

Asigra Cloud Backup v14.2

Overview Guide

August 2020

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Asigra Inc.

Asigra Inc. makes no representation or warranty, express, implied, or statutory, with respect to, and assumes no responsibility for the accuracy, completeness, sufficiency or usefulness of the information contained herein.

This document may contain sample screen shots, used to demonstrate Asigra Cloud Backup™ procedures. All information appearing in this document is used for illustration purposes only, and should be considered fictitious

The software described in this document is furnished under a license agreement. It is against the law to copy the software on any medium except as specifically allowed in the license agreement.

"Asigra", the Asigra logo, "Asigra Cloud Backup", "Recovery is Everything", and "Recovery License Model" are trademarks of Asigra Inc. All other brand and product names are, or may be, trademarks of their respective owners.

79 Brisbane Road, Toronto, Ontario, Canada M3J 2K3

Release Date: August 2020

Contents

1 About this guide	5
1.1 Intended audience	5
1.2 Formatting conventions	5
2 Introducing Asigra Cloud Backup	7
2.1 Software overview	7
2.1.1 About the backup process	8
2.1.2 About the restore process	9
2.1.3 About online file generations	10
2.2 Product documentation	12
2.2.1 Server software documentation	12
2.2.2 Client software documentation	13
2.2.3 Tools software documentation	13
3 Asigra Cloud Backup components	15
3.1 DS-License Server	15
3.1.1 DS-License Server types	16
3.1.2 DS-License Server models	17
3.1.3 DS-License Server RLM components	17
3.2 DS-System	18
3.2.1 DS-System configurations	20
3.2.2 DS-System types	21
3.3 DS-Client	24
3.3.1 DS-Client configurations	24
3.3.2 DS-Client types	27
3.4 BLM Archiver	27
3.5 DS-Billing	30
3.6 DS-NOC	31
3.7 Management Console	32

1 About this guide

This guide provides an overview of the main Asigra Cloud Backup concepts and features.

1.1 Intended audience

This guide is intended for anyone who requires a high-level overview of the Asigra Cloud Backup solution.

1.2 Formatting conventions

The following formatting conventions are used in this guide:

Bold

Bold font identifies components, window and dialog box titles, and item names.

Italic

Italic font identifies references to related documentation.

`Monospace Font`

Monospace font identifies text that you should type or that the computer displays.

NOTE: Notes emphasize information that is useful but not essential, such as tips or alternative methods for performing a task.

IMPORTANT: Important notes emphasize information that is essential to the completion of a task and draw special attention to actions that could adversely affect the operation of the application or result in a loss of data.

About this guide

Formatting conventions

2 Introducing Asigra Cloud Backup

This chapter provides a high-level overview of the Asigra Cloud Backup solution.

2.1 Software overview

The Asigra Cloud Backup solution is an end-to-end converged data protection solution that delivers maximum security, reliability, manageability, and affordability for private, public, and hybrid clouds for businesses of any size. The agentless DS-Client software collects data from across the LAN before deduplicating, compressing, encrypting, and transmitting the data to the DS-System central data backup repository. Since the software is agentless, there is no need to install and maintain countless agents.

For mobile devices such as laptops, smart phones, and tablets, Asigra's dedicated client apps ensure that all your data can be backed up and restored.

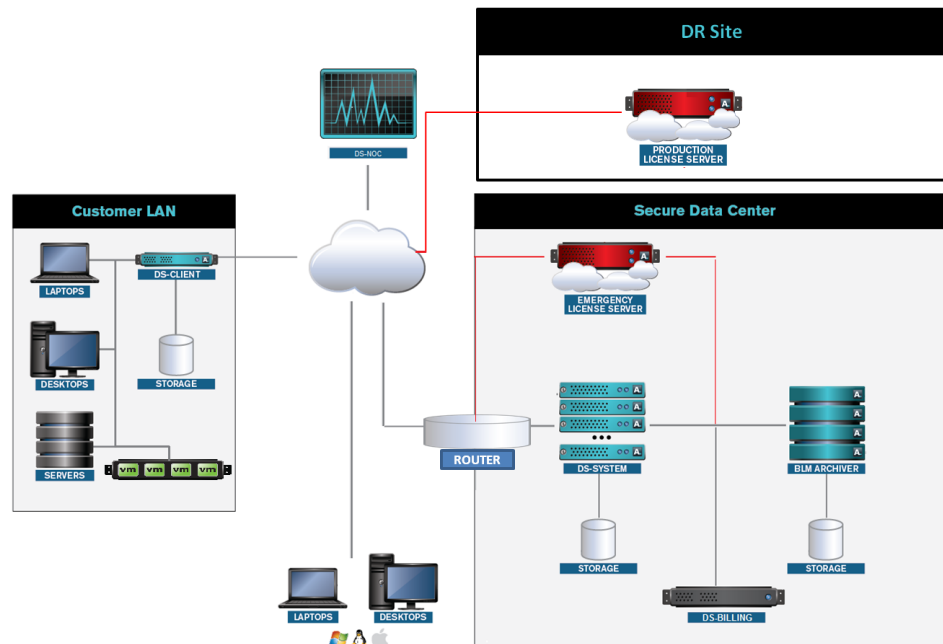


Figure 1 Software architecture

2.1.1 About the backup process

This section provides an overview of the backup process.

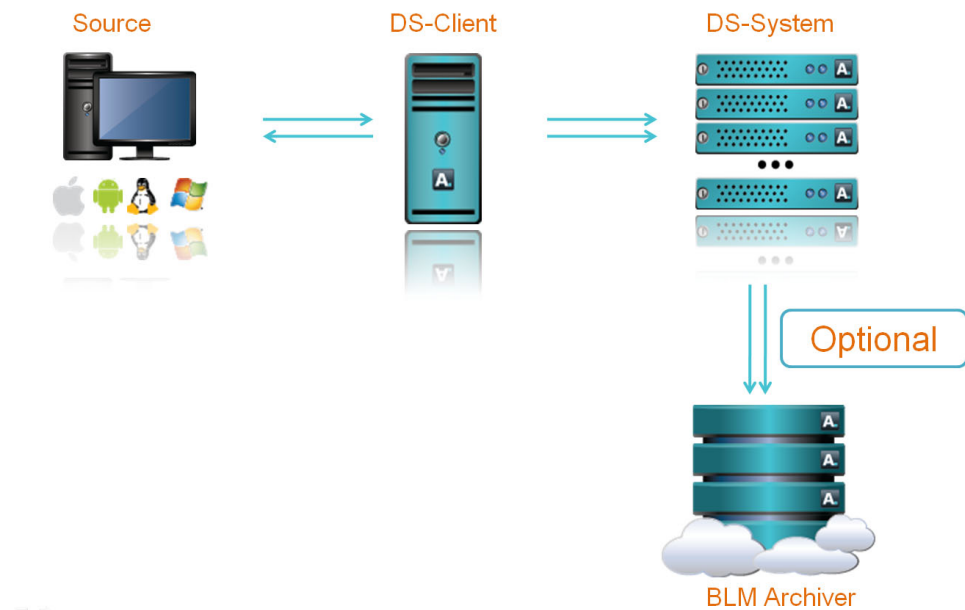


Figure 2 Backup process

The basic steps in the backup process are:

1. The backup is started by schedule or on demand.
2. DS-Client connects to the source computer, scans for data to be backed up for each file, and retrieves the data. Backup data is handled through block-level processing, with changed blocks of data in a file being isolated in subsequent backup sessions.
3. DS-Client processes the data and then performs compression and encryption (even if data was encrypted at source).
4. DS-Client sends the data to the DS-System, which puts the files in online storage. Only the changed blocks are sent to the DS-System. Asigra Cloud Backup features “incremental forever” backups: once a file is sent to DS-System, it is normally never sent again in its entirety.
5. DS-System optionally sends the data to the BLM Archiver, as requested.

