SIMPLIFY TODAY. READY TOMORROW.

SERVICE DESCRIPTION

DSFILE

Version:	1.02
Date:	October 2021
Status:	Released

Prepared by:

Dan Frith
Product Lead

Level 8, 300 Ann Street
Brisbane, QLD, 4000

1300 799 908
digitalsense.com.au

CONTENTS

TABLES

FIGURES

DOCUMENT RECORD

Document Information
Author: Dan Frith
Status: Released
Version: 1.02
Date Created: 2020.07.20
Date Issued: 2021.10.25
Location: DSFile_ServiceDescription_v1.02.docx
ServiceNow:

Table 1 - Document Record

REVISION HISTORY

Revision Number	Author	Issue Purpose	Date
0.01	Michael Anderson	Document creation	2020.07.20
0.02	Dan Frith	Minor updates	2020.07.23
0.03	Dan Frith	Minor updates	2020.09.07
0.04	Jon Pannell	Review	2020.09.09
1.0	Jon Pannell	Created as 1.0 release	2020.09.09
1.01	Dan Frith	Add Vscan, new template	2021.07.20
1.02	Dan Frith	Minor updates	2021.10.25

Table 2 - Revision History

RELEASE APPROVAL

This document is approved for release.

Version:

Name:

Position: , Digital Sense

Signature:

Date:

1. INTRODUCTION

The DSFile solution delivers a large-scale, multi-site file storage platform. Key attributes of the platform include:

- On-demand, self-service storage provisioning;
- POSIX-compliant shared file storage;
- Broad network access;
- Platform (operating system and host) agnostic support;
- Secure multi-tenancy support;
- Elasticity and scalability;
- Support for automation and orchestration, including RESTful API access;
- Multiple performance tiers;
- Storage efficiency technologies;
- Custom reporting capabilities; and
- Built-in capacity and evergreen lifecycle management.

A key feature of the storage offering is that it does not require the user to have workloads hosted on the Digital Sense cloud platform.

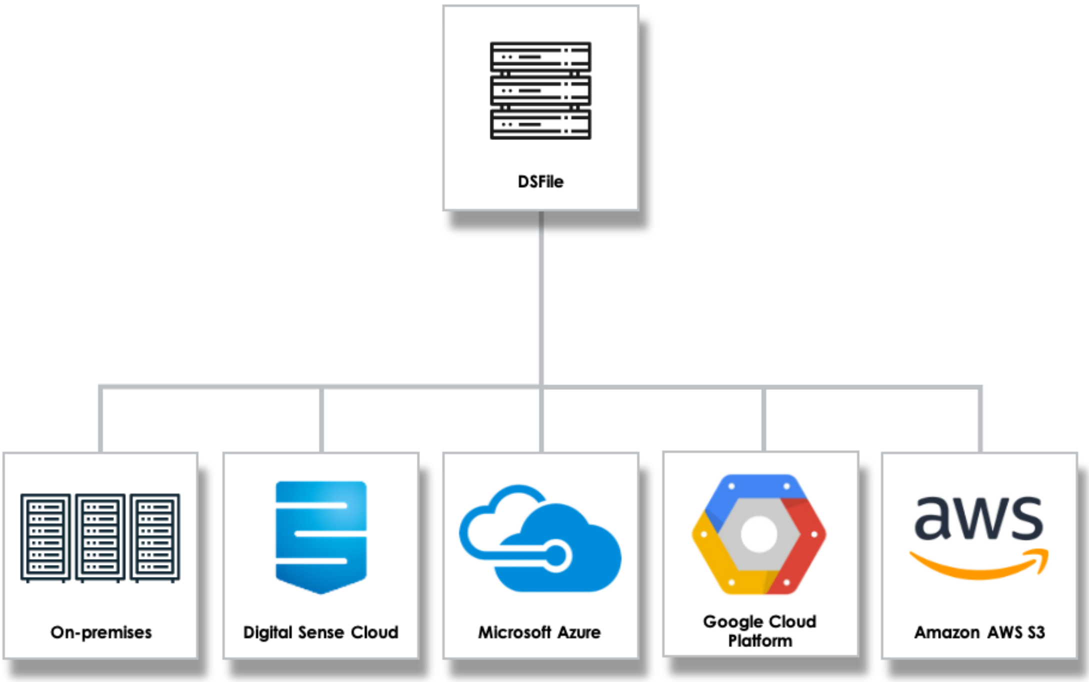

Figure 1 - DSFile - Logical Overview

1.1 PERFORMANCE TIERING

Four tiers of storage are offered to the customer via DSFile:

