# Skylar AI Installation Guide

Version 2.3.0

# Table of Contents

# Chapter 1

# System and Sizing Requirements for Skylar AI

## Overview

The installation and configuration of Skylar AI and Skylar Advisor uses Harbor for the registry and Helm for deployment. The Skylar AI platform is deployed as a single Helm umbrella chart containing over 20 microservices, databases, and supporting infrastructure components.

This chapter details the different cluster requirements for Skylar Analytics and Skylar Advisor, and it also includes requirements for only Skylar Analytics if you are currently not using Skylar Advisor. This chapter also includes the required and recommended infrastructure dependencies for a Skylar AI deployment.

This chapter covers the following topics:

# Cluster Requirements for Skylar Analytics and Skylar Advisor

**IMPORTANT:** Before beginning the installation process, verify that your environment has the **required** versions of Kubernetes and the container runtime (where relevant) listed in the following sections.

## Cluster Requirements for Skylar Analytics

- **Kubernetes**: Version 1.32 or later (Skylar Analytics only).

  You can run the following command to verify your environment:

  ```
  kubectl version
  ```

  **NOTE:** Kubernetes upgrades must be performed one minor version at a time. If you are planning a cluster upgrade, see the Kubernetes upgrade documentation.

- **Storage**: Configured EBS StorageClass capable of dynamic PV/PVC provisioning. Storage cannot be NFS-backed, as this is not supported by ScienceLogic databases. Also, you must have one storage class marked as *default*.
- **Attached Storage Capacity**: Recommended 1 TB or more total storage capacity. This requirement varies by tenant datapoints per minute (DPM) requirements. For more sizing information, see *Cluster Sizing Guidelines for Skylar Analytics*.
- **Node Storage Capacity**: Around 300 GB per node of internal storage for images and Kubernetes-related functions. Ensure that the root directory has most of this space provisioned. For more sizing information, see *Cluster Sizing Guidelines for Skylar Analytics*.
- **Networking**: Currently, only IPv4 is supported. IPv6 is not supported at this time.
- **External Networking**:
  - The Skylar AI Kubernetes cluster will need Internet access to **https://registry.scilo.tools/**. This connection can be through a proxy if needed (additional configuration required).
  - 443 connectivity from the Skylar One instance to the Skylar AI Kubernetes cluster.
- **Deployment Options**:
  - Self-hosted Kubernetes clusters, such as bare metal or VMware
  - Cloud-managed Kubernetes services (EKS, GKE, AKS)

## Additional Requirements for Skylar Advisor

**IMPORTANT:** If you are installing only Skylar Analytics, you can skip this topic.

- **Storage**: For Skylar Advisor, ScienceLogic requires that you use RWX Storage configurations only for Skylar Advisor services. This is in addition to the RW EBS storage class required for Skylar Analytics.
- **Kubernetes**: Version 1.35 with ContainerD 2.1 or cri-o 1.32 or later runtime.

  You can run the following commands to verify your environment:

  ```
  kubectl version
  ```

  ```
  containerd --version
  ```

- **GPU resources provisioning**: You need to dynamically allocate GPU resources that can be correctly provisioned to Kubernetes nodes under the **[Resources]** tab. Examples would be NVIDIA time-slicing/MIG or VMware vGPU.
- **GPU Driver**. Version 570.195.03 with CUDA 12.8.

For more sizing information, see *Cluster Sizing Guidelines for Skylar Analytics*.

## Third-Party Chart Dependencies for Skylar Analytics and Skylar Advisor

Skylar AI includes several third-party Helm charts from Bitnami, Chainguard, and other providers:

- **Bitnami Charts**: ClickHouse, PostgreSQL HA, and associated components
- **Maintenance Notice**: ScienceLogic validates and updates third-party chart versions with each Skylar AI release. However, customers are responsible for:
  - Security patching of third-party components between Skylar AI releases
  - Vulnerability management for non-Skylar AI components
  - Understanding the security posture of included third-party dependencies

For additional Skylar Advisor configuration information, see *Cluster Sizing Guidelines for Skylar Advisor*.

