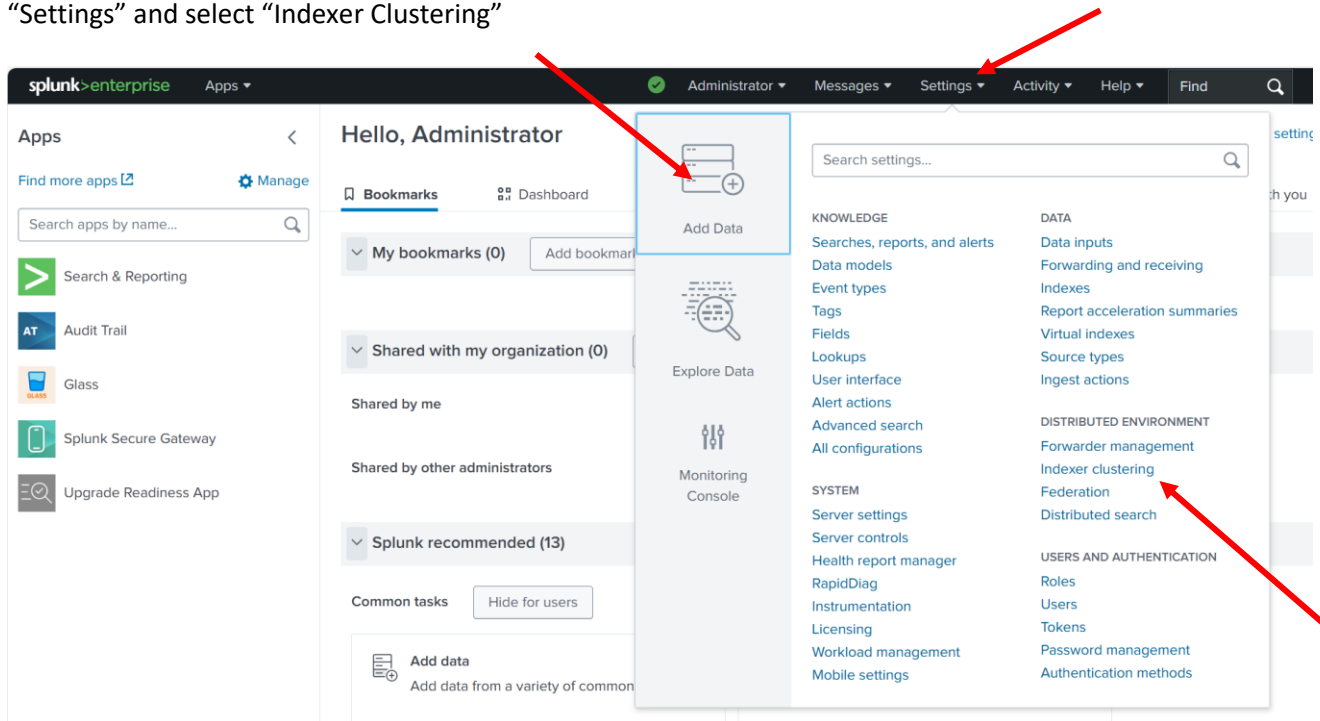
- Copy the glass_app installed using [Section 3.2.2](#) and [3.2.3](#), from “\$Splunk_Home/etc/apps” to location “\$Splunk_Home/etc/manager-apps” or “\$Splunk_Home/etc/master-apps” (in case of old Splunk versions) on the Manager/Master node.

```
[root@ip-172-31-17-113 manager-apps]# sudo cp /opt/splunk/etc/apps/glass_app /opt/splunk/etc/manager-apps/
```

- After performing above steps, Glass app should be present in “\$Splunk_Home/etc/manager-apps” or “\$Splunk_Home/etc/master-apps” (for older Splunk versions), only the changes inside the manager-apps or master-apps are replicated to peers.

```
[ec2-user@ip-172-31-17-113 ~]$ sudo ls /opt/splunk/etc/manager-apps/  
cluster glass_app splunk_ingest_actions  
[ec2-user@ip-172-31-17-113 ~]$
```

- To push changes from Manager Node to Peer Indexer nodes, use Manager node UI and click on “Settings” and select “Indexer Clustering”



- Click on "Edit" and select "Configuration Bundle Actions"

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Indexer Clustering: Manager Node

Edit More Info Documentation

✓ All Data is Searchable ✓ Search Factor is Met

3 searchable 0 not searchable
Peers

4

- Node Type
- Manager Node Configuration
- Configuration Bundle Actions
- Data Rebalance
- Rolling Restart
- Disable Indexer Clustering

Peers (3) Indexes (4) Search Heads (1)

filter 10 per page

i	Peer Name	Fully Searchable	Status	Version	Buckets
>	ip-172-31-21-97.us-east-2.compute.internal	✓ Yes	Up	9.4.0	643
>	ip-172-31-16-126.us-east-2.compute.internal	✓ Yes	Up	9.4.0	643
>	ip-172-31-25-178.us-east-2.compute.internal	✓ Yes	Up	9.4.0	643