- Extreme;
- Performance;
- Value; and
- Archive

The key characteristics used to define the different storage tiers are primarily based on performance, including guaranteed IOPS and maximum latency levels. Each tier is designed to deliver a target IOPS per TB ratio.

- Extreme - target 4000 IOPS per TB ratio, 4ms latency, with minimum RPO of 30 mins
- Performance - target 1500 IOPS per TB ratio, 8ms latency, with minimum RPO of 30 mins
- Value - target 200 IOPS per TB ratio, 20ms latency, with minimum RPO of 4 hours
- Archive – No SLA

All of these IOPS targets assume a minimum 30% Random Read and 32K block size.

1.2 DSFILE DEDICATED

The DSFile Dedicated service offering delivers dedicated storage and associated infrastructure to clients. It can be hosted in a variety of locations, including:

- Customer on-premises / colocation;
- Customer remote offices; and
- Within Digital Sense data centres.

1.3 DSFILE SHARED

The DSFile Shared service offering delivers the same capabilities as the DSFile Dedicated solution but uses shared infrastructure to host client storage. Storage is connected to compute over IP, with support for a variety of network connection mechanisms.

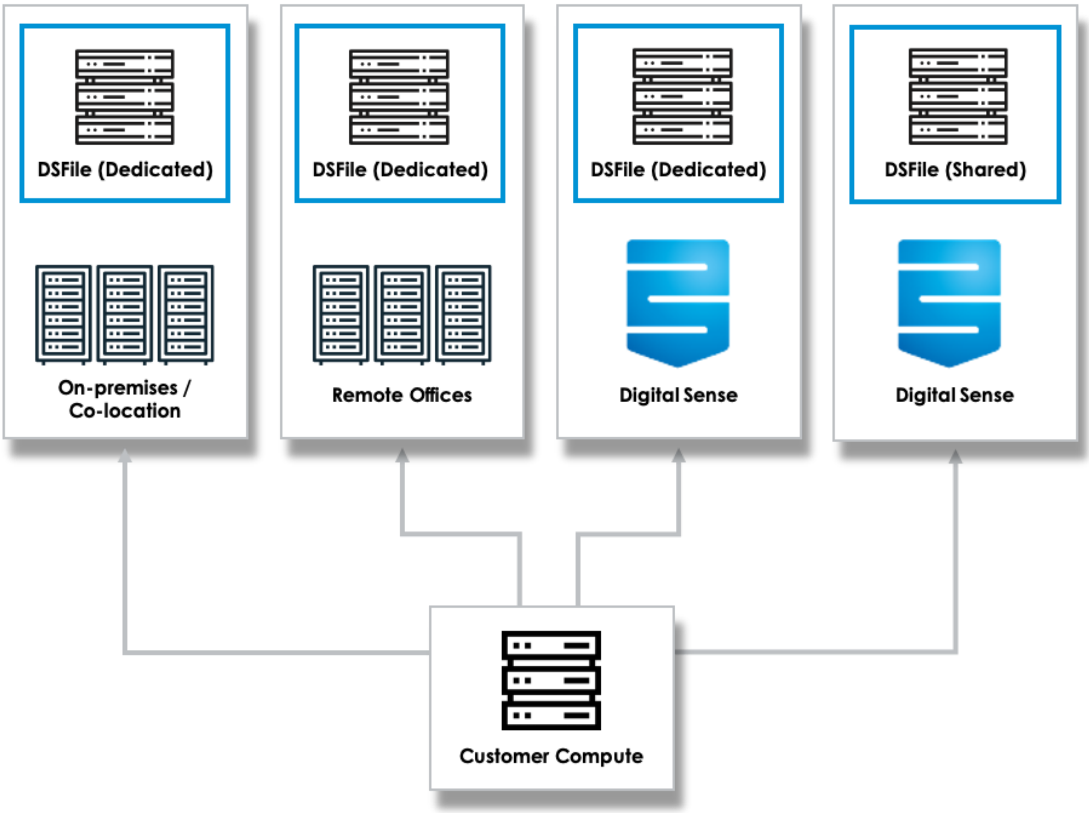

Figure 2 - DSFile Shared

1.4 DSFILE DR

DSFile DR provides the ability to protect dedicated customer storage via replication to DS hosted storage in a shared or dedicated fashion. The DSFile solution currently offers support for Digital Sense supplied file storage solutions. It is expected that third-party arrays (subject to Digital Sense validation) will be supported in future versions of the product. Further information on the supported replication technologies is provided in Section 1.8.2.

DSFile DR currently offers support for customer hosted storage (DSFile-compatible arrays only). It is anticipated that third-party arrays will be supported in a future release of the product.

The service stores protected data on the following environments:

- Customer hosted storage (secondary); and
- Digital Sense hosted (Dedicated or Shared).

1.5 AUDITING

DSFile auditing is a security measure that tracks and logs SMB and NFS events on selected volumes. Auditing enables administrators to track potential security weaknesses and provides evidence of security breaches.

The following events can be audited:

- SMB file and folder access;
- SMB logon and logoff;
- Central access policy staging; and
- NFS file and directory access.

Please be aware that requesting that auditing be enabled on volumes will affect the performance of the volume and may void SLA commitments.

1.6 ENCRYPTION KEY MANAGEMENT

Digital Sense's DSFile service encrypts all data, including snapshot copies, and metadata. Access to the data is via a unique XTS-AES-256 key, one per volume. An onboard key manager can be configured to serve keys to the storage nodes. An onboard key manager is a built-in tool that serves keys to nodes from the same storage system as the data. Keys are saved on the cluster to provide node and system failover protection to the keystore.

An additional backup of the storage encryption keys will be stored inside Digital Sense's double encrypted password management database.