# Cluster Sizing Guidelines for Skylar Analytics

This section lists the recommended configuration for your Skylar Analytics environment based on your expected volume of data, measured in *datapoints per minute* (DPM).

The following sizings are only for the Skylar Analytics application. You will need to consider additional resource requirements for system and cluster level services. In other words, do not size a node to just the requirements listed below.

Also, these sizing are for a single tenant cluster. Skylar AI can be multi-tenant, which will change the sizing recommendations as more Data Visualization tenants are added.

## Micro Deployment for Customer Proof Of Concept (POC)

- **DPM Range**: 0 - 5,000 DPM (datapoints per minute)
- **Target Use Case**: POC environments
- **Data Visualization**: 5 CPU and 32 GB RAM

**Estimated Total**: 18 cores, 80 Gi RAM

- About 150 Gi free space for every Kubernetes node for images, logs, etc.
- About 250 Gi attached storage for database mounts.

## Small Deployment

- **DPM Range**: 5,000 - 30,000 DPM
- **Target Use Case**: Development, QA, and penetration-testing environments
- **Data Visualization**: 5 CPU and 32 GB RAM

**Estimated Total**: 25 cores, 70 Gi RAM

- About 150 Gi free space for every Kubernetes node for images, logs, etc.
- About 512 Gi attached storage for database mounts.

## Medium Deployment

- **DPM Range**: 30,000 - 215,000 DPM
- **Target Use Case**: Small production environments
- **Data Visualization**: 5 CPU and 64 GB RAM

**Estimated Total**: 34 cores, 225 Gi RAM

- About 150 Gi free space for every Kubernetes node for images, logs, etc.
- About 1 Ti Storage attached storage for database mounts.

## Large Deployment

- **DPM Range**: 215,000 - 300,000 DPM
- Target Use Case: Production environments with moderate to high load
- **Data Visualization**: 5 cpu and 64gb RAM

**Estimated Total**: 53 cores,432 Gi RAM

- About 150 Gi free space for every Kubernetes node for images, logs, etc.
- About 2 Ti Storage attached storage for database mounts.

## Extra Large Deployment

- **DPM Range**: 300,000 - 900,000 DPM
- **Target Use Case**: High-scale production environments with heavy workloads
- **Maximum Single Instance**: 977,000 DPM
- **Data Visualization**: 8 CPU and 128 GB RAM

**Estimated Total**: 93 cores, 700 Gi RAM

- About 150 Gi free space for every Kubernetes node for images, logs, etc.
- About 4 Ti Storage attached storage for database mounts.

# Cluster Sizing Guidelines for Skylar Advisor

The sizing guidelines for Skylar Advisor are independent of Skylar Analytics. For example, you could have a medium-sized deployment of Skylar Analytics with a small-sized deployment of Skylar Advisor. These requirements are in addition to the requirements of Skylar Advisor.

The deployment size is based on the number of expected active concurrent users and the size of the Corpus in Skylar Advisor.

## Small Deployment

- **GPU**: 4 NVIDIA RTX 6000 GPUs or 4 NVIDIA l40s
- **CPU**: 80 cores
- **Memory**: 450 GB memory
- **Storage**: 250 GB of node memory
- **Attached Storage**: Depends on the expected Corpus size
- **Number of active concurrent users**: 1-15

## Medium Deployment

- **GPU**: 4 NVIDIA H100 or H200s
- **CPU**: 90 cores
- **Storage**: 650 GB of node memory
- **Memory**: 250 GB memory
- **Attached Storage**: Depends on the expected Corpus size
- **Number of active concurrent users**: 16-30

## Large Deployments

- **GPU**: 8 NVIDIA H100 or H200 GPUs
- **CPU**: 170 cores
- **Memory**: 1 Tb
- **Storage**: 250 GB of node memory
- **Attached Storage**: Depends on the expected Corpus size
- **Number of active concurrent users**: 31-120

# Required Infrastructure Dependencies

> **IMPORTANT:** The information in this section is relevant for both Skylar Analytics and Skylar Advisor deployments.

