Data Backup and Recovery SLA

Created by Joe Brancaleone, last modified by Kenneth Cooper on Mar 22, 2022

Table of Contents

General Overview

The Enterprise Infrastructure division of the Office of Information Technology (OIT) provides a Data Backup and Recovery Service to the UCI campus. This service is designed to retain copies of data specified by a customer for a defined period of time to avoid unintentional loss. Data retention policies are specified in this document. As explained in the customer responsibilities section, the customer must determine which data types being backed up and retained are applicable to the UC records retention policy as defined by UCOP: https://recordsretention.ucop.edu/

This is a service level agreement (SLA) between OIT and Data Backup and Recovery Service customers. The term "customer" includes campus customers (i.e., academic and research personnel) and internal customers (i.e., internal OIT units and administrative personnel). The scope of this document includes:

- Services provided by OIT to Data Backup and Recovery Service customers.
- Levels of response time, availability and support associated with these services.
- Responsibilities of the OIT service provider and the customer.
- Processes for requesting services and getting help.

This SLA is reviewed annually, or as otherwise needed. It remains valid until revised or terminated. Any changes to the SLA will be reflected here and announced to the service's subscribers.

Service Description

2.1 Service Scope

OIT's Data Backup and Recovery Service is a centralized, network-based service to save point-in-time copies of data residing on servers located at on-premise data centers on the UCI campus in Irvine, CA.

For physical servers, a client agent is installed locally with elevated privileges. The agent can be configured locally or remotely by the backup administrator to determine which data sets will be copied to the central server. On a fixed schedule, the central server connects to each locally installed client to initiate a transfer of data. The amount of data transfer varies based on change rate of data on the client-side since the previous transfer of data.

Virtual servers may be backed up at the image level, "agentless", or use the same agent based process as physical servers; to avoid unnecessary load on the virtual server environment the backup technology utilized for virtual servers will be determined by best practices and specific customer requirements. This work is done

collaboratively with the virtual server owner. Equivalent protections are provided for virtual servers compared to the backup process for physical servers.

Servers being backed up by this service are referred to in this document as source servers or client-side servers.

2.2 Data Retention and Service Levels

For each source server, full backups, incremental backups, and/or synthetic full backups of the data will be performed according to the service schedule and backup technology. A full backup is a backup of all files defined by the customer as being within the scope of the backup service. An incremental backup is a backup of all files changed since the last backup occurred whether it was a full or incremental backup. A synthetic full backup is an incremental backup combined with a synthesizing of all previous incremental data to create a new full backup. Note that on any given period, the type of backup being taken always results in all changes to the source server's data being captured since the last backup of any type.

Veeam

- Standard Retention: The historically intiial backup is a complete full, then once a day incremental backup with 42 restore points (if 1 backup a day is taken this results in 6 weeks of backups)

Networker

- Standard Retention: Once a day backup with 6 - 8 weeks retention. A full backup is performed once per month and is retained for 1 - 2 months. The rest of the month incremental backups are taken.
- In the event of a failed or aborted full save, incrementals since the last successful full backup will be retained at least until the next successful full backup.

Extended and Policy based Options

- Custom schedules and retentions can be scheduled upon request and review. These will only be implemented in accordance with existing document retention policies (at UC and/or departmental levels) appropriate for the source data to be backed up and retained. For example, production database servers retain once-a-month full backups for 13 months to comply with business record policies.

2.3 Equipment and Software

The service uses a number of hardware and software components to deliver backup capabilities across a number of platforms.

- Hardware
  - Large capacity physical storage servers, leveraging redundant arrays of inexpensive disk (RAID)-based landing targets (also known as Disk to Disk or D2D backup).
  - Enterprise storage appliances with additional security, capacity-saving, and performance features. Data set candidates are limited to production level data requiring multi site replication, additional data security, etc
- Software
  - Dell EMC Networker for physical servers and virtualized database servers. Licensing is based on calculated capacity for one global set of full backups.
  - Veeam Backup and Replication for physical and virtual servers. Licensing is based on the number of sockets (i.e., physical CPU's) of the physical host server running a virtual machine that is backed up, in addition to the number of Veeam agents deployed for physical hosts being backed up.
  - NetApp Snap technology for array-based replication and snapshots. Licensing is based on the array model.

