DISASTER RECOVERY AS A SERVICE

SERVICE DESCRIPTION

SUMMIT

Service overview

Summit's Disaster Recovery as a Service (DRaaS) is a combination of automated protection of virtual machines, a managed service to coordinate the ongoing real-time replication of data between two sites, managed failover testing on a regular basis, and managed failover & fail-back in the event of a declared disaster. Our DRaaS provides the ability to failover a virtualized environment to a Summit data center in response to a declared disaster. Upon declaration of a Disaster Event, together we will perform the pre-defined set of activities set forth in a mutually agreed-upon Runbook. DRaaS includes regular testing of failover and failback, with the option to run additional tests.

You will define a Source site and a Target site for recovery. The Source site can be at a Customer-operated premise, a colocation environment in one of our secure, resilient data centers, or in our Enterprise Cloud or a custom Private Cloud. The Target site will be in our Enterprise Cloud or a custom Private Cloud.

We begin by working with you to assess your needs, examining the virtual environment, the physical infrastructure, and the network connectivity options. Summit will verify the Customer's desired Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

Assessment includes an inventory of the applications used in the environment, with an eye toward understanding application dependencies, data flow, and level of importance. This information is used to map applications into priority groups and tiers to ensure that applications failover in the correct order and priority.

The Source location and Target destination for replication will be defined. All of this information is documented in a Runbook, maintained by Summit and available via our portal.

We will then implement the hardware and software necessary to support your DRaaS requirments. Secure network connectivity will be provisioned and maintained for the term of the service. During normal operations, we will monitor the replication processes and confirm the expected replication Service Level Agreements (SLAs) are met. We will also keep the configurations of Summit-operated physical assets used with the Service in sync, including firewalls, switches, routers, clusters, hypervisors, SANs, and network transit.

An initial failover and failback test will be performed for all VMs and applications protected by the Service. A separate, annual, full test of failover and failback procedures is also included with the Service. You can elect to have Summit run additional testing through the term of the Service, with options for a sandbox or full tests.

A sandbox test includes booting up replicated VMs in the Target site with your verification of data integrity and application functionality, but does not include full network testing or failback of VMs. A full test includes all failover and failback procedures documented in the Runbook.

In the event of disaster, failover and failback of applications will follow a collaboratively planned method and an organized plan for recovery. Together, we will pre-define the disaster criteria and business rules that would lead to a disaster event.

You will define the person(s) who can declare a disaster and request failover. You will also designate a different person(s) who will verify the declaration and approve the request. These steps reduce the likelihood of an error state in one part of your infrastructure leading to an unintentional disaster being declared.

You will have the option to continue to run the VMs at the Target site as long as needed (additional fees may apply). Once the timeframe for failback to the Source site is determined, we will follow the plan for failback documented in the Runbook. Again, we will verify the operational state of the VMs in the Source location and you will verify the operational state of applications and related software tools operated by your team.

You can also get information, request changes, view the Runbook, and review service ticket history about the DRaaS service in general through our Customer Portal.

Key features

A managed service

Our Managed Services team supports the underlying hardware, software, storage platforms and network connectivity used to deliver the DRaaS Service, as well as administers and monitors the backup and recovery processes put in place. You will receive a weekly DRaaS Service Report detailing the status of backup jobs, completion of jobs, and any other information about the jobs. You may open support requests to create or alter scheduling, change data retention policies, or get any additional information about the service.

Key features of our DRaaS include, but are not limited to:

- Based on proven, best-in-class hardware and software
- Highly-available, resilient, and secure design
- Automated protection of virtual machines in near real-time
- Managed failover and failback of VMs
- Collaborative planning and assessment of your needs
- Based on your defined RPO, RTO, and business unique needs
- Includes synchronization of physical devices used with the Service
- Service documented in Summit-maintained Runbook
- Initial and Annual full failover & failback test, with option for additional tests
- Complete infrastructure configuration & administration by Summit engineers
- 24x7 continuous monitoring, alerting, and support of the infrastructure
- Secure Customer Portal for documentation & service requests

Day-to-day management

The DRaaS service, including all associated hardware and software, is monitored 24x7x365 by Summit's Service Desk. Should any issues or anomalies be detected with the Services, a member of the Service Desk team will take corrective action as planned and notify you immediately. From time to time, we will perform scheduled maintenance activities on the infrastructure supporting the service. You will be notified in advance for all scheduled maintenance. Should a service-impacting emergency maintenance be required, we will use commercially reasonable efforts to notify you upon execution of the maintenance.