### Ingress Controller

HTTP/HTTPS traffic routing and SSL termination:

- **Required**: An ingress controller must be installed and configured
- **Recommended**: ingress-nginx controller
- **Alternatives**: AWS Load Balancer Controller, GKE Ingress, Azure Application Gateway, Traefik, or HAProxy Ingress

### OpenTelemetry Operator

Install the OpenTelemetry Operator with custom image:

```
# Install OpenTelemetry Operator with custom image
helm registry login
helm install opentelemetry-operator
```

```
oci://registry.scilo.tools/skylar/opentelemetry-helm-charts/opentelemetry-
operator \
  --version 0.114.0 \
  --namespace opentelemetry-operator \
  --create-namespace \
  --set "manager.collectorImage.repository=registry.scilo.tools/skylar/sl-
otelcol" \
  --set "manager.collectorImage.tag=0.16" \
  --set admissionWebhooks.certManager.enabled=false \
  --set admissionWebhooks.autoGenerateCert.enabled=true
```

**TIP:** If the formatting in the code snippets in this document are not retained when you copy and paste them, use the code snippets in the online version of this manual.

If you are using Cert-Manager for your certificate management, you can remove the following lines:

```
--set admissionWebhooks.certManager.enabled=false \
--set admissionWebhooks.autoGenerateCert.enabled=true
```

# Recommended Infrastructure Components

**IMPORTANT:** The information in this section is relevant for both Skylar Analytics and Skylar Advisor deployments.

## Load Balancing

A load balancer solution is needed to distribute traffic across worker nodes:

- **Self-hosted**: F5 BIG-IP, HAProxy with floating IP, or MetalLB
- **Cloud**: Application Load Balancer (ALB) or Network Load Balancer (NLB)

## DNS and TLS Requirements

Required:

- **FQDN**: A fully qualified domain name pointing to the load balancer
- **TLS Certificate**: Valid TLS certificate for the FQDN, provided as a Kubernetes secret

## Optional Monitoring Integration

Prometheus-based Monitoring

- **Supported**: Integration with existing Prometheus deployments
- **Benefits**: Custom metrics export from Skylar AI services

# Chapter 2

# The Installation Process for Skylar AI

## Overview

The installation and configuration of Skylar AI and Skylar Advisor uses Harbor for the registry and Helm for deployment. The Skylar AI platform is deployed as a single Helm umbrella chart containing over 20 microservices, databases, and supporting infrastructure components.

This chapter explains how to get access to the registry for the installation, how to run the installation, and how to validate your installation.

This chapter covers the following topics:

# Registry Access Setup

**IMPORTANT:** The information in this section is relevant for both Skylar Analytics and Skylar Advisor deployments.

## Step 0: Pre-flight Validation

Perform all of the following validations before continuing to Step 1:

1. Verify the Kubernetes version; the minimum is version 1.35:

   ```
   kubectl version
   ```

2. Verify the container runtime version; ContainerD 2.1 or later is required:

   ```
   containerd --version
   ```

3. Verify that the GPU Operator is running:

   ```
   kubectl get pods -n gpu-operator
   ```

4. Verify that GPUs are visible to Kubernetes:

   ```
   kubectl describe nodes | grep -A5 'nvidia.com/gpu'
   ```

5. Verify that storage classes are available:

   ```
   kubectl get storageclass
   ```

6. Test the registry login:

   ```
   helm registry login registry.scilo.tools
   ```

7. Verify that the ingress controller is running (adjust the namespace for your controller):

   ```
   kubectl get pods -n ingress-nginx
   ```

8. When all of the checks have passed, continue to Step 1.

## Step 1: Obtain Registry Credentials

1. Navigate to the registry at https://registry.scilo.tools/. The Harbor landing page appears.
2. Click **[Login via OIDC Provider]**.
3. Click **[Customer Login]**.
4. Enter your Salesforce credentials provided by ScienceLogic.

5. Click your name in the top right corner and select *User Profile*.
6. Click the copy icon in the ***CLI Secret*** field for use in the next steps.