1.7 ANTIVIRUS

In partnership with leading vendors' solutions, Digital Sense's DSFile storage devices support integrated antivirus functionality (Vscan) to protect business critical files. Vscan integration can detect and prevent the spread of malicious virus code on storage networks before your data is compromised.

Antivirus functionality integrated with the DSFile system supports off-box integration points with antivirus servers to help protect your business-critical data against known and unknown threats. Off-board servers use remote procedure calls and an authenticated SMB connection. Multiple servers can be configured to support one or more storage devices for redundancy and performance.

Please be aware that configuring antivirus for volumes will affect the apparent performance of the volume and may void SLA commitments.

The table below outlines the various responsibilities of the customer and Digital Sense with regards to the Vscan solution.

Service Description	DS	Customer
Provide a managed[1] DSFile Vscan 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 (Trend Micro ServerProtect) used to provide the DSFile Vscan service.	✓	
Vscan Components		
Configuration of Antivirus Server and Connector	✓	
Management of service account credentials	✓	
Addition of SVM to Antivirus Connector	✓	
Antivirus Engine		
Deployment of Trend Micro ServerProtect	✓	
Clustered Data ONTAP		
Configuration of Scanner Pool, Scanner Policy, On-Access Policies, and Vscan File-Operations Profile. (Digital Sense will be responsible for the configuration of the policy to meet customer requirements / expectations)	✓	✓
Access		
Provide administrative access to Tenant Active Directory environment to allow ONTAP / Vscan appliances to use the tenant's Active Directory for authentication.		✓
Provide remote access and elevated security accounts for Vscan management, operation, maintenance and customer environment support.		✓
Maintenance		
Manage Windows virtual machines and Trend Micro ServerProtect software within customer environment (patch and update etc.).	✓	
Ensure antivirus server signature updates are performed regularly (A weekly check that the updates are happening daily).	✓	
Ensure Vscan connection to Trend Micro environment is maintained	✓	
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.		✓
Provide remote technical assistance in the event of an antivirus event.	✓	
Provide Monthly Service Report detailed any service issues, major AV events, and pending platform upgrades.	✓	
Provide access to DSFile Vscan software portal [2]	✓	
Provide visibility of scanning pools and health.	✓	
Provide ability to perform manual scans.	✓	
Monitor reports / dashboards of DSFile Vscan results and determine if further action by the customer is required.	✓	✓
Provide customer contact details for escalation, reporting and alerting.		✓
Submit Service Requests and report incidents via the Digital Sense online Service Management Portal (ServiceNow)		✓
Implement Service Requests within SLA requirements.	✓	

[1] Note that it is the customer's responsibility to address any detected virus issues. Digital Sense will make reasonable efforts to assist where possible.