The details about what data should be backed up, when it should be backed up, and other related information is stored in the backup set definition.

2.1.2 About the restore process

This section provides an overview of the restore process.

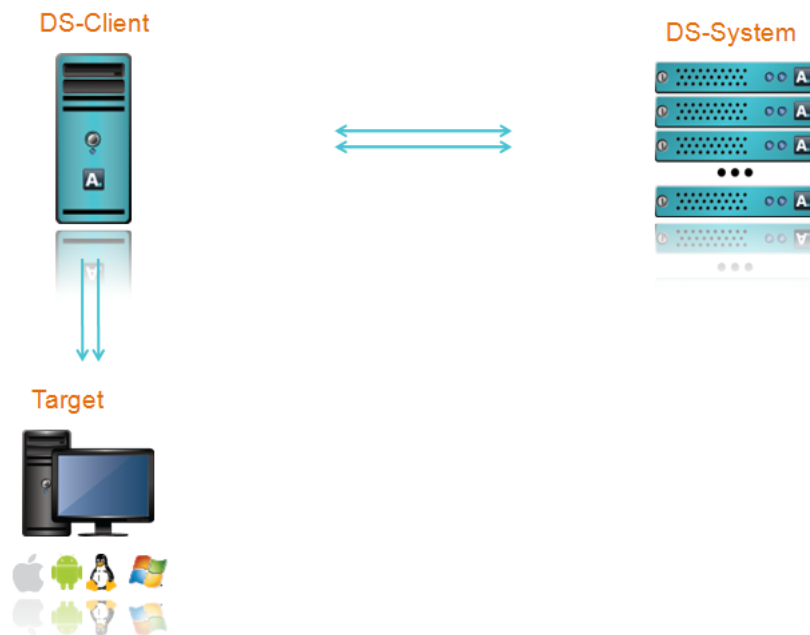


Figure 3 Restore process

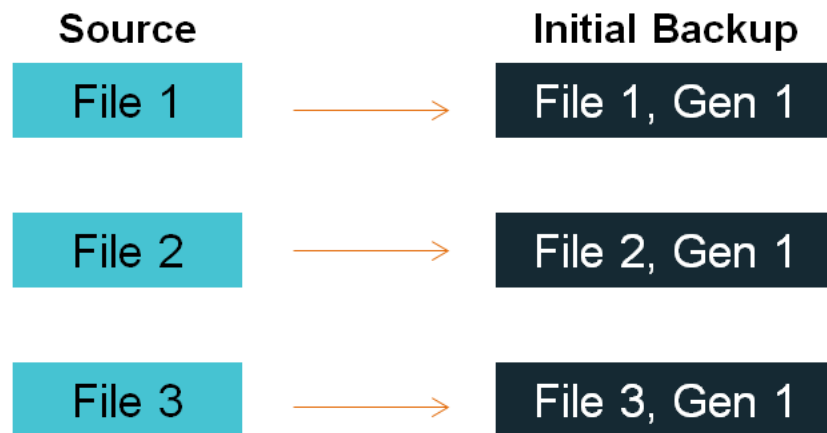
The basic steps in the restore process are:

1. The restore is started on demand. Depending on the backup set type, you can select all or part of the backup, the specific generation, and the target destination for the data.
2. DS-Client requests the data for restore from DS-System.
3. DS-System retrieves the data from online storage, reconstructs the data to the requested generation, and sends it to the DS-Client.
4. DS-Client decrypts, decompresses, and stores the data on the target destination.

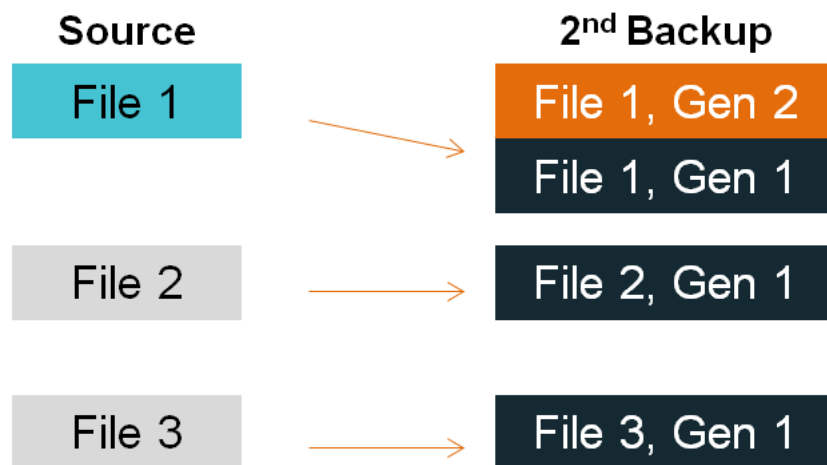
2.1.3 About online file generations

When DS-Client processes the backup data, each file is backed up individually. Each version of a file kept online is called a “generation”. Each file generation is independent of other files and stored individually (for files that are greater than 32 KB). By default, 30 generations of a file are stored.

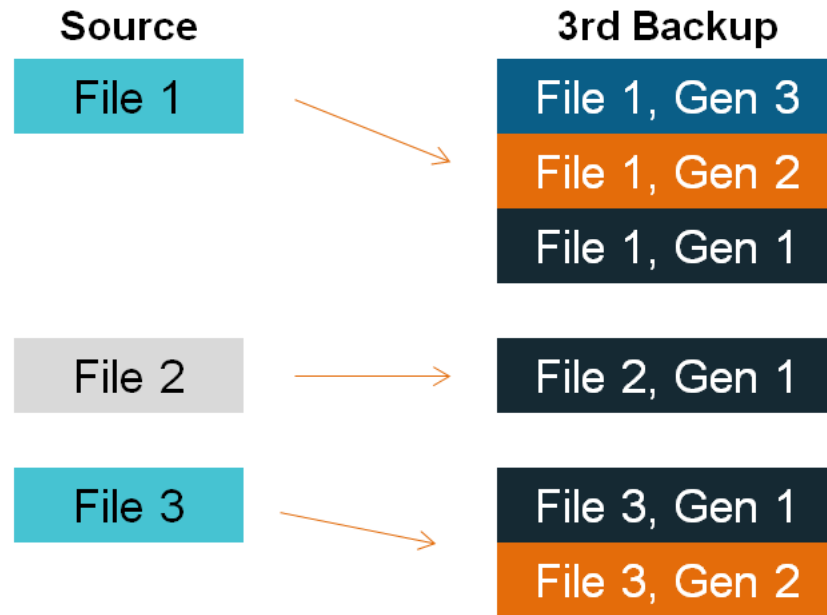
During the initial backup, all files are backed up creating the first generation of files.



During the second backup, DS-Client detects and backs up only new files and the files that have been changed. The new files will have their 1st generation created and the existing files that had been backed up previously will now have a 2nd generation.



The process is repeated for subsequent backups. The new files will have their 1st generation created and the existing files that had been backed up previously will now have a 2nd generation or 3rd generation created depending on how many generations have been created previously.



There are three types of generations: Regular, Master, and Delta.