Change management

DRaaS provides simple and efficient means to make controlled changes to Client environments. System changes are serviced by the Managed Services Team through support requests. Changes follow a well-defined approval process, and most changes can be executed quickly by Summit's Managed Services Team.

Incident management

DRaaS includes the monitoring of the overall health of the Backup & Recovery platform and the handling of the daily activities of investigating and resolving alarms or incidents. Summit creates pre-defined playbooks that are used to rectify alarms and incidents in a way that minimizes disruption to each Client's environment.

Provisioning management

Designed to meet a Client's specific needs, DRaaS allows Clients to configure backup parameters and allocate additional resources to support rapidly changing envionments. These changes are managed through the timely handling of submitted support requests by our Managed Services Team.

Patch management

DRaaS takes care of all infrastructure system patching activities to help keep resources current and secure. When updates or patches are released from infrastructure vendors, Summit applies them in a timely and consistent manner to minimize the impact on Client business.

Access management

DRaaS enables clients to securely connect to the Service in the manner they require – be it API access, HTTPS, Cross Connects or Dedicated Physical Connectivity. Our team will make sure that the connection is maintained.

Security management

DRaaS protects Client information assets and helps keep all DRaaS infrastructure secure. All systems are logically separated and only available to the appropriate DRaaS environment. All Summit DRaaS services have encryption at rest and in-flight enabled by default for all Clients.

Continuity management

Summit can provide Restore / Recover services as an additional, on-demand service. In the event of a failure or outage that impacts the Client's business, or at their request, Summit can perform a restore of these backups as needed. Summit also offers comprehensive Disaster Recovery as a Service capabilities which introduces formal SLA and automation to the restore / recover processes.

Monitoring and reporting

All Summit DRaaS environments include comprehensive Health and Performance Monitoring. Weekly or monthly reports including the status of backup jobs and the associated storage utilization are available.

What makes this service unique?

Your business is unique — so is our service

We work with you to understand your data protection needs and configure the DRaaS parameters to support your unique business, financial, and technological requirements.

Custom policies

You can adjust the retention policies, encryption methods, and data locations to fit these requirements as your business changes.

Custom replication strategies

You may also choose to have backup data replicated to a third Summit-operated data center to provide additional physical redundancy should security, governance or compliance requirements dictate.

Roles, responsibilities and process

Successful Managed Services are the result of transparency and collaboration. Clearly defined processes and a detailed outline of roles and responsibilities are where this collaboration begins.

Our DRaaS Service is preceded by defined Consult and Plan, Design and Build processes. These critical steps establish the foundation for the execution of the Service and align these critical processes with your unique business needs.

Consult

We follow a proven, structured process of automated data collection and personal interviews with key business stakeholders, IT infrastructure, and application teams to successfully complete the Discovery process.

The outcome of these efforts includes identification of identification of business drivers and the discovery / analysis of your existing environment including Business and IT Governance processes, Infrastructure configurations and Networking and Security policies.

Our Managed Services and Solutions teams will coordinate with you to gather all details necessary to configure any hardware and software required for the DRaaS service. This includes establishing required secure network connectivity and bandwidth between the Source site and the Target site, establishing a list of Disaster Recovery Administrators, and installing any replication software or hypervisor drivers. Other client-specific requirements, such as traffic forwarding policies, procedures, or third-party requirements, will also be reviewed. This information is documented and stored in the Technical Design Workbook. The Technical Design Workbook is used to create a Customer Workbook that is shared with you after Implementation.

The Technical Design Workbook provides all necessary information to our engineers to ensure that information-gathering is complete and the Service will be able to address your needs. This may include network diagrams, configuration details and requirements, special security considerations, and more. The Technical Design Workbook will serve as a basis for configuration detail and will be utilized in the long-term planning and execution of the Service.

