CenturyLink Service Guide

Managed Disaster Recovery Service 1.0

Version: December 17, 2019

This Service Guide ("SG") sets forth a description of the Managed Disaster Recovery Service 1.0 offered by CenturyLink, including technical details and additional requirements or terms. This SG is subject to and incorporated into the Agreement, CenturyLink TS Service Exhibit and the Hosting Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order. For avoidance of doubt, any references in the Agreement, Schedule, or Service Orders to SSG, shall mean SG.

Service Description

1. **Standard Service Description:** Managed Disaster Recovery Service 1.0 ("MDRS" or "Service") is a Managed Hosting product. "MDRS" may also be referred to as "Disaster Recovery Management Services" or "DRMS" in any applicable orders or invoices. The Service leverages CenturyLink's proprietary SafeHaven software to offer disaster recovery ("DR") solutions and services. The Service includes installation, configurations, administration, 24X7 monitoring, maintenance, audit, test and at time of disaster ("ATOD") services as detailed herein.

   The MDRS is dependent upon the following:

   a) Supported Production Platforms and Supported Recovery Platforms: Customer must already have a Supported Production and Recovery Platform. If a CenturyLink Supported Production and/or Recovery Platform, then it must be purchased under a separate Service Order and Service Attachment. If a Customer provides the Supported Production and/or Recovery Platforms, then Customer is responsible for ensuring such platforms are enabled per the requirements of MDRS described in this SG. The Recovery Platforms enable connectivity for WAN sync and for Recovery Servers.

   b) Customer must purchase a DR Manager resource as a mandatory add-on service. CenturyLink delivers a mandatory DR Manager role as part of the Service. DR Manager is a CenturyLink assigned person who organizes the installation, audit sessions, test activities and ATOD services. Please refer to the DR Manager section below and Table 3 for additional terms and a more detailed description of the DR Manager role and responsibilities.

   The MDRS is available in certain CenturyLink premises as detailed herein or at a customer's premises. CenturyLink shall not be liable for any failure to perform in the event Customer does not fulfill Customer's responsibilities and requirements as detailed herein and in the event of Customer's errors or omissions in setting up the required environment. Please refer to Table 3 Roles and Responsibilities for MDRS for more details. In addition CenturyLink is not responsible for any loss or corruption of data or information. CenturyLink's obligations related to data are exclusively governed by the Security and Compliance section of the applicable Service Schedule or Service Exhibit.

   SafeHaven Software Components: The SafeHaven software contains the following components (I) SafeHaven Replication Node (SRN); (II) Replication Agent (RA); (III) Central Management Server (CMS); and (IV) SafeHaven Console. SRNs are individual virtual servers deployed in the Supported Production and Supported Recovery Platforms. An SRN hosted in a Supported Production Platform is called a production SRN and an SRN hosted in a Supported Recovery Platform is called a recovery SRN. Data is synced from a Supported Production Platform SRN to a Supported Recovery Platform SRN. The Replication Agent is a component installed on a Primary Server to replicate data from local disk to a production SRN. CMS is an individual virtual server installed on the Supported Recovery Platform and it coordinates the communications among SRNs and tracks the SRN status. The SafeHaven Console is the interface displaying the SRN status and configurations. Users launch the SafeHaven Console from a customer server and interact with it to perform disaster recovery administration tasks. Additional information is available in the SafeHaven Overview, located here: www.ctl.io/knowledge-base/disaster-recovery/safehaven-overview/ and technical details are available at www.ctl.io/knowledge-base/disaster-recovery/safehaven-4/.

Licensing and Third Party Terms: If any third-party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with the Service, Customer agrees to be bound by any additional licensing terms and conditions applicable to such third-party software and that it will use such third-party software strictly in accordance with such terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third-party software.

1.1. Installation: MDRS installation includes SafeHaven deployment and monitoring system installation. Please refer to Table 3 Roles and Responsibilities for MDRS
for more details.

1.1.1. Supported Operating Systems for Primary Servers: Table 1 Supported OS and SafeHaven Protection Group Matrix shows the supported Operating System ("OS") types and versions of a Primary Server. A Primary Server with a different OS cannot be protected by MDRS.

1.1.2. Supported Production and Recovery Platforms (as defined in this SG): Table 2 illustrates the Supported Production and Recovery Platform combinations.

