

# IBM® Guardium®

## Essentials-2025



## Disclaimer:

- This session provides an introductory overview of product features and is intended solely as a supplementary learning resource. It is not suitable for implementation purposes. Accurate deployment requires a thorough understanding of the product, its intended use, and environment—none of which are covered in this session.
- Content is subject to change as the product evolves. We do not accept responsibility for decisions made based on this material, and any actions taken are at your own risk. We disclaim liability for any resulting damages.
- For the most current and accurate IBM documentation, please refer to: <https://www.ibm.com/docs/en/gdp>
- By continuing to participate, you acknowledge and accept these terms. If you do not agree, please disconnect from the session.

**Speaker for today:**



**Can Wang**

**Technical Support Professional, Data Security**

# IBM Guardium Essentials-2025

## 8-Session Kickstart Series

Master the Foundations of Data Security Monitoring & Compliance

| Session   | Date         | Topic                                        | Registration Link                                               |
|-----------|--------------|----------------------------------------------|-----------------------------------------------------------------|
| Session 1 | Aug 26 (Tue) | What is IBM Guardium & How It Works          | <a href="https://ibm.biz/IBMGE-S1">https://ibm.biz/IBMGE-S1</a> |
| Session 2 | Aug 28 (Thu) | Installing & Configuring Guardium Appliances | <a href="https://ibm.biz/IBMGE-S2">https://ibm.biz/IBMGE-S2</a> |
| Session 3 | Sep 02 (Tue) | GIM & WINSTAP Deployment                     | <a href="https://ibm.biz/IBMGE-S3">https://ibm.biz/IBMGE-S3</a> |
| Session 4 | Sep 04 (Thu) | Introduction to Guardium Policies            | <a href="https://ibm.biz/IBMGE-S4">https://ibm.biz/IBMGE-S4</a> |
| Session 5 | Sep 09 (Tue) | GIM & S-TAP for UNIX/Linux                   | <a href="https://ibm.biz/IBMGE-S5">https://ibm.biz/IBMGE-S5</a> |
| Session 6 | Sep 11 (Thu) | Guardium Reports, Entities & Attributes      | <a href="https://ibm.biz/IBMGE-S6">https://ibm.biz/IBMGE-S6</a> |
| Session 7 | Sep 16 (Tue) | Guardium Alerts & Audit Process              | <a href="https://ibm.biz/IBMGE-S7">https://ibm.biz/IBMGE-S7</a> |
| Session 8 | Sep 18 (Thu) | Aggregation, Backup & Restore in Guardium    | <a href="https://ibm.biz/IBMGE-S8">https://ibm.biz/IBMGE-S8</a> |

Use above links to Register for each session!

Session 8:

# IBM® Data Security

## Aggregation, Backup and Restore in Guardium

-Can Wang

Technical Support Professional, IBM Software Support (Data Security)



# Agenda

- Guardium Data Management Overview
- ↓
- Guardium Aggregation: Data Export & Data Import
- ↓
- DEMO 1: Data Export & Data Import
- ↓
- Guardium Data Archive, Purge & Data Restore
- ↓
- DEMO 2: Data Archive, Purge & Archive Restore
- ↓
- Guardium System Backup & Restore Backup
- ↓
- DEMO 3: System Backup & Restore Backup
- ↓
- Considerations for Aggregation, Archive and Backup
- ↓
- Q&A



