IT MODERNISATION RECOVERY INCREMENT 1

WP07 - SYSTEMS INTEGRATION AND CORE CAPABILITIES

ENTERPRISE CORE SERVICES (ECS)

SERVICE DESIGN PACKAGE

Effective date.....: 25-Apr-23
Version No .....: 1.1
Issued by.....: ITM Project Office
Approved by .....: Martin Diepstraten, POLARIS Technical Design Authority

Document Control

Title:	Service Design Package - Enterprise Core Services (ECS)
Version:	1.1 - DRAFT
Date:	25-Apr-23
Classification:	NATO UNCLASSIFIED
Filename:	NU-ITMRC1- Service Design Package (SDP) ECS
Storage location:	ITM-RC1 Portal

Table of Amendments

Version	Date	Description
0.1	31 May 22	NCI Agency initial update of SDP to align with architecture and new project scope.
0.2	02 Dec 22	Detailed updates to chapter 2, clean-up of all other chapters
0.3	16 Dec 22	QA Validation, adaptation to standard document and naming
1.0	20 Dec 22	Initial release for Checkpoint-1.
1.1	21 Apr 23	Update following change of Datacenter location (CR1) and some further small changes.

Stakeholder Details

Role	Name	Signature
Author	Marc Mengerink Marc.Mengerink@ncia.nato.int Senior Engineer, NCI Agency	Marc Mengerink Digitally signed by Marc Mengerink Date: 2023.04.25 10:14:56 +02'00'
Approver	Martin Diepstraten Martin.Diepstraten@ncia.nato.int POLARIS Technical Design Authority, NCI Agency	Martin Diepstraten Digitally signed by Martin Diepstraten Date: 2023.04.25 10:25:00 +02'00'

Contents

List of Figures

List of Tables

1. EXECUTIVE SUMMARY

0001 Enterprise Core Services (ECS), provided as part of the NATO Operational Network (ON), is providing core services to end users and systems up to and including the NS classification.

0002 ECS provides the foundation core services required for Infrastructure as as Service (IaaS), Client Provisioning Services (CPS), and Service Management and Control (SMC) Services.

0003 Additionally, ECS enables end users with authentication, email- and instant messaging, voice and video conferencing, file sharing and web portals for collaboration.

0004 The ECS implementation consists of the following key subcomponents**:**

A. Directory Services, based primarily on Microsoft Active Directory (AD) and Microsoft Identity Manager (MIM)
B. Email Messaging, based primarily on Microsoft Exchange
C. Unified Communications, based on Microsoft Skype for Business (SfB)
D. Portal Services, based on Microsoft SharePoint
E. Database Platform Services, based on Microsoft SQL and Oracle

0005 This document addresses the high-level service design and topology of each service, as well as low-level configuration detail, including component implementation and security measures. Service management, including tools, Standard Operating Procedures (SOPs), staffing requirements, and Key Performance Indicators (KPIs) are also addressed.

2. INTRODUCTION

0006 The goal of the ECS design is to detail how the ECS components are and will be implemented (technical design) and operated to provide ECS integrated with the private IaaS cloud infrastructure, Client Provisioning and Service Management tools supporting the NATO enterprise.

0007 ECS consists of 7 services which will be detailed further in the document:

A. Directory Services.
B. Email Messaging Services.
C. Unified Communications Services.
D. Portal Services.
E. Database Platform Services.
F. Core Services Cyber Security Services
G. Core Services Domain Service Management and Control (SMC)

2.1. Purpose and Scope

0008 This SDP includes information specific to ECS, including directory services, email messaging, unified communications, database- and portal services. This document details information pertinent to these solutions, including technical architecture and design, and service management and tools.

0009 The key ECS and related document dependencies are visualised in **Figure 1 – Architecture Design Products**, below.

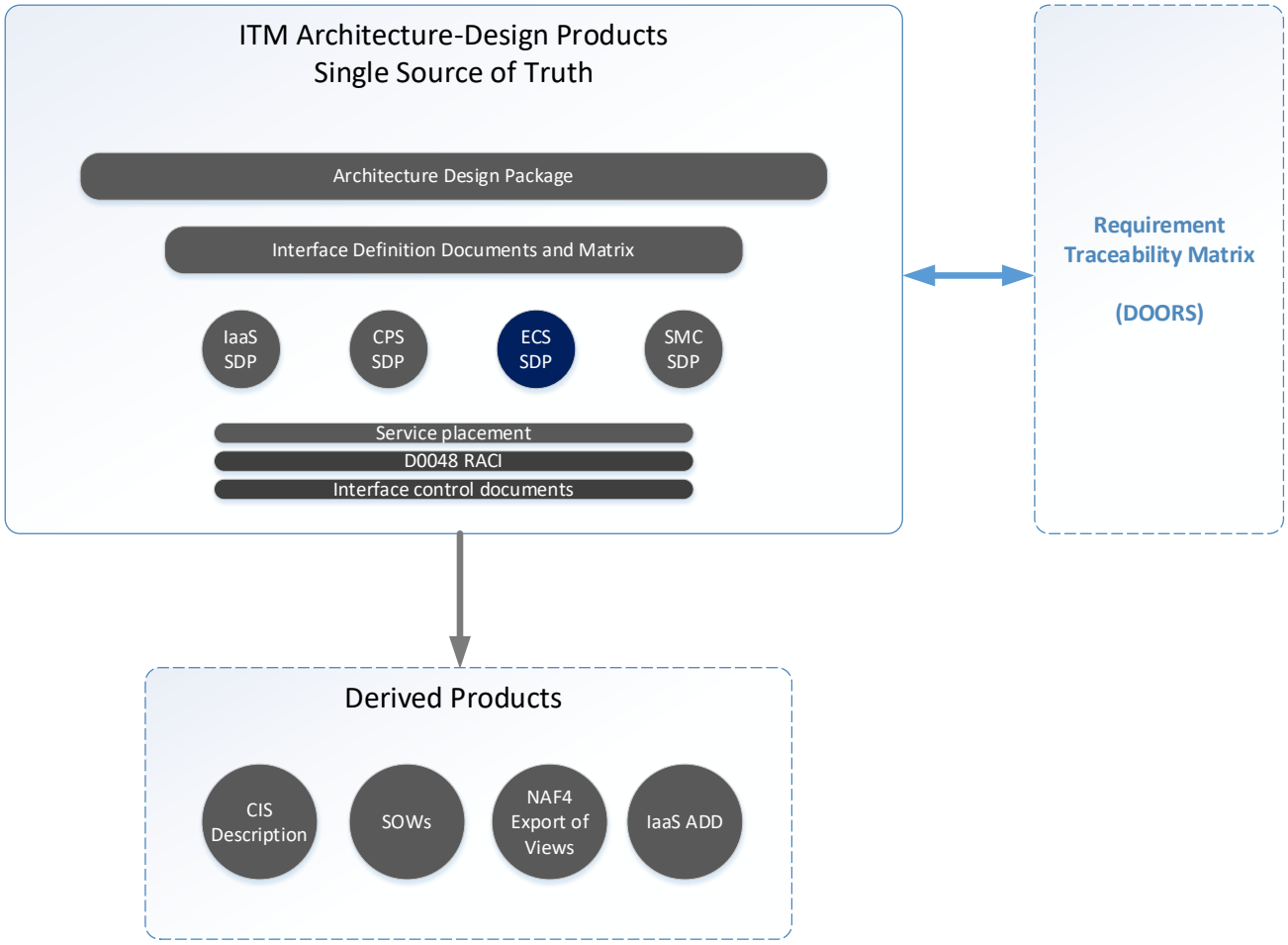

Figure 1 – Architecture Design Products

2.2. Document Organisation

0010 The organization of this SDP details ON Application Design in the following sections:

A. ***Section 3 Service Design and Topology*** – Describes service architecture and key service/subservice concepts;

B. ***Section 4 Service Solution*** – Describes the sub-service solution and component implementation design for hardware/software, security measures, and implementation design rationale for service levels;

C. ***Section 5 Service Management and Tools*** – Describes the detailed implementation for hardware/software component design of subservice area domain management and element management;

D. ***Section 6 Service Processes*** – Provides SOPs associated with ON processes for design;

E. ***Section 7 Service Organization Skill Level Requirements*** – Provides the level of manpower linked to skill levels;

F. ***Section 8 Service Measurement*** – Describes the mechanisms for collecting, analyzing and reporting required KPI information;

G. ***Annex A (Sub)services Interface Control Document (ICD)*** – Network communication provided for each service and subservice;

H. ***Annex B Component to ICD mapping table*** – Describes mapping of each hardware/software component (interface) to service interfaces that are identified either in Internal Subservices ICD, or the External Services ICD in the Architecture Design Document ICD annex;

I. ***Annex C NATO ON Procedures and Work Instructions*** – Provides procedures associated with ON processes related to the ON technical services groups (IaaS, CPS, ECS, SMC);

J. ***Annex D Operation Roles and Responsibilities*** – Provides manpower required to undertake ON operational and support tasks; and

K. ***Annex E Ports and Protocols Usage***. – Describes the ports and protocols used by each of the ECS services

L. ***Annex F Software to be used*** – Lists all software used by ECS.

M. ***Annex G ECS Site Scope*** – Provides a list of all sites within scope of ITM-RC 1 project, including the number of end users per site.

N. ***Annex H Data Classification Markings*** – Provides a list of the NATO Data Classification labels.

2.3. Points of Contact

0011 The ECS SDP is under the responsibility and maintained by ITM Engineering Team itm.engineering@ncia.nato.int .

0012 Changes to future design must be approved by Polaris Technical Design Authority (TDA).

POC	Role	Responsibility
itm.engineering@ncia.nato.int	Organizational Ownership	Shared Ownership of the SDP
POLARIStda@nr.ncia.nato.int	Polaris Technical Design authority	Approve the SDP

Table 1 PoC Information

2.4. Glossary

0013 The common abbreviations found throughout this document are listed in **Table 2**,below.The reader is also invited to refer to the ITM Glossary of Abbreviations (link) and the NATO Glossary of Abbreviations (link).

Acronym or Term	Definition
A/V	Antivirus
AV	Audio and Video
AD	Active Directory
ADBA	Active Directory-Based Activation
AD-DS	Active Directory-Directory Services
AD-FS	Active Directory Federation Services
AD-LDS	Active Directory Lightweight Directory Services
ADUC	Active Directory Users and Computers
AES	Advanced Encryption Standard
AG	Availability Groups
AIS	Automated Information System
API	Application Programming Interface
APP	Application
AuthN	Authentication
AuthZ	Authorisation
BPS	Boundary Protection Service
BiSC-AIS	Bi-Strategic Command Automated Information System
CA	Certificate Authority
CAS	Central Admin Server (SharePoint)
CNO	Cluster Name Object
COI	Community of Interest
CPS	Client Provisioning Services
CPU	Central Processing Unit
CRL	Certificate Revocation List
DAG	Database Availability Group
DB	Database
DBRR	Data Backup, Replication and Recovery
DC	Datacentre
DDI	DNS, DHCP, and IPAM
DDOS	Distributed Denial of Service
DFS	Distributed File System

Acronym or Term	Definition
DFS-R	Distributed File System Replication
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DML	Definitive Media Library
DMZF	DMZ Forest
DN	Distinguished Name
DNS	Domain Name System
DOORS	Dynamic Object-Oriented Requirements System
DR	Disaster Recovery
EAC	Exchange Administration Centre
ECS	Enterprise Core Services
EN	Enhanced Node
ePO	ePolicy Orchestrator
ESSO	Enterprise Single Sign-On
ESX	Elastic Sky X (Enterprise-class, type-1 hypervisor)
FAS	Functional Area Services
FSMO	Flexible Single Master Operations
FSW	File Share Witness
FTE	Full Time Equivalent
GAL	Global Address List
GB	Gigabyte
GC	Global Catalogue
GPMC	Group Policy Management Console
GPO	Group Policy Object
HA	High Availability
HDD	Hard Disk Drive
HLB	Hardware Load Balancing
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
IAAC	Identity & Authentication Access Control
IaaS	Infrastructure as a Service
ICD	Interface Control Document
IDAM	Identity And Access Management
IDF	Identity Forest
IDS	Intrusion Detection System

Acronym or Term	Definition
IIS	Internet Information Service
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IMAP/S	Secure Internet Message Access Protocol
IOPS	Input/Output Operations Per Second
ITSM	IT Service Management
IP	Internet Protocol
IPAM	IP Address Management
IPC	Information Protection Control
IPS	Intrusion Prevention System
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITM	IT Modernization
ITM-RC1	Information Technology Modernization Recovery - Increment 1
JBOD	Just a Bunch of Disks
KMS	Key Management Services
KPI	Key Performance Indicator
LAN	Local Area Network
LAPS	Local Administrator Password Solution
LDAP	Lightweight Directory Access Protocol
LDAP/S	Secure LDAP
LFF	Large Form Factor
LSA	Local Security Authority
MCDB	MetaCacheDataBase
MECM	Microsoft Endpoint Configuration Manager (formerly: SCCM System Center Configuration Manager)
MFA	Multi-Factor Authentication
MIM	Microsoft Identity Manager
MIME	Multipurpose Internet Mail Extensions
MS	Microsoft
NATO	North Atlantic Treaty Organisation
NCIRC	NATO Computer Incident Response Capability
NCSC	NATO Cyber Security Centre
NEDS	NATO Enterprise Directory Service
NPKI	NATO PKI
NR	NATO Restricted

Acronym or Term	Definition
NS	NATO Secret
NTP	Network Time Protocol
NU	NATO Unclassified
ON	Operational Network
OOS	Office Online Server
OU	Organisational Unit
OWA	Outlook Web App
PA	Preferred Architecture
PAM	Privileged Access Management
PBX	Private Branch Exchange
pCPU	Physical Central Processing Unit
PDC	Primary Domain Controller
PDP	Policies, Directives, guidance and Procedures
PFE	Purchaser furnished information, Equipment, Infrastructure and Services
PKI	Public Key Infrastructure
POC	Points Of Contact
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAC	Real Application Clusters (RAC)
RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
RFC	Request for Comments
RID	Relative Identifier
RN	Remote Node
RPO	Recovery Point Objective
RSSO	Remedy Single Sign On
RTO	Recovery Time Objective
SAML	Security Assertion Mark-up Language
SCOM	System Centre Operations Manager
SCP	Secure Copy Protocol
SDDC	Software Defined Datacentre
SDP	Service Design Package

Acronym or Term	Definition
SfB	Skype for Business
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SMB	Server Message Blocks
SMC	Service Management and Control
SMIME	Secure Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SMTPS	Secure SMTP
SN	Standard Node
SOC	Service Operations Centre
SOP	Standard Operating Procedure
SOW	Statement of Work
SP	SharePoint
SPBM	Storage Policy Based Management
SQL	Structured Query Language
SRM	Site Recovery Manager (VMware)
SRTP	Secure Real-time Transport Protocol
SSD	Solid State Drive
SSL	Secure Sockets Layer
SSMS	SQL server Management Studio
STS	Security Token Service
SVF	Service Forest
SfB	Skype for Business
TB	Terabyte
TBC	To Be Completed
TCAS	Titus Central Admin Server
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSOM	TrueSight Operations Management
TSCO	TrueSight Capacity Optimization
TSIM	TrueSight Infrastructure Management
TSO	TrueSight Orchestration
UC	Unified Communications
UCE	Unsolicited Commercial Email
UDP	User Datagram Protocol

Acronym or Term	Definition
ULS	Unified Logging System
UPN	Unified Principal Name
URL	Uniform Resource Locator
vCPU	Virtual Central Processing Unit
VDI	Virtual Desktop Infrastructure
VIP	Virtual IP
VM	Virtual Machine
VOIP	Voice Over IP
VRA	vRealize Automation
VTC	Video Teleconference
WAF	Web Application Firewall
WAL	Workflow Activity Library
WAP	Windows Application Proxy
WCF	Web Content Filter
WFE	Web Front End
WID	Windows Internal Database
WINS	Windows Internet Naming System
WNES	Windows Native Enrolment Servers
WSFC	Windows Server Failover Cluster
XML	Extensible Markup Language
XSS	Cross-Site Scripting

Table 2 - Glossary of Abbreviations

2.5. Reference Documents

0014 This SDP presumes the reader has ready access to all the reference documents listed in **Table 3 - References** below. These reference documents provide the necessary additional supporting details for the full contextual understanding of the interdependency information presented in this design document.

Document	Description
[NCIARECCEN-4-111258] Agency Standard Operating Procedure – SOP 06.03.01 – Operational Naming and Addressing of NATO ICT Infrastructure	Operational Naming and Addressing of NATO ICT Infrastructure
STANAG 1059 - (Edition 8)	Standardization Agreement – Letter Codes for Geographical Entities
AC/322-N(2017)0109 – Annex 1 NU_NATO_Enterprise_Naming_Directive	NATO Enterprise Naming Directive for ICT Services

Document	Description
Service Design Package – Client Provisioning Services (CPS)	Describes the NATO ON desktop delivery and management capabilities, application delivery, mobile device management, print, and scanning services, and wireless local-area network (LAN) connectivity for all NATO users.
Service Design Package – Infrastructure as a Service (IaaS)	Describes the NATO ON Infrastructure as a Service design.
Service Design Package – Service Management and Control (SMC)	Describes the NATO ON Enterprise SMC services and processes to monitoring and metering all NATO ON infrastructure and services
Service Placement	The Service placement details where the Service and sub-services are deployed in addition to detailing major dependencies with other services. The Service placement is complementary to the Service Design Package.
Data Map	Attribute mapping table defining the attribute data flow between NEDS and MIM.
Exchange Server Role Requirements Calculator	Calculator from Microsoft that helps calculating the required configurations according to input requirements provided. Current file: MS_Exchange ITM-R Incr1 V1.2

Table 3 - References

3. SERVICE DESIGN AND TOPOLOGY

0015 The ECS service consists of 7 subservices. **Figure 2 - ECS Full Service Model Architecture** depicts the current hierarchy and known characteristics.

3.1. Service Architecture/Model

0016 The ECS consists of the following key subcomponents**:**

A. Directory Services, based on Microsoft Active Directory (AD)
B. Email Messaging, based on Microsoft Exchange
C. Unified Communication Services, based on Microsoft Skype for Business
D. Portal Services, based on Microsoft SharePoint
E. Database Platform Services, based on Microsoft SQL
F. Core Services Cyber Security Services
G. Core Services Domain SMC Services

0017 All ECS services integrate with the other three ON core service areas, including:

A. IaaS, for all networking, storage, and virtualization requirements
B. SMC tools and equipment, for all management requirements
C. CPS, in support of access to user-facing ECS services

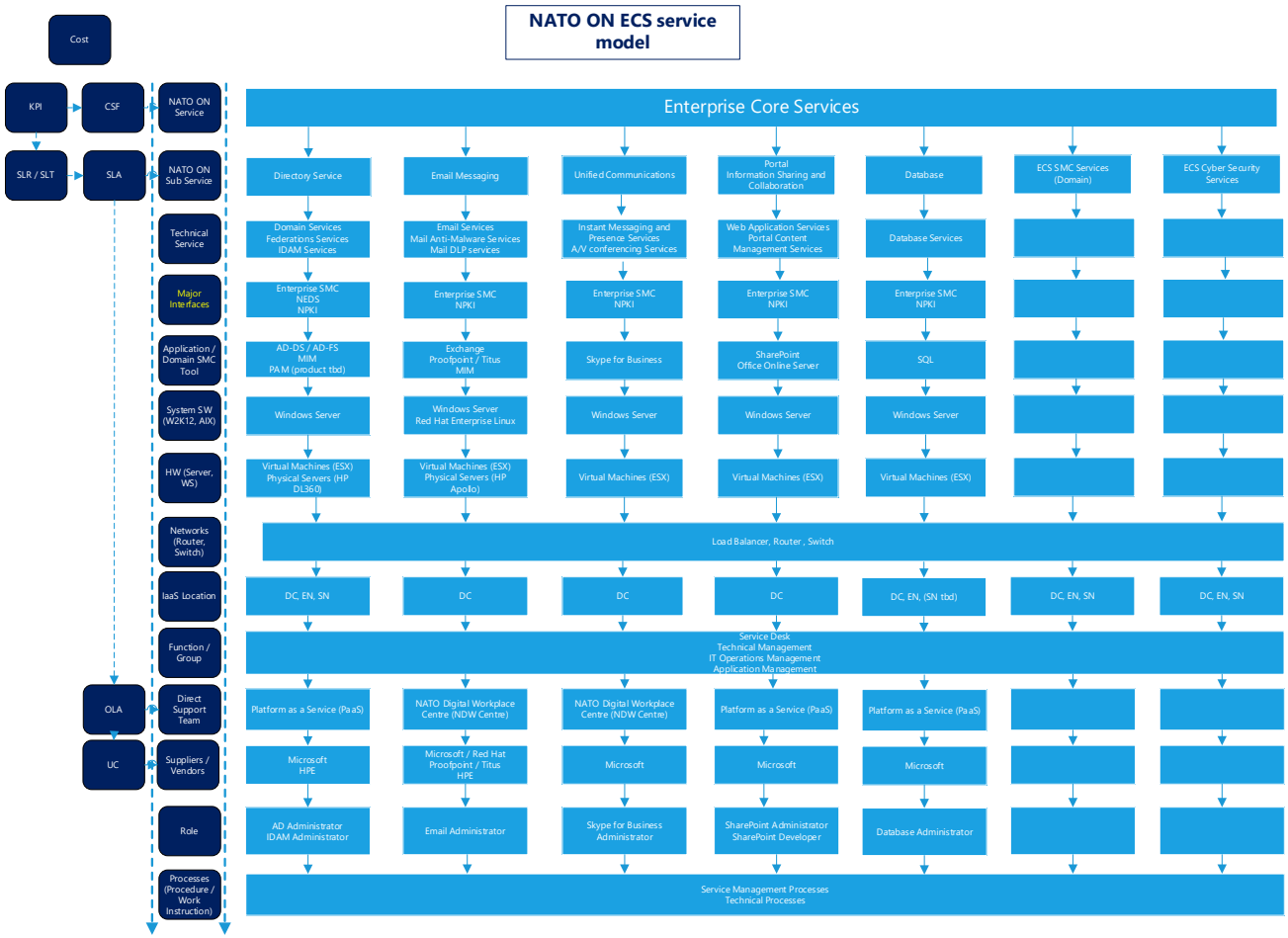

Figure 2 - ECS Full Service Model Architecture

0018 The subsequent sections outline the subservice topology and design of all components that make up ECS.

3.1.1. Directory Services

This section provides the concepts, high-level architecture and implementation strategy for the ECS Directory Service.

3.1.1.1. Concepts

0019 The Directory Services architecture is designed with the following core functional concepts in mind:

A. **Security.** Implementing a strict least privilege model, with audited separation of duties and satisfaction of key operational constraints, including:
   A.1. Using dedicated administrative accounts for systems administration tasks, not accounts used for daily interactive core business tasks. Lifecycle of these accounts are managed by the Identity and Access Management (IDAM) service as described in this design. Access Management for the administrative accounts is managed by the Privileged Access Management (PAM) service[1].
   A.2. Isolating administrative accounts from production user accounts, treating the forest as the security boundary
   A.3. Implement DNSSEC, enforcing authoritative zone data to be digitally signed,

B. **Availability.** Ensuring that all resources required to run the director services (Domain Controllers, Federation Servers, Identity Management Servers, and Distributed File Servers) are sufficiently sized and perform adequately, including requirements for local site independent operation for authentication and authorization.

C. **Scalability.** Ensuring the infrastructure can scale in response to increased application or user authentication and authorization demands.

D. **Recoverability.** Ensuring the deployed directory services environment is resilient and fully recoverable, within established limits, minimizing data loss.

E. **Compatibility.** Ensuring the directory services environment can support the full set of modern authentication and authorization protocols, including Kerberos, the Security Assertion Mark-up Language (SAML), and the Lightweight Directory Access Protocol (LDAP).

F. **Integrity.** Ensuring the data stored and offered by the directory service are accurate and unmodified.

G. **Integration.** The Directory Service integrates with other ON services as follows:
   G.1. The IaaS Service provides networking services, including LAN services, global and local load balancing, boundary protection, compute and storage services
   G.2. The CPS Service provides patching and end-point protection services.
   G.3. The SMC Service provides enterprise monitoring and logging services. The SMC service maintains the data required to perform historical trend analysis of health and capacity usage.

3.1.1.2. High Level Architecture

0020 The proposed directory services architecture includes the following key elements:

- Multiple AD Forests separating user/application services and management services.
- Microsoft Identity Manager (MIM) to manage the directory services environment, including object provisioning and data integrity enforcement, as well as synchronization of data from external sources, such as external directory services for address list provisioning and the NATO Enterprise Directory Service (NEDS).

[1] PAM is out of scope for the ECS design but is part of the D48 required security mechanisms. The PAM interfaces are identified at the IDD table.

- Identity federation services, based on Microsoft Windows Active Directory Federated Services (AD-FS), to support federation with external partners, and to support NPKI-based authentication and authorisation within each enclave.
- Distributed File System Replication (DFS-R) for namespace replication and high availability across the enterprise.
- Active Directory-integrated Network Time Protocol (NTP), Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS), to support network time synchronization, network name resolution and automated client IP address assignment. AD DNS integrates with the DDI Infoblox appliances for as root DNS services, IP Address Management (IPAM) and DHCP scope management as defined in the Service Design Package – Infrastructure as a Service (IaaS).
- AD-based license activation (ADBA), to support Microsoft Windows and Microsoft Office software activation.

3.1.1.2.1. Microsoft Active Directory

0021 ECS configures Microsoft Active Directory to support user authentication and authorization, as well support directory-integrated applications.

3.1.1.2.2. Forest and Domain Architecture

0022 ECS deploys or upgrades Active Directory forests on the Operational Network (ON), as follows:

3.1.1.2.3. Identity Forest (IDF) for user identities and functional application services

0023 The IDF identity and resource forest hosts user identities as well as functional application services. The first IDF forest will uplift the existing operational AIS (AIS.NATO.INT) forest. The AIS Forest consists of two domains, the primary NS AIS domain and one sub-domain named NEC CCIS. The NECCCIS sub-domain is providing directory services for the Northern European Command, Command and Control Information System (NEC CCIS).

3.1.1.2.4. Service Forest (SVF) for management of IaaS services

0024 The SVF service forest will separate the identity and resource forest with the management services required for the IaaS and SMC services. It will host all IaaS and SMC related services that can be consumed by the IDF. This is a new forest (NXXX.NATO.INT[2]).

3.1.1.2.5. DMZ Forest (DMZF) for demilitarized zone (DMZ)

0025 The DMZF is a dedicated forest for and hosted within the DMZ providing ON WAN connectivity (BPS-1 Security Zone). The DMZF provides directory services for applications requiring edge components in the DMZ that can be integrated in Windows Active Directory. The existing operational N0178 Forest will be used and uplifted for this purpose. (N0178.NATO.INT)

0026 The distribution of services between the forests is listed in the Service Placement documentation.

3.1.1.2.6. Forest Trusts

0027 A number of trust relationships are established in the ON environment to support authentication (AuthN) and authorization (AuthZ) requirements:

[2] DNS name to be provides ed according to [NCIARECCEN-4-111258] Agency Standard Operating Procedure – SOP 06.03.01 – Operational Naming and Addressing of NATO ICT Infrastructure

A. ECS establishes a two-way forest trust between SVF forests and IDF forest. This two-way trust is essential to ensure access to resources between these two forests.

B. ECS limits authentication across all external trusts by selective authentication,[3] using global security group membership, controlled by the IDAM service, as appropriate in each environment. This forest trust architecture is shown in **Figure 3 - NATO Forest Trust Architecture**. Note there are existing trust connection with external parties which will remain in place.

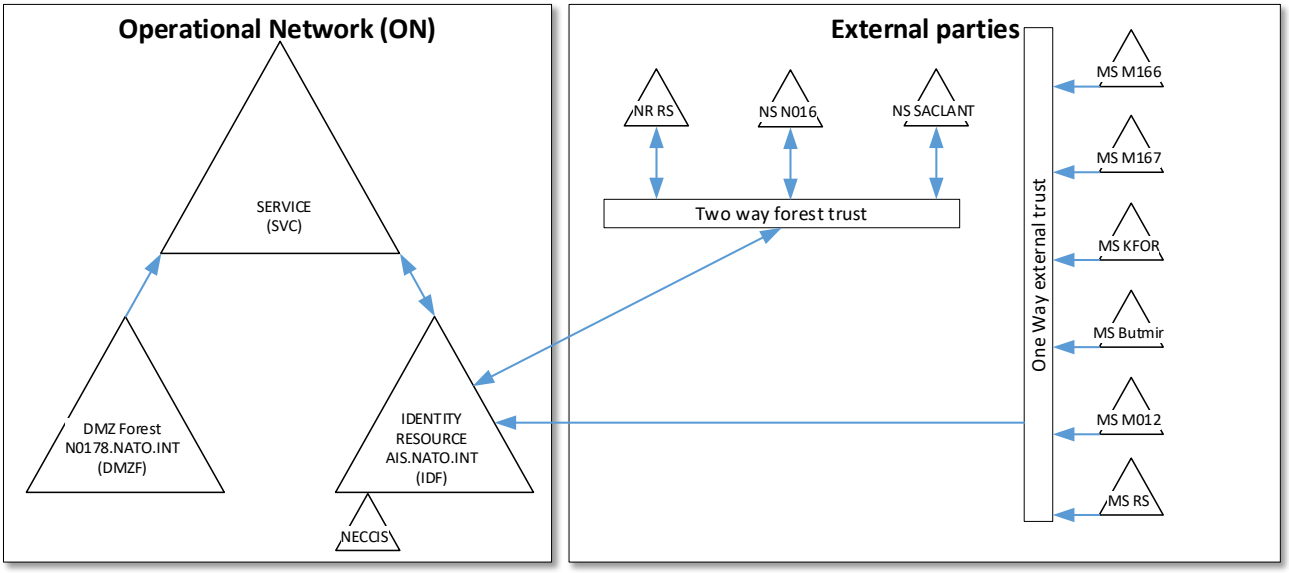

Figure 3 - NATO Forest Trust Architecture

3.1.1.2.7. Domain Controller Placement

0028 Domain Controllers will be placed at all Datacentre (DC) Node, Enhanced Node (EN) and Standard Node (SN) sites. These sites all have local infrastructure to provide core directory services in case of WAN links failure. Remote Nodes (RN) will not host any local infrastructure, with the exception of a campus LAN for clients to connect to. Remote nodes will not host any Domain Controllers.

0029 A single physical domain controller is assigned for each ON Windows Forest, at each datacentre. These physical domain controllers mitigate the risk of a virtualization environment failure. The physical domain controllers in datacentre BEL-BRU-01[4] shall host the domain-wide Flexible Single Master Operations (FSMO) roles for each domain in each forest (RID Master, Infrastructure Master and PDC Emulator) – with the rarely-used forest-wide FSMO roles (Domain Naming Master and Schema Master) moved to a virtual domain controller in BEL-BRU-01. The amount of domain controllers shall be sized according to Microsoft's recommendation defining a density of approximately 1000 users per domain controller core.[5]

0030 Additional virtualized domain controllers support directory service availability, and at each datacentre as needed to support user load at those locations. Each virtual domain controller is configured with 2 vCPU cores to support 2000 users. The physical domain controllers are configured with 1x 8 core pCPU.

0031 All RNs consume AD and DNS services from the DC nodes.

0032 Additional domain controllers deploy to current/future sites as user growth and subsequent deployment require. All domain controllers configure as Global Catalogue (GC) servers.

[3] https://technet.microsoft.com/en-us/library/cc794747(v=ws.10).aspx
[4] See ECS Site Scope for details on the Node ID's, user numbers and physical locations.
[5] https://social.technet.microsoft.com/wiki/contents/articles/14355.capacity-planning-for-active-directory-domain-services.aspx

3.1.1.2.8. Site Architecture

0033 An AD site is a collection of subnets serviced by one or more domain controllers. Each physical DC, EN and SN location is configured as a site in each AD domain. The ON architecture follows a hub/spoke model:

A. Datacentres configure to replicate in a circular fashion with each other, for the IDF, SVF and DMZF.
B. Each EN and SN site replicates with each DC to ensure replication redundancy for the IDF.

0034 As the scope of this project does not include all sites within the IDF, site links towards sites that are out-of-scope shall remain unchanged.

