IT MODERNISATION RECOVERY INCREMENT 1

WP07 - Systems Integration and Core Capabilities

Client Provisioning Services (CPS) Service Design Package (SDP)

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:	Client Provisioning Services (CPS) Service Design Package (SDP)
Version:	1.1 RELEASE
Date:	25-Apr-23
Classification:	NATO UNCLASSIFIED
Filename:	NU-ITMRC1- Service Design Package (SDP) CPS
Storage location:	Service Design Package (SDP) CPS

Table of Amendments

Version	Date	Description
0.1	01/12/2022	NCI Agency initial update of SDP to align with architecture and new project scope
0.3	07/12/2022	Adding missing chapters, restructuring the document and addressing major comments.
1.0	20/12/2022	Initial release for Checkpoint 1.
1.1	21st April 2023	Update following change of Datacenter location (CR1) Note: Chapter 4-8 + Annex A-E include outdated figures that require updating.

Author and Reviewers Details

Organisation	Name	Signature
Author	Jean-Francois Suret Jean-Francois.Suret@ncia.nato.int Senior Architect, NCI Agency	Jean-Francois Suret Digitally signed by Jean-Francois Suret Date: 2023.04.25 18:53:30 +02'00'
Reviewer	Marc Mengerink Marc.Mengerink@ncia.nato.int Senior Engineer, NCI Agency	Marc Mengerink Digitally signed by Marc Mengerink Date: 2023.04.25 13:19:05 +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 15:52:29 +02'00'

Contents

List of Figures

List of Tables

1. EXECUTIVE SUMMARY

0001 This Service Design Package (SDP) for the Client Provisioning Service (CPS) outlines design for North Atlantic Treaty Organisation (NATO) Operational Network (ON). The design includes several subservices - physical and virtual desktop delivery, application delivery, Campus LAN, User Profile, Print and Scan, Client provisioning Cyber Security and Client provisioning Service Management and Control. The Purchaser receives a CPS to access the user applications at the required service levels based on an efficient service delivery method. CPS allows all user types to access the services on the Operational Network (ON) from multiple infrastructure nodes Datacentres (DCs), Enhanced Nodes (ENs), Standard Nodes (SNs), Remote Nodes (RNs), and Service Operation Centres (SOC). CPS delivers the benefit to the Purchaser of a centrally managed fit-for-purpose client hardware resources such as desktops or laptops. This SDP provides the overall integrated ON design for CPS The CPS Solution meets the Purchaser’s functional requirements and is fit for purpose. This SDP describes how the solution meets the Purchaser’s performance requirements and is fit for use.

2. INTRODUCTION

0002 The goal of the CPS design is to detail how the CPS subervices deployment are and/or will be implemented (technical design) and operated to provide client services usable from location within the NATO enterprise.

0003 Client Provisioning Services (CPS) consists of 7 services which will be detailed further in the document:

- Campus LAN Services.
- Desktop Provisioning Services.
- Application Provisioning Services.
- User Profile Services.
- Print and Scan Services.
- Client Provisioning Cyber Security Services.
- Client Provisioning Service Management and Control (SMC) Services.

2.1. Purpose and Scope

0004 The purpose of these Client Provisioning Services is to provide the end users secure, coherent, highly cost-efficient, and standardized IT services.

0005 These services will ensure familiar, highly available user-facing services while enabling users to work from the various locations across the NATO Enterprise. Additionally, the standardization and coherent use of technologies will enable the delivery of highly cost efficient services and value realization for the service provider.

0006 The NATO ON CPS Solution leverage the IaaS, ECS and Enterprise SMC services and to enable access to all required user facing services.

2.2. Document organisation

0007 The SDP is organised in the following sections:

- ***Section 3 Service Design and Topology*** **–** Describes Service Internal Architecture and key service/subservice concepts, implementation strategy, and provides the distribution of services to networked NATO ON locations;
- ***Section 4 Service Solution Implementation details*** **–** Describes the sub-service solution and component implementation design for hardware/software, security measures, and implementation design rationale for service levels;
- ***Section 5 Service Management and Tools*** **–** Describes the detailed implementation for hardware/software component design of subservice area domain management and element management;
- ***Section 6 Service Processes*** **–** Provides standard operating procedures associated with NATO ON processes for design;
- ***Section 7 Service organisation Skill Level Requirements*** **–** Provides the level of manpower linked to skill levels;
- ***Section 8 Service Measurement*** **–** Describes solution to collect, analyse and report the required KPI information;
- ***Annex A (Sub)services Interface Control Document (ICD)*** **–** Provides for each subservice where the service is subdivided into multiple subs-services;

- ***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 appendix;
- ***Annex C Procedures and Work Instructions*** – Provides procedures associated with NATO ON processes related to the NATO ON technical services groups (IaaS, CPS, ECS); and
- ***Annex 4 Operation Roles and Responsibilities*** – Provides manpower required to undertake NATO ON operational and support task.
- ***Annex E - Virtual Desktop Design*** – provides the design and topology of the Virtual Desktop parts of the Desktop and Application provisioning subservices.

2.3. Points of Contact

0008 The CPS SDP is under the responsibility and maintained by ITM Engineering Team itm.engineering@ncia.nato.int .

0009 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

2.4. Glossary

0010 Table 1 below, lists common abbreviations and acronyms found throughout this document.

Acronym or Term	Definition
ACT	Allied Command Transformation
AD	Active Directory
AD-DS	Active Directory - Directory Services
AD-FS	Active Directory - Federated Services
AD-LDS	Active Directory - Lightweight Directory Services
AGS	Alliance Ground Surveillance
API	Application Projecting Interface
APT	Advance Persistent Threat
CA	Certificate Authority
CAS	Central Administration Site
CPS	Client Provisioning Services
CPU	Central Processing Unit
DB	Database

Acronym or Term	Definition
DC	Domain Controller
DDR	Discovery Data Record
DFS-R	Distributed File System Replication
DHCP	Dynamic Host Configuration Protocol
DLPe	Data Loss Prevention Endpoint
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name System
DPM	Data Protection Manager
DSM	Dual Stack Model
EAC	Exchange Administrative Centre
ECS	Enterprise Core Services
ENS	Endpoint Security
FIM	File Integrity Monitor
GB	Gigabyte
GPO	Group Policy Object
HA	High Availability
HTML	Hypertext Transfer Mark-up Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
IaaS	Infrastructure as a Service
ICD	Interface Control Document
IIS	Internet Information Service
IOPS	Input/Output Operations Per Second
IP	Internet Protocol
IPS	Exploit Prevention
ISE	Identity Services Engine
NATO ON	NATO Operational Network
JFC	Joint Force Command
KMS	Key Management Services
KPI	Key Performance Indicator
LAN	Local Area Network
LANDCOM	Land Command
LDAP	Lightweight Directory Access Protocol
MA	Management Agent
MAK	Multiple Activation Key

Acronym or Term	Definition
MIM	Microsoft Identity Manager
MnT	Monitoring and Troubleshooting Node
MSMS	McAfee Security for Microsoft SharePoint
NAC	Network Access Control
NATO	North Atlantic Treaty Organisation
NCS	NATO Command Structure
NHQ	NATO Headquarters
NPKI	NATO PKI
NR	NATO Restricted
NS	NATO Secret
NTP	Network Time Protocol
NU	NATO Unclassified
OU	Organisational Unit
P2P	Peer-to-Peer
PAN	Policy Administration Node
PKI	Public Key Infrastructure
PSN	Policy Service Node
PXE	Preboot Execution Environment
QoS	Quality of Service
RAM	Random Access Memory
RBAC	Role-Based Access Control
RDL	Remote Desktop Licensing
RDS	Remote Desktop Services
RDSH	Remote Desktop Session Host
RF	Radio Frequency
RFC	Request For Comments
RMS	Remote Management Server
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SADR	Super-Agent Distributed Repositories
SAML	Security Assertion Mark-up Language
SAN	Subject Alternative Name
MECM	Microsoft Endpoint Configuration Manager
SDP	Service Design Package
SHAPE	Supreme Headquarters Allied Powers Europe
SID	Security Identifier

Acronym or Term	Definition
SMB	Server Message Blocks
SMC	Service Management And Control
SOC	Service Operations Centre
SOP	Standard Operating Procedure
SQL	Structured Query Language
SSL/TLS	Transport Layer Security / Secure Sockets Layer
TB	Terabyte
TBD	To Be Determined
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TIP	Trusted Identity Provider
UCE	Unsolicited Commercial Email
UDP	User Datagram Protocol
UEM	Unified Endpoint Management
ULS	Unified Logging System
VDI	Virtual Desktop Infrastructure
VIP	Virtual IP
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
WAL	Workflow Activity Library
WSUS	Windows Server Update Services

Table 1 - Glossary

2.5. Reference Documents

0011 This SDP expects the reader to have ready access to all the reference documents listed in Table 2 below. These reference documents provide the necessary additional supporting details for the full contextual understanding of the interdependency information, which is being presented in this design document.

Document	Description
Architecture Document Package ADP	Describes the NATO ON services, systems, organizational entities, and their relationships to each other and to their environment
Service Design Package ECS	Describes the NATO ON directory services, email messaging, unified communications and portal services.
Service Design Package IaaS	Describes the NATO ON Networking, IaaS, Storage, Security services.
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

Table 2 - References

3. SERVICE DESIGN AND TOPOLOGY

0012 The ADP is the overarching document describing the services implemented and/or leveraged to establish the NATO ON.

0013 This SDP details the CPS services and subservices required to implement the NATO ON.

0014 This SDP is part of the authoritative source of information regarding Architecture and Design aspects.

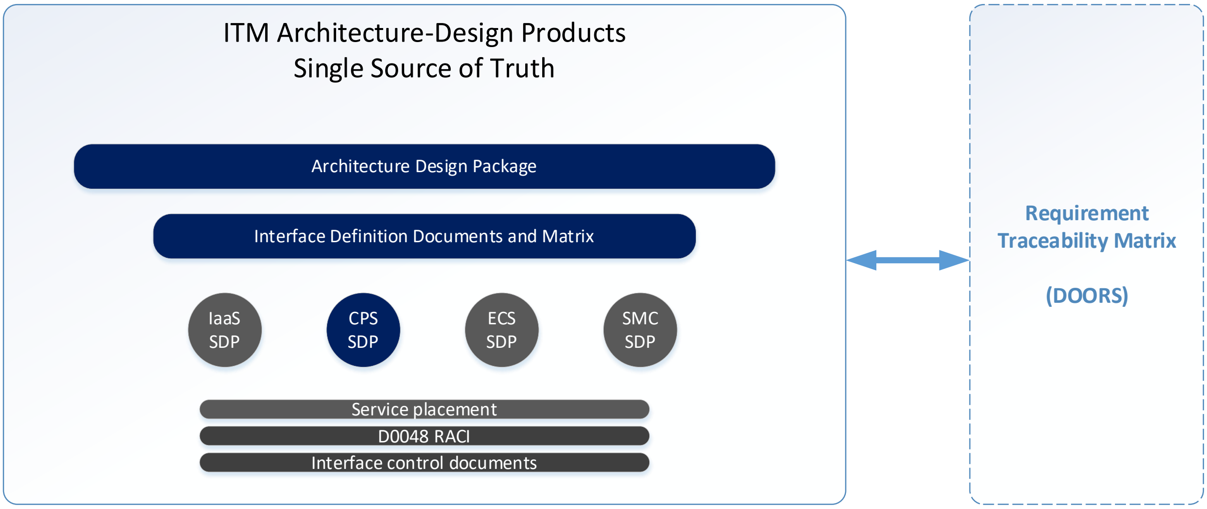

ITM Architecture-Design Products
Single Source of Truth
Architecture Design Package
Interface Definition Documents and Matrix
IaaS SDP
CPS SDP
ECS SDP
SMC SDP
Service placement
D0048 RACI
Interface control documents
Requirement Traceability Matrix
(DOORS)

Figure 1 - Architecture-Design Products

3.1. NATO Operational Network Client Provisioning General Aspects

0015 The NATO Operational Network Client Provisioning Services (NATO ON CPS) are designed to provide users with a digital desktop environment, to further use and access the NATO ON services and applications, from the various subscriber sites of the NATO Enterprise.

0016 Client Provisioning Services are providing the required component and services to establish NATO ON user Node. The user nodes are composed of all elements required for a user to further gain access to the NATO ON services regardless of where the services are hosted.