2.4 OIT Racks in Science Library Data Center

The equipment that provides the backup service is located in the Science Library Data Center (SLDC). This equipment is hardened against environmental failures by leveraging earthquake protection tables, an uninterrupted power supply (UPS), and data center chilled water cooling. Locating this equipment separately from the data sources increases the resilience of the data in the event of a local disaster.

2.5 Operational Support

OIT provides assistance and consulting to customers and potential customers seeking options to save copies of their data. OIT will assist customers with troubleshooting issues related to using the service, including escalating the issue to the underlying third party vendors as appropriate. OIT can assist customers with the recovery of data saved to OIT's Data Backup and Recovery Service.

2.6 Standard: Off-site Secure Copy of Data

OIT makes secure offsite copies (also known as backup saveset clones) of backup data to a remote location. This feature is enabled by default for all service subscribers.

2.7 Standard: Data Encryption

Networker, Veeam Backup and Replication, and/or enterprise storage appliances are configured to encrypt data at rest and in transit within the service. Encryption requires adequate processing power on the backup source server. Backup encryption is used with AES 256 bit encryption protected by managed pass phrases. Backup data copied to off campus locations is also encrypted.

2.8 Assumptions and Limitations

- For sensitive data that requires strict security compliances (examples include data subject to the requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, California Senate Bill (SB) 1386 of 2003, or UCOP's Business & Finance Bulletin IS-3 Electronic Information Security), it is the responsibility of the data owner to assess whether use of the OIT Data Backup and Recovery Service is compatible with any data security requirements.
- This service is not intended as a long-term/forever archival service. Data sets created from backup jobs have expiration dates (short term through long term) and are automatically removed from the service database once the expiration date is reached.
- This service is not intended to back up end-user computing devices such as desktops, laptops or other mobile devices.
- The source server being backed up must be accessible via the network from the central server and remain on-line through the completion of the data transfer.
- The source server being backed up must have sufficient resources to run the local client agent. Some features, such as data encryption, will consume significant local resources like processing power, memory and storage I/O.
- The source server operating system (OS) must be one of the client agent's supported operating systems. See Appendix for a list of supported OSes.
- If the source server requires local applications such as database backup tools to interact with the backup application, local privileged credentials on the source server must be shared with the backup administrative server.

Roles and Responsibilities

3.1 Service Recipient Responsibilities and Requirements

Customer responsibilities and/or requirements in support of this Agreement include:

- **Ensuring compliance to campus policy, UC policy and associated security requirements, including UC retention periods. Detailed information on these retention periods and the data they apply to can be found at: *https://recordsretention.ucop.edu/***
- Determine what data needs to be backed up. By default the software will attempt to backup all eligible data that is NOT excluded.
- Adequate technical knowledge to perform routine restores as a self service.
- Ensuring backups are being performed properly by reviewing all logs the client software creates, client configuration and email reports from each service run.
- Work with the service team to reschedule a full backup in the event of a failed or aborted full backup.
- Communicating specific service availability requirements to the service team.
- Submitting service requests through the OIT Help Desk or Service Now for new services, changes to existing backup service, or technical support.
- Availability of customer representative(s) when resolving a service-related incident or request.
- When necessary, provide a contact person who is technically able to install, upgrade and configure software on the system and look at various logs.
- With procedural assistance from OIT, obtain, install, upgrade, and customize as necessary, appropriate client software for the system. The cost of any client software installed on the source server is included in the monthly service charge.
- Provisioning adequate network connectivity to the campus network for both backup and restore functions. (If a system is replaced, connectivity to the campus network must exist before a restore of the backed up data can be done.)
- Notify OIT via a service request if significant changes are made to the data on the server being backed up, e.g. adding or removing local disks, adding or removing local data sets. A change is considered significant if the save set changes by more than 25% compared to a previous equivalent save set.
- Notify OIT via a service request if changes are made to the primary service recipients, email addresses for notifications and reports for the server being backed up.