[2] In a DSFile Vscan service, Role Based Access Controls are implemented to limit the ability to modify scanning policies and service configuration.

Table 3 - Vscan Service Responsibilities

1.8 REPLICATION

1.8.1 Supported Replication Topologies

The solution supports multi-site replication to deliver high levels of availability and resiliency. Additionally, support for replication of file data to cloud services is part of the solution. A number of topologies are supported, including:

- On-premises to on-premises storage;
- On-premises to Digital Sense hosted (DSFile Dedicated);
- On-premises to Digital Sense hosted (DSFile Shared); and
- Digital Sense hosted to Digital Sense hosted (Shared or Dedicated).

It is anticipated that bi-directional replication and higher fan-in / fan-out ratios will be supported in later versions of the offering.

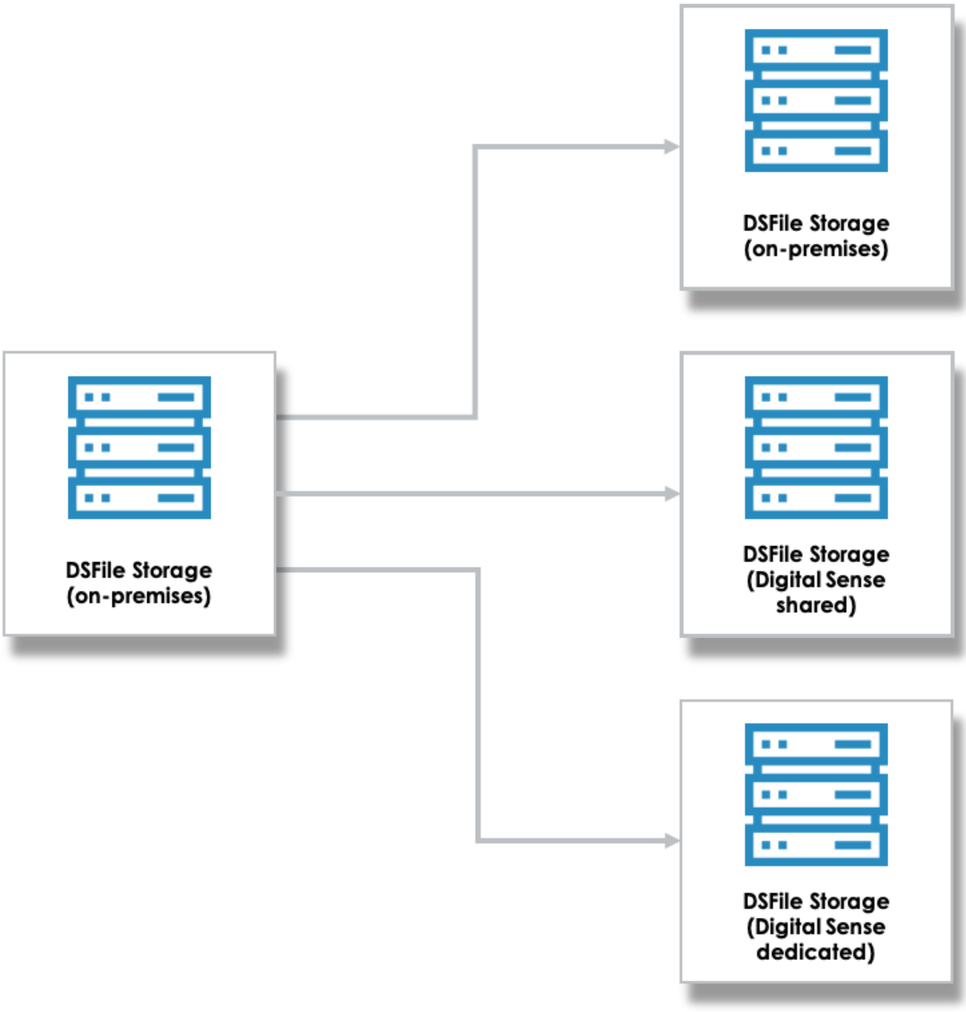

Figure 3 - Replication Topologies

Supported replication protocols are IP-based. Replication can be either synchronous or asynchronous, depending on the distance between sites and available bandwidth.