1.2. Configuration: CenturyLink configures SafeHaven software and the Supported Recovery Platform Servers as per the detailed information displayed in Table 3 Roles and Responsibilities for MDRS.

1.3. Administration: Customer is given access to the solution via the SafeHaven Console from which Customer can view the protected servers and replication status. Customer can take certain administrative actions marked with "X" in the Customer column in Table 3 Roles and Responsibilities for MDRS. CenturyLink shall not be liable for any failure to perform in the event of Customer's error or omissions. CenturyLink shall not be responsible for the changes that are made via the SafeHaven Console by Customer.

1.4. 24X7 Monitoring: CenturyLink enables monitoring on SafeHaven components and Windows Primary Servers. Table 5 provides details of the monitoring probes deployed on SafeHaven components. No monitors are available or deployed on Linux Servers.

1.5. Maintenance: The Audit and Maintenance section in Table 3 shows the audit range and corresponding maintenance scope. CenturyLink engineers take actions to troubleshoot the issues that have caused the alerts on SafeHaven components and Supported Recovery Platform.

1.6. Audit Services: Audit services identify new servers, disk changes, applications modifications, connectivity and computing resource alterations on the Supported Production Platform and reflect the modifications on the Supported Recovery Platform. See Audit section in Table 3 which details the audit scope and descriptions.

1.7. Testing: CenturyLink provides semiannual Test-Failover as part of the service. SafeHaven Test-Failover is an isolated test in which the connectivity between Primary Servers and the corresponding Supported Recovery Platform Servers are temporarily cut off. To avoid workload interruptions, tests and alterations on the Supported Recovery Platform will not be routed back to the Supported Production Platform. Table 3 shows the test scope, as well as CenturyLink and Customer responsibilities during test.

1.8. At-Time-Of-Disaster (ATOD) Services: MDRS includes monitoring signals when there is a disaster, however, Customers must decide whether they will formally declare a disaster with CenturyLink and receive ATOD Services or handle the disaster themselves. To declare a DR event, Customer must contact the Global Support Desk to initiate a P1 ticket. CenturyLink will provide 24x7 support throughout the declared ATOD event. Once per calendar year, CenturyLink will provide the ATOD Services specific to one declared event at no charge. Should Customer submit more than one disaster declaration form annually, any such additional ATOD Services must be purchased separately for a standard fee as determined by CenturyLink. If Customer does not submit any disaster declarations within a calendar year, then the free instance of ATOD Services is forfeited for that year. Please refer to Table 3 for more details.

2. **Customer Responsibilities:** Customer is responsible for all tasks marked with an "X" in the Customer column in Table 3 for MDRS and Table 4 for DR Replication, as applicable depending on services ordered by Customer. Customer acknowledges and agrees that its failure to perform its obligations set forth in Tables 3 and 4, as applicable, may result in CenturyLink's inability to perform the services and/or additional fees and CenturyLink shall not be liable for any failure to perform in the event of Customer's failure.

2.1. Provide Contact: Designate and maintain a Customer Contact during the service term and renewal term (including current contact information). "Customer Contact" means a technical point of contact with sufficient knowledge, authority and access to address configuration issues, event notifications, system or infrastructure modifications and authentication of applicable systems.

2.2. Provide Technical Support. Customer agrees to provide to CenturyLink technical support, log-in privileges where required and on-going support. Customer shall ensure Supported Production and

Supported Recovery Platforms are provisioned with servers, local incremental and replica storage, network connectivity, CPU and memory resources, and other infrastructure components; and replication is operational.

2.3. Neither Customer nor its representatives shall attempt in any way to circumvent or otherwise interfere with any security precautions or measures of CenturyLink relating to the Service or any other CenturyLink equipment.

2.4. Customer acknowledges and agrees that it is solely responsible for selecting and ensuring its software and systems are up to date and supportable.

2.5. Customer further acknowledges and agrees that CenturyLink's SLA only applies to currently supported configurations (including but not limited to related operating systems or software) at the time SLA support requests are triggered. If any configuration or version is identified as "unsupported" by a vendor, the Services are subject to all of the following conditions and/or requirements: (i) a service level objective ("SLO") referring to CenturyLink's reasonable effort to provide support will apply in lieu of any other applicable SLA and will automatically apply from the time CenturyLink receives notice from the vendor of such unsupported service,; (ii) CenturyLink, in its reasonable discretion may elect to charge the customer for any support or additional tasks/work incurred by CenturyLink resulting from Customer's continued use of unsupported configuration until Customer purchases the required and supported upgrades or extended support at an additional cost from the vendor. The requirement to purchase upgrades or extended support from vendor shall apply at any time, regardless of any contract term, term commitments, or renewal periods. Customer's failure to do so may result in CenturyLink's inability to provide the Services and CenturyLink shall have no liability therefrom.