3.2. Service Model

0017 The CPS service consists of 7 subservices as described in the NATO ON service tree.

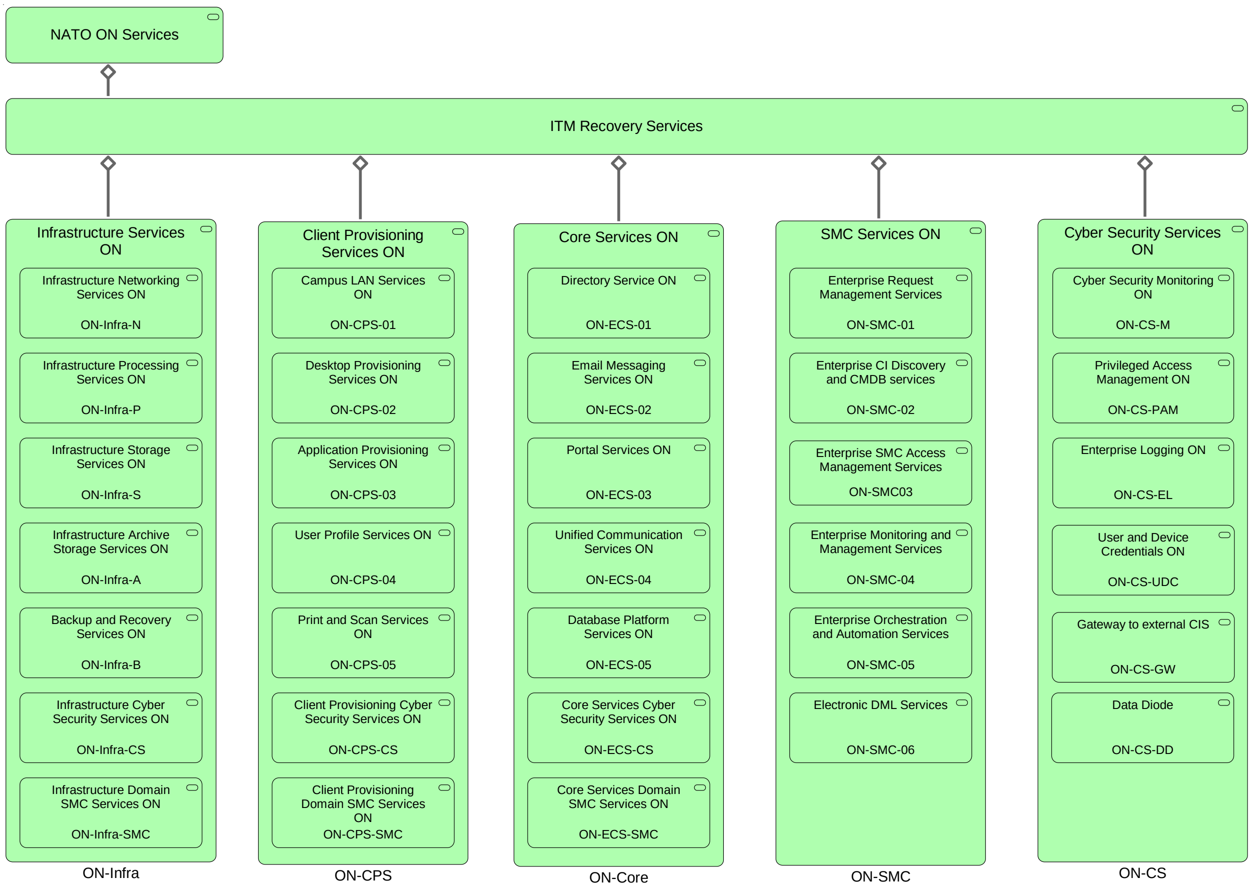

NATO ON Services
ITM Recovery Services
Infrastructure Services ON
Infrastructure Networking Services ON
ON-Infra-N
Infrastructure Processing Services ON
ON-Infra-P
Infrastructure Storage Services ON
ON-Infra-S
Infrastructure Archive Storage Services ON
ON-Infra-A
Backup and Recovery Services ON
ON-Infra-B
Infrastructure Cyber Security Services ON
ON-Infra-CS
Infrastructure Domain SMC Services ON
ON-Infra-SMC
ON-Infra
Client Provisioning Services ON
Campus LAN Services ON
ON-CPS-01
Desktop Provisioning Services ON
ON-CPS-02
Application Provisioning Services ON
ON-CPS-03
User Profile Services ON
ON-CPS-04
Print and Scan Services ON
ON-CPS-05
Client Provisioning Cyber Security Services ON
ON-CPS-CS
Client Provisioning Domain SMC Services ON
ON-CPS-SMC
ON-CPS
Core Services ON
Directory Service ON
ON-ECS-01
Email Messaging Services ON
ON-ECS-02
Portal Services ON
ON-ECS-03
Unified Communication Services ON
ON-ECS-04
Database Platform Services ON
ON-ECS-05
Core Services Cyber Security Services ON
ON-ECS-CS
Core Services Domain SMC Services ON
ON-ECS-SMC
ON-Core
SMC Services ON
Enterprise Request Management Services
ON-SMC-01
Enterprise CI Discovery and CMDB services
ON-SMC-02
Enterprise SMC Access Management Services
ON-SMC03
Enterprise Monitoring and Management Services
ON-SMC-04
Enterprise Orchestration and Automation Services
ON-SMC-05
Electronic DML Services
ON-SMC-06
ON-SMC
Cyber Security Services ON
Cyber Security Monitoring ON
ON-CS-M
Privileged Access Management ON
ON-CS-PAM
Enterprise Logging ON
ON-CS-EL
User and Device Credentials ON
ON-CS-UDC
Gateway to external CIS
ON-CS-GW
Data Diode
ON-CS-DD
ON-CS

Figure 2 - NATO ON Service Tree – confined to ITM Recovery Increment 1 scope

3.3. Campus LAN Subservice Topology

0018 The Campus LAN service provides interfaces for all end-user devices including NS workstations, NS telephones, NS VTC, NS LAN device management and any other specific community of interest endpoints.

0019 The Campus LAN service is delivered as a Software Defined Access (SD-Access) solution composed of switching fabric, SD-Access components, and it interfaces with the wide area network. All networking services are implemented as dual stack supporting IPv6 and IPv4.

3.3.1. Security separation.

0020 The Campus LAN is leveraging Network Access Control (NAC with 802.1x) to provide end-user device authentication.

0021 The Campus LAN is configured to:

- Authenticate devices, based on NPKI certificates,
- Verify their security posture,
- Assign them in the appropriate virtual LAN (VLAN) or scalable group tags (STGs)
- Enforce separation of devices in segregated logical network groups,
- And apply network access controls specific to such group.

3.3.2. Switching Fabric

0022 The switching fabric is composed of Cisco switches. The switching topology used is a redundant collapsed core campus switching architecture. This topology is composed of two layers, the core/aggregation layer, and the edge/access layer. In this topology, the core and aggregation functions are performed by the same layer (core/aggregation devices) instead of being separate layers.

0023 The edge/access layer is used for connecting endpoints. Edge/access switches have an uplink to the core/aggregation switches.

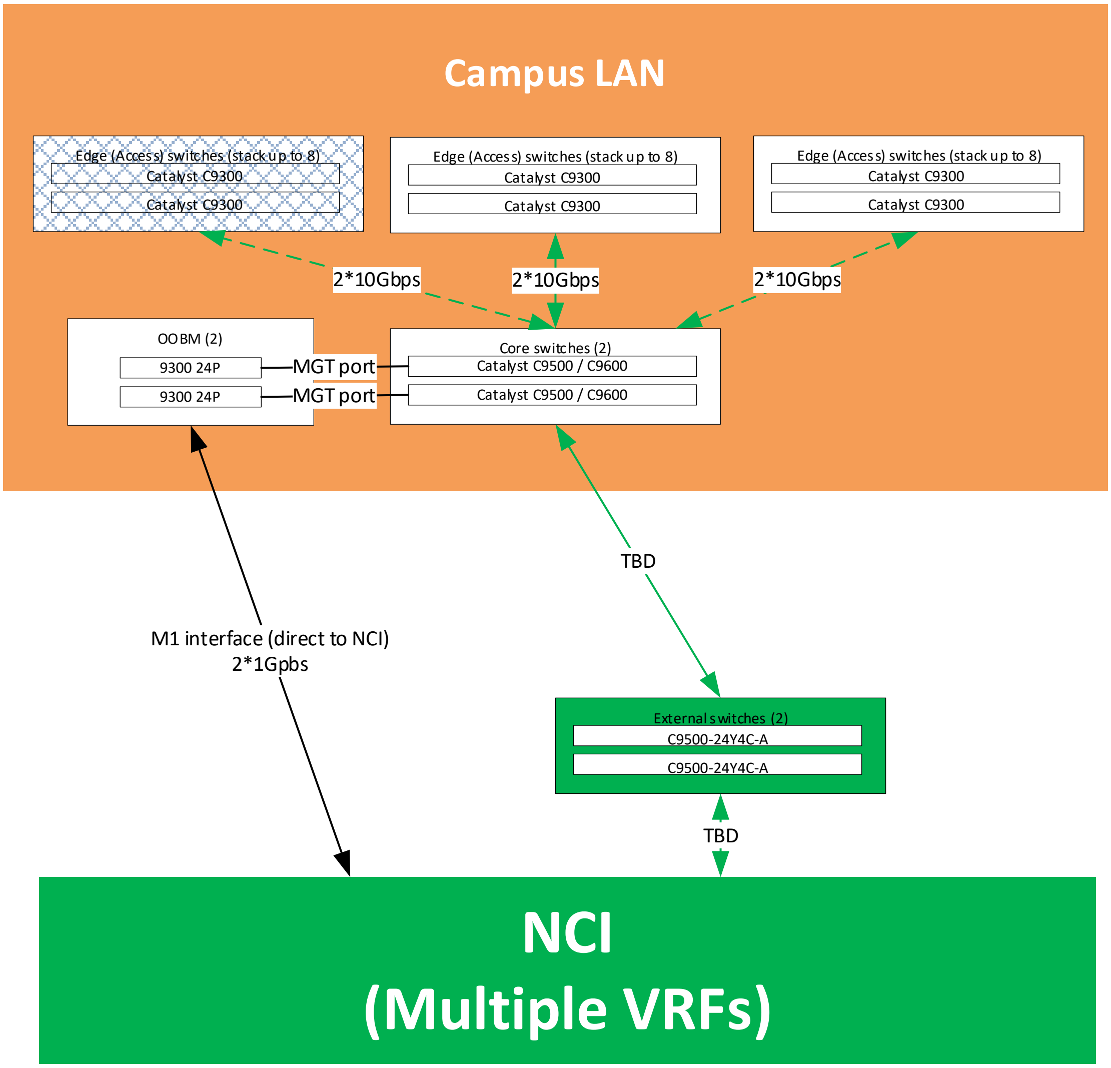


Figure 3 - Switching Fabric Topology for EN and SN

0024 For small sites (e.g. remote nodes), the three functions, core, aggregation and access are collapsed in a single layer.