1.8.2 Replication Mechanisms

The product supports replication of data via either native or third-party replication tools, depending on the deployed storage infrastructure. For example, if a customer wants to replicate data from a non-Digital Sense supplied storage environment to a Digital Sense hosted DSFile environment, a third-party replication tool is required.

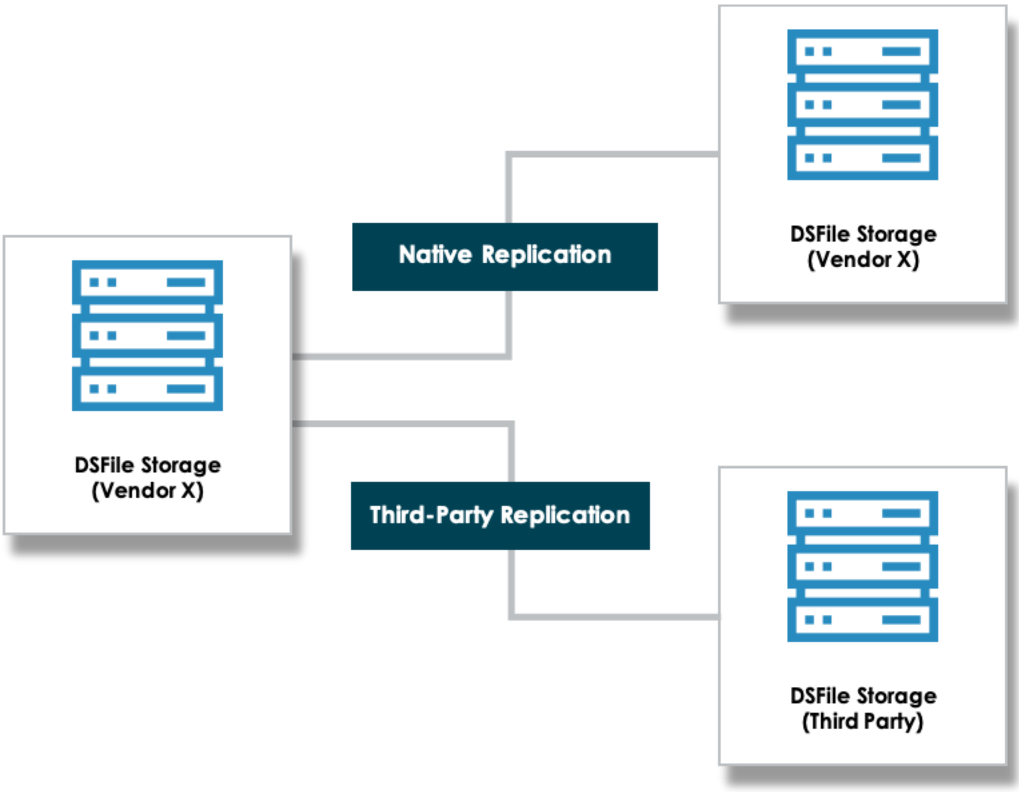
Native Replication
DSFile Storage (Vendor X)
DSFile Storage (Vendor X)
Third-Party Replication
DSFile Storage (Third Party)

Figure 4 - Native and Third-Party Replication

1.9 AUTHENTICATION

Authentication is the process of verifying the identity of an entity. Before users can create SMB connections to access data contained on the Storage Virtual Machine, they must be authenticated by the domain to which the SMB server belongs. The SMB server supports two authentication methods:

- Kerberos; and
- NTLM (NTLM v1 or v2).

The Kerberos protocol provides strong authentication within a client / server environment using a shared secret key cryptology system.

