DIGITAL SENSE
An OvertheWire Company

SIMPLIFY TODAY. READY TOMORROW.

SERVICE DESCRIPTION

DSPROTECT AVAILABILITY

Version: 2.01
Date: July 2021
Status: Released

Prepared by:

Dan Frith
Head of Technology

Level 8, 300 Ann Street
Brisbane, QLD, 4000

1300 799 908
digitalsense.com.au

CONTENTS

TABLES

DOCUMENT RECORD

Document Information
Author: Dan Frith
Status: Released
Version: 2.01
Date Created: 2020.07.20
Date Issued: 2021.07.20
Location: DSProtect_Availability_ServiceDescription_v2.01.docx
ServiceNow:

Table 1 - Document Record

REVISION HISTORY

Revision Number	Author	Issue Purpose	Date
2.00	Dan Frith	Document creation	2021.06.01
2.01	Dan Frith	Minor updates	2021.07.20

Table 2 - Revision History

RELEASE APPROVAL

This document is approved for release.

Version:

Name:

Position: , Digital Sense

Signature:

Date:

1. INTRODUCTION

The Digital Sense DSProtect Availability service provides complete protection for virtual machine workloads that are located within the Digital Sense Cloud or located on-premises, in private clouds and off-site. The DSProtect Availability service can provide a fully replicated environment at one or many Digital Sense Availability Zones.

2. SERVICE DETAILS

The DSProtect Availability service provides several disaster recovery options for virtual machines running on a customer premises or within DSCloud. The service is fully managed and requires little to no customer interaction during business-as-usual activities. Where a recovery operation is required, customers can choose their involvement from full management of the disaster recovery operation through to a hands-off approach where Digital Sense manages all aspects of the recovery effort.

The details of the service are covered in the following sections.

2.1 TECHNICAL ARCHITECTURE

The DSProtect Availability solution leverages the Zerto software application and is a hypervisor-based replication technology. Software agents are used to facilitate the replication and protection activities and these agents are installed on the VMware vSphere or Microsoft Hyper-V hosts. Each host that will replicate a virtual machine will require the agent installed. The agent installation is performed during the Service Initiation phase.

Protection is only available for running virtual machines and is based on constant block level replication with no scheduling and has no performance impact on the protect virtual machines. Other features include:

- Protection Group based where virtual machines are added to a grouping for recovery;
- One to many simultaneous replication – see Replication Type 3 below;
- Cross hypervisor replication;
- Support for VMware vMotion and VMware Storage vMotion;
- Compression algorithms used for replication process to efficiently utilise network connections;
- Enables bandwidth throttling and Quality of Service (QoS);
- Uses dynamic and compressed journaling. The journal (period available for rollback) can be custom defined but is configured for 4 hours by default; and
- Allows automatic protection of new virtual machines created after initial configuration.

At each site (primary and secondary, or multiple secondary sites) a Virtual Replication Appliance (VRA) is required. This is based on an architecture of one VRA per hypervisor host using a single vCPU, 4GB RAM and 12GB of disk based virtual machine. Each VRA also requires a single IP address for continuous virtual machine block-level replication. Where a customer has a dedicated Digital Sense DSCloud service, the VRA consumption will be charged based on the standard DSCloud fees.

2.2 REPLICATION TYPES

Digital Sense offers a range of different replication options to protect virtual machines and enable simple and effective recovery in the event of a range disaster scenarios, from complete site loss through to single virtual machine protection.

2.2.1 DSCloud – DSCloud

For customers using the DSCloud service, providing a Disaster Recovery environment is a straightforward process. Virtual machines can be replicated from the current Availability Zone (AZ) to a secondary Digital Sense AZ. This approach has the shortest lead time and can be established without any downtime or disruption to the DSCloud tenancy.

This replication type requires no customer network connectivity requirements as the replication takes place over the Digital Sense Data Centre Grid and the connectivity is included within the service. Customers using DSCloud will typically have a Digital Sense DSConnect connection to the AZ and may consider a secondary connection to the replication target AZ.

2.2.2 Customer Site Private Cloud – DSCloud

Customers with an on-premises virtualised environment can replicate their virtual machines (using Zerto) to one of the DSCloud AZs. A network connection from the customer site to the AZ is required and it is recommended that a DSConnect service be used for this connection. However, a customer can also connect via a customer provisioned link or over the internet using a VPN.