2.6. Customer consents to CenturyLink's and its affiliates or subcontractors' use and transfer to the United States, or other countries, data or information (including Customer Contact information such as names, phone numbers, addresses and/or email addresses) of the Customer for the sole purpose of: (i) fulfilling its obligations under the Agreement; and (ii) providing information to Customer about CenturyLink's products and services. Customer represents that it will ensure that all information provided to CenturyLink is accurate at all times and that any business contact has consented to CenturyLink's processing of such information for the purposes identified herein.

3. DR MANAGER MANDATORY ADD-ON SERVICE

The following additional terms shall apply to the DR Manager add-on service:

CenturyLink will provide all of the tasks identified in Table 3 as part of the minimum service package provided by CenturyLink. Customer will be billed a minimum MRC for a minimum number of hours of DR Manager Services based on the number of VMs in service and will be billed at a standard hourly rate denoted on the Service Order for any additional hours required to perform the minimum tasks. Customer may at any time, request additional hours of DR Manager Services which will be billed by CenturyLink on an hourly basis. Standard service hours are as follows: for a quantity of 1-30 VMs, the # of DR Manager hours included are 6.25 per month; 31-75 VMs is 11.25 hours per month and 76 - 150 VMs is 16.25 hours per month. Monthly hours cannot be shared between Customer accounts. All service hours will occur during standard working hours, local time. Customer authorizes CenturyLink to bill and Customer agrees to pay any hours worked beyond the standard or contracted hours that are requested by Customer, including requests to continue work or projects that are submitted to CenturyLink via electronic mail. Notwithstanding the foregoing, CenturyLink reserves the right to require the execution of a Change Order before commencing any work in excess of such standard or contracted hours.

Nothing herein or in the performance of the DR Manager Service shall transfer to Customer any CenturyLink Technology, and all right, title and interest in and to CenturyLink Technology will remain solely with CenturyLink, its affiliates and their licensors. Notwithstanding anything to the contrary herein, CenturyLink will not be prohibited or enjoined at any time by Customer from utilizing any skills or knowledge acquired during the course of providing the Services, including, without limitation, information publicly known or available or that could reasonably be acquired in similar work performed for another customer of CenturyLink. Customer agrees to provide all necessary access and permissions related to Customer technology, systems and/or proprietary information necessary for CenturyLink to provide the DR Manager Service and further consents to CenturyLink access, processing, use and/or transfer of any Customer information or data (including to or from the United States) for the sole purpose of fulfilling its obligations hereunder. As used herein, "CenturyLink Technology" means the proprietary technology of CenturyLink and its licensors, including services, software tools, hardware designs, algorithms, software (in source and object forms), user interface designs, architecture, class libraries, report formats (including for runbooks), objects and documentation (both printed and electronic), network designs, know-how, trade secrets and any related intellectual property rights throughout the world and also including any derivatives, improvements, enhancements or extensions of CenturyLink Technology conceived, reduced to practice, or developed during CenturyLink's performance of the DR Manager Service.

Customer consents to CenturyLink collecting and compiling system, log or usage data to determine trends. CenturyLink may associate this information with similar information of other Customers so long as such information is merged and/or anonymized in a manner that will not in any way reveal the information as being attributable to any specific Customer.

3.1. Customer Responsibilities specific to the DR Manager add-on services are as follows:

Notwithstanding anything to the contrary, the parties expressly agree that nothing herein shall convey or be construed to convey or otherwise transfer any intellectual property or other proprietary rights held by CenturyLink, its vendors or licensors.

Notwithstanding any other provision or understanding to the contrary in any document, CenturyLink makes no representation, warranty, or guarantee that any of the Tasks performed hereunder comply with or satisfy any applicable governmental or industry data security standard. If such Tasks include security services provided by CenturyLink, Customer acknowledges that CenturyLink may not identify all possible incidents or vulnerabilities and CenturyLink expressly disclaims any responsibility for any unidentified or misidentified incidents or vulnerabilities. If CenturyLink provides an assessment, certification, report, or similar material to Customer hereunder, such material is developed in good faith as to its accuracy at the time of inspection or review by CenturyLink and provided AS IS.