192.168.33.217:8001/en-US/manager/system/clustering_push

6. Click "Validate and Check Restart"

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Configuration Bundle Actions

Click Push to distribute the configuration bundle to the set of peers. Optionally, validate the bundle and check if peer restart is required without distributing the bundle, or rollback to the previous bundle. [Learn More](#)

< Back to Manager Node

Validate and Check Restart Push Rollback

Bundle Information:

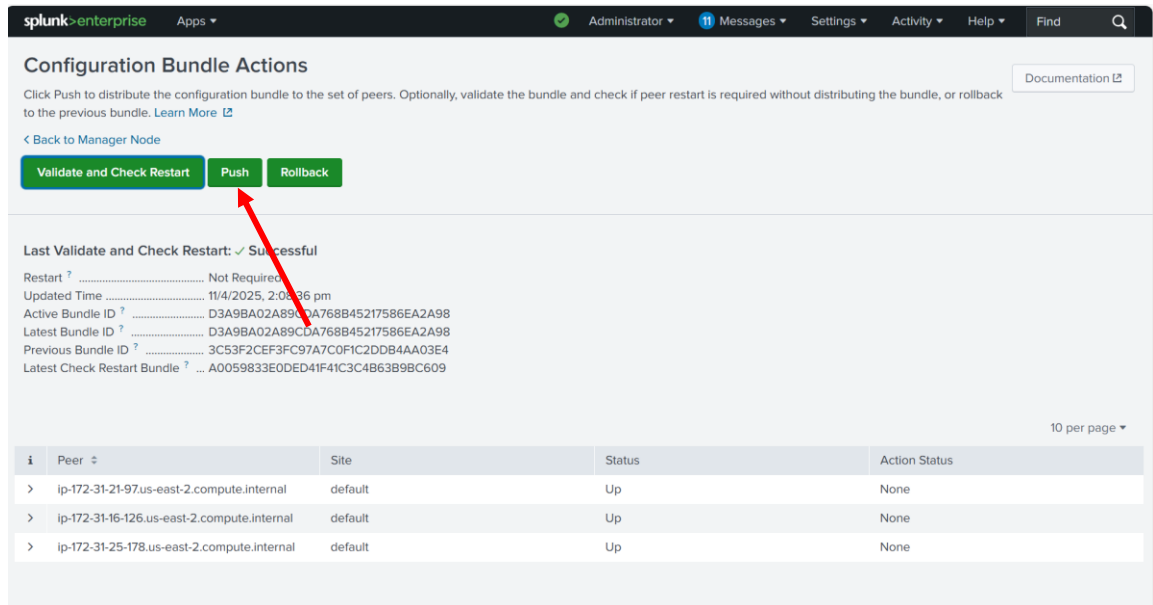
Updated Time 11/4/2025 4:08:36 pm
 Active Bundle ID ? D3A9BA02A6CCDA768B45217586EA2A98
 Latest Bundle ID ? D3A9BA02A89CDA768B45217586EA2A98
 Previous Bundle ID ? 3C53F2CEF3FC97A7C0F1C2DDB4AA03E4

▲ ip-172-31-17-113.us-east-2.compute.internal: [Not Critical]No spec file for: /opt/splunk/etc/manager-apps/glass_app/local/logging.conf

10 per page

i	Peer	Site	Status	Action Status
>	ip-172-31-21-97.us-east-2.compute.internal	default	Up	None
>	ip-172-31-16-126.us-east-2.compute.internal	default	Up	None
>	ip-172-31-25-178.us-east-2.compute.internal	default	Up	None

7. Once the validation is successful click on "Push"



- After successful deployment to all the Peer nodes, please restart all the Peer nodes. The Glass app will be available on the Peer nodes at path `/etc/peer-apps/`

3.2.5 Deploy the Glass app to Search Head Node

Please follow the steps given in the section “[3.1 On Splunk Single Instance Setup](#)” to deploy the Glass App on Search Head node if there is a single Search Head node.