The SMB service on the storage controller must be able to communicate with the Active Directory domain controllers to properly manage file access control. Therefore, the Storage Virtual Machine LIFs must be configured to allow access to the Active Directory servers

2. SERVICE OPERATIONS

The below table outlines Digital Sense's roles and responsibilities in the delivery of the service offerings. While specific roles and responsibilities have also been identified as being owned by you, any roles or responsibilities not contained in this Service Description are either not provided with the service offering or are viewed to be your responsibility. Digital Sense's service level commitments are outlined below.

Service Description	DS	Customer
Facilities		
Provide and maintain sufficient data centre floor space	✓	
Provide and maintain sufficient power and cooling within the installation sites	✓	
Provision and maintenance of intra and inter-site network connectivity required to support data replication and remote management including DSFile storage platform and TCP/IP connectivity	✓	
Infrastructure Configuration		
Procurement of equipment	✓	
Physical installation of equipment	✓	
Supply / capacity increase and maintenance of network cabling required to support the environment including connectivity to Digital Sense or End Customer servers	✓	
Decommission of infrastructure	✓	
Removal of decommissioned hardware from Digital Sense sites	✓	
Installation and configuration of management software	✓	
Data erasure on hardware	✓	
Configuration of features of DSFile storage infrastructure	✓	
Enable features of DSFile storage infrastructure	✓	
Storage Management		
Create and provision storage for customers	✓	
Initiate DSFile service request		✓
Document and request DSFile storage connectivity as per agreed service request processes	✓	
Validate requests for connectivity	✓	
Testing and verification of provision of service from End Customer's systems	✓	✓
Provide hardware break / fix support – Digital Sense Provided Environment	✓	
Perform regular hardware and software maintenance planning – Digital Sense Provided Environment	✓	

Table 4 - Facilities, Infrastructure, and Storage Management

2.1 SUPPORT

The service offering includes support for reported problems as they relate to DSFile service availability.

Service Description	DS	Customer

Provide a fully managed object storage service including ensuring the service is "evergreen" (patching, software updates, hardware maintenance, firmware updates, security updates, hardware refresh etc.)	✓	
Develop initial network design (if DSFile storage is accessed via non-Internet methods)	✓	✓
Deploy hardware and assets on site where required	✓	
Provide suitable data centre facilities for onsite deployed hardware (including environmental aspects – rack space, power, UPS, cooling, and security etc.)		✓
Provide elevated security accounts for operation, maintenance and customer environment support as required		✓
Proactively monitor and resolve incidents within the DSFile storage environment	✓	
Forward automated events and alerts from proactive monitoring to customer[i]	✓	
Maintain and store audit logs	✓	
Provide object storage online user portals	✓	
Provide customer contact details for escalation		✓
Provide customer contact details for operational reports		✓
Provide customer contact details for alerting		✓

Table 5 - Support

2.2 TRANSITION ACTIVITIES

The DSFile solution is based on a standard configuration, however certain aspects of the services are tailored to match the customer's environment. For users of the DSFile solution, a brief Service Initiation phase is required to ensure that the appropriate connectivity is in place. The Service Initiation phase includes design workshops and planning sessions with a detailed design document developed (if required).

Implementation of the service uses the design document and the Digital Sense Transition Methodology to ensure that the transition of services is executed successfully.

The Service Initiation and Transition phase includes:

- Reviewing existing storage requirements;
- Understanding future storage requirements in terms of capacity and performance;
- Reviewing current security and encryption policies and aligning these with the standard Digital Sense design;
- Design of the connectivity solution;
- 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.

The cost of the service initiation could vary considerably depending on the complexity of the migration and transition. The cost of the service initiation will be based on the effort required for each implementation as detailed in the transition plan developed.

2.3 MONITORING

Digital Sense will provide the following monitoring services:

- Monitoring of the DSFile service at the physical, logical, and network layers and ensuring availability as per the agreed service levels.

You will be responsible for the following monitoring activities:

- Monitoring of customer-operated endpoints, applications, and networks to ensure access to the DSFile service is maintained.