In this configuration, Digital Sense will install agents within the customer's Microsoft Hyper-V or VMware vSphere host environment. This is a process that requires administrative access to the Host Servers and is a software only solution. The process typically takes minutes and has no effect on running virtual machines or virtual machine operations.

2.2.3 Customer Site Private Cloud – Multiple DSCloud Availability Zones

Customers with an on-premises virtualised environment can also replicate their virtual machines to multiple DSCloud AZs. This approach may be used to replicate virtual machine Protection Groups to multiple AZs for specific disaster recovery purposes such as to provide multiple RPO scenarios.

A network connection from the customer site to the Digital Sense Data Centre Grid is required and it is recommended that a DSConnect service be used for this connection. This will allow a single network connection to access both AZs used for recovery. In this configuration, Digital Sense will need to install agents within the customer Microsoft Hyper-V or VMware vSphere host environment in the same manner as Replication Type 2.

2.2.4 DSCloud – Customer Site Private Cloud

Where a customer has virtual machines deployed within DSCloud and still maintains an on-premises virtualised environment, the on-premises solution can be used as a recovery option for replication and disaster recovery. Using the opposite approach to Replication Type 2, virtual machines can be replicated back into the customer virtualised data centre.

A network connection from the customer site to the Digital Sense AZ is required and it is recommended that a DSConnect service be used for this connection. In this configuration, Digital Sense will need to install agents within the customer Microsoft Hyper-V or VMware vSphere host environment in the same manner as connection type 2.

Replication is provided as a crash-consistent replication service. Where operating system and application support exist, an application-consistent replication may also be achieved. This will require interaction within the virtual machine by way of software agent and / or scripts and may incur additional service management fees.

2.3 VIRTUAL MACHINE RECOVERY

During a recovery operation, Protection Groups are used as a basis for recovery. Recovery can be of complete site(s), applications or virtual machines.

During the Service Initiation phase, Protection Groups are defined and can consist of one or more virtual machines. A typical grouping could be based on an application such as a database server, application server and a collection of web servers. By arranging virtual machines into Protection Groups, the configuration of start / boot order and other dependencies can be allowed for to ensure any failover occurs consistently and in an order that ensures applications return to normal operation without incident.

Other features of the virtual machine recovery include:

- Recovery possible to thousands of points in time within the Journal default of four hours;
- Cross-hypervisor virtual machine conversion;
- Orchestrated and automated failover during a defined disaster recovery event;
- No snapshots on the recovery virtual machine;
- Failback with reverse protection to ensure a DR reversal can be implemented successfully;
- Ability to perform non-disruptive failover testing;
- Automatic re-IP addressing and re-MAC addressing of virtual machines to provide transparency during a failover; and
- Recovery reports can be generated for post incident reviews or compliance.

2.4 MIGRATION OPPORTUNITIES

The DSProtect Availability service can be used as a migration approach for moving virtual machines into the DSCloud environment. By establishing the DSProtect Availability service, customers can replicate virtual machines to the DSCloud service and then perform a failover. Once the failover has occurred, the DSProtect Availability service can then continue as an ongoing service, replicating virtual machines back to the original customer site or to a Digital Sense secondary DSCloud AZ.

Note that Zerto may also be used to migrate between certain cloud hypervisors based on the hardware-agnostic nature of the platform.

2.5 DSCLOUD RESOURCES

Where a replication type utilises a Digital Sense facility, the fees associated with compute and disk storage will be an additional cost over and above the DSProtect Availability fees.

Disk storage at the Digital Sense Secondary AZ will be consumed from the DSCloud catalogue and any virtual machine resources used during a recovery operation will also be consumed from the DSCloud catalogue. To ensure that any recovery operation can be initiated at any time, all compute resources within the DSCloud environment must be Reserved.

For Replication Type 4, when replication is from Digital Sense DSCloud to a customer site Private Cloud, there must be sufficient compute resources reserved to allow a recovery operation to be performed at any time.

2.6 DATA CENTRE PRESENCE

The DSProtect Availability service uses the DSCloud platform as the destination for replication protection. Therefore, any AZ equipped with DSCloud is a suitable replication point. A customer site may also be a replication point where virtual machines located within the DSCloud service are being replicated back to the customer site.