When contacting OIT for assistance, please provide the following:

- Detailed description of the problem
- Time frame the problem occurred within
- Local client-side agent configuration files
- Local client-side agent and system log files, if applicable.

The service subscriber is responsible for canceling service. Billing will continue until a cancellation request is received via ServiceNow and acknowledged by OIT.

3.2 Service Provider Responsibilities and Requirements

OIT's responsibilities and requirements in support of this Agreement include:

- Providing backup status reports via email to designated contacts for each system and each service run.
- Providing access to the server-side Networker database for users to query the details associated with their server, i.e. data saved, date of service run, service run schedule, etc.
- Providing the capability for customers to initiate routine restores.
- Maintenance of OIT-approved physical hardware of the service including server and storage administration.
- Maintenance of the OIT-approved software environment of the service including applying patches and upgrades.
- Informing subscribers of client-side patches and upgrades.
- Consistent resource monitoring and subsequent tuning and advisement as it pertains to the overall service performance.
- Coordinating with vendors for any licensing, maintenance and support requests.
- Capacity planning for server-side resources (physical servers, disk storage, cloud services).
- Availability to work with customers to reschedule a full backup in the event of a failed or aborted full.

In the event of client-side and/or server-side performance problems, save or restore sessions in progress maybe be canceled at the discretion of OIT, in order to prevent service impact from client-side and/or server-side performance. OIT will notify the appropriate subscriber of the action taken.

The Data Backup and Recovery Service has been designed to avoid contention between compute, RAM and storage I/O operations; however, the potential for resource contention exists. If resource contention occurs due to a server host failure or resource over-allocation, production systems will have priority over development and test systems. OIT may also remove data from the service ahead of the normal expiration schedule to maintain the overall health of the service. Service recipients of the impacted backup data will be informed of the issue, actions taken and impact.

3.3 Parties & Escalation

OIT Help Desk, oit@uci.edu, (949) 824-2222, https://uci.service-now.com

Fields all support requests, creates trouble tickets, and engages OIT staff to resolve.

Data Center Infrastructure Group (oit-dci@uci.edu)

Joe Brancaleone (jbrancal@uci.edu)
Mitchell Stratford (mstratfo@uci.edu)
Allen Fann (afann1@uci.edu)

Primary, secondary and tertiary supporter of the Data Backup and Recovery Service. Responsible for overall management and monitoring of the service including the underlying servers and storage.

Ken Cooper (cooperk2@uci.edu)

Service escalation contact and SLA document owner.

Service Management

4.1 Hours of Support

OIT provides 24x7 support and monitoring of the overall service environment. Support for all service requests is normally provided during normal business hours of 8am to 5pm on weekdays (excluding University designated holidays). Support outside of these hours is provided only on an emergency basis (see section 4.3 for criteria on urgent requests), or if scheduled in advance.

4.2 Service Requests

All service requests should be initiated by contacting the OIT Help Desk via phone, email or ServiceNow. The OIT Help Desk will create a support ticket for tracking purposes and contact OIT support staff as needed.

4.3 Response Times

Requests for adding new servers should be completed within 10 business days, if all information is accurately provided and resources are available to handle the new data. If the request cannot be completed within 10 business days, the requestor will be contacted via phone or e-mail with an explanation for the delay.

All other support requests will receive a response according to their urgency. Urgent support problems will be responded to within 2 hours during business hours and within 4 hours outside of business hours. Non-urgent requests will receive a response by the next business day.

OIT will determine the urgency of each request using the following criteria as best provided by an authorized requestor:

- Significant number of people affected.
- Academic and Administrative deadlines.
- Significant impact on the delivery of instruction.
- Significant or lasting impact on student academic performance.
- Significant risk to law, rule, or policy compliance.
- Significant harm or financial loss to the university.