Regular generations

Regular generations contain the entire contents of the file and do not depend on other generations for restore. A regular generation of a file is created if any one of the following conditions is met:

- The file is less than 32 KB or greater than 1 PB.
- The backup set is configured to store less than 3 online generations.
- The file is an executable, DLL, or driver file being backed up without the “backup streams” option enabled.

Master generations

Master generations contain the entire contents of the file and are created during the initial backup of a file that qualifies for delta processing. A master generation of a file is only created if any one of the following conditions is met:

- Something happens to the DS-Client database.
- The latest online generation is corrupted or deleted by the customer.
- DS-Client is configured to send a full master generation to the DS-System.

Delta generations

Delta generations contain only the changes to the file since the previous backup. Each delta generation has pointers to the previous and next delta generation. To recreate the file, the master is combined with the subsequent deltas, up to the selected generation. The DS-Delta algorithm analyzes files at the block level and the processing is generic, meaning it will work on any binary file.

A delta generation of a file is only created if all of the following conditions are met:

- The file is between 32 KB and 1 PB.
- The backup set is configured to store 3 or more online generations.
- The file is not an executable, DLL, or driver file being backed up without the “backup streams” option enabled.

2.2 Product documentation

This guide is part of a comprehensive documentation set for the Asigra Cloud Backup software that includes the following documents.

2.2.1 Server software documentation

- **BLM Archiver User Guide** — Describes how to use the BLM (Backup Lifecycle Management) Archiver application to archive data.
- **DS-Billing User Guide** — Describes how to use the DS-Billing application to maintain and generate billing information.
- **DS-License Server CLM User Guide** — Describes how to use the DS-License Server CLM (Capacity License Model) application to validate license quotas for DS-Systems and BLM Archivers.
- **DS-License Server RLM User Guide** — Describes how to use the DS-License Server RLM (Recovery License Model) application to validate license quotas for DS-Systems and BLM Archivers.
- **DS-NOC User Guide** — Describes how to use the DS-NOC (Network Operations Center) application to manage the system through a web-based interface.
- **DS-System User Guide** — Describes how to use the DS-System application to manage the DS-System data vault.
- **Server Software Installation Guide** — Describes how to install and upgrade the server software, including DS-License Server, DS-System, DS-NOC, BLM Archiver, and DS-Billing.

2.2.2 Client software documentation

- **Client Software Installation Guide** — Describes how to install and upgrade client software, including the DS-Client, DS-Mobile Client, and DS-Notebook Client.
- **DS-Client Mass Deployment Guide** — Describes how to use the DS-Client mass deployment feature to deploy and configure a large number of DS-Clients.
- **DS-Client Oracle SBT User Guide** — Describes how to use the System Backup to Tape (SBT) feature with the DS-Client application to back up and restore Oracle data.
- **DS-Client User Guide** — Describes how to use the DS-Client application to back up and restore data on a Windows, Linux, or Mac machine.
- **DS-Mobile Client Mass Deployment Guide** — Describes how to use the DS-Mobile Client mass deployment feature to deploy and configure a large number of DS-Mobile Clients.
- **DS-Mobile Client User Guide** — Describes how to use the DS-Mobile Client application to back up and restore data on a laptop computer.
- **DS-Notebook Client (Mac) User Guide** — Describes how to use the DS-Notebook Client application to back up and restore data on a Mac Notebook.
- **Management Console User Guide** — Describes how to use the Management Console web-based interface to back up and restore data on a Windows, Linux, or mac machine.

2.2.3 Tools software documentation

- **Tools User Guide** — Describes how to install and use various tools to optimize the performance of the software.

3 Asigra Cloud Backup components

This section provides a basic overview of the main Asigra Cloud Backup components.

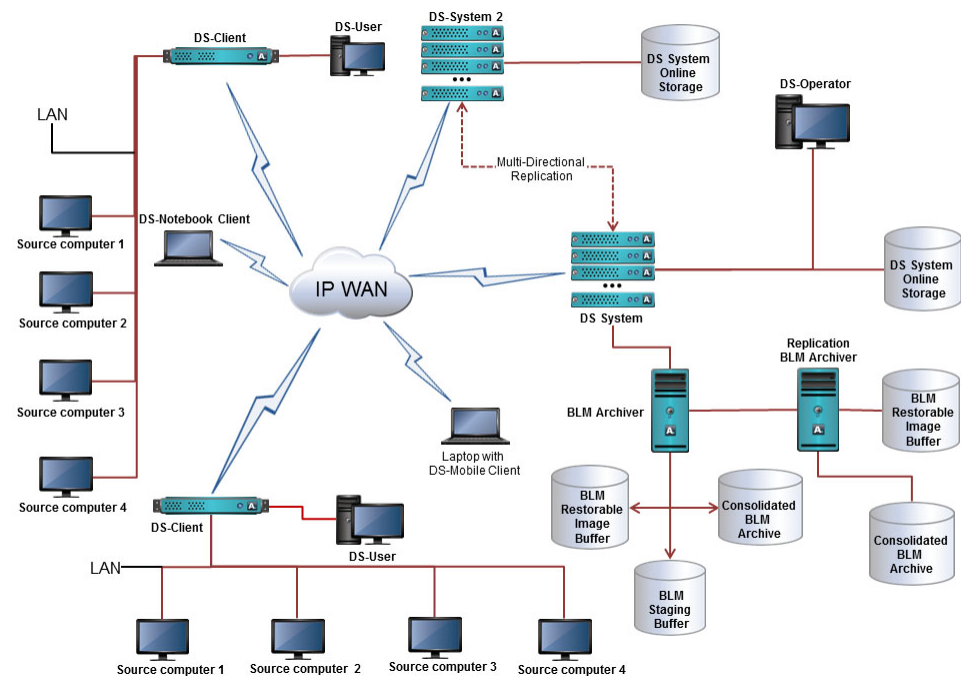


Figure 1 Asigra Cloud Backup components

3.1 DS-License Server

This section provides a high-level overview of DS-License Server and explains how licensing is handled. For details on how to install and use DS-License Server, see the *Server Software Installation Guide* and the *DS-License Server User Guide*.

The DS-License Server gives you flexibility when allocating licenses by allowing you to purchase a bulk license amount and distribute that amount among your DS-Systems and BLM Archivers as required.

The DS-License Server validates the licenses for your DS-System and BLM Archiver installations. Once validated, you can create DS-Client accounts on the DS-System and back up data to DS-System online storage. The data can also be copied or moved to BLM Archiver storage.

The DS-License Server runs as a service on Windows or a daemon on Linux and must always be accessible 24/7 via a TCP/IP connection from the DS-System and BLM Archiver installations, for those products to validate their licenses.