### Step 2: Sign into Helm Registry (Required)

You must authenticate with the Helm registry before proceeding with any chart operations. You authenticate with the registry using your Harbor CLI credentials (from step 6 in the previous procedure):

```
helm registry login registry.scilo.tools --username <your-harbor-username>
```

### Step 3: Download the Skylar AI Chart

Use Helm to pull the Skylar AI**Chart.yaml** file from the registry , using the registry login from Step 2:

```
helm pull oci://registry.scilo.tools/skylar/skylar-charts
```

Decompress the charts:

```
tar -xvf skylar-charts-x.x.x.tgz
```

### Scaling Profiles

Choose the appropriate scaling profile based on your environment. These scaling profiles can be located within the downloaded Helm chart inside the sizing directory. Please work with your ScienceLogic Sales Engineer to understand which scaling profile you will need to deploy. Most Proof of Concepts (PoC) systems can be deployed with a *small* profile.

> **NOTE:** This document will use **small.yaml** in the following steps, though larger deployments will need other files such as **medium.yaml** or **large.yaml**.

## Installation Process

> **IMPORTANT:** Unless noted otherwise, the information in this section is relevant for *both* Skylar Analytics and Skylar Advisor deployments.

### Step 1: Environment Configuration

You will need to prepare the Helm override files with environment-specific details. Inside the decompressed **skylar-charts** you will find an example directory.

If you are deploying Skylar Analytics, populate the **examples/override-analytics.yaml** by creating a copy locally:

```
cp skylar-charts/examples/override-analytics.yaml .
```

```
cp skylar-charts/sizing/analytics-small.yaml .
```

If you are using a proxy for egress Internet traffic, be sure to un-comment the sections that set the `HTTP_PROXY/HTTPS_PROXY/NO_PROXY` environment variables in the **override-analytics.yaml** file.

If you are also deploying Skylar Advisor with Skylar Analytics, you will need to complete the **examples/override-advisor.yaml** file. For Skylar Advisor you will need a fourth override that specifies the GPU-specific tolerations and resources. You will need to work directly with your sales engineer to come up with this configuration. You can find examples of this file inside the sizing directory, such as **sizing/l40s-rtx6000-combined.yaml** or **sizing/h100-resources.yaml**:

```
cp skylar-charts/examples/override-advisor.yaml .
```

```
cp skylar-charts/sizing/l40s-rtx6000-combined.yaml .
```

If you are also deploying Skylar Advisor, you will want to be aware of the following requirements:

- A GPU sizing file is necessary. Work with ScienceLogic to determine the best configuration.
- Skylar Advisor requires a `storageClass` that allows RWX, because Skylar Advisor requires a shared filesystem across services.

## Monitoring the Integration (Optional)

If you have an existing Prometheus setup, you can configure it to scrape metrics from Skylar AI services.

In the **override.yaml** file, enable the metrics endpoints:

```
global:
  enableMonitoring: true
```

This setting exposes Prometheus metrics endpoints on Skylar AI services that can be scraped by your existing Prometheus deployment. Configure your Prometheus to discover and scrape these endpoints based on your service discovery method, such as Kubernetes service discovery or static configurations.

You can ingest your scraped metrics from Prometheus into Skylar One leveraging the "SL1 Prometheus" PowerPack.

## Ingress Controller-Specific Annotations

Inside the **override-analytics.yaml** file, you will need to add annotations specific to your ingress controller. Skylar AI recommends the following ingress annotations. Each controller will be different, so the ingress nginx annotations below are only an example. If you are using Traefik or some other ingress controller, you will need to work with a ScienceLogic Sales Engineer to understand the comparable annotations.