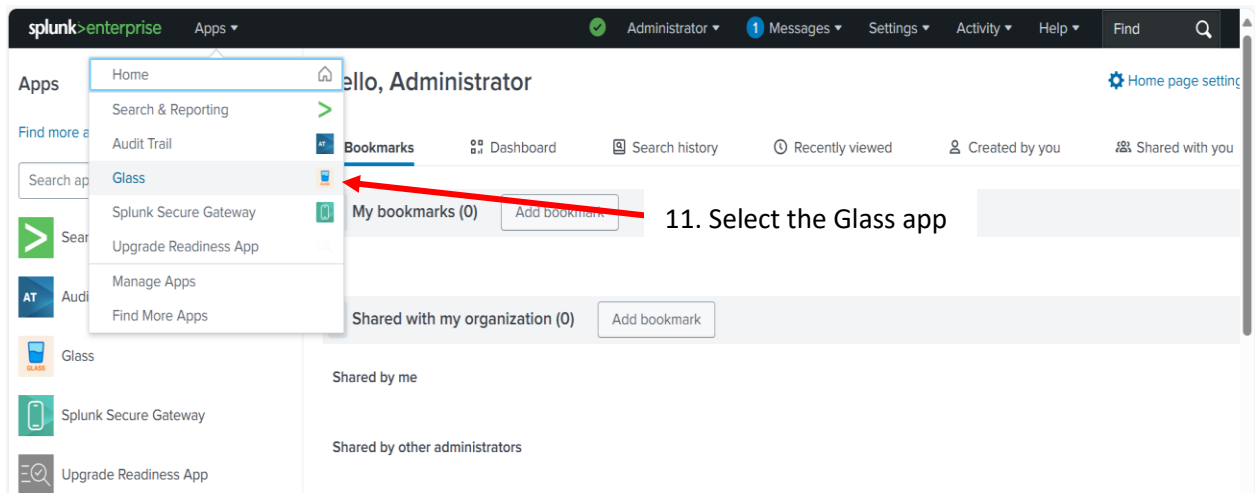
In case of Search Head Cluster use the Search Head deployer to deploy the app.

Note: In case of Splunk Cluster, configuration added on the setup page should be same on Peer nodes as well as Search Head Nodes.

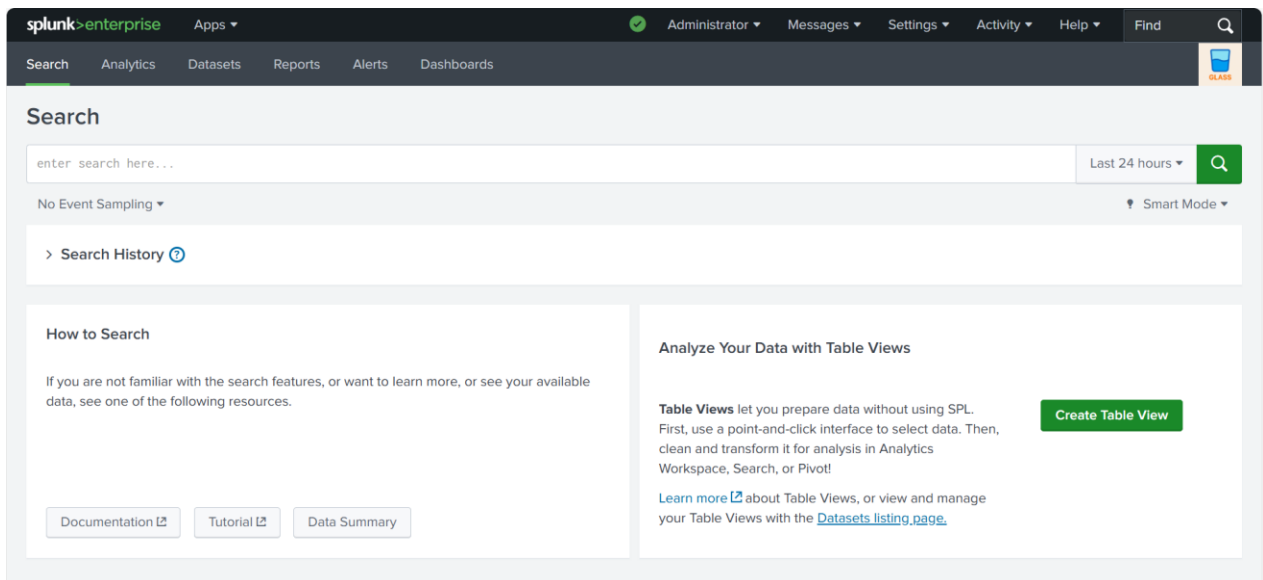
4 Usage Instructions

4.1 Opening the Glass App on Splunk UI

- Login to Splunk instance and select the Glass app



2. After Glass app selection, you will be directed to Glass App Home page



3. Run the Glass app commands to use its features

- a. Command to archive the data from Splunk frozen directory to Remote Long-term Storage
| archive
- b. Command to list the buckets for all the indexes which are archived. It helps to explore before performing the restore.
| catalog --from_date="2025-01-01 00:00:00" --to_date="2025-01-31 23:59:00"
- c. Command to list all buckets for a specific index which are archived. It helps to explore before performing the restore.
| catalog --from_date="2025-01-01 01:00:00" --to_date="2025-12-31 23:59:00" --index=index_name

- d. Command to restore the archived buckets for the given time window for all the indexes.

```
| restore --from_date="2025-01-01 00:00:00" --to_date="2025-01-31 23:59:00"
```

- e. Command to restore the specified multiple archived buckets for the given time window and the specified index.