Replication Destinations - Data Centres
Digital Sense, Kenmore, QLD
NEXTDC B1, QLD
Polaris, QLD
Customer Data Centre

Table 3 - DSProtect Availability – Supported Replication Destinations

3. SERVICE INITIATION

Providing a disaster recovery strategy and protecting virtual machines from the effects of a disaster event is a complex activity and requires a full understanding of the disaster recovery strategy and the virtual machines that are to be protected. The DSProtect Availability service is based on a standard design methodology, however certain aspects of the service are tailored to match the customer's environment. The DSProtect Availability service should be incorporated into an organisation's overall disaster recovery and business continuity strategy.

A Service Initiation phase is used to gather data and tailor the Digital Sense solution to match a customer's exact virtual machine protection requirements. The Service Initiation phase includes a design workshop and planning session with a detailed virtual machine protection document developed. Implementation of the service uses the design document and the Digital Sense Transition Methodology to ensure that the transition of the service is executed successfully.

The Service Initiation and Transition Phase include:

- Reviewing existing virtual machine protection regimes, policies and any applications or systems providing existing virtual machine protection;
- Defining the scope of the virtual machine replication including all systems to protect and systems excluded;
- Reviewing the RTO, RPO and replication requirements and if required modify the standard design to suit;
- Installing all components of the solution within the customer Hypervisor environment;
- Installing the Virtual Replication Appliances (VRA) within the primary and secondary guest environments;

- Ensuring application sociability of the DSProtect Availability Replication components with existing backup or replication software and determine solution;
- Designing of the replication solution, including Protection Groups, replication throttling, and journal retention period based on Digital Sense standard replication principles;
- Planning the timing and implementation of the service in line with the transition methodology;
- Presenting a transition plan for customer approval; and
- Implementing the transition plan and design.

A customer's existing disaster recovery environment may use one or many solutions to achieve the virtual machine protection requirements of the business and may use a variety of products or services from different vendors. Therefore, the cost of the service initiation could vary from the standard costs shown in the fees section of this service description depending on the complexity of the migration and transition.

For example, the installation of VRAs may require a significant amount of effort depending on the number of hosts supported. Therefore, the fees for service initiation may require additional effort and will be detailed in the transition plan developed.

4. SERVICE RESPONSIBILITIES

From Services Initiation through to daily operations, there are many roles and responsibilities to ensure the service outcome is achieved. Whilst this is a fully managed service and Digital Sense will take responsibility for the success of the service, there are requirements from both a Digital Sense and customer perspective.

Service Description	DS	Customer
Provide a fully managed DSProtect Availability service including ensuring the service is 'ever-green' (patching, software updates, hardware maintenance, firmware updates, security updates, hardware refresh etc.)	✓	
All licensing requirements for the software (Zerto) used to provide the DSProtect Availability service.	✓	
Deploy Virtual Replication Appliance (VRA) virtual machine and install hypervisor host agents within customer environment where required.	✓	
Provide administrative access to Hypervisor environment for VRA and agent installation.		✓
Provide remote access and elevated security accounts for VRA and agent management, operation, maintenance and customer environment support.		✓
Manage VRA virtual machine and agents within customer environment (patch and update etc.).	✓	
Ensure reserved compute resources at customer data centre are maintained (Replication Type 4).		✓
Ensure sufficient disk space is available at customer site for ongoing replication operations (Replication Type 4)		✓

Ensure reserved compute resources at Digital Sense AZ are maintained (Replication Type 1,2 and 3).	✓	
Ensure sufficient disk space is available at Digital Sense AZ for ongoing replication operations (Replication Types 1,2 and 3).	✓	
In a Private or Dedicated cloud model pay additional fees for reserved compute. In all deployment models pay for disk storage at Digital Sense DSCloud AZs.		✓
Maintain an adequate network connection for replication. Size must be the minimum recommended by Digital Sense at Service Initiation and as recommended at each Service Management Meeting.[1]		✓
Develop initial replication policies, RPO / RTO targets, Protection Groups and DSProtect Availability configurations.	✓	✓
Maintain and manage ongoing replication configuration and Protection Group membership/policies.	✓	
Approve changes to replication configuration and Protection Group membership/policies.		✓
Review replication configuration and Protection Group membership/policies at least quarterly.	✓	✓
Proactively monitor the DSProtect Availability replication environment to ensure replication is maintained and is within RTO and RPO requirements.	✓	
Ensure protected virtual machine at primary site are in a 'running' state (powered off virtual machines cannot be protected).		✓
Provide remote technical assistance in the event of a failover event.	✓	
Provide Monthly Service Report detailed any service issues, major DR events, pending platform upgrades and upcoming DR testing	✓	
Provide access to DSProtect Availability software portal [2]	✓	
Provide visibility of replication environment and health.	✓	
Provide ability to perform test failovers.	✓	
Provide ability to perform live failovers.	✓	
Provide customer contact details for escalation, reporting and alerting.		✓
Provide Service Request catalogue items for DSProtect Availability replication services.	✓	
Submit Service Requests and report incidents via the Digital Sense online Service Management Portal (ServiceNow)		✓
Perform failover testing as detailed within submitted Service Request.	✓	
Implement Service Requests within SLA requirements.	✓	

