Product Spotlight

Backup and disaster recovery

Introduction

Laboratory operations are business critical, as business processes depend on the data generated. Interruptions to these operations cause higher costs and revenue loss. Therefore, system downtime resulting from an emergency should be as short as possible.

A business continuity plan (BCP) ensures continued operation at pre-defined acceptable levels after a disruptive incident. Business continuity planning is a process to develop a foolproof system for prevention and recovery from potential threats to a company that risk continued business operation. The disaster recovery plan (DRP) is a key part of the business continuity plan, describing how to recover and protect business IT infrastructure in event of disaster and provides detailed steps on how to restart, reconfigure and recover the systems, software and network.

The chromatography data system (CDS) is a key software for the laboratory, but also a key part of the IT infrastructure and must be included in the DRP. Thermo Scientific™ Chromeleon™ Chromatography Data System (CDS) provides automated fallback systems, for maximum system availability during maintenance or disastrous events, and each of the components of an enterprise environment must be addressed in the DRP.

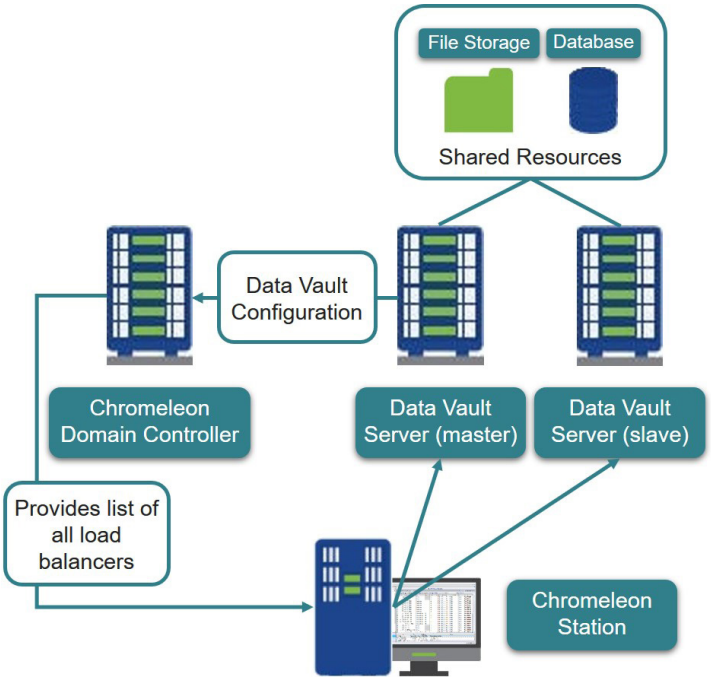

Figure 1. Built-in load balancing capabilities

Automated fallback systems

Built-in load balancing and failover protection

While load balancing (sharing workload between two or more servers) and failover (automated switching between servers should one fail) is often handled by IT, Chromeleon CDS does provide its own load balancing and failover for the Data Vault Service, which handles the data exchange between the Data Vaults and the Chromeleon Client. Load balancing allows distribution of workloads across multiple computing resources, usually servers (Figure 1). In case a server fails or is taken offline for maintenance, the other server(s) simply takes over, keeping the system online. This increases reliability through redundancy and, in addition, provides a capability for server maintenance.

Network failure protection

Ensuring continuous operation and preventing data loss or corruption during a network outage is key to maintaining laboratory operations, data integrity and compliance. Chromeleon software provides unique, industry-leading Network Failure Protection (NFP) functionality to deliver 24/7 uptime in two key ways:

- Network-based resources required to properly operate the software — such as license information and user management data — are automatically cached on local instrument controllers and client computers ensuring continued software operation, as a 7 day recovery period is automatically enabled, allowing time for the issue to be resolved or for a longer-term solution to be implemented.
- Chromeleon software's unique XVault™ technology ensures continuous operation and data security (Figure 2). During data acquisition, sequences are always run in the XVault, present on each local instrument controller, and the acquired data is synchronized centrally. In case of network failure, NFP mode is automatically enabled and data acquisition continues, with the data stored on the local computer. While in NFP mode, the data interrupted during acquisition can be accessed via the XVault for processing, and reporting, and new sequences can be started — all in accordance with compliance and data integrity guidelines. After network recovery, the interrupted data is automatically uploaded and synchronized to the central server. Additionally, any new sequences initiated while in NFP mode can be uploaded within the Chromeleon Client, ensuring data integrity and compliance.