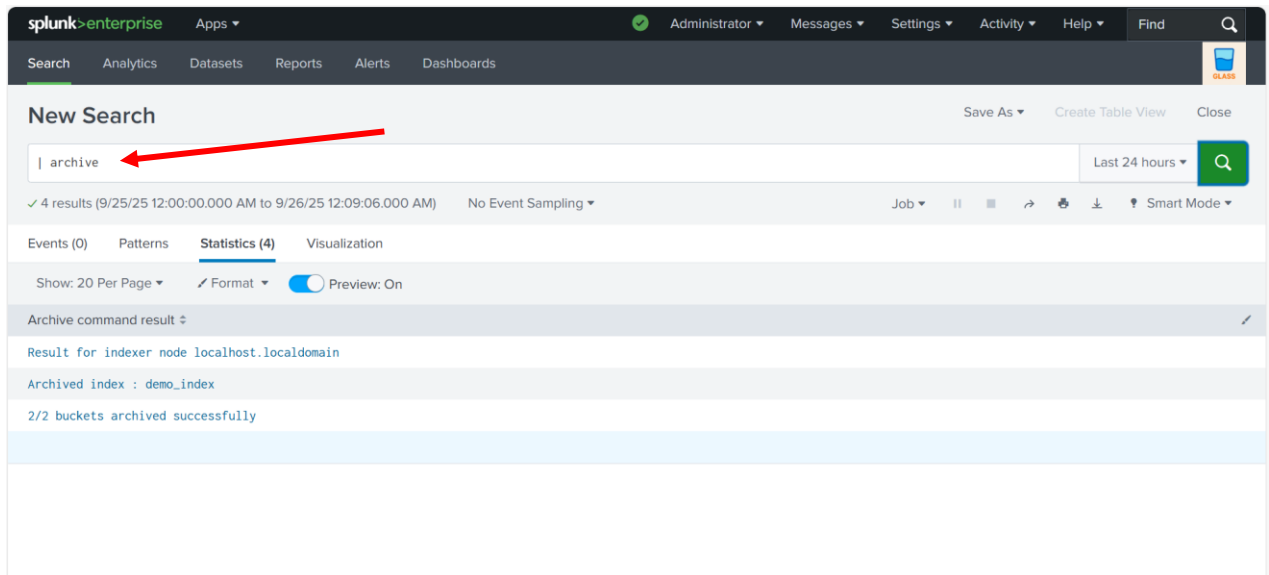
```
| restore --from_date="2025-01-01 01:00:00" --to_date="2025-01-31 23:59:00" --index=index_name --buckets bucket1_name bucket2_name
```

4.2 Running “archive” command

Archive command is used to archive the data from Splunk Instance’s frozen directory to Remote Long-term storage (S3 compatible storage).

- To archive run the below command:

```
| archive
```



4.3 Running “catalog” command

Catalog command helps to explore before performing the restore. Following are different ways to execute catalog command.

- To list the buckets for all the indexes which are archived run the below command:

```
| catalog --from_date="2025-01-01 00:00:00" --to_date="2025-01-31 23:59:00"
```

- To list all buckets for a specific index which are archived run the below command:

```
| catalog --from_date="2025-01-01 01:00:00" --to_date="2025-12-31 23:59:00" --index=index_name
```


The screenshot shows the Splunk Enterprise interface. A red arrow points to the search bar where the command `| catalog --from_date="2025-09-01 00:00:00" --to_date="2025-09-30 23:59:59"` has been entered. The search results show 4 results for the command. The table below displays the results:

batch	timestamp	index_name	bucket_name	bucket_size	indexer_node	time_taken
1	2025-09-26 00:09:14	demo_index	db_1757782533_1757782414_13	244.40 KB	localhost.localdomain	00:00:07
1	2025-09-26 00:09:15	demo_index	db_1757782652_1757782534_14	240.67 KB	localhost.localdomain	00:00:01

4.4 Running “restore” command

- To restore the archived buckets for the given time window for all the indexes:

```
| restore --from_date="2025-01-01 00:00:00" --to_date="2025-01-31 23:59:00"
```

- To restore the specified multiple archived buckets for the given time window and the specified index:

```
| restore --from_date="2025-01-01 01:00:00" --to_date="2025-01-31 23:59:00" --index= index_name -
-buckets bucket1_name bucket2_name
```

****NOTE:** [Restart](#) the Splunk instance after restore.

The screenshot shows the Splunk Enterprise interface with the search bar containing the command `| restore --from_date="2025-09-01 00:00:00" --to_date="2025-09-30 23:59:59"`. The search results show 7 results for the command. The table below displays the results:

batch	timestamp	index_name	bucket_name	bucket_size	indexer_node	time_taken
1	2025-09-26 00:09:14	demo_index	db_1757782533_1757782414_13	244.40 KB	localhost.localdomain	00:00:07
1	2025-09-26 00:09:15	demo_index	db_1757782652_1757782534_14	240.67 KB	localhost.localdomain	00:00:01