0035 Site link replication is a delta replication of changed domain information only. Site links between the datacentres replicate every 15 minutes; each node site link replicates with a datacentre every 30 minutes. Within a site, domain controllers replicate every 15 seconds for most domain data, and urgently and immediately for certain account information, including:

A. Assigning an account lockout, which a domain controller performs to prohibit a user from logging on after a certain number of failed attempts
B. Changing the account lockout policy
C. Changing the domain password policy
D. Changing a Local Security Authority (LSA) secret, which is a secure form in which private data are stored by the LSA (for example, the password for a trust relationship)
E. Changing the password on a domain controller computer account
F. Changing the relative identifier (RID) master role owner, which is the single domain controller in a domain that assigns relative identifiers to all domain controllers in that domain

0036 Site link costs ensure the primary replication source is favoured wherever possible, by tabulating a cost that is relative to the bandwidth and distance between a node and each datacentre, as shown in the following **Table 4 - AD Site Links**:

Domain	Node Type	Link	Site	DC	Ste Link Name	Cost	Replication (minutes)
IDF, SVF, DMZF	DC	Primary	BEL-BRU-01	ITA-LAG-01	BEL-BRU-01:ITA-LAG-01	50	15
IDF	EN	Primary	DEU-GEI-01	BEL-BRU-01	DEU-GEI-01:BEL-BRU-01	100	30
IDF	EN	Secondary	DEU-GEI-01	ITA-LAG-01	DEU-GEI-01:ITA-LAG-01	200	30
IDF	EN	Primary	DEU-RAM-01	BEL-BRU-01	DEU-RAM-01:BEL-BRU-01	100	30
IDF	EN	Secondary	DEU-RAM-01	ITA-LAG-01	DEU-RAM-01:ITA-LAG-01	200	30
IDF	SN	Primary	DEU-UED-01	BEL-BRU-01	DEU-UED-01:BEL-BRU-01	100	30
IDF	SN	Secondary	DEU-UED-01	ITA-LAG-01	DEU-UED-01:ITA-LAG-01	200	30
IDF	EN	Primary	DEU-ULM-01	BEL-BRU-01	DEU-ULM-01:BEL-BRU-01	100	30

Domain	Node Type	Link	Site	DC	Ste Link Name	Cost	Replication (minutes)
IDF	EN	Secondary	DEU-ULM-01	ITA-LAG-01	DEU-ULM-01:ITA-LAG-01	200	30
IDF	SN	Primary	DEU-WES-01	BEL-BRU-01	DEU-WES-01:BEL-BRU-01	100	30
IDF	SN	Secondary	DEU-WES-01	ITA-LAG-01	DEU-WES-01:ITA-LAG-01	200	30
IDF	SN	Primary	ESP-TOR-01	ITA-LAG-01	ESP-TOR-01:ITA-LAG-01	100	30
IDF	SN	Secondary	ESP-TOR-01	BEL-BRU-01	ESP-TOR-01:BEL-BRU-01	200	30
IDF	EN	Primary	GBR-NOR-01	BEL-BRU-01	GBR-NOR-01:BEL-BRU-01	100	30
IDF	EN	Secondary	GBR-NOR-01	ITA-LAG-01	GBR-NOR-01:ITA-LAG-01	200	30
IDF	SN	Primary	ITA-GRA-01	ITA-LAG-01	ITA-GRA-01:ITA-LAG-01	100	30
IDF	SN	Secondary	ITA-GRA-01	BEL-BRU-01	ITA-GRA-01:BEL-BRU-01	200	30
IDF	EN	Primary	ITA-LEN-01	ITA-LAG-01	ITA-LEN-01:ITA-LAG-01	100	30
IDF	EN	Secondary	ITA-LEN-01	BEL-BRU-01	ITA-LEN-01:BEL-BRU-01	200	30
IDF	SN	Primary	ITA-POG-01	ITA-LAG-01	ITA-POG-01:ITA-LAG-01	100	30
IDF	SN	Secondary	ITA-POG-01	BEL-BRU-01	ITA-POG-01:BEL-BRU-01	200	30
IDF	EN	Primary	NLD-BRU-01	BEL-BRU-01	NLD-BRU-01:BEL-BRU-01	100	30
IDF	EN	Secondary	NLD-BRU-01	ITA-LAG-01	NLD-BRU-01:ITA-LAG-01	200	30
IDF	EN	Primary	NOR-STA-01	BEL-BRU-01	NOR-STA-01:BEL-BRU-01	100	30
IDF	EN	Secondary	NOR-STA-01	ITA-LAG-01	NOR-STA-01:ITA-LAG-01	200	30
IDF	EN	Primary	POL-BYD-01	BEL-BRU-01	POL-BYD-01:BEL-BRU-01	100	30
IDF	EN	Secondary	POL-BYD-01	ITA-LAG-01	POL-BYD-01:ITA-LAG-01	200	30
IDF	SN	Primary	POL-BYD-02	BEL-BRU-01	POL-BYD-02:BEL-BRU-01	100	30
IDF	SN	Secondary	POL-BYD-02	ITA-LAG-01	POL-BYD-02:ITA-LAG-01	200	30
IDF	SN	Primary	PRT-LIS-01	ITA-LAG-01	PRT-LIS-01:ITA-LAG-01	100	30

Domain	Node Type	Link	Site	DC	Ste Link Name	Cost	Replication (minutes)
IDF	SN	Secondary	PRT-LIS-01	BEL-BRU-01	PRT-LIS-01:BEL-BRU-01	200	30
IDF	EN	Primary	TUR-IZM-01	BEL-BRU-01	TUR-IZM-01:BEL-BRU-01	100	30
IDF	EN	Secondary	TUR-IZM-01	ITA-LAG-01	TUR-IZM-01:ITA-LAG-01	200	30
IDF	EN	Primary	USA-NOR-01	BEL-BRU-01	USA-NOR-01:BEL-BRU-01	100	30
IDF	EN	Secondary	USA-NOR-01	ITA-LAG-01	USA-NOR-01:ITA-LAG-01	200	30

Table 4 - AD Site Links

0037 **Figure 4 - AD Site Replication** shows the overall AD site replication topology

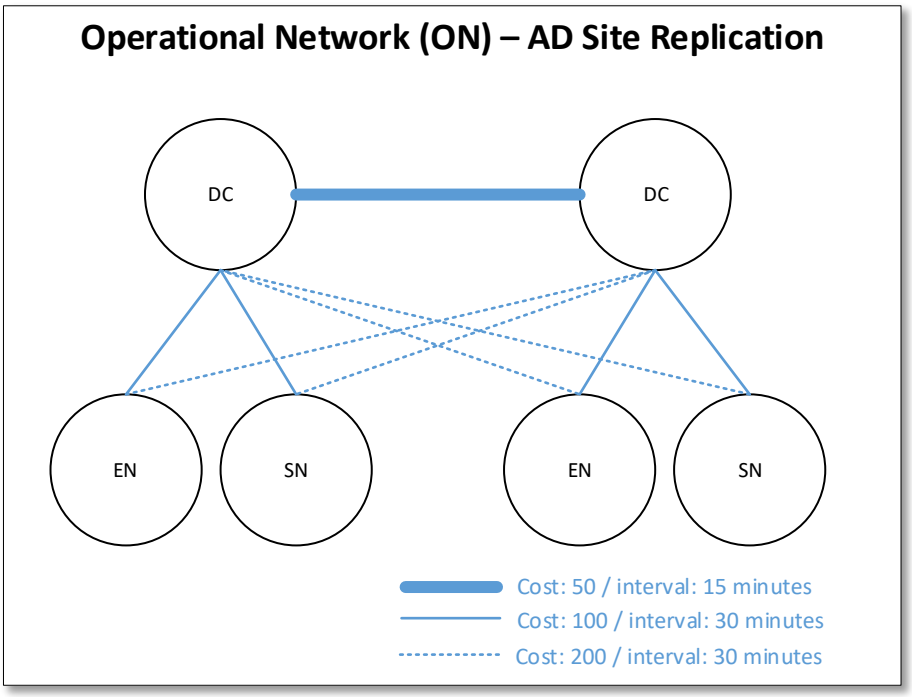

Figure 4 - AD Site Replication

3.1.1.2.9. OU Structure

0038 The defined organisational unit (OU) structure will be mirrored on each domain. The goal of the OU structure is to:

A. Simplify the OU structure to align to the operational support model, from a highly delegated and manual admin model to a centralized and automated admin model.

B. Ensure OUs are created as necessary to support the application of different Group Policy Objects (GPOs), implying a hierarchical structure based on object type and service.

0039 To ensure consistency and to simplify deployment and management, ECS deploys a similar OU structure on all domains (IDF/SVF/DMZF):

0040 The following top level OU's will be used:

A. NATO Accounts contain sub-OUs for external users, local users, test users and service accounts.

B. NATO Groups contain sub-OUs for legacy groups synched from trusted domains, groups managed by MIM, and groups unmanaged by MIM.

C. NATO Clients contain sub-OUs for each kind of domain-joined workstation in each environment (thin clients, thick clients, VDI clients, SOC workstations, etc.).

D. NATO Services contain sub-OUs for each ON service lane (CPS, ECS, IaaS and SMC). Each technology (Exchange, Skype, etc.) have resources provisioned under a dedicated sub-OU within the appropriate service lane.

0041 The initial proposed OU structure for the first 2 levels is shown in **Table 5 - Initial OU Structure** ci-dessous. Additional OU's for deeper levels will be created as required.

L1	L2	L..	Purpose
NATO Accounts			All user objects under this OU
	External		External (shadow) accounts
	Services		Service accounts managed by IDAM tool
	Users		User accounts managed by IDAM tool
	Disabled		User accounts managed by IDAM tool that are disabled. (expired or decommissioned)
	Staging		Used for migration
NATO Groups			All group objects under this OU
	Legacy		Legacy groups imported/synchronized from trusted domains
	Managed		Security groups managed by IDAM tool
	Unmanaged		Security groups not managed by IDAM tool
	Staging		Used for migration
NATO Clients			All domain joined client hardware under this OU
	Thick		All thick client workstations
	Thin		All thin client devices (not sure whether they will be domain joined)
	VDI		All Virtual Desktops
NATO Services			
	CPS		All CPS related server objects: Print, Scan, Application Provisioning, LAN, Desktop Provisioning, SCOM, MDM, etc.
	ECS		All ECS related server objects: Identity, UC, Portal, Databases, File, etc.
	IAAS		All IaaS related server objects: Backup, Archive, Virtualisation, etc.
	SMC		All SMC related server objects: ITSM, Discovery, TSOM, TSCO, TSIM, TSO, Splunk, RSSO, etc.
	FAS		All Functional Area Services (FAS) related server objects: TOPFAS, DHS, MCCIS, JOCWATCH, etc.

Table 5 - Initial OU Structure

3.1.1.2.10. Group Policy Object (GPO) Structure

0042 The NCIRC technical centre (Cyber Security) provides the baseline of GPOs to be applied as a minimum, with additional delta GPOs created as needed to support application and system functionality specific to the domains. The Windows Server built-in Group Policy Manager will be used to manage the group policies in each domain. The GPO configuration observes the following best practices:

A. The number of GPOs processed affects system boot time and user logon time, and also complicates troubleshooting. The number of GPOs applied to a given machine or user limited wherever possible.

B. Loopback processing increases troubleshooting complexity and avoided wherever possible.

C. Any scripts called via GPO stored in the *SYSVOL* folder, and not stored in the policy itself.

D. To further limit troubleshooting and complexity, GPOs are applied at the domain and OU level (and not at sites, whenever possible), and are filtered using AD security groups and/or WMI targeting only as explicitly necessary.

3.1.1.2.11. PKI Services

0043 The NATO Public Key Infrastructure (PKI) service provides all certificates issued to the NATO Enterprise IT services.

A. Entrust Windows Native Enrolment servers (WNES) are deployed in each domain and in each availability zone order to allow for domain joined servers to automatically request PKI machine certificates (via GPO)

B. All the necessary certificate trust chains are added to all domain-joined system certificate stores via Group Policy.

C. Each windows domain will be configured to trust the NPKI certificate Root CA for authentication (to allow for users to authenticate based on PKI certificates).

C.1. This will require the windows UPNs to be made available to the PKI Registration authority system via NEDS.

D. Additional integration and SOPs are required to handle application/web server certificate and the use of SSL interception/Web application firewalls.

3.1.1.2.12. Microsoft Identity Manager (MIM)

0044 MIM simplifies and secures identity and access management (IDAM) with automated workflows, business rules, and easy integration with heterogeneous platforms across the datacentre and externally. Also, MIM manages directory object provisioning based on business policy, and implements workflow-driven provisioning through a single browser-based interface. In the NATO ON environment, MIM manages the directory service by:

A. Provisioning and managing all production mailbox-enabled user accounts in the IDF. Hereby maintaining authoritative control of the visual identity for all user accounts such as display name, email address, department, address, telephone etc.

B. Provisioning and managing all non-person entity accounts (service accounts) in the IDF, DMZ and SVF.

C. Provisioning and managing user accounts for testing purposes in the IDF, DMZ and SVF.

D. Provisioning and managing the membership of distribution lists in the IDF.

E. Enabling user accounts for Instant Messaging (IM) and presence usage in the IDF.

F. Provisioning and managing membership of security groups in the Identity, DMZ and Service Forests.

G. Provisioning and managing users personal file shares (home drive) and SharePoint MySite.

0045 MIM consumes input from the NEDS, which acts as a broker between various information sources (e.g. HR / Security Databases). At the same time MIM also provides information back via NEDS to these sources for which MIM / Active Directory is the authoritative source of that data (e.g. SMTP address, UPN Value). This data is required by those sources for example for the generation of smartcards. **Figure 5 - High Level IDAM workflow** depicts the high level overview of the systems involved and the information flow.

0046 Both NEDS and MIM will tweak some of the data to get it in the correct format to meet the standards for naming according to the naming policy (see section 3.1.1.2.27 Naming Conventions).

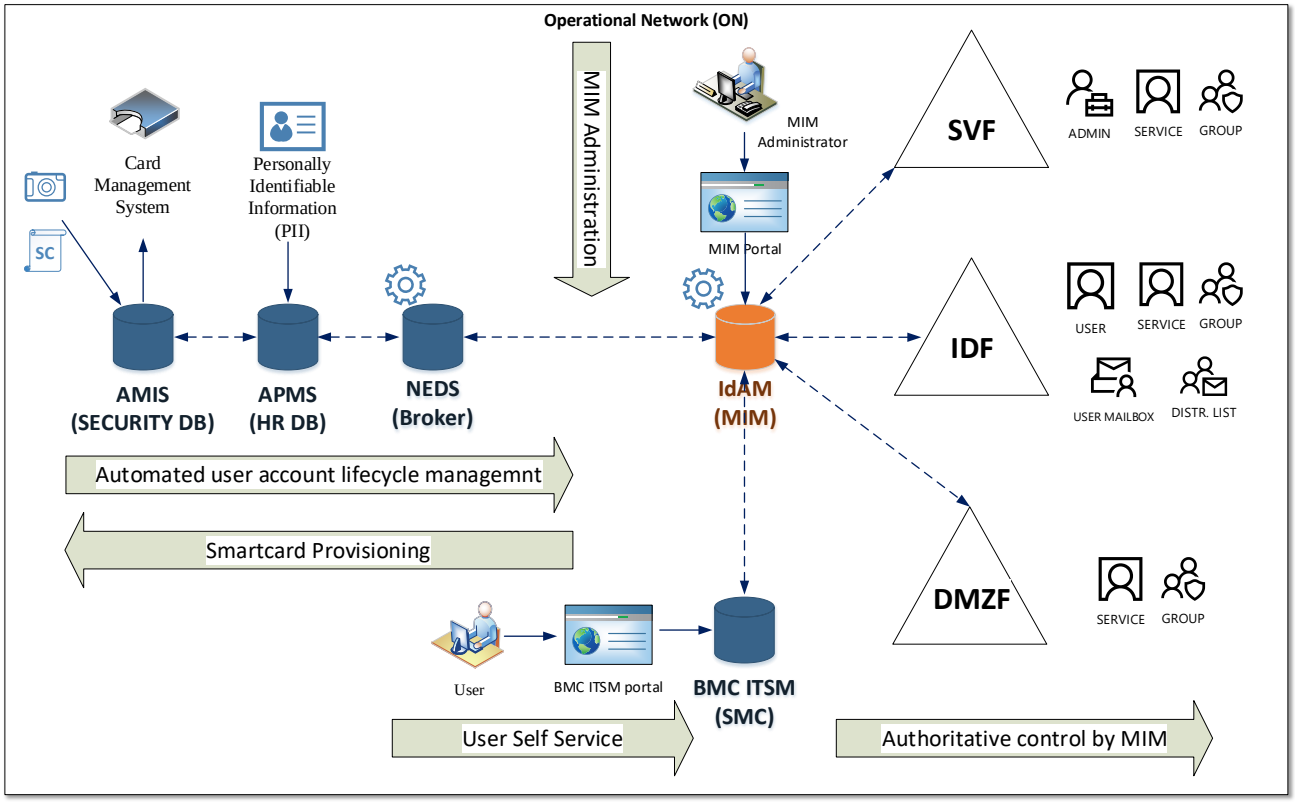

Figure 5 - High Level IDAM workflow

0047 ON users will be able to request mailbox or distribution list resource provisioning or access, as well as group access (access to defined services), which can either be automatically approved or require approval.

0048 MIM administrators can utilize the MIM portal as an interface to user and group management. The MIM portal will give administrators the ability to manage user and group objects as needed. The specific details related to identity management workflow and life cycle are to be developed during the implementation phase of the ON environment, based on both existing and desired business processes.

3.1.1.2.13. Attribute Mapping

0049 The common set of Active Directory schema attributes are extended by Microsoft Exchange and Skype for Business to support messaging services. The authoritative data sources for certain attributes and their data flow between MIM and NEDS is defined in the attribute Data Map.

3.1.1.2.14. Server Placement

0050 MIM is to be deployed in an active/passive architecture providing high availability within the active datacentre and a replica in the passive datacentre for disaster recovery purposes. (Figure 6)

0051 All MIM components are deployed in both Datacentres, leveraging the SQL Always-On availability groups for data synchronization.

0052 MIM deploys in the SVF, and includes the following core components:

A. SQL Server Always-On clusters, deployed at both Datacentres configured in an Always on High Availability and Disaster Recovery fashion allowing automated failover within the datacentre, but manual failover between datacentres.

B. The MIM Synchronization Service, deployed as active (hot) servers at the BEL-BRU-01 Datacentre, and as passive (warm spare) servers at the ITA-LAG-01 Datacentre

C. The MIM Portal Service, deployed on load-balanced servers at each datacentre

Figure 6 depicts the high level architecture.

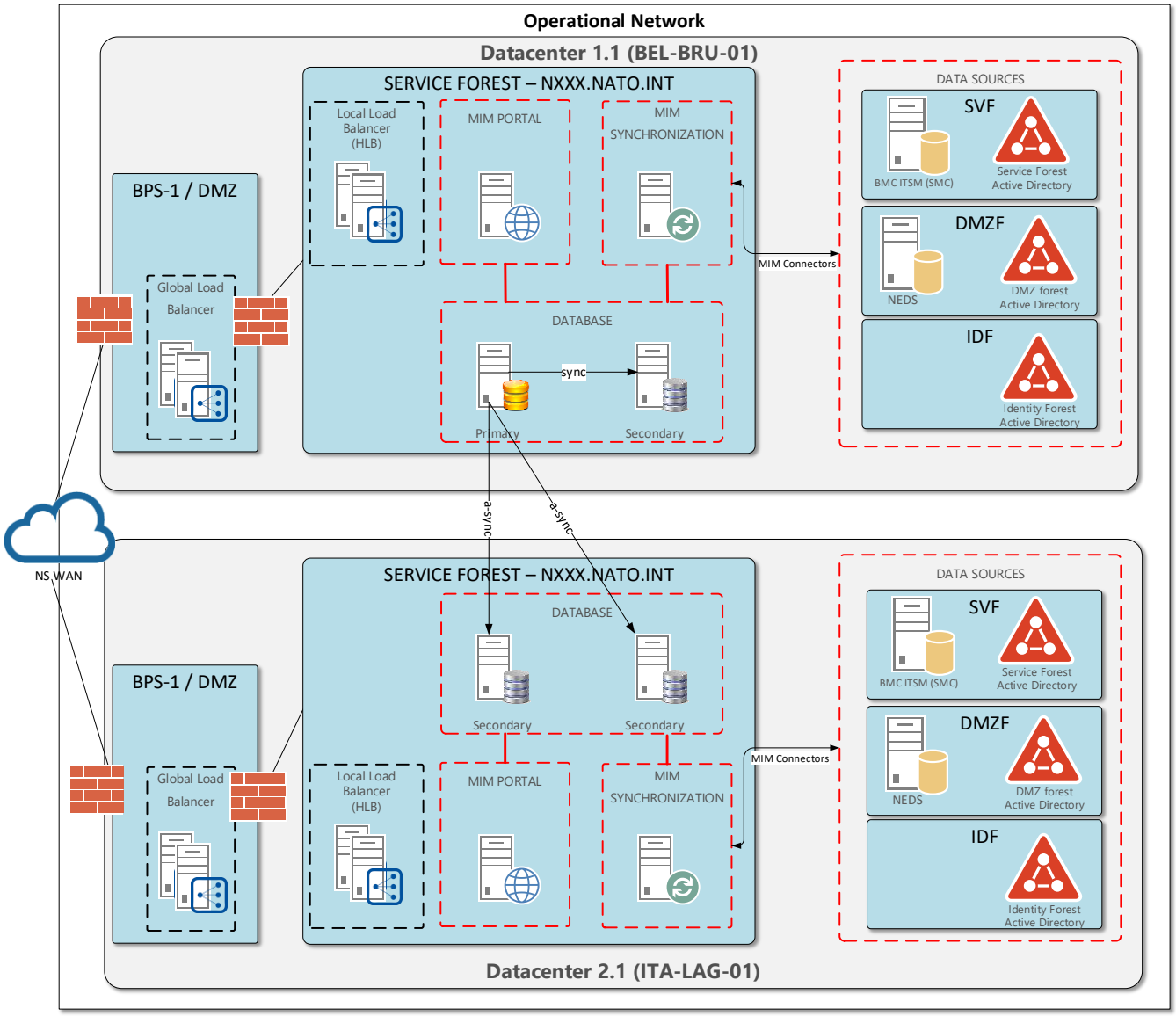

Figure 6. - MIM Server Site Architecture

3.1.1.2.15. MIM Synchronization Service

0053 The MIM Synchronization Service is the heart of the MIM solution. The Synchronization Service connects disparate data sources together, and controls directory provisioning based on a series of rules defined for each data source.

0054 The MIM Synchronization Service is deployed in the SVF to accomplish the following core identity management and governance tasks:

A. Consume user identities from the NEDS, and publish back AD-generated data such as usernames and email addresses
B. Provision administrative accounts[6] in the Service Forest.
C. Provision and manage production mailbox-enabled user accounts in the IDF.
D. Provision and manage personal file shares (home drives) and Sharepoint MySites for production user accounts in the IDF.
E. Provision and manage the membership of distribution lists in the IDF.
F. Provision and manage non-person entity (service) user accounts in all forests.
G. Provision and manage dedicated user accounts for testing in all forests.
H. Provision and police the membership of security groups in all forests.
I. Provision and manage shard mailboxes in the IDF.
J. Maintain authoritative control of user accounts names and email addresses.

0055 In support of these tasks, MIM will require connectors to exchange data with the following sources:

A. AD connectors to the IDF, Service Forest and DMZF.
B. LDAP connectors to the NATO Enterprise Directory System (NEDS).
C. LDAP connector to the ProofPoint mail routing AD-LDS instance [7]
D. Connectors to the MIM Portal
E. SQL Connectors to Remedy BMC SQL database

3.1.1.2.16. MIM Portal Service

0056 The MIM Portal Service is a browser-based interface used for managing users, groups, credentials, policies and reporting.

0057 MIMWAL[8] may be leveraged as a Workflow Activity Library (WAL) solution for MIM that supports configuring complex workflows. The MIMWAL deploys onto the MIM Portal Servers to support building out a workflow-based IDAM solution. MIMWAL will be used for streamlining approval processes and workflows to MIM.

3.1.1.2.17. BMC Remedy ITSM integration

0058 The Self-Service provisioning service, provided by BMC Remedy ITSM (enterprise SMC), will provide the capabilities for users to request services, as part of request fulfilment capabilities, from a single interface and provides the following capabilities in order to accomplish the following end-user core tasks,

A. Request and authorise the creation of new users.
B. Request and authorise the creation of new distribution lists.
C. Request membership to a distribution list
D. Request access to a specific group, application or service.

3.1.1.2.18. MIM Self-Service Password Reset

0059 The MIM self-service password reset functionality will not be used for the ON environment.

3.1.1.2.19. Microsoft AD-FS

0060 Microsoft AD-FS enables single sign-on access to systems and applications located across organisational boundaries. It uses a claims-based access control authorisation model to maintain application security and implement federated identity. Trust relationships are established with realms (both local and foreign) supporting SAML-based authentication. This

[6] Access management for privileged accounts (administrators) will be handled outside MIM, by the PAM solution.
[7] T.b.d. whether to use AD-LDS or the AD from the DMZF AD instead.
[8] https://github.com/Microsoft/MIMWAL

allows organisations to provide global access to internal resources in a controlled and authenticated fashion, without having to maintain a database of usernames and passwords for foreign users.

0061 In the ON environment, an AD-FS farm with two AD-FS servers as Security Token Service (STS) identity providers are deployed at each datacentre in both Identity and Service Forests. These farms are configured to trust the internal directory service, for authentication of both internal and external. The farm hosts the set of claims relevant to AD-FS integrated solutions in the enterprise, such as SharePoint. The first server in each farm (the primary federation server) hosts a read/write copy of the Windows Internal Database (WID) store the AD-FS configuration database; the second server in each farm (the secondary federation server) hosts a read-only copy of the WID, but promoted to primary in the event of a primary server failure.

0062 In support of mission partner access to internal portal resources, the Web Application Proxy (WAP) provides services in the BPS-1 (ON) security zones at each datacentre. This capability configures to point to the load-balanced AD-FS farm at each datacentre, with failover across Datacentres via a global load balancer. The full AD-FS architecture is shown in **Figure 7**.

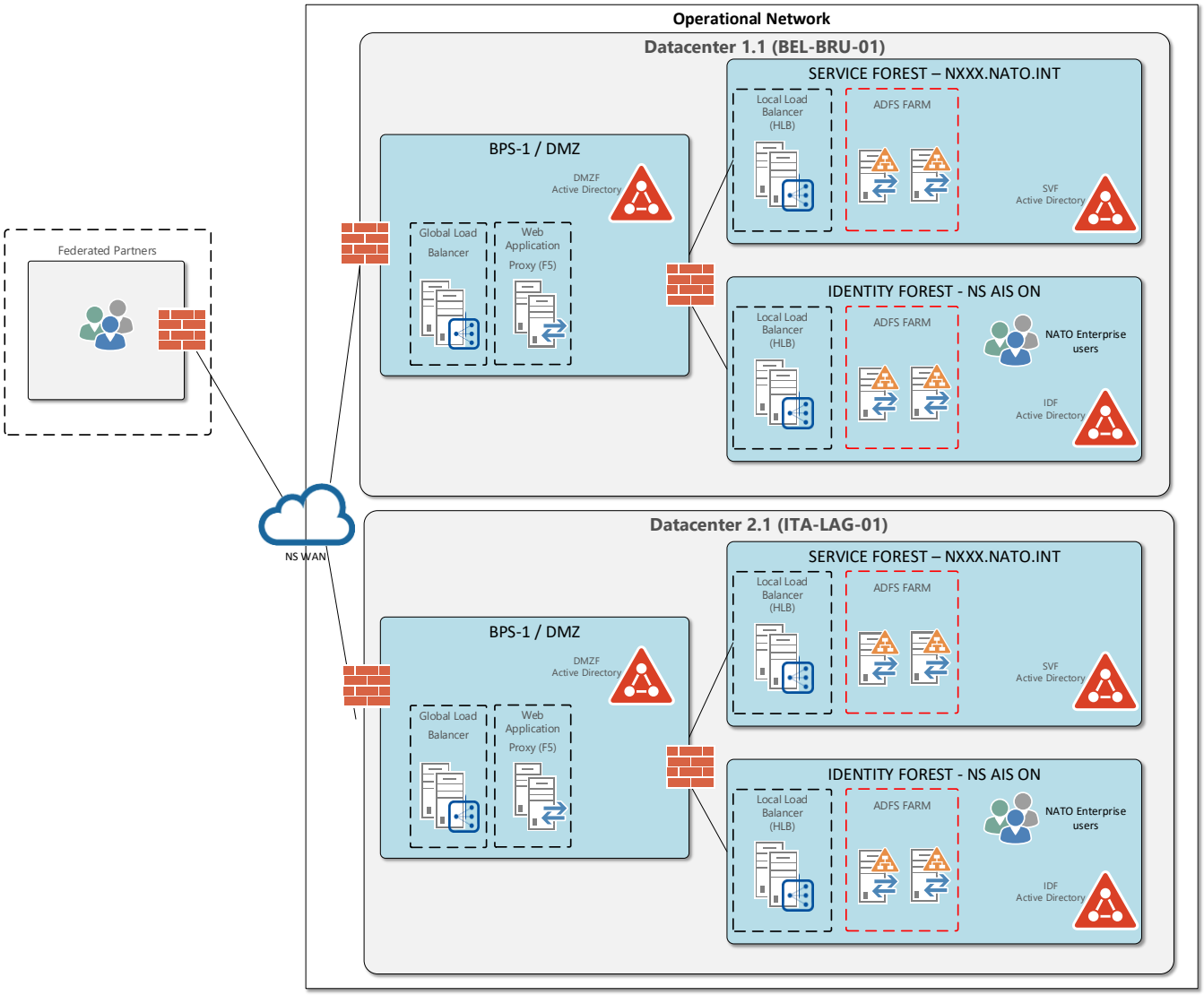

Figure 7 - AD-FS Architecture

3.1.1.2.20. Distributed File System

0063 Distributed File System (DFS) allows the creation of a single harmonized enterprise shared folder architecture. Shared folders deployed on different file servers organise into one or more logically structured namespaces. Each and every namespace appears to users as a single

shared folder with a series of subfolders, and data stored under each subfolder may be automatically replicated amongst other servers in the enterprise.

0064 For the ON environment, DFS will be implemented to support high availability file sharing between sites, single domain based namespaces, and file replication for certain core services. Its primary use cases are providing high available storage spaces for end users: user desktop client profiles and personal storage drive (home drive), as well as shared folders to host existing business related file shares and file sharing for the Unified Communications service (SfB). It will also provide file sharing for the Definitive Media Library (DML), file shares in which the definitive and authorized versions of all software configuration items are securely stored. The DFS may be extended in the future for applications requiring file sharing and replication.

0065 File sharing will be implemented on Microsoft Windows Server Failover Clustering (WSFC) on virtual machines to provide local high available file services. A dedicated windows server failover cluster of 2 nodes will be implemented at each site hosting infrastructure (DC, EN and SN).

0066 The WSFC servers will run on Windows Server. All clusters will be configured DFS Replication, and File Server Resource Manager Windows roles. The clusters in the Datacentres will be configured with DFS Namespaces integrated with the domain. Domain namespaces and shared folders support technologies as needed. Replication of namespaces will be performed based on user location to ensure continued access to files in the event of a disaster. The folders on the DFS-R namespace servers will be mapped back to the shares.

0067 The DFS-R namespace servers will be used to advertise & replicate data between the standard nodes, enhanced nodes and the regionally closest datacentre. Additionally the namespaces are replicated between the datacentres to ensure access to all users in the event of a site going down.

0068 The DFS-R namespace server architecture is shown in **Figure 8**.

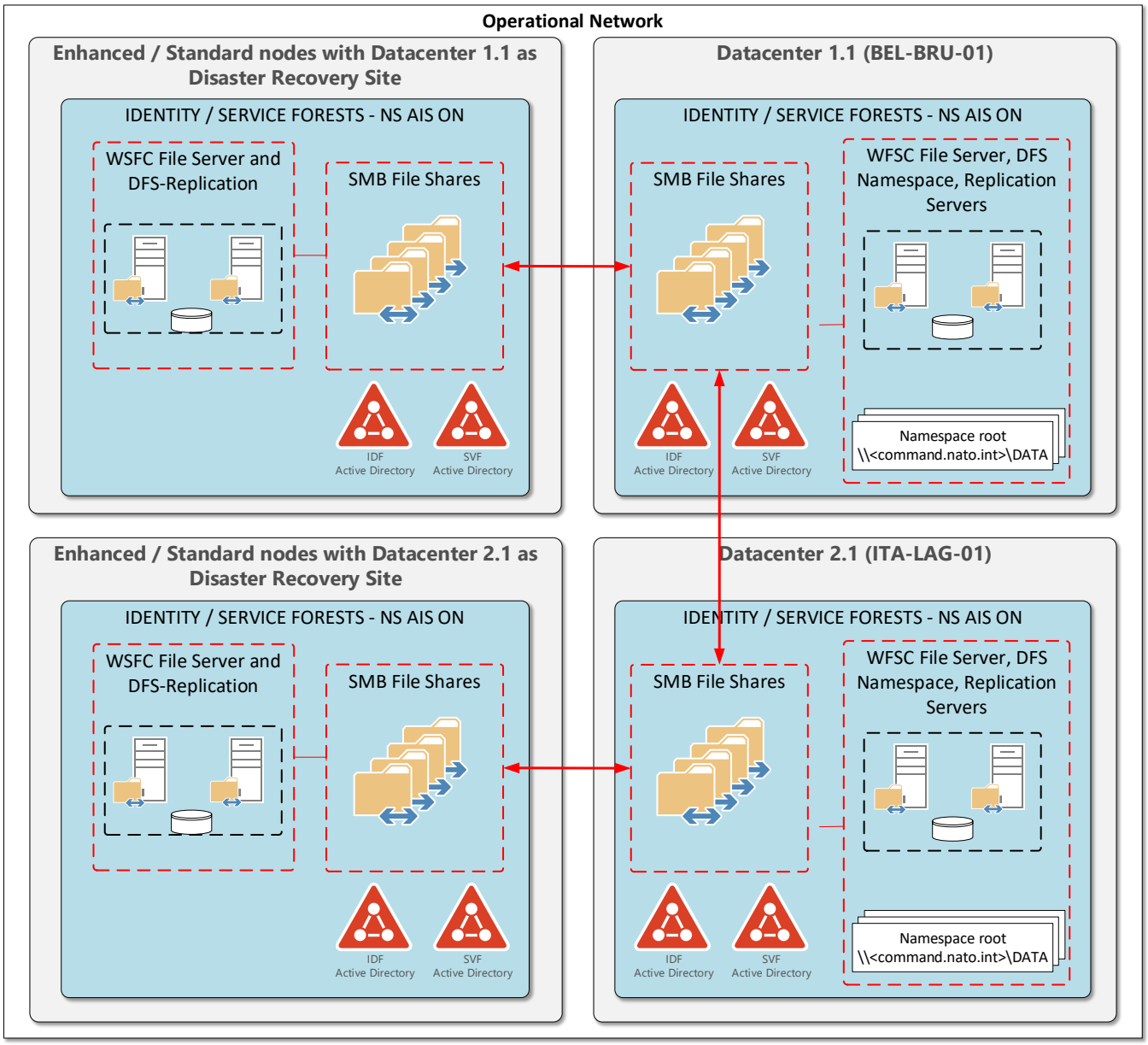

Figure 8 - DFS-R Architecture

3.1.1.2.21. Network Services

0069 The addresses network protocols integrate tightly with the Directory Service, including NTP, DNS and ADBA.

3.1.1.2.22. NTP

0070 NTP synchronization within a domain is extremely important for a variety of reasons, including application functionality, Kerberos authentication, and timestamp consistency. The following aspects are implemented by the NTP architecture:

A. All servers and appliances configured for the UTC (0:00) time zone
B. All non-domain-joined physical systems and appliances are configured to point to existing datacentre Stratum 1 time servers located in the datacentre locations. This includes all ESX hosts, as well as the datacentre hosting the PDC emulator FSMO role in each domain
C. All non-domain-joined virtual systems and appliances are configured to synchronize time settings with the underlying virtual host

D. All domain-joined servers and workstations in each domain are configured to draw time settings from local domain controllers as both primary and secondary time sources

E. All other devices in each domain are configured to pull time settings from the PDC emulator in each domain as a primary, and from a local NATO Stratum 1 time server as a secondary

F. For all forests, a domain controller acts as the time source for the domain. These domain controllers will reach out to NATO stratum 1 time servers to ensure time on the domain in synched with the rest of the NATO ecosystem. All infrastructure within the ON domains will point to the domain controllers for NTP. The NATO stratum 1 time servers are outlined in **Figure 9.**

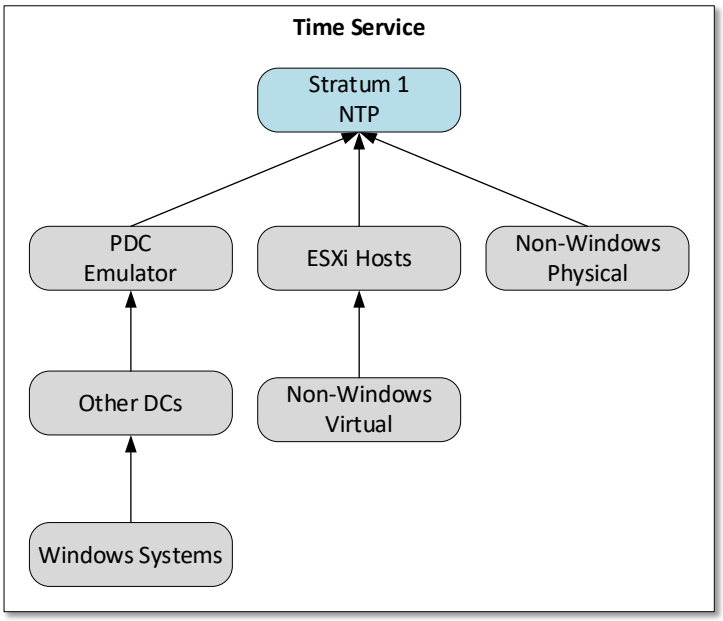

Figure 9 - ON NTP Architecture

3.1.1.2.23. DNS

0071 The DNS is a hierarchical decentralized naming system for computers, services, or other resources connected to the internet or a private network. Amongst other tasks, DNS translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with underlying network protocols.