Plan, design and build

The data gathered and objectives defined in Consult inform the configuration and process requirements for your Service. Plan, Design and Build brings these to life.

During this phase we will deliver the official, comprehensive analysis of the current environment. This documentation includes, but is not limited to, Infrastructure Diagrams and network connectivity requirements – identifying how systems are accessed, used and managed today – and where risks are present.

Our technical teams will perform testing on the Summit-operated infrastructure that supports the Service. This includes, but is not limited to, validating software configuration, system redundancy verification, verifying network connectivity, monitoring and alerting configurations, including verification of data replication, and activation of the Service in the Customer Portal. Any deficiencies found will be corrected and re-tested until the system functionality is verified. Requests for customer-specific test criteria will be reviewed by Summit and evaluated on a case-by-case basis.

Run and operate

Now that your environment is successfully configured and verified as ready for production, the official DRaaS can begin. This is where we begin delivery of proactive day-to-day management, administration, monitoring, and support for your backup and restore environment

and processes.

The Project Manager or Provisioning staff will schedule a Customer Hand-Off Meeting with a member of the Managed Services team, either in person or via conference bridge. The Meeting is designed to advise the Customer of the state of the service, the current configuration, and answer any general questions about the Service.

Training is also provided on the Summit Customer Portal, including providing any access credentials to the Customer, walking the Customer through support engagement procedures, and general interaction with the Portal.

The Project Manager will also share the final/completed Customer Workbook, which takes the data from the Technical Design Workbook and Implementation process and acts as a the “as-built” documentation of the Service.

Summit Managed Services staff will coordinate with the Customer to create the initial replication schedule, create the protection groups, and configure the VMs for replication. At this time, the data retention settings will also be configured.

Once the replication has been configured, the initial synchronization from the Source site to the Target site will begin. After this initial sync has been completed, any new or changed data will continue to be replicated in the background from the Source site to the Target site. After the initial Disaster Recovery runbook has been created, our staff will work with your staff to perform an initial, one-time, full test of the disaster recovery plan. We will work with you to identify a mutually agreed-upon time for the test. Also, you will be required to have staff available to participate in the test to perform the data and application verification, as well as coordinate work on Customer-operated infrastructure that may need to be performed during the test.

Optimize and evolve

The final component of our DRaaS is the ongoing optimization and evolution of your environment. This phase has us focused on infrastructure performance and cost management. Monthly or quarterly reviews provide updates and opportunities for additional environment optimizations based upon changing business requirements and environment performance. Any opportunities identified are shared directly with your IT and leadership teams to inform strategy and decisions.

Our team is available to work with the your staff to conduct periodic testing of the Disaster Recovery Plan. The Service includes one (1) full failover & failback test per year. Regularly scheduled tests may also be added as part of your service. To schedule these tests, please open a support case. For information about the fees for additional tests, please contact sales@summitHQ.com for more information.

Many times, the Service will be integrated with additional Services provided by Summit. Some examples include Enterprise Cloud, Private Transport, and Managed Backup. All services and products necessary to complete the deployment will be completed either in tandem or in a phased approach during this post-implementation configuration period.

Over time, the Runbook may need modifications to it to reflect your changing needs and environment. Our Managed Services team will need to be contacted if any modifications are needed for the runbook or runbook procedures. You should open a support case with Summit to request these changes.

Using the baseline information in the Technical Design Workbook, the Summit Engineering team will configure the baseline parameters for initial operation.

The variables include:

- Change protection groups
- Increase/decrease number of VMs
- Runbook changes (priority changes, application changes)
- Altering priority for VMs

You do not have access to the hardware and software infrastructure used to deliver DRaaS, which is administered by Summit.

Should any changes to the Service be necessary, you can open a support case with Summit to request the work. Requests for non-standard changes will be reviewed by Summit and evaluated on a case-by-case basis.

For any of the other Managed Services used along with the DRaaS service, please refer to the appropriate Service Description for further information regarding those services.

Customer success and service operations

The foundation of every Summit Managed Backup and Recovery Service is collaboration. All customer success and service operations workflows have been designed to minimize response time, mitigate risk and optimize collaboration so knowledge transfer occurs when and where necessary.