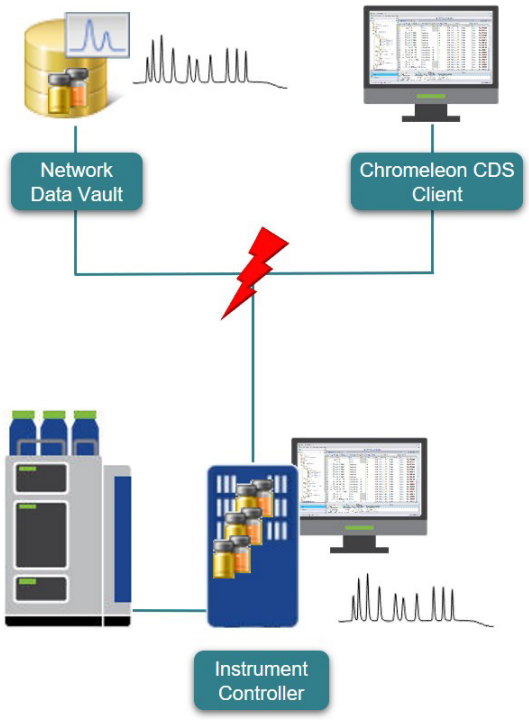

Figure 2. Network failure protection

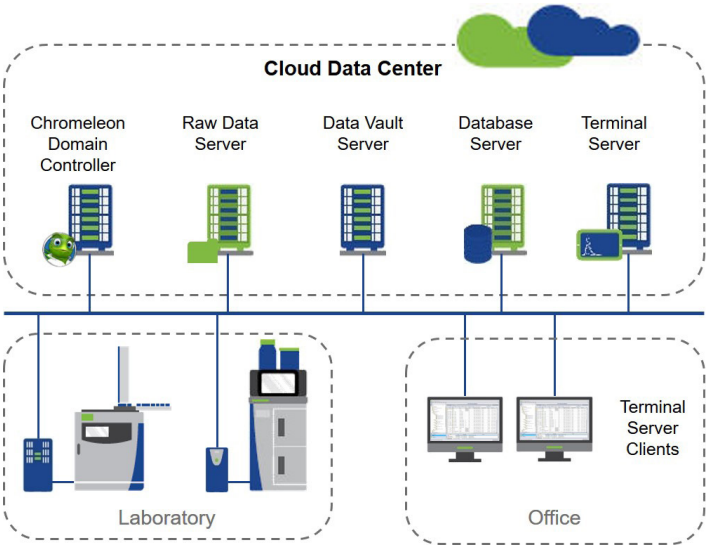

Figure 3. Example of cloud implementation

Cloud deployment

Shifting Chromeleon software deployment to the cloud, provides increased security to ensure business continuity. Within a cloud infrastructure, servers, clients and central data storage can be hosted with an external cloud service provider (Figure 3).

Every business can get the security level that fits the organization and cloud service providers take serious care of their data centers and ensure that they are protected both virtually and physically. By moving parts to the cloud you'll get seamless data backup as data is stored in multiple places in the cloud, removing a single point of failure.

Chromeleon software components

Chromeleon software's modular architecture provides resilience and scalability, adaptable to the needs of the business. The installation can be a single, stand-alone workstation, where a computer is connected to an instrument, to a global wide area network, connecting multiple sites around the world (Figure 4). Depending on the installation, the individual components that need to be considered for backup and disaster recovery are the instrument control hardware, Client, Chromeleon Domain Controller and the Data Vault Servers.