0072 Active Directory integrated DNS is applied and configured as follows:

A. The DNS server role installed on every domain controller points to itself as a primary DNS server, and another domain controller in the same AD site as a secondary DNS server.

B. AD-integrated DNS is required for each domain, with secure dynamic updates enabled as well as DNSSEC[9] implemented using nPKI on all zones listed in **Table 6 -DNS Namespaces.**

Namespace	Description
AIS.NATO.INT	Administrative name for the Identity & Resource Domain
NECCCIS.AIS.NATO.INT	Administrative name for the Identity & Resource sub-domain for NECCCIS community
Nxxx.NATO.INT	Administrative name for the Service Domain (SVF) – [xxx] to be determined

[9] Implementation if DNSSEC for existing DNS zones are to be planned and executed with care in coordination with NATO to avoid any disruption of services.

Namespace	Description
N0178.NATO.INT	Administrative name for the BPS-1 DMZ Domain
shape.nato.int	Visual naming for SHAPE command
jfcnp.nato.int	Visual naming for Allied Joint Force Command Naples
mc.nato.int	Visual naming for Allied Maritime Command
nagsf.nato.int	Visual naming for Alliance Ground Surveillance Force
act.nato.int	Visual naming for Allied Command Transformation
lc.nato.int	Visual naming for Allied Land Command
ncia.nato.int	Visual naming for the NATO Communications and Information Agency
ncisghq.nato.int	Visual naming for the NATO Communications and Information Systems Group
<Table entries to be extended to include all commands and agencies within scope>	

Table 6 -DNS Namespaces

A. The ON zones defined in Table 6 -DNS Namespaces are delegated to the new ON DNS at the NATO enterprise level.

B. The current root DNS servers are to be transitioned to InfoBlox Appliances hosted in the BPS-1 DMZ in both datacentres to be integrated seamlessly with Active Directory, providing a robust solution for managing DNS and DHCP services. The DDI based on InfoBlox is described in the Service Design Package – Infrastructure as a Service (IaaS).

C. Each IDF, SVF and DMZF DNS server is configured to forward all queries up to the Infoblox root DNS servers hosted in the BPS-1 DMZ.

D. The root DNS has conditional forwarders for each trusted or trusting domain to facilitate communication with tenant domains, pointing to DNS servers that are authoritative for each domain namespace. For external name resolution, forwarders specify for perimeter DNS servers in the NATO environment.

E. .NATO.INT TLD is hosted on the root DNS servers. The root DNS servers are to be migrated from the existing root DNS servers, currently hosted on the IDF. (Listed in **Table 7**, below).

Location	Forest	Details
BEL-CAS-01	IDF (AIS.NATO.INT)	NSDW2DC1 (XX.XXX.22.51)
BEL-CAS-01	IDF (AIS.NATO.INT)	NSDW2DC1 (XX.XXX.22.51)
BEL-CAS-01	IDF (AIS.NATO.INT)	NSDW2DC2 (XX.XXX.22.52)
ITA-LAG-01	IDF (AIS.NATO.INT)	NSDW3DC1 (XX.XXX.135.51
ITA-LAG-01	IDF (AIS.NATO.INT)	NSDW3DC2 (XX.XXX.135.52)

Table 7 – Existing DNS

F. Forward lookup zones are configured for each local authoritative namespace, and reverse lookup zones are configured for each subnet on the network.

G. Record aging/scavenging is enabled at both the DNS server level and on every zone, with scavenging set to seven (7) days.

H. All DNS servers for each zone are configured for scavenging. Refresh intervals for each DNS entry is 7 days per Microsoft best practices

I. WINS forward lookup and Root Hints capabilities are not used. Other DNS Advanced settings are left at their default settings.

0073 **Figure 10** below depicts the DNS architecture.

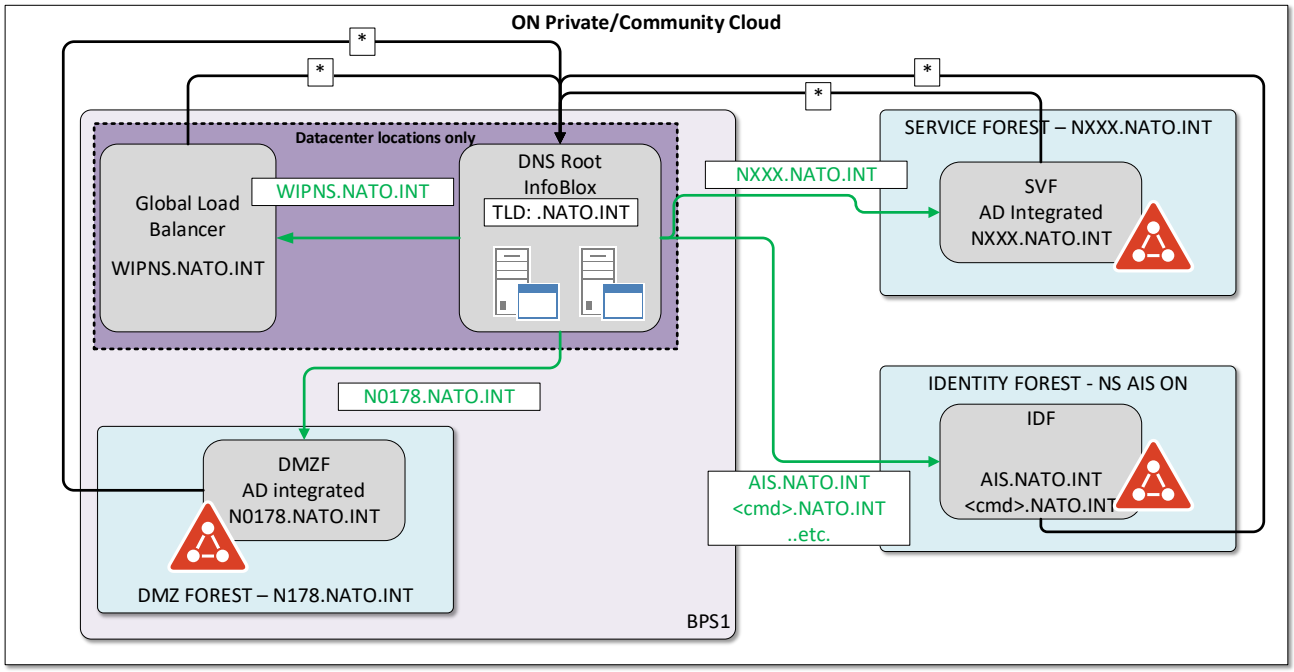

Figure 10 - DNS Architecture

3.1.1.2.24. ADBA

0074 Active Directory-Based Activation (ADBA) integrates Microsoft software (Windows and Office) activation with Active Directory Domain Services. This solution offers a number of key advantages over historical activation mechanisms, specifically:

A. No single physical computer is an activation server, because activation services are distributed throughout the domain, and are managed by any domain controller. ADBA eliminates the need for Key Management Services (KMS) servers across the enterprise.

0075 For the ON environment, the ADBA service is to be deployed on all three forests: IDF, SVF and DMZF. Each forest requires activation for using ADBA by applying customer-specific volume license keys (CSVLK).

3.1.1.2.25. KMS

0076 In case of non-domain joined hosts and tenant systems that are unable to use the ADBA, KMS servers will be added as needed to ensure all endpoints can us volume activation.

3.1.1.2.26. DHCP

0077 DHCP is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. The desktop provisioning service described in the Service Design Package – Client Provisioning Services (CPS) requires DHCP services for both thick (workstation) and thin (VDI) clients.

0078 The ON DHCP architecture (see **Figure 11**) will take into account high availability of DHCP services at all locations as follows:

A. Two virtual DHCP servers will be deployed at each datacentre, with DHCP load-balanced failover configured between them, configured 50% - 50%.

B. One virtual DHCP server will be deployed at each Enhanced Node and Standard Node.

C. One virtual hot-standby DHCP server will be deployed at each datacentre, each configured as a failover server for half the DHCP servers deployed at each Enhanced and Standard Node.

0079 DHCP will be configured as follows across the environment:

A. All DHCP servers will be authorised in the IDF AD and configured for conflict detection.
B. DHCP relay agents will be configured on all client subnet routers.
C. DHCP lease times will be configured for fourteen (14) days.
D. DHCP policies will be configured as needed to support different classes of client device.
E. TCP/IP configuration for servers and appliances will be applied statically; however, all client endpoints will be configured to pull TCP/IP configuration settings from a local DHCP server.
F. To facilitate failover to a warm standby server at each datacentre, all DNS entries will be registered by clients, and not by a DHCP server.
G. DHCP Scope options can be added in order to centrally manage network settings for IPv4 and IPv6

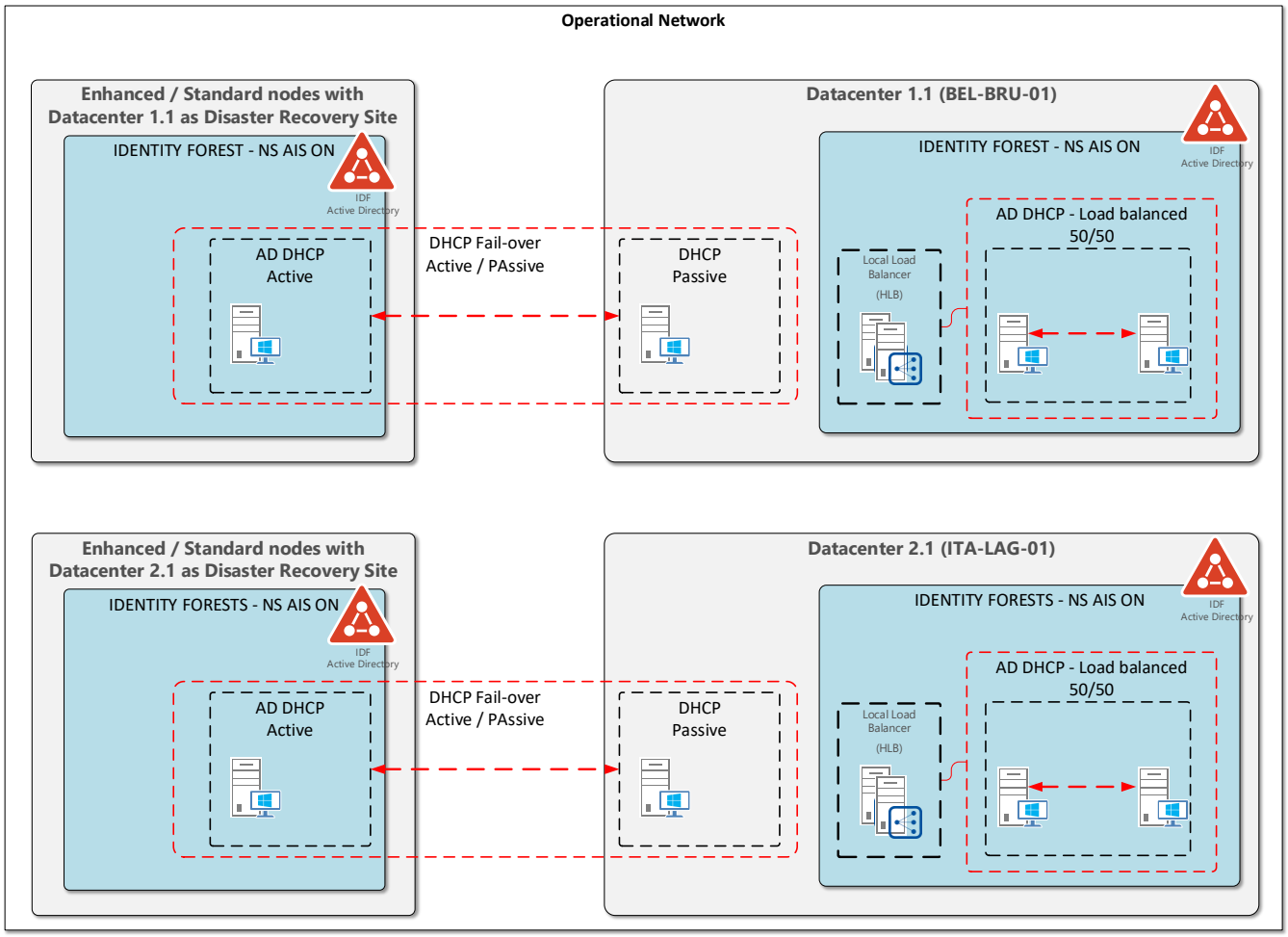

Figure 11 - DHCP Architecture

3.1.1.2.27. Naming Conventions

0080 This section addresses the operational naming of NATO IT services. This includes naming convention for AD related objects including DNS, organizational Units, Computer, Group Policy Objects, User and Security Group Objects and their attributes (e.g. DisplayName).

0081 The ON environment will require standard, unambiguous and unique naming parameters as will be outlined in the NATO naming policies. At time of writing, the current NATO naming

directives[10] are under review to be updated. Once the new directive(s) are published, these shall be followed for implementation for the ON. Close coordination with NATO is required in case the new naming policy directives do not provide sufficient detail.

0082 For user related identities, the NEDS shall provide all data attributes needed to support a common, standardized management of naming attributes. The MIM Service, as described earlier in this document, will automate the provisioning of these identities, hence a clear naming policy to support the automation in MIM is required. The following **Table 8** lists an example of the data attributes populated by MIM / AD, using multiple values sourced by NEDS:

AD Attribute	Description
cn (common name)	The name that represents an object. Generated from givnName and sn (surname)
distinguishedName	The DN is the name that uniquely identifies an entry in the directory. Generated from givnName, sn (surname) and location in the active directory hierarchy
sAMAccountName	The logon name used to support clients and servers running early versions of the MS operating system. This is generated from sn (surname) and command where the user is assigned to.
userPrincipalName	This attribute contains the UPN that is an Internet-style login name for a user based on the Internet standard RFC 822. By naming convention, this should map to the user email smtp address. The value is generated using the users givenName, sn (surname) and the domain name.
displayName	The display name for an object. Generated from the combination of the users first name, middle initial, and last name including organizational and grade/rank information.
mail	The user's primary email smtp address, matching the userPrincipalName.

Table 8 - List of data attributes to be populated by MIM/AD

0083 For non- user identity related naming, such as computer objects or functional mailboxes, clear policies are required to prepare the automated provisioning of IaaS resources (VM's), distribution lists and functional mailboxes requested via the ITSM portal. In addition, standardized and descriptive naming shall be used for Organizational Units, Group Policies, etc.

3.1.2. Email Messaging Services

0084 Email services will be reintegrated in a redundant manner as in-place in the current IDF (Bi-SC AIS) environment, based on Microsoft Exchange.

0085 The Email Data Loss Prevention (DLP), which is enabled by Titus for messaging and ProofPoint secure email gateways shall be implemented to support mail flows and mail DLP based on the Titus based security classification marking of messages

[10] [NCIARECCEN-4-111258] Agency Standard Operating Procedure – SOP 06.03.01 – Operational Naming and Addressing of NATO ICT Infrastructure and AC/322-N(2017)0109 – Annex 1 NU_NATO_Enterprise_Naming_Directive

0086 This section provides the concepts and high-level architecture for the Email Messaging service.

3.1.2.1. Concepts

0087 The Email Messaging Service architecture design contains the following core functional concepts:

A. **Security.** The following security practices for messaging are addressed for the e-mail design:
   - A.1. A strict least privilege model, with audited separation of duties. Exchange ships with a role-based access control (RBAC) model, which is suitable for these requirements.
   - A.2. Administrative access will be managed by a Privileged Access Management (PAM) service.
   - A.3. Malware inspection, and other perimeter controls.
   - A.4. Data loss prevention, and message inspection.

B. **Availability.** Mailbox servers are sized to ensure performant operation across the enterprise, including requirements for local site independent operation and fit for use over low bandwidth (<0.5Mbps) and high latency (>1sec) links.

C. **Scalability.** Ensure the infrastructure can scale in response to increased demand for email services, either for end users or applications.

D. **Recoverability.** The deployed messaging environment is resilient and fully recoverable to supporting a 4 hour Recovery Time Objective (RTO) and 8 hour Recovery Point Objective (RPO).

E. **Interoperability.** The email messaging environment is RFC compliant, and capable of supporting applications that require email services.

F. **Integration.** The Messaging Service integrates with other ON services as follows:
   - F.1. Besides end user messaging, the messaging service shall be integrated with core services for email notifications (e.g. Approval notifications, notifications on documents users follow.)
   - F.2. The IaaS Service provides networking services, including LAN services, boundary protection, compute and storage services.
   - F.3. The CPS Service provides patching- (MECM), monitoring- (SCOM), anti-virus (McAfee) protection services as well as file and message classification services (Titus client).
   - F.4. The SMC Service provides enterprise monitoring and logging services. The SMC service maintains the data required to perform historical trend analysis of health and capacity usage.

3.1.2.2. High Level Architecture

0088 The designed email messaging architecture includes the following key elements:

A. Dedicated directory-integrated messaging environments at each datacentre location based on Microsoft Exchange, including highly available deployments within the Bi-SC AIS IDF.

B. Titus Classification for Information Protection Control (IPC)

C. Proofpoint Protection Servers in the DMZs (BPS-1), for perimeter mail gateway functionality.

D. An Office Online Server (OOS) farm at each datacentre, for full document preview and online web document editing.

E. Global Address List for the NATO Enterprise. Mail recipients (contacts) are synchronized via the existing GAL synchronization service in the N178.NATO.INT (DMZF) forest.

3.1.2.3. Microsoft Exchange

Microsoft Exchange is an AD-integrated application compliant with industry standard messaging protocols. The latest approved version of Exchange listed in the NATO Roadmaps is to be implemented. The design in this document is based on Microsoft Exchange 2019.

3.1.2.3.1. Organisation Configuration

0089 The existing Exchange organisation on the AIS (IDF) forest will be uplifted to the target ON design described in this section. This organisation is implemented by detaching Exchange Admin functions from Domain Admin functions. This model restricts Exchange admins from creating directory objects directly (users/groups/contacts) and keeps Exchange admins from modifying non-Exchange attributes on objects. SMTP is the message transport mechanism of choice across the enterprise and for external email delivery, although other transport mechanisms (such as X.400 and Session Initiation Protocol (SIP)) meet application-specific requirements.

3.1.2.3.2. Administration

0090 The Exchange Admin Centre (EAC) is the default browser-based mechanism for Exchange organisation management. This tool allows remote management of the Exchange environment at all levels, from individual elements (e.g., mailbox settings) to the overall Exchange organisation (domain) configuration. The EAC console automatically discovers and adds new exchange servers. The EAC supports fine-grained role-based permissions, based on Active Directory security groups. Exchange uses the default set of administrative roles, unless a specific requirement emerges implying the creation of supplemental roles. **Table 9** describes these default roles.

Role	Description
Compliance Management	This role group allows a specified user, responsible for compliance, to properly configure and manage compliance settings within Exchange in accordance with their policy.
Delegated Setup	Members of this management role group have permissions to install and uninstall Exchange on provisioned servers. Do not delete this role group.
Discovery Management	Members of this management role group can perform searches of mailboxes in the Exchange organisation for data that meet specific criteria.
Help Desk	Members of this management role group can view and manage the configuration for individual recipients and view recipients in an Exchange organisation. Members of this role group can only manage the configuration each user can manage on his or her own mailbox. Additional permissions can be added by assigning additional management roles to this role group.
Hygiene Management	Members of this management role group can manage Exchange anti-spam features and grant permissions for antivirus products to integrate with Exchange.
Organisation Management	Members of this management role group have permissions to manage Exchange objects and their properties in the Exchange organisation. Members can also delegate role groups and management roles in the organisation.
Public Folder Management	Members of this management role group can manage public folders. Members can create and delete public folders and manage public folders. Public folder settings such as replicas, quotas, age limits and permissions as well as mail-enable and mail-disable public folders.

Role	Description
Recipient Management	Members of this management role group have rights to create, manage and remove Exchange recipient objects in the Exchange organisation.
Records Management	Members of this management role group can configure compliance features such as retention policy tags, message classifications, transport rules, and more.
Server Management	Members of this management role group have permissions to manage all Exchange servers within the Exchange organisation, but members do not have permissions to perform operations that have global impact in the Exchange organisation.
View Only	Members of this management role group can view recipient and configuration objects and their properties in the Exchange organisation.

Table 9 - Exchange Administrative Roles

3.1.2.3.3. Server Architecture

0091 Each datacentre hosts multiple physical mailbox servers. These systems have the ability to fail across datacentres via Database Availability Group (DAG) configuration.

0092 Exchange and active directory have leverage the MIM service for mailbox and distribution lists management (provision, change, de-provision, membership).

0093 In order to comply with availability and data recovery requirements, DAGs on each network include four copies of every database. Two copies are kept at each datacentre to comply with Microsoft's 'Preferred Architecture' (PA) guidance[11] for high availability. The primary active databases are balanced between each datacentre, allowing user mailboxes to be homed at a location with the lowest possible latency.

0094 ProofPoint Protection Servers are deployed in the DMZ (BPS-1) at the Datacentre locations to address security requirements such as malware and content scanning at the gateway. Exchange server based malware and content scanning will be implemented on a new product which is to be determined. (Currently using Symantec Mail Security for Microsoft Exchange).

0095 The messaging high level architecture is shown in Error! Reference source not found.

[11] https://docs.microsoft.com/en-us/exchange/plan-and-deploy/deployment-ref/preferred-architecture-2019?view=exchserver-2019

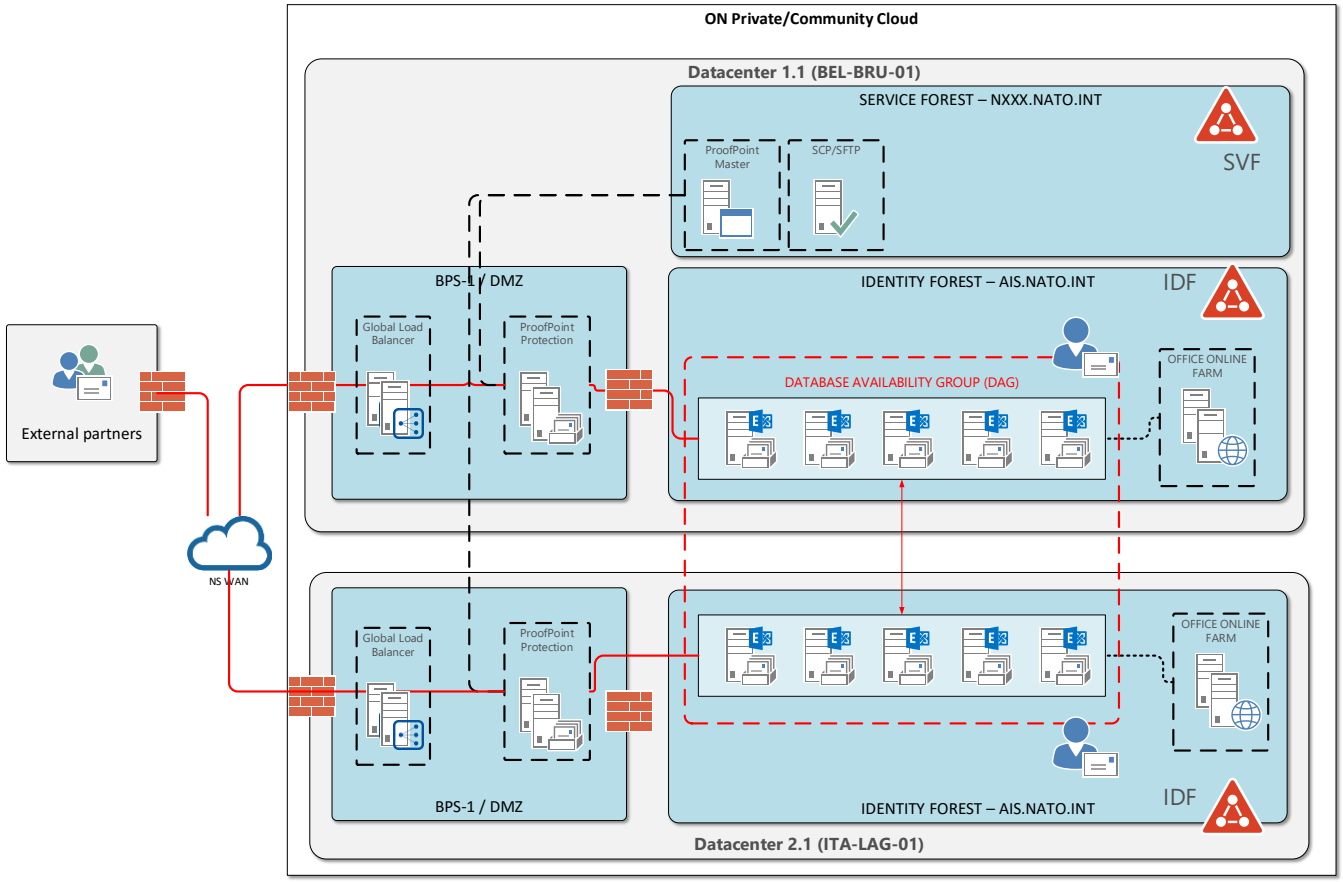

Figure 12 ON Messaging Server Architecture

3.1.2.3.4. Exchange DAG Configuration

0096 DAGs are configured on each datacentre as follows:

0097 Exchange DAGs require a file share witness (FSW) to arbitrate database failover within the DAG. The FSW is on a dedicated File Share Witness server at a 3rd location (to be determined), and provides automated DAG failover in the event of a datacentre failure.

0098 The database has four copies of every mailbox database – two at each datacentre. ECS configures three database instances in each DAG as High Availability (HA) copies and one instance as a Lagged Copy with a 7-day log replay lag. Additional servers (with additional databases) added as necessary to support user growth.

0099 Database lag copy logs automatically play down when one of the following conditions is true:

- When a low disk space threshold (10,000MB) is reached
- When physical corruption is detected, and a lagged DB copy must be page-patched
- When there are fewer than three available healthy HA copies for more than 24 hours

0100 User locations will be attributable in active directory using a custom city attribute. With the location attributes in place, users have their mailbox hosted at the datacentre with the lowest latency to their local site. To ensure even distribution of DAG copies monthly rebalances will be performed to ensure no datacentre is over provisioned. During a rebalance users locations will be checked and verified that they are still tied to the datacentre with the lowest latency.

0101 ECS maintains following mailbox types:

- Personal mailbox: mailbox assigned to a single person containing persons first- and lastname in the display and SMTP address naming. Set as primary mailbox. Each user will receive a personal mailbox by default. The default storage quota will be initially set to 10 GB.

- Functional Mailbox: mailbox assigned to a single person containing persons function in the display and SMTP address naming. No personal name is assigned to this mailbox. The default storage quota will be 10 GB as well.
- Organizational Mailbox: mailbox assigned to an organizational element. Containing organizational element in the display name and SMTP address. (a.k.a. shared mailboxes)
- Distribution Lists: mail enabled security group that is used to send emails to multiple pre-defined recipients.

0102 The lifecycle of mailbox and distribution lists are maintained via MIM. Triggers for provisioning and de-provisioning of distribution lists, functional and organizational mailboxes come from the ITSM service. Triggers (provisioning, changes, de-provisioning) for personal mailboxes are provided from the NEDS system and are automated.

3.1.2.3.5. Sizing

0103 To model the Exchange server and storage, the Exchange Server 2019 Sizing Calculator[12] is used, which uses a variety of data points, including system availability and failover, user count, server hardware, and returns DAG sizing and IOPS calculations as output.

0104 ECS considers the following key requirements in running these calculations:

- Messaging service is fully resilient across 2 Datacentre locations.
- The Exchange availability requirements are set to 8 hours Recovery Point (RPO, i.e. 8 hours of acceptable data loss) and 4 hours Recovery Time (RTO, i.e. 4 hours to restore the service).
- There are three user profiles:
  - 20% of users sending 50 messages/day
  - 60% of users sending 100 messages/day
  - 20% of users sending 150 messages/day
- Server is sized based on current amount of mailboxes including an instant growth for 25% beyond current numbers provided, as well as the number of messages send per tier. For the calculation input, initial and maximum mailbox sizes are reduced to 1.5GB / 5GB for Tier 1 and 2, and 1/5GB/10GB for Tier 3, as shown in **Error! Reference source not found.**.
- The capacity of Exchange will be expanded by scaling out (adding servers) when required.

- Exchange server hardware selected is based on HP Apollo 4200 Gen10 24 LFF13. See details in **Table 10 Exchange Server Hardware configuration.**

Key Components	Specification	Amount
CPU	Intel Xeon-Gold 6252 (2.1GHz/24-core) – SPECint2017 Rate Value: 232	2
Memory	HPE 32GB (1x32GB) Dual Rank x4 DDR4-2933 CAS-21-21-21 Registered Smart Memory Kit	8
Boot disks	HPE 960GB SAS 12G Mixed Use LFF	2
DB Disks	HPE 10TB SAS 12G Business Critical 7.2K LFF LP 1-year Warranty Helium 512e Multi Vendor HDD	10
Mail Cache Disks	HPE 1.6TB SAS 12G Mixed Use SFF SC Multi Vendor SSD	2

[12] https://aka.ms/Exchange2019Calc
[13] Hardware specifications will be reviewed upon ordering and may be updated to better or newer configurations when required.

Network	HPE Ethernet 10/25Gb 2-port SFP28 BCM57414 Adapter	3

Table 10 Exchange Server Hardware configuration

- The Apollo 4200 Gen10 contains 24LFF slots in the front, and is extended in the rear of the chassis with an additional disk cage of 6SFF as depicted in **Figure 13 HP Apollo 24 LFF – Exchange Server**.

Figure 13 HP Apollo 24 LFF – Exchange Server

0105 The results from the Exchange Server 2019 Sizing Calculator using the details above is summarized as follows:

1 DAG consisting of:

- 4 copies per database (3 none-lagged / 1 lagged)
- 180 databases.
- 720 database copies
- Distributed over 10 servers (5 per Datacentre)

Each server has 72 database copies of which:

- 18 are active
- 36 are none lagged passive databases
- 18 are lagged databases

Storage Sizing Details:

- OS disks:
    - 2x 960 GB LFF (RAID-1)

Recommended Transport Database Location:

- Dedicated RAID-1 Disk
- As OS disks are 960GB LFF, this volume will be hosted as a second partition on the OS boot drive.

DB and LOG Requirements:

- 18 Database Volumes per server with 4 Database copies per volume
- Database + Log copy size: 2062 GB
- Total Database + Log Volume Space required per server: 148453 GB
- JBOD storage using 10TB disks will have an optimal number of 18 disks per server.

MetaCacheDataBase (MCDB) Space Required (6%): 8907 GB

- MCDB will require a target 1:3 ratio between SSD and HDD devices per server.
- 18 DB/LOG HDDs require 6 MCDB SSD devices per server.

- Restore Volume
    - Restore Volume Space required 8681 GB, requires 1 HDD of 10 TB.

- Auto Reseed Volume:
    - 1 HDD of 10 TB
- Total Disks required:
    - LFF HDD: 20x 10TB for Databases, Logs, AutoReseed and Restore.
    - SFF SDD: 6x 1.6 TB SSD for MCDB
    - LFF HDD: 2x 960 GB for the Operating System (RAID1)
- Disk slots available:
    - 2x LFF

0106 The detailed Calculator Sizing results can be found in Exchange Server Role Requirements Calculator.

3.1.2.3.6. Accepted Domains

0107 It is not expected that there will not be a change in the domain naming in the foreseeable future, hence the currently defined accepted domains will remain the same. There is a possibility that the domain suffix for the enterprise will be aligned to a single domain suffix (e.g. @nato.int) pending the outcome of the naming policy directives update.

3.1.2.3.7. Email Address Policies

0108 User accounts and settings will be aligned to naming standards, assigning all users a primary and unique SMTP address. This assignment uses authoritative information from the NEDS and is executed by MIM. A number of additional proxy addresses are stamped for various purposes, including:

- Any legacy email addresses previously assigned to the user
- SIP addresses, in support of VoIP services
- X500 addresses, based on the legacyExchangeDN in the legacy environment.