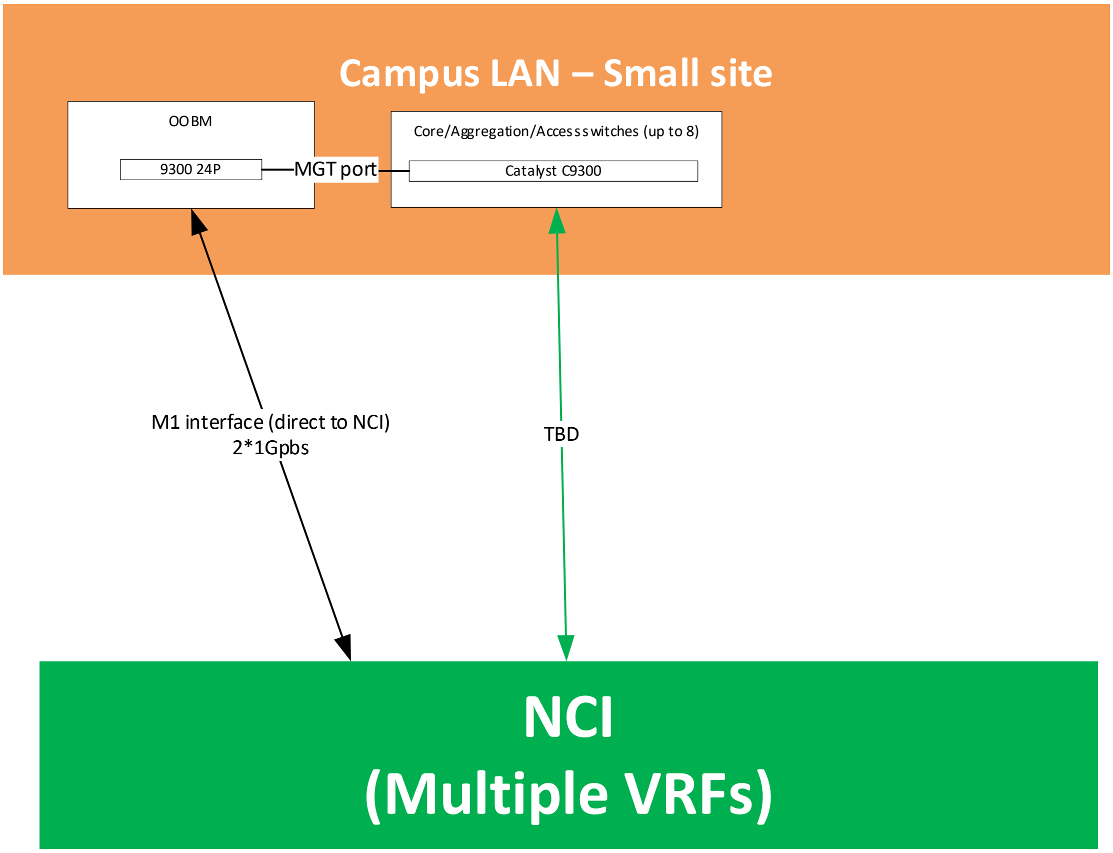


Figure 4 - Switching Fabric Topology for small sites (RN)

0025 In addition out of band management switches are used for the management and configuration of the network fabric to provide resilient access in case of outages.

0026 NATO ON Campus LAN switching equipment listed below detail the product models and their corresponding use case.

Product	Use Case
Catalyst C9500 or C9600	Core/Aggregation for EN/SN
Catalyst C9300	Access switches for EN/SN
TBD	Collapsed core/access for Remote nodes
Cisco C9300_24T_A	Out of band management switches
Cisco C9500_24Y4C_A_	External switches

Table 3 - NATO ON Campus LAN Switching Fabric

3.3.3. SD-Access components

0027 Both cisco DNA Center and Cisco Identity Services Engine (ISE) are required to manage and monitor the Campus LAN Services:

3.3.3.1. Cisco DNA Centre:

0028 Cisco DNA Centre is used to manage the SD-Access network. Cisco DNA Center consists of following workflows:

- Design: Device global settings, site profiles, templates.

- Policy: Virtual networks, endpoint assignment, policy contract, QoS
- Provision: Device provisioning and inventory management.
- Assurance: Proactive monitoring with analytics.
- Platform: Provides northbound interface for other applications through APIs.

0029 Cisco DNA center is deployed as a three node deployment as part of the NCI Domain service management system (DSMS) spread across the datacentres to provide high availability.

Sub-service/component	Security Zone	Tenancy type	Identity domain	Clustering Domain	Resource Cluster	Site
SD-Access management (DNA Center)	Not Applicable	Not Applicable	NCI DSMS	Not Applicable	Not Applicable	DC

Table 4 - SD-Access

3.3.3.2. Cisco Identity Services Engine (ISE):

0030 ISE is an integral and mandatory component of SD-Access for implementing network access control policy. ISE performs policy implementation, enabling dynamic mapping of users and devices to scalable groups, and simplifying end-to-end security policy enforcement.

0031 While Cisco ISE through the tightly integrated REST APIs administers the configuration elements (e.g. scalable group tags SGTs), Cisco DNA Center is used as the pane of glass to manage and create configuration elements and define their policies.

0032 ISE is composed of 3 elements, Policy administration nodes (PAN) deployed in the Datacentres (NCI DSMS), Monitoring and Troubleshooting Node (MnT) deployed in the datacentres (NCI DSMS) and Policy Service Nodes(PSN) deployed in datacentres and Enhanced Nodes.

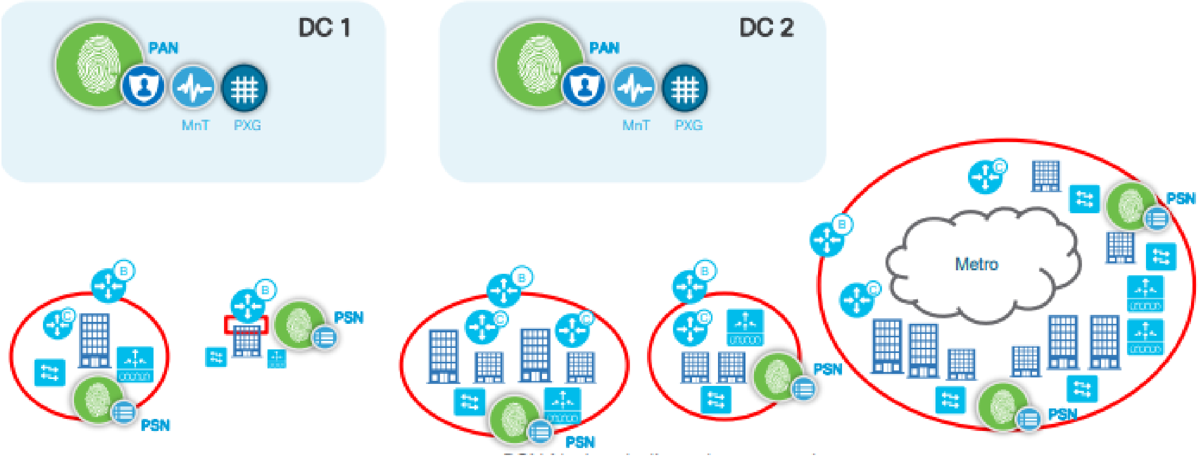


Figure 5 - SD-Access ISE Deployment

Sub-service/component	Security Zone	Tenancy type	Identity domain	Clustering Domain	Resource Cluster	Site
Identity service (ISE) - Policy Service Nodes (PSN)	Not Applicable	Not Applicable	NCI DSMS	NCI DSMS	NCI DSMS	DC,EN
Identity service (ISE) - Policy Administration node (PAN)	Not Applicable	Not Applicable	NCI DSMS	NCI DSMS	NCI DSMS	DC
Identity service (ISE) - Monitoring and Troubleshooting (MnT)	Not Applicable	Not Applicable	NCI DSMS	NCI DSMS	NCI DSMS	DC

Table 5 - Identity Services

3.3.4. NCI Wan Interface

0033 Each Campus LAN Node must interface to the WAN via the external switches deployed at the site.

0034 The connexion must provide logically segregated connectivity to support the separation of the defined community of interest (COI). For each COI, a logical routing instance (VRF) is required to be extended over the WAN via SIOP-5 interfaces (logical separation).

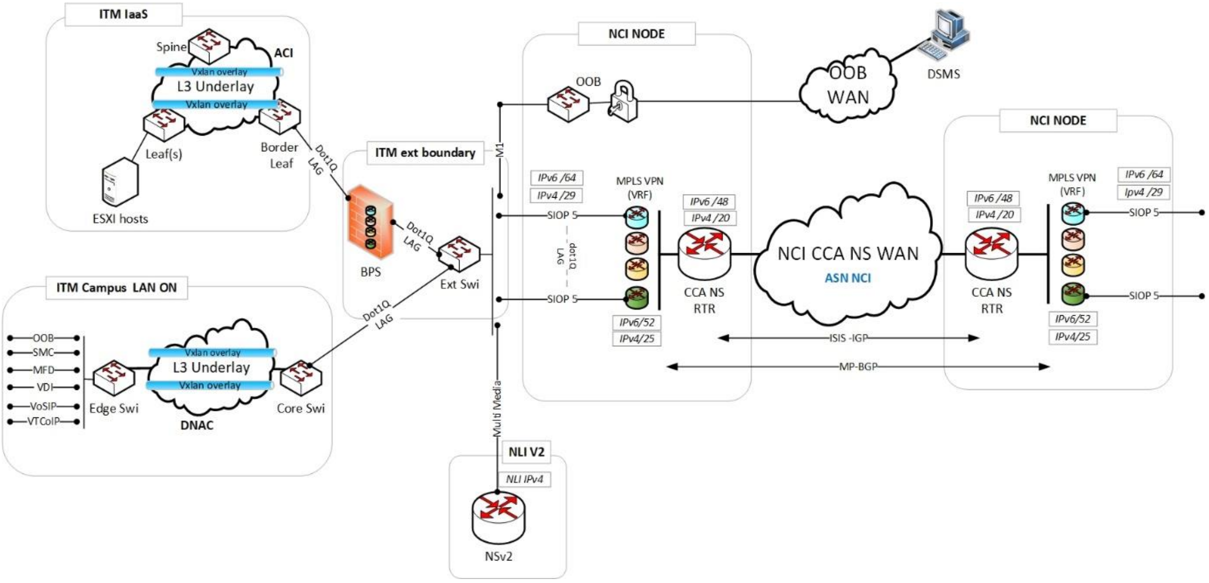


Figure 6 - NATO ON Campus LAN and NCI Interconnectivity

0035 The details on how the routing is implemented is/will be detailed in the service solution section.

3.4. Desktop Provisioning

0036 Desktop Provisioning Subservice consists of Virtual Desktop, Physical Desktop, and Thin client.

3.4.1. Service Distribution

0037 The distribution of Desktop subservice components is shown in Table 6 below.

Subservice	System Component	Datacentre	Node Deployment (refer to IaaS SDP)
Virtual Desktops	VDI Pod	All Datacentres +	Datacenters and VDI locations
Virtual Desktops	Wyse Management Suite	All Datacentres	Datacenters and VDI locations
Desktop and Application Delivery	MECM – Primary Server	All Datacentres	Datacenters
Desktop and Application Delivery	MECM – Distribution Server	All Datacentres	All Enhanced/Standard Nodes where IaaS infrastructure is present
Application Delivery	VMware AppVolumes	Same as Virtual Desktops subservice above	
Application Delivery	RDSH (users) and RDSH (administrators)	All Datacentres	Datacenters

Table 6 - Service Distribution

3.4.2. Client Device Baseline Definition

0038 This baseline definition aims to provide a description of minimum software required to operate in any of the information domains to create a common understanding and promote interoperability.