*This session and its demo are based on **Guardium V12.1***



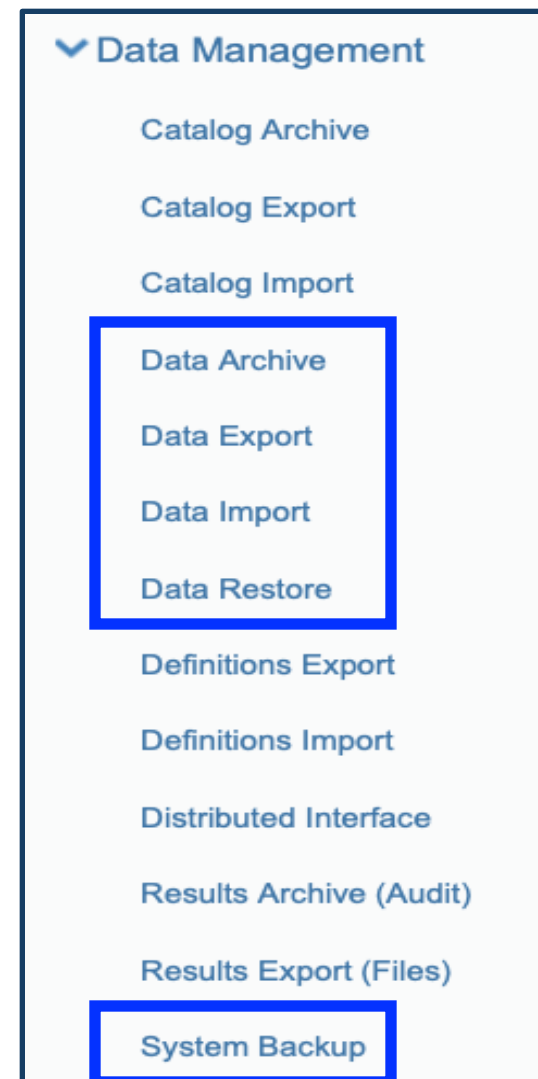
# Guardium Data Management Overview

## 1. Data stored in Guardium appliance

- **Audit data:** From Guardium agents or Guardium supported interception methods
  - ✓ **dynamic traffic data** a.k.a dynamic tables (*session, instance, full sql, etc.*)
  - ✓ **static traffic data** a.k.a **static tables** (*access, construct, object, field, sentence, etc.*)
- **Guardium's configuration setting**
- **Guardium's self monitoring info**

## 2. Guardium's Typical Data Management Activities (focus of this training)

- Guardium Data Aggregation (Data Export and Data Import)
- Guardium Data Archive, Purge, and Data (Archive) Restore
- Guardium System Backup & System Backup Restore



# What is Guardium's Data Aggregation?

## Definition:

Collect and merge information from multiple Guardium® units into a single Guardium **Aggregator** appliance to offload the reporting and analysis function from the collectors, while also providing a consolidated view of the data from multiple collectors.

## Data Aggregation consists of:

### ➤ Data Export:

Exporting data on a regular(e.g. daily) basis from the source appliances to the Aggregator (copying daily export files to the aggregator)

### ➤ Data Import:

Aggregator then goes over the uploaded files, extracts each file and merges it into the internal repository on the **Aggregator**

**NOTE: Hierarchical Aggregation** is also supported, where multiple aggregators merge upwards to a higher-level, central aggregator. Useful for multi-level views



For more details: [\*IBM Guardium V12.x Data Aggregation\*](#)



# Data Export

For more details: [IBM Guardium V12.x Exporting Data](#)



GUI > Manage > Data Management > **Data Export**

- Purpose of Data Export is to send data from appliance to aggregator via **SCP** in daily chunks
  - ✓ Source appliance can be collector or aggregator (2-level aggregation)
- Each day's data is stored in a **separate file that is both compressed and encrypted**(using Shared Secret)
- The Export includes **daily dynamic data**; and **daily incremental static data**, OR **full static data** if “**next\_export\_static**” is **on** for one of the following scenarios:
  - ✓ On the 1<sup>st</sup> day of each month
  - ✓ When Data Export is configured to a new aggregator
  - ✓ When user executes the CLI command: “*store next\_export\_static on*”
- Test file is sent to the defined Aggregator using **SCP** when configuration is saved

**Data Export**

Configuration

☒ Export

\* Export data older than  Day(s) ▾

Ignore data older than  Day(s) ▾

☒ Export values

\* Host  ▾

Secondary Host  ▾

# Data Import

## Configuration (only available on Aggregator):

GUI > Manage > Data Management > **Data Import**

- Import job is handling files exported from collector (or aggregator in case of 2nd-level aggregation) ordered by dates
- Import job analyzes import file name, decrypts and merges each exported file one by one, from **the oldest to the newest**
- **NOTE:**
  - ✓ The **Shared Secret** must be **identical** between the source appliance and the Aggregator; otherwise, decryption will fail
  - ✓ Target aggregator's **version and patch level** must be the same or higher than the source appliance's
  - ✓ Daily exported data from each source appliance can only be Imported into Aggregator **once** (avoids duplicates)