3.1.2.3.8. Send/Receive Connectors

0109 SMTP creates receive connectors as needed to support SMTP-enabled software and devices. SMTP creates send connectors such as:

- for the MIM Service
- for the Remedy ITSM SMC Service
- for any multifunction printer/scanner devices
- Other mail-enabled software [TBC]

0110 SMTP creates send connectors as follows:

- A smart host configures any address spaces specific to the NATO HQ email system, the deployable CIS messaging systems and any other NATO email systems.
- The ProofPoint appliance VIP (hosted in BPS-1) is the default domain (*) for all outbound mail. The ProofPoint appliance scans and either rejects or forwards email as appropriate. These appliances are the perimeter mail guards for any email outbound from the ON environment.

3.1.2.3.9. Mail Flow Architecture

0111 Prior to sending any message, the Titus Message Classification suite enforces classification marking as described in section 3.1.6.1 Information Protection Control (IPC)**.**

0112 The Titus add-in for Outlook/OWA blocks incorrectly marked messages and warns the user of potential data breaches, in case the email violates a security policy (e.g. sending a higher

classification labelled message to a lower classification recipient). Classification of recipients are based on the domain name of the email address.

0113

0114 All emails to recipients outside the Exchange Organization will traverse the ProofPoint Mail gateway in BPS-1. ProofPoint will perform a deep inspection of files for key word analysis and regex checks for content that is not a candidate for release. Messages failing ProofPoint scanning are quarantined; messages that pass ProofPoint scanning are forwarded to their destination by either using DNS MX records, or Smart Hosts for explicit NATO domains. Message release functionality is to be enabled by administrative workflow.

0115 TITUS is integrated with McAfee DLP to reduce the risk of data loss by analysing the sensitivity and the context of the data being transmitted, and take appropriate action (e.g. allow, block, etc.)

3.1.2.3.10. Client Connectivity

0116 Client connectivity supports a number of devices and mechanisms, on both networks, using a variety of protocols, and from both physical (desktop/laptop/mobile) and VDI end-points, as outlined in Table 11 - Client Connectivity**.**

Client	Access Mechanism	Protocol
Thick clients, VDI, laptops	Outlook desktop client,	MAPI over HTTP, Exchange Autodiscover
Browser	Outlook Web Access (OWA)	HTTPS (TLS)

Table 11 - Client Connectivity

3.1.2.3.11. PKI Services

0117 The messaging service provides Secure Multipurpose Internet Mail Extensions (SMIME) support by leveraging the NATO PKI infrastructure for digital signatures. Outlook points to NATO PKI-issued smart card private keys for this messaging function. The ON Messaging service will check CRLs of the issuing authorities to ensure certificates are valid and sign the message with the user's private key. Email Gateways will have a trust with the NATO PKI authorities to facilitate signing of messages using smart cards.

3.1.2.3.12. Backup and Recovery

0118 Recovery of mailbox items will need to occur within 4 hours to match the RTO. The maximum acceptable data loss for email is set to 8 hours (RPO).

0119 In order to facilitate data backup and recovery in the messaging environment, ECS implements the following protections:

- To mitigate the accidental deletion of a mailbox, Exchange-deleted mailbox recovery is left at its default setting of thirty (30) days. This feature allows a system administrator to restore a deleted mailbox by reattaching it to an Active Directory user account.
- If an accidental deletion of a mail or calendar item occurs, thirty (30) days of deleted item recovery (undelete) allows users to self-recover any accidentally deleted email during this time period.

0120 To support long-term recovery of Exchange data, the ECS Email Messaging solution integrates with the IaaS Backup solution as follows:

- VEEAM backup integrates with the physical dedicated Exchange servers for Exchange backups.

- Backups are executed against inactive database copies of each database. Backup frequency and retention are to be defined together with NATO.

0121 In order to mitigate the risk of widespread Exchange organization corruption (for example, due to a malware or ransomware attack), the Exchange database lag copies allow seven (7) day point-in-time recovery at the database level.

0122 In order to mitigate the risk of a datacentre failure, the Exchange DAG architecture described under

0123 Exchange DAG Configuration allows the restoration of Exchange services without meaningful data loss.

3.1.2.3.13. Antimalware Protection

0124 The Mail Security service for Microsoft Exchange must provide defence-in-depth against email malware exposure. This service helps secure and protect the ON environment from malicious software that might enter the environment through out-of-band mechanisms, and may transfer via email. Exchange scans all transactions and messages sent or received for malware (viruses and spyware) using the Mail Security service. If the service detects malware, the message truncates, a notification is sent to both senders and administrators, and the infected message deleted.

0125 Antimalware service are provided at the network perimeter by ProofPoint. The built-in Anti-spam protection in MS Exchange will not be enabled.

3.1.2.4. ProofPoint

0126 ProofPoint Protection Server is deployed at the network perimeter to provide malware protection, spam detection, and regulatory compliance. ProofPoint provides substantial benefits above a native Exchange Edge Server deployment, including:

- 99.999% service availability
- 99% blocked or redirected spam
- 100% virus protection
- Less than 1 minute email latency

3.1.2.4.1. Server Placement

0127 The ON ProofPoint solution consists of a single ProofPoint cluster that includes two load-balanced ProofPoint virtual appliances serve as agent servers hosted in BPS-1 (NS DMZ) segment, at both datacentre sites. A single ProofPoint master server virtual appliance, hosted at BEL-BRU-01 site, which manages and configures the enterprise ProofPoint configuration. (The ProofPoint agent servers function without this master server, and so this system does not need to be highly available.)

- An additional master server virtual appliance hosted on the PFE provided internet connected environment, located at BEL-BRU-01 site, in order to download software updates and patches that for the isolated (air-gapped) ON ProofPoint deployment.
- An SCP/SFTP server, located at the BEL-BRU-01 site, backs up the ProofPoint master server configuration, and to support system patching

0128 All four ProofPoint agent appliances are load-balanced globally against a single published MX record. This configuration helps ensure inbound and outbound mail delivery, and reduces the risk of an outside hacker’s accessing the master ProofPoint Protection Server or appliance.

3.1.2.4.2. ProofPoint Protection

0129 ProofPoint Protection includes all the malware scanning and Message Content Filtering capabilities of the ProofPoint solution, including:

- Malware protection, against regularly updated A/V signatures
- Unsolicited Commercial Email (UCE) protection, against a database of known spammers
- Zero-hour malware protection, against suspicious active content
- Phishing protection, against organisation directory enumeration attacks
- Evaluation of inbound and outbound email messages on the basis of administrative rules, such as keyword analysis of message and attachment contents (including document footers and headers), i.e., message content filtering. Additionally message headers will be checked for classification labels.

3.1.2.4.3. Message Quarantine

0130 The ProofPoint Web Application allows users to view messages in the Quarantine or Incident Queue using a browser. Administrators manage ProofPoint tasks such as creating Safe Senders and Blocked Senders list, choosing a language and selecting a policy for filtering spam.

0131 ProofPoint sends a list of quarantined messages (a digest) to end users. Users view the list of messages in the Quarantine or Incident Queue. The users request message release, or request message release and the addition of the sender of the message to a personal Safe Senders list. Administrators have the ability to examine quarantined messages and release messages inappropriately quarantined.

3.1.3. Unified Communication Services

0132 This section provides the concepts, high-level architecture, and implementation strategy for the ECS Unified Communications (UC) Service, based on Skype for Business (SfB). The latest approved version of SfB listed in the NATO Roadmaps is to be implemented. The design in this document is based on SfB 2019.

3.1.3.1. Concepts

0133 The UC Service architecture design is based on the following core functional concepts:

1. **Security:** Ensuring confidentiality goals by encrypting communications via 128-bit Transport Layer Security (TLS) encryption. Audio and video (AV) traveling is encrypted by using Secure Real-time Transport Protocol (SRTP) and 128-bit Advanced Encryption Standard (AES) stream encryption.
2. **High Availability:** High scheduled uptime through the deployment of redundant components and paired pools is accomplished through:
   - Server placement – SfB servers are designed for High Availability to meet capacity and resiliency requirements for each region. This ensures that if a single server fails, another one within the pool is available to handle the expected load.
   - Pool Pairing – SfB server roles are grouped within a pool. Each datacentre will have an active pool for that region. Each pool supports connections from users assigned to a given pool. Users are assigned to a pool based on their geographical location.
   - Global Load Balancing for common URLs – providing HA for simple URL's (Common URLs e.g. meet / dial) via Global Load Balancer to provide more regionalized traffic and support disaster recovery.
   - Database HA – SfB Servers strongly rely on SQL Servers. To improve availability of the SQL Server, SfB leverages SQL Server AlwaysOn.
   - File server replication using a Windows DFS-R file share to improve availability of the file service.
3. **Audio Quality:** Acceptable audio quality achieved through quality of service (QoS) and SfB codecs.

4. **Supportability:** Full compliance with current Microsoft best practices and system requirements.
5. **Scalability:** Sufficient capacity for future growth through a scalable solution.
6. **Interoperability:** Sufficiently flexible design enables interaction with other communication infrastructure and investments within the organisation, such as video conferencing rooms and telephony private branch exchanges (PBXs). Integration with VTC rooms and PBX is out of scope for ITM-RC1 project.
7. **Integration:** The Unified Communications Service integrates with other ON services as follows:
   - Integrate with Exchange Server to exchange user presence information between Outlook /Exchange and SfB.
   - The IaaS Service provides networking services, including LAN services, load balancing, boundary protection, processing, storage and virtualization services.
   - The CPS Service provides Windows patching services, monitoring as well as anti-virus protection services.
   - The SMC Service provides enterprise monitoring and logging services. The SMC Service maintains the data required to perform historical trend analysis of health and capacity usage.

3.1.3.2. High Level Architecture

0134 The proposed SfB architecture includes the following key elements:

- A Front-End server pool, which provides the core SfB functionality.
- The Edge Server role, which supports SfB federation with other NATO SfB systems.
- SQL Back-end servers, which hosts SfB data (user and server)
- The Office Online Server role, which shares Office files in a video conference. This role is not a SfB role, and is shared with the Messaging and Portal Services.
- A dedicated File Share (DFS), supporting the Front-end role and logging, as well as the SQL Server AlwaysOn file share witness capability at each datacentre.

0135 The SfB architecture excludes:

- Mediation, Video Interop Server and Director Servers, as there are currently no requirements for the functions these servers provide.
- Persistent Chat as it is no longer supported in SfB 2019.

0136 This solution supports the following features:

- IM and Presence
- Peer-to-Peer Communication
- Audio and Video
- Multi-Conferencing
- Application Screen Sharing and White boarding
- External Federation

3.1.3.2.1. Server Sizing

0137 Microsoft recommends one Front-end Skype for Business Server be deployed for every 6,600 users in the Front-end pool. The existing front-end pool size uses 5 front-end servers to host the complete environment.[14]. The pools are hosted at both datacentres (BEL-BRU-01 and

[14] Based on recommendations from recently executed Microsoft Risk Assessment Program for Skype for Business.

ITA-LAG-01) and are each sized identically in order to provide for resiliency between pools, so all active users are supported by a single site in the event of a site failover.

0138 Skype for Business shall be initially deployed on a virtual platform. This requires meeting these very specific virtual platform requirements[15] to include the following:

- Maintain a 1:1 ratio of virtual CPU to physical CPU.
- Don't move a guest server while it's operating.
- Migration of a live system and portability of a virtual machine aren't supported.
- Disable hyper-threading on all hosts.
- Don't configure dynamic memory on host servers.
- Use fixed or pass-through disks rather than dynamic disks.
- Allow for 6-10 percent overhead for hypervisors beyond what the virtual guest requires.

3.1.3.2.2. Front-End and Edge Server Pool

0139 The Front-end Server is the core SfB server role, and runs many basic SfB functions. A Front-end pool is a set of Front-end Servers, configured identically, working together to provide services for a common group of users. A pool of multiple servers running the same role provides scalability and failover capability.

Server Placement

0140 One Front-end pool is deployed at each datacentre, with 5 servers in each pool providing high availability for the front-end. Pool Pairing is used to provide disaster recovery between the 2 Datacentres. Pool Pairing establishes a one-to-one relationship between Front-end server pools, allowing user data replication from one pool to another; in case of a pool failure, the paired pool absorbs the workload (and users) from the failed pool.

0141 Edge Servers enable SfB collaboration outside the organisation’s firewalls. These include users from federated partner organisations on the same classification level.

0142 There are currently a handful of SfB federations including federation with:

- NATO Mission in IRAQ
- UK MOD
- Joins Support Enabling Command
- Allied Rapid Reaction Corp.

0143 One Edge Server pool is deployed in the BPS-1 DMZ at each datacentre. Each Edge Server pool contains two Edge servers. **Figure 14 Skype for Business topology.**

[15] https://docs.microsoft.com/en-us/skypeforbusiness/virtualization-guidance

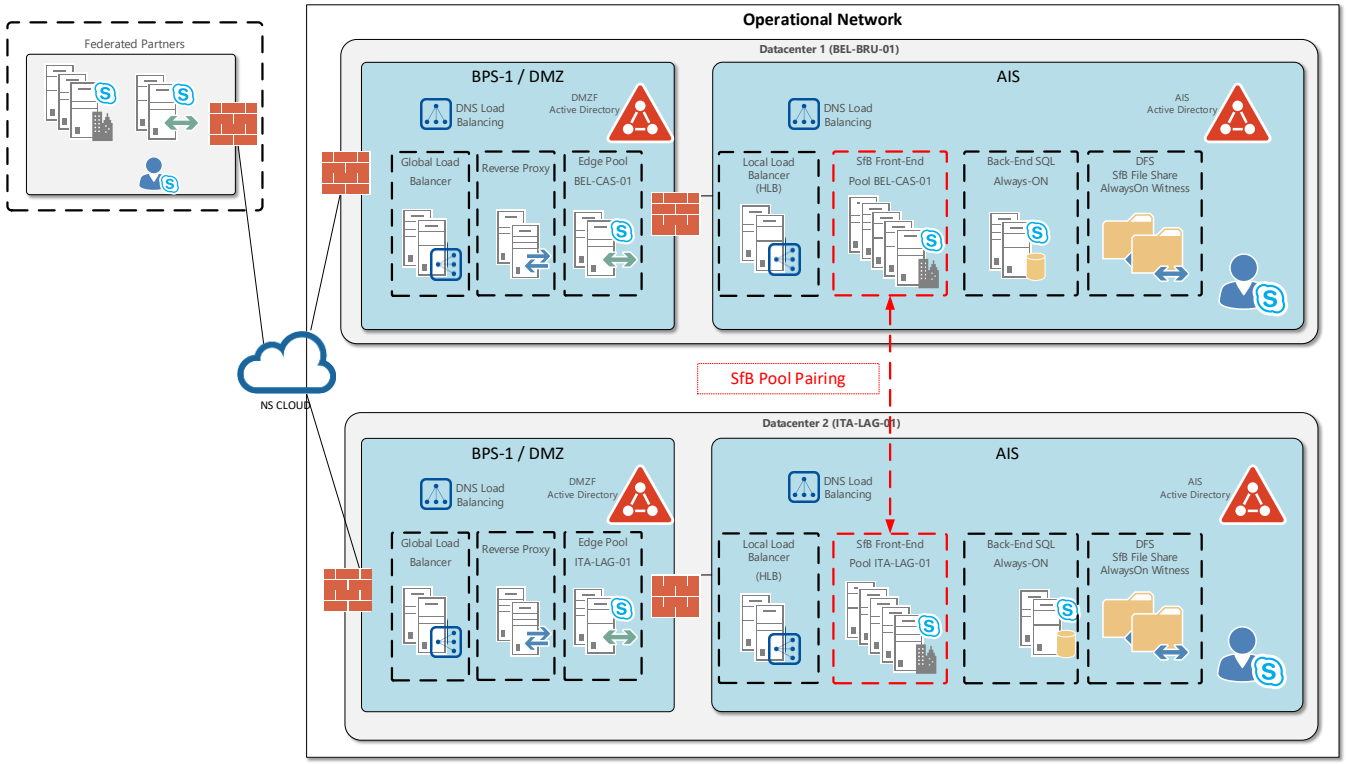

Figure 14 Skype for Business topology

3.1.3.2.3. Load Balancing

0144 Load balancing in SfB is applied to the Front End Pools and Edge servers. The intended SfB design is based using both DNS load balancing and Hardware Load Balancing (HLB). The Load Balancing services from the Service Design Package – Infrastructure as a Service (IaaS) are to be leveraged.

- DNS load balancing offers several advantages such as simpler administration, more efficient troubleshooting, and the ability to isolate much of your SfB traffic from any potential HLB problems. DNS load balancing balances the network traffic for server to server SIP traffic, media traffic and all client-to server traffic between Clients and Edge Servers.
- HLB is used for client to server web (HTTP) traffic to the front-end servers, as this is not supported by DNS load balancing.
- Global Load Balancing is used to load balance the common simple URL's (e.g. discover, dialin, meet). This enables servicing a request to a particular user based on their geography. The advantages will be that the traffic will be more regionalized and it also provides an automated redirection in case of disaster in one of the datacentres.

3.1.3.2.4. Monitoring

0145 The monitoring service in SfB provides a way for administrators to collect usage and quality data for the communication sessions taking place in their organisation, allowing them to identify trends and problems. Ongoing monitoring of system deployment allows administrators to catch problems early and keep the organisation's users satisfied.

0146 The SfB monitoring service does not require a separate server role (as was the case in earlier Lync versions); instead, the monitoring service is built into each Front-end server and shall be enabled.

0147 Monitoring data can share a SQL Server instance with other types of data. Typically, the call detail recording database (LcsCdr) and the Quality of Experience database (QoEMetrics) share the same SQL instance.

0148 The Monitoring role collocates on each Front-end server of each Front-end server pool. Monitoring databases collocate in the same SQL Server instance as the rest of the SfB databases.

3.1.3.2.5. Archiving

0149 Archiving agents are available on every Front End and will be enabled and configured. The archiving data storage shall be placed on a separate SQL instance provided by the database services and are not co-located with the SfB back-end databases to avoid Archiving disk space issues affecting the SfB service.

3.1.3.2.6. Back-End Tier

0150 Skype for Business Server relies heavily on SQL Server technology. Both Front-end and Monitoring Services require Back-end servers, which shall be collocated on the same SQL Server instance.

0151 In order to achieve high availability targets, SQL Server AlwaysOn Availability Groups (AGs) are deployed, with a DFS-R hosted file share witness. The back-end tier will be provided by the database service as described in section Database platform - Microsoft SQL Server for Skype for Business.

3.1.3.2.7. Office Online Server

0152 Skype for Business Server provides enhanced PowerPoint sharing features by using Office Online Server (OOS). OOS is a shared infrastructure allowing software such as Exchange Server, SfB, or SharePoint to have access to Office documents. The OOS architecture is described in section 3.1.6.2.

3.1.3.2.8. File Share

0153 Skype for Business Server requires a file share so computers throughout the topology can exchange files. The ON environment leverages DFS-R file shares for each Front-End Pool, as well as for each SQL AlwaysOn as a File Share Witness. The DFS-R file sharing service is to be implemented as part of core directory services (see also section describing Distributed File System)

3.1.4. Portal Services

0154 This section provides the concepts, architecture, and implementation strategy for the ECS Portal Services subservice, based on SharePoint. The latest NATO approved version of Skype for Business is to be implemented. The design in this document is based on SharePoint Server Subscription Edition.

3.1.4.1. Concepts

0155 The Portal Services architecture design includes the following core functional concepts:

1. **Security.** Ensures the implementation of a strict least-privilege model, with audited separation of duties. This includes ensuring the satisfaction of a number of key operational constraints, including:
   - Ensuring system administration tasks are performed using dedicated administrative accounts not used for daily interactive core business tasks.
   - Ensuring administrative accounts are isolated from production user accounts, treating the forest as the security boundary.
   - Ensuring SharePoint service applications and IIS Worker Process accounts use separate service accounts for isolation, and provide a virtual boundary of security.

- Ensuring all traffic – external from the end user to SharePoint and internal server-to-server communication within the SharePoint application itself – uses TLS encryption.
- Ensuring two-factor PKI-based user authentication. AD-FS shall be configured with SharePoint prior to the user migration. This will provide federation and will allow users outside of our domain to be federated within SharePoint.
- Implementing SharePoint-aware anti-malware scanning, while ensuring that SharePoint features are not blocked by the scanning

2. **Availability.** Ensures all SharePoint services load balance, properly size, and have at minimum N+1 redundancy as well as are fit for use over low bandwidth (<0.5Mbps) and high latency (>1sec) links.
3. **Scalability.** Ensures the infrastructure scales in response to increased application or user-based activity by leveraging on-premises server virtualization in conjunction with PowerShell automation and scripting.
4. **Recoverability.** Ensures the deployed SharePoint services meets a 4 hour Recovery Time Objective (RTO) and 8 hour Recovery Point Objective (RPO), including the ability to provide object level restore capabilities.
5. **Compatibility.** Ensures SharePoint services integrate with other line of business applications with a minimised level of effort and are compatible with all client office applications.
6. **Integrity.** Ensures the SharePoint Service provides standardized metadata tagging capabilities that map to the agency metadata standards for appropriate tagging, classification, and retention, or records management guidelines.
7. **Integration.** The Portal Service integrates with other ON services as follows:
   - The IaaS service provides networking services, including LAN services, F5 global load balancing, boundary protection, virtualization, backup, and storage services.
   - The CPS service provides Windows patching services as well as SharePoint Cumulative Patches through Microsoft Endpoint Configuration Manager.
   - The SMC service provides enterprise monitoring and logging services, as well as Windows anti-virus protection. SharePoint surfaces metrics to the Enterprise SMC tools, for the purpose of predicting growth and proactively adjusting resources. The SMC service maintains the data required to perform historical trend analysis of health and capacity usage.
   - Email Messaging for sending email notifications from SharePoint to Exchange Mail Servers
   - Database Services for hosting SharePoint configuration and content databases.
   - AD-FS Services for user authentication and authorization

3.1.4.2. High-Level Architecture

0156 SharePoint services centralize at the two datacentres (BEL-BRU-01 and ITA-LAG-01). This topology will be an active-passive configuration, where BEL-BRU-01 will remain the primary datacentre location, while ITA-LAG-01 is the secondary datacentre, which will be brought online only in case of a failure of primary datacentre.

0157 The Portal Services architecture includes the following key elements at each site:

- Centralized administration, via the Central Admin Server (CAS) role
- Authentication (AuthN) and Authorisation (AuthZ) Tier
- Web Services Tier
- Application Services Tier
- Data Tier
- Office Online Server
- McAfee Security for Microsoft SharePoint

- Management Server
- Workflow Manager
- My Sites – One Drive for Business

3.1.4.2.1. Server Sizing and Placement

0158 Highly redundant and globally load-balanced SharePoint Server farms deploy at each datacentre, to include:

- Multiple load-balanced front-end servers, the CAS management role will be hosted in application server, in support of remote management at the element manager and management domain level.
- Multiple Application Servers.
- Multiple load-balanced Workflow Servers
- Multiple clustered Back-End SQL Servers (See Database platform - Microsoft SQL Server for Central SharePoint Farm)
- A SharePoint Management Server

0159 Based on SharePoint Server Subscription Edition's new 'MinRole' architecture, ON Portal Services follows a 'medium/large farm' design. A medium/large farm design for high availability (HA) includes:

- Six web front-end servers
- Four distributed cache servers
- Four Application servers
- Two web front-end crawl servers
- Three Workflow Management servers
- Two Office Online servers
- Four Index / Query servers
- Four other component servers
- One SharePoint Management Server

0160 The back-end consists of two or more SQL Database servers configured in an always-on availability group.

0161 **Figure 15 ON SharePoint topology overview** shows the server placement corresponding to this architecture.

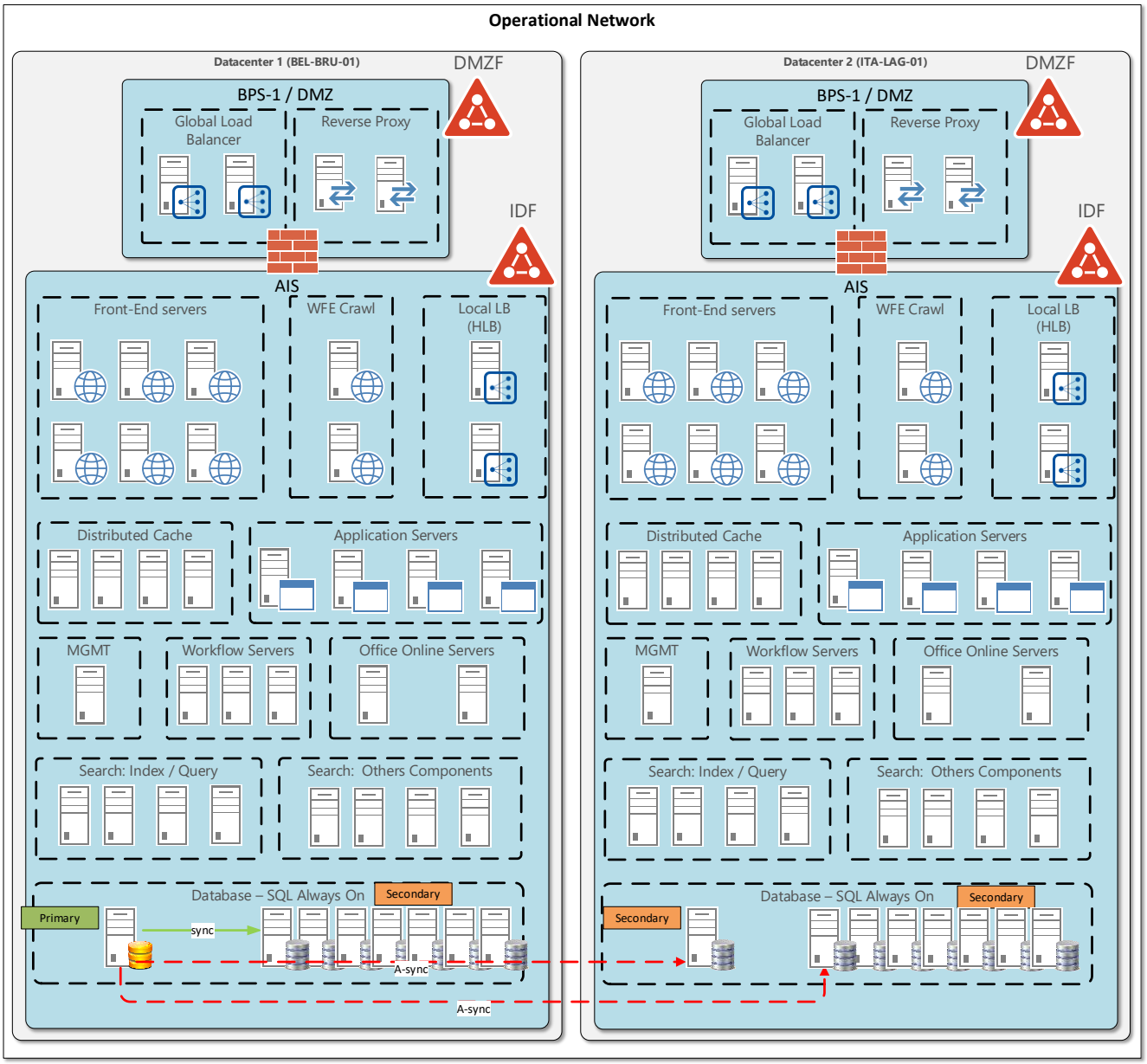

Figure 15 ON SharePoint topology overview

0162 A single SharePoint farm supports a maximum of 500 content databases. A single content database contains up to 4TB[16] of content, although the recommended maximum content database size is 200GB. As summarized in Error! Reference source not found., the ON Portal Service design for 1 farm supports:

- 20 SharePoint Web Applications
  - The legacy use of path-based URLs increases the number of Web Applications required to support the large number of URLs required at NATO.
  - The use of Host header site collection reduces the number of Web Applications. A single web application will be initially deployed.
- 25,000 MySites
  - The maximum supported number of MySite site collections is 500000 per farm. The current architecture easily supports 25000 MySites, without additional scaling.

[16] Only supported when the following requirement is met: Disk sub-system performance of 0.25 IOPS per GB. 2 IOPs per GB are recommended for optimal performance.

- Each ON Portal Service enclave provides MySite resources for each user, under the ON https://me.nato.int Web Application.

0163 More SharePoint farms may be required when limitations for a single farm are reached.

Web Application	Estimated Number of Site Collections in Web Application	Maximum GB Per Site Collection	Total Storage Required
we.nato.int	500	200 GB	100TB
me.nato.int	25000	1 GB	25 TB

Table 12 Sharepoint Sizing

3.1.4.2.2. Authentication (AuthN) and Authorisation (AuthZ) Tier

0164 AuthN within the main SharePoint Web Application occurs via AD-FS. Any legacy AuthN/AuthZ mechanisms (e.g., NTFS, Forms, etc.) will need to be changed to support PKI-based access through AD-FS, based on NATO PKI-issued user certificates. All AuthN/AuthZ functions will be performed using MFA and therefore cannot use a legacy authentication method.

0165 SharePoint is accessible external domains with an extended AD-FS token trust. The IDF on which the portal is hosted will establish trust between the external domain requesting access and the IDF that is hosting content.

3.1.4.2.3. Web Services Tier

0166 The web services tier consists of multiple SharePoint Web Front End (WFE) servers in a load-balanced farm. Each WFE standardizes to enable all software, patches, and plugins installations in an identical format. Should any WFE become unavailable, SharePoint services operate with no negative impact to users. This type of continuity augments the load balancing traffic based on the number of users leveraging the service and service availability via the IaaS load balancing service. The Web Tier is 100% virtual within each datacentre. The virtualization of this tier, and all subsequent tiers, provides the most flexibility to scale the architecture, either horizontally or vertically. This architecture ensures no loss of information when an error occurs, an operation fails or network connectivity becomes degraded. This design specifically accommodates use over low bandwidth (<0.5Mbps) and high latency (>1sec) links.

0167 The proposed design calls for six WFE Servers at each datacentre. Each WFE server is protected by McAfee VirusScan Enterprise and McAfee Security for Microsoft SharePoint.

0168 Certain guidelines and configuration settings perform on the WFEs to establish a baseline and best practice for SharePoint, to include:

(1) Logs – SharePoint logs. All SharePoint logs move to a separate partition on the virtual server itself, including ULS and IIS Logs.

(2) Page File – All systems, including the SharePoint WFEs, have a reduced page file ‘not OS managed’ and the page file move to a dedicated volume. The page file is normally 1.5 to 3 times the memory allocated to the system. The goal of virtualizing the systems is to leverage as much physical memory as possible while reducing disk contention. The page file adjusts in the event a memory dump is required.

(3) Only Web Services configure on the WFEs. No other SharePoint Service Applications configure. This allows the WFEs to only serve their intended purpose.

(4) The McAfee Firewall configures only specific ports required for the use of SharePoint. This includes Web Service ports, 80/443 for inbound communication and any outbound communication to the other servers within the SharePoint farm.

0169 Web Application Firewall (WAF) and Web Content Filtering (WCF) capabilities implement protection for the SharePoint farms from security threats like Distributed Denial of Service (DDoS) attacks, Web Services (e.g., XML) attacks, and SQL Injection and Cross Site Scripting (XSS). These functionalities will be deployed as part of IaaS.

3.1.4.2.4. Application Services Tier

0170 The Application Services Tier is a SharePoint-centric component that provides a highly resilient and fault-tolerant Shared Service Applications layer. This tier provides additional services besides standard HTTP calls leveraged to further enhance the user's overall experience and use of the system. All service applications deploy within the overall SharePoint Service Design, including those that are key to the overall use of SharePoint, including SharePoint Enterprise Search and Office Web Applications. All traffic to and from the SharePoint Application Services Tier is TLS encrypted.

3.1.4.2.5. Distributed cache

0171 SharePoint's Distributed Cache architecture is a flexible service within SharePoint and manages the Logon Token Cache holds claims-based authentication session tokens. The Distributed Cache is automatically tuned to support up to 10,000 concurrent users and will be hosted on dedicated servers to support a large user base.

3.1.4.2.6. Managed Metadata Services

0172 Managed Metadata Services is used to build upon and enhance the information architecture within SharePoint by allowing administrators the ability to create managed terms (e.g., classification labels) associated to Web Applications, Site Collections, and custom content types. Administrators may define a controlled list of terms to allow the farm to follow a standardized data labelling scheme, to include terms or phrases to help enhance both the Enterprise Search experience, farm security, and the filtering of web parts that present data to the user page.

3.1.4.2.7. Enterprise Search

0173 Of all the Service Applications within SharePoint, Enterprise Search is the most important of the Service Applications. Enterprise Search configures and enables the crawl of all web-based content within SharePoint itself. ECS automates the Enterprise Search with the exception of crawl schedules, additional/external content sources, and the actual architecture itself. From an architectural standpoint, the crawler is the device performing the crawling of content within any source (including internal SharePoint content). Its responsibility is to crawl content based on predefined iFilters, and to push discovered information to the Service Application's database. The WFEs run a query service to look locally for a copy of all the searched content previously collected by the crawler and present the end user with a result. The data itself, once crawled, gets published to a file share on each WFE. This automated file share has permission for the appropriate accounts to crawl it.

3.1.4.2.8. MySites

0174 MySites deploys throughout the enterprise farms at both active farm in BEL-BRU-01 and passive farm ITA-LAG-01. User MySites pages publish to AD for easy end-user access and discovery. The most important MySites configuration is with respect to total size of the personal site for each user and who can leverage the service. This threshold of size is scoped at 1GB but may be revisited during farm deployment. MySites is customized by applying NATO provided template and configuration options.

Workflow Services

0175 The workflow engine in SharePoint Server Subscription Edition allows users to build complex workflows and leverage the latest technology within the Microsoft Service Bus architecture. The Service Bus presented is a dedicated and required Service Bus for the use of SharePoint

only. It is not the same service bus used by BizTalk or any other component within Microsoft. This Service Bus is simply for coordinating actions within sites that leverage complex workflows. These enhanced capabilities include:

- A visual workflow development experience that uses a Visio 2013 add-in
- A new action that enables no-code web service calls from within a workflow
- New actions for creating a task and starting a task process
- New coordination actions that let you start a workflow built on the SharePoint 2010 Workflow platform from a workflow built on the SharePoint 2013 Workflow platform
- A new Dictionary type
- New workflow building blocks such as Stage, Loop, and App Step
- High Density and Multi-Tenancy
- Elastic Scale
- Activity / Workflow Artefact Management
- Tracking and Monitoring
- Instance Management
- Fully Declarative Authoring
- REST and Service Bus Messaging
- Managed Service Reliability

0176 Workflow is backwards-compatible with previously created workflows built within the new workflow engine. While it is supported to build and execute the older class of workflows, it is highly recommended all future workflows create and execute within the SharePoint Server Subscription Edition Workflow Manager. SharePoint leverages the app-fabric bus to execute and maintain the state of the workflow.