0039 The baseline definition at a glance:

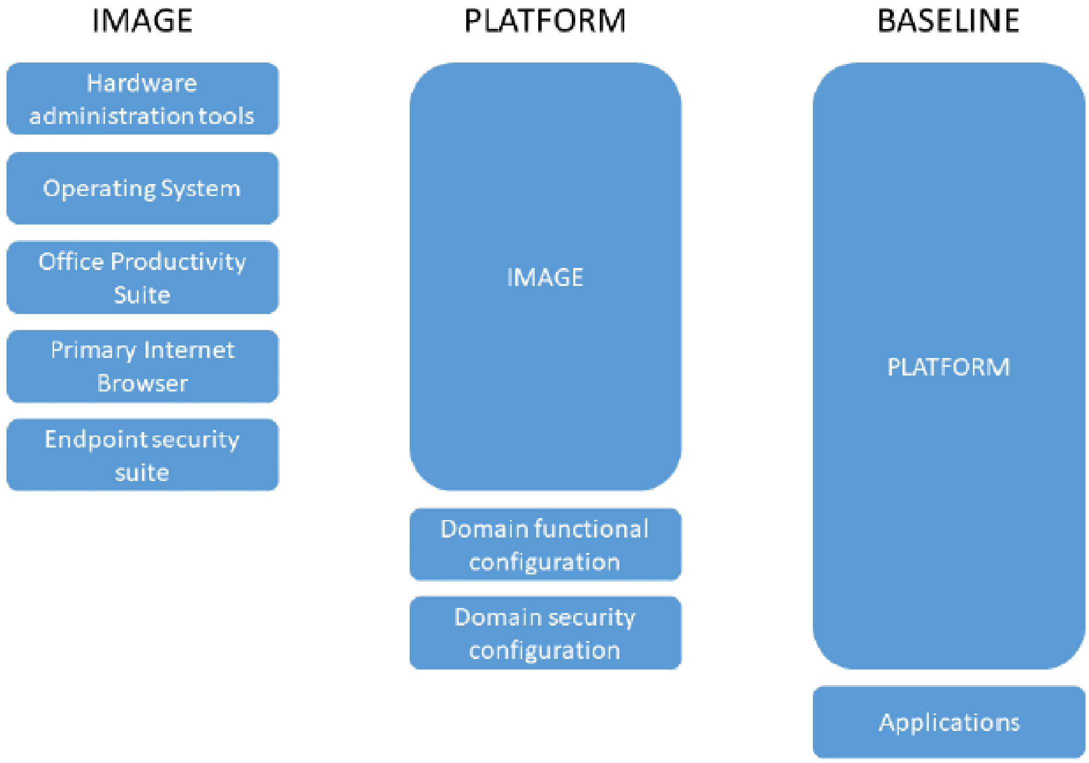


IMAGE
Hardware administration tools
Operating System
Office Productivity Suite
Primary Internet Browser
Endpoint security suite
PLATFORM
IMAGE
Domain functional configuration
Domain security configuration
BASELINE
PLATFORM
Applications

Figure 7 - Client Device Baseline

3.4.2.1. Image

0040 The image will contain minimal software necessary to use on any information domain and is device type dependent. All software installed with the image is mandatory for all end user devices in scope. The minimal software components that comprise the image are:

- Hardware administration tools which enable hardware monitoring and configuration such as BIOS, driver updates (when applicable);
- Microsoft Windows client operating system;
- Microsoft Office productivity suite;
- Primary Internet browser;
- Endpoint security suite;
- Security and forensic applications;
- Supplicant to enable 802.1x NAC/NAP (when applicable).

3.4.2.2. Platform

0041 In addition to the core image, various platforms will have additional software such as:

- Message and file classification and marking software;
- PKI integration software;
- Smartcard management software;
- VDI enabling agents.

3.4.2.3. Baseline

0042 The baseline is what the end users are using and it contains in addition to the platform any user-specific applications (either commercial or NATO-developed) together with the required dependencies and configuration.

3.4.3. Virtual Desktop

0043 The Virtual Desktop Subservice topology and design is described in Annex E to keep the coherence and completeness of the Virtual Desktop solution.

3.4.4. Physical Desktop

0044 The Microsoft Endpoint Configuration Manager (MECM) Operating System Deployment feature provides MECM administrative users with a tool for creating task sequences deploying to physical desktops regardless of model and VDI master images. The task sequence consists of a Windows client operating system image, a boot image, device drivers and the complete list of applications for the NATO client platform. The MECM infrastructure distributes all of the task sequence components to the DCs, ENs and SNs. Desktops will PXE boot into a task sequence in order to receive the image from MECM from the local (or closest distribution point server).

0045 The client device is a fixed client physical desktop (diskless or not)**.** Physical desktops provision via MECM using boot media, PXE Boot or offline USB Media with a hardened Windows client Enterprise operating system and all of the applications in the NATO platform**.** A PXE boot occurs in a NAC-enabled environment. Once the machine is on the network in the staging area, it receives a NPKI machine certificate becoming NAC compliant. MECM provides follow-on maintenance of the physical desktops such as operating system patching, Windows feature updates and third-party software updates at regular intervals.

0046 Physical desktop interoperate with NAC solution, which satisfies the requirement.

3.4.5. Thin Client

0047 The Wyse Management Suite provides administrative users with tools for the deployment and management of the thin clients. For example, a task to deploy the Windows client/IoT operating system image, the VMware Horizon Client, management agents and system patches. Thin clients will be deployed with Windows IOT to create a lightweight deployment that minimizes end-point configuration and shifts the majority of management to the centralized services in VDI.

0048 Thin clients will be deployed to a desk and upon initial start-up will obtain the necessary configuration via DHCP scope options to register with WMS using an official NATO PKI certificate to receive the policies and required Windows IOT image. The WMS application will run discover probes on a daily basis to discover, interrogate and inventory all newly provisioned devices. This data will be moved to the central CMDB via True-sight database update pulls. Once registered with WMS server, the thin client will receive all the necessary policies. Items such as login banners and lock screen will be instituted via policy to ensure they match configuration to NATO.

0049 All thin client management will be performed by the Wyse Management Suite to centrally manage and configure the deployed clients. Wyse Management Suite instance will be deployed in one of the datacentres and a remote repository server will be deployed in each datacentre, enhanced and standard node where VDI is deployed. High-availability of WMS is achieved via the backup and restore service. Updates to the thin clients will be packaged and deployed monthly to ensure devices have up to date patches. Each WMS repository will host an authoritative source of software, Operating Systems and patches. WMS will house all approved images for Windows IOT that will be used on the end points. Additionally, all updates for any applicable software and patches will be added to centralized repository for consumption by the WMS nodes. The gold images for Windows IOT will be updated regularly to keep all devices secure. In tandem with gold image update, monthly patch deployments will occur on the thin clients and non-compliance with patching schedules will be reported to the centralized Wyse Management Suite. Windows IOT baseline will include the deployment of PKI certificate for NAC compliance (via WMS).

0050 Wyse Management Suite will track all assets that are deployed at each individual node. This data will be pulled by BMC Atrium into the centralized configuration management database. The WMS will also manage all alerts and reports generated from individual thin clients. Errors related to issues such as authentication failures, application crashes, new image deployment failures, etc. These error logs are collected by the WMS for review by SOC admins. Additionally alerts will be forwarded to logging services (Splunk) to ensure they are available for review.

3.4.6. Updates, upgrades and patching

0051 While the NCI Agency will endeavour to define in advance the versions of the software to be used for the implementation activities in scope and maintain them until the piece of work is handed over from the Contractor to the Purchaser, it is recognized that the work, the Contractor is performing in the scope of this CPS services, contributes to the overall security posture of the NATO network(s). This entails that during implementation and integration activities, the Contractor shall keep the systems up to date at all times, this to include:

- Update of endpoint security definitions;
- Regular updates for Microsoft products after Purchaser’s internal testing and approval process has been completed (outside the scope of the CPS services).

0052 In an event, when a major or minor version updates of software product(s) (such as McAfee ePO, VMware Horizon, etc.) are required due to cybersecurity threats, this will be raised as an exception and handled with urgency.

3.5. Application Provisioning Subservice Topology

0053 The Application Provisionoing subservice consists of two components – Microsoft Endpoint Configuration Manager and Remote Desktop Session Hosts for users and administators.

3.5.1. Microsoft Endpoint Configuration Manager

0054 Microsoft Endpoint Configuration Manager (MECM) is leveraged for any local application provisioning. MECM management services are deployed at the datacentres locations, while distribution repositories are implemented at all sites where an IaaS is available.

Sub-Service/ Component	Security Zone	Tenancy type	Identity domain	Clustering Domain	Site
Microsoft Endpoint Configuration	Common Infrastructure and Common Core Services (NATO-ON-SZ-SRV-001)	Multi-Tenant	Global NS (Service) - SVC	Workload domain	DC

Manager - MECM					
Microsoft Endpoint Configuration Manager - MECM Distribution Repository NS AIS	ACT/ACO (Bi-SC) (NATO-ON-SZ-TNT-001)	Multi-Tenant	NS AIS - IDF	Workload domain	DC,EN,SN

Table 7 - Microsoft Endpoint Configuration Manager

3.5.2. Remote Desktop Session Hosts

0055 Remote Desktop Session hosts (RDSH) is used for remote application delivery. RDSH services are deployed at the datacenters and separate environment are deployed for administrators and “tenant” end users.

Sub-service/ Component	Security Zone	Tenancy type	Identity domain	Clustering Domain	Site
RDS (administrators)	Common Infrastructure and Common Core Services (NATO-ON-SZ-SRV-001)	Multi-Tenant	Global NS (Service) - SVC	Workload domain	DC
RDS (users)	ACT/ACO (Bi-SC) (NATO-ON-SZ-TNT-001)	Multi-Tenant	NS AIS - IDF	Workload domain	DC

Table 8 - Remote Desktop Session

3.5.3. VMware AppVolumes

0056 Due to the tight integration with the VDI subservice, VMware AppVolumes is described in Annex E.5.

3.6. User Profile Subservice Topology

0057 Profile Management is key to the success of any VDI and physical desktop deployment. When utilising VDI and physical desktops in a non-persistent fashion users still require the perception of a persistent desktop, meaning maintaining the user’s session, user data and application customizations (i.e., favourites, redirected folders, user level operating system customizations and layout).

0058 User profile management solution provides consistent end user experience (look and feel) and access to user data regardless of where the user logs on – either a VDI desktop or a physical desktop.

0059 The user profile consists of two main components:

3.6.1. User settings and preferences

0060 The user preferences are Windows OS and application specific settings that are customized by the end users and shall roam regardless where the user logs in (on AIS in the scope of the project).

3.6.2. User data

0061 The user data share will be the primary location for storing user data (such as documents, spreadsheets, etc.) The user data share will have a quota per user.

0062 The user data will be stored at the primary site of the end user and made highly available via DFS Replication, see ECS SDP document for further details. The user data will be replicated for failover to a datacentre location. Should site failover is required to be executed, the user data share may failover in a manual way. When the end user logs in from another location, s/he will access the user data via the same entry point as usual over the network.

3.7. Print and Scan Subservice Topology

0063 The printing and scanning service is already existing and in use across many NCS sites in a managed printing service fashion with an external provider. The NATO ON will integrate with the service and extend its coverage to the sites in scope of CPS SDP. The service consists of the following components:

3.7.1. Multifuncational devices

0064 The service uses external contractor provided and owned devices and complementery services.

3.7.2. Follow-me printing and scanning backend

0065 The service uses backend servers and software which provide the follow-me printing and scanning functionality across all the sites. The backend uses with Directory and Email services for user identities and scanning functionality respectively.

0066 In order to support the service, printer servers are deployed at all DC,EN and SN locations.

Sub-service/component	Security Zone	Tenancy type	Identity domain	Clustering Domain	Site
Print Servers	Common Infrastructure and Common Core Services (NATO-ON-SZ-SRV-001)	Multi-Tenant	Global NS (Service) - SVC	Workload domain	DC,EN,SN

Table 9 - Remote Desktop Session

3.8. Client Provisioning Cyber Security Subservice Topology

0067 All services deployed as part of Client Provisioning services integrates or supplement NATO Cyber Security services. Client provisioning services include specific cyber security components described in 0189.

3.8.1. Integration with NATO Enterprise Logging and SIEM.

0068 All CPS services are integrating with the NATO Enterprise logging/SIEM based on Splunk.

0069 Systems are configured either to :

- Send the logs to the logging server/ Splunk Heavy forwarder
- Provide a mechanism to allow the Splunk heavy forwarder to pull the logs from the target.

3.8.2. Endpoint protection

0070 The Cyber Security subservice includes endpoint protection tools which are present on all servers and clients as per the implementation details in the next chapter.

3.8.3. Security controls

0071 The Cyber Security subservice contains as well security controls which are implemented on the respective endpoints. In the next chapter are detailed the security controls related specifically to the client devices

3.8.4. NATO Cyber Security Services Integration

0072 The NATO Cyber Security Center (NCSC) is delivering, managing and operating NATO Cyber Security Services. The NATO ON CPS services deployed are integrated with those services. This will follow the same principle as described in the IaaS SDP Chapter 2.7.

3.9. Client Provisioning Service Management and Control (SMC) Subservice Topology

3.9.1. Campus LAN

0073 The component used for managing and controlling the Campus LAN services are described in 3.3.3. In addition, the component integrate with Enterprise SMC and NCI DSMS

3.9.2. Desktop Provisioning

0074 End-user monitoring has for main objective to gather metrics and allow the evaluation of end-user experience based on them for both VDI and physical desktops connected via the Campus LAN service.

0075 The metrics collected include basic endpoint performance, network performance and latency, logon performance, desktop session performance, including applications and processes and in the case of a VDI desktop, the relevant backend measures (CPU, memory, datastore performance, network latency, VMware performance).

0076 The subservice implementation include the deployment of the required backend components and endpoint agents to the VDI and physical desktops in scope. This includes as well, the initial configuration of data gathering and built-in reporting functionality.