Customer will specifically identify and provide CenturyLink with access to all relevant Customer-controlled information, resources and locations required to complete the Scope of Work set forth above.

Customer will provide CenturyLink contact information (name, phone, email) for all Customer team members with whom CenturyLink will interface.

Customer will attend a weekly review call/meeting with the CenturyLink Project Manager, to review in collaboration, the weekly report and next steps.

Neither Customer nor its representatives shall attempt in any way to circumvent or otherwise interfere with any security precautions or measures of CenturyLink relating to the Service or any other CenturyLink equipment.

CenturyLink is not responsible for the hardware, software licenses, and vendor maintenance support for any devices not listed in this SG.

While performing the Services, if CenturyLink encounters (i) any concealed or unknown condition, (ii) a Customer responsibility contained herein is not met, or (iii) a delay caused by Customer, then the scope, schedule and/ or fees may be equitably adjusted as necessary via execution of a change order. If the parties cannot agree to the change order, CenturyLink shall not be obligated to deliver the affected Services.

If so required, Customer will provide suitable workspace for CenturyLink resources working at the Customers facility with closed door rooms, including adequate environmental controls, lighting, telephones and network access including Virtual Private Network ("VPN") access via the internet.

4. **Additional Services:** At Customer's option and expense, Customer can purchase the following additional services for an additional fee. These additional services are available only if Customer has purchased MDRS.

a) DR Replication for Active Directory ("AD"). CenturyLink offers this optional add-on service for configuring and maintaining a secondary AD instance in the Supported Recovery Platform. Customer and CenturyLink responsibilities specific to this DR Replication Service are detailed in Table 4 Roles and Responsibilities for DR Replication for AD. The secondary AD instance is tailored to Customer's MDRS and enables the continuation of AD services to support authentication for the VMs running in the DR infrastructure during a Failover. In order for CenturyLink to deliver this Service, Customer is required to grant administrator access permissions on the Customer's Supported Production Platform AD server to CenturyLink. CenturyLink will use commercially reasonable efforts to secure the administrator permissions provided by Customer.

i. A CenturyLink supported virtual machine with Managed Operating Systems Service is a requirement for AD as it provides the infrastructure (CPU, RAM, Disk, Windows Operating system including AD, local area network connectivity) to deliver secondary AD services.
ii. A separate isolated network or disabling of replication will be used so that changes made to AD services during test will not impact Supported Production Platform AD services.
iii. After a test, we will demote domain controller and promote it again so nothing from the test can impact the Supported Production Platform.
iv. The Customer is responsible for removing the domain controller from unmanaged AD on the Supported Production Platform since neither the network or replication to the Supported Production Platform will allow for the removal of AD server when we perform the demotion.
v. During an outage or disaster, CenturyLink will seize FSMO roles if needed to help keep the environment stability (managed or unmanaged AD).
vi. Monitoring of DR Replication for AD is detailed in Table 6 Monitors for Secondary Active Directory Server. CenturyLink enables 24x7 monitoring on the secondary AD instance. Table 6 provides details of the components that are monitored.
vii. The Customer responsibilities set forth in Section 2 above must be met for this DR Replication for AD Service.
viii. This domain controller will be used for DR and only for DR as usage for other purposes may cause impact to the Supported Production Platform.

Appendices

Table 1 Supported OS and SafeHaven Protection Group Matrix

OS Type	OS Version	Local Cache Protection Group	Replica Protection Group
Windows	2008 R1 (64 bit) 2008 R2 (64 bit) 2012 R1 (64 bit) 2012 R2 (64 bit) 2016 (64 bit) 2019 (64 bit)	X X X X X X	X X X X X X
Ubuntu	12.04 (32 and 64 bit) 14.04 (32 and 64 bit) 16.04 (32 and 64 bit)		X X X
Red Hat Enterprise	5 series (32 and 64 bit) 6 series (32 and 64 bit) 7 series (32 and 64 bit)		X X X
CentOS	5 series (32 and 64 bit) 6 series (32 and 64 bit) 7 series (32 and 64 bit)		X X X
openSUSE	11 series (32 and 64 bit) 13 series (32 and 64 bit)		X X