Restore command result

Result for indexer node localhost.localdomain

Restored index : demo_index

2/2 buckets restored successfully

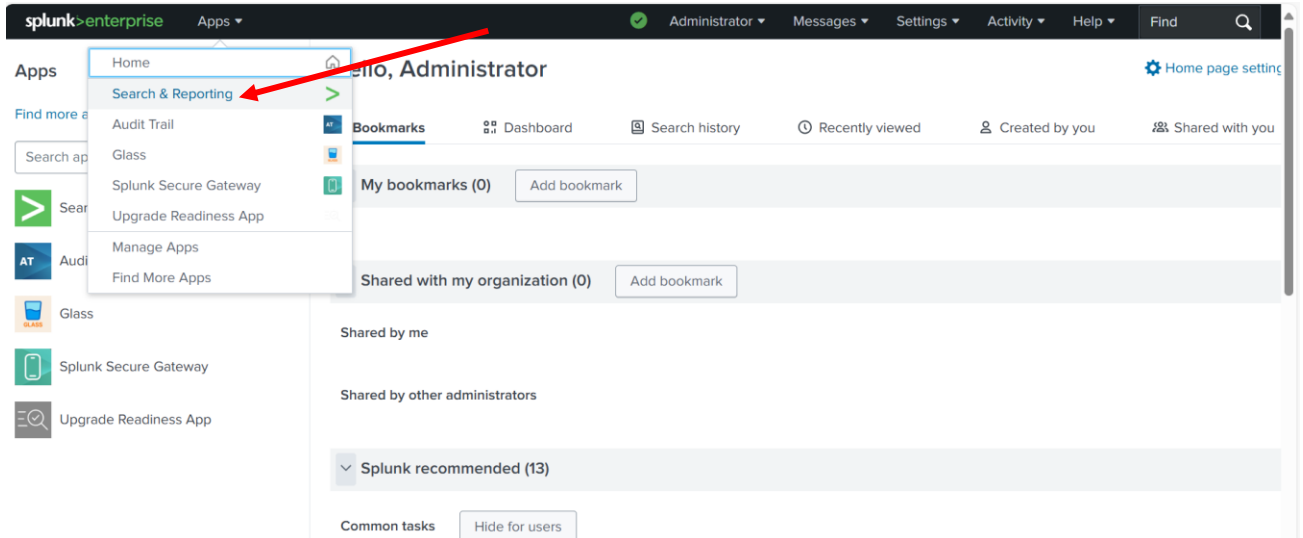
Total execution time - 0:00:16.727984

Please restart the splunk server to ensure the changes take effect.!!

4.5 Confirming the Restored Data in Splunk

4.5.1 Steps to run the Splunk Search query to confirm the restored Data from Splunk Search:

- Open Splunk UI in Browser and login. Click on Apps and Select “Search and Reporting”.



- Type the below query in the Search text box and execute as shown in the below image.

```
index="$INDEX_NAME" | rename _bkt as bucketId | rename _cd as cd | stats count by bucketId,cd,_raw |  
join type=left bucketId [|dbinspect index=$INDEX_NAME] | search state="thawed" | table  
_raw,bucketId,state,splunk_server
```

****Note: Replace \$INDEX_NAME with your Index Name in the above query, wherever it occurs.**

****Note: Execute this query before and after the Restore command execution to compare the results and verify restore is working correctly.**

New Search

index='demo_index' | rename _bkt as bucketId | rename _cd as cd | stats count by bucketId,cd,_raw | join type=left bucketId [dbinspect index='demo_index'] | search state='thawed' | table _raw,bucketId,state,splunk_server