3.9.3. Enterprise SMC

0077 The NATO ON IaaS domain SMC services integrate with the Enterprise SMC services. For each domain SMC service/tool, identification of the required type of interface will be defined as part of the detailed design and detailed in the separate IDD (Interface Description Document) matrix.

0078 The interfaces will follow the approach described below:

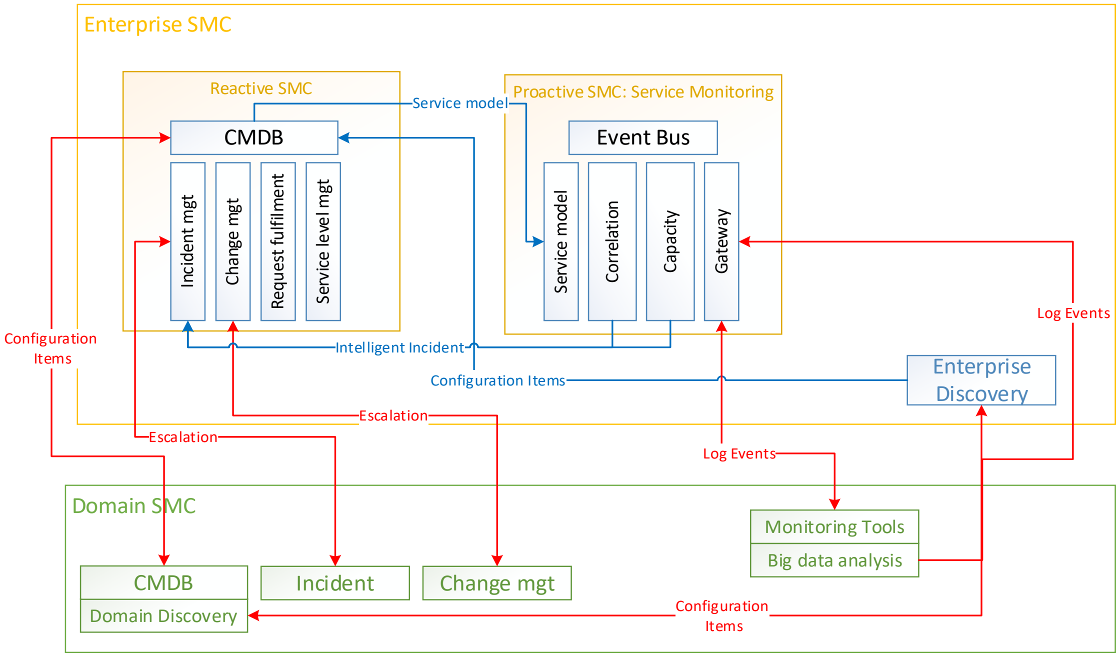


Figure 8 - Interfaces types between domain SMC and Enterprise SMC

0079 The relationship between Enterprise SMC tools and Domain SMC is described below:

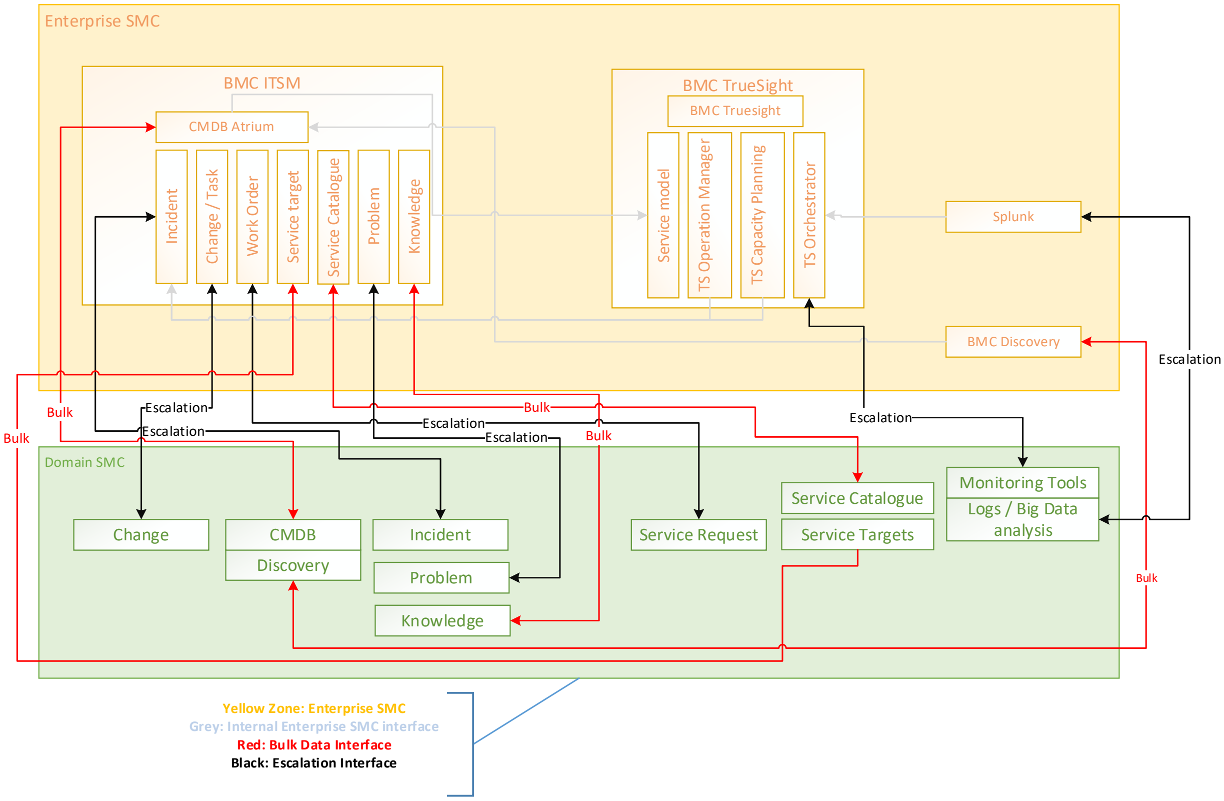


Figure 9 - Enterprise SMC and Domain SMC relationship

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

0080 This section address the design and implementation aspects and will be further detailed during implementation wherever necessary.

4.1. Campus LAN Service Solution

0081 Content will be developed during project impementation.

4.2. Desktop Provisioning Service Solution

0082 Desktop provisioning is broken up into the following subservices: Virtual Desktops, Physical Desktops, Profile Management and End User Monitoring. Each plays as important role in defining the desktop provisioning experience across the NATO ON architecture.

0083 Users will authenticate to desktops and virtual desktops using two-factor authentication NPKI smart cards. The user's Active Directory user account will be linked to the user's smart card NPKI certificates to perform authentication to the ON network. Reference ECS document for enterprise service dependency (NPKI, DNS, DHCP) availability in case of WAN outage.

4.2.1. Virtual Desktop Service Solution

0084 Detailed description of the Virtual Desktop Subservice is in Annex E.

4.2.2. Physical Desktop Service Solution

0085 The MECM Operating System Deployment feature provides MECM administrative users with a tool for creating task sequences they can deploy to physical desktops and laptops regardless of model. The task sequence is comprised of a Windows client operating system image, a boot image, device drivers and the complete list of applications that make up the NATO client device platform. All of the components that make up the task sequence are then distributed to all the distribution points in the MECM infrastructure.

0086 There will be three methods for operating system deployment: PXE-Initiated and Boot Media using USB for online systems and Stand Alone Media for systems that are offline. Physical desktops will be added to BMC's Asset Management via the Enterprise SMC interface once the machines are deployed and online. Desktops will be imaged on a separate/dedicated network ports, or switch or VLAN. This will ensure a fully patched system is deployed on the network. After the machine is moved to Production network, the machine will automatically be moved to the Remediation Zone for updated virus updates.

4.2.2.1. MECM Operating System Deployment

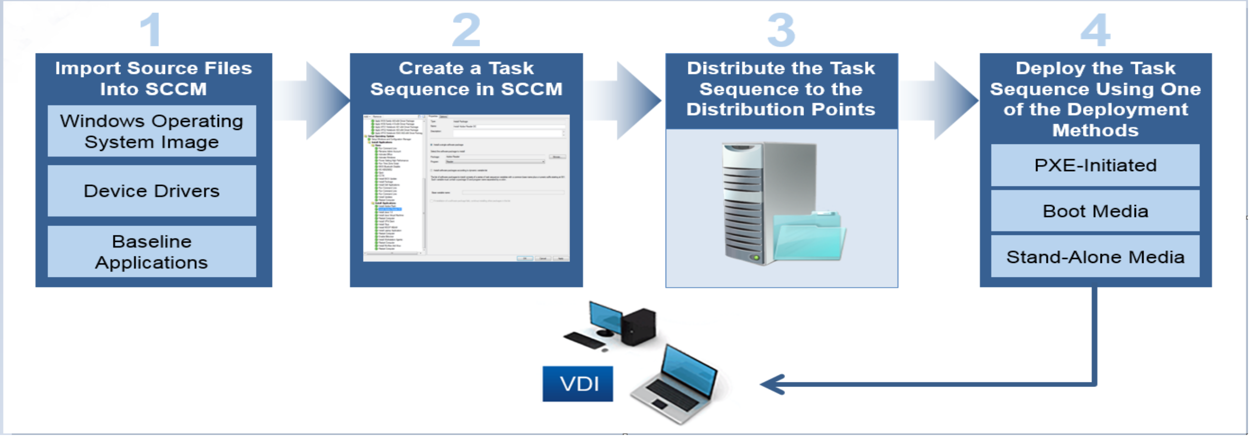

1
Import Source Files Into SCCM
Windows Operating System Image
Device Drivers
Baseline Applications
2
Create a Task Sequence in SCCM
3
Distribute the Task Sequence to the Distribution Points
4
Deploy the Task Sequence Using One of the Deployment Methods
PXE-Initiated
Boot Media
Stand-Alone Media
VDI

Figure 10 - MECM Operating System Deployment

0087 Physical desktops and VDI master images will be provisioned via MECM on the ON network with a hardened client device platform. The physical device will be provisioned at the local site in order reduce the time to image the machine and maintain the ability to image physical devices if the WAN link is down. After the machine is imaged and deployed, all applications will also be delivered via MECM task sequences or via VMware AppVolumes. All follow-on maintenance of the physical desktops and VDI master images will also be conducted via MECM for operating system patching and software deployment/patches at regular intervals or when available.

0088 Users that require high-performance endpoints for graphics processing on ON will be assigned a physical workstation or a GPU-enabled VDI Desktop pool. CPS uses MECM to deploy applications supporting GPU acceleration and offloading. Desktop provisioning usage prevents degradation to the other infrastructure services like storage or network performance due to specific events by using dedicated self-contained storage. The storage has high IOPS to handle specific events. IaaS provides the network QoS, providing preferred service when specifically detected.

0089 The physical desktops and thin clients hardware devices are provided by NATO.

0090 More detail on the MECM deployment in found in the Application Provisioning Subservice Topology section.

4.2.3. Thin Client Service Solution

0091 Dell Wyse Thin Clients on the ON network will be managed by the Wyse Management Suite (WMS) Server that will be hosted in the datacentre IaaS. Through DHCP scope options, the thin clients will be directed to a datacentre WMS Server. Within the WMS, several tasks will be created in order to configure the thin client with all the required software and security to include but not limited to BIOS updates, VMware Horizon Client, AppLocker, background images and certificates.

0092 The Wyse Management Suite within the datacentre will be run as a virtual host. The current implementation of WMS will be able to support up to ten thousand thin clients. The pro version will also allow for additional sorting and organizational capabilities for different types of Nodes. Additionally VMware SRM will be leveraged to ensure that a virtual copy of the host can be brought online at the Data Centre or locally in the event of a host failure. The requirements for the virtual host of the WMS and software repositories is as follows:

Node	Type	Domain	Server Role

Datacenter IaaS Nodes	DC	ON services domain	Thin client management server
VDI EN and SN IaaS Nodes	EN	ON services domain	Thin client distributed repository
ETEEN IaaS Nodes	EN	ON services domain	Thin client management server
IREEN @ NU	REF	IREEN	Thin client management server

Table 10 - Wyse Management Suite deployment

Role	Server Name	Operating System	RAM (GB)	CPU (count)	Storage
Thin client management server	TBD	Windows Server latest approved	16	4	C:\ OS (300GB)
Thin client distributed repository	TBD	Windows Server latest approved	16	4	C:\ OS (300GB)

Table 11 - Wyse Management Suite role requirements

0093 As the non-domain joined thin clients boot up for the first time on the network, the DHCP scope options will dictate the thin client checking in with a WMS Server in order to receive applications and customizations. Since multiple locations of the Dell Wyse Thin Client are deployed, each location of thin clients will have to be managed separately in folders within the WMS server.