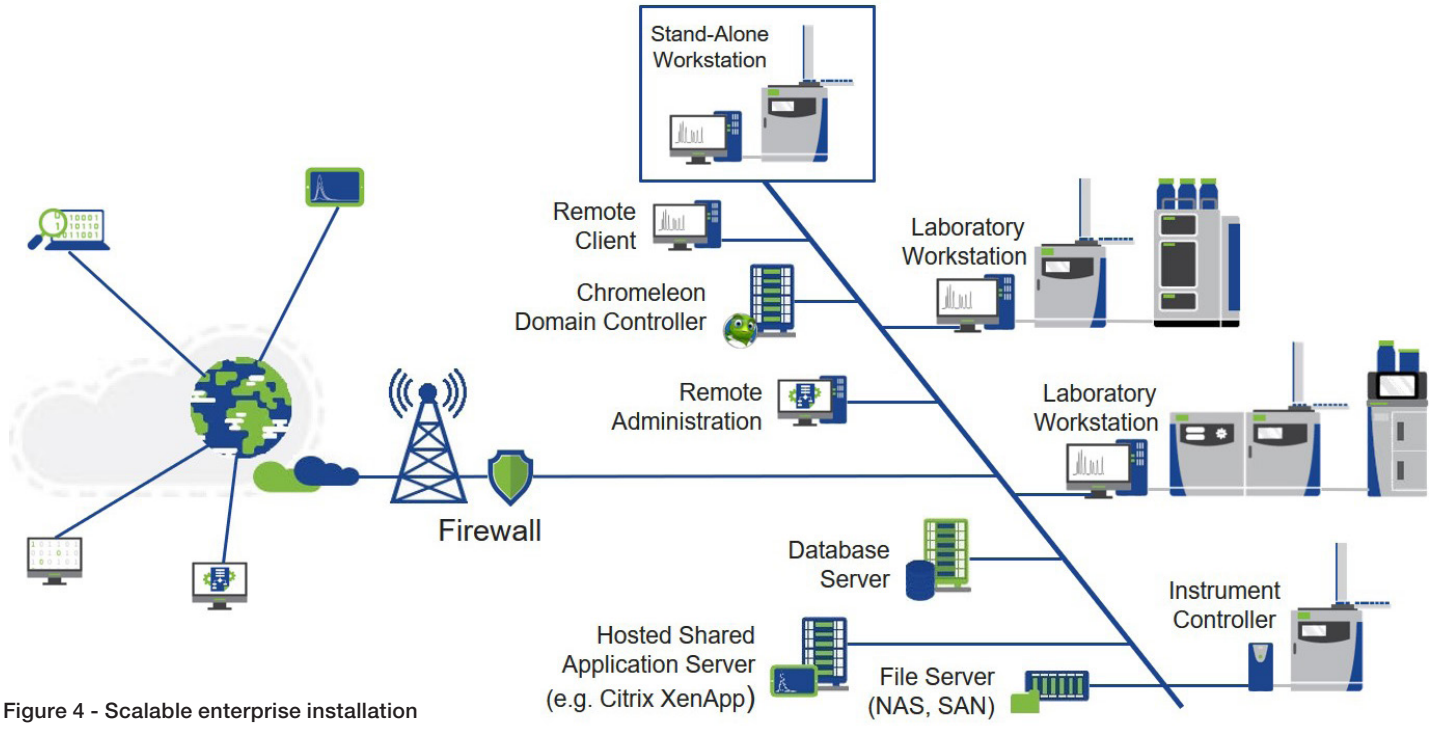

Figure 4 - Scalable enterprise installation

Instrument Controller

The Instrument Controller (Figure 5) controls all data exchange to and from the instruments and for quick recovery the general practice is to have preinstalled replacement equipment or computer image available. As instruments may (slightly) differ and therefore require individual configurations, it's important to backup the instrument configuration file from each Instrument Controller. This allows for a quick recovery of the instrument configuration, without going through this manually. In addition, the Instrument Controller may contain drivers which are not included in Chromeleon CDS, and these should be stored in a safe place as well.