Service Description	DS	Customer
Monitoring		
Configure the standard set of identified events, thresholds, and the required resources to be monitored for infrastructure services	✓	
DSFile storage and related network fabric monitoring	✓	
Maintain monitoring tools and agents	✓	
Monitor in scope infrastructure housekeeping routines	✓	
Log events and notifications, including resource affected, specific event type, and time of detection	✓	
Notify the appropriate contact when an incident has been detected in accordance with the notification procedures as defined in the incident and problem management section.	✓	
Respond to, and take appropriate action on alerts relating to the DSFile storage environment	✓	
Document and maintain procedures to be followed in the event of a storage alert event	✓	
Provide monthly DSFile storage usage reports	✓	

Table 6 - Monitoring

2.4 INCIDENT AND PROBLEM MANAGEMENT

Digital Sense will provide incident and problem management services aligned with ITIL recommended practices. These services include detection, classification, escalation, and resolution, and will be recorded in Digital Sense's IT Service Management Tool (ServiceNow). These incident and problem management services only relate to the provided service covering:

- DSFile platform availability, including software, hardware, and networks operated by Digital Sense to deliver the service.

You are responsible for the incident and problem management activities including detection, classification, escalation, and resolution relating to:

- Customer-operated platforms, applications, or services leveraging the DSFile service;
- Customer-operated endpoints (such as Internet browsers or web applications) that use the DSFile service; and
- Customer-operated networks that the abovementioned services use to access the DSFile service.

Service Description	**DS**	**Customer**
Incident Management		
Maintain Digital Sense Incident Management processes and policies	✓	
Incident creation in Service Desk Tracking System. Each time an authorised person contacts the Service Desk and provide a unique reference number for each case	✓	
Provide logs and route support for incidents and service requests according to the escalation process	✓	
Open incident tickets for genuine automated alerts	✓	
Assign incident priority to each incident	✓	
Perform incident notification according to the escalation management procedures	✓	
Evaluate incident impact to SLA	✓	
Resolve incidents, interface with third parties where required to assist in incident resolution	✓	
Close incidents upon confirmation of successful resolution	✓	
Problem Management		
Maintain customer Problem Management processes and policies		✓
Compile RCA post incident	✓	
Review and present RCA Findings	✓	
Review incident and RCA information	✓	
Identify problems, diagnose root causes and initiate actions to improve or correct the problem including interface with third parties as required to resolve problems	✓	
Adopt RFC process for Problem Management to link with change control	✓	
Periodic trending analysis of problems based on review of #, types and status	✓	
Report on problem management activity	✓	

Table 7 - Incident and Problem Management

2.5 CHANGE MANAGEMENT

The Digital Sense Change Management procedures are outlined in the following document:

- DS-OS0008 Service Operations - Change Management V0.2.docx

An overview of the change management processes is provided below.

Service Description	**DS**	**Customer**
Change Management		

Provide process and templates for requesting, approving, applying and recording changes	✓	
Apply agreed Change Management processes for all changes	✓	✓
Initiate change requests through change control process	✓	✓
Report change activity	✓	
Configuration Management		
Maintain customer Configuration Management processes and policies		✓
Develop / maintain technology architecture standards and best practices	✓	
Maintain Digital Sense Configuration Management system	✓	
Update Configuration management database on completion of change in line with customer configuration management process	✓	
Provide reports on configuration items and changes	✓	
Release Management		
Adopt a suitable process for ensuring new releases in the Controlled Environment are tested, verified as tested, version controlled and recorded in the Configuration Management database	✓	✓

Table 8 - Change, Configuration, and Release Management

2.6 SECURITY

The end-to-end security of the DSFile solution is shared between Digital Sense and you. Digital Sense will provide the security for the aspects of DSFile over which it has sole physical, logical and administrative level control. You are responsible for the aspects of the service over which you have administrative level access or control. The primary areas of responsibility between Digital Sense and you are detailed below.

Digital Sense will use commercially reasonable efforts to provide:

- Physical security of data centre locations hosting the DSFile infrastructure;
- Information security of the DSFile platform, including operating environment, account security, and security of supporting infrastructure;
- Network security of the DSFile platform, including network transit under the control of Digital Sense;
- Security monitoring of the DSFile platform, including intrusion detection and vulnerability prevention within Digital Sense operated networks; and
- Patching and vulnerability management of the DSFile platform, including regular security patching of platform vulnerabilities.