0094 The Easy Setup application will be pushed to the thin clients in order to turn the Wyse Thin Clients into kiosks. Once this application is deployed, the only application that can be executed is the VMware Horizon Client. NATO provided security hardening guidance will be applied via WMS. Furthermore, AppLocker policies will be pushed out via WMS to further lock down the device.

4.2.4. Integration with network infrastructure

0095 NATO-provided NAC solution will provide network admission control service in the NATO ON Campus LAN environment. Any end device that is connected to access layer switch will be required to go through a NAC authentication process. By default, all access layer switch ports will be placed in an untrusted VLAN with no access on the network. Once a device is connected to the access switch, the switch will initiate the 802.1x authentication process with the device.

0096 In a campus LAN environment, a typical end-user device would be a NATO ON desktop PC or thin client with appropriate window supplicant or Cisco NAC agent, which is a module within the Cisco AnyConnect client. With the 802.1x supplicant or using NAC agent, the client can perform an Active Directory Single Sign-On (AS SSO) process to authenticate. If authentication is successful, the NAC server will perform a posture assessment of the client based on NATO IA policy. If policy checks are successful, the client is then put into a role-based user VLAN allowing access to the LAN. If there is any failure in the policy checking process, the client is then put into a remediation zone with limited access to enterprise remediation resources such as an anti-virus server and patching server.

0097 Access control list will be applied based on device profile, and it can further limit device access to required network resources only. Authenticated users will also go through a regular re-validation process to ensure that the end device and/or user remains in compliance with NATO IA policies.

0098 The Desktop Provisioning Subservice is tightly integrated with the NATO NAC solution to functional correctly.

4.3. Application Provisioning Service Solution

0099 The Application Provisioning Subservice provides an application provisioning platform, allowing a flexible application delivery of centrally managed applications to the users and deployed from central repositories. The Application Provisioning Subservice description is in terms of capability, scalability and availability terms. The Application Provisioning subservice is decomposed into three further subservices: MECM; AppVolumes and RDSH.

0100 Except the applications part of the core image and platform, which are installed natively, all remaining applications will be provided by the Purchaser in an MSIX format. MECM delivers packaged applications to physical desktops. For virtual desktops, AppVolumes delivers packaged applications. If an application does not function properly in the MSIX format, RDSH can also be used to deliver applications should the other methods prove to be incapable of delivering any given application. Applications request via the App Store are provided by the Enterprise SMC.

4.3.1. MECM Service Solution

4.3.1.1. MECM Overview

0101 Microsoft Endpoint Configuration Manager (MECM) is the central systems management tool for deploying, updating and managing the NATO device environment to include workstations, VDI and servers. MECM allows administrators to deploy applications, operating system images, software updates and compliance configurations that may repeat across various workstation and server types, enterprise wide. This process provides consistency, simplifies desktop management and reduces overall administrative costs.

0102 MECM extends and works alongside existing Microsoft technologies and solutions including:

- Active Directory Domain Services for security, service location, configuration and discovery of users and devices that are to be managed.
- SQL Server as a distributed change management database, integrating with SQL Server Reporting Services to produce reports to monitor and track the management status.

0103 Windows Management Instrumentation (WMI) stores, accesses and manages client computer information.

0104 Application management in MECM provides a set of tools and resources that help the MECM administrator to create, manage, deploy and monitor applications in the enterprise in a centralized manner. MECM automates the deployment and continuous updating of applications to physical desktops and the Master VDI device (baseline locally installed applications only). The MECM infrastructure distributes all of the task sequence components to the DCs, ENs and SNs. There are two types of deliveries in MECM: Packages (legacy) and Applications.

4.3.1.2. Packages

0105 MECM continues to support legacy packages and projects used in MECM 2007/2012. A deployment using packages and projects might be more suitable than a deployment using an application when deploying any of the following:

- Scripts do not install an application on a computer, such as a script to reboot the computer.
- 'One-off' scripts do not need to be continually monitored.
- Scripts run on a recurring schedule and cannot use global evaluation.
- Sets of drivers

4.3.1.3. Applications

0106 An application in MECM contains the files and information required to deploy software to a device. Applications are similar to packages but contain more information to support smart deployment. An application must contain one or more deployment types containing the installation files for a software package. By using deployment types with applications, the user creates one application containing multiple installation files for a software package on different platforms such as an x86- or x64-bit device.

0107 MECM uses rules configured to determine when, where, and what device receives a software package.

4.3.1.3.1. MECM Infrastructure

Node	Type	Identity Domain	Server Role
Primary DC	DC	NATO ON services domain	Primary Site Server SQL Database (2) Software Update Point Distribution Point Server
Secondary DC	DC	NATO ON services domain	Distribution Point Server Primary Site Server (Disaster Recovery) SQL Database (2) (Disaster Recovery) Software Update Point (Disaster Recovery)
All	EN	NATO ON services domain	Distribution Point Server
All	SN	NATO ON services domain	Distribution Point Server
IREEN@NU	DC	NATO ON services domain "simulated"	Simulation of the 2DCs deployments

Table 12 - MECM Infrastructure

Note: *Disaster Recovery explained later in this SDP.

4.3.1.3.2. MECM Server Requirements

Role	Server Name	Operating System	RAM (GB)	CPU (count)	Storage
Primary Site	TBD	Windows Server latest approved	24GB	8	C:\OS (60GB) D:\MECM (200GB) E:\Data (500GB) F:\Content (4TB) P:\Page File (36GB)
SQL Database	TBD	Windows Server latest approved	32GB	16	C:\ OS (60GB) D:\Binaries (20GB) E:\Data (175GB) F:\TempDB (50GB) G:\Logs (100GB) H:\Backups (150GB) P:\Page File (96GB)
SQL (SQL Cluster)	TBD	Windows Server latest approved	32GB	16	C:\ OS (60GB) D:\Binaries (20GB) E:\Data (175GB) F:\TempDB (50GB) G:\Logs (100GB) H:\Backups (200GB) P:\Page File (96GB)
Software Update Point	TBD	Windows Server latest approved	16GB	8	C:\OS (60GB) D:\WSUS (1TB) P:\Page File (24GB)
Distribution Point	TBD	Windows Server latest approved	8GB	4	C:\OS (60GB) D:\Data (3TB) P:\Page File (12GB)
Primary Site (DR)	TBD	Windows Server latest approved	24GB	8	C:\OS (60GB) D:\MECM (200GB) E:\Data (500GB) F:\Content (4TB) P:\Page File (36GB)
SQL Database (DR)	TBD	Windows Server latest approved	64GB	16	C:\ OS (60GB) D:\Binaries (20GB) E:\Data (175GB) F:\TempDB (50GB) G:\Logs (100GB) H:\Backups (150GB) P:\Page File (96GB)
SQL (SQL Cluster) (DR)	TBD	Windows Server latest approved	64GB	16	C:\ OS (60GB) D:\Binaries (20GB)

Role	Server Name	Operating System	RAM (GB)	CPU (count)	Storage
					E:\Data (175GB) F:\TempDB (50GB) G:\Logs (100GB) H:\Backups (200GB) P:\Page File (96GB)
Software Update Point (DR)	TBD	Windows Server latest approved	16GB	8	C:\OS (60GB) D:\WSUS (1TB) P:\Page File (24GB)

Table 13 - MECM Server Requirements

4.3.1.4. PKI Integration

0108 MECM shall integrate with and consume the internal NATO PKI service currently in use by NATO for all certificate needs for site systems, clients, etc. in place of using self-signed certificates. The guidance provided by Microsoft shall be used when implementing the certificate usage within MECM.

4.3.1.5. MECM details

0109 For the service interface, MECM is the central systems management tool for deploying, updating and managing the NATO device environment to include workstations and servers. MECM allows administrators to deploy applications, operating system images, software updates and compliance configurations that may repeat across various workstation and server types, enterprise wide. This process provides consistency, simplifies desktop management and reduces overall administrative costs. Application management in MECM provides a set of tools and resources enabling the MECM administrator to create, manage, deploy and monitor applications in the enterprise in a centralized manner. MECM automates the deployment and continuous updating of applications to physical desktops, laptops and the Master VDI device (baseline locally installed applications only). The applications distribute to all the distribution points in the MECM infrastructure located in the DCs, ENs and SNs. Figure 11 displays the service interface interaction diagram and description.

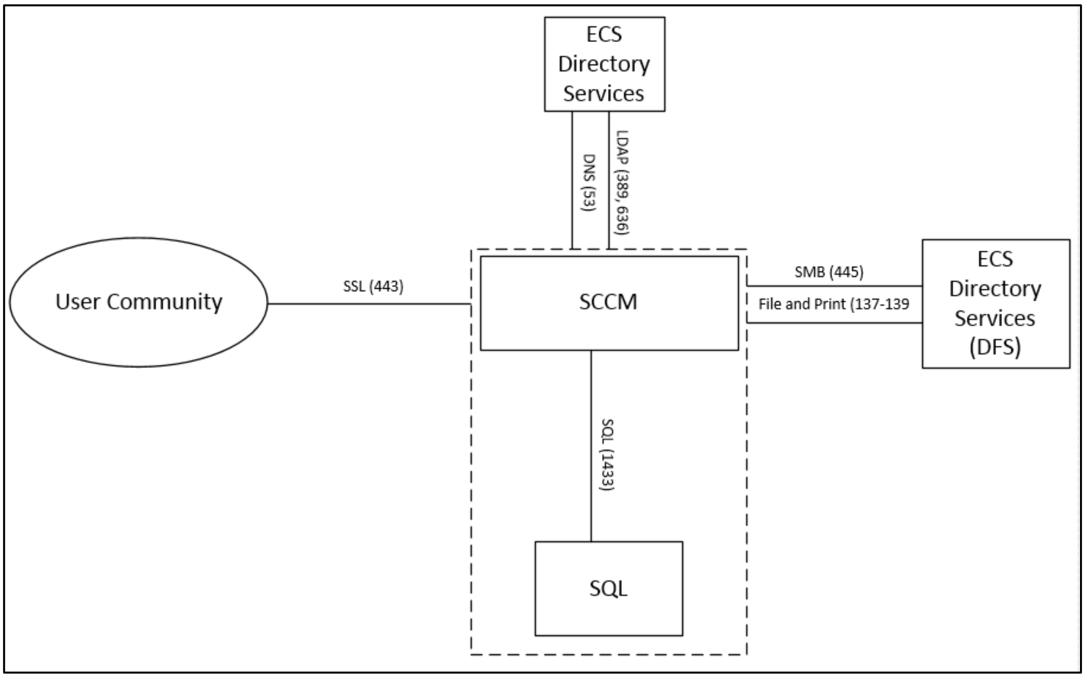


Figure 11- MECM Service Interface Interaction Diagram

Source	Destination	Port/Protocol	Description
MECM	ECS Directory Services	389, 636	Query Security Group
MECM	ECS Directory Services	53	Name Resolution
MECM	ECS Directory Services (DFS)	445, 137-139	Application Package Accessibility
MECM	SQL	1433	Database Communication

Table 14 - External Interface

0110 MECM will deliver the base operating system for both physical and (initial) virtual desktop image as well as delivery applications to physical desktops and laptops.

4.3.1.5.1. MECM Site Design Decision for ON

0111 A MECM stand-alone primary site can support up to 175,000 clients and allows for centralised management and reporting of all managed clients within that site.

0112 When MECM is installed for the first time, a MECM site is created that is the foundation from which to manage devices and users in the environment. This will be a stand-alone primary site. A stand-alone primary site is suitable for the NATO deployment and in order to accommodate future growth of the environment, it can be added to a Central Administration Site (CAS) at a later point in time (if needed).

0113 Due to the number of managed devices falling within the supportability limits of a single MECM hierarchy, and because no additional requirements exist that would require a separate hierarchy for organisational, political, security or administration purposes, a single MECM site will be used.