The following diagram shows the components and relevant port information for the DS-License Server:

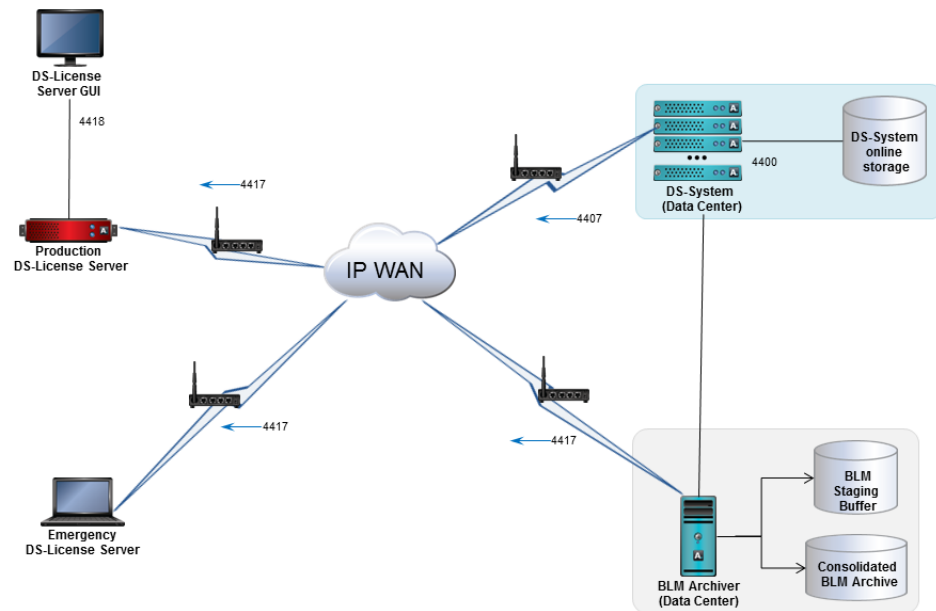


Figure 2 DS-License Server component interaction

3.1.1 DS-License Server types

The Production DS-License Server provides a total licensed capacity, from which you can distribute to the DS-System and BLM Archiver accounts.

In case of issues with the Production DS-License Server or if connectivity is lost between the Production DS-License Server and a DS-System or BLM Archiver, the Emergency DS-License Server provides failover license authentication for your DS-System and BLM Archiver installations.

Each production HASP USB key comes with a companion emergency USB key that allows you to configure the Emergency DS-License Server.

The Emergency DS-License Server provides failover license authentication your DS-System and BLM Archiver installations, if they cannot connect to the production license server.

3.1.2 DS-License Server models

The DS-License Server provides an aggregate licensed capacity that can be allocated to different DS-Systems and BLM Archivers installed in the same geographical location or in different geographical locations. Two licensing models are available: the Capacity License Model (CLM) and the Recovery License Model (RLM). Each model has its own DS-License Server installation.

Capacity License Model

The Capacity License Model (CLM) consists of a physical HASP USB key and a software license file, which maintains the license information. Payment for a CLM license is based on the storage capacity of the license. CLM embeds the cost of recovering 100% of your data, regardless of how much or how little you actually recover.

Recovery License Model

The Recovery License Model (RLM) consists of a physical HASP USB key and online access to the master Asigra Licensing Server, which maintains the license information. Payment for a RLM license is based on the storage capacity of the license, and the amount of data recovered over the previous license term.

RLM comes with measurement tools that quantify recovery usage. These amounts are used to calculate a score that determines the price of your renewal license. You can have a low fixed annual rate for backup storage, and a variable rate for recovery based on the percentage of data recovered.

3.1.3 DS-License Server RLM components

The DS-License Server RLM includes the following three major components:

- Asigra Recovery Tracker
- Recovery Performance Score
- Disaster Recovery Drill

Asigra Recovery Tracker

The Asigra Recovery Tracker is a powerful analytics engine that measures recovery performance by providing:

- The number of recoveries performed each year.
- The amount of data recovered.
- The source of data loss.
- The reason for restore.

The Recovery Performance Score

The Recovery Performance Score (RPS) is measured on a scale from 0-10. This scale corresponds to a price per GB for recovery. As the recovery performance improves, you will pay less for recovery on a per GB basis.

A score of 0 means that you are recovering 25% or more of your backed up data, and you pay the price per GB corresponding to a performance score of 0. This upper limit ensures cost predictability, because you can estimate a best-case and a worst-case billing scenario from year to year.

NOTE: RPS is the percentage of your data that is actually recovered during the recovery term.

Disaster Recovery Drill (DR Drill)

This capacity is the total disaster recovery drill amount that you can assign to your DS-Systems and BLM Archivers.

Recovery drills are scheduled events that can be tracked and priced separately from actual data recovery. If you set the quota on a license to "0", the DS-System or BLM Archiver will not be able to perform recovery drills.

Recovery drills can be purchased as needed. You must schedule the drill at least 30 days in advance, and perform the drill within 10 days. The drill capacity expires at the end of the term.

3.2 DS-System

This section provides a high-level overview of DS-System. For details on how to install and use DS-System, see the *Server Software Installation Guide* and the *DS-System User Guide*.

The DS-System is a licensed component that receives and processes requests from DS-Clients and serves as the main repository for backed up data. Other DS-System tasks include:

- managing customer accounts and DS-Client accounts
- recording comprehensive activity, event, and audit trails
- handling online generations and eliminating common files
- enforcing storage quotas

The following diagram provides an overview of the major components that interact with the DS-System.

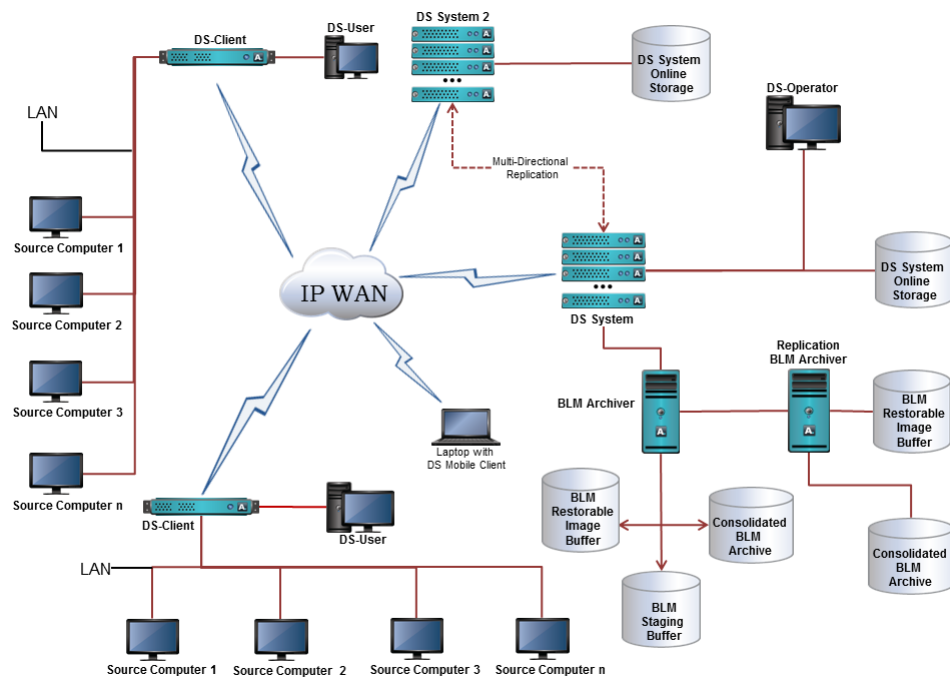


Figure 3 DS-System component interaction

The DS-System authenticates DS-Clients, receives encrypted backup data from DS-Clients, and stores the data in DS-System online storage. When a restore is requested, DS-System prepares and sends the data to the DS-Client, which handles the actual restore of the data to the appropriate location.



Figure 4 Interaction between the DS-System and DS-Client

The DS-System consists of the following components:

- DS-System software, which runs as a service or daemon.
- DS-Operator, which is the remote management software for the DS-System.
- DS-System database (Microsoft SQL Server or PostgreSQL).
- DS-System online storage.