Data Import

✕ Data import is not scheduled for execution

Schedule by Day Select days Every Day

Repeat Day  
Schedule tasks to run more than once each day Month

☐ Repeat every 1 hours

☐ Within each hour, run every 1 minutes

★ Start schedule at 3:30 AM

Begin schedule 8/30/2025 3:35 PM

☒ Activate schedule Uncheck this option to suspend the schedule.

☐ Auto run dependent jobs Select this option to enable automatically run dependent jobs

Save Reset Delete Pause Run Once Now



# **DEMO 1:**

## **Data Export & Data Import**



11:21



User Interface



User Interface Search



admin  
admin admin



Machine Type  
Managed Unit



## Get Started on Data Protection with Guardium

View Best Practices



### 1. Manage Your Assets

Manage Databases



Manage Applications



# I. Data Export & Data Import



### 5. Advanced Analytics

Risk Spotter



Active Threat  
Analytics



Install Basic Security  
Monitoring Policy



Investigation  
Dashboard



Guardium release notes

What's new in V12.1

# Data Archive (1)

GUI > Manage > Data Management > **Data Archive**

- The purpose of Archive job is to backup data in daily chunks and send to an **external storage system** for audit data retention
- Each day's data is stored in a separate file that is both **compressed and encrypted** (using the Shared Secret)
- The **format of the archive data file name** is one of:
  - <day of data>-<Guardium system name>-w<time of zip>-d<execution date>.dbdump.enc
  - <day of data>-<Guardium system name>-w<time of zip>-d<execution date>.agg.<guard ver>.tar.gz.enc
- The Archive includes **daily dynamic data**; and **daily incremental static data, OR full static data** if “**archive\_static\_table**” is **on** for one of the following scenarios:
  - ✓ On the 1<sup>st</sup> day of each month
  - ✓ When the target destination configuration for Data Archive is changed
  - ✓ When user executes the CLI command: “*store archive\_static\_table on*”
- Test file is sent to the external storage system using **the configured protocol info** when the configuration is saved



# Data Archive (2)

Data Archive

Configuration

☒ Archive

\* Archive data older than  Day(s)

Ignore data older than  Day(s)

☒ Archive values

\* Protocol ☒ SCP ☐ SFTP (Formerly FTP) ☐ AMAZON S3 ☐ IBM COS (Formerly Cleversafe)

\* Host

\* Directory

\* Port

\* Credential type ☒ Assign credentials ☐ External password

\* Username

\* Password

\* Re-enter password

## All supported external storage systems:

- **SCP** for archive or backup
- **SFTP** for archive or backup
- **Amazon S3** for archive or backup
- **IBM COS** (formerly Cleversafe) for archive or backup
- **ECS** for archive or backup
- **NFS** backup
- **Tivoli Storage Manager** for archive or backup

## NOTE:

Use CLI command “**store storage-system**” to add or delete a storage system for archiving or system backup. ([command link](#))



For more details about External storage system: [IBM Guardium V12.x Configuring external storage](#)



# Purge

For more details: [IBM Guardium V12.x Purging data](#)



GUI > Manage > Data Management > **Data Archive** > **Purge** section **OR**

GUI > Manage > Data Management > **Data Export** > **Purge** section

- Purge data to free up space and speed up access operations on the internal database
- Purge is triggered **after** Archive or Export completes
- If **both** Export and Archive are configured, Purge will be invoked only after **Archive**.
- Purge does not delete records that are still "**in use**" (e.g., open sessions)
- Purge will not run on days for which data has not been exported or archived, unless the following is selected:

☒ Purge

\* Data older than

☒ Allow purge without exporting or archiving

**NOTE:** The purge operation does not purge restored data whose age is within the “**Don’t purge restored data for at least [X]**” timeframe specified by a Data Restore operation.