**TIP:** If the formatting in the code snippets in this document are not retained when you copy and paste them, use the code snippets in the online version of this manual.

```
#ingress-nginx
```

```
global:
  ingress:
    className: external
    annotations:
      nginx.ingress.kubernetes.io/proxy-body-size: 1024m
      nginx.ingress.kubernetes.io/proxy-buffer-size: 512k
      nginx.ingress.kubernetes.io/proxy-buffering: "on"
      nginx.ingress.kubernetes.io/proxy-buffers-number: "4"
      nginx.ingress.kubernetes.io/proxy-max-temp-file-size: 1024m
      nginx.ingress.kubernetes.io/proxy-read-timeout: "300"


skylar-auth:
  ui:
    ingress:
      className: external
      sl1embed:
        annotations:
          nginx.ingress.kubernetes.io/rewrite-target: "/skylar-auth/sl1em-
bed"
          nginx.ingress.kubernetes.io/configuration-snippet: |
            more_clear_headers "Content-Security-Policy";
            more_set_headers "Content-Security-Policy: frame-ancestors:
*;";


 #If deploying advisor add in the below
 skylar-advisor-ui:
  ingress:
    annotations:
      # enables launching content residing outside our domain (eg:
storylane)
      nginx.ingress.kubernetes.io/configuration-snippet: 'more_clear_head-
ers "Content-Security-Policy"; more_set_headers "Content-Security-Policy:
frame-ancestors: *;";'
```

## Step 2: Deploy the Skylar AI Platform

Run the following steps to deploy the Skylar AI platform with the scaling profile and customer overrides:

**TIP:** If the formatting in the code snippets in this document are not retained when you copy and paste them, use the code snippets in the online version of this manual.

```
helm upgrade --install skylar-production \
  oci://registry.scilo.tools/skylar/skylar-charts \
  --namespace skylar-production \
  --create-namespace \
  --values sizing/analytics-small.yaml \
  --values /path/to/override.yaml
```

**NOTE:** For non-reference GPU configurations, a custom Advisor sizing file must be built. Contact ScienceLogic engineering for assistance.

If you are enabling Skylar Advisor, add:

```
--value override-advisor.yaml
--value l40s-rtx6000-combined.yaml
```

**NOTE:** The second **.yaml** file name above is just an example. You can name this file based on the GPU being deployed.

When running the Helm install command, you can open a second and third terminal to monitor pod creation and events in parallel while the Helm install runs:

1. Open a second terminal, full pod state, that refreshes every two seconds:

   ```
   watch kubectl get pods -n skylar-production
   ```

   **NOTE:** The `watch` command is preferred over `kubectl get pods -w` because `-w` only shows incremental changes, while `watch` shows the full current state.

2. Open a third terminal and watch for error events:

   ```
   kubectl get events -n skylar-production --sort-by='.lastTimestamp' -w
   ```

### Step 3: Configure TLS Certificate (Optional)

> **NOTE:** You can skip this step if you have automated certificate management (such as cert-manager) or deployment processes that handle TLS configuration.

Create a TLS secret with your provided certificate and private key:

```
kubectl create secret tls skylar-tls-secret \
  --cert=path/to/your/certificate.crt \
  --key=path/to/your/private.key \
  --namespace=skylar-production
```

## Validation and Access

> **IMPORTANT:** The information in this section is relevant for both Skylar Analytics and Skylar Advisor deployments.

### Verify Deployment Status

Run the following commands to verify your deployment was successful:

1. Check to see if all pods are running:

   ```
   kubectl get pods -n skylar-production
   ```

2. Verify the ingress configuration:

   ```
   kubectl get ingress -n skylar-production
   ```

### Access the Platform

1. Verify DNS Resolution:

   ```
   nslookup skylar.yourdomain.com
   ```

2. Navigate to the Skylar AI user interface using your provided FQDN, such as https://skylar.<*yourdomain*>.com.
3. Log in for the first time with the default email of skylar@sciencelogic.com.
4. Set a password for your first login. The password must be at least 15 characters, with at least one special character required.

5. To set up a new Skylar AI account, see *Provisioning a New Account*.
6. For more information about other Skylar AI settings, see *Configuring Skylar AI System Settings*.

If your first login results in a timeout loop after password change:

1. Press **[Ctrl]**+**[Shift]**+**[Delete ]**and clear the browser cache and cookies.
2. If the issue persists, try a different browser.
3. Wait 2-3 minutes and retry the login.