18,750 events (before 9/26/25 12:13:41.000 AM) No Event Sampling

Events Patterns **Statistics (18,750)** Visualization

Show: 20 Per Page Format Preview: On

_raw	bucketId	state	splunk_server
Simulated log entry 79298505-9d4f-470d-a50d-a2a702650977 at 2025-09-13T16:53:34Z	demo_index-13-A96D08C0-0D93-44A2-BF8C-F0A1B7118127	thawed	localhost.localdomain
Simulated log entry 43c0e9a0-7b59-41b4-a2f9-1765ff02a184 at 2025-09-13T16:53:34Z	demo_index-13-A96D08C0-0D93-44A2-BF8C-F0A1B7118127	thawed	localhost.localdomain
Simulated log entry 4574e214-0a58-459a-a904-50d23c802d85 at 2025-09-13T16:53:38Z	demo_index-13-A96D08C0-0D93-44A2-BF8C-F0A1B7118127	thawed	localhost.localdomain
Simulated log entry 071c2d5e-6ecf-4320-a2a5-3e217c40695d at 2025-09-13T16:54:16Z	demo_index-13-A96D08C0-0D93-44A2-BF8C-F0A1B7118127	thawed	localhost.localdomain
Simulated log entry 7b1d7678-6b61-45fa-92d5-699c47a913ca at 2025-09-13T16:54:16Z	demo_index-13-A96D08C0-0D93-44A2-BF8C-F0A1B7118127	thawed	localhost.localdomain
Simulated log entry e292d92d-a702-485b-b1b1-ad0bfffeda2 at 2025-09-13T16:54:16Z	demo_index-13-A96D08C0-0D93-44A2-BF8C-F0A1B7118127	thawed	localhost.localdomain
Simulated log entry 8ca6b9cf-2eb3-4203-ae07-9f69e202f26e at 2025-09-13T16:54:16Z	demo_index-13-A96D08C0-0D93-44A2-BF8C-F0A1B7118127	thawed	localhost.localdomain
Simulated log entry dd7934f8-ce07-4484-856d-2f5629ad59ba at 2025-09-13T16:54:16Z	demo_index-13-A96D08C0-0D93-44A2-BF8C-F0A1B7118127	thawed	localhost.localdomain
Simulated log entry 1fcd5cc9-54a7-4fc8-9452-ec8c073a6656 at 2025-09-13T16:54:16Z	demo_index-13-A96D08C0-0D93-44A2-BF8C-F0A1B7118127	thawed	localhost.localdomain

- The restored data is placed in the thawed state in Splunk. Therefore, when you run the above query after restoring data using the Glass App, the results will include records where the "state" field is set to thawed. However, if you run the same query before restoring, the same records will not be visible in the result as that Data was archived and not searchable anymore in Splunk.

4.5.2 Steps to confirm the restored data from the Splunk CLI:

You can also confirm if the buckets are present in the thawed directory from the Splunk terminal after successful restore execution, at the below path:

ls \$SPLUNK_HOME/var/lib/splunk/\$INDEX_NAME/thaweddb

Example:

ls /opt/splunk/var/lib/splunk/demo_index/thaweddb

5 Operational Notes

- In case of Splunk Cluster Setup, it is recommended to execute the Glass App commands from the Search Head node, as the Search Head node will distribute the command execution on all the Peer Nodes.
- Whenever a command is executed on Search Head node, it will fetch the list of Peer Nodes from the Master Node using the Fetch Peer Details API. Then the command will be executed separately on each Peer and once the command execution completes, the cumulative result will be displayed on the Search Head node UI.
- Glass App related logs are generated at the path **\$SPLUNK_HOME/var/log/splunk/glass_app/** in the below log files:
 - glass_setup.log – Keeps the logs for the Setup Page operations of the Glass App.
Retention Policy: stores last 10 files of 5 MB each

- glass_app.log – Keeps the logs for the Glass App command executions.
Retention Policy: stores last 10 files of 10 MB each
- 4. Catalog DB and other Glass App related data is kept at location:
\$SPLUNK_HOME/var/lib/splunk/glass_app/
- 5. In case any Peer node goes down in case of Cluster Setup the Glass DB Catalog file from the failed Peer node will be restored on the newly added replacement Peer node in the Cluster.

6 Splunk Configuration

For Cluster environment, use the Master/Manager node to configure the Indexes for all the Peers.

6.1 Traditional Architecture

1. Edit/create splunk **indexes.conf** at location **\$SPLUNK_HOME/etc/system/local** and add/edit the below configuration for your Splunk Index.
 - a. Add the Index name below for which you need to apply the settings
[index_name]
 - b. Properties to roll buckets on the basis of time:
maxHotIdleSecs, frozenTimePeriodInSecs
 - c. Properties to roll buckets on the basis of size/Count:
maxWarmDBCount, maxDataSize, maxTotalDataSizeMB
 - d. Properties to define frozen directory path:
coldToFrozenDir

Every index should be configured with unique frozen directory path to correctly identify which bucket belongs to which index.

2. Splunk properties explanation

maxHotIdleSecs = 3600

This property defines the maximum time the Hot bucket is in Idle state before moving it to Warm state.

maxDataSize = 1

This property defines the maximum size for a hot bucket. When a hot bucket reaches this size, it rolls to warm. This attribute also determines the approximate size for all buckets. This property is in MB.

maxWarmDBCount = 1

This property defines the maximum number of warm buckets. When the maximum is reached, warm buckets begin rolling to cold.

maxTotalDataSizeMB = 500

This property defines the maximum size of an index. When this limit is reached, cold buckets begin rolling to frozen.

frozenTimePeriodInSecs = 300

This property defines the maximum age for a bucket in warm/cold state, after which it rolls to frozen.

`coldToFrozenDir = <path>`

Add the Location for archived data in this property. If set, the indexer will archive frozen buckets into this directory just before deleting them from the index.