# Data Restore

GUI > Manage > Data Management > **Data Restore**

## ➤ Restore Targets:

- ✓ Collector archives → same/different collector or aggregator;
- ✓ Aggregator archives → same/different aggregator.

## ➤ Shared Secret Requirement:

Target appliance must use the same, or has imported the shared secrets used by the source appliance:

- ✓ Use <CLI>**aggregator backup keys file** on the source appliance where the Archive was generated
- ✓ Use <CLI> **aggregator restore keys file** on the target appliance where the Archive needs to be restored

## ➤ Catalog Entry Requirement: Target appliance must have the **catalog entry** for each Archive file that needs to be restored. If the catalog doesn't exist on the target:

- ✓ Method1: <GUI>**Catalog Export/Import** between source and target appliances
- ✓ Method2: <GUI>**Catalog Archive** on the target appliance, to add catalog entry location for the Archive

## ➤ Version Requirement: Target appliance's version and patch level ≥ source appliance's

## ➤ Prevent Purging Restored Data: Set retention days in "*Don't purge restored data for at least [X] days*".

## ➤ Collector only: Stop Sniffer first via CLI: *stop inspection-core*

## ➤ Static Data Restore Rule: Use one of these two methods:

- ✓ Restore the first day of the month and all the following days until the target date.
- ✓ Restore the target date and then the first day of the following month.

## ➤ Duplicate Prevention: If the target appliance already contains the data, the **same data cannot be restored** to avoid duplicates.

Data Restore Search Results

Configuration

Don't purge restored data for at least  (days)

Restore Data

| Select                              | Host Name   | From Date             |
|-------------------------------------|-------------|-----------------------|
| <input checked="" type="checkbox"/> | ind-trg-col | 2025-08-23 00:00:00.0 |