We recognize your business, and your customers, operate 24x7x365. We have designed and operate our business to be here for you, whenever and however necessary to ensure your success.

Customer success team

Summit provides each customer with comprehensive resources to deliver ongoing service and support for your cloud environment. From sales, solution architecture and certified engineer support on our Service Desk, to customer success and executive management sponsorship, you will have experts with you every step of the way.

How to contact Summit support

Summit uses cases to identify incidents and provide support to our clients until the incident is resolved. Case identification and review is conducted using the Summit Customer Portal. Each Summit client is supplied with accounts that are permissioned to create, update and view their cases.

Getting support

Case Creation – Customer Portal

Support cases submitted to Summit are submitted using the Summit Customer Portal. The portal is accessible at: https://www.summithq.com/login-and-support/.

To create a support case:

- Log into the Summit Customer Portal.
- Select "Create Case".
- You receive an automatic confirmation of the successful case creation, including the case number.
- Summit Service Desk staff review the case for accuracy, confirm the Severity Level, and send acknowledgement of case receipt to you.
- Summit Service Desk agent & Cloud Services Engineer work to resolve the support case.
- Case updates are provided at set intervals as determined by the Severity Level.
- Case is Resolved & Marked for Closure.

Case Creation – Telephone

We recognize there may be times when a support case required the immediacy only a phone call can provide. Support cases may be created by calling the Summit Service Desk at +1 312-829-1111, Ext. 2. Telephone submitted support cases utilize a similar support operation, with a few modifications.

To create a support case:

- Call the Summit Service Desk at +1 312-829-1111, Ext. 2.
- Summit Service Desk Agent verifies caller identity, captures relevant information, creates the support case, and assigns a Severity Level.
- Summit Service Desk agent & Cloud Services Engineer work to resolve the support case.
- Case updates are provided at set intervals as determined by the Severity Level.
- Case is Resolved & Marked for Closure.

Case Escalation Paths

Summit provides several, formal options for support case escalation. Escalations occur to set a support case to a desired Severity Level, as outlined below.

Primary Escalation Path - This method is preferred as it is the most efficient method for raising the Severity Level of a case. To create a support case, you will:

- Log into the Summit Customer Portal.
- Navigate to the appropriate case.
- Click the "Escalate Case" link.
- Select the desired Severity Level and submit.

Alternate Case Escalation Path(s) - Additional Case Escalation paths are also available. However, it is important to note that Alternate Case Escalation Paths will not be as expedient as the Preferred Escalation Path.

Alternate Escalation – Case Response

You may submit a response to an existing case and simply request an escalation to the desired Severity Level. The Severity Level will be raised once a Service Desk Agent has reviewed and processed the request.

Alternate Escalation Path - Phone Support

- You may call the Summit Service Desk at +1 312-829-1111, Ext. 2.
- The Summit Service Desk Agent will verify the caller's identity and the support case number. You verbally request escalation to the desired Severity Level.
- The Summit Service Desk Agent updates the case accordingly.

Response time

All Summit customers can set the severity level of their support cases. The severity level you select will determine the response time. You can select the following severity levels when submitting a support case:

Infrastructure Administration (Proactive Services)

Severity Level	Description	Response Time SLA
Critical / Level 1	Critical Issues include business-critical system outages or issues causing extreme business impact.	15-minute response time
High / Level 2	High Severity Level issues include the impairment of production systems, impaired application performance, and moderate business impact.	30-minute response time
Normal / Level 3	Normal Severity Level issues include standard service issue requests and minimal business impact.	1-hour response time
Low / Level 4	Low Severity Level issues include general information requests, questions and guidance from Summit team members, arranging prescheduled maintenance activities.	4-hour response time
Informational / Level 5	Informational Issues include general questions, how-to style requests, or reports.	24-hour response time

As standard business practice, Summit's Service Desk acknowledges all support cases within 15 minutes of case creation. The response times identified in the table above represent the average time required to remediate such issues. Please note the response time to resolution of your issue may vary based upon circumstances and configurations unique to your business and your cloud architecture. Any support cases created without a severity level selected will be set to "Level 3 – Normal" by default.