> **NOTE:** The timeout issues might differ between NGINX and Traefik ingress controllers. Report occurrences to ScienceLogic support for investigation.

# Chapter

# 3

# Troubleshooting and Security for Skylar AI

## Overview

This chapter includes a list of common issues with the installation process for Skylar AI. This chapter also include security considerations, backup and recovery procedures, and a list of potentials topics where you might need to contact Skylar AI Enablement.

This chapter covers the following topics:

# Troubleshooting the Installation Process

**IMPORTANT:** The information in this section is relevant for both Skylar Analytics and Skylar Advisor deployments.

## Common Issues

### Images Pull Slowly or Appear to be Stuck

If images are pulling very slowly or appear to be stuck during Helm install, try the following procedures:

- Check if the images are actively pulling instead of being stuck by running:

```
kubectl describe pod <pod-name> -n skylar-production | grep -A10
Events
```

- Test the manual pull speed to isolate registry vs. Kubernetes behavior:

```
skopeo copy docker://registry.scilo.tools/skylar/<image>:<tag>
oci:/tmp/test-pull
```

- Optional: limit concurrent image downloads in **/etc/containerd/config.toml**:

```
max_concurrent_downloads = 3
```

```
sudo systemctl restart containerd
```

### Image Pull Failures

- Verify that the registry secret is correctly configured.
- Check that the CLI secret is still valid in Harbor.
- Ensure the namespace has access to the registry secret.
- Verify that the Helm registry login was successful.

### TLS Certificate Issues

- Verify that the TLS secret contains a valid certificate and key.
- Check that certificate matches the FQDN.
- Ensure the certificate is not expired.

### DNS Resolution Issues

- Verify that the FQDN points to the correct load balancer IP.
- Check the DNS propagation if recently updated.

### Ingress Controller Issues

- Verify that the ingress controller is running and healthy.
- Check the ingress controller logs for errors.
- Ensure that the ingress class name matches your controller.
- Verify that the ingress annotations are compatible with your controller.

### Pod Startup Failures

- Check the resource constraints and storage availability.

### Database Connection Issues

- Ensure that the ClickHouse and PostgreSQL pods are healthy.

### Large Upload/Download Issues

- Verify that the ingress controller supports large request bodies (256 MB and up).
- Check the proxy timeout configurations.
- Ensure that the proper buffering settings are applied.

## Cloud-Specific Issues

### AWS

- Check the IAM permissions for EBS/EFS access.

### GCP

- Verify the service account permissions for persistent disks.

### Azure

- Ensure the proper RBAC for storage resources.

# Useful Commands

## Deployment Status Commands

To check the deployment status:

```
helm status skylar-prod -n skylar-production
```

To view pod logs for troubleshooting:

```
kubectl logs <pod-name> -n skylar-production
```

To describe the pod for detailed information

```
kubectl describe pod <pod-name> -n skylar-production
```

## Infrastructure Verification Commands

To check the ingress controller status (adjust the namespace based on your setup):

```
kubectl get pods -n ingress-nginx
```

To check persistent volume claims:

```
kubectl get pvc -n skylar-production
```

To test registry connectivity:

```
kubectl run test-registry --image=registry.scilo.tools/skylar/skylar-
charts:latest \ --dry-run=client -o yaml | kubectl apply -f -
```

# Registry Authentication Issues

If you encounter image pull errors:

- Make sure the CLI secret has not expired in Harbor.
- Re-authenticate with the Helm registry login.
- Verify that the Kubernetes secret was created correctly.
- Make sure the secret exists in the correct namespace.

# TLS Certificate Issues

If you encounter TLS-related problems:

- Verify that the certificate is valid for your FQDN.
- Make sure the certificate is in PEM format.

- Include intermediate certificates if required.
- Verify that the private key matches the certificate.

### Ingress Controller Issues

If ingress resources are not working:

- Verify that the ingress controller is running.
- Make sure the ingress class name matches your controller.
- Check the ingress controller logs for configuration errors.
- Make sure the backend services are healthy and have endpoints.
- Make sure the ingress annotations are supported by your controller.