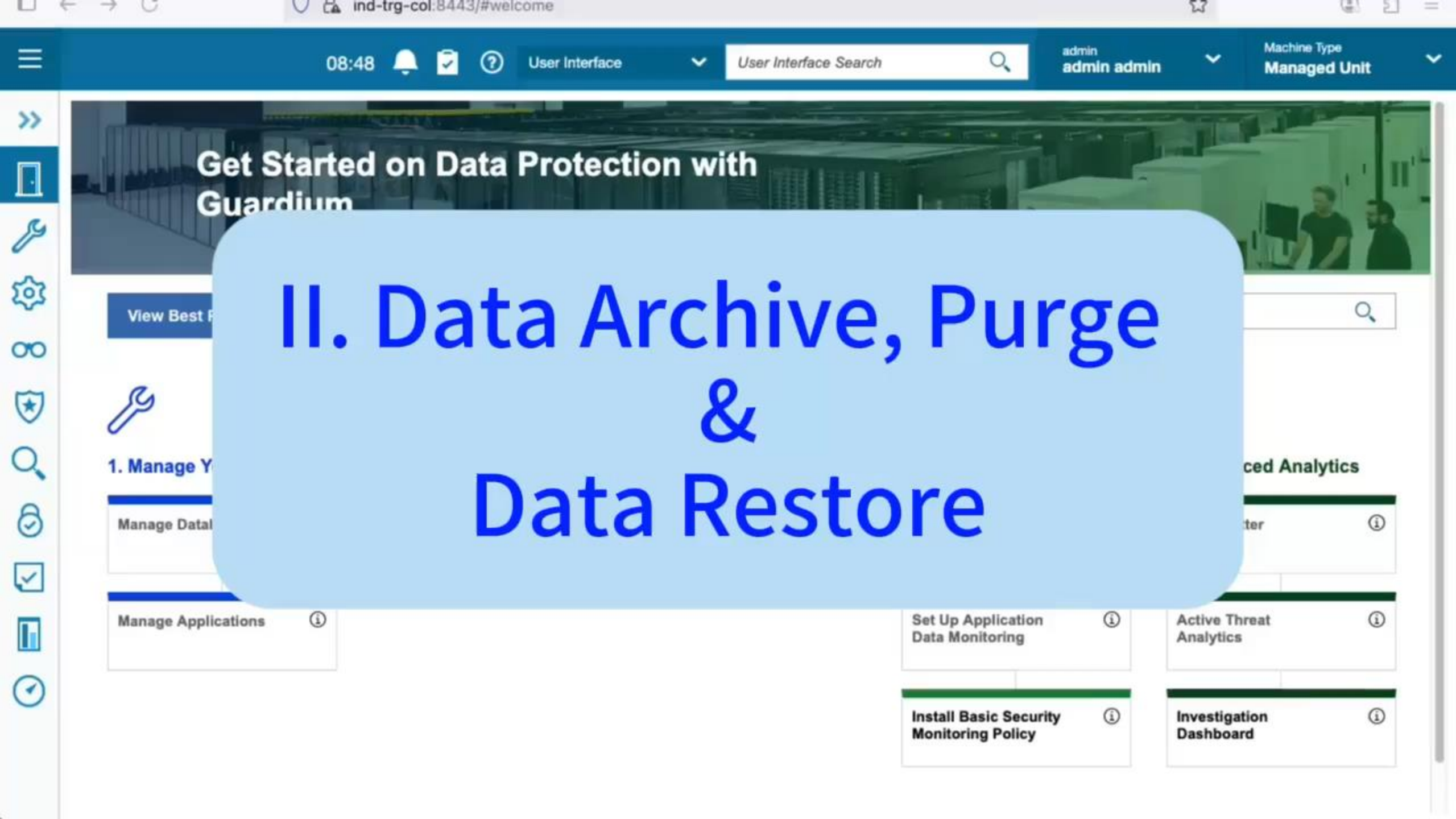
Records: 1 to 1 of 1

For more details: [IBM Guardium V12.x Restoring archived data](#)



# **DEMO 2:**

## **Data Archive, Purge & Data Restore**



Get Started on Data Protection with  
Guardium

## II. Data Archive, Purge & Data Restore

View Best Practices



1. Manage Your Data

Manage Data

Manage Applications

Advanced Analytics

Set Up Application  
Data Monitoring

Active Threat  
Analytics

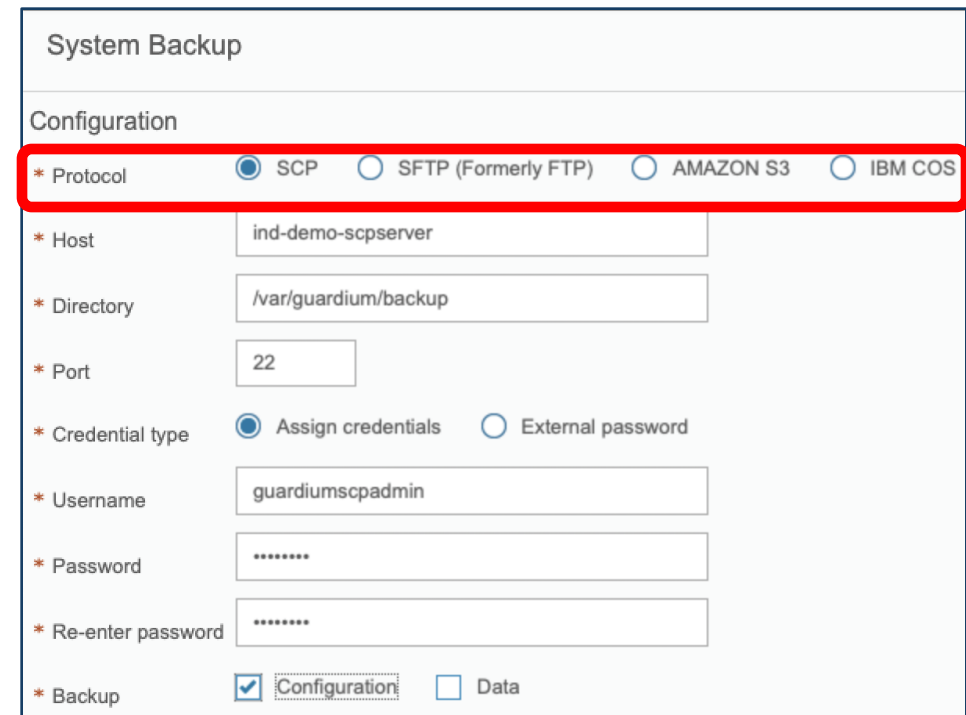
Install Basic Security  
Monitoring Policy