0114 The primary site requires a MECM license and supported 64-bit SQL Server Enterprise Edition.

4.3.1.5.2. Primary Site Name and Site Code Design Decision for ON

0115 The MECM primary site needs to be assigned a name and a unique three-character site code. It is good practice to devise a site code naming convention that allows for uniqueness, also taking into account any future expansion. The following naming convention will be used for the primary site server:

Site Code	Role Description
TBD	Primary Site server

Table 15 - Primary Site Name and Site Code Design Decision for ON

4.3.1.5.3. MECM Site System Roles

0116 MECM supports multiple site system roles and the decision to split a MECM site onto multiple virtual servers was driven mostly by the capacity, scalability and availability requirements below:

4.3.1.5.4. Primary Site Server

MECM Role Installed	Role Description
Site Server	A site server is the computer on which MECM Setup can be run, and it provides some core functionality for the site.
Management Point	A management point provides policy and content location information to clients. It also receives configuration data from clients. In MECM, the management point also tales on the server locator point functionality and completes site assignments.
Distribution Point	A distribution point contains source files for clients to download. Content distribution can be controlled by using bandwidth throttling and scheduling options.
Application Catalogue Web Service Point	An Application Catalogue web service point provides software information to the Application Catalogue website from the Software Library.
Application Catalogue Website Point	An Application Catalogue website point provides users with a list of available software.
Fallback Status Point	A fallback status point helps monitor client installation and identify the clients that are unmanaged because they cannot communicate with their management point.
Service Connection Point	Connects to Microsoft cloud services. Is used to update and service the MECM installation.

Table 16 - Primary Site Server

4.3.1.5.5. Software Update Point Server

MECM Role Installed	Role Description
Software Update Point	A software update point integrates with Windows Server Update Services (WSUS) to provide software updates to MECM clients. Updates will be provided on external media by NATO and manually imported.

Table 17 - Software Update Point Server

4.3.1.5.6. SQL Server

MECM Role Installed	Role Description
Site Database Server (Clustered)	A site database server hosts the SQL Server database to store information about assets and configuration data. The role will be installed on a dedicated SQL Server for increased performance and availability. In addition, a dedicated gigabit network connection is required between the SQL cluster and the site server for performance purposes. In order to support a SQL Clustering scenario for high availability, the site database must reside on a remote server.
Reporting Services Point	A reporting services point integrates with SQL Server Reporting Services to create and manage reports for MECM.

Table 18 - SQL Server

4.3.1.5.7. Distribution Point Server

MECM Role Installed	Role Description
Distribution Point	A distribution point contains source files for clients to download. Content distribution can be controlled by using bandwidth throttling and scheduling options. NATO would like locations which are classified as datacentres (DCs), Enhanced Nodes (ENs) and Standard Nodes (SNs) to have Distribution Points. Therefore, each location should be able to facilitate software distribution, operating system deployment and software updates deployment. Software updates will be distributed over the WAN. Server patch management uses the same distribution points.

Table 19 - Distribution Point Server

4.3.1.5.8. MECM Service Account and Security Group Requirements

0117 As part of the MECM Design process, a number of Active Directory groups and user accounts have been identified. The accounts and groups will need to be established in the NATO Active Directory environment for correct and secure operation of the MECM environment. All service accounts will be group Managed Service Accounts.

0118 Access to MECM functionality is controlled via permissions and roles. Individuals that require the ability to perform certain actions within MECM (including running reports) will need to be granted the respective permissions. As a best practice, Microsoft recommends that groups, as opposed to users, are used to define MECM permissions. Also, the ‘principle of least privilege’ should be followed.

0119 MECM uses role-based administration to provide management of security and securable objects. Role-based administration introduces security roles and security scopes that logically group actions and access to objects and assign these to administrative users. Functional considerations for the use of role based administration include:

- Security roles are a grouping of typical administrative tasks that are assigned to multiple administrative users or groups.

- Security scopes are tags applied to site objects, such as deployments or collections, which limit the objects that groups of administrators can see in the Configuration Manager console.
- Combinations of security roles and security scopes can define what site objects an administrative user can view and manage.
- The MECM console shows only the objects in the security scope and security roles that are defined for the administrative user. The console will also only display the collections that the administrator has been allowed to view or manage.
- Predefined security roles are provided, and it is possible to create new security roles and security scopes.
- Security scopes and security roles are replicated as global data and can be configured and used at any single site in the hierarchy.

4.3.1.5.9. Service Accounts

0120 The following service accounts are required to complete the installation and configuration of MECM.

0121 Where possible, the service accounts will be Group Managed Service account type.

Service Accounts	Purpose	Security Impact
TBD	SQL Server Agent Service	Logon on as service, other User Rights Assignments controlled via GPO
TBD	SQL Server Database Engine Service	Logon on as service, other User Rights Assignments controlled via GPO
TBD	MECM Installation Account	Local administrative rights on all ConfigMgr Site Servers and SQL servers. Also gets 'sysadmin' role on SQL servers
TBD	MECM Client Push Install Account	Local administrative rights on all workstations controlled by GPO
TBD	MECM Network Access Account	Content access for Operating System Deployment (machine builds)
TBD	MECM Domain Join Account used during OSD	Rights to join computers to specific OUs
TBD	SQL Reporting Services Account	Domain account for use with Reporting Services

Table 20 - Service Accounts

4.3.1.5.10. Security Groups

0122 The following security groups are required to complete the configuration of MECM.

Administrative Groups	Purpose	Type
ENT MECM Admins	Grants all permissions in Configuration Manager. The administrative user who first creates a new Configuration Manager installation is associated with this security role, all scopes and all collections.	Global

Administrative Groups	Purpose	Type
	Ensure that the group has **Full Control** on the **SYSTEM** Container in Active Directory.	
ENT Application Deployment Manager	Grants permissions to deploy applications. Administrative users who are associated with this role can view a list of applications, and they can manage deployments for applications, alerts, templates and packages, and projects. Administrative users who are associated with this role can also view collections and their members, status messages, queries, conditional delivery rules and App-V virtual environments.	Global
ENT Infrastructure Administrator	Grants permissions to create, delete and modify the Configuration Manager server infrastructure and to perform migration tasks.	Global
ENT Operating System Deployment Manager	Grants permissions to create operating system images and deploy them to computers. Administrative users who are associated with this role can manage operating system upgrade packages and images, task sequences, drivers, boot images and state migration settings.	Global
ENT Software Update Manager	Grants permissions to define and deploy software updates. Administrative users who are associated with this role can manage software update groups, deployments and deployment templates.	Global
ENT MECM Servers	Contains all MECM servers in the hierarchy for various purposes in security configurations.	Global
ENT MECM Reports	Grants permissions to the MECM Reporting Services	Global
ENT MECM Read	Grants Read-Only permissions to MECM and permissions to run the remote administration tools that help users resolve computer issues **[1218].**	Global

Table 21 - Security Groups

4.3.1.5.11. MECM Initial configuration

0123 MECM supports the following configuration to enable the O&M activities of each IaaS, ECS and CPS subservice and its specific requirements, this to include but not limited to:

- Dedicated collections and sub-collections (groups) of servers for each subservice. For example all servers with Microsoft SQL Server, all domain controllers, etc. This includes dedicated security roles and permissions sets for each subservice so that only administrators responsible for that specific subservice have permissions.
- Maintenance windows are defined on each collection.
- Patches are either made available and manually installed by the responsible personnel or automatically patched with the explicit agreement of the Purchaser.

4.3.1.5.12. MECM Client Install Design

0124 MECM allows the installation of the MECM Client software via a number of methods including client push installation, software update point installation and installation during operating system deployment, installation via Group Policy and installation via a logon initiated script. The installation method that will be used for the NATO deployment is client push installation and logon initiated script.

0125 The MECM client can be installed remotely via a client push from the MECM site server to a client computer. The client push can be configured to be triggered automatically after a computer is discovered, or it can be initiated manually by an administrator using the MECM Administrator console. Client push has the following requirements:

- o The MECM site server's computer account or a designated client push account is in the Administrators local group of the target computer has been configured. This is accomplished using Group Policy.
- o No firewall on the target computer blocks incoming Server Message Blocks (SMB) connections to local file shares.

4.3.1.5.13. MECM Client Push Installation

0126 The Client Push Installation Account needs to be configured for the site before this method of client deployment can occur.

4.3.1.5.14. Configure MECM Site Components

0127 Users can configure site components to control the behaviour of site system roles at a site. Configurations for site system roles apply to each instance of a site system role at a particular site. These configurations must be made at each site individually, and they do not apply to multiple sites.

4.3.1.5.15. Software Distribution Site Component

0128 The network access account needs to be configured in the console before successfully deploying operating systems and software.

4.3.1.5.16. Management Point Site Component

0129 Configuration Manager Clients use management points to locate services and to find site information such as boundary group membership and PKI certificate selection options. Clients also use management points to find other management points in the site as well as distribution points from which to download software. Management points also help clients to complete site assignment and to download client policy and upload client information.

4.3.1.5.17. Collection Membership Evaluation Site Component

0130 Use this task to set how often collection membership is incrementally evaluated. Incremental evaluation updates a collection membership with only new or changed resources.

4.3.1.5.18. MECM Resource Discovery Methods

0131 This section details the resource discovery design decisions for the NATO environment. Resource discovery's purpose is to locate and gather information about resources on the network. Resources include computers, servers, routers, switches, hubs and any other object that has an IP address, such as gateways, communication servers or printers. MECM can discover computer resources such as UNIX workstations, even if those computers will not become MECM clients. Resources also include Active Directory user accounts and user groups.

0132 MECM provides a number of different types of discovery and installation methods that can be employed in the NATO environment. Different combinations of discovery and installation methods can be chosen to locate resources and install MECM client software.

0133 MECM provides the following types of discovery methods:

- Heartbeat Discovery
- Network Discovery
- Active Directory Forest Discovery
- Active Directory System Discovery
- Active Directory User Discovery
- Active Directory Group Discovery

0134 When a resource is discovered, the discovery component generates a Discovery Data Record (DDR) and forwards it to the MECM site database at the primary site.

0135 A DDR is a set of information about the discovered resource. DDR properties depend on the type of resource that is discovered. For example, a DDR for a computer will have a different set of properties than a DDR for a user account. A DDR for a computer might have the following properties:

- MECM Unique Identifier (SMSUID)
- NetBIOS name
- IP addresses
- IP subnets
- Operating system name and version
- Resource domain or workgroup
- Last logon user name
- Agent name (the discovery method that generated the DDR)

0136 MECM uses key properties within the DDRs to match incoming discovery information to existing resources in the discovery database. This approach enables MECM to uniquely identify each resource.

0137 Although all MECM discovery methods serve to generate discovery data, the different methods discover different types of resources and serve different purposes. The table below summarises the MECM resource discovery methods.

Method	Discovered Resource	Initiated By	Paired Client Installation Method
Heartbeat Discovery	Computers	Agent residing on installed MECM clients	N/A. Only available for systems that are already MECM clients
Network Discovery	System resources	MECM servers poll network devices and watch network traffic	None
Active Directory System Discovery	Computers	MECM site server polls domain controllers	Client Push Installation
Active Directory User Discovery	Users	MECM site server polls domain controllers	None

Method	Discovered Resource	Initiated By	Paired Client Installation Method
Active Directory Group Discovery	Groups / OUs	MECM site server polls domain controllers	None

Table 22 - MECM Resource Discovery Methods

4.3.1.5.19. Active Directory System Discovery

0138 Active Directory System Discovery will be the primary means of discovering new computers for management by MECM.

0139 Active Directory System Discovery will only create an instance of a discovered system if a system account exists in Active Directory and also if there is a corresponding DNS host record. Where there are instances of stale records existing both in Active Directory and DNS, MECM must be configured to remove all stale records (computers that have not logged into Active Directory for a pre-defined number of days, or have not changed their computer account password for a pre-defined number of days) through an automated task.

4.3.1.5.20. Active Directory Group Discovery

0140 Active Directory Group Discovery will be enabled at the primary site where Active Directory System Discovery is enabled. Since Active Directory Group Discovery works only for already discovered computers, it will be scheduled to run after Active Directory System Discovery.