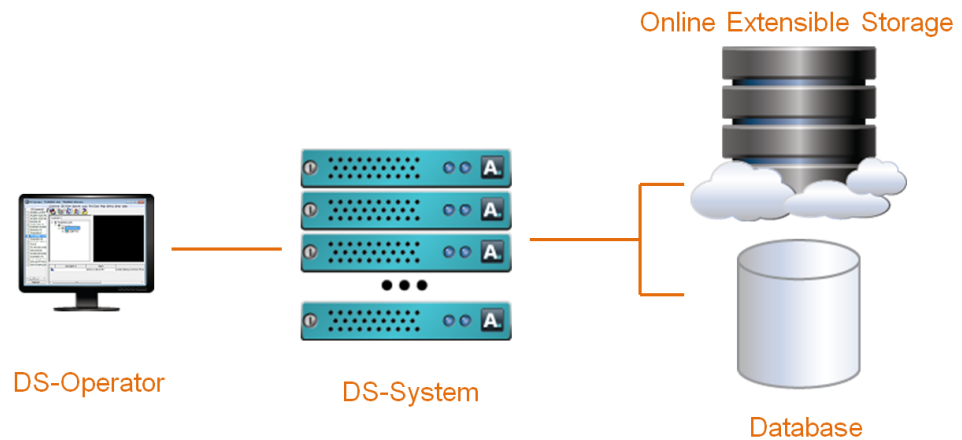


Figure 5 DS-System components

3.2.1 DS-System configurations

DS-System can be deployed in standalone or N+1 configuration.

Standalone DS-System

The standalone DS-System configuration is an installation that has its own database and online storage.

NOTE: A standalone DS-System can be migrated to an N+1 DS-System configuration, retaining the same database and DS-System online storage by installing additional DS-System nodes and upgrading the DS-System license.

N+1 DS-System

An N+1 DS-System configuration consists of several DS-Systems working together to provide backup and restore services for DS-Clients. The DS-System nodes work together with a common database and common DS-System online storage. This formation provides both fault tolerance and load balancing.

At least 3 DS-System nodes are required in an N+1 configuration. Each node performs its own storage and retrieval activities. Any node can provide any DS-Client with services. All the nodes must be on the same LAN.

One node, which is called the DS-Director, is chosen at random to be the main node and keeps track of the data storage, provides notifications for the entire N+1 configuration, and distributes scheduled activities across the DS-System leaf nodes.

The benefits of using an N+1 DS-System configuration include performance, scalability, and redundancy. All the nodes share the backup processing load and if a node fails, the N+1 DS-System continues to function. Hardware can be added to the extensible storage as required.

3.2.2 DS-System types

The following table describes the different types of DS-System licenses that can be configured in the DS-License Server.

Type	Data Accepted
FullFeatured (Standalone or N+1)	<p>A FullFeatured DS-System license is a full service (production) DS-System and can accept data from the following types of DS-Client:</p> <ul style="list-style-type: none"> • FullFeatured DS-Client • DS-Mobile Client <p>Note: This is the only type of DS-System that can allocate Local-Only Storage.</p>
Mobile (Standalone or N+1)	<p>A Mobile DS-System license is a full service (production) DS-System and can accept data from the following types of DS-Client:</p> <ul style="list-style-type: none"> • DS-Mobile Client (Windows) • DS-Notebook Client (Mac) <p>A Mobile DS-System can only be licensed using a DS-License Server CLM (Capacity License Model).</p> <p>Note: Local-Only Storage cannot be allocated.</p>
Replication (Standalone or N+1)	<p>A Replication DS-System license is not for production and can only accept data from a production DS-System. It cannot receive backup data directly from DS-Clients.</p> <p>Any production DS-System that has Replication enabled can send its backed up data to a replication DS-System. A Replication DS-System allows replication of data between DS-Systems and responds to restore requests from DS-Clients.</p> <p>Note: Local-Only Storage cannot be allocated.</p>

Table 1 DS-System types

Replication DS-System

Replication can be performed between two or more DS-Systems that are in different data centers. The benefits of using replication include redundancy and high availability. You always have a secondary backup of the DS-System online storage and DS-Clients can switch from a failed DS-System to the replication DS-System for on demand restores.

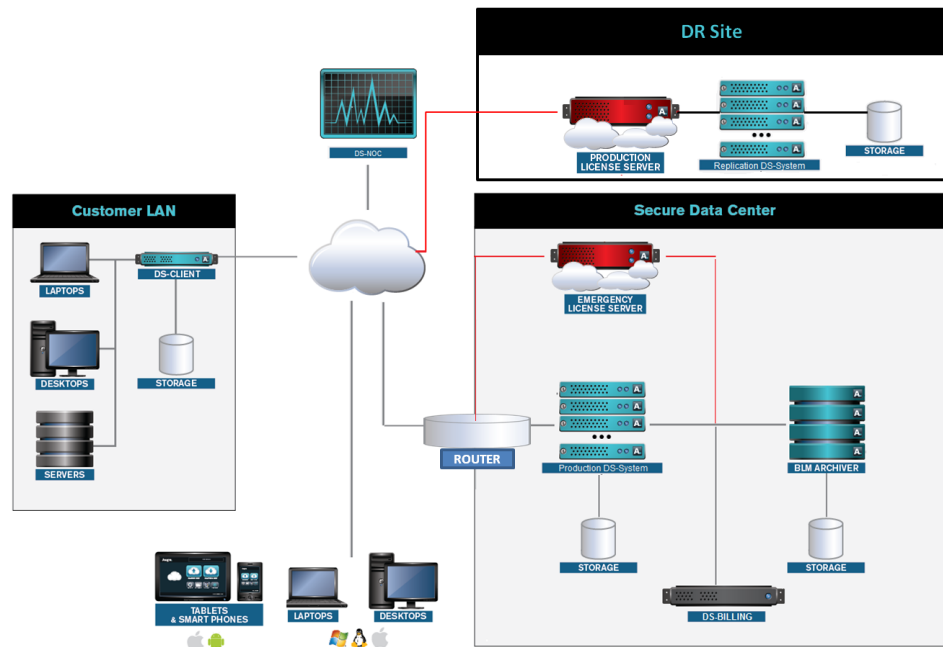


Figure 6 Replication overview

Replication Licensing

Replication must be enabled in your DS-License Server license that you purchase. The replication capacity is separate from the online capacity.

Replication is at the DS-Client level. The data replicated between the two DS-Systems is the data residing on the DS-System online storage that can be restored. Replication is platform independent, meaning one DS-System can run on Linux, while the other runs on Windows.

Replication is automatically triggered when a backup activity completes for a backup set. After the master generation is processed, replication becomes incremental forever for subsequent backups.

An added benefit is that if a file corruption occurs on one DS-System, then the replicated copy on the other DS-System can be used for repair.

In case of a total loss of the primary DS-System, you can back up to the replicated DS-System with a manual re-configuration of the license. The DS-Clients must be re-configured to point to the IP address of the alternate DS-System.