Investigation  
Dashboard

# System Backup

GUI > Manage > Data Management > **System Backup**

- System backup stores all the necessary **data** and **configuration** values to restore a Guardium appliance.
- Two options available:
  - ✓ **Configuration**: to back up important configurations and definitions
  - ✓ **Data**: to back up all data (Not needed if you are archiving data regularly)
- **Data** and **Config Backups** are stored in **separate compressed and encrypted files** and sent to the specified **destination** by using the configured transfer method
- To prevent backup filling up /var disk, backup reports an **error if the backup is over 50%**. For example:  
*ERROR: /var backup space is at 60% used. Insufficient disk space for backup.*



System Backup

Configuration

\* Protocol ☒ SCP ☐ SFTP (Formerly FTP) ☐ AMAZON S3 ☐ IBM COS

\* Host ind-demo-scpserver

\* Directory /var/guardium/backup

\* Port 22

\* Credential type ☒ Assign credentials ☐ External password

\* Username guardiumscpadmin

\* Password .....

\* Re-enter password .....

\* Backup ☒ Configuration ☐ Data

Note: Use “**store storage-system**” to add or delete a storage system for archiving or system backup. ([command link](#))



# Restore Backup

## CLI: restore backup

### Restore Backup Procedure

1. Use an **ISO** to install new appliance with proper type (collector or aggregator)
2. Configure required **network setting**
3. **License:**
  - ✓ Standalone unit or CM – apply the license
  - ✓ Managed unit – register to its CM to get license
4. Make sure the newly built appliance is at **an equal or higher version** than the source appliance where the backup was taken
5. Use '**restore backup**' cli command to restore backup (config and/or data)
  - ✓ NOTE for managed unit: It is **not** necessary to restore the configuration backup because the definitions are pooled from central manager