3.1.4.2.9. Data Tier

0177 The Data Tier is the most critical tier in the overall SharePoint Service architecture. This tier includes almost 98% of all the data placed within SharePoint, including web pages, list items, documents, images, and video. All SharePoint services require a stable, resilient and highly available data architecture. The data architecture consists of multiple SQL Server instances in an AlwaysOn–enabled cluster. The cluster itself is a Windows cluster where the AlwaysOn availability group listeners are published for exclusive WFE and Application Tier use.

0178 SQL Servers are configured in an Always on High Availability and Disaster Recovery fashion, each pair of SQL Servers contains at least one Availability group with a maximum of 20 Databases per AG

0179 Availability groups are configured with one primary node and one secondary node in the BEL-BRU-01 (active) site and one or more secondary nodes in ITA-LAG-01 (passive) site.

0180 The data replication between the primary and secondary node in BEL-BRU-01 is made synchronously, the data replication between the primary node in BEL-BRU-01 and the secondary nodes in ITA-LAG-01 are made asynchronously.

0181 Automatic failover can occur between any of the nodes within the active BEL-BRU-01 site, however only manual failover is possible to the passive ITA-LAG-01 site.

0182 Separating the SP Config and Services Databases from any SP Content Databases is common in large environments requiring resiliency. This type of design allows for the scaling of services either vertically or horizontally.

3.1.4.2.10. Office Online Server

0183 SharePoint leverages the OOS farm described in Section **3.1.6.2**. All SharePoint OOS Web Service calls are secured via TLS.

3.1.4.2.11. McAfee Security for Microsoft SharePoint

0184 McAfee Security for Microsoft SharePoint deploys into the farms. This toolset ensures a SharePoint deployment does not spread malware, store inappropriate content, or lead to data loss. Key product features include:

- Malware scanning of all content upload, including virus scanning and malicious code threats.
- Real-time and scheduled scans of Web Applications, websites, folders and specific file types.
- Rule-based content filtering, to prevent inappropriate or unauthorized content downloads and uploads.
- Central management and reporting, integrated with McAfee ePolicy Orchestrator.
- Enhanced quarantine management.

3.1.4.2.12. Backup and Recovery

0185 The backup and restore of SharePoint SQL Server databases will be performed by the IaaS Backup and Recovery service based on VEEAM.

- The following items will be included in the backup:
- All SharePoint Content within the ContentDBs (documents, list items, web pages, workflows, customizations through Designer)
- All SharePoint Service Application Data including Enterprise Search
- System State, IIS Metabase, Registry
- Custom Code, any DLLs located on the local system used by SharePoint Workflows
- Unified Logging System (ULS) Logs, IIS Logs

3.1.4.2.13. Management Server

0186 The design calls for a single Management Server to allow for third-party tools requires a console application to function. The server runs the following tool sets:

- Windows Task Manager – schedules tasks for reporting information or consolidation of ULS logs
- ULS Viewer – analyses ULS logs in real-time during day-to-day operations of SharePoint
- PowerShell – manages farm-wide functions and for reporting of health within SharePoint

3.1.5. Database Platform Services

0187 This section provides the concepts, high-level architecture, and implementation strategy for the Database services.

3.1.5.1. Concepts

0188 The Database service architecture design contains the following core functional concepts:

(1) **Security.** To ensure the implementation of best security practices for database platforms, we include:

(2) A strict least privilege model, with audited separation of duties.

(3) Disabling of SQL Authentication mode on the SQL servers, especially in AG configurations.

(4) Login synchronization between SQL Server nodes in AG configurations

(5) **Availability.** SQL Server databases are configured in Always on High Availability Groups with Disaster recovery solution which ensure that we meet the expected SLA agreement in terms of service availability and disaster recovery. For the DR location, the database synchronization is performed asynchronously and failover to the DR location will only be performed manually.

(6) **Scalability.** We ensure the infrastructure can scale in response to increased demand for database services, either for end users or applications.

(7) **Recoverability.** The deployed SQL Server database platforms environment is resilient and fully recoverable, within established limits.

(8) **Interoperability.** The database platforms are capable of supporting applications that require different versions/components of SQL Server and associated tools.

3.1.5.2. High Level Architectures

0189 All databases will be hosted on a virtual platform leveraging VMware as described in the Service Design Package – Infrastructure as a Service (IaaS).

0190 The database services will provide centralized databases for core services and functional applications. **Table 13 Core applications requiring database services** below provides an initial overview of the services from ECS, IaaS and SMC that require databases. Where required, database servers will be dedicated to a single application, such as SharePoint or Skype for Business. Some databases not requiring a lot of resources or performance shall share database instances where possible, taking into account SQL DB version, security zone, AD domain, physical location and high availability requirements.

0191 Databases at the Datacentre locations will be hosted on dedicated ESX cluster(s) in order to optimize the license costs, based on CPU sockets/cores. Databases at Enhanced nodes will share the load with other generic compute workloads. Initially 12 different SQL cluster types are identified to be required. This is to be reviewed upon finalizing the low level design. (See also Service Placement).

Core applications requiring Database Services	Location(s)	VCF Domain	AD Domain	Service Area	DB Type
Skype for business	Both DC	workload	IDF	ECS	SQL
SharePoint Central Farm	Both DC	workload	IDF	ECS	SQL
MS Systems Center Operations Centre (SCOM)	Both DC	workload	SVF	CPS	SQL
McAfee ePolicy Orchestrator	Primary DC	workload	SVF	CPS	SQL

Core applications requiring Database Services	Location(s)	VCF Domain	AD Domain	Service Area	DB Type
Titus Classification suite	Primary DC	workload	SVF	ECS	SQL
VMware vRealize Automation	t.b.d.	management	SVF	IaaS	SQL
VEEAM One (Backup and Archive)	Both DC	management	SVF	IaaS	SQL
VMware Horizon	All VDI locations	workload	SVF	CPS	SQL
VMware App Volumes	All VDI locations	workload	SVF	CPS	SQL
MS Endpoint Configuration Manager	Primary DC	workload	SVF	CPS	SQL
BMC Remedy ITSM / SSO and TrueSight Orchestration (TSO)	Both DC	workload	SVF	SMC	SQL
BMC TrueSight Capacity Optimization / Operation Management (TSOM/TSCO)	Both DC	workload	SVF	SMC	Oracle
MS Identity Manager	Both DC	workload	SVF	ECS	SQL
Privileged Access Management	Both DC	workload	SVF	CS	t.b.d.
Remote Desktop Services (RDS) for administrators	Both DC	workload	SVF	CPS	SQL
Remote Desktop Services (RDS) for users	Both DC	workload	IDF	CPS	SQL

Table 13 Core applications requiring database services

0192 The detailed list of all database clusters currently identified are listed in the Service Placement document.

0193 The database high level architectures will consist of the following types of database integrations:

(1) SfB is deployed in an Active/Active manner in the IDF. The data replication is provided at application level, therefore the database architecture consists of two independent clusters with local HA only.

(2) SQL Farm for the Central SharePoint Service (See Portal Services) will be deployed using Multi-site Active/Passive deployment using dedicated SQL cluster in the IDF. Local HA in the active farm leveraging synchronous and a-synchronous commit to the passive farm.

(3) MS System Center operations Manager (SCOM) is deployed in an active-active manner leveraging the duplicate SCOM management group[17] in the SVF. This requires two independent clusters with local HA (similar to SfB database layer).

(4) McAfee E-policy Orchestrator, Titus classification suite and MS Endpoint Configuration Manager (MECM) are only deployed at the primary datacentre (BEL-BRU-01) on the SVF. It will be integrated with VMware Site Recovery Manager (SRM) to fail-over to the secondary datacentre (ITA-LAG-01) in case of a disaster. Therefore, only a single

[17] https://learn.microsoft.com/en-us/system-center/scom/plan-hadr-design?view=sc-om-2022

database cluster will be required configured as Always-On providing local HA. It will be integrated with the DR replication and SRM mechanisms provided by the IaaS.

(5) VDI requires database support for Horizon and AppVolumes services. VMware Horizon will be hosted in the SVF at locations providing VDI services. There is no fail-over required for these back-end services, however, it will leverage the same cluster used for AppVolumes, which does require to be highly available at the local site. The Horizon and AppVolumes databases are therefore hosted on a two node SQL Always-On cluster at each site that has a VDI infrastructure.

(6) Remote Desktop Services are deployed for two purposes: Once for administrators providing administrative tools accessed only by administrators and once for specific user applications to be accessed by the user community. The RDS farm for administrators will be hosted in the SVF at both datacentres, the service for the user community will be hosted on the IDF in both datacentres. For both RDS Farms, local SQL Always-On clusters will be implemented.

(7) The BMC Remedy ITSM suite provides integrated ITIL functionality across the Service Management processes. Remedy Single Sign-On (RSSO) is an add-on to the Remedy platform. TrueSight Orchestration (TSO) is a general purpose workflow execution engine allowing integrations between many products with full implementation of business logic and controls. These services are to be implemented in both datacentres in an active/passive fashion, leveraging SQL Always-ON to provide the database services.

(8) BMC TrueSight Operations Management (TSOM), with TrueSight Capacity Optimization (TSCO), provide the interfaces for performance monitoring, event management, resource planning, and optimization of ON components and resources. These services are to be implemented in both datacentres in an active/passive fashion, based on Oracle databases leveraging Oracle Data Guard to provide high availability in case of a disaster.

(9) MS Identity Manager (MIM) will be deployed using Multi-site Active/Passive deployment using dedicated SQL cluster in the SVF. Local HA in the active farm leveraging synchronous and a-synchronous commit to the passive farm.

(10) Privileged Access Management (PAM) will be used to designate special access or abilities above and beyond that of a standard user. Privileged access allows securing infrastructure and applications, maintaining the confidentiality of sensitive data and critical infrastructure. The tool and architecture for PAN is at this moment not hence no database design can be made at this point.

(11) VMware vRealize Automation. The deployment for this service hosted on the management cluster requires to be highly available. The exact HA architecture is to be worked out in the IaaS subservice, after which the SQL architecture can be determined.

(12) VEEAM One is responsible for collecting data from Veeam Backup & Replication servers, and storing this data into the database. The architecture for VEEAM one is to be defined, including the requirements for the SQL database architecture.

3.1.5.2.1. Database platform - Microsoft SQL Server for Skype for Business

0194 SfB is deployed in an active/active manner at application level. Data replication is established using SfB pool-pairing. Independent SQL Always-On clusters are required providing local HA **(Figure 16 HA Database Cluster architecture for Skype for Business and SCOM**) with following characteristics:

(1) Two WSFCs will be used, one at each datacentre, hosted together with the application in the IDF.

(2) SQL Servers within a datacentre are configured in an Always on High Availability fashion.

(3) Each pair of SQL Servers contains at least one AG with a maximum of 20 Databases per AG

(4) Each AG within a datacentre is configured to have the following structure: one primary node and one secondary node.

(5) The data replication between the primary and secondary node is made synchronously

(6) Automatic failover can occur between any of the nodes within a datacentre

(7) Cross site redundancy is achieved at application level by SfB Pool Pairing methodology.

(8) Strict settings will be implemented for supporting SfB virtual deployment on VMware.

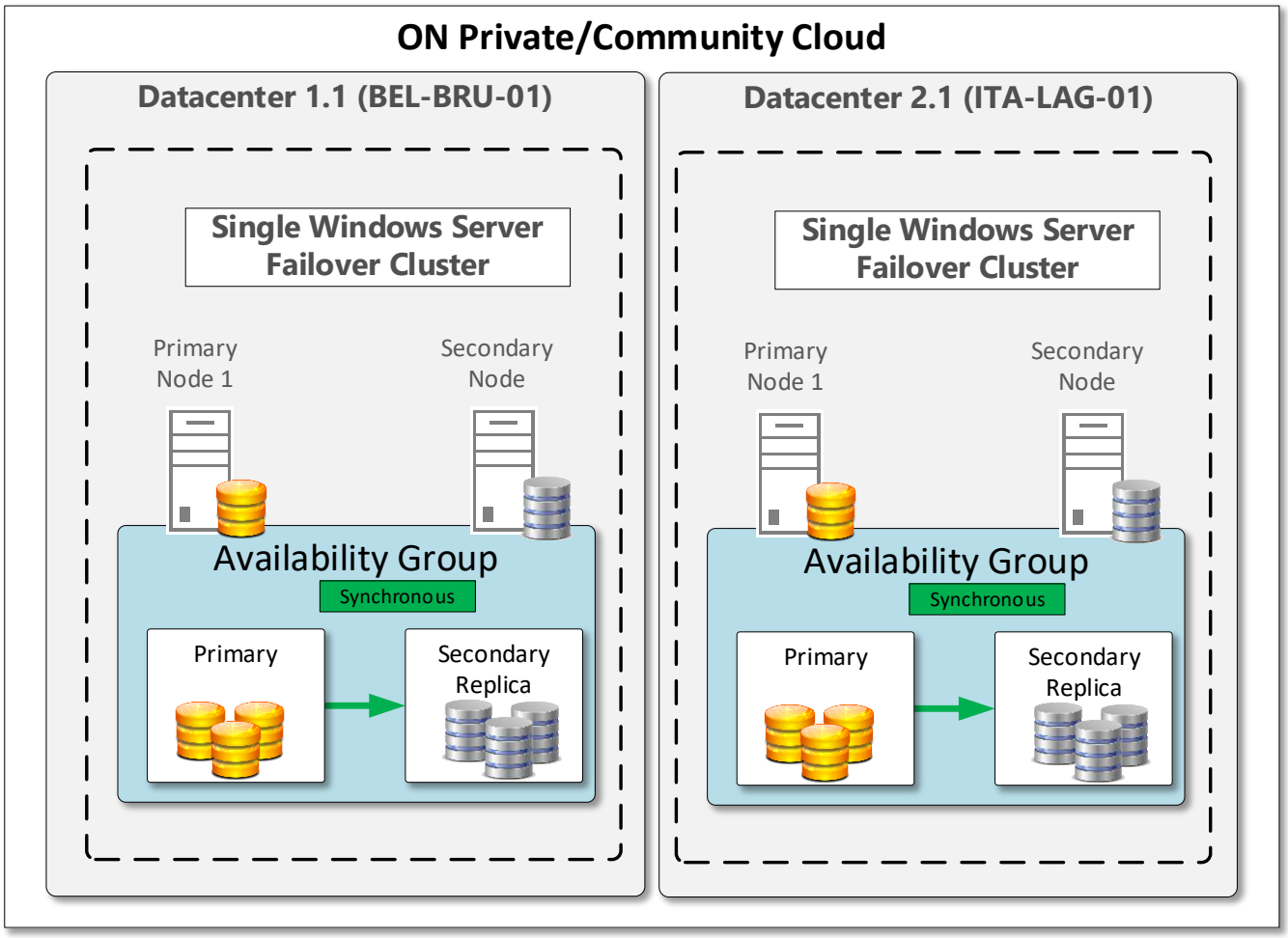

Figure 16 HA Database Cluster architecture for Skype for Business and SCOM

3.1.5.2.2. Database platform - Microsoft SQL Server for Central SharePoint Farm

0195 The database service for the Central SharePoint Portal (See Portal Services) is described in this section. It requires a multi-site Active/Passive deployment using dedicated SQL cluster. Local HA in the active farm leveraging synchronous and a-synchronous commit to the passive farm. (**Figure 17 SQL Active Passive with Always On Availability Groups for SharePoint Central Farm**)

0196 A single Windows Server Failover Cluster (WSFC) will be used across both datacentres, hosted together with the application in the IDF.

- SQL Server design can be converted to a distributed AG topology [18] if a multi datacentre or multiple DR nodes will be required for each AG.

0197 SQL Servers are configured in an Always on High Availability Active/Passive fashion between the 2 datacentres.

0198 Each datacentre contains at least one Availability Group (AG) with a maximum of 20 Databases per AG.

0199 Each AG is configured to have four nodes: one primary node and one secondary node in the primary datacentre (BEL-BRU-01) and 2 secondary nodes in the secondary datacentre (ITA-LAG-01). It is estimated that 6 primary SQL nodes are required, hence a total of 24 SQL nodes in total for this farm.

0200 The data replication between the primary and secondary nodes in the primary datacentre (BEL-BRU-01) is made synchronously.

0201 The data replication between the primary nodes in the primary datacentre (BEL-BRU-01) and the secondary nodes in the secondary datacentre (ITA-LAG-01) is made asynchronously. This is due to the latency between the primary and secondary datacentre where synchronous replication is not possible.

0202 Automatic failover can occur between any of the nodes in the primary datacentre (BEL-BRU-01)

0203 Only manual failover is allowed to the secondary datacentre (ITA-LAG-01)

[18] https://learn.microsoft.com/en-us/sql/database-engine/availability-groups/windows/distributed-availability-groups?view=sql-server-ver16#disaster-recovery-and-multi-site-scenarios

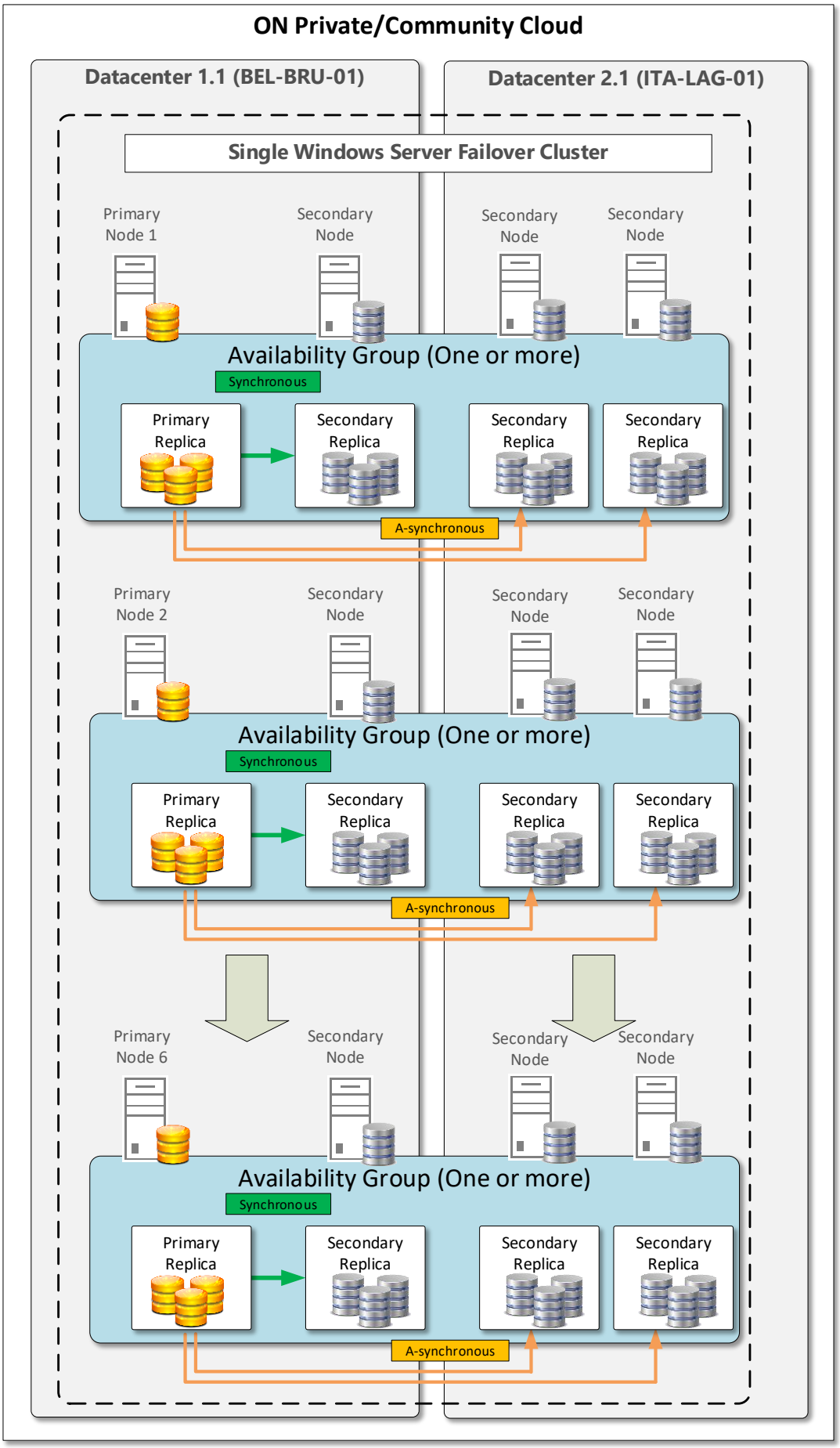

Figure 17 SQL Active Passive with Always On Availability Groups for SharePoint Central Farm

0204 The database tier includes almost 98% of all the data placed within SharePoint, including configuration databases, content databases and service management databases (e.g.: Search, Workflow, MMS, Extranet Manager). All SharePoint services require a stable, resilient and highly available data architecture. The data architecture consists of multiple SQL Server instances in an AlwaysOn–enabled cluster. The cluster itself is a Multi-Subnet Failover cluster where the AlwaysOn availability group listeners are published for exclusive WFE and Application Tier use.

0205 Data synchronously replicates between the AG nodes within the primary datacentre (BEL-BRU-01), and provides Application resiliency in conjunction with data protection if a system were to sustain any downtime. The nodes residing in the primary datacentre will be configured to synchronously commit transactions and with automatic failover enabled. The DR nodes located in the secondary datacentre (ITA-LAG-01) are configured as an exact same replica of the nodes in the primary datacentre with the difference that the Availability Groups are configured to be asynchronous commit and manual failover. Based on a case by case scenario, the bandwidth between the replicas in the primary datacentre and the secondary datacentre should be enough to sustain the continuous flow of transaction.

0206 The SQL architecture itself provides a stretched cluster environment in the form of multi-subnet failover cluster where nodes within the same cluster are in different locations. The automated failover process provides ease of administration if an unplanned outage occurs. This requires a file share witness hosted on the DFS-R infrastructure (ref. Distributed File System) at each datacentre.

0207 Each SQL Server Always On implementation requires a Windows Failover Cluster (WFC). The WFC publishes the Availability Group Listener using both the DNS FQDN, and IP addresses responsible for allowing SharePoint to connect to the underlying SQL Server instance. Two IP addresses are required for each AG from both the BEL-BRU-01 and ITA-LAG-01 subnets in order to create an extended Availability Group. Unlike traditional SQL Server failover clusters, each node within the AlwaysOn Cluster has a dedicated SQL Server instance unaware of any partners within the environment. The dedicated instances run individually, and only communicate through a heartbeat network which belongs to the Windows Cluster for the purposes of creating and servicing the Availability Group.

0208 The Windows Cluster Name Object (CNO) itself is only created for administrative purposes. Neither end users nor the SharePoint system itself connect directly to the Windows Cluster name. The Availability Group Listeners are the sole connection point for SharePoint.

0209 The only exceptions are the SessionState and Usage and Health databases, which will not be added to an Availability Group. The connection strings will use the server name on which they are created. Both SessionState and Usage and Health databases will be kept in Simple recovery model in order to avoid uncontrolled growth of the log files. Any other databases which do not require adding to the AG will be discussed on a case by case basis.

0210 In both instances, Active Directory creates a virtual CNO for the Availability Groups and the cluster. By using a multi-subnet failover clusters, all the AG CNOs will require an IP address corresponding from each subnet in which the actual servers are created. At any given point, only one IP address will be online in WSFC and reply to ping in order to prevent round-robin situations.

0211 Separating the SP Config and Services Databases from any SP Content Databases is common in large environments requiring resiliency. This type of design allows for the scaling of services either vertically or horizontally. In SharePoint, adding more SQL Server AlwaysOn Cluster nodes (i.e., ‘scaling out’) is usually the best route. The separation of the SP Configuration databases is done even more granularly since an availability group is created for SP Config DBs and one AG for Service databases. If particularly required, the Service databases can be separated from all the other configuration databases and have their own cluster, two or more SQL Servers, one or more AGs dedicated, otherwise the service

databases can be hosted in the same cluster and SQL Server nodes as the other configuration databases.

0212 In terms of Configuration/Services the databases do not get synchronized between BEL-BRU-01 and ITA-LAG-01 which means that there will be a completely different set of AGs for BEL-BRU-01 Configuration/Services and ITA-LAG-01 Configuration/Services and implicitly a different set of databases.

0213 Only Availability Groups dedicated to the content databases get extended to ITA-LAG-01 and, on ITA-LAG-01 side, the content databases will only be available for read-only purposes.

0214 Microsoft Best practices suggest that no SharePoint content database should be bigger than 200GB. Also, each database file will be stored on a different VM disk.

0215 In terms of storage workload configuration, best practices[19] for running SQL on VMware VSAN are to be applied leveraging Storage Policy Based Management (SPBM).

0216 A VM disk design figure is presented below for an overview of a generic configuration

DISK DESIGN TEMPLATE						C	D	G	I	J	O	P	
							LUN1	LUN4	LUN6	LUN7	LUN10	LUN11	
OS	Edition	Purpose	Host Name	vCPUs	RAM	OS2	SYSTEM DB	TEMP DB	DATA	DATA	LOG	LOG	Disk Summary
WIN 2K19	Standard	Config	XXXXXXXX	8	32	150	50	200					400
WIN 2K19	Standard	Config	XXXXXXXX	8	32	150	50	200					400
WIN 2K19	Standard	Content	XXXXXXXX	4	48	150	50	200					400
WIN 2K19	Standard	Content	XXXXXXXX	4	48	150	50	200					400
WIN 2K19	Standard	Content	XXXXXXXX	4	48	150	50	200					400
WIN 2K19	Standard	Content	XXXXXXXX	4	48	150	50	200					400

Figure 18 VM Disk Design

i) The SQL Server components will be installed on a dedicated VM disk, not on the default C drive

ii) The page file will also be moved to another dedicated drive, or the D drive.

0217 The following is breakdown of the SharePoint SQL layout as it pertains to this architecture:

- There are a total of sixteen SQL servers, with eight servers at each datacentre (BEL-BRU-01 and ITA-LAG-01).

3.1.5.2.3. Database platform - Microsoft SQL Server for SCOM

0218 SCOM is deployed in an active-active manner leveraging the duplicate SCOM management group. This requires two independent clusters with local HA (similar to SfB database layer – **see Figure 19 Database layer for e-Policy Orchestrator – Primary DC only with DR leveraging SRM**). The Service Design Package – Client Provisioning Services (CPS) describes in detail the architecture of SCOM using duplicate management groups.

3.1.5.2.4. Database platform - Microsoft SQL Server for e-Policy Orchestrator, Titus Classification suite and MECM

0219 As described in the Service Design Package – Client Provisioning Services (CPS), McAfee E-policy Orchestrator is only deployed at the primary datacentre (BEL-BRU-01). It will be integrated with VMware Site Recovery Manager (SRM) to fail-over to the secondary datacentre (ITA-LAG-01) in case of a disaster. (**Error! Reference source not found.**) HA within the datacentre is still required and provided by a two node WSFC Always-On AG architecture. The same configuration applies to the Titus Classification service, as described

[19] https://blogs.vmware.com/virtualblocks/2019/03/26/considerations-for-running-microsoft-sql-server-workloads-on-vmware-vsan/

in 3.1.6.1. as well as the MS EndPoint Configuration Manager (MECM) as described in the Service Design Package – Client Provisioning Services (CPS)

0220 All these services will be hosted in the Service Forest.

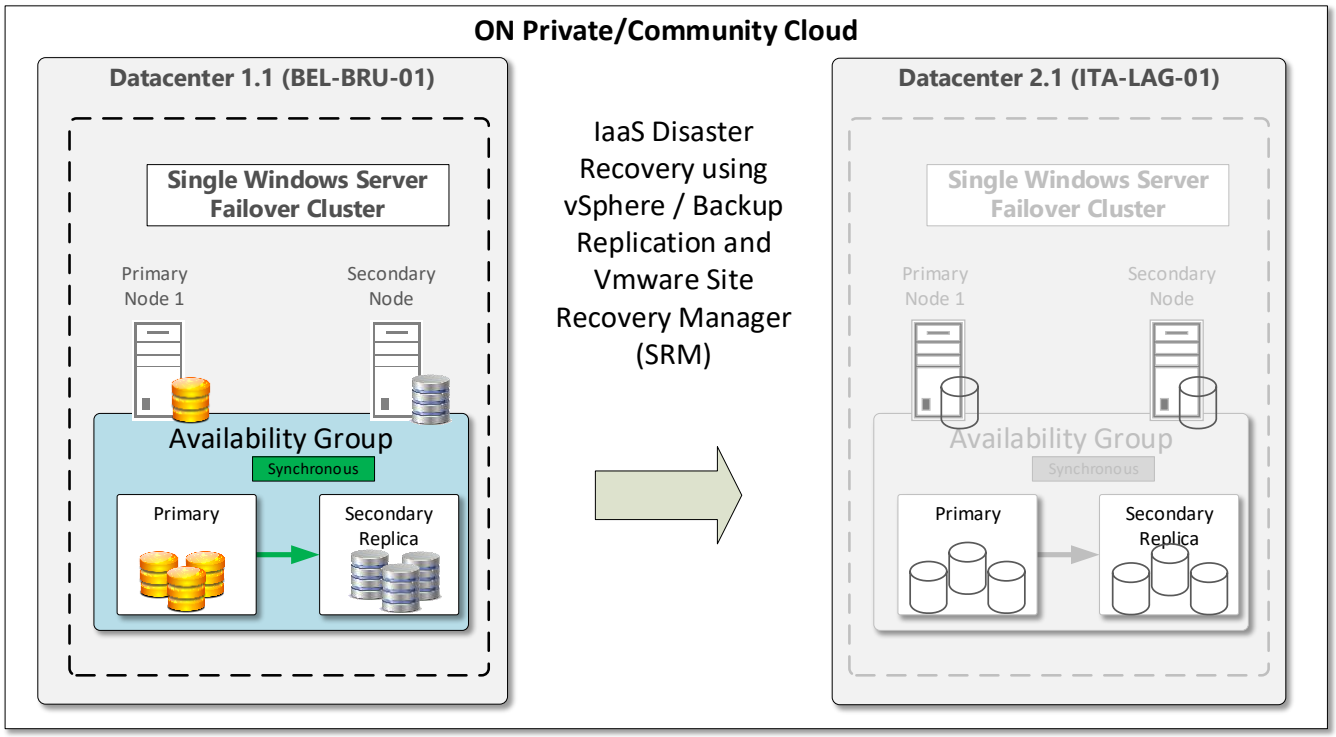

Figure 19 Database layer for e-Policy Orchestrator – Primary DC only with DR leveraging SRM

3.1.5.2.5. Database platform - Microsoft SQL Server for VMware Horizon and VMware AppVolumes

0221 VMware Horizon utilizes a local SQL Server database for tracking user session data such as logins and logouts and auditing administrator activities that are performed in the Horizon Administrator console. No fail-over of the Horizon database is required.

0222 App Volumes uses a Microsoft SQL Server database to store configuration settings, assignments, and metadata. This database is a critical aspect of the design, and it must be accessible to all App Volumes Manager servers. An App Volumes instance is defined by the SQL database. Multiple App Volumes Manager servers may be connected to a single SQL database.

0223 As AppVolumes require HA, a local two-node SQL Always-On cluster is foreseen to host both AppVolumes and Horizon databases. **See Figure 20**.

0224 In case of a disaster at a local site, clients are to be re-directed to the Horizon and AppVolumes servers of their assigned disaster recovery datacentre node.