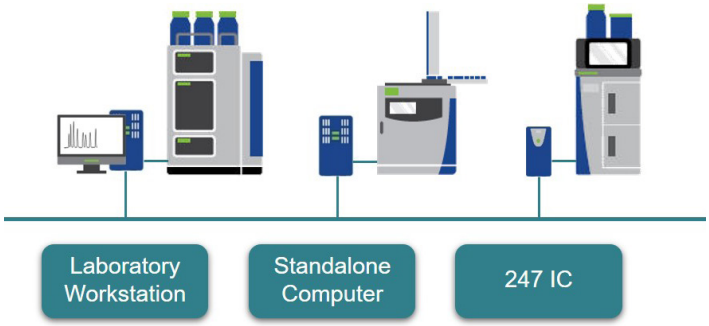

Figure 5 - Instrument Controller devices

Additional considerations are to limit the number of instruments connected to the Instrument Controller, as this limits the number potentially unavailable due to Instrument Controller failure. Also, the Chromeleon Scheduler can move recent method files directly onto an Instrument Controller for continued operation in case of a network outage.

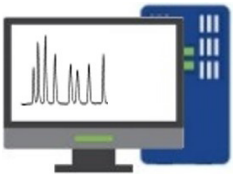

Figure 6 - Chromeleon Client

Client

The Chromeleon Client (Figure 6) is the user interface for accessing chromatography data for data acquisition, processing and reporting. As with the Instrument Controller, replacement equipment and computer images are a way to recover from disaster. However, hosted shared application server solutions, where the client part is running on a remote server and is distributed across the network for users to work with the Chromeleon software, further limit the risk of hardware failure.

Figure 7 - Chromeleon Domain Controller

Chromeleon Domain Controller

The Chromeleon Domain Controller (Figure 7) is the central source of information of all Chromeleon CDS resources, like user management, scheduler tasks, system maintenance tasks, Data Vaults and licenses. This Discovery information is cached on local Instrument Controllers and Clients, ensuring that when the Domain Controller goes down data can still be acquired and accessed from the servers hosting the Data Vault. Hosting the Domain Controller on a virtual machine is common practice. Virtualization software has tools built-in to make frequent backups, so operation can be quickly recovered in case of a disaster. In addition, specific information, like user management configuration and software licenses, can be backed up separately.

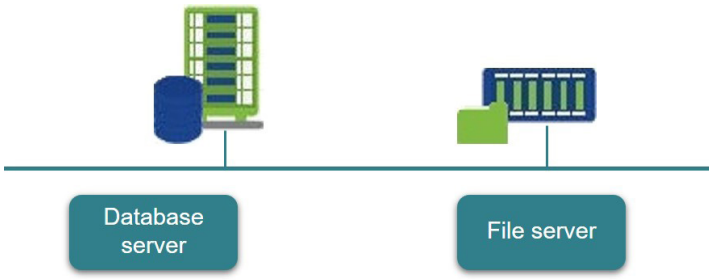

Figure 8 - Data Vault servers

Data Vault Server(s)

The Data Vault servers (Figure 8) are a set of servers where the individual Data Vault components reside, including the raw data files and the database. Depending on the installation type and size, this can be on separate servers or combined.