6.2 Smartstore Architecture

1. Edit/create splunk **indexes.conf** at location **`$SPLUNK_HOME/etc/system/local`** and add/edit the below configuration for your Splunk Index.
 - a. Add the Index name below for which you need to apply the settings
`[index_name]`
 - b. Properties to roll buckets on the basis of time:
`maxHotIdleSecs, frozenTimePeriodInSecs`
 - c. Properties to roll buckets on the basis of size/Count:
`maxWarmDBCount, maxDataSize, maxTotalDataSizeMB`
 - d. Properties to define frozen directory path:
`coldToFrozenDir`
Every index should be configured with unique frozen directory path to correctly identify which bucket belongs to which index.
2. Configure the remote S3 compatible volume where Warm buckets will be stored
 - a. Property to specifies the Volume name (All volume stanzas begin with "volume:")
`[volume:remote_store]`
 - b. Property to specifies whether the volume definition is for indexer local storage or remote.
This property is optional. Applicable values [local | remote]. Default value is "local"
`storageType = remote`
 - c. Property to specifies the location where all indexes that will use this volume reside.
If storageType is set to "local" then the 'path' points to the location on the file system where all indexes that will use this volume reside.
If storageType is set to "remote" then the 'path' points to the remote storage location where indexes reside. The format for this setting is: `<scheme>://<remote-location-specifier>`
`path = <path on server>`
 - d. Property to specifies the URL of the remote storage system supporting the S3 API.
`remote.s3.endpoint = <URL>`
 - e. Property to specifies the access key to use when authenticating with the remote storage system supporting the S3 API.
`remote.s3.access_key = <access_key>`
 - f. Property to specifies the secret key to use when authenticating with the remote storage system supporting the S3 API.
`remote.s3.secret_key = <secret_key>`

Note: - If this property is set then the Index use Smartstore architecture for bucket storage. Presence of this setting means that this index uses remote storage, instead of the local file system, as the main repository for bucket storage. format: [volume:volume_name/index_name]

remotePath = volume:volume_name/index_name

7 Troubleshooting

7.1 Restart Splunk instance

1. Restart using UI
 - Go to Splunk Web in your browser and sign in
 - Select the Settings menu
 - Under System, select Server controls
 - Select Restart Splunk
 - Select OK to confirm the restart
2. Restart using CLI
 - Go to %SPLUNK_HOME%/bin
 - Run the command ./splunk restart

Note: - Restart using UI can sometimes take longer than expected or fail to complete. In these cases, it's recommended to perform a restart via the command-line interface (CLI)

8 Uninstall and cleanup

8.1 Splunk Single Instance Setup

1. Go to the node's deployment apps folder:

`cd $SPLUNK_HOME/etc/apps/`

```
[root@localhost ~]# cd /opt/splunk/etc/apps/
[root@localhost apps]# sudo ls
alert_logevent      learned             SplunkForwarder    splunk_monitoring_console
alert_webhook       legacy             splunk_gdi          splunk_rapid_diag
appsbrowser         python_upgrade_readiness_app splunk_httpinput    splunk-rolling-upgrade
audit_trail         sample_app         splunk_ingest_actions splunk_secure_gateway
glass_app           search            splunk_instrumentation splunk-visual-exporter
introspection_generator_addon splunk_archiver    splunk_internal_metrics user-prefs
journald_input      splunk-dashboard-studio SplunkLightForwarder
launcher            SplunkDeploymentServerConfig splunk_metrics_workspace
[root@localhost apps]#
```

2. Remove the app:

`sudo rm -rf glass_app`

```
[root@localhost apps]# sudo rm -rf glass_app
```

3. Remove the logs directory:

`sudo rm -rf $SPLUNK_HOME/var/log/splunk/glass_app`

```
[root@localhost apps]# sudo rm -rf /opt/splunk/var/log/splunk/glass_app
```

4. Remove the metadata directory:

```
sudo rm -rf $SPLUNK_HOME/var/lib/splunk/glass_app
```

```
[root@localhost apps]# sudo rm -rf /opt/splunk/var/lib/splunk/glass_app
```

5. Restart Splunk Server

8.2 Splunk Cluster Setup

8.2.1 On Master and Peer Indexer Nodes

1. Go to the manager/master node's deployment apps folder:

```
$SPLUNK_HOME/etc/manager-apps/
```

or

```
$SPLUNK_HOME/etc/master-apps/
```

```
[root@localhost ~]# cd /opt/splunk/etc/manager-apps/  
[root@localhost manager-apps]# sudo ls  
_cluster glass_app  
[root@localhost manager-apps]#
```

2. Remove the app:

```
sudo rm -rf glass_app
```

```
[root@localhost manager-apps]# sudo rm -rf glass_app
```

3. Push the Updated Bundle from Manager Node's UI

Configuration Bundle Actions

Click Push to distribute the configuration bundle to the set of peers. Optionally, validate the bundle and check if peer restart is required without distributing the bundle, or rollback to the previous bundle. [Learn More](#)

[Documentation](#)

[Back to Manager Node](#)

[Validate and Check Restart](#) [Push](#) [Rollback](#)