You are responsible for:

- Information security of all applications, endpoints, and services accessing the DSFile platform on your behalf;
- Network security of all applications, endpoints, and services accessing the DSFile platform; and
- Security Monitoring of all applications, endpoints, and services accessing the DSFile platform.

2.6.1 Compromised Infrastructure

Digital Sense reserves the right to suspend servers or any related elements or whole customer accounts if compromised servers are detected. This step is to ensure continued availability of the service and protect Digital Sense's infrastructure and business operations.

2.7 SERVICE METRICS

The monitoring and management solution will provide capacity and performance monitoring, system health statistics, real time alerts, and element management to ensure SLAs are adhered to.

The DSFile service will take advantage of LogicMonitor for capacity and performance monitoring, alerts and statistical analytics, including:

- Volume capacity warning and error alarms will be consumed by Digital Sense: The 'Volume Nearly Full' and 'Volume Full' thresholds will be configured as 70% and 80% respectively;
- Performance monitoring and incident root-cause analysis; and
- Identification of workloads that are impacting other volumes.

2.8 ENCRYPTION

The DSFile platforms employ a software-based technology for encrypting data at rest one volume at a time. An encryption key accessible only to the storage system ensures that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen.

When provisioned for the Customer all data (including snapshot copies) and metadata is encrypted. Access to the data is given by a unique XTS-AES-256 key, one per volume. An onboard key manager can be configured to serve keys to the storage nodes. An onboard key manager is a built-in tool that serves keys to nodes from the same storage system as the data. Keys are saved on the cluster to provide node and system failover protection to the keystore.

3. BUSINESS OPERATIONS

This section summarises processes for ordering, scaling, renewing, suspending, and terminating the service.

3.1 ORDERING AND INVOICING

Details of ordering and invoicing are included in the standard Digital Sense Master Services Agreement (MSA), available from your Digital Sense account representative.

3.2 RENEWAL

Digital Sense reserves the right to not renew any service offering at the end of its subscription term. If this is the case Digital Sense will notify you 30 days prior to the end of the subscription term.

3.2.1 Auto-Renewal

The service will be automatically renewed at the end of the subscription term unless you notify Digital Sense in writing 30 days prior to the end of the subscription term.

3.2.2 Modify Subscription Service at End of Term

The subscription service terms may be modified at the end of the contract term. Both parties must agree to any changes to the contract in writing 30 days prior to the end of the subscription term.

3.3 SUSPENSION AND RE-ENABLEMENT

In the event that an account is suspended for non-payment, or any other reason, Digital Sense will restrict access to all service components and block all traffic across its public IP addresses. Digital Sense will retain these service components with configurations and data intact until the issue is resolved or the subscription expires or is terminated.

Service re-enablement will be initiated immediately upon resolution of the account issues that led to the suspension. Public IP traffic blocks will also be removed.

3.4 TERMINATION

Upon termination of the contract, customer data will be retained on the DSFile storage platform for 30 days. It is the responsibility of the customer to work with Digital Sense to obtain a copy of the data (if required) prior to its removal from the service.

4. GLOSSARY

The following table provides a brief glossary of terms used in this document.

Term	Definition
AWS	Amazon Web Services. A public cloud service operated and sold by Amazon.
DA	Disaster Avoidance
DR	Disaster Recovery
LTR	Long Term Retention
NAS	Network Attached Storage
NFS	Network File System. A file protocol for accessing resources over a network.
RPO	Recovery Point Objective. Reflects the amount of data that potentially could be lost during a data loss event.
RO / BO	Remote Office / Branch Office. An office that is located in a different or remote geographical area to that of the company headquarters.
RTO	Recovery Time Objective. Refers to the amount of time it takes to recover from a data loss event and how long it takes to return to service.
SAN	Storage Area Network
SMB	Server Message Block. A file protocol for accessing resources over a network.
STR	Short Term Retention
VCD	VMware Cloud Director
VCF	VMware Cloud Foundation
VLAN	Virtual Logical Area Network
VM	Virtual Machine

Table 9 - Glossary