## Security Considerations

> **IMPORTANT:** The information in this section is relevant for both Skylar Analytics and Skylar Advisor deployments.

### Security Best Practices

- **Registry Credentials**: Store CLI secrets securely and rotate them regularly.
- **TLS Certificates**: Ensure certificates are from trusted CAs and renewed before expiration.
- **Network Policies**: Consider implementing Kubernetes network policies to restrict inter-pod communication.
- **RBAC**: Configure appropriate role-based access controls for the Skylar AI namespace.
- **Ingress Security**: Configure appropriate security headers and rate limiting on your ingress controller.
- **Secrets Management**: Use external secret management solutions, such as HashiCorp Vault, or AWS Secrets Manager for production.
- **Cloud Security**: Follow cloud provider security best practices.
- **Third-Party Components**: Monitor security advisories for included third-party components.

### Third-Party Security Responsibilities

While ScienceLogic validates and updates third-party chart versions with each Skylar AI release, customers should:

- **Monitor Security Advisories**: Stay informed about security issues in included third-party components.
- **Plan for Updates**: Be prepared to upgrade Skylar AI when security patches are available.

- **Vulnerability Assessment**: Include third-party components in security scanning and assessment processes.
- **Risk Management**: Understand the security posture of all included dependencies.

# Backup and Recovery

> **IMPORTANT:** The information in this section is relevant for both Skylar Analytics and Skylar Advisor deployments.

## Critical Data Components

Skylar AI stores critical data in the following persistent volumes, which must be backed up regularly.

### ClickHouse Data Volumes

- Contains analytics data, metrics, and time-series information.
- Recommended backup frequency: Daily with 30-day retention.

### PostgreSQL Data Volumes

- Contains application metadata, user data, and configuration.
- Recommended backup frequency: Daily with 30-day retention.

## Backup Strategy Options

This section covers the different types of backup strategies you can use with Skylar AI.

### Volume-Level Backups

- Use cloud provider snapshot capabilities, such as AWS EBS, GCP Persistent Disks, or Azure Disks.
- Implement Kubernetes volume snapshots using CSI drivers.
- Consider third-party backup solutions like Velero for comprehensive cluster backup.

### Application-Level Backups

- Database-native backup tools for ClickHouse and PostgreSQL.
- Export application configuration and secrets.
- Backup Helm chart values and deployment configurations.

### Hybrid Approach

- Combine volume snapshots for fast recovery with application-level backups for granular restore options.
- Implement both local and off-site backup storage for disaster recovery.

## Backup Verification

### Regular Testing Requirements

- Monthly: Test backup restoration procedures in non-production environment.
- Quarterly: Full disaster recovery simulation.
- Document and validate recovery time objectives (RTO) and recovery point objectives (RPO).

### Monitoring and Alerting

- Monitor backup job completion and success rates.
- Alert on backup failures or missing backups.
- Verify backup accessibility and integrity.

## Configuration Backup

### Helm and Kubernetes Configuration

- Export and store Helm values files.
- Backup Kubernetes secrets and ConfigMaps.
- Maintain version-controlled infrastructure as code.

> CAUTION: Store configuration backups containing secrets in encrypted storage with restricted access. Never commit secrets to version control systems.

For detailed backup implementation guidance, consult your cloud provider's backup documentation and the Kubernetes Backup Best Practices.

# Support

**IMPORTANT:** The information in this section is relevant for both Skylar Analytics and Skylar Advisor deployments.

For deployment assistance, configuration guidance, or troubleshooting support, contact Skylar AI Enablement. They can provide:

- Environment-specific override file templates.
- Scaling recommendations based on your requirements.
- Custom configuration for enterprise integrations.
- Cloud-specific deployment guidance.
- Registry access troubleshooting.
- TLS certificate configuration assistance.
- Ingress controller configuration guidance.
- Post-deployment optimization.
- Third-party component guidance (limited to integration aspects only).

**NOTE:** Support for third-party components, such as Bitnami charts, is limited to integration and configuration guidance. For issues specific to these components, consult their respective documentation and support channels.

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010