Table 2 Supported Production and Recovery Platforms

Supported Production Platform	Supported Recovery Platform
CenturyLink Cloud	CenturyLink Cloud
CenturyLink Cloud	AWS
CenturyLink Cloud	Microsoft Azure
Customer-provided VMware Environment	CenturyLink Cloud
Customer-provided VMware Environment	AWS
CPCvCF	AWS
AWS	AWS
CenturyLink Dedicated Cloud Compute	Microsoft Azure
Customer-provided VMware Environment	Microsoft Azure
AWS	Microsoft Azure
CenturyLink Dedicated Cloud Compute	CenturyLink Cloud

Table 3 Roles and Responsibilities for MDRS

Activity	Task	CenturyLink Engineer	CenturyLink DR Manager	Customer
Installation	Create and distribute protected server inventory lists		X	
	Evaluate and advise on requirements needed for Customer Premise in terms of connectivity, storage, email relay configuration, computing resources reservation etc.		X	
	Prepare the Supported Production Platform to meet the SafeHaven requirements in terms of connectivity, storage, email relay configuration, computing resources reservation etc.			X
	Organize meetings for Customer and CenturyLink engineers to start the installation		X	
	Create and deploy SafeHaven Replication Nodes (SRN) on primary and Supported Recovery Platform sites	X		
	Create and deploy SafeHaven CMS on Supported Recovery Platform site	X		
	Create SafeHaven Cluster	X		
	Establish and verify connectivity among CMS, SRNs, Supported Primary Platform Servers and Supported Recovery Platform Servers	X		
	Set up the email relay for Periodic DR Report	X		
	Deploy Supported Recovery Platform Servers	X		
	Provide interdependencies among Primary Servers			X
	Create Protection Groups (PGs) based on the provided interdependencies and Supported Recovery Platform Servers	X		
	Authorize CenturyLink to install RA on Primary Servers			X
	Install RA on Primary Servers and start local disk replication	X		
	Install and configure monitoring system	X		
Configuration	Configure connectivity setting files on Supported Primary Platform Servers for network recovery	X		
	Configure the replication rate to coordinate with Primary Servers' daily workloads	X		
	Configure the WAN sync rate	X		

	Configure the Supported Recovery Platform Servers' boot up sequence	X		
	Configure the Supported Recovery Platform Servers' boot up delay time	X		
	Configure email relay for Periodic DR Reports	X		
Administration	Edit the email list to receive periodic reports	X		X
	Edit the frequency of receiving the regular reports	X		X
	Edit the WAN sync speed	X		X
	Edit the checkpoint interval for each PG	X		X
	Launch PG Failover	X		X
	Review Disaster Recovery Emergency Team (DRET) member assignments and verify the contact information is accurate and up to date		X	
	Problem escalation and root cause analysis reporting		X	
	Quarterly proactive touch point calls		X	
	Bi-annual executive reviews		X	
	Submit billing service credit request and related inquiries, if necessary		X	
	Review and validate the creation of operational runbooks		X	
	Quarterly conference call meeting to review capacity and performance data and configuration changes to identify improvements and any potential critical items to present to Customer		X	
	Identify and recommend opportunities for		X	
	automation and simplification			
	Present new infrastructure solutions and improved utilization proposals to Customer		X	
Audit & Maintenance	Authorize CenturyLink to modify RA settings on Primary Servers during maintenance window			X
	Services running on SRNs	X		
	Services running on CMS	X		
	Remaining disk space of SRNs and CMS	X		
	Add protected server(s) to PG	X		
	Remove protected server(s) from PG	X		
	Create new PGs	X		
	Add new disk(s) to protection	X		
	Remove protected disks	X		
	Expand protected disks	X		
	Pause Local Replication	X		
	Restart Local Replication	X		
	Pause the WAN sync	X		
	Restart the WAN sync	X		
	Upgrade SafeHaven software with any Minor Releases	X		