4.3.1.5.21. Active Directory User Discovery

0141 Active Directory User Discovery will discover Active Directory users, which can then be used by MECM to build collections. This enables targeting of users for functions such as software distribution. It is possible to use security groups identified by **Active Directory System Group Discovery** for application deployment and to utilise the user discovery information identified by **Active Directory User Discovery** for reporting purposes.

4.3.1.5.22. Heartbeat Discovery

0142 Heartbeat Discovery will be used to maintain up-to-date discovery data on clients that would not normally be affected by one of the other discovery methods as well as to supplement and update information stored in the site database where the discovery data has been logged by other discovery methods.

4.3.1.5.23. Active Directory Forest Discovery

0143 Discovers Active Directory sites and subnets, and creates Configuration Manager Boundaries for each site and subnet from the forests which have been configured for discovery. Using this discovery method, the Active Directory or IP subnet boundaries can automatically be created that are within the discovered Active Directory Forests. This is very useful with multiple AD Site and Subnet, instead of creating them manually.

4.3.1.5.24. MECM Boundaries

0144 The boundaries need to be configured before communication will occur between the MECM server infrastructure and the device clients.

0145 A boundary is a network location on the intranet that can contain one or more devices that are to be manage. Boundaries can be an IP subnet, Active Directory site name, IPv6 Prefix, or an IP address range, and the hierarchy can include any combination of these boundary types. To use a boundary, the boundary to one or more boundary groups must be added. Boundary groups are collections of boundaries. By using boundary groups, clients on the intranet can find an assigned site and locate content when they have to install software such as applications, software updates and operating system images. A boundary does not enable clients to be managed at the network location. To manage a client, the boundary must be a member of a boundary group. Simple boundaries do nothing, they must be added to one or more boundary groups in order to work.

0146 There are multiple ways that a MECM boundary can be defined, including use of Active Directory sites, an IP Subnet, IPv6 prefix or IP Address Range. The recommended approach for defining MECM site boundaries is Active Directory Sites.

4.3.1.5.25. Boundary Group Design

0147 For Content Location, we want clients to get their content locally at their respective location. We will create Distro Boundary groups, add only their Active Directory Sites Boundary and assign their local Distribution Point.

4.3.1.5.26. MECM Client Settings

0148 This section will explain how to create custom MECM client settings and how to deploy them.

0149 Client settings are used to configure deployed agents. This is for configuration like:

- Enabling hardware inventory agent
- Schedule software distribution evaluations
- Set scan schedules
- BITS throttling
- Etc.

0150 Client settings are specified at the collection level. Different settings for specific collections, overlapping settings are set using a priority setting. For example, different settings for different sites or for a workstation client setting and a server client setting.

0151 The **Default Client Settings** are applied to all clients in the hierarchy automatically. **Default Client Settings** do not need to be deployed to apply them. By default it has a 10,000 priority value (This is the lower priority). All others custom client settings can have a priority of 1 to 9,999, which will always override the **Default Client Settings** (the higher priority is 1). To change any of the settings in the **Default Client Settings**, create a **Custom Client Device Setting** or **Custom Client User Setting** and deploy it to the required collections to apply it.

4.3.1.5.27. MECM Patch Management

0152 Software updates in MECM provides a set of tools and resources that can help manage the complex task of tracking and applying software updates to client computers in the enterprise. An effective software update management process is necessary to maintain operational efficiency, overcome security issues and maintain the stability of the network infrastructure. However, because of the changing nature of technology and the continual appearance of new security threats, effective software update management requires consistent and continual attention.

0153 For the NATO sites in scope on ON, latest up-to-date software updates for the Microsoft Operating System and applications for both workstations and servers will be provided by NATO and manually imported into the WSUS server. The software updates will be then distributed the latest software updates that apply to the NATO environment to all of the distribution points. Each site's computers will receive the software updates on regularly scheduled intervals.

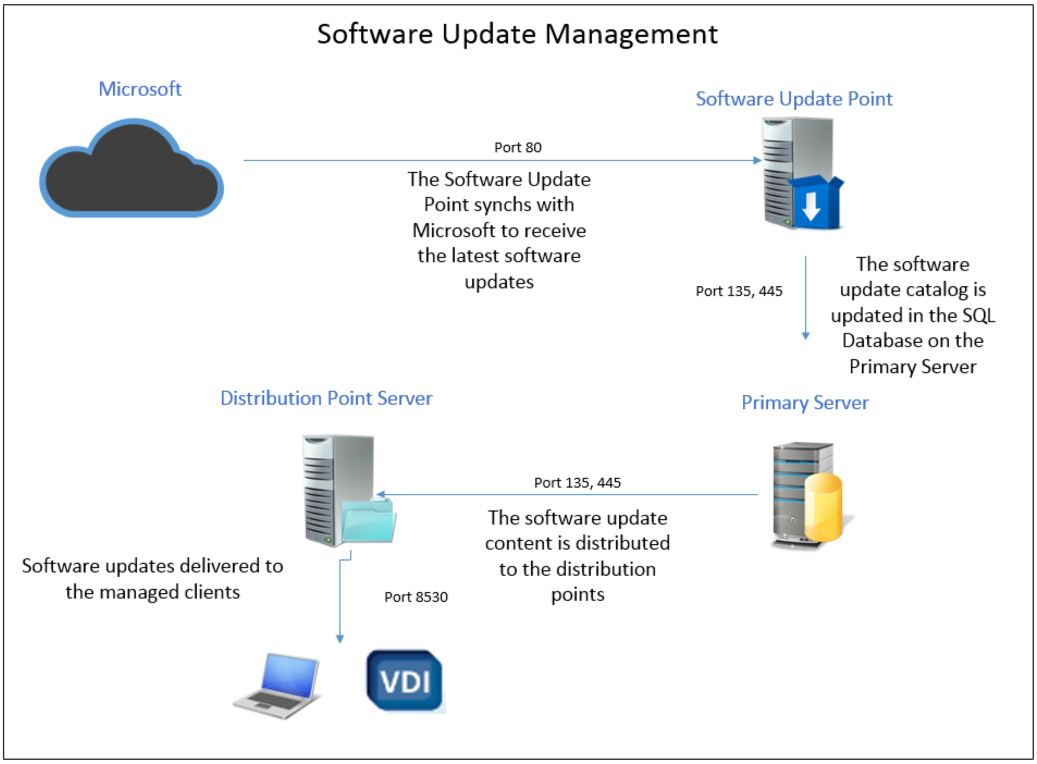

Software Update Management
Microsoft
Software Update Point
Port 80
The Software Update Point synchs with Microsoft to receive the latest software updates
Port 135, 445
The software update catalog is updated in the SQL Database on the Primary Server
Distribution Point Server
Primary Server
Port 135, 445
The software update content is distributed to the distribution points
Software updates delivered to the managed clients
Port 8530
VDI

Figure 12 - Software Update Management

4.3.1.5.28. MECM Console

0154 The MECM console is the centralised primary tool used for administration and troubleshooting of managed clients. MECM administrators use the MECM console to accomplish the day-to-day tasks such as operating system deployment, software distribution and patch management as well as configuring the site, maintaining the MECM site database and monitoring the health of the MECM hierarchy.

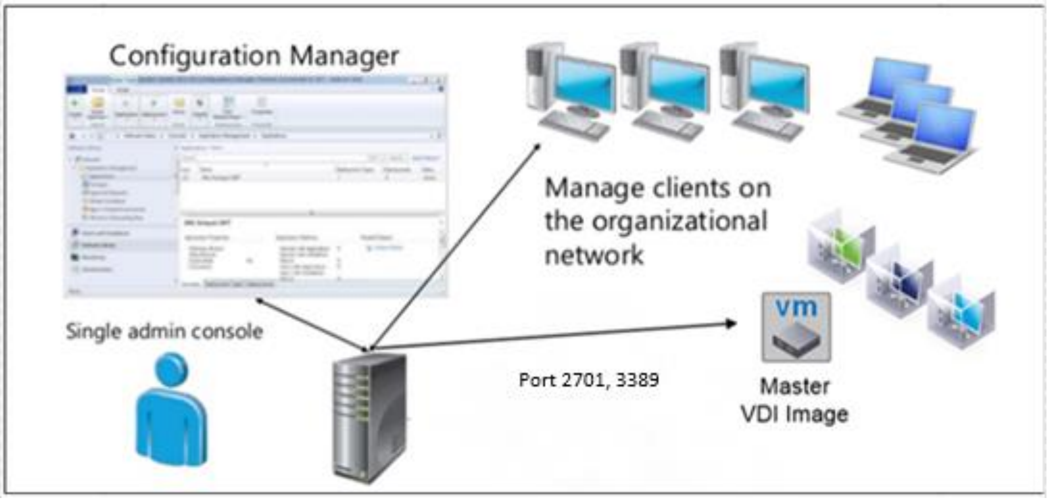


Figure 13 - MECM Console

4.3.1.5.29. MECM Remote Tools Management

0155 The remote tools feature in MECM allows permitted viewers to access any client computer in the MECM site that has the remote tools client agent components installed. Remote tools are deployed as part of the MECM agent.

4.3.1.5.30. MECM Remote Assistance

0156 Remote Assistance allows an administrator to access a client device while a user is logged in. This feature requires the end-user to accept the request of the administrator and a machine cannot be remote controlled when no one is logged on. This feature allows for technical support to assist in troubleshooting issues with the end-user without having to do a deskside visit**.**

4.3.1.5.31. MECM Remote Control

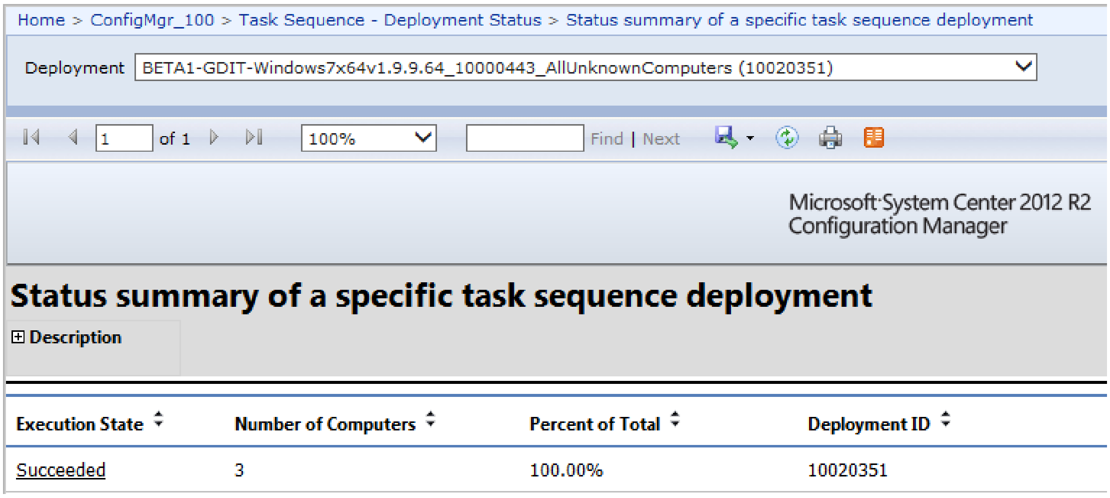
0157 Remote Control is a feature of MECM which allows an administrator to troubleshoot hardware and software configuration problems on remote client computers and to provide remote help desk support when access to the user’s computer is necessary. Remote Control can be used whether the user is logged into their machine or not.

4.3.1.5.32. MECM Reporting

0158 SQL Server Reporting Services is a server-based reporting platform that provides comprehensive reporting functionality for a variety of data sources. The reporting services point in Configuration Manager communicates with SQL Server Reporting Services to copy Configuration Manager Reports to a specified report folder, to configure Reporting Services settings and to configure Reporting Services security settings. Reporting Services connects to the Configuration Manager Site database to retrieve data that is returned when a reports are run.

0159 Reporting helps gather, organise and present information about users, hardware and software inventory, software updates, applications, operating system deployment, site status and other Configuration Manager operations in the organisation. Reporting provides a number of predefined reports that can be used without changes, or that can be modified to meet requirements, and custom reports can be created.

0160 Reporting gives a status of a particular task sequence whether it’s Running, Succeeded or Failed**.**



Home > ConfigMgr_100 > Task Sequence - Deployment Status > Status summary of a specific task sequence deployment

Deployment: BETA1-GDIT-Windows7x64v1.9.9.64_10000443_AllUnknownComputers (10020351)