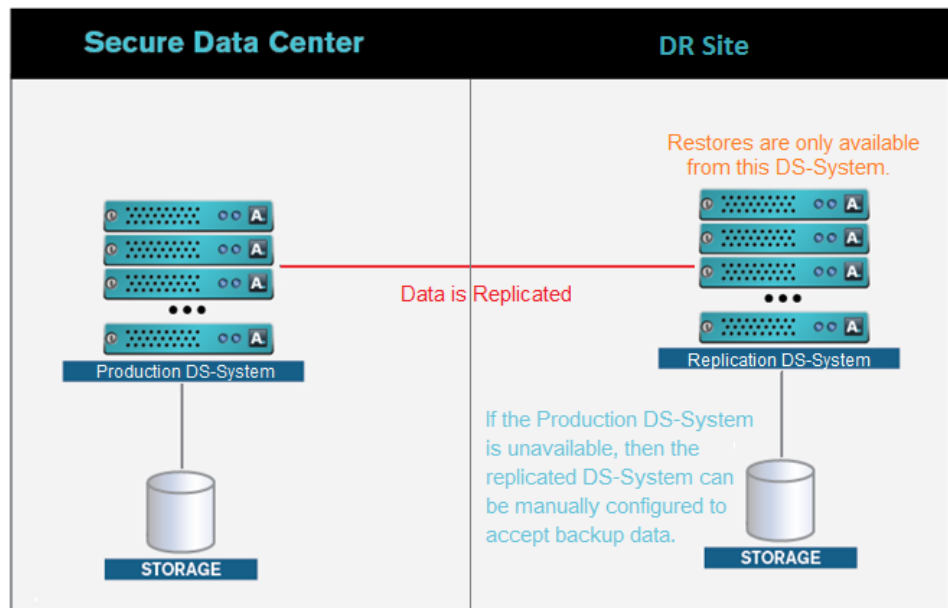


Figure 7 Replication licensing

3.3 DS-Client

This section provides a high-level overview of DS-Client. For details on how to install and use DS-Client, see the *Client Software Installation Guide* and the *DS-Client User Guide*.

DS-Client is responsible for defining the backup sets that determine what data is to be backed up from the source computers and for sending the backed up data through an IP WAN to DS-System for storage.

During the backup process, DS-Client extracts, compresses, and encrypts the data for backup. Only new or modified data is backed up, thereby accelerating the backup transmission time. The backup data is sent to the secure, off-site data center that hosts the DS-System vault. Restore is performed on demand via the same DS-Client.

Ease of use comes from the agentless architecture, which requires that you need to install DS-Client on only one LAN computer (thereby eliminating the need to install software on every target backup/restore computer). As long as the computer is on the same network as the target backup/restore computers, you can browse data, back it up, and restore it as required.

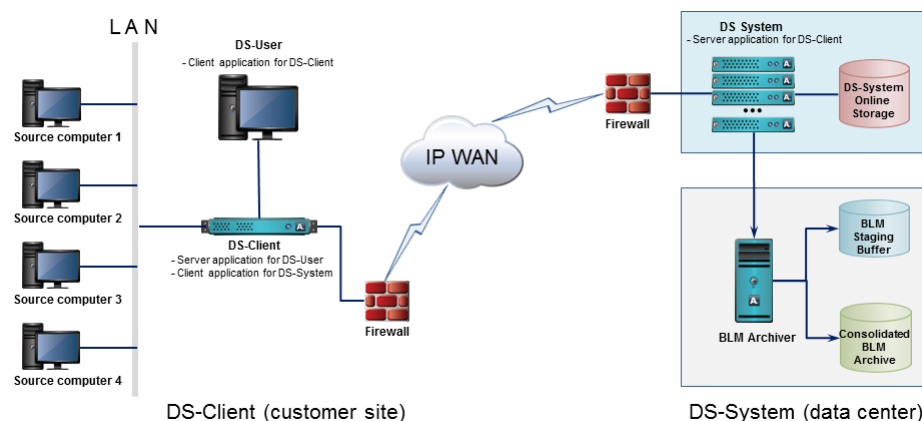


Figure 8 DS-Client component interaction

3.3.1 DS-Client configurations

DS-Client can be deployed in a standalone or Grid DS-Client configuration.

Standalone DS-Client

The standalone DS-Client configuration consists of one DS-Client service working with one database to provide agentless backup and restore of a LAN environment. The standalone DS-Client configuration is available in a Windows, Linux, or Mac environment. The DS-Client consists of the following components:

- DS-Client software, which runs as a service or daemon.
- DS-User, which is the remote management software for the DS-Client.

- DS-Client database (Microsoft SQL Server or PostgreSQL).
- DS-Client local storage (optional).



Figure 9 DS-Client components

Grid DS-Client

The Grid DS-Client consists of two or more DS-Client services working with one common database to provide agentless backup and restore for larger LAN environments. The Grid DS-Client configuration is available in a Windows environment only.

Each DS-Client performs its own backup and restore activities, but all have access to a shared DS-Client database. The multiple nodes allow maximum load balancing (all the nodes can access the same source data for backup and restore). All the nodes in a grid must be on the same LAN.

DS-System treats the Grid DS-Client as a single DS-Client, which requires that each node has the same registration information. Grid DS-Client provides the following benefits:

- **Performance** — Balances the communication and processing load across multiple DS-Client nodes.
- **Scalability** — Provides the ability to easily add more hardware as needed.
- **Redundancy** — Ensures a high level of availability. If a DS-Client node fails, the grid will continue to function.

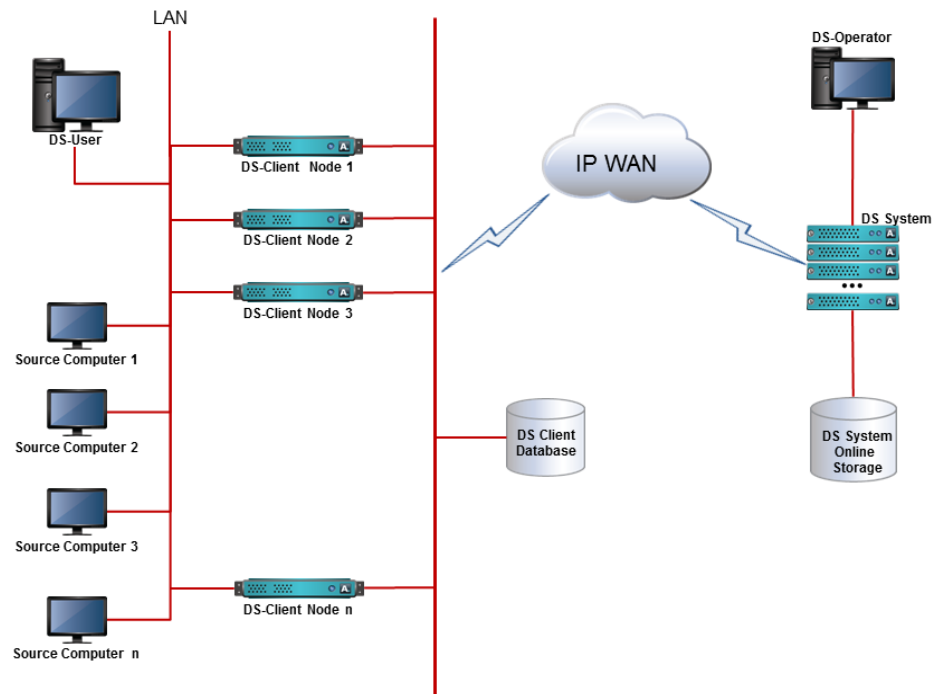
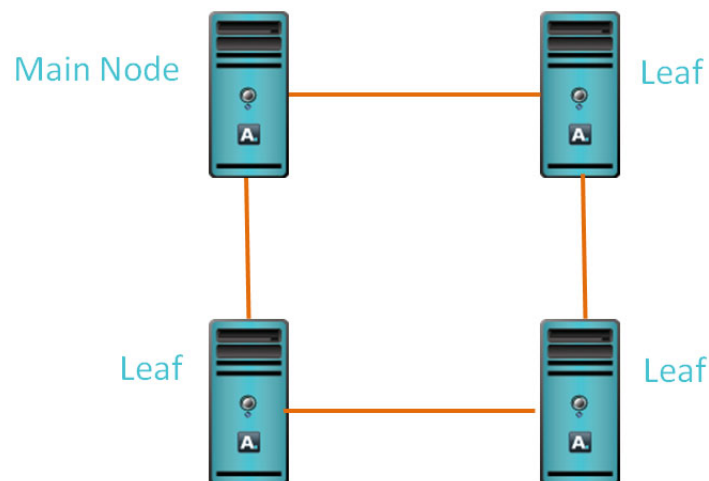


Figure 10 Grid DS-Client components

All DS-Client nodes can access each of the data sources so that backup and restore services keep running even if some of the nodes of the Grid DS-Client fail. This ensures that even if a node terminates unexpectedly, only the backup sets with processes running on the unresponsive computer will be affected.