0225 The VMware Horizon and AppVolumes implementation is described in the Service Design Package – Client Provisioning Services (CPS)

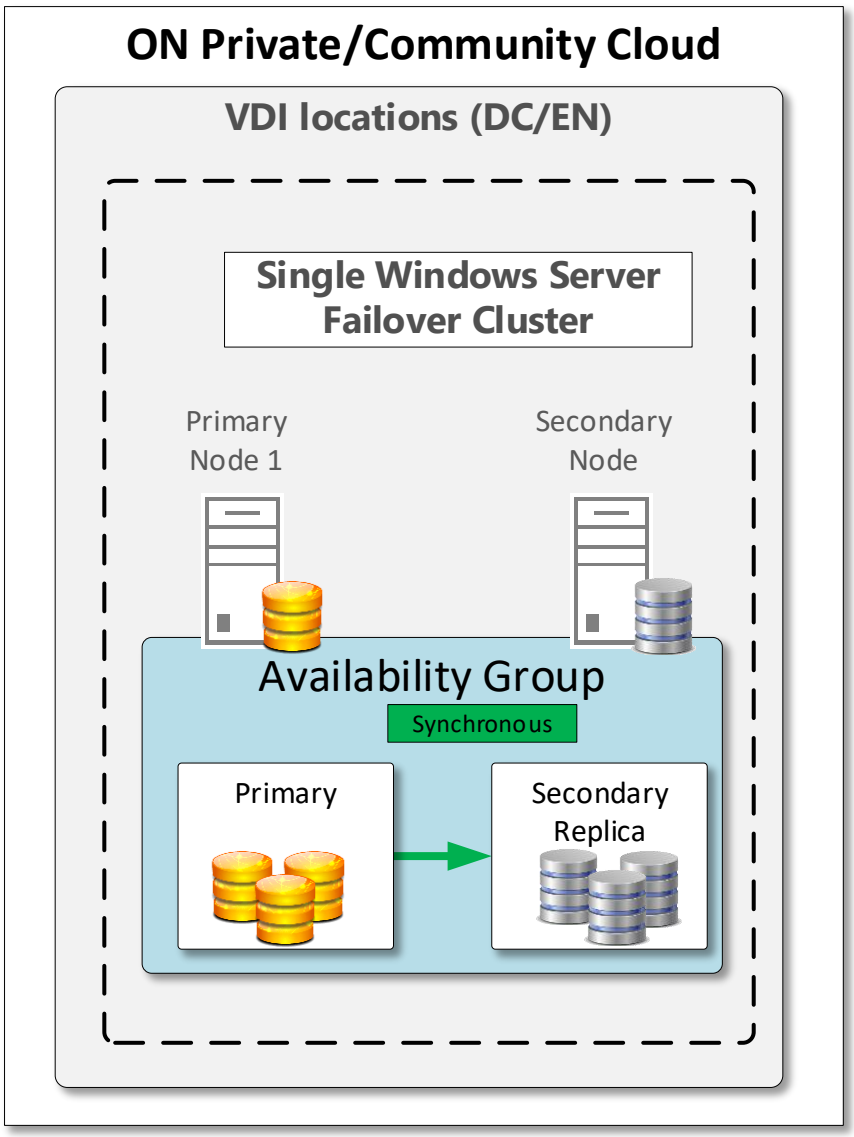

Figure 20 SQL Always-On cluster to support VDI

3.1.5.2.6. Database platform - Microsoft SQL Server for RDS

0226 The RDS services are described in the Service Design Package – Client Provisioning Services (CPS). For each purpose, RDS user applications and RDS admin applications farms, a local SQL Always on cluster will be used at each datacentre location, providing local and cross-site high availability. As the two different farms are to be implemented in different forests and both datacentres, a total of 4 RDS farms including SQL clusters are to be deployed. See **Figure 21 SQL Farms for RDS.**

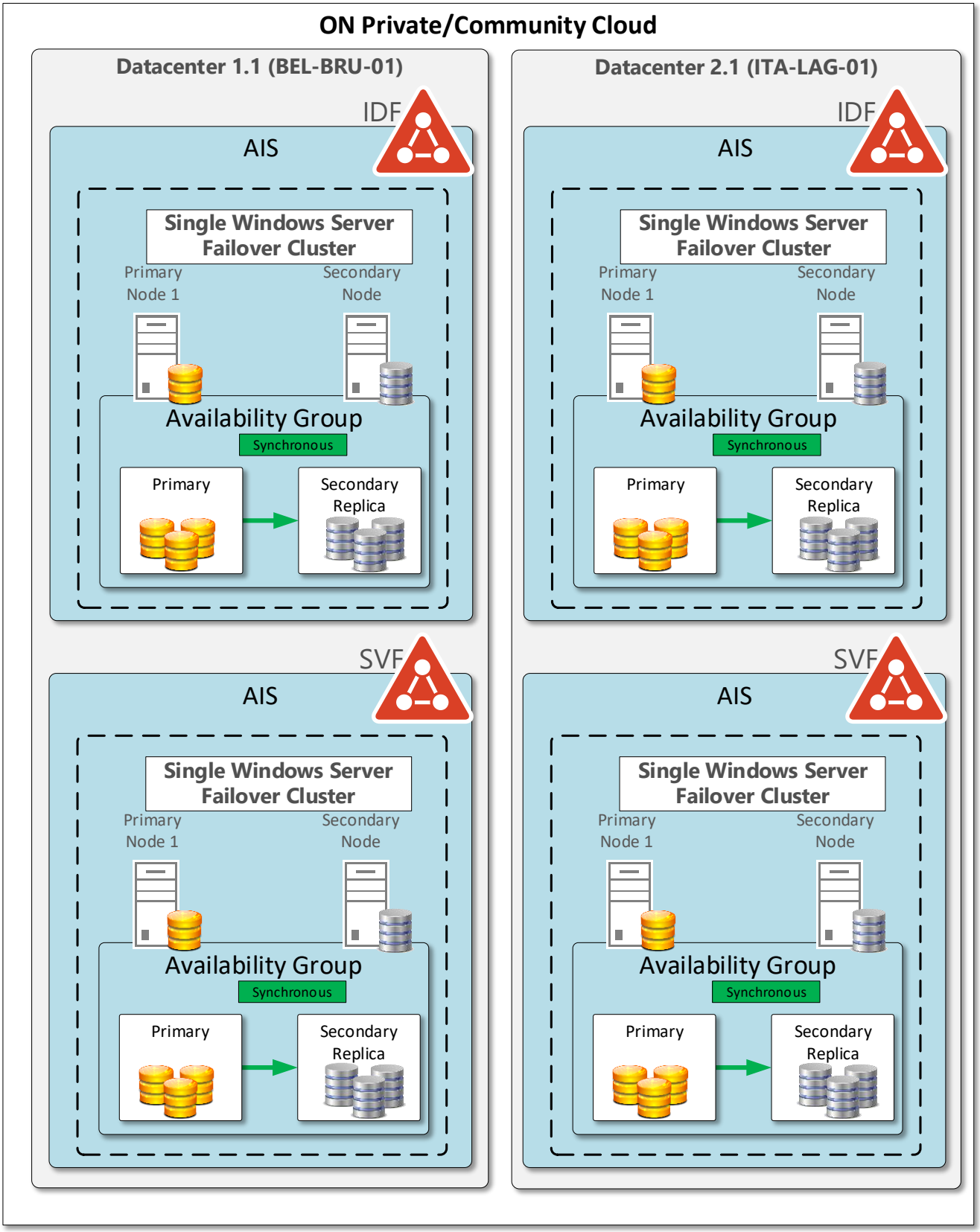

Figure 21 SQL Farms for RDS

3.1.5.2.7. Database platform - Microsoft SQL Server for BMC Remedy ITSM, SSO and TSO.

0227 The BMC Remedy ITSM suite with add-on Remedy Single Sign-On (RSSO) as well as TrueSight Orchestration (TSO) are deployed in active/passive mode between the two datacentres. All three services can share the database SQL servers which will provide local HA within the datacentre, and fail-over to the other datacentre for DR purposes. A two-node

SQL Always on cluster with AG's will be implemented per datacentre as depicted **in Figure 22 Active/Passive SQL Windows Server Failover Cluster for BMC Remedy ITSM/SSO and TSO.**

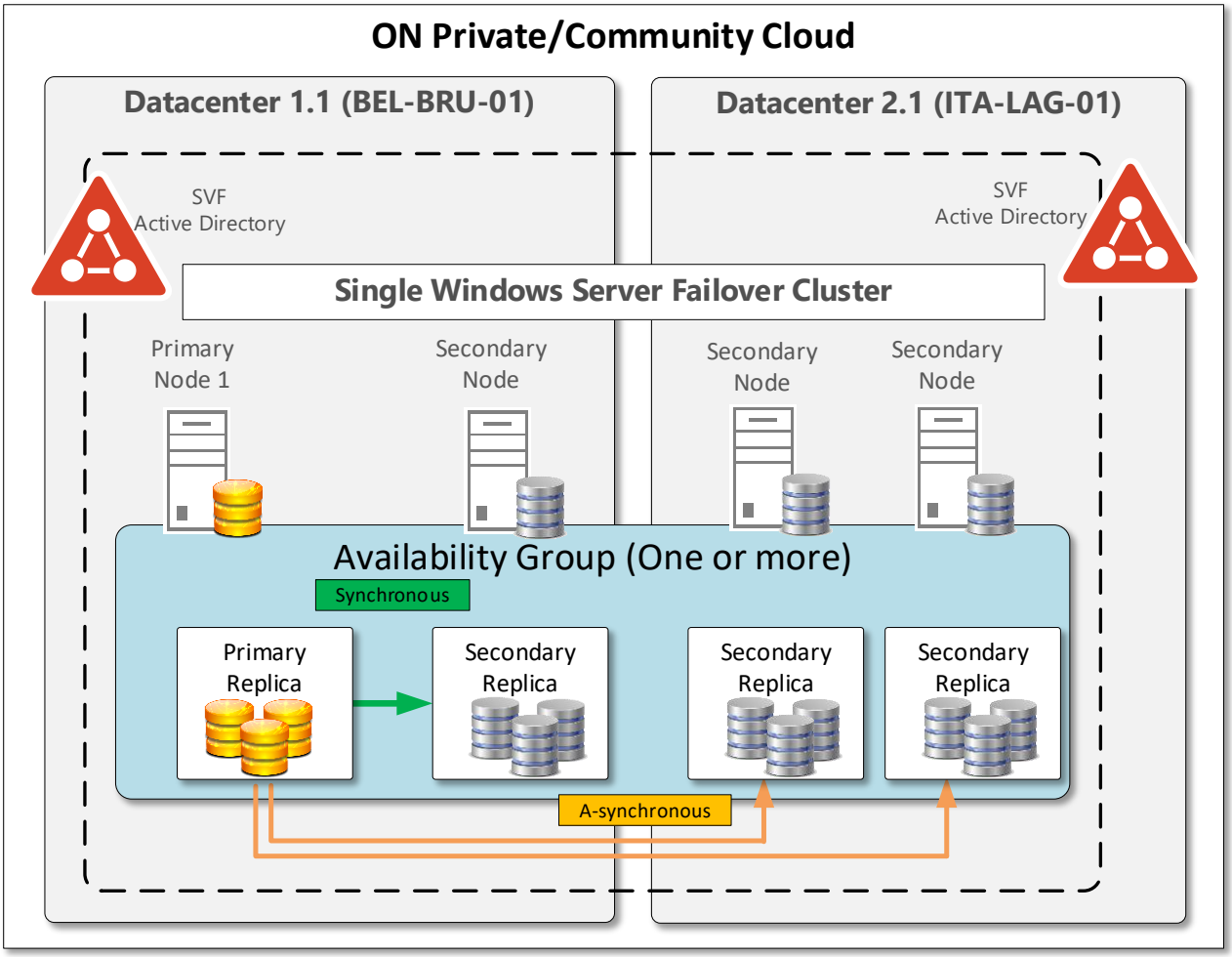

Figure 22 Active/Passive SQL Windows Server Failover Cluster for BMC Remedy ITSM/SSO and TSO

3.1.5.2.8. Database platform - Oracle Server for BMC Truesight Capacity Optimization and Operation Management

0228 BMC TrueSight Operations Management (TSOM), with TrueSight Capacity Optimization (TSCO) are deployed in active/passive mode between the two datacentres. Two-node Oracle Real Application Clusters (RAC) will be hosted at each datacentre leveraging RAC to provide high availability within the datacentre and Oracle Data Guard to provide DR across the datacentres.

0229 Oracle Data Guard is a high availability and disaster-recovery solution that provides very fast automatic failover. Furthermore, the standby databases can be used for read-only access.[20]

3.1.5.2.9. Database platform - Microsoft SQL Server for MIM

0230 The MIM service as described earlier in section Microsoft Identity Manager (MIM) of this document will be implemented in an active/passive manner in the datacentres leveraging SQL Always-On AG's to replicate the data and provide HA. **Figure 23 SQL Architecture for MIM** below outlines the SQL topology for MIM, hosted in the IDF.

[20] Oracle HA solution and RAC on VSAN 8

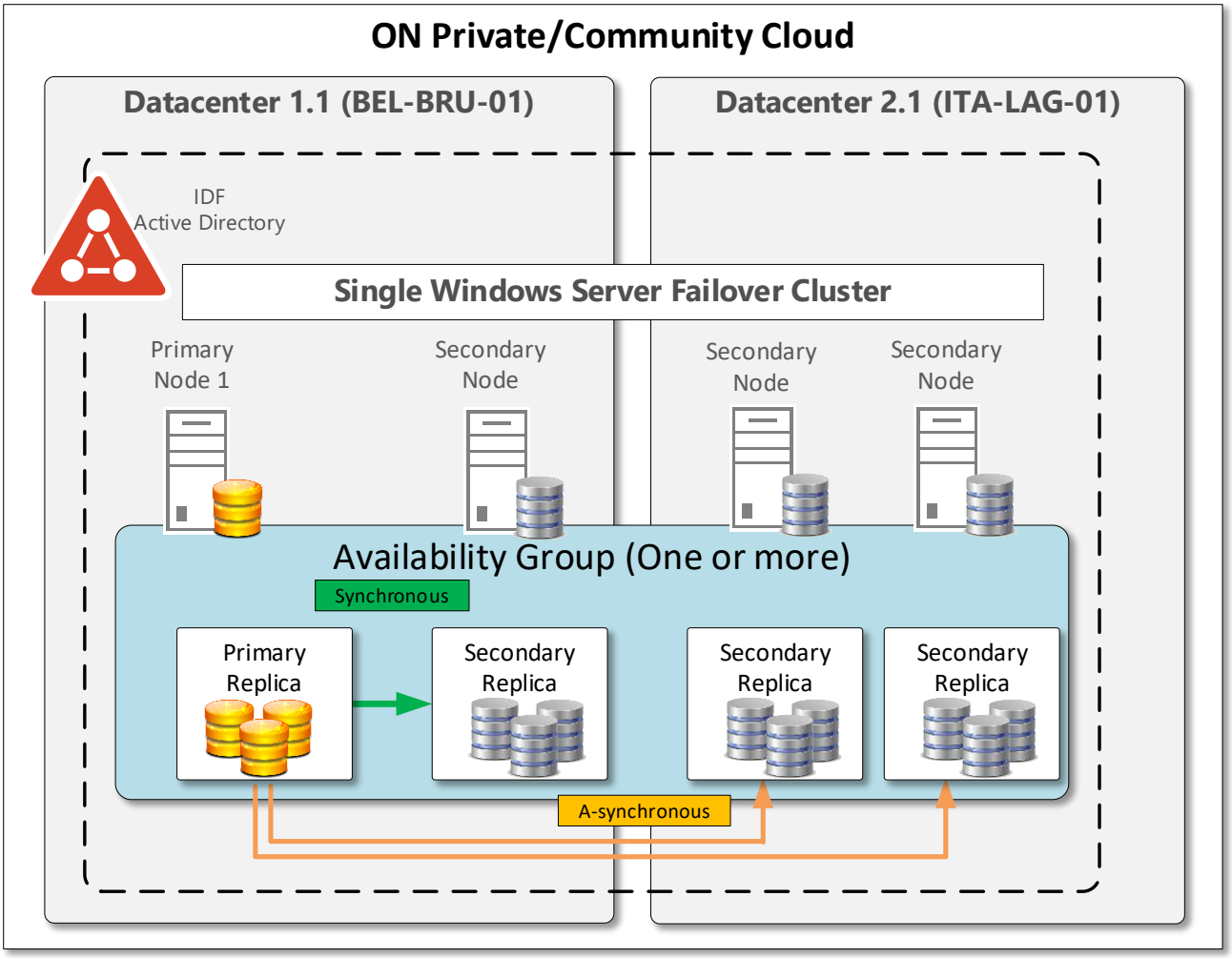

Figure 23 SQL Architecture for MIM

3.1.5.2.10. Database platform - Microsoft SQL Server for VMware vRealize Automation

0231 VMware vRealize Automation (vRA) enables administrators to automate the deployment of a set of VMs, or a blueprint of the way a particular set of VMs should be deployed. It provides a secure portal where authorised administrators, developers or business users can request new IT services and manage specific cloud and IT resources, while affirming compliance with business policies.

0232 As part of the core SDDC tools, it will be hosted on a separate physical ESX management cluster. The vRealize Automation service is to be highly available from the primary datacentre and able to resume services in the secondary datacentre in case of a disaster.

0233 The SQL architecture is to be developed once the detailed design for IaaS is worked out.

3.1.5.3. Administration

0234 The SQL Server Management Studio (SSMS) is the default desktop-based application for Database management. This tool allows for the remote management of the SQL server databases in the environment at all levels, from individual elements (e.g. particular database) to the overall instances (e.g. using remotely registered SQL servers). SQL Servers uses role-based permissions with the highest permissions being system administrators, reserved only to the SQL Server Database Administrators.

3.1.5.4. Backup and maintenance strategies

0235 The SQL Server backup and restore component provides an essential safeguard for protecting critical data stored in your SQL Server databases. To minimize the risk of catastrophic data loss, you need to back up your databases to preserve modifications to your data on a regular basis. A well-planned backup and restore strategy helps protect databases against data loss caused by a variety of failures.

0236 In terms of backup, the database platform services leverage the backup solution provided by the IaaS to a maximum extend, which is based on using VEEAM. All backups are stored locally and at the remote designated DR datacentre for the particular site. VEEAM provides transaction-consistent backups of SQL and Oracle databases

0237 In terms of database maintenance, the Ola Halengren[21] scripts can be leveraged to provide maintenance scripts as follows:

0238 The maintenance scripts are split as follows:

- Index Maintenance job
- Error log cycling
- Integrity Checks
- Mail History Purge job
- Agent Start alert job

3.1.5.5. Management Servers for ON

0239 Management SQL Servers will have full control over the production SQL Servers and will have installed all the necessary tools for the management and monitoring of the entire SQL Server farm:

- Latest SQL Server management server
- Remote desktop connection to all the production SQL Servers
- Remote access to all the SQL Server instances from SSMS
- PowerBI desktop installed
- DBA Tools PowerShell modules installed

3.1.6. Shared Enterprise Core Services

0240 Information Protection Control services provided by Titus and Document collaboration services provide by the Office Online Services are consumed by multiple core services as described in this section.

3.1.6.1. Information Protection Control (IPC)

0241 The Titus Classification Enterprise Suite collection of tools addresses IPC (i.e., data marking). This application enforces information governance and security policies, enabling security classification marking of files. This suite includes:

- Titus Message Classification, which integrates with Outlook
- Titus Classification for Microsoft Office, to support classification of Office documents
- Titus Classification for Desktop, for classification and policy enforcement of any Windows file
- Titus Classification for OWA, to support message classification in OWA
- Titus Reporting, for real-time assessment of message classification

[21] https://ola.hallengren.com/

0242 Each of these tools is installed on its respective client, provided by CPS, with settings specified at the enterprise level via the Titus Central Admin Server (TCAS). One TCAS server is deployed at the BEL-BRU-01 datacentre. Settings files are stored in a domain SYSVOL subfolder on each enclave to ensure access and replication across the enterprise, and are replicated to all clients via Group Policy.

0243 The TITUS client will enforce markings for each object accessed by the user in order to ensure all data in any ON repository contains a marking to its classification. **Table 14 List of functions and their TITUS labelling process** breaks down various ON services and how TITUS will integrate with them:

0244

ON Service	TITUS application	Integration with Service
SharePoint/Portal Services	Titus Classification for Microsoft Office	All documents uploaded will require classification marking from a user prior to upload
Outlook/Email	Titus Message Classification	User will be prompted and required to mark all outgoing emails
Local documents and files	Titus Classification for Desktop and Titus Classification for Office	Users will have the ability to mark any windows file. For MS Office based documents, TITUS marking will be required prior to saving any document.

Table 14 List of functions and their TITUS labelling process

0245 Restrictions will be applied by both TITUS and ProofPoint appliance to prevent unauthorized dissemination. TITUS will prevent dissemination of correctly classified messages to inappropriate destinations or recipients. ProofPoint will prevent dissemination of incorrectly classified messages.

0246 Supported classification markings on the ON are listed in **Table 56** Data Classification Markings

3.1.6.2. Office Online Server (OOS)

0247 Office Online Server (OOS) allows organisations to deliver browser-based versions of Word, PowerPoint, Excel and OneNote, among other capabilities:

- Integrated with SharePoint Server, OOS supports sharing and collaborating on Office documents
- Integrated with Exchange Server, OOS supports viewing and editing Office file attachments in OWA
- Integrated with Skype for Business Server, OOS enables high fidelity viewing of PowerPoint Online when sharing PowerPoint presentations during meetings

0248 OOS is deployed on two servers at each datacentre, load-balanced both globally and within each datacentre. Exchange, Skype for Business, and SharePoint point to the OOS VIP for Office Online services. OOS VIP has a reverse-proxy rules in the BPS-1 DMZ to support external access to this service for federated partners only. Figure 24 OOS Architecture shows this architecture.

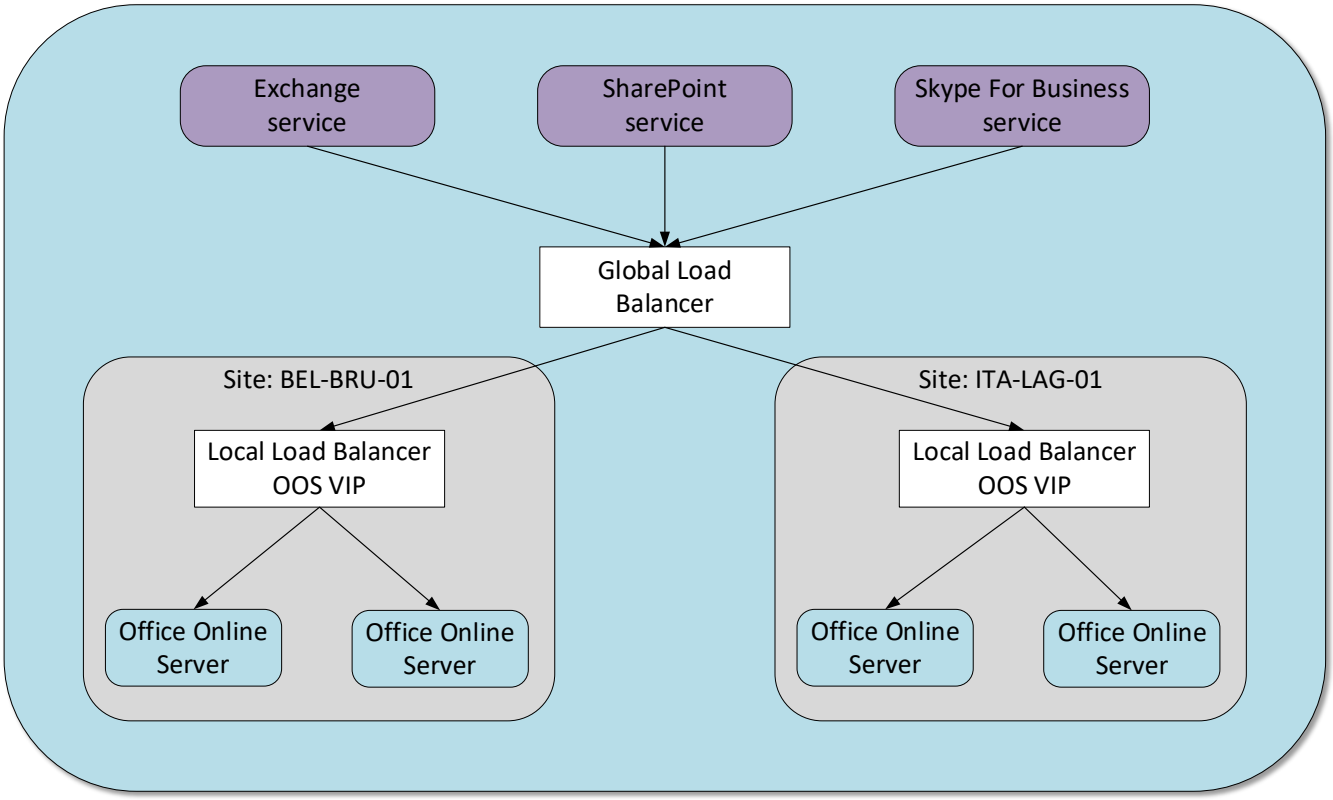

Figure 24 OOS Architecture

3.1.7. Core Services Cyber Security Services

3.1.7.1. BPS-1 Topology

0249 BPS-1 is described in the Service Design Package – Infrastructure as a Service (IaaS) and is composed of all system and services allowing for the secure communication between security zones and from/with external system and services. BPS-1 contains physical firewalls. The DMZ virtual services are deployed on the dedicated DMZ hardware, and segregated from internal resources. IaaS services Include DDI and Load Balancer services.

0250 ECS deploys the following services in the BPS1 DMZ:

- DMZF: Active Directory DMZ Forest (see section 3.1.1). For any domain joined objects, this forest will provide the common any AD services such as
  - License activation (ADBA)
  - Group Policy management
  - DNS, NTP
  - AD-FS: Integration for AD-FS proxy leveraging the Web Application Proxy (WAF) provided by the IaaS service
  - SfB Edge services enabling federation with external SfB partners (See section 3.1.3)
- Email gateway services:
  - ProofPoint Gateway for contents scanning (AV and IPC (See section 3.1.2.4)) and mail routing.
  - GAL synchronization integrating the ON environment (AIS) with the existing GAL Synchronization service hosted in the DMZF

3.1.7.2. Integration with NATO Enterprise centralized Logging and SIEM.

0251 All ECS services are integrating with the NATO Enterprise logging/SIEM based on Splunk.

0252 Systems are configured either to :

· Send the logs to the logging server/forwarder

· Provide a mechanism to allow the Splunk heavy forwarder to pull the logs from the target.

3.1.7.3.

3.1.7.4. BPS4 Topology

0253 The BPS4 function will be re-designed as a Diode as a Service, the IaaS services will leverage the Diode as a Service in order to enable data transfer between lower classification system and services and higher classification system and services (e.g. as part of lifecycle management to transfer patches/firmware/updates etc.) as well as enable email transfer from lower to higher classification.

0254 The Diode as a Service Email component will be configured to forward messages to the BPS1 ProofPoint Mail gateway, where all messages will be scanned for AV/Malware before routed further to the ON Exchange servers.

0255 Files will be transferred to designated file shares hosted by the DFS sub-service provided by ECS, where it will be scanned by McAfee Endpoint Security.

3.1.7.5. Security hardening

0256 All services deployed are required to be hardened, so that only required functions are enabled, and that access to services are authorized only from applicable consumers (user, device and/or service).

0257 Security hardening is developed and implemented as part of the automation and orchestration as well as enforced by AD Group Policies.

0258 Security hardening include the implementation of:

- NCIRC Hardening guides and Group Policies.
- DISA guides.
- Vendor specific hardening guidance.
- Remediation to identified vulnerabilities.

3.1.7.6. NATO Cyber Security Services Integration

0259 The NATO Cyber Security Centre (NCSC) is delivering, managing and operating NATO Cyber Security Services. The NATO ON IaaS and the services deployed on top of the IaaS (e.g. ECS) must integrate with those services. This is described in detail in the Service Design Package – Infrastructure as a Service (IaaS).

3.1.8. Core Services Service Management and Control

0260 The majority of the management tools are described in each of the relevant service design topologies.

0261 In addition we will integrate with the automation and orchestration tools provided by IaaS.

4. SERVICE SOLUTION [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

0262 This section provides additional detail on the ECS subservices, including component implementation design, security measures implementation, service level implementation, and subservice configuration.

4.1. Directory Service

0263 This section addresses the configuration and implementation of the ECS Directory Service.

4.1.1. Component Implementation Design

0264 The ECS Directory Service low-level design is addressed below.

4.1.1.1. Subservice Configuration

0265 The configuration of the ECS Directory Service, including implementation and integration requirements, is shown in **Table 15 Directory Services Configuration**.

Subservice	Configuration	Setting
AD-DS	ON Identity Domain (IDF) FQDN	ais.nato.int
AD-DS	ON DMZ Domain (DMZF) FQDN	N178.nato
AD-DS	ON Service Domain (SVF) FQDN	t.b.d. (format: Nxxx.nato.int where xxx is a number assigned by the Naming and Registration Authority (NRA))
AD-DS	ON Identity Domain (IDF) NetBIOS Name	AIS
AD-DS	ON DMZ Domain (DMZF) NetBIOS Name	N178
AD-DS	ON Service Domain (SVF) NetBIOS Name	Nxxx (where xxx is a number assigned by the Naming and Registration Authority (NRA))
AD-DS	Identity Forest (IDF) Trust	Two-way between identity and service/DMZFs at same security classification only
AD-DS	Identity domain schema extensions	Exchange, Skype for Business, SharePoint, and MS Endpoint Configuration Manager
AD-DS	Sites	
AD-DS	Site Links	
AD-DS	Subnets	<TBC>
AD-DS	OU structure	The initial OU structure is depicted in Table 5 - Initial OU Structure
AD-DS	GPO structure	NCIRC GPOs ON Delta GPOs
AD-DS	Directory attribute map	Listed in Data Map spreadsheet
ADBA	CSVLK License Keys	t.b.d.
DFS-R	Namespaces	\\nxxx.nato.int\sysvol \\ais.nato.int\user \\ais.nato.int\software \\ais.nato.int\application \\ais.nato.int\fsw \\ais.nato.int\skype
DNS	Conditional Forwarders	All trusted/trusting domains
DNS	Forwarders	[Perimeter DNS servers]
DNS	Aging/Scavenging	7 days (zones and server)
AD-FS	ON Federation Service Name	<t.b.d.> [internal] auth.nato.int [external]
AD-FS	Federation Service Display Name	<t.b.d.>

Table 15 Directory Services Configuration

4.1.2. Security Measures Implementation

0266 **Table 16 Directory Services Security** addresses the security measures specific to the ECS Directory Service.

Requirement	NATO ON Solution
SM01a - Malware Protection for Server	McAfee Endpoint Security- client will be installed on all servers to monitor and report on breaches. McAfee Endpoint services are managed by EpO, as detailed in the Service Design Package – Client Provisioning Services (CPS)
SM12 - Strong Authentication	AD integration with NPKI service – using active directory authentication with MFA of tokens for NPKI will allow for strong authentication enforcement.
SM13 - Enterprise Single Sign-On (ESSO)	AD-FS PKI-enabled federation – AD-FS trusts will allow for identities to be seamlessly used between forests.
SM16H - Intrusion Detection and Prevention System (IDS/IPS) - Host Based	McAfee Endpoint Security Threat protection module – Threat prevention uses exploit prevention capabilities to prevent host based intrusions.
SM21a - System and Security Logging & Auditing - Infrastructure and Servers	All Directory Service server event log data syslog to Splunk (initially default logging, to be tuned as required) – windows heavy forwarders will gather event log data and forward to Splunk for analysis
SM26 - Contingency planning	DBRR through IaaS Backup capability
SM30a - NPKI - User certificate	AD integration with NPKI service – using active directory authentication with MFA of tokens from smartcards for NPKI.
SM31 - Security Zones	Directory Service for the ON environment ensure physical separation of networks with different classifications. The Data Diode in place to ensure data can only flow from NU/NR AIS to ON and not the other way
SM32 - Policies, directives, guidance and procedures (PDP)	Implementation of NATO provided security policies, directives and procedures – will comply with all NATO provided policy and will conduct security audits as needed *to be verified*
SM33 - Load Balancing / Failover	DC replication – All forests and domains are built to replicate data to all physical sites to ensure continuity of operations.
SM34 - Labelling (aka Information Protection Control or IPC)	TITUS clients added to endpoint to enforce labelling policies.
SM37 - OS security settings and Group Policy Object (GPO)	NCIRC mandatory GPOs and additional delta GPOs deployed to support enterprise security and application functionality – GPOs will be deployed and updated regularly
SM42 - Identity & Access Management (IAM)	IDAM controlled via MIM, approval workflow processes, and connectivity to NEDS Local administrator rights managed via Group Policy and Microsoft's Local Administrator Password Solution (LAPS) tool
SM44 - Time Synchronisation	NTP synchronization with Datacentre Stratum 1 NTP sources in place at the datacentres
SM48 - Password Management	Password policy enforced via Domain GPO – strong passwords will be required to comply with security policy
SM49 - Identity & Authentication, Access Control (IAAC)	AD-integrated authentication and access control with NPKI MFA. PAM functions control admin controls.

Table 16 Directory Services Security

4.2. Email Messaging Service

0267 This section addresses the configuration and implementation of the ECS Email Messaging Service.

4.2.1. Component Implementation Design

0268 The ECS Email Messaging Service low-level design is addressed below.

4.2.1.1.1. Subservice Configuration

0269 The configuration of the ECS Email Messaging Service, including implementation and integration requirements, is shown in **Table 17 Email Messaging Service Configuration**.

Subservice	Configuration	Setting
Titus Classification	ON settings file storage location	\\ais.nato.int\sysvol\titus
Titus Classification	NS classification tags	See Table 56 Data Classification Markings
ProofPoint	DNS Server IP addresses	<t.b.d.>
ProofPoint	Authoritative inbound address spaces (ON)	See Table 6 -DNS Namespaces
Exchange	ON Autodiscover URL	https://autodiscover.ais.nato.int /autodiscover/autodiscover.xml
Exchange	Address Lists	Based on company and/or department attribute
Exchange	Default Details Template	Modified to reflect NATO attribute labels
Exchange	Quick Contact Card	Modified to reflect NATO attribute labels
Exchange	Deleted item recovery	30 days
Exchange	DAG configuration	See Section 3.1.2 Email Messaging Services
Exchange	Exchange DB lag copy log play down	7 days
Exchange	User mailbox size	10GB quota (initial setting)
Exchange	Maximum message size	20MB (initial setting)
Skype for Business	Office Online Server Farm [ON]	<t.b.d.>

Table 17 Email Messaging Service Configuration

4.2.2. Security Measures Implementation

0270 **Table 18 Email Messaging Service Security** addresses the security measures specific to the ECS Email Messaging Service.

Requirement	Implementation
SM01d - Malware Protection for Server Database	McAfee Endpoint Security - client will be installed on all database servers to monitor and report on breaches
SM4 - AV for Email services	The Mail Security service for Microsoft Exchange and SSL offloading with F5– clients will be installed on the Exchange servers as well as office plugins for desktop clients. Clients will check for malicious mail. F5 appliances will handle SSL orchestration to offload work of Exchange servers.
SM5 - AV for Web services	F5 AV service - WAF will be installed to monitor traffic for malicious activity
SM6 - SMTP AV/Proxy	ProofPoint at network perimeter – servers will be installed in the DMZ to inspect content for keywords and other data that should not leave system and will be quarantined for inspection.
SM11 - IPSec or TLS	TLS certificates on all mailbox servers – certificate based access and encryption for all mail traffic

Requirement	Implementation
SM16h - IDS/IPS Host-based	McAfee Endpoint Security Threat protection module - McAfee IPS and IDS devices will be placed in the DMZ to monitor for intrusions
SM21a - System and Security Logging & Auditing	All Mailbox server event log data syslog to Splunk (initially default logging, to be tuned as required) – Initially will take in all windows event and AD data from exchange servers.
SM21b - System and Security Logging & Auditing - Applications	All Mailbox server event log data syslog to Splunk (initially default logging, to be tuned as required). EMS agents installed on Exchange hardware to gather health and capacity usage information.
SM26 - Data Backup, Replication and Recovery (DBRR)	DBRR through DAG architecture and deleted item and deleted mailbox recovery as well as IaaS backup service based on Veeam.
SM29 - Encryption-Decryption /Cryptography	Public keys stored in AD; private keys stored on smart card and designated for SMIME digital signatures in Outlook desktop client
SM30a - NPKI Users, in conjunction with SM12	Public keys stored in AD to facilitate digital signature validation. OWA secured with TLS based on NPKI-issued certificates.
SM30b - NPKI Devices, in conjunction with SM17	NPKI-issued certificates installed on all email servers; NAC inherited from IaaS service.
SM32 - Policies, directives and procedures (PDP)	Implementation of NATO provided security policies, directives and procedures
SM33 - Load Balancing / Failover (LB/FO)	Mailbox databases can fail over to other DAGs – DAG replication described in section 3.1.2
SM34 - Information Protection Control (IPC) – a.k.a. Classification Level / Data Labelling	Titus Message Classification (Outlook client and OWA) – Titus plugin to be added to all ITM desktops to ensure all documents are labelled by a user prior to saving, sending or uploading.
SM35 – NR Message Quarantine	ProofPoint – Servers will be placed in the BPS-1 DMZ for inspection of all messages prior to release. All quarantined messages can be reviewed and released or automatically removed over time.
SM36 - Vulnerability Scanning & Compliancy	NCIRC vulnerability scanning agents installed on all servers based on NCIRC provided guidance – Scans will be initiated during non-interfering hours to minimize impact to the environment. Cadence of scans will be established
SM37 - Group Policy Object (GPO)	Configured in Active Directory using GPMC – GPOs will be applied as new policies and procedures mandate. All hosts will be domain joined and will receive updated after reboot or logoff
SM38 - Quality of Service (QoS)	Email packets tagged per GPO settings to facilitate QoS.
SM42 - Identity & Access Management (IdAM)	MIM provisions and manages all user accounts and mailboxes – requests will be made through the MIM portal and be approved or denied by an approving body. The MIM synch service will make requests to AD to update accounts through APIs.
SM49 - Identity & Authentication, Access Control (IAAC)	AD-integrated authentication and access control, at both the user level for Outlook desktop mailbox access, as well as at the administrator level for role-based access control. Supplemental PKI-based authentication for OWA access, in addition to AD authentication.
SM56 - Data Diode	Mail transfer up via Data Diode Service

Table 18 Email Messaging Service Security

4.3. Skype for Business Service

0271 This section addresses the configuration and implementation of the ECS Skype for Business Service.

4.3.1. Component Implementation Design

0272 The ECS Skype for Business low-level design is addressed below.

4.3.1.1. Subservice Configuration

0273 The configuration of the ECS Skype for Business Service, including implementation and integration requirements shown in **Table 19 Skype for Business Service Configuration**.