Table 4 - Service Responsibilities

While the DSProtect Availability service is fully managed, some customers may wish to take on certain management responsibilities based within the on-premises hypervisor environment. This may include installation of Zerto software agents, VRA establishment and general administrative tasks. Where a customer chooses this approach, additional roles and responsibilities will be applicable to the customer to ensure currency of agents, VRA and other components within the on-premises hypervisor environment. Digital Sense may also review service levels where a customer takes responsibility for these management and administrative tasks.

[1] Link size may need to be changed over the period of the service to cater for changes in virtual machine replication volumes. Digital Sense recommend a DSConnect service with access to the Digital Sense Data Centre Grid be used.

[2] In a DSProtect Availability service, Role Based Access Controls are implemented to limit the ability to modify protection groups and service configuration.

4.1 SERVICE REQUESTS

Customers may request services from the standard DSProtect Availability service catalogue. Service requests are executed based on the standard Digital Sense operational services for Service Requests. The following table details the service catalogue items for the DSProtect Availability service. Note that a number of these services can also be performed by the customer via the DSProtect Availability Portal.

Service Request Description	Included Quantity	Fee per SR[3]
Add / remove Hypervisor Host (agent and VRA installation/removal) fee per host	None	$200.00
Create new VM Protection Group	6 / annum	$500.00
Modify existing VM Protection Group	6 / annum	$250.00
Remove existing VM Protection Group	Unlimited	N/A
Failover Test VM Protection Group to secondary AZ	2 / annum	$250.00
Ad-Hoc customer generated reports using portal	Unlimited	N/A
Ad-Hoc Digital Sense generated simple reports	6 / annum	$60.00
Ad-Hoc Digital Sense generated complex reports	None	POA
Portal Request – New User Account	5 / annum	$30.00
Portal Request – Modify User Account	5 / annum	$30.00
Portal Request – Delete User Account	unlimited	N/A
Portal Request – Reset Password	unlimited	N/A

Table 5 - Service Requests

4.2 OPERATIONAL SERVICES

Digital Sense provides operational services for each of its services as part of the Digital Sense Service Management practice. The operational services are based on the best practice ITIL service management principles. The following table provides an overview of the operational services included with the DSProtect Availability service.

Operational Service Description	Included
Incident Management	✓
Major Incident Management	✓
Problem Management	✓
Service Request Management	✓
Event Management	✓
Escalation Management	✓
Change and Release Management	✓
Configuration Management	✓
Knowledge Management	✓
Capacity Management	✓
Security Management	✓
Availability Management	✓
Service Level Management	✓

[3] The fee per Service Request in excess of the included quantity.

Continual Service Improvement	✓

Table 6 - Operational Services

A Service Delivery Manager (SDM) is assigned and is responsible for all service management aspects of the service including governance and reporting. The SDM will arrange periodic Service Management Meetings as part of the governance process. Please refer to the service descriptions for each of the operational services for further details and roles and responsibilities.

4.3 SERVICE SPECIFIC SLAS

Digital Sense provides a standard set of SLAs for Incident, Major Incident and Service Request management (and these apply to problem, change and release management in support of Incident management). These SLAs are based on Business Impact and Urgency, assigned a priority of 1-5 and are ITIL aligned. See the Standard Common SLA document for details on Incident and Service Request SLAs.

For the DSProtect Availability service, the table below details specific Service Levels that will apply to the DSProtect Availability service.