One of the DS-Clients in the grid is chosen at random to be the main node. The main node is the synchronization point that tracks what activities are running and ensures that the leaf nodes do not run conflicting activities. The main node sends notifications, triggers scheduled activities, and distributes activities to the other nodes based on the number of activities running and the CPU usage.

3.3.2 DS-Client types

DS-Client comes in several different product types. The DS-Client you select is determined based on the device and data source that needs to be protected.

- **DS-Client (Windows)** — Backs up data in Windows environments.
- **DS-Client (Linux)** — Backs up data in Linux environments.
- **DS-Client (Mac)** — Backs up data in Mac OS X environments.
- **DS-Mobile Client (Windows)** — Backs up data on Windows laptop computers that are not connected to the LAN all the time.
- **DS-Notebook Client (Mac)** — Backs up data on Mac notebook computers that are not connected to the LAN all the time.

For details on how to install and use each product, see the *Client Software Installation Guide* and the corresponding user guide.

3.4 BLM Archiver

This section provides a high-level overview of BLM Archiver. For details on how to install and use BLM Archiver, see the *Server Software Installation Guide* and the *BLM Archiver User Guide*.

The BLM Archiver is an optional component that is used for long-term data archiving on lower cost media.

BLM Archiver receives data from the DS-System and stores the data in the BLM Archiver's staging buffer, consolidation buffer, or cloud storage. One BLM Archiver can receive data from many DS-Systems. When a restore of the archive data is required, a restorable image is created and the resulting data is shipped or downloaded to the DS-Client that encrypted the data. The DS-Client can then be used to restore the data.

BLM Archiver can replicate its data to other BLM Archivers running in different geographical locations. The BLM Archiver that sends the replication data is the Production BLM Archiver and the BLM Archiver that receives the replication data is the Replication BLM Archiver.

BLM Archiver consists of five components:

- BLM Archiver software, which manages the process of handling BLM functions, indexes archived data, and generates the necessary restore packages when restore requests are received.
- BLM staging buffer, which temporarily stores archive data when transferred from DS-System.
- BLM consolidated storage, which permanently stores archive data after being processed by BLM Archiver until the data is moved or data destruction occurs.

- BLM cloud storage, which permanently stores archive data transferred from staging buffer or consolidated storage, until data destruction occurs.
- BLM restorable image buffer, which stores the data requested to be restored from the archive so it can be copied to media and shipped to a customer location or downloaded using the DS-NOC.

The following diagram provides an overview of the major components of the BLM.

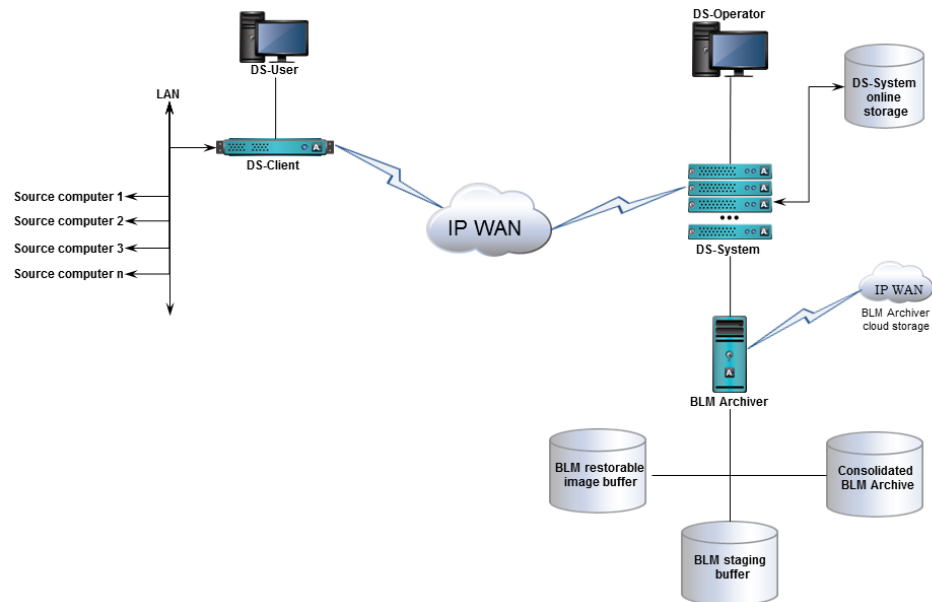


Figure 11 BLM Archiver component interaction

The BLM Archiver is responsible for the following tasks:

- Accepting archive requests from the DS-System (initiated from DS-Client or DS-System).
- Accumulating archive data into a staging buffer before moving it (consolidating) into a full BLM archive, which is a large file which contains data consolidated from several BLM requests belonging to the same DS-Client's backup set.
- Consolidating several archives into a BLM archive (disk-based, with optional data release to a tape library by a third-party HSM/Archive application).
- Performing indexing of archived data (DS-System \ DS-Client \ backup set \ request \ files).
- Generating BLM archive restorable images that can be restored using the DS-Client. A copy of the restorable image can be generated to media and shipped to the customer or can be downloaded by the customer using the DS-NOC.

There are two types of BLM Archiver licenses that can be configured from the DS-License Server:

- **FullFeatured** — This is the full service (production) BLM Archiver license that can receive backup set data from DS-Systems and can replicate its archive packages to a Replication BLM Archiver.
- **Replication** — This type of license only allows replication of existing BLM archive package data to the Replication BLM Archiver. It is not a production license and cannot receive data from DS-Systems. However, it does allow BLM GUI or DS-NOC connections to search and retrieve the archived data or request data destruction.

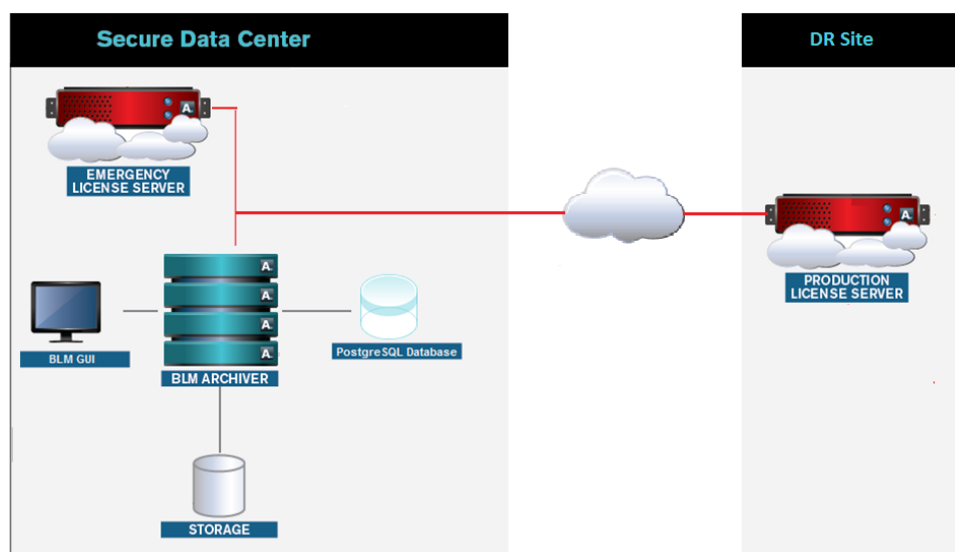


Figure 12 BLM Archiver licensing

3.5 DS-Billing

This section provides a high-level overview DS-Billing. For details on how to install and use DS-Billing, see the *Server Software Installation Guide* and the *DS-Billing User Guide*.