	Delete SafeHaven PGs	X		
	Delete Supported Recovery Platform Servers	X		
	Update the network configurations, computing resource changes etc. on the Supported Recovery Platform to reflect the changes on the Supported Production Platform	X		
	Create audit report to include (where possible) improvement and remediation suggestions		X	
	Uninstall SafeHaven	X		
Testing	Coordinate semi-annual test for the DR solution		X	
	On the Supported Recovery Platform, authorize CenturyLink to verify the recovered files and applications			X
	Initiate SafeHaven Test-Failover operation	X		
	Check to see if Supported Recovery Platform Servers boot up successfully	X		
	Set up connectivity for the Supported Recovery Platform Servers	X		
	Network isolation between Supported Production Platform Servers and Supported Recovery Platform Servers	X		
	Test and verify the supported applications are working properly on Supported Recovery Platform Servers	X		
	Delete Test-Failover clone and restore the DR environment	X		
	Collect feedback from Customer and assist with post-test report generation		X	
	Create post-test report and update the runbook		X	
	Review post-test report and updated runbook with stakeholders and discuss any adjustments to processes and/or environment, necessary, to more directly align with business objectives		X	
	Share with different parties the updated runbook and post-test report		X	
ATOD service	Contact CenturyLink support desk at 888-638-6771 and request a P1 incident ticket be open <Customer Name>. Use the following verbiage in the ticker; “We would like to invoke our disaster recovery process. We are using the Managed Disaster Recovery Services product and would like our DR Manager (State DR Manager’s name) contacted as soon as possible.” In addition, provide a list of the impacted Protection Groups including the region/data center in the P1 ticket.			X

	Manage communications and send recovery status updates to all parties		X	
	Confirm all team members have documented recovery procedures, inventory lists, and that they have reviewed the recovery procedures		X	
	Lead a discussion with Customer to agree upon the Recovery Point		X	
	Failover the Protection Group to the agreed Recovery Point		X	
	Execute the recovery procedures according to runbook	X		
	Server level recovery. Make sure that the Supported Recovery Platform Servers are booted up successfully and validate that the Primary Server images are recovered.	X		
	Best effort for application Recovery. For applications that are native to the Windows OS residing on servers protected by SafeHaven, applications are started during a test or real Failover. All configurations within the applications will remain the responsibility of Customer. Applications that are unable to start due to configuration issues within the application shall be the responsibility of the Customer	X		
	Recover Managed OS components. For OS managed by CenturyLink, restoring Managed OS components on Recovery Server is included in the Failover services	X		
	Setup monitoring system on recovery site	X		
	Notify Customer that Failover services are complete	X		
	Send recovery status updates to all parties		X	

Table 4.0 – Roles and Responsibilities for DR Replication with Active Directory

Activity	Task	CenturyLink Engineer	CenturyLink DR Manager	Customer
Installation	Grant CenturyLink Admin access to the Customer’s AD.			X
	Install and configure monitoring system on the secondary AD.	X		
	Network connectivity between Customer’s AD and the secondary AD.			X
	Create secondary AD server on the recovery environment and add them to the existing domain, ensure full and continuous AD database replication.	X		
Audit & Maintenance	Reflect the changes on secondary AD servers including OS update, AD application changes.	X		
	Grant CenturyLink Admin access to the Customer’s AD.			X
	Enable appropriate administrative access logging.			X
Testing	Validate and test successful AD replication prior to network connectivity isolation including: A. Validate successful site to site replication. B. Create test object on AD server in primary site, validate successful replication.	X		
	Verify connectivity and AD domain resolution of recovered servers in all sites.	X		
	Validate and remediate any AD domain issues during network isolation/test failover, assist with domain related troubleshooting as failover servers brought online.	X		

	Move/sieze AD FSMO roles to secondary/DR site, only if deemed necessary for successful Failover operations.	X		
	Move/sieze AD FSMO roles to primary site, only if moved during previous test step.	X		
	Test Validation			X
	Backout changes	X		
	Coordinate re-establishing connectivity between Supported Production Platform AD and secondary DR AD.	X		
	Establish connectivity between Supported Production Platform AD and secondary DR AD.			X
	Validate and test successful AD Replication after test completed and network connectivity is restored A. Validate successful site to site replication. B. Create test object on AD server in primary site, validate successful replication on AD server in secondary/DR site.	X		
ATOD service	Assess state of AD site replication and connectivity: A. Full connectivity outage between AD servers/sites. B. Is restore of primary site possible and what is the estimated time until restore of primary site? C. Make note of replication state and last good replication between primary/secondary sites.	X		
	Move/sieze AD FSMO roles to secondary DR site: A. Required if primary site is hard down with no estimated time for restore, and/or application servers in secondary site require roles available for successful operations. B. Optional if primary site restore expected within 24 hours, and/or application servers in secondary site DO NOT require roles available for successful operations.	X		
	Verify connectivity and AD domain resolution of Safehaven servers in secondary/DR site.	X		