Service level agreements

Summit provides two Availability SLAs for Cloud MSP customers.

Standard Cloud Application Management: We provide the following uptime SLA: 99.95% availability of the Cloud Application to respond to incoming requests from all endpoints for Standard Cloud Application configurations. If the Cloud Application's availability is disrupted, and the disruption lasts for more than 21 minutes, you shall be eligible for a credit.

High Availability Cloud Application Management: We provide the following uptime SLA: 99.99% availability of the Cloud Application to respond to incoming requests from all endpoints for High Availability Cloud Application configurations. If the Cloud Application's availability is disrupted, and the disruption lasts for more than six (6) minutes, you shall be eligible for a Credit as set forth below.

The SLA for Cloud Resources will be dependent upon the Cloud Platform(s) selected by Summit and you. You can find current version of the Cloud Application Management SLA on our website at www.summithq.com.

Account reviews

Summit offers quarterly and annual Account Reviews for all Managed Service Partnerships. These collaborative sessions aim to provide greater visibility into the technical, operational, financial and business aspects of your company and your Cloud. Account Reviews also provide you with a way to offer direct feedback, including areas of improvement, on the status of your Partnership with Summit.

An Account Review agenda includes:

- Introductions
- Technical, Operational, Business Updates
- Service & Performance Metrics/Dashboard Review
- Optimization Recommendations
- SLA Adherence & Support Ticket Review
- Access Control List (ACL) Review Q&A/Discussion

Upon completion of each account review, you should be confident that we are flexing our services and approach to meet you where you are and have a plan to take you where want to go so that you can focus on what matters most for your customers and your business.

Responsibility matrix

We are committed to solving your Backup and Recovery challenges so you can focus on what matters most.

Each Summit Managed Services Partnership operates with the understanding that there are two parties involved in supporting your environment: your in-house experts and ours.

The DRaaS Service, including all Summit-operated hardware and software, is monitored by our Managed Services Team and Service Desk. Should any issues or anomalies be detected with the Service, a member of the Summit Managed Services Team or Service Desk team will take corrective action as planned and notify the customer.

From time to time, we will perform scheduled maintenance activities on the infrastructure supporting the service. Customers will be notified in advance for all scheduled maintenance. Emergency maintenance may be required and performed without advance notice. Should a service-impacting emergency maintenance be required, we will use commercially reasonable efforts to notify Customer upon execution of the maintenance.

The following responsibility matrix defines the roles and responsibilities for each phase:

Consult responsibilities

Managed Service	SUMMIT	Customer
Identify Business Drivers	Y	Y
Align Business Drivers with Project	Y	Y
Current Infrastructure	Y	Y
Current Applications	Y	Y
Application Dependency Mapping	Y	Y
RTO/RPO Assignments	N	Y

Plan, design and build responsibilities

Plan and Design Managed Service	SUMMIT	Customer
Greenfield Architecture	Y	N
Total Cost of Ownership	Y	N
Migration Plannning	Y	N
Security and Compliance Requirements	Y	N

Build Managed Service	SUMMIT	Customer
Proof of Concept / Pilot Environment	Y	N
Environment Build-Out (New)	Y	N
Environment Remediation (Existing)	Y	N
Connectivity Between Souce and Target Locations	Y	N
Network Provisioning (IP Addresses, VLAN Configuration, VPN)	Y	N
Establish DR Services and Resources	Y	N
Environment Migration	Y	N
Runbook Coordination	Y	Y

Run and operate responsibilities

Configuration Management Managed Service	SUMMIT	Customer
DRaaS Infrastructure Patching and Updates	Y	N
DRaaS Infrastructure Configuration Management Automation	Y	N
DRaaS Infrastructure and Environment Audit Logging	Y	N
Credential Management and Resets	Y	N

Monitoring and Alerting Managed Service	SUMMIT	Customer
Connectivity Between Source and Target Locations	Y	N
DRaaS Services / Replication Services	Y	N
Hardware Health and Availability	Y	N
Cluster Capacity	Y	N
Infrastructure Alert Response and Triage	Y	N
Environment Alert Response	Y	N