Urgent requests should be submitted by phone to the OIT Help Desk.

4.4 Service Management

OIT will use the OIT Change Policy and oit-changes mailing list to announce all significant and impactful changes to the Data Backup and Recovery Service. OIT will keep service subscribers informed of information relevant to them.

All changes will be announce in advance. Changes that cause a service interruption will be scheduled at least 7 days in advance. Changes that are not expected to cause a service interruption may be announced the day of the change. Exceptions may occur in response to emergencies.

4.5 Charges

Customers will be billed monthly via campus recharge unless other arrangements are made at the time of the service request.

Pricing for OIT services is maintained on the OIT website:

http://www.oit.uci.edu/data-backups

Appendix A: Networker

A.1 Supported Platforms and Operation Systems

Please refer to Dell/EMC compatibility guides for comprehensive and updated information

Networker Backup Server 19.4.x supports the following client platforms and operating systems:

Client Agent Backups:

MS Windows 2008 and newer

All major Linux Distributions (RHEL, CentOS, Fedora, Oracle, Ubuntu, SuSE, Debian, etc), x86 & 64 bit

MacOS

Solaris x86

Solaris Sparc

Intel

HP

VMWare

Application Hot Backup (Networker module for Databases and Applications):

MySQL 5.1, 5.5, 5.6 , 5.7, 8 on Linux x86 and x64

Oracle 11gR2, 12cR1 on Linux, Solaris, Windows

MS SQL 2005, 2008, 2012, 2014, 2017 and newer

Microsoft Exchange 2007, 2010, 2013, 2017 and newer

NDMP Client Connect (NAS manufacturers):

NetApp

Dell

EMC

Isilon

IBM

Oracle

etc.

A.2 Data Recovery Considerations and Procedures

Networker User programs are included in client packages installed on systems being backed up by Networker ('recover' in Linux, Networker User Recover GUI in Windows).

This provides the ability to perform self-service restores of files and data from available backups.

Data recovery may also require assistance by the Data Center team:

- Older backup set(s) needed for recovery appear unavailable if they reside in archival locations and a Data Center initiated retrieval process is needed to make the backup set(s) available for data recoveries. For example, Amazon Glacier is where older full backups for Networker reside, so any tape archived in S3 Glacier is retrieved to S3 using standard retrieval method which is typically within 3-5 hours. Once tapes are retrieved into S3 the backup data is then accessible for recovery.

- Firewall rules must be added to allow connections between Networker infrastructure and the target server in order to restore data.

- For different types of data sets other than filesystem data (RMAN database backups, MySQL Enterprise Backups, etc) Networker admin involvement may be needed to either provide info to the data owner, or otherwise assist in the success of the recovery process.

- Other various unexpected issues that may arise during the recovery procedure.

Customers are encouraged and expected to open a Service Now incident with the Data Center team whenever assistance with data recovery is needed. Incident Priority should reflect the criticality of the problem.

Appendix B: Veeam

B.1 Supported Platforms and Operation Systems

VMWare virtual machines (agentless image backups):

Platform: Veeam supports all VM objects in our current VMWare 6.5 environment, which include Virtual Hardware version 13 and all pervious hardware versions retroactively supported by our vcenter.

Operating Systems:

MS Windows 7, 8, 10, 2008 Server and newer

All major Linux Distributions (RHEL, CentOS, Fedora, Oracle, Ubuntu, SuSE, Debian, etc), x86 & 64 bit

MacOS

Physical (Veeam Agent):

Platforms: All major manufacturers of servers, desktops and laptops

Operating Systems:

- Both 64-bit and 32-bit:
- Microsoft Windows 7 SP1
- Microsoft Windows 8.x
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
    - * Server Core installations of Microsoft Windows Server OSs are not supported.
    - * Microsoft Failover Clusters are not supported.
- Any Linux kernel from version 2.6.32 and above

SLA Review & Update

The document owner is responsible for facilitating regular reviews of this document.

Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties.

The document owner will incorporate all subsequent revisions and obtain mutual agreements and approvals as required.