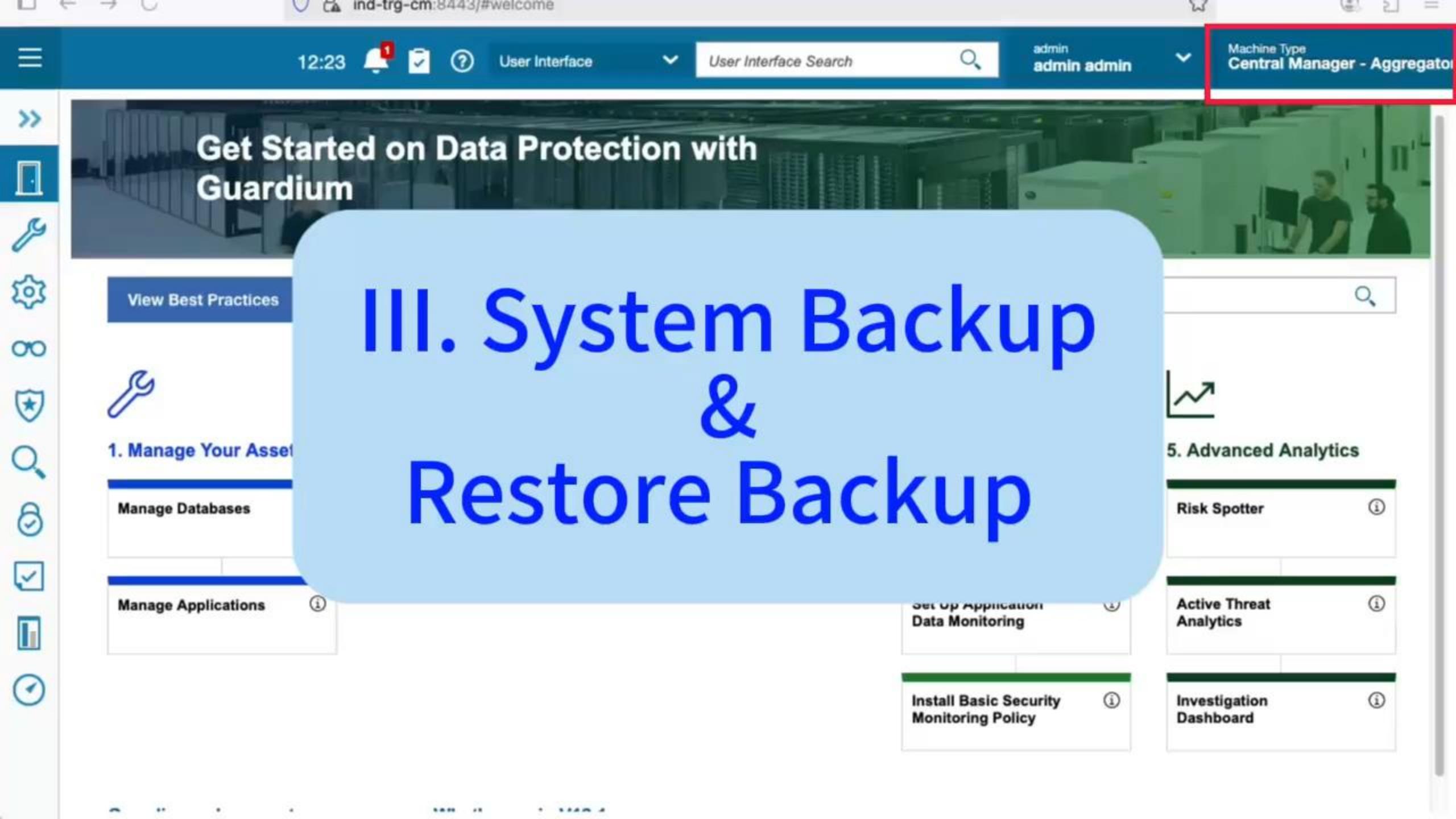
| Item                   | Action Needed                                                    |
|------------------------|------------------------------------------------------------------|
| License                | Re-install manually; or register to the CM if it's managed unit. |
| SSL Certificates       | Reinstall manually (not backed up)                               |
| Language               | <cli>: store language (default: English)                         |
| NTP Settings           | <cli>: store system time_server (with hostname/state)            |
| Time Zone              | <cli>: store system clock timezone                               |
| Enterprise Search data | Not saved in backup (unavailable in restored dashboard)          |

Table: Items not backed up and must be installed/configured manually



# **DEMO 3:**

## **System Backup & Restore Backup**



### III. System Backup & Restore Backup

# Considerations for Aggregation, Archive and Backup

## ➤ Scheduling Guidelines:

- ✓ **Basic Scheduling:** Ensure Aggregation, Archive, and System Backup jobs are scheduled with the required frequency (e.g., daily, weekly, monthly)
- ✓ **Job Duration Estimation:** Use the "Run Once Now" function to roughly estimate the duration of each job. Use this information to set schedules and monitor operations.
- ✓ **Key Notes for Aggregators:**
  - Ensure the Aggregator's **Data Import** schedule is triggered **after** the Collector's **Data Export** completes.
  - Ensure the Aggregator's **Data Archive** schedule is triggered **after Data Import** completes.

## ➤ Only one aggregation-related job can run at any given time

- ✓ If a new aggregation process is triggered while another aggregation, archiving, or backup job is already in progress, the new aggregation process will fail and return the error message:

*"Another aggregation process is currently running, **please check the schedule.**"*

## ➤ Note on Large Archive/Export Files

- ✓ Exercise caution with large daily Archive/Export files. Such files take longer to generate and process, which can degrade aggregation performance and delay other scheduled jobs.
- ✓ Since Archive/Export data consists of audit logs logged as per the currently installed Policy, **persistent large files indicate a need to review and optimize the existing Policies as needed.**



# Appendix: Data Import - How to Recover Failed Import

In case Import process fails, the import file is copied to a dedicated location within Aggregator with a **failed suffix**

**E.g** `739865-ind-trg-col.xxxxxxxxxxx.com-w20250909.144427-d2025-09-06.agg.120.tar.gz.enc.read_failed`

After the problem that caused the previous import failure is resolved, the failed import files can be restored by CLI commands:

1. List failed import: `<cli>aggregator list failed imports`
2. Recover failed import:  
`<cli> aggregator recover failed import <all | filename>`

Next Import job will pick up recovered file and will try to import the data again.