Subservice	Configuration	Setting
Skype for Business	Internal and External DNS records creation	Pismonwcsfe001.ais.nato.int Meet.nato.int Dialin.nato.int Lyncdiscover.nato.int Lyncdiscoverinternal.nato.int Sip.nato.int Skpe.nato.int Sfbwebintmon.nato.int Sfbwebextmon.nato.int Sfbadminmon.ais.nato.int Pismonwcsepmon001.ais.nato.int
Skype for Business	Open internal and external FWs ports	Open ports in all the required FWs
Skype for Business	SIP Domain definition	
Skype for Business	Simple URLs definition	[TBC]
Skype for Business	Administrative access URL definition	https://sfbadmin.ais.nato.int
Skype for Business	Front-End Pool FQDN definition	prsmonwcsfe001.ais.nato prslagwcsfe001.ais.nato
Skype for Business	Edge Pool Definition	prsmonwcsep001.ais.nato prslagwcsep001.ais.nato
Skype for Business	Resiliency Definition	prsmonwcsfe001.ais.nato prslagwcsfe001.ais.nato
Skype for Business	Internal Web Services	sfbwebint.ais.nato
Skype for Business	External Web Services	sfbwebext.ais.nato
Skype for Business	Mediation Pool FQDN	prsmonwcsmp001.ais.nato prslagwcsmp001.ais.nato
Skype for Business	Office Online Server Farm	oos.ais.nato
Skype for Business	Edge Server Installation	This role is collocated into BPS-1

Table 19 Skype for Business Service Configuration

4.3.2. Security Measures Implementation

0274 **Table 20 Skype for Business Service Security** addresses the security measures specific to the ECS Skype for Business Service.

Requirement	Implementation
SM01d - Malware Protection for Server Database	McAfee Endpoint Security
SM4 - AV for Email services	Not applicable to SfB Service
SM5 - AV for Web services (e.g. SharePoint)	Not applicable to SfB Service
SM6 - SMTP AV/Proxy	Not applicable to SfB Service

Requirement	Implementation
SM7abc - Web Content Filtering (WCF)	F5
SM11 - IPSec or TLS	TLS certificates on all mailbox servers
SM16h - IDS/IPS Host-based	Palo Alto Threat Protection
SM21a - System and Security Logging & Auditing	All SfB server event log data syslog to Splunk (initially default logging, to be tuned as required)
SM21b - System and Security Logging & Auditing - Applications	All SfB server event log data syslog to Splunk (initially default logging, to be tuned as required)
SM26 - Data Backup, Replication and Recovery (DBRR)	Backup by enterprise backup service
SM29 - Encryption-Decryption /Cryptography	All services configured with AES/SSL/TLS
SM30a - NPKI Users, in conjunction with SM12	Not applicable to SfB Service
SM30b - NPKI Devices, in conjunction with SM17	Not applicable to SfB Service
SM32 - Policies, directives and procedures (PDP)	Implementation of NATO provided security policies, directives and procedures
SM33 - Load Balancing / Failover (LB/FO)	Pools load balanced within Datacentres and stretched across Datacentres
SM34 - Information Protection Control (IPC) – a.k.a. Classification Level / Data Labelling	Inherited from Messaging Service
SM35 – NR Message Quarantine	Not applicable to SfB Service
SM36 - Vulnerability Scanning & Compliancy	NCIRC vulnerability scanning agents installed on all servers based on NCIRC provided guidance
SM37 - Group Policy Object (GPO)	Configured in Active Directory using AGPM
SM38 - Quality of Service (QoS)	Monitored, tuned, and managed within SfB, and configured via GPO where possible.
SM42 - Identity & Access Management (IAM)	Inherited from Directory Service
SM49 - Identity & Authentication, Access Control (IAAC)	Inherited from Directory Service
SM56 - Data Diode	Not applicable to SfB Service

Table 20 Skype for Business Service Security

4.4. Portal Service

0275 This section addresses the configuration and implementation of the ECS Portal Service.

4.4.1. Component Implementation Design

0276 The ECS Portal Service low-level design is addressed below.

4.4.1.1. Subservice Configuration

0277 The configuration of the ECS Portal Service including implementation and integration requirements shown in **Table 21 Portal Service Configuration**.

Subservice	Configuration	Setting
Web Services Tier	Main web application URL	https://we.nato.int
Web Services Tier	MySites web application URL	https://me.nato.int
Web Services Tier	MySites per-user storage limit	1GB initially
Web Services Tier	Microsoft SharePoint Foundation Web Application	Automatically Configured
Application Services Tier	Access Services 2010	Removed in SP Subscription
Application Services Tier	Secure Store Service	Configured based on future needs for Performance Point or based on Custom Solutions currently installed.
Application Services Tier	PowerPoint Conversion Service	Caching enabled based on usage testing
Application Services Tier	Request Management	Automatically Configured
Application Services Tier	SSP Job Control Service	Automatically Configured
Application Services Tier	PerformancePoint Service	removed in SP Subscription
Application Services Tier	Visio Graphics Service	Automatically Configured / Caching fine-tuned at site
Application Services Tier	Managed Metadata Web Service	Configuration done per NCMS policy
Application Services Tier	Microsoft SharePoint Foundation Administration	Automatically Configured
Application Services Tier	Portal Service	Automatically Configured
Application Services Tier	Microsoft SharePoint Foundation Sandboxed Code Service	Not used for NATO
Application Services Tier	Microsoft SharePoint Foundation Tracing	Automatically Configured
Application Services Tier	SharePoint Server Search	Configuration done per organisational needs / Crawl schedules configured per site / Crawl content configured at site.
Application Services Tier	App Management Service	Automatically Configured
Application Services Tier	Security Token Service	Automatically Configured
Application Services Tier	Machine Translation Service	Not available for usage
Application Services Tier	Application Discovery and Load Balancer Service	Automatically Configured
Application Services Tier	Microsoft SharePoint Foundation Usage	Automatically Configured
Application Services Tier	Microsoft SharePoint Foundation Subscription Settings Service	Automatically Configured
Application Services Tier	Search Administration Web Service	Automatically Configured
Application Services Tier	Word Automation Services	Automatically Configured
Application Services Tier	User Profile Service	Only started on a single Application Server but configured per organisation and AD architecture ‘OU’
Application Services Tier	Business Data Connectivity Service	Not authorized, not available for usage.
Application Services Tier	Lotus Notes Connector	Not Used
Application Services Tier	Microsoft SharePoint Foundation Workflow Timer Service	Automatically Configured
Application Services Tier	Access Services	Removed in SP Subscription

Subservice	Configuration	Setting
Application Services Tier	Microsoft SharePoint Insights	Automatically Configured / Fine-tuned at a later time if needed.
Application Services Tier	Search Host Controller Service	Automatically Configured
Application Services Tier	Information Management Policy Configuration Service	Automatically Configured
Application Services Tier	Microsoft SharePoint Foundation Incoming E-Mail	Not authorized, not available for usage.
Application Services Tier	Search Query and Site Settings Service	Configured during Search setup
All SharePoint Servers	Claims to Windows Token Service	Configured with Claims to Token Service account and Kerberos Constrained Delegation – determined at site.
All SharePoint Servers	Microsoft SharePoint Foundation Timer	Automatically Configured

Table 21 Portal Service Configuration

4.4.2. Security Measures Implementation

0278 **Table 22 Portal Service Security** addresses the security measures specific to the ECS Portal Service.

Requirement	Implementation
SM01d - Malware Protection for Server Database	McAfee Endpoint Security - client will be installed on all database servers to monitor and report on breaches
SM1b - AV for Application Server	McAfee Security for Microsoft SharePoint – client will be installed on all application servers and will check in with ePO for policy and data updates.
SM5 - AV for Web Services	McAfee VirusScan Enterprise *or F5?*
SM12 - Strong Authentication (User Token)	PKI / 2 Factor Auth with AD-FS - using active directory authentication with MFA of tokens for NPKI will allow for strong authentication enforcement.
SM16h - IDS/IPS Network	Palo Alto Threat Protection – Palo Altos are placed in the DMZs to monitor traffic for malicious activity.
SM20 - (Web) Application Firewall and other proxy/reverse proxy	IaaS Service (F5) – F5 reverse proxy and WAFs are fronting portal services to handle load balancing with SharePoint applications to ensure no server is overloaded.
SM21a - System and Security Logging & Auditing	Windows System Event Logs / ULS / SQL Logs and IIS Logging to Splunk (initially default logging, to be tuned as required)
SM21b - System and Security Logging & Auditing - Applications	Windows System Event Logs / ULS / SQL Logs and IIS Logging to Splunk (initially default logging, to be tuned as required)
SM26 - Data Backup, Replication and Recovery (DBRR)	SQL AlwaysOn for HA and DR; for data backup – integration with IaaS Backup and Recovery service based on Veeam.
SM28 - IT Forensic	Managed by NCIRC
SM29 - Encryption-Decryption /Cryptography	SQL Server Encryption / Database at rest Encryption – uses transparent data encryption on SQL servers to ensure stolen drives are not accessible.

Requirement	Implementation
SM30a - NPKI Users, in conjunction with SM12	PKI / 2 Factor Auth with AD-FS – establish trusts with NPKI authorities to trust certificates from smart cards in addition to strong password enforcement from Active Directory
SM32 - Policies, directives and procedures (PDP)	Implementation of NATO provided security policies, directives and procedures - will comply with all NATO provided policy and will conduct security audits as needed *to be verified*
SM33 - Load Balancing / Failover (LB/FO)	Load Balancing provided by IaaS Load Balancing Service – F5 reverse proxies will be used to control portal access to ensure no single application server is overwhelmed
SM34 - Information Protection Control (IPC)	Data labelling will be enforced using Titus for MS Office
SM36 - Vulnerability Scanning & Compliancy	NCIRC vulnerability scanning agents installed on all servers based on NCIRC provided guidance
SM37 - Group Policy Object (GPO)	Configured in Active Directory using GPMC - GPOs will be applied as new policies and procedures mandate. All hosts will be domain joined and will receive updates after reboot or logoff
SM42 - Identity & Access Management (IAM)	Active Directory, AD-FS, MIM – MIM portal will facilitate provision, modification and deletion of user accounts. PAM will control administrative access to services.
SM48 - Password Management	Active Directory, AD-FS, MIM – Strong passwords will be enforced via group policy.
SM49 - Identity & Authentication, Access Control (IAAC)	Active Directory, AD-FS, MIM - MIM portal will facilitate user requests for provision and deletion. PAM will control administrative access to services.
SM50 – DDoS	Standard currently under development
SM55 - Data manipulation and consistency	Implementation of Taxonomy within SharePoint.

Table 22 Portal Service Security

4.4.2.1. Security Measures Implementation (ON)

0279 [TBC]

4.5. Database Service

0280 This section addresses the configuration and implementation of the SQL Server Services.

4.5.1. Component Implementation Design

0281 The Database SQL Servers low-level design is addressed below.

4.5.1.1. Subservice Configuration – Generic settings

0282 The generic configuration of the Database Services that applies to all database services, including implementation and integration requirements shown **in Table 23 Database Service – Generic Configuration.**

Subservice	Configuration	Setting
Active Directory Services	Cluster configuration	Cluster Name CNO
Infrastructure Services	Cluster configuration	Cluster IP Address from both the Primary and DR location
Infrastructure Services	Cluster configuration	Failover Feature

Subservice	Configuration	Setting
Infrastructure Services	Server configuration	.net 4.7 Feature or above
Infrastructure Services	Cluster and quorum configuration	Quorum (FileShare) made available
Active Directory Services	Cluster permissions on Active directory objects	Cluster computer name object has Full Control on Quorum
Database Service	Infrastructure configuration	Check Disk Config and drive letters
Active Directory Services	Cluster permissions on Active directory objects	Is AD Cluster Object Disabled
Infrastructure Services	Infrastructure configuration	Page.sys file of OS max 16384 MB
Active Directory Services	Cluster permissions on Active directory objects	Has the Cluster AD object permissions on AG AD Object entry
Active Directory Services	Cluster permissions on Active directory objects	Has the Cluster AD object permissions on DNS entry
Infrastructure Services	Infrastructure configuration	All drives NTFS Formatted at 64k Thick provision eager zeroed
		McAfee Exclusions for (MDF/NDF/LDF/BAK/TRN/Mass Mail) and the /.sqlservr.exe location
Infrastructure Services	Infrastructure configuration	Power Options set to High Performance
Active Directory Services	SQL Server service account configuration	gmsa Service Account for SQL Engine
Active Directory Services	SQL Server service account configuration	gmsa Service Account for SQL Agent
Database Service	SQL Server configuration	Disable TCP Dynamic Ports in Config Manager
Database Service	SQL Server configuration	Set Static Ports to 1433 in Config Manager
Database Service	SQL Server configuration	Trace flag 1117, 1118, 3226 Globally Enabled (Pre SQL 2016 Servers)
Database Service	SQL Server configuration	Shared Memory Protocol Disabled (Client Config & 32bit / Net Config)
Database Service	SQL Server configuration	Disable SQL Browser (default instances only)
Database Service	SQL Server configuration	Named Pipe Protocol Enabled (Client Config & 32bit / Net Config)
Active Directory Services	Active directory GPO configuration	Perform Volume Maintenance Granted (SecPol / Group Policy)
Active Directory Services	Active directory GPO configuration	Lock Pages in Memory Granted (SecPol / Group Policy)

Subservice	Configuration	Setting
Database Service	SQL Server configuration	Max Memory Set (OS Memory - 10%, round down to next GB, or OS-4) (001)
Database Service	SQL Server configuration	Min Memory Set (Max Memory / 2) (001)
Database Service	Cluster configuration	Public NW (Control Panel) - DNS and Register this connection in DNS
Database Service	Cluster configuration	HeartBeat NW - No DNS and NO Register this connection in DNS
Database Service	Cluster configuration	HeartBeat Network for Cluster only

Table 23 Database Service – Generic Configuration Settings

4.5.1.2. Subservice Configuration – Service specific settings

0283 This section describes the settings specific per Database implementation.

0284 The specific configuration of the Database Services for Microsoft SQL Server for Skype for Business is shown in **Table 24 Database Service –DB Configuration Settings for Microsoft SQL Server for Skype for Business**

0285 Subservice	Configuration	Setting
Active Directory Services	Cluster configuration	
Infrastructure Services	Cluster configuration	
Infrastructure Services	Cluster and quorum configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Database Service	Infrastructure configuration	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	SQL Server service account configuration	
Database Service	SQL Server configuration	
Active Directory Services	Active directory GPO configuration	
Database Service	SQL Server configuration	
Database Service	Cluster configuration	

Table 24 Database Service –DB Configuration Settings for Microsoft SQL Server for Skype for Business

0286 The specific configuration of the Database Services for Microsoft SQL Server for Central SharePoint Farm is shown in **Table 25 Database Service –DB Configuration Settings for Microsoft SQL Server for Central SharePoint Farm**

0287 Subservice	Configuration	Setting
Active Directory Services	Cluster configuration	
Infrastructure Services	Cluster configuration	
Infrastructure Services	Cluster and quorum configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Database Service	Infrastructure configuration	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	SQL Server service account configuration	
Database Service	SQL Server configuration	
Active Directory Services	Active directory GPO configuration	
Database Service	SQL Server configuration	
Database Service	Cluster configuration	

Table 25 Database Service –DB Configuration Settings for Microsoft SQL Server for Central SharePoint Farm

0288 The specific configuration of the Database Services for Microsoft SQL Server for SCOM is shown in **Table 26 Database Service –DB Configuration Settings for Microsoft SQL Server for SCOM**

0289 Subservice	Configuration	Setting
Active Directory Services	Cluster configuration	
Infrastructure Services	Cluster configuration	
Infrastructure Services	Cluster and quorum configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Database Service	Infrastructure configuration	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	SQL Server service account configuration	
Database Service	SQL Server configuration	
Active Directory Services	Active directory GPO configuration	
Database Service	SQL Server configuration	
Database Service	Cluster configuration	

Table 26 Database Service –DB Configuration Settings for Microsoft SQL Server for SCOM

0290 The specific configuration of the Database Services for Microsoft SQL Server for e-Policy Orchestrator, Titus Classification suite and MECM is shown in **Table 27 Database Service –DB Configuration Settings for Microsoft SQL Server for e-Policy Orchestrator, Titus Classification suite and MECM**.

0291 Subservice	Configuration	Setting
Active Directory Services	Cluster configuration	
Infrastructure Services	Cluster configuration	
Infrastructure Services	Cluster and quorum configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Database Service	Infrastructure configuration	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	SQL Server service account configuration	
Database Service	SQL Server configuration	
Active Directory Services	Active directory GPO configuration	
Database Service	SQL Server configuration	
Database Service	Cluster configuration	

Table 27 Database Service –DB Configuration Settings for Microsoft SQL Server for e-Policy Orchestrator, Titus Classification suite and MECM

0292 The specific configuration of the Database Services for Microsoft SQL Server for VMware Horizon and VMware AppVolumes is shown in **Table 28 Database Service –DB Configuration Settings for Microsoft SQL Server for VMware Horizon and VMware AppVolumes**

0293 Subservice	Configuration	Setting
Active Directory Services	Cluster configuration	
Infrastructure Services	Cluster configuration	
Infrastructure Services	Cluster and quorum configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Database Service	Infrastructure configuration	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Infrastructure Services	Infrastructure configuration	

0293 Subservice	Configuration	Setting
Active Directory Services	SQL Server service account configuration	
Database Service	SQL Server configuration	
Active Directory Services	Active directory GPO configuration	
Database Service	SQL Server configuration	
Database Service	Cluster configuration	

Table 28 Database Service –DB Configuration Settings for Microsoft SQL Server for VMware Horizon and VMware AppVolumes

0294 The specific configuration of the Database Services for Microsoft SQL Server for RDS is shown in **Table 29 Database Service –DB Configuration Settings for Microsoft SQL Server for RDS**.

0295 Subservice	Configuration	Setting
Active Directory Services	Cluster configuration	
Infrastructure Services	Cluster configuration	
Infrastructure Services	Cluster and quorum configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Database Service	Infrastructure configuration	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	SQL Server service account configuration	
Database Service	SQL Server configuration	
Active Directory Services	Active directory GPO configuration	
Database Service	SQL Server configuration	
Database Service	Cluster configuration	

Table 29 Database Service –DB Configuration Settings for Microsoft SQL Server for RDS

0296 The specific configuration of the Database Services for Microsoft SQL Server for BMC Remedy ITSM, SSO and TSO is shown in **Table 30 Database Service –DB Configuration Settings for Microsoft SQL Server for BMC Remedy ITSM, SSO and TSO**.

0297 Subservice	Configuration	Setting
Active Directory Services	Cluster configuration	
Infrastructure Services	Cluster configuration	
Infrastructure Services	Cluster and quorum configuration	
Active Directory Services	Cluster permissions on Active directory objects	

0297 Subservice	Configuration	Setting
Database Service	Infrastructure configuration	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	SQL Server service account configuration	
Database Service	SQL Server configuration	
Active Directory Services	Active directory GPO configuration	
Database Service	SQL Server configuration	
Database Service	Cluster configuration	

Table 30 Database Service –DB Configuration Settings for Microsoft SQL Server for BMC Remedy ITSM, SSO and TSO

0298 The specific configuration of the Database Services for Oracle Server for BMC Truesight Capacity Optimization and Operation Management is shown in **Table 31 Database Service –DB Configuration Settings for Oracle Server for BMC Truesight Capacity Optimization and Operation Management**.

0299 Subservice	Configuration	Setting
Active Directory Services	Cluster configuration	
Infrastructure Services	Cluster configuration	
Infrastructure Services	Cluster and quorum configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Database Service	Infrastructure configuration	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	SQL Server service account configuration	
Database Service	SQL Server configuration	
Active Directory Services	Active directory GPO configuration	
Database Service	SQL Server configuration	
Database Service	Cluster configuration	

Table 31 Database Service –DB Configuration Settings for Oracle Server for BMC Truesight Capacity Optimization and Operation Management

0300 The specific configuration of the Database Services for Microsoft SQL Server for MIM is shown in **Table 32 Database Service – DB Configuration Settings for Microsoft SQL Server for MIM**

0301 Subservice	Configuration	Setting
Active Directory Services	Cluster configuration	
Infrastructure Services	Cluster configuration	
Infrastructure Services	Cluster and quorum configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Database Service	Infrastructure configuration	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	SQL Server service account configuration	
Database Service	SQL Server configuration	
Active Directory Services	Active directory GPO configuration	
Database Service	SQL Server configuration	
Database Service	Cluster configuration	

Table 32 Database Service – DB Configuration Settings for Microsoft SQL Server for MIM

0302 The specific configuration of the Database Services for Microsoft SQL Server for VMware vRealize Automation is shown in **Table 33 Database Service – DB Configuration Settings for Microsoft SQL Server for VMware vRealize Automation**

0303 Subservice	Configuration	Setting
Active Directory Services	Cluster configuration	
Infrastructure Services	Cluster configuration	
Infrastructure Services	Cluster and quorum configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Database Service	Infrastructure configuration	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	Cluster permissions on Active directory objects	
Infrastructure Services	Infrastructure configuration	
Active Directory Services	SQL Server service account configuration	
Database Service	SQL Server configuration	

0303 Subservice	Configuration	Setting
Active Directory Services	Active directory GPO configuration	
Database Service	SQL Server configuration	
Database Service	Cluster configuration	

Table 33 Database Service – DB Configuration Settings for Microsoft SQL Server for VMware vRealize Automation

4.5.2. Security Measures Implementation

0304 **Table 34 Database Service Security** addresses the security measures specific to the ECS Database Service.

Requirement	Implementation
SM01d - Malware Protection for Server Database	McAfee Endpoint Security
SM11 - IPSec or TLS	TLS certificates on all database servers
SM16h - IDS/IPS Host-based	Palo Alto Threat Protection
SM21a - System and Security Logging & Auditing	All SQL server event log data syslog to Splunk (initially default logging, to be tuned as required)
SM21b - System and Security Logging & Auditing - Applications	All SQL server event log data syslog to Splunk (initially default logging, to be tuned as required)
SM26 - Data Backup, Replication and Recovery (DBRR)	Backup by IaaS enterprise backup service (Veeam)
SM29 - Encryption-Decryption /Cryptography	All services configured with AES/SSL/TLS SQL Server Encryption / Database at rest Encryption – uses transparent data encryption on SQL servers to ensure stolen drives are not accessible.
SM32 - Policies, directives and procedures (PDP)	Implementation of NATO provided security policies, directives and procedures
SM33 - Load Balancing / Failover (LB/FO)	High available configurations leveraging SQL Always-On AGs and Oracle RAC/Data Guard.
SM34 - Information Protection Control (IPC) – a.k.a. Classification Level / Data Labelling	Data labelling not applicable to database services
SM36 - Vulnerability Scanning & Compliancy	NCIRC vulnerability scanning agents installed on all servers based on NCIRC provided guidance
SM37 - Group Policy Object (GPO)	Configured in Active Directory using GPMC

Requirement	Implementation
SM38 - Quality of Service (QoS)	Monitored, tuned, and managed within SQL, and configured via GPO where possible.
SM42 - Identity & Access Management (IAM)	Inherited from Directory Service
SM49 - Identity & Authentication, Access Control (IAAC)	Inherited from Directory Service
SM56 - Data Diode	Not applicable to SQL Services

Table 34 Database Service Security

5. SERVICE MANAGEMENT AND TOOLS [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

0305 This section provides detail on ECS service management and tools, including integration points with the enterprise SMC service, as well as management of ECS subservices.

5.1. Service Area Management

0306 The integration touch points between SMC enterprise management and the ECS service is delineated in **Table 35 ECS Service Management**.

Subservice	Software	Connection Point	Description
[ALL]	Remedy management agent	Remedy	Requests for new directory objects, including security groups, distribution lists, organisational units, and contact objects
[ALL]	MECM client	MECM Service	Support enterprise patching for all systems
[ALL]	McAfee VirusScan client	ePO Server	Support malware protection for all systems
[ALL]	SCOM client	SCOM Service	Supports enterprise monitoring
[ALL]	SYSLOG client	Splunk Service	Supports enterprise reporting

Table 35 ECS Service Management

5.2. Subservice Area and Element Management

0307 **Table 36 Subservice Management Tools** delineates the tools required to manage each sub-service and system element.

Subservice	Software	Tool	User	Purpose
[ALL]	[ALL]	Remote Desktop Protocol (RDP)	Server Admin	Remote access to console
[ALL]	[ALL]	HP One View	Server Admin	Out of band server access
[ALL]	[ALL]	vCenter	Server Admin	Remote access to virtual machines
[ALL]	[ALL]	PowerShell	Server Admin	Service scripting
Directory Service	AD-DS	Active Directory Users and Computers	AD Admin	Manage domain
Directory Service	AD-DS	Active Directory Sites and Services	AD Admin	Manage forest configuration
Directory Service	AD-DS	Active Directory Domains and Trusts	AD Admin	Manage domain and trust configuration

Subservice	Software	Tool	User	Purpose
Directory Service	AD-DS	Active Directory Schema Administrator	AD Admin	Manage forest schema
Directory Service	AD-FS	AD-FS Console	AD Admin	Manage AD-FS Farm
Directory Service	AD-LDS	AD-LDS Wizard	AD Admin	Create new LDAP services and application partitions
Directory Service	AD-DS, AD-LDS	LDP.EXE	AD Admin	Test/browse LDAP partitions
Directory Service	AD-DS, AD-LDS	ADSIEDIT.MSC	AD Admin	Manage LDAP Services
Directory Service	DFS-R	DFS.MSC	AD Admin	Manage and configure DFS-R
Directory Service	DNS	DNS.MSC	AD Admin	Manage and configure DNS
Directory Service	ADBA	Volume Activation Tool	AD Admin	Manage and configure ADBA activation keys
Directory Service	GPMC	GPMC Console	GPO Admin	Manage GPOs
Directory Service	MIM	MIM Portal	MIM Admin	Configure and manage portal
Directory Service	MIM	MIM Sync Service	MIM Admin	Configure and manage synchronization engine
Directory Service	[ALL]	PAM Tool to be determined	[ALL]	Request Admin credentials
Messaging Service	Exchange	Exchange Admin Console (EAC)	Messaging Admin	Configure and manage Exchange
Messaging Service	Exchange	Exchange PowerShell	Messaging Admin	Configure and manage Exchange
Messaging Service	Proofpoint	Proofpoint Master Application	Messaging Admin	Configure and manage Proofpoint
Messaging Service	Titus	Titus Administrator	Messaging Admin	Configure and manage Titus
Messaging Service	Titus	Titus Reporting Console	Messaging Admin	Review reports
Portal Service	SharePoint	Central Administration	SharePoint Admin	Central Administration Server used to administer the SharePoint Farm Configuration
Portal Service	SharePoint	SharePoint Designer	SharePoint Developer	Create custom workflows
Portal Service	SharePoint	ULS Viewer	SharePoint Admin	Analyse ULS logs
Portal Service	SharePoint	SharePoint Manager	SharePoint Admin	Reporting and solution drill-down
Database Service	SQL Server	SQL Management Studio	SQL Admin	SSMS is used to manage the SQL Always on Cluster
Database Service	SQL Server	Redgate SQL Monitor	SQL Admin	Redgate SQL Monitor is used to monitor the

Subservice	Software	Tool	User	Purpose
				SQL databases. [TBC]
Skype for Business	Skype for Business	SfB Server Control Panel	SfB Admin	Manage SfB service
Skype for Business	Skype for Business	SfB Server PowerShell	SfB Admin	Manage SfB configuration
Skype for Business	Skype for Business Topology	SfB Topology builder	SfB Admin	Manage SfB topology
Skype for Business	Skype for Business	Skype for business control panel	SfB Admin	View a list of all SfB servers in the topology and check service status.
Skype for Business	Skype for Business Resource Kit	[various]	SfB Admin	Troubleshooting
Skype for Business	Skype for Business Debugging Tools	[various]	SfB Admin	Troubleshooting
Skype for Business	Statistics Manager	Dashboard solution	SfB Admin	View KHI calculations in real-time as well as graphed performance counters aggregated across the infrastructure
Skype for Business	Stress and Performance Tool	Stress and Performance Tool	SfB Admin	Perform a variety of performance-related testing with user load for your SfB server environment
[ALL]	Veeam	Veeam Backup Enterprise Manager	IaaS Admin	Allows for backing up and restoring AD objects, DFS file shares, mailboxes, databases and portal contents in the event of deletion or data loss

Table 36 Subservice Management Tools

6. SERVICE PROCESSES [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

0308 There are five category 1 and 12 category 2 ITIL processes designated to support the process implementation and ON Services implementation (a total of 17 ITIL processes). Each of the 17 ITIL process documents (SOPs/Steps/Work Instructions) is provided in draft form as a separate set of artefacts to provide the information requirements of SDP Section 5.1 and SDP Annex C for each of the ON Services. Please refer to the SMC SDP for additional information on process design and implementation. This approach is based on our understanding of the requirement, SDP Section 5 and SDP Annex C and refers to ITM SOW Section 10 which is focused on the category 1, category 2 and category 3 ITIL processes.

0309 We understand the term 'ON Processes' to mean only the ITIL processes referenced in SOW Section 10, the ITIL process documents, and the associated processes, procedures, and Work Instructions for inclusion in the Operations Manual. Each ITIL process document includes a process overview diagram with initial roles identified to manage each process and a list of the KPIs to support the process objectives.

0310 covers all ECS sub-services, and provides a reference for the ITIL processes directly supporting each ON Service operating in a production environment. Refer to the separate ITIL Process Documentation Artefacts for process overview and workflow.

0311 lists SMC as an ON Capability as it provides the integrated tool sets and processes used in ON Service support and delivery.

ITIL Life Cycle Stage	ITIL Processes Directly Supporting ON Services Operating In Production Environment	Notes for CPS, ECS, IaaS Services	ON Service ON Capability			
			IaaS	CPS	ECS	SMC
SS	Financial Management for IT Services	Charge back and cost information				
SD	Service Level Management	Provide information for service reviews and improvement opportunities				
SD	Availability Management	Monitoring and reporting of actual service and infrastructure availabilities to meet service levels.				
SD	Capacity Management	Monitoring and reporting of service and infrastructure performance and capacities to meet service levels.				
SD	IT Services Continuity Management	Testing and support of continuity plans.				
SD	Information Security Management	Recurring validation of security control effectiveness.				
ST	Change Management	Raise RFC to add, modify or remove anything with impact on the service.				
ST	Service Asset and Configuration Management	Provide Asset / CI information and configuration control				
ST	Release and Deployment Management					
ST	Service Validation and Testing					
ST	Change Evaluation					

ITIL Life Cycle Stage	ITIL Processes Directly Supporting ON Services Operating In Production Environment	Notes for CPS, ECS, IaaS Services	ON Service ON Capability			
			IaaS	CPS	ECS	SMC
ST	Knowledge Management	Collection and management of the Know How of the IT Organisation to support and deliver the service.				
SO	Request Fulfilment					
SO	Incident Management	Log incident for unplanned interruption to the service.				
SO	Access Management	User permission management.				
SO	Problem Management	Detection and elimination of the cause of the problem.				
SO	Event Management	Monitoring and resolution of alerts or notifications with impact to the service.				

Table 37 ITIL Processes Directly Supporting ON Service in Production

7. SERVICE ORGANISATIONAL SKILL LEVELS [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

0312 To maintain consistency and avoid conflicting information between design documents containing the same information, please refer to SMC SDP document for Section 6.0 content.

7.1. Service Organisational Skill Levels Requirements

0313 To maintain consistency and avoid conflicting information between design documents containing the same information, please refer to SMC SDP document for Section 6.1 content. See Annex D of this SDP for service specific man-power level and skills.

8. SERVICE MEASUREMENT[PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

0314 This section details the mechanisms for collecting, analysing and reporting on component and service metrics and measures that feed into and support agreed-upon KPIs.

8.1. KPI Design

0315 The objective of service measurement is identification and collection of data/information that identifies and quantifies service value-adds and contributions to achieving organisation goals. Service measurement identifies indicators of service risks, issues and improvement opportunities. The objective of service reporting is to analyse and deliver service measurement information (reports) in a format that will facilitate action by decision makers.

0316 Service measurement gathers the data from approved ON/SMC monitoring tools, or from manual data/information gathering methods, and report on progress towards achieving agreed upon KPIs. The service measurement information provides linkage between higher-level ON, service, or process goals and objectives, critical success factors, metrics, and measures. As used in this KPI design, a 'measure' (raw data) is defined as a number derived from taking a measurement, such as the weight or temperature of something, the number of website visits, or the number of logged incidents. In contrast, a 'metric' is defined as a calculation between two measures. The calculation is typically expressed as a percentage, ratio, fraction, decimal or the like.