Security Managed Service	SUMMIT	Customer
DRaaS Network Configuration and Security Protection	Y	N
Data Encryption Enforcement	Y	N
Key Management	Y	N
Compliance Support	N	Y

Run and operate responsibilities continued

Infrastruture Administration Managed Service	SUMMIT	Customer
Hypervisor Administration (Summit-Operated Infrastructure)	Y	N
Firmware Patching & Updates (Summit-Operated Infrastructure)	Y	N
Configuration Changes (per Customer)	Y	N
Change Management (Summit Change Management Process)	Y	N
On-Demand Recovery Support (Items Outside of Service)	Y	N

Support Managed Service	SUMMIT	Customer
Onsite Sparing of Identical Hardware (U.S. Locations)	Y	N
Hardware Troubleshooting (Summit-Operated Infrastructure)	Y	N
Hardware Replacement (Summit-Operated Infrastructure)	Y	N
Hardware Maintenance (Summit-Operated Infrastructure)	Y	N
Replications Tools and Software	Y	N
Support / Incident Portal	Y	N
Incident Response	Y	N
Request Response	Y	N
Custom Dashboard and Reporting	Y	N
On-Demand Recovery Support (Items Outside of Service)	Y	N

Optimize and evolve responsibilities

Change Management Managed Service	SUMMIT	Customer
DRaaS Infrastructure Resources	Y	N
DRaaS Application Configuration	Y	N
Protection Groups	Y	N
Increase / Decrease VMs	Y	N
Alerting Priority for VMs	Y	N
RTO/RPO Modifications	N	Y

Failover Testing Managed Service	SUMMIT	Customer
Annual Failover / Failback Testing	Y	Y

Audit Trails Managed Service	SUMMIT	Customer
DRaaS Infrastructure Logs	Y	N
OS-Level Logs	Y	N
Application-Level Logs	Y	N
Platform Compliance Initiatives	Y	N

Key assumptions

SUMMIT

- Summit will retain exclusive administrative access to the Summit-operated infrastructure of the Disaster Recovery Service for the duration of the agreement.
- In general, Summit is not able to make any assumptions regarding your environment, applications, or business processes. All relevant information must be provided by you for this portion of the service.
- Summit does not offer business impact analysis consulting services. Summit can work with your during the sales process to identify gaps in preparation for a business continuity plan and offer recommendations to third parties that can offer consulting services.
- Summit cannot define which systems are critical for your business, computing environment, or critical business processes. This type of data, including Recovery Point (RPO) and Recovery Time Objectives (RTO), must be supplied by the Customer.

Customer

- Customer is responsible for providing all instructions and procedures that Summit will follow during a disaster or fail back event. This includes identifying critical business processes and mapping servers and virtual machines to those processes, as well as the restoration order during a DR event.
- Customer must inform Summit of any requested modifications or changes to the Runbook. This includes the removal or addition of any physical servers or virtual machines involved in the Disaster Recovery Service.
- Customer is responsible for performing any necessary business impact analysis and to defining critical business processes, as well as mapping these processes to individual systems.
- Customer is responsible for the installation and operation of any and all scripts and applications installed on any customer managed servers or virtual machines.
- Customer is responsible for the security of all scripts and applications installed on your servers. Summit does not provide security auditing or disinfection of exploited software or servers.
- Customer is responsible for maintaining current backups of customer-owned data. Summit offers a fully managed backup service for physical and virtual servers, including the Enterprise Cloud. Please contact sales@summitHQ.com more information.
- Customer is responsible for maintaining the list of authorized personnel on the Summit Customer Portal, Enterprise Cloud Portal or Private Cloud Portal.
- Customer is responsible for maintaining any user accounts created for the Enterprise Cloud or Private Cloud. Summit is not responsible for any unauthorized access to the Enterprise Cloud or Private Cloud resources due to out of date access list information.
- Customer will designate and maintain a Customer Contact who can be made available to Summit for troubleshooting or questions.

Tired of tech that underdelivers?

Let’s fix that. Get IT infrastructure that works at summithq.com.