NOTE: Be cautious when set to recover 'all'! By triggering Import to import all might fill up the Aggregator

For more details about the CLI commands: [IBM Guardium V12.x Aggregator CLI Commands](#)



# Appendix: Clean Static Orphans

- Orphans are records in static tables (GDM\_OBJECT, GDM\_FIELD, GDM\_SENTENCE, GDM\_CONSTRUCT, etc.) that have no connection to sessions
- Orphans Cleanup invoked at the **end of the daily purge process**. It can be switched on/off by the following cli command:  
**store run\_cleanup\_orphans\_daily [on|off]**
- We recommend to keep it on to clean orphaned records daily
- On Aggregator, you can use the following CLI command to optimize Orphans Cleanup performance if needed:  
**store aggregator orphan\_cleanup\_flag [small | large | analyze]**

Find more about the above two CLI commands: [\*IBM Guardium V12.1 Aggregator CLI Commands\*](#)



# References: Basic Knowledge

- Managing data: archive, restore, aggregation, and system backup: <https://www.ibm.com/docs/en/gdp/12.x?topic=system-managing-data-archive-restore-aggregation-backup>
- Data aggregation: <https://www.ibm.com/docs/en/gdp/12.x?topic=backup-data-aggregation>
- Configuring the data archive: <https://www.ibm.com/docs/en/gdp/12.x?topic=data-configuring-archive>
- Purging data: <https://www.ibm.com/docs/en/gdp/12.x?topic=backup-purging-data>
- Restoring archived data: <https://www.ibm.com/docs/en/gdp/12.x?topic=data-restoring-archived>
- Configuring system backup: <https://www.ibm.com/docs/en/gdp/12.x?topic=backup-configuring-system>
- Restoring a Guardium system: <https://www.ibm.com/docs/en/gdp/12.x?topic=backup-restoring-guardium-system>
- Data and Result catalogs: <https://www.ibm.com/docs/en/gdp/12.x?topic=backup-data-result-catalogs>
- Viewing days whose data was not archived or exported: <https://www.ibm.com/docs/en/gdp/12.x?topic=mdarasb-viewing-days-whose-data-was-not-archived-exported>
- Configuring external storage: <https://www.ibm.com/docs/en/gdp/12.x?topic=backup-configuring-external-storage>
- Archiving (audit) results: <https://www.ibm.com/docs/en/gdp/12.x?topic=data-archiving-audit-results>
- Exporting (files) results: <https://www.ibm.com/docs/en/gdp/12.x?topic=backup-exporting-files-results>

# References: Common Troubleshooting

- Data Export configuration change from a Guardium managed system's GUI fails with error:  
<https://www.ibm.com/docs/en/gdp/12.x?topic=aggregation-data-export-configuration-change-from-guardium-managed-systems-gui-fails-error>
- UI banner warning: Data not exported or archived:  
<https://www.ibm.com/docs/en/gdp/12.x?topic=aggregation-ui-banner-warning-data-not-exported-archived>
- Health alerts and UI banner warning: Old partitions found:  
<https://www.ibm.com/docs/en/gdp/11.5.0?topic=aggregation-health-alerts-ui-banner-warning-old-partitions-found>
- Purging data to resolve a full disk when the GUI is down:  
<https://www.ibm.com/docs/en/gdp/12.x?topic=pd-purging-data-resolve-full-disk-when-gui-is-down>
- Guardium aggregation jobs can never be started - "db\_utilization\_summary.sh already running":  
<https://www.ibm.com/support/pages/guardium-aggregation-jobs-can-never-be-started-dbutilizationsummarysh-already-running>

Q&A

Any   
Questions?

Thank you for your attention!



**Feedback & Suggestions are welcome at:**  
[datasec\\_ap\\_support@wwpdl.vnet.ibm.com](mailto:datasec_ap_support@wwpdl.vnet.ibm.com)