Service Level Agreement	**Target Value**
Recovery Point Objective (RPO)	1 Hour
Recovery Time Objective (RTO)	4 Hours

Table 7 - Service Level Agreements – RPO and RTO Targets

For this service, the table below details specific Service Levels that will apply to Service Requests. See the Standard Common SLA document for details on Service Request SLAs.

Service Level Agreement	**Response and Implementation Time**
Add additional Hypervisor Host (agent and VRA installation)	P3 – Medium Priority
All Protection Group and Replication Configuration moves, adds and changes	P3 – Medium Priority
Provide assistance during a DR event	P1 – Very High Priority
Test Failovers	P4 – Low Priority
Ad-Hoc Digital Sense generated reports	P3 – Medium Priority
Portal Request – User moves/add/change	P3 – Medium Priority
Portal Request – Reset Password	P1 – Very High Priority

Table 8 - Service Level Agreements - Service Requests

4.3.1 System Availability

The system availability target for DSProtect Availability is not specified as the service is outcome based. System availability will be managed to achieve the defined outcome and SLAs.

4.4 SERVICE SPECIFIC REPORTING

In addition to the standard reports provided as part of the operational services, the following table details the reports delivered that are specific to the DSProtect Availability service.

Service Specific Report	Delivery Mechanism	Frequency
Point-in-time current RPO achieved	Email	Service Request
DSProtect Availability Protection Groups overview	SMM	Quarterly
Failover Test Outcome	Email	Post Test
Post Disaster Recovery Overview	Email	Post DR Event

Table 9 - Service Specific Reporting

The Service Management Meeting (SMM) is held periodically to review all aspects of the service.

4.5 ONLINE PORTALS

The DSProtect Availability service provides several portals.

- **DSCloud Administration Portal** – For managing DSCloud components of the service;
- **DSProtect Availability Portal** – enabling customer-based reporting and administration. For Public and Private customers, this is via the Cloud Director tenancy. For Dedicated customers, this is via the Zerto Self-Service Portal;
- **Service Management Portal** – Incidents and Service Requests can be managed using the Digital Sense Service Management portal (ServiceNow). https://support.digitalsense.com.au

5. PRICING

The fees for the DSProtect Availability service are based on several factors:

- **Establishment Fee** – A fee for the Service Initiation including setup of Hypervisor agents and all configuration and administration services to commission the replication protection;
- **Virtual Machine Protection** – A fee for each protected virtual machine included in a replicated Protection Group; and

- **Base Service and Service Management Fee** – This is a base fee for the DSProtect Availability service including service management activities. This fee may be waived or adjusted depending on virtual machine protection volumes or customer specific service inclusions.

The following table details the pricing for the DSProtect Availability Service.

Pricing Category	Fee per Month	One off Fee
Zerto Managed Services Establishment (one to one DC)	N/A	$4,500.00[4]
Zerto Managed Services Establishment (one to many DC)	N/A	$4,500.00[5]
Virtual Machine Protection (fee per replicated VM)	$99.00	N/A
Failover Test[6]	N/A	$900.00
Technical assistance in the event of a DR failover or DR recovery[7]	N/A	Rate Card

Table 10 - DSProtect Availability Pricing

5.1 ADDITIONAL FEES

Additional charges will also be incurred for the replicated virtual machine reserved compute and disk storage usage at each DSCloud Availability Zone. Virtual machine resources will be consumed from the DSCloud Catalogue and resources must be reserved. Please see the Digital Sense DSCloud Service Description for more information and service catalogue-based pricing.

A suitable network connection will also be required, and the use of DSConnectis recommended. Please see the Digital Sense DSConnect Service Description for more information and service catalogue-based pricing.

All fees shown are exclusive of GST and are based on a minimum term of 12 months. Discounts may apply for longer terms. Minimum virtual machine volumes may also apply.

[4] Cost of the service initiation could vary from the standard cost depending on the complexity of the migration and transition.
[5] Cost of the service initiation could vary from the standard cost depending on the complexity of the migration and transition.
[6] The fee for a Failover Test includes failing over of a single protection group within business hours, with a maximum of 10 virtual machines. Multiple failover tests can be conducted simultaneously or sequentially, and each test will incur the fee. Tests performed outside business hours will attract additional charges.
[7] Assistance during the first 4 hours of any Disaster Recovery event is included in the DSProtect Availability Service at no charge. Rate Card fees apply after the first 4 hours.