DS-Billing is an optional component that maintains and generates billing information and billing reports for registered DS-Systems and BLM Archivers.

The primary function for DS-Billing is to generate billing related usage reports such as invoices, commissions, and storage usage. In RLM license environments, DS-Billing also tracks and calculates the Recovery Performance Score for billing objects.

Normally, one DS-Billing server installation is sufficient for an entire organization, because it can connect to all the billing components (DS-Systems and BLM Archivers) that it can access via a TCP/IP connection.

The DS-Billing GUI is the remote management software for the DS-Billing server and can be used to manage customer accounts, DS-Client accounts, sales groups, billing scales, charge plans, consolidated invoices.

The following diagram provides an overview of the major components of DS-Billing.

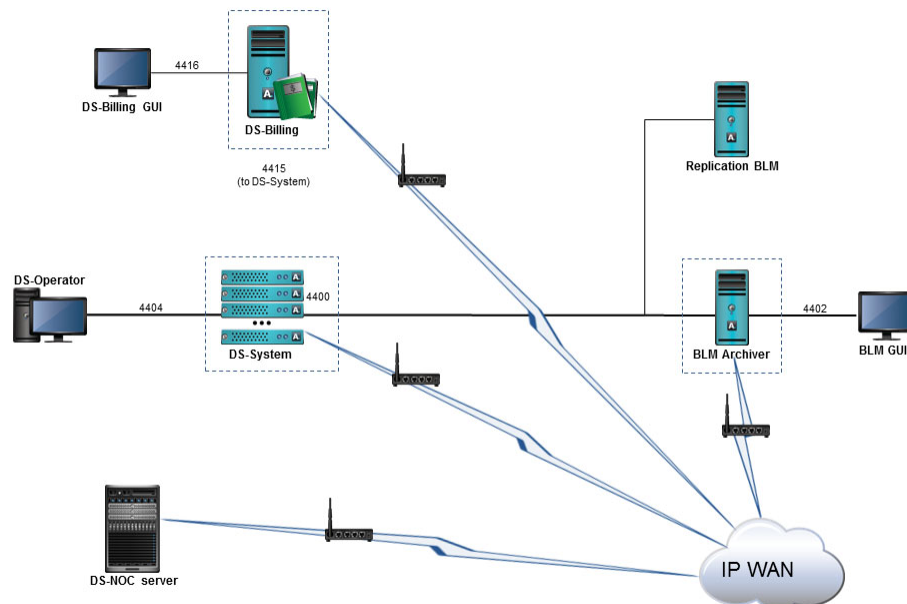


Figure 13 DS-Billing components

3.6 DS-NOC

This section provides a high-level overview of DS-NOC. For details on how to install and use DS-NOC, see the *Server Software Installation Guide* and the *DS-NOC User Guide*.

The DS-NOC (Network Operation Center) is an optional component that allows you to access DS-License Servers, DS-Systems, DS-Clients, BLM Archivers, and DS-Billing servers through a web-based interface.

DS-NOC is used to monitor and perform most of the duties of the individual applications and can be installed on any platform that supports PostgreSQL, Java JRE, and Apache Tomcat.

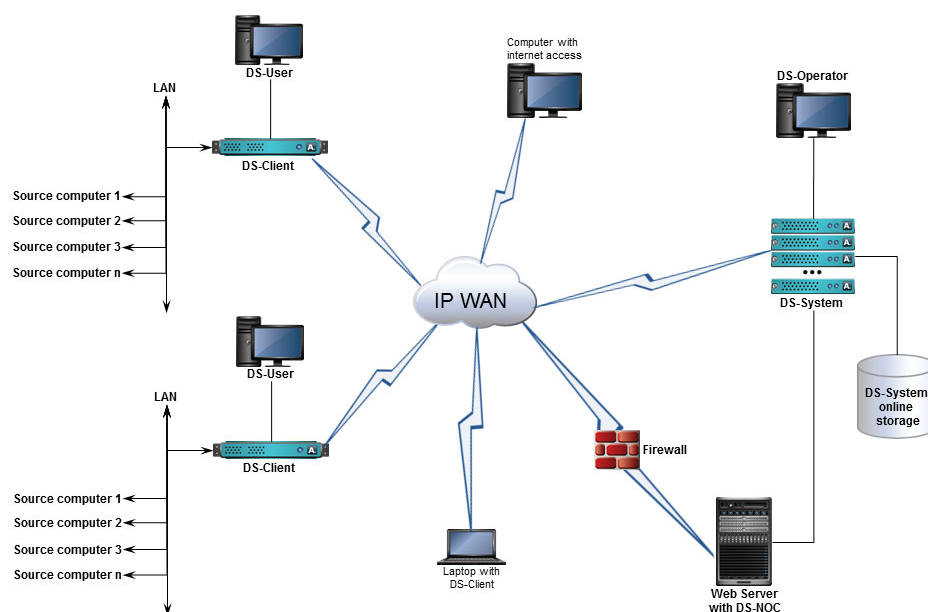
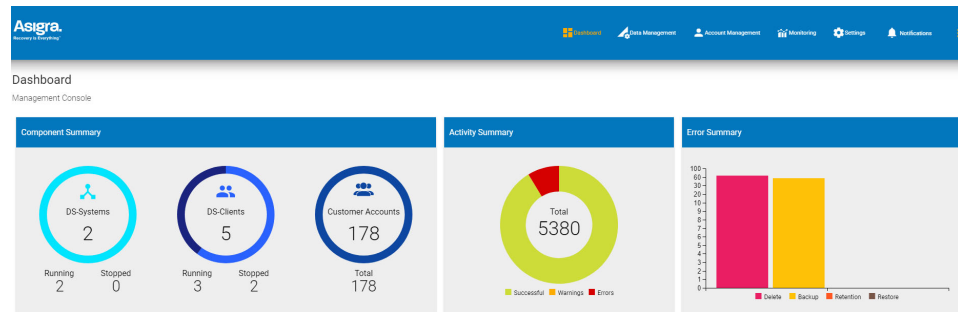


Figure 14 DS-NOC components

3.7 Management Console

This section provides a high-level overview of the Management Console. For details on how to install and use the Management Console, see the *Client Software Installation Guide* and the *Management Console User Guide*.

Management Console is a modern web-based application that simplifies the backup and recovery process by providing a centralized environment to manage DS-Systems, DS-Clients, backup sets, schedules, retention rules, and more.



An interactive dashboard provides a real-time view of your data and the responsive web interface adapts to the screen size of your device.

Users can easily apply their own branding to the Management Console and translate the interface into over 100 languages.

The Management Console Application Programming Interface (API) is based on the RESTful (Representational State Transfer) framework and allows developers to use their preferred programming languages and tools to integrate with the Management Console. To access the API documentation, add /docs to the end of the Management Console URL.