	Validate and remediate any AD domain issues, assist with domain related troubleshooting as Failover servers brought online.	X		
	Validate successful monitoring of AD domain and server health for secondary/DR site.	X		

Table 5 Components of SafeHaven Monitored by CenturyLink

Monitoring	Description
Server CPU	Alarm once the CPU of SafeHaven node spins up to 90%
Server Memory	Alarm once the memory consumption is more than 90%
Disk Space	Alarm when free space on SRN primary disk is less than 5G
CMS service	Alarm when the manager service on CMS is not running
Uptime check	Alarm when a Safehaven infrastructure VM goes down.

Table 6 Elements of OS Monitored for Secondary Active Directory Server

Monitoring	Description	Frequency
Monitor the new technology file replication service (“NTFRS”) process	Alarm when NTFRS process spins CPU up to 90%	5 Min
Monitor the distributed file system replication (“DFSR”) process	Alarm when the DFSR process spins CPU up to 90%	5 Min
Monitor AD Domain Trust Status	Alarm when the “TrustIsOK” value is False	1 Hour
Monitor the total number of replication partners that have failed to synchronize	Alarm if the number of replication partner is greater than 0	1 Hour
Monitor Lan Manager service	Raise an alarm if Lan Manager service is in “continue pending” state	5 Min
Monitor File Replication service	Raise an alarm if File Replication service is in “continue pending” state	5 Min
Monitor DNS Client	Raise an alarm if DNS Client is in “continue pending” state	5 Min
Monitor Security Accounts Manager software	Raise an alarm if Security Accounts Manager software is in “continue pending” state	5 Min
Monitor Intersite Messaging service	Raise an alarm if Intersite Messaging service is in “continue pending” state	5 Min

Monitor Kerberos Key Distribution Center service	Raise an alarm if Kerberos Key Distribution Center service is in “continue pending” state	5 Min
Monitor Distribution Center Net Logon service	Raise an alarm if Distribution Center Net Logon service is in “continue pending” state	5 Min

Definitions

Active Directory (“AD”): A Microsoft Windows Operating System directory service that authenticates and authorizes users, applications and servers in a Windows domain network delivering core tasks such as signing and enforcing security policies for all servers and installing or updating software.

Amazon Web Services (AWS) EC2: Elastic Compute Cloud product from AWS.

Amazon Web Services (AWS) Elastic Block Storage (EBS): storage for use with AWS EC2.

Central Management Server (CMS): SafeHaven CMS is part of SafeHaven Cluster. It gathers information about status of SRN nodes, status of Protection Groups, Recovery Point history, job history, WAN sync speed, un-synced data and presents the information via the SafeHaven Console. CMS receives commands from SafeHaven Console and distributes the commands to SafeHaven Replication Nodes to execute.

CenturyLink Cloud: CenturyLink Cloud is a single cloud platform offering enterprise cloud services ideal for business apps, IaaS, PaaS, SaaS, DBaaS and cloud management via a user-friendly control portal.

CenturyLink Dedicated Cloud Compute (DCC): CenturyLink DCC is a dedicated cloud infrastructure providing secure virtualized hosting.

CenturyLink Private Cloud on VMware Foundation: This platform is a dedicated CenturyLink cloud infrastructure based on VMware Cloud Foundation for secure, software defined virtualized hosting.

Disaster Recovery Plan: The Disaster Recovery Plan is a SafeHaven built-in plan which maps Primary Server to Recovery Server and defines the boot up and power off sequence of the servers within every Protection Group.

Distributed File System Replication (“DFSR”) is used by Microsoft as a multi-master replication engine that keeps folders synchronized on multiple servers. Global parameters and certain replicated folder-specific parameters are configured for DFSR using AD.

Failover: Failover switches the workloads from Supported Production Platform site to the Supported Recovery Platform site. SafeHaven Failover is Protection Group based so that applications and servers within the same group are consistent. SafeHaven Failover stops the WAN sync from primary site to recovery site and brings up the Recovery Servers based on the determined checkpoints. MDRS coordinates different CenturyLink teams to recover applications during Failover. Failover may also be related to the additional DR Replication Service.