0317 **Table 38 Technical Support Requirements** is the KPI design for service measurement data and information, and serves as an example provided as part of updating and optimising the KPI design and metrics for each service, monitoring service-based testing, and in support of Full System Acceptance (FSA).

ECS – Enterprise Messaging Service Objective – Provide Email Service and Support to NATO Enterprise	
Critical Success Factor 1.0 [what (actions) must happen to succeed] (Performance Objective)	**Maintain Email Capacity to Meet Current and Future Operational Needs**
KPI ID	1.0.1
KPI Description [If our actions are succeeding (effect)] (Desired Outcome/Result)	Messaging service storage capacity to support operational, backup, and archive messaging needs, per classification enclave
Service Measure 1 (what to measure at the component level) (what would prevent success/outcome/result/ dependencies)	Number of Emails Received (per user/COI/Site); size w/ attachments
Service Measure 2	Number of Emails Sent (per user/COI/Site); size w/ attachments
Component Measure 3	Total Useable Email Storage Capacity
KPI Metric (Formula)	(Total Number of Emails Received & Sent/Total Useable Email Storage Capacity) x 100
KPI Target	>25% Email useable storage capacity, per classification enclave
Frequency	Data Collection Frequency: Daily (7 days per week)
	Reporting Frequency: Monthly (Calendar), by 10th day of following Month
Responsible Parties	Data/Information Collector: GDIT

ECS – Enterprise Messaging Service Objective – Provide Email Service and Support to NATO Enterprise	
	Data/Information Customer: NCI Agency Capacity Manager
Data Source	Microsoft Systems Centre Operations Manager (SCOM)
Reporting Format	For one time snapshot report – stacked bar chart showing proportion of storage capacity required to total usable free disk space
	For trend report – line chart to show progress over each reporting period

Table 38 Technical Support Requirements

0318 The approved NATO ON/SMC tool sets, as mapped to ON processes and service components, used to capture, store, and process (via threshold monitoring) the service-specific KPI measurement data (Section 18, SOW) for use in standardised reports and dashboards in compliance with the NCI Agency's information quality and classification standards. Access control levels used to ensure service measurement data and reports are transparent and available across management and functions based on defined roles and responsibilities.

0319 ECS Service KPI will need to be further defined/refined with linkage to NATO ON service goals and objectives as the detailed design is further developed.

0320 The KPI design solution for service measurement and service reporting includes the following activities, which provide the basis for a standard measurement and reporting process:

- Build, test, and deploy measurement data collection, storage, processing, analysis, and reporting to satisfy KPI requirements.
- Review and evaluate service-critical success factors and KPIs for 'what should be measured' and 'what can be measured' adjusting or (re)negotiating requirements and/or expectations as necessary.
- Provide early life support for transition and review tasks including how to request a report or make changes to a report.
- Deploy measurement and reporting change request and incident reporting procedures as part of process tailoring.
- Update the Service Catalogue if applicable.
- Publish service measurement and service reporting standards.
- Establish service measurement and service reporting controls and governance.
- Provide information to NCI Agency staff/users/support staff so they are aware of service measurement and service reporting capabilities.
- Establish access control levels for reports based on organisation information classification standards.
- Verify service measurement and reporting requirements map to ON standard tool capabilities for capturing, processing and analysing data, and reporting the data/information.
- Continual identification of capability gaps and propose design solution(s) for gap closure.

8.2. KPI Measures and Metrics Analysis and Reporting

0321 Measures and metrics for service-level-defined KPIs will be monitored and collected via four main methods. They are:

- A combination of real-time automated alerts from SMC tools and reports generated by enterprise monitoring personnel.
- Manual review of automated alerts, via SOPs implemented by system administrators
- User reports through service desk and service-desk-ticket tends analysis
- Review of vendor service and equipment maintenance activities

0322 All information related to KPI measurement for availability, capacity and performance is consolidated in the enterprise management dashboard, and analysed as required to ensure that system targets for confidentiality, integrity and availability are maintained.

8.3. Measurement Collection

0323 Measurements to support KPIs are collected on all ECS subservices. The following tables outline the measurements for defined KPI availability, capacity and performance of the service sub-services, dependencies and the monitoring/collection tool set.

Subservice	Measure	Data	Monitoring/Collection
Email	Email delivery delay	Seconds	SCOM
Email	No. of Emails received and No. of emails sent	Per user, COI, site	SCOM
Email	Peak Email sent/ received	Per site, Time of day, rate (emails per minute)	SCOM

Table 39 Messaging Service KPI Collection

Subservice	Measure	Data	Monitoring/Collection
SharePoint	Web page response time	Amount of time required to refresh end-user screen from point that 'enter' command is given from end-user device.	SCOM
SharePoint	Number of hits	Per website, time of day, or event (e.g., NATO summit) related, rate (hits per minute)	SCOM
SharePoint	Number of downloads	Per website, time of day, or event (e.g., NATO summit) related, rate (hits per minute)	SCOM

Table 40 Portal Service KPI Collection

Subservice	Measure	Data	Monitoring/Collection
Database	Database Throughput	It is the volume of work done by database server over a unit of time such as per second, or per hour. It is usually measured as number of queries executed per second.	SCOM
Database	Database Response or Latency	It is the average response time per query, for database server. It shows how long database server has to work before it gets a query result.	SCOM
Database	Database Connections	Number of open database connections to see if they are choking database servers.	SCOM

Table 41 Database Service KPI Collection

ANNEXES

Annex A (SUB)SERVICES INTERFACE CONTROL DOCUMENT [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

A.1. Introduction

0324 This annex will be developed during detailed design and implementation.

Annex B COMPONENT TO ICD MAPPING TABLE [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

0325 This annex will be developed during detailed design and implementation.

Annex C NATO ON PROCEDURES AND WORK INSTRUCTIONS [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

C.1. Introduction

0326 There are five category 1 and 12 category 2 ITIL processes designated to support the NATO ON process implementation (a total of 17 ITIL processes). Each of the 17 ITIL process documents (SOPs/Steps/Work Instructions) is provided in draft form as a separate set of artefacts and are referenced in Section 5 and Annex C of the IaaS, CPS, ECS, and SMC SDPs and for inclusion in the Operations Manual. Each process document includes a process overview diagram with initial roles identified to manage each process.

0327 The Service Operation Function of the service desk includes roles for the specified service operation processes. The service desk function includes the combined role of incident manager/request fulfilment manager and service desk analyst to resolve incidents or service requests. Additional combined roles may be proposed after the final development of the consolidated authority matrix to avoid combining accountability for strongly related processes such as incident and problem management or change and release management. The major ON technical service groupings use applicable ITIL process workflows and linkages as deployed in the BMC ITSM Toolset, online service catalogue or user self-service portal.

0328 The draft ITIL process documentation provides the start point for subsequent process tailoring and reviews of critical success factors and KPIs to meet the NCI Agency's operational needs as part of the tool set implementations. Based on the out-of-the-box ITSM Uplift approach in the NATO Enterprise SMC Systems Document, the draft ITIL processes support the out-of-the-box capabilities of BMC Remedy. The draft ITIL process documentation reflects the NCI Agency–provided process maps and models.

0329 The draft ITIL process documents include links to other processes, sub-processes and functions and are based on the BMC ITSM Toolset user interface, or non–tool set manual processes. A high-level ITIL 2011 Life Cycle Interface Visio Diagram is provided as a supporting document to depict the major data/information flows amongst each of the service life cycle phases and processes. This interface diagram is a working/living diagram and intended to facilitate and support the customization/fine tuning of the draft ITIL processes to meet the NCI Agency's operational needs. In addition, this type of ITIL interface diagram is used to support service-based test scenarios to verify and validate ITIL process information flow and the integration of tool sets, processes, and people. Test scenarios/use cases are based on ITIL process triggers, such as those listed within the ITIL 2011 Edition Publications, or ITSM Toolset training materials developed around use cases to validate user training/skills. These test scenarios are coordinated, reviewed and approved as part of the service transition phase.

0330 The proposed incremental ITIL process implementation follows a related function/logical support grouping approach, with priority to the more visible service operation processes. Category 1 ITIL processes denoted by (1) below are enterprise-level implementations.

[User/End User/Requester Support]

- Event Management
- Incident Management (1)
- Problem Management
- Change Management (1)
- Release and Deployment Management
- Request Fulfilment (1)
- Knowledge Management

  - [Operations Management Support]

- Availability Management
- Capacity Management

- [Integrity of ITSM Support]

- Financial Management for IT Services
- Service Asset and Configuration Management (1)
- Information Security Management (1)
- Access Management
- IT Service Continuity Management
  - [NCI Agency Management Support]
- Service Level Management
  - [Service Planning Support]
- Service Validation and Testing
- Change Evaluation

0331 The proposed model to implement the integrated ITIL processes across people, process, and technology in Wave 1 shown in **Table 42 Process Implementation Model.**

	Process Implementation Model				
People:	Define Roles	Responsibility Matrix	Education and Training	Process Workshops	Refresher Training
Process:	Assess Current State	High Level Process Model	Detailed Integrated Process Model	Process Implementation	Post Implementation Review
Technology:	Tool Requirements	Tool Install	Configure Tool, User and Configuration Account Creation	Tool Available, User Account Creation	Tool Operations and Maintenance

Table 42 Process Implementation Model

C.2. Directory Service

0332 ECS Directory Service SOPs are presented in **Table 43 Directory Service SOP Definition**, including description, actors, frequency of execution, tools, and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
AD-DS	Promote Domain Controller	AD Admin	As Needed	DC Promo	ITM-SOPECSOM-001
AD-DS	Demote Domain Controller	AD Admin	As Needed	DC Promo	ITM-SOPECSOM-002
AD-DS	Create OU	AD Admin	As Needed	ADUC	ITM-SOPECSOM-003
AD-DS	Delete OU	AD Admin	As Needed	ADUC	ITM-SOPECSOM-004

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
AD-DS	Create Machine Object	AD Admin	As Needed	ADUC	ITM-SOPECSOM-005
AD-DS	Delete Machine Object	AD Admin	As Needed	ADUC	ITM-SOPECSOM-006
AD-DS	Create Site	AD Admin	As Needed	ADUC	ITM-SOPECSOM-007
AD-DS	Create Site Link	AD Admin	As Needed	ADUC	ITM-SOPECSOM-008
AD-DS	Create Subnet	AD Admin	As Needed	ADUC	ITM-SOPECSOM-009
AD-DS	Import Schema Modification	AD Admin	As Needed	PowerShell	ITM-SOPECSOM-010
AD-DS	Apply Hotfix/Service Packs	AD Admin	As Needed	Server Manager	ITM-SOPECSOM-011
AD-DS	Create Trust	AD Admin	As Needed	AD Domains and Trusts	ITM-SOPECSOM-012
AD-DS	Transfer or Seize FSMO Role	AD Admin	As Needed	AD Domains and Trusts, AD Users and Computers	ITM-SOPECSOM-013
AD-DS	Perform Authoritative Directory Restore	AD Admin	As Needed	NTDSUTIL	ITM-SOPECSOM-014
AD-DS	Verify Replication Report	AD Admin	1x/day	PowerShell	ITM-SOPECSOM-015
AD-DS	Check DC Event Logs	AD Admin	1x/day	Server Manager	ITM-SOPECSOM-016
AD-DS	Validate AD Trust	AD Admin	1x/week	PowerShell	ITM-SOPECSOM-017
AD-DS	Review Time Sync Report	AD Admin	1x/week	PowerShell	ITM-SOPECSOM-018
AD-DS	Review AuthN Report	AD Admin	1x/week	PowerShell	ITM-SOPECSOM-019
AD-DS	Review SPN Conflicts	AD Admin	1x/week	PowerShell	ITM-SOPECSOM-020
AD-DS	Validate DC Disk Space	AD Admin	1x/week	Server Manager	ITM-SOPECSOM-021

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
AD-DS	Validate Directory Backup	AD Admin	1x/month	[IaaS Team]	ITM-SOPECSOM-022
AD-LDS	Build LDAP namespace	AD Admin	As Needed	Server Manager	ITM-SOPECSOM-023
AD-FS	Create/Delete/Modify Trust	AD Admin	As Needed	AD-FS Console	ITM-SOPECSOM-024
AD-FS	Create Claim	AD Admin	As Needed	AD-FS Console	ITM-SOPECSOM-025
DNS	Create Zone	AD Admin	As Needed	DNS Console	ITM-SOPECSOM-026
DNS	Create Forwarder	AD Admin	As Needed	DNS Console	ITM-SOPECSOM-027
DNS	Create Conditional Forwarder	AD Admin	As Needed	DNS Console	ITM-SOPECSOM-028
ADBA	Add License Key	AD Admin	As Needed	ADBA Console	ITM-SOPECSOM-029
AGPM	Create GPO	AD Admin	As Needed	GPMC Console	ITM-SOPECSOM-030
AGPM	Modify GPO	AD Admin	As Needed	GPMC Console	ITM-SOPECSOM-031
AGPM	Link GPO	AD Admin	As Needed	GPMC Console	ITM-SOPECSOM-032
MIM	Create MA	MIM Admin	As Needed	MIM Sync	ITM-SOPECSOM-033
MIM	Modify MA	MIM Admin	As Needed	MIM Sync	ITM-SOPECSOM-034
MIM	Create Run Profile	MIM Admin	As Needed	MIM Sync	ITM-SOPECSOM-035
MIM	Execute Run Profile	MIM Admin	As Needed	MIM Sync	ITM-SOPECSOM-036
MIM	Modify Schema	MIM Admin	As Needed	MIM Sync	ITM-SOPECSOM-037
MIM	Modify MIM Portal	MIM Admin	As Needed	MIM Portal	ITM-SOPECSOM-038
MIM	Investigate Sync Conflicts	MIM Admin	1x/day	MIM Sync	ITM-SOPECSOM-039

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
MIM	Execute Full Sync	MIM Admin	1x/week	MIM Sync	ITM-SOPECSOM-040
[ALL]	Check all server application logs	[ALL]	1x/day	Windows Event Viewer	ITM-SOPECSOM-041

Table 43 Directory Service SOP Definition

C.3. Email Messaging Service

0333 ECS Email Messaging Service SOPs are presented in **Table 44 Email Messaging Service SOP Definition**, including description, actors, and frequency of execution, tools and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
Exchange	Deploy Mail Server	Exchange Admin	As Needed	EAC	ITM-SOPECSOM-042
Exchange	Export/Import Email	Exchange Admin	As Needed	PowerShell	ITM-SOPECSOM-043
Exchange	Export/Import Email	Exchange Admin	As Needed	PowerShell	ITM-SOPECSOM-044
Exchange	Apply Hotfix/Service Packs	Exchange Admin	As Needed	Server Manager	ITM-SOPECSOM-045
Exchange	Create Send Connectors	Exchange Admin	As Needed	EAC	ITM-SOPECSOM-046
Exchange	Verify Disk Space	Exchange Admin	1x/day	Server Manager	ITM-SOPECSOM-047
Exchange	Verify SMTP Queues	Exchange Admin	1x/day	EAC	ITM-SOPECSOM-048
Exchange	Verify DB Availability and Health	Exchange Admin	1x/day	EAC	ITM-SOPECSOM-049
Exchange	Check Server Application Logs	Exchange Admin	1x/day	Windows Event Viewer	ITM-SOPECSOM-050
Exchange	Check All Services	Exchange Admin	1x/day	Windows Services	ITM-SOPECSOM-051

Table 44 Email Messaging Service SOP Definition

C.4. Skype for Business Service

0334 ECS Skype for Business Service SOPs are presented in **Table 45 Skype for Business SOP Definition** including description, actors, frequency of execution, tools and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
SfB	Run SfB Services Report Script and Mitigate	SfB admin	1x/day	PowerShell, console, etc.	ITM-SOPECSOM-052
SfB	Verify Weekly Rollover of Backup Script	SfB admin	1x/day	PowerShell, console	ITM-SOPECSOM-053
SfB	Run Get-CsManagementStoreReplicationStatus	SfB admin	1x/day	PowerShell	ITM-SOPECSOM-054
SfB	Run Synthetic Transactions	SfB admin	1x/day	Watcher node (optional), PowerShell	ITM-SOPECSOM-055
SfB	Verify SfB Control Panel Topology	SfB admin	1x/day	SfB CSCP Portal	ITM-SOPECSOM-056
SfB	View and Analyse Monitoring Server Reports	SfB admin	1x/day	Microsoft SCOM Portal	ITM-SOPECSOM-057
SfB	Media Quality Summary	SfB admin	1x/day	SQL Report portal	ITM-SOPECSOM-058
SfB	Server Performance Report	SfB admin	1x/day	Microsoft SCOM Portal	ITM-SOPECSOM-059
SfB	Device Report	SfB admin	1x/day	SQL Report portal	ITM-SOPECSOM-060
SfB	Failure Distribution Report	SfB admin	1x/day	SQL Report portal	ITM-SOPECSOM-061
SfB	Top Failures Report	SfB admin	1x/day	SQL Report portal	ITM-SOPECSOM-062
SfB	Verify Daily Backup Script runs	SfB admin	1x/day	PowerShell, schedule tasks log	ITM-SOPECSOM-063
SfB	Peer-To-Peer Activity Report	SfB admin	1x/day	SQL Report portal	ITM-SOPECSOM-064
SfB	Conference Summary Report	SfB admin	1x/day	SQL Report portal	ITM-SOPECSOM-065
SfB	User Activity Report	SfB admin	1x/day	SQL Report portal	ITM-SOPECSOM-066
SfB	View and Remediate Event Viewer Logs	SfB admin	1x/day	Microsoft Event viewer	ITM-SOPECSOM-067
SfB	Verify Archiving functionality	SfB admin	1x/day	PowerShell	ITM-SOPECSOM-068

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
SfB	Check for Skype for Business Updates	SfB admin	1x/day	WSUS /Microsoft SfB portal	ITM-SOPECSOM-069
SfB	Verify SfB Disk Space	SfB admin	1x/month	Microsoft SCOM Portal	ITM-SOPECSOM-070
SfB	Check Certificate Status	SfB admin	1x/year	MMC	ITM-SOPECSOM-071
SfB	Run Skype for Business Best Practices Analyser	SfB admin	1x/year	Skype for Business Best Practices Analyser Tool	ITM-SOPECSOM-072
SfB	Trial Restore from a backup to a lab environment	SfB admin	1x/year	PowerShell, Console	ITM-SOPECSOM-073

Table 45 Skype for Business SOP Definition

C.5. Portal Service

0335 ECS Portal Service SOPs are presented in **Table 46 Portal Service SOP Definition**, including description, actors, frequency of execution, tools and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
SharePoint Central Administration	Create Web Applications	SharePoint Admin	As Needed	Central Administration	ITM-SOPECSOM-074
SharePoint Central Administration	Create Site Collections	SharePoint Admin	As Needed	Central Administration	ITM-SOPECSOM-075
SharePoint Sites / Services	Create Sub Sites	SharePoint Admin	As Needed	Internet Explorer / Connection Point	ITM-SOPECSOM-076
SharePoint Central Administration	Configure Service Applications	SharePoint Admin	As Needed	Central Administration	ITM-SOPECSOM-077
SharePoint Central Administration	Configure Crawl / Search settings	SharePoint Admin	As Needed	Central Administration	ITM-SOPECSOM-078
SharePoint Central Administration	Monitor ULS Logs	SharePoint Admin	Daily	PowerShell	ITM-SOPECSOM-079
SQL Server Administration	Monitor System Logs and SQL Logs	SharePoint / SQL Administrator	Daily	SQL Management Studio	ITM-SOPECSOM-080
SQL Server Administration	Monitor Backups	SharePoint / SQL Administrator	Daily	SQL Management Studio	ITM-SOPECSOM-081

Table 46 Portal Service SOP Definition

C.6. Database Service

0336 ECS Database Service SOPs are presented in **Table 47 Database Service SOP definition**, including description, actors, and frequency of execution, tools and reference number.

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
SQL Server Administration	Monitor System Logs and SQL Logs	SharePoint / SQL Administrator	Daily	SQL Management Studio	[TBC]
SQL Server Administration	Monitor Backups	SharePoint / SQL Administrator	Daily	SQL Management Studio	[TBC]

Table 47 Database Service SOP definition

Annex D OPERATION ROLES AND RESPONSIBILITIES [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

0337 **Table 48 ECS Roles and Responsibilities** below provides service specific role and estimated man-power levels (FTE) required to undertake the ON ECS operational and support tasks. [TBC]

Role	FTE	Education	Experience	Certifications	Skills & Responsibilities

Table 48 ECS Roles and Responsibilities

Annex E PORTS AND PROTOCOLS USAGE

0338 This section describes the ports and protocols used by each of the ECS services.

Port	Protocol	Source	Target	Description
53/tcp/udp	DNS	All Clients All Servers	DNS Servers	Name Resolution
88/tcp	Kerberos	All Windows Clients Domain Controllers	Domain Controllers	Kerberos AuthN Forest Trusts
123/tcp	NTP	All Systems	Stratum 1 Servers Domain Controllers ESXi Hosts	Time Synchronization
135/tcp	RPC	All Clients	All Servers	RPC
137/udp 138/udp 139/udp	NetBT	All Clients	All Servers	NetBIOS over TCP
389/tcp	LDAP	MIM Sync Server	LDAP data sources	LDAP sync
443/tcp	SSL	Federated Clients	AD-FS WAP Servers	HTTPS
445/tcp	SMB	DCs	DFS-R Shares	SYSVOL replication
464/tcp/udp	Kerberos PW	All Windows Clients	Domain Controllers	Password Change
514/tcp	SYSLOG	All Servers	Splunk	Enterprise Audit
636/tcp	LDAP/S	All Clients MIM Sync Server	Domain Controllers LDAP Data Sources	Secure LDAP sync AuthN Forest Trust
1433/tcp	SQL	MIM Sync Server	DB Data Sources MIM DB Server	DB Sync DB Read/Write
3268/tcp	GC	All Windows Clients	Domain Controllers	Global Catalogue Lookup
3269/tcp	GC/S	All Windows Clients	Domain Controllers	Secure Global Catalogue Lookup
3389/tcp	RDP	Admin Clients	All Servers	Remote Management
5722/tcp/udp	DFS-R	DFS-R Servers	DFS-R Servers DFS-R Namespace Servers	DFS-R Replication
49443/tcp	PKI Auth	Federated Clients	AD-FS WAP Servers	PKI Authentication

Table 49 Ports and Protocols Used by the Directory Service

Port	Protocol	Source	Target	Description
25/tcp	SMTP	Clients Application Servers Mailbox Servers Proofpoint Servers McAfee DLP Servers	Mailbox Servers Proofpoint Servers McAfee DLP Servers	SMTP Message Delivery
53/tcp/udp	DNS	Mailbox Servers	DNS Servers	Name Resolution
88/tcp	Kerberos	Mailbox Servers	Domain Controllers	Kerberos AuthN
123/tcp	NTP	Mailbox Servers	Domain Controllers	Time Synchronization
123/tcp	NTP	Mailbox Servers	Domain Controllers	Time Synchronization
135/tcp	RPC	Proofpoint Master	Proofpoint Agents	Configuration Push
143/tcp	IMAP	Mobile Clients	Mailbox Servers	Message Download
443/tcp	SSL	All Clients Admin Clients	Mailbox Servers Titus Reporting Server	OWA Enterprise Admin Console

Port	Protocol	Source	Target	Description
				Message Reporting
445/tcp	SMB	Mailbox Servers	File Share	File Share Witness
465/tcp	SMTP/S	Clients Application Servers Mailbox Servers Proofpoint Servers McAfee DLP Servers	Mailbox Servers Proofpoint Servers McAfee DLP Servers	Secure SMTP Message Delivery
514/tcp	SYSLOG	All Servers	Splunk	Enterprise Audit
636/tcp	LDAP/S	Mailbox Servers	Domain Controllers	Secure LDAP Query
809/tcp	TLS	All Servers	OOS Farm	Document View/Edit
993/tcp	IMAP/S	Mobile Clients	Mailbox Servers	Message Download
3269/tcp	GC/S	Mailbox Servers	Domain Controllers	Secure Global Catalogue Lookup
3389/tcp	RDP	Admin Clients	Mailbox Servers	Remote Management

Table 50 Ports and Protocols Used by the Messaging Service

Port	Protocol	Source	Target	Description
53/tcp/udp	DNS	Skype Servers	DNS Servers	Name Resolution
123/tcp	NTP	Skype Servers	Domain Controllers	Time Synchronization
135/tcp	RPC	Skype F/E Server	Skype F/E Server	Front-End service
443/tcp	HTTPS	Skype Clients Skype F/E Server Reverse Proxy Servers	Skype Servers	User Access Web Farm Communications Mobility Services
445/tcp	SMB	Skype DB Servers Skype F/E Server	DFS-R Share Skype F/E Server	File Share Witness Master Replicator Agent service
448/tcp	SIP	Skype Client	Skype F/E Server	Bandwidth Policy Service
514/tcp	SYSLOG	All Servers	Splunk	Enterprise Audit
1024-65535/tcp/udp	SRTP	Skype Clients	Skype Servers	Audio/Video App Sharing
1433/tcp	SQL	Skype Servers	Skype DB Server	DB Read/Write
1434/udp	SQL Browser	All Servers	Skype DB Server	SQL Browser
3389/tcp	RDP	Admin Clients	Mailbox Servers	Remote Management
5060/tcp	SIP	Skype F/E Server	Skype F/E Server	Front-End service
5061/tcp	SIP	Skype Clients Skype F/E Server	Skype Servers Skype F/E Server	External Dial-In Front-End service
5062/tcp	SIP	Skype Clients	Skype F/E Server	IM Conferencing service
5063/tcp	SIP	Skype Clients	Skype F/E Server	Audio/Video Conferencing service
5064/tcp	SIP	Skype Clients	Skype F/E Server	Conferencing Attendant service
5065/tcp	SIP	Skype Client	Skype F/E Server	Application Sharing service
5067/tcp	TLS	PSTN Gateway	Mediation Servers	Mediation Service
5067/tcp	SIP	Skype Clients	Mediation Servers	Mediation service
5068/tcp	SIP	Skype Clients	Mediation Servers	Mediation Service

Port	Protocol	Source	Target	Description
		PSTN Gateway		
5070/tcp	SIP	Skype Clients Skype Front-End Servers	Mediation Servers	Mediation Service
5070/tcp	SIP	Skype Clients	Mediation Servers	Mediation service
5071/tcp	SIP	Skype Client	Skype F/E Server	Response Group service
5072/tcp	SIP	Skype Clients	Skype F/E Server	Conferencing Attendant service
5073/tcp	SIP	Skype Client	Skype F/E Server	Conferencing Announcement service
5075/tcp	SIP	Skype Client	Skype F/E Server	Call Park service
5076/tcp	SIP	Skype Client	Skype F/E Server	Audio Test service
5080/tcp	SIP	Skype Client	Skype F/E Server	Bandwidth Policy Service
5081/tcp	SIP	Skype Clients	Mediation Servers	Mediation service
5082/tcp	SIP	Skype Clients	Mediation Servers	Mediation service
5086/tcp	MTLS	Skype Servers	Skype Servers	Mobility Services component
5087/tcp	MTLS	Skype Servers	Skype Servers	Mobility Services component
8057/tcp	TLS	Skype Clients	Skype F/E Server	Web Conferencing service
8058/tcp	TLS	Skype Clients	Skype F/E Server	Web Conferencing Compatibility service
8060/tcp	MTLS	Skype Servers	Skype Servers	Web server component
8061/tcp	MTLS	Skype Servers	Skype Servers	Web server component
8080/tcp	HTTPS	Skype F/E Server	Reverse Proxy Servers Skype Servers	Federated User Support Web Component External Access
8404/tcp	MTLS	Skype Client	Skype F/E Server	Response Group service
49152-57500/tcp/udp	SIP	Skype Client	All internal servers	Audio Conferencing
49152-65535/tcp	SIP	Skype Client	Skype F/E Server	Application Sharing service
49443/tcp	HTTPS	Skype Servers	Reverse Proxy Servers	Federated User Support
57501-65535/tcp/udp	SIP	Skype Clients	Skype F/E Server	Audio/Video Conferencing service

Table 51 Ports and Protocols Used by the Skype for Business Service

Port	Protocol	Source	Target	Description
25/tcp	SMTP	Application Server	Exchange Server	Email Delivery
53/tcp/udp	DNS	All Clients All Servers	DNS Servers	Name Resolution
88/tcp	Kerberos	All Servers	Domain Controllers	Kerberos AuthN
123/tcp	NTP	All Servers	Domain Controllers	Time Synchronization

Port	Protocol	Source	Target	Description
137/udp 138/udp 139/udp	NetBT	All Servers	Domain Controllers	NetBIOS over TCP
443/tcp	SSL	Clients AD-FS Servers	Front-End Servers	Website Access
445/tcp	SMB	All Servers	DFS-R Shares	Blob Storage FSW
514/tcp	SYSLOG	All Servers	Splunk	Enterprise Audit
636/tcp	LDAP/S	All Servers	Domain Controllers	Secure LDAP Query
809/tcp	TLS	All Servers	OOS Farm	Document View/Edit
1433/tcp	SQL	All Servers	SharePoint DB	DN Read/Write
3269/tcp	GC/S	All Servers	Domain Controllers	Secure Global Catalogue Lookup
12291/tcp	HTTPS	Front-End Servers	Front-End Servers	SharePoint Workflow Services
49443/tcp	HTTPS	Front-End Servers	Reverse Proxy Servers	Federated User Support

Table 52 Ports and Protocols Used by the Portal Service

Port	Protocol	Source	Target	Description

Table 53 Ports and Protocols Used by the Database Service [TBC]

Annex F SOFTWARE TO BE USED [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

Vendor	Product	Edition	Latest Version	AFPL Latest version	Version to be used
Microsoft	Server	Essentials, Standard, Datacentre	2022 21H2	2019 Ver 1809 build 17763.1697	

Table 54 Software to be Used

Annex G ECS SITE SCOPE

Site ID (location)	Site (name)	City	Country	Node Type	#Users
BEL-BRU-01	NATO HQ	Brussels	Belgium	NS DC Node	23
BEL-CAS-01	Camp Casteau / SHAPE Barracks	Casteau	Belgium	NS Enhanced Node	2389
BGR-GOR-01	Camp Gorna Malina	Gorna Malina	Bulgaria	NS Remote Node	15
CZE-LIP-01	Hranicka Barracks	Lipnik nad Becvou	Czech Republic	NS Remote Node	5
DEU-GEI-01	NATO Air Base Teveren Geilenkirchen	Geilenkirchen	Germany	NS Enhanced Node	145
DEU-RAM-01	Ramstein Air Base	Ramstein-Miesenbach	Germany	NS Enhanced Node	1393
DEU-UED-01	Paulsberg Barracks	Uedem	Germany	NS Standard Node	266
DEU-ULM-01	Wilhelmsburg Barracks	Ulm	Germany	NS Enhanced Node	35
DEU-WES-01	Schill Barracks	Wesel	Germany	NS Standard Node	160
DNK-HAD-01	Haderslev Barracks	Haderslev	Denmark	NS Remote Node	50
ESP-TOR-01	Torrejon Air Base	Torrejon de Ardoz	Spain	NS Standard Node	269
GBR-BLA-01	Blandford Camp	Blandford	United Kingdom	NS Remote Node	10
GBR-NOR-01	Northwood HQ	Northwood	United Kingdom	NS Enhanced Node	836
GRC-PRE-01	Aktion National/Lefkada Airport	Preveza	Greece	NS Remote Node	115
HRV-PLE-02	Marko Zivkovic Barracks	Pleso (Zagreb)	Croatia	NS Remote Node	10
HUN-SZE-01	Zamolyi Barracks	Szekesfehervar	Hungary	NS Remote Node	15
ITA-GRA-01	Grazzanise Air Base	Grazzanise	Italy	NS Standard Node	130
ITA-LAG-01	NATO Base Lago Patria	Lago Patria (Naples)	Italy	NS DC Node	1476
ITA-LEN-01	Naval Air Station Sigonella	Lentini	Italy	NS Enhanced Node	578
ITA-POG-01	Poggio Renatico Air Base	Poggio Renatico	Italy	NS Standard Node	440
ITA-TRA-01	Airport Vincenzo Florio	Trapani	Italy	NS Remote Node	20
LTU-VIL-04	Kairiukscio Barracks	Vilnius	Lithuania	NS Remote Node	10
NLD-BRU-01	Hendrick Barracks	Brunssum	Netherlands	NS Enhanced Node	1615

Site ID (location)	Site (name)	City	Country	Node Type	#Users
NOR-ORL-01	Main Air Station Orland	Orland	Norway	NS Remote Node	20
NOR-STA-01	Jatta Barracks	Stavanger	Norway	NS Enhanced Node	393
POL-BYD-01	Szubinska 2	Bydgoszcz	Poland	NS Enhanced Node	196
POL-BYD-02	Szubinska 105	Bydgoszcz	Poland	NS Standard Node	60
PRT-LIS-01	Avenida Tenente Martins	Lisbon	Portugal	NS Standard Node	106
ROU-BUC-02	HQ Air Force Staff Barracks	Bucharest	Romania	NS Remote Node	15
SVK-RUZ-01	Zarevuca Barracks	Ruzomberok	Slovakia	NS Remote Node	20
TUR-IZM-01	General Vecihi Akin Garrison	Izmir	Turkey	NS Enhanced Node	833
TUR-KON-01	Konya Air Base	Konya	Turkey	NS Remote Node	20
USA-NOR-01	NSA Hampton Roads, Suite 100	Norfolk	United States of America	NS Enhanced Node	1123

Table 55 Site Scope

Annex H DATA CLASSIFICATION MARKINGS (ON)

Classification markings[22]
NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC
NATO UNCLASSIFIED
NATO RESTRICTED
NATO CONFIDENTIAL
NATO SECRET
NATO UNCLASSIFIED RELEASABLE TO <Location, Org>[23]
NATO RESTRICTED RELEASABLE TO <Location, Org>
NATO SECRET RELEASABLE TO <Location, Org>
NATO UNCLASSIFIED
NATO RESTRICTED
NATO CONFIDENTIAL

Table 56 Data Classification Markings

[22] This list of classifications is to be updated

[23] There will be a number of variations for locations and organizations for the “RELEASABLE TO” labels. (e.g. RELEASABLE TO KFOR)