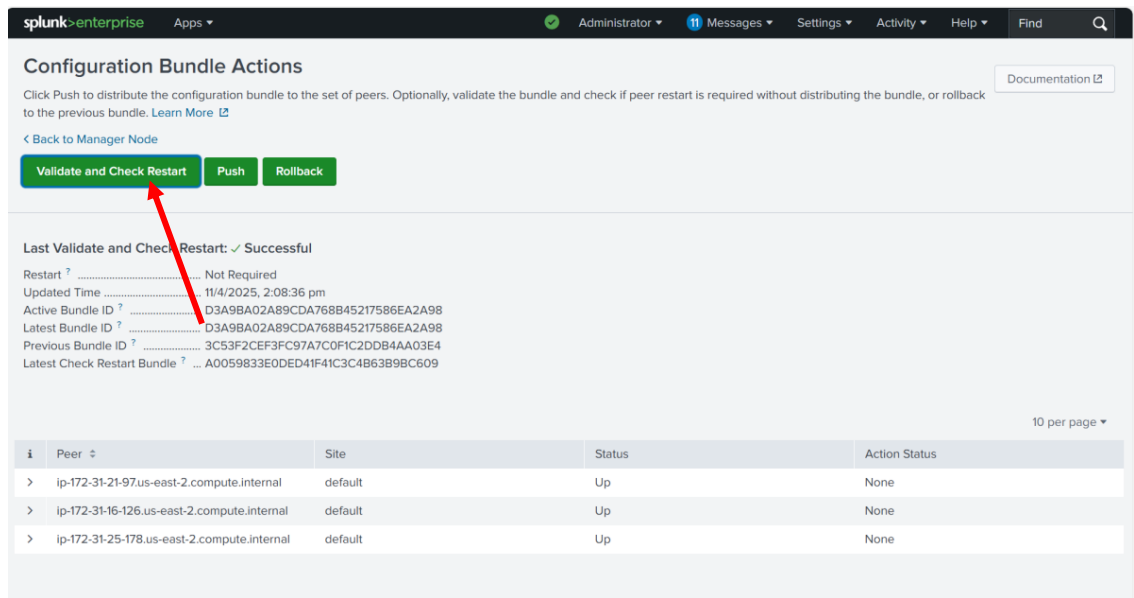
Bundle Information:

Updated Time 11/4/2025, 2:08:36 pm
Active Bundle ID D3A9BA02A89CDA768B45217586EA2A98
Latest Bundle ID D3A9BA02A89CDA768B45217586EA2A98
Previous Bundle ID ? 3C53F2CEF3FC97A7C0F1C2DDB4AA03E4

⚠ ip-172-31-17-113.us-east-2.compute.internal: [Not Critical]No spec file for: /opt/splunk/etc/manager-apps/glass_app/local/logging.conf

10 per page ▾

i	Peer	Site	Status	Action Status
>	ip-172-31-21-97.us-east-2.compute.internal	default	Up	None
>	ip-172-31-16-126.us-east-2.compute.internal	default	Up	None
>	ip-172-31-25-178.us-east-2.compute.internal	default	Up	None



- After the bundle push, check indexers to confirm the app was removed:

```
sudo ls $SPLUNK_HOME/etc/peer-apps/
```

or

```
sudo ls $SPLUNK_HOME/etc/slave-apps/
```

```
[root@localhost ~]# sudo ls /opt/splunk/etc/peer-apps/  
cluster splunk ingest actions Splunk ML Toolkit
```

- Remove the logs directory from Manager and Peer Nodes:

```
sudo rm -rf $SPLUNK_HOME/var/log/splunk/glass_app
```

```
[root@localhost apps]# sudo rm -rf /opt/splunk/var/log/splunk/glass_app
```

- Remove the metadata directory Manager and Peer Nodes:

```
sudo rm -rf $SPLUNK_HOME/var/lib/splunk/glass_app
```

```
[root@localhost apps]# sudo rm -rf /opt/splunk/var/lib/splunk/glass_app
```

- Restart Splunk Server

8.2.2 On Search Head Node

Please follow the steps given in the section “[7.1 Splunk Single Instance Setup](#)” to Uninstall the Glass App on Search Head node.

9 Acknowledgement

- Splunk Traditional Tiered Hierarchical Archive

<https://docs.splunk.com/Documentation/Splunk/9.3.2/Indexer/Automatearchiving>

2. Splunk Smartstore Archive

<https://docs.splunk.com/Documentation/Splunk/9.3.2/Indexer/ConfigureSmartStore>

3. Splunk Archive Policy

<https://docs.splunk.com/Documentation/Splunk/9.3.2/Indexer/Setaretirementandarchivingpolicy>

4. Splunk Configuration

<https://docs.splunk.com/Documentation/Splunk/9.3.2/Indexer/Configureindexstorage>

5. Splunk App Anatomy

<https://dev.splunk.com/enterprise/docs/developapps/createapps/appanatomy>