Flexible Single Master Operation (“FSMO”): Specialized domain controller roles employed to prevent conflicts when making changes to AD objects.

Kerberos: Kerberos is a cross platform network authentication protocol. It is both open source and commercially supported. Microsoft Windows 2000 and later use Kerberos as its default authentication method. Joining a client to a Windows domain means enabling Kerberos as default protocol for authentications from that client to services in the Windows domain and all domains with trust relationships to that domain.

Local Cache: Local Cache is a type of Protection Group. A Local Cache Protection Group adopts a small amount of storage associated with the Supported Production Platform SRN acting as WAN sync cache to transmit data from Supported Production Platform to recovery environment.

Local Replica: Local Replica is a type of Protection Group. Local Replica Protection Group keeps a copy of Primary Server image on the primary SRN for WAN sync and recovery purposes.

Local Replication: Local Replication means copying data from Primary Server disks to Supported Production

Platform SRN disks.

Minor Release: Minor Releases (x.Y.z) are vehicles for delivering minor features developments, enhancements to existing features, and defect corrections. They incorporate all applicable error corrections made in prior Minor Releases.

New Technology File Replication Service (“NTFRS”) is used by Microsoft for the SYSVOL directory share. SYSVOL is a folder which resides on every domain controller and contains public files that need to be accessed by clients and kept synchronized between domain controllers.

Periodic DR Report: Periodic DR Report is sent to Customers via email to demonstrate the SafeHaven Cluster information, Protection Group status, WAN sync speed, RPO, and un-synced data. Customer obtains general idea of the DR solution through the Periodic DR Report.

Protection Group (PG): A Protection Group contains one or more application servers with a single recovery policy. It is recommended to group multiple interdependent servers into one Protection Group to keep the application consistency for Failover. A Protection Group is built between a pair of SafeHaven Replication Nodes.

Primary Server: A Primary Server bears Customer’s workloads. The Replication Agent is installed on the Primary Server to replicate data. Every Primary Server has a corresponding Recovery Server with same computing resources on the recovery environment. A Primary Server may also be referred to as a Supported Production Platform Server herein.

Recovery Point: SafeHaven Recovery Point is used to perform Test-Failover and Failover. It offers the ability to fail over a Protection Group to a specific time point. Recovery Point is used to determine the RPO.

Recovery Server: A Recovery Server is a stand-by server of the Primary Server. In the SafeHaven solution, Recovery Server is only powered on during Test-Failover or Failover.

Recovery Point Objective (RPO): Recovery Point Objective is the maximum targeted period in which data might be lost due to a major incident.

Replication Agent: Replication Agent is an agent installed on Windows Primary Servers to perform replication from Primary Server disks to Supported Production Platform SRN disks.

SafeHaven Cluster: SafeHaven Cluster is the fundamental infrastructure consisting of one SafeHaven CMS and multiple pairs of SRNs. Protection Groups reside under SafeHaven Cluster.

SafeHaven Console: SafeHaven Console is a user interface for managing SafeHaven solutions. It displays platforms, SafeHaven Replication Nodes, CMS and Protection Groups. A user can change the WAN sync speed, checkpoint interval, configure the periodical report and configure the built-in Disaster Recovery Plan via it. User also initiate the Test-Failover and Failover operations from it.

SafeHaven Replication Node (SRN): SafeHaven Replication Node is an Ubuntu server that controls Protection Group WAN sync, executes the Test-Failover and Failover commands.

Supported Production Platform means CenturyLink Cloud, Dedicated Cloud Compute, CenturyLink Private Cloud on VMware Cloud Foundation, Amazon Web Services EC2, Amazon Web Services Elastic Block Storage, Microsoft Azure virtual machines and disk storage or Customer-provided environments that utilize VMware virtualization.

Supported Recovery Platform means CenturyLink Cloud, Amazon Web Services EC2, Amazon Web Services Elastic Block Storage, Microsoft Azure virtual machines and disk storage.

Test-Failover: SafeHaven Test-Failover is a bubble test which isolates the Supported Production Platform’s Primary Servers from Recovery Servers to achieve zero-interruption on the Supported Production Platform.

WAN sync: WAN sync copies data from the Supported Production Platform SRN to the Supported Recovery Platform SRN.