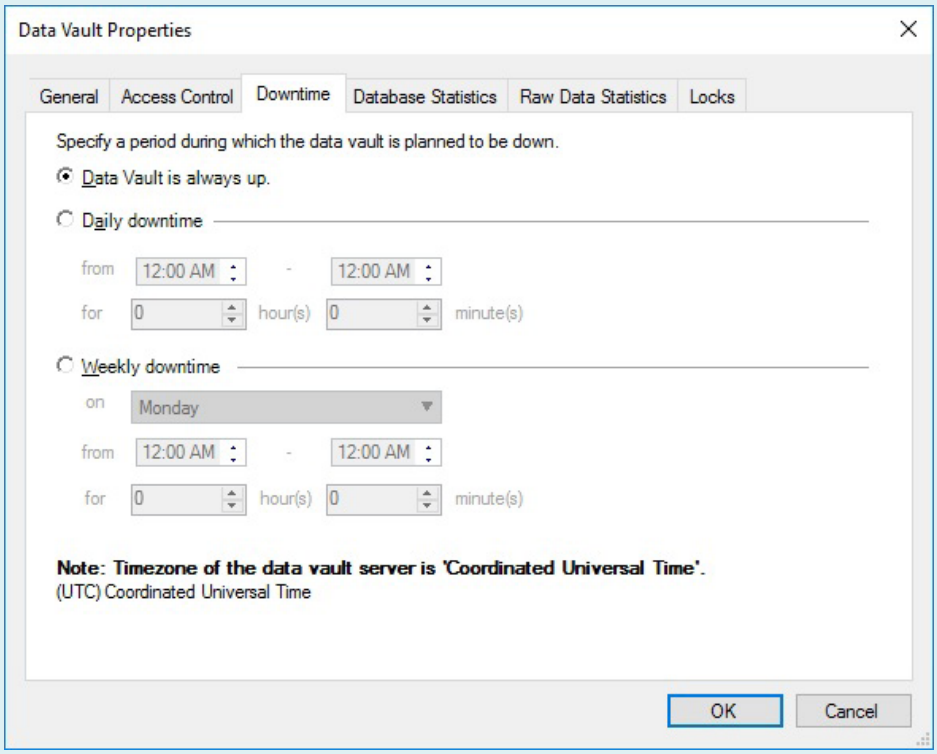

Figure 9 - Data Vault availability

Though Chromeleon software uses these servers for data storage, they are not part of the Chromeleon CDS enterprise installation as such, but do fully integrate into the existing IT environment. Therefore, the backup is managed by the currently existing procedures and additional safety measures, like mirroring and clustering for database installations and raid storage for raw data. Depending on the database used it may be required to set a Data Vault downtime during backup (Figure 9).

Considerations

Data archival

Though data archival is not related to the backup process, it is an important part of the total data lifecycle. One big advantage of archiving data 'at rest' is the streamlining of the backup process by the provision of a clean and lean working environment and less frequently changing archive area.

Data archival can be performed in multiple ways:

- Automatically move completed data to an archival Data Vault
- Move completed data outside of the CDS using an external storage container (*.cmbx)
- Move completed data to a Scientific Data Management System (SDMS), like Thermo Scientific™ Data Manager™ which is part of Thermo Scientific™ SampleManager™ Laboratory Information Management System (LIMS)

thermo scientific

Support and maintenance agreement

A support and maintenance agreement (SMA) or service level agreement (SLA) is an important part of a BCP, providing help with quick recovery after an event. It will secure your Chromeleon CDS installation with several key benefits to maximize and future-proof your investment, increase productivity and minimize the risk of business interruption.

The SMA includes technical support provided by dedicated Thermo Fisher Scientific professionals, who offer professional investigation and issue resolution via follow-the-sun methodology and exclusive access to various resolution resources. In addition, product updates are included, both for Long Term Support releases — enabling utmost stability and robustness over an extended period with minimized validation efforts — and Feature Releases — to stay up to date with the newest technologies and latest advancements.

Conclusion

While backup and disaster recovery are key for proper execution of the DRP, it's also a difficult one. Chromeleon CDS provides the tools to help IT executing the DRP — built-in fallback tools, like load balancing and failover protection, support for cloud deployment, all to prevent the need for backup and disaster recovery. The software's scalable architecture enables dedicated backup procedures per enterprise component, reducing the backup effort. The enterprise support plan provides assistance and support for system recovery after disastrous events. Chromeleon CDS is the solution for business continuity, providing security and ensuring quick recovery after disastrous events.

Find out more at **thermofisher.com/chromeleon**

ThermoFisher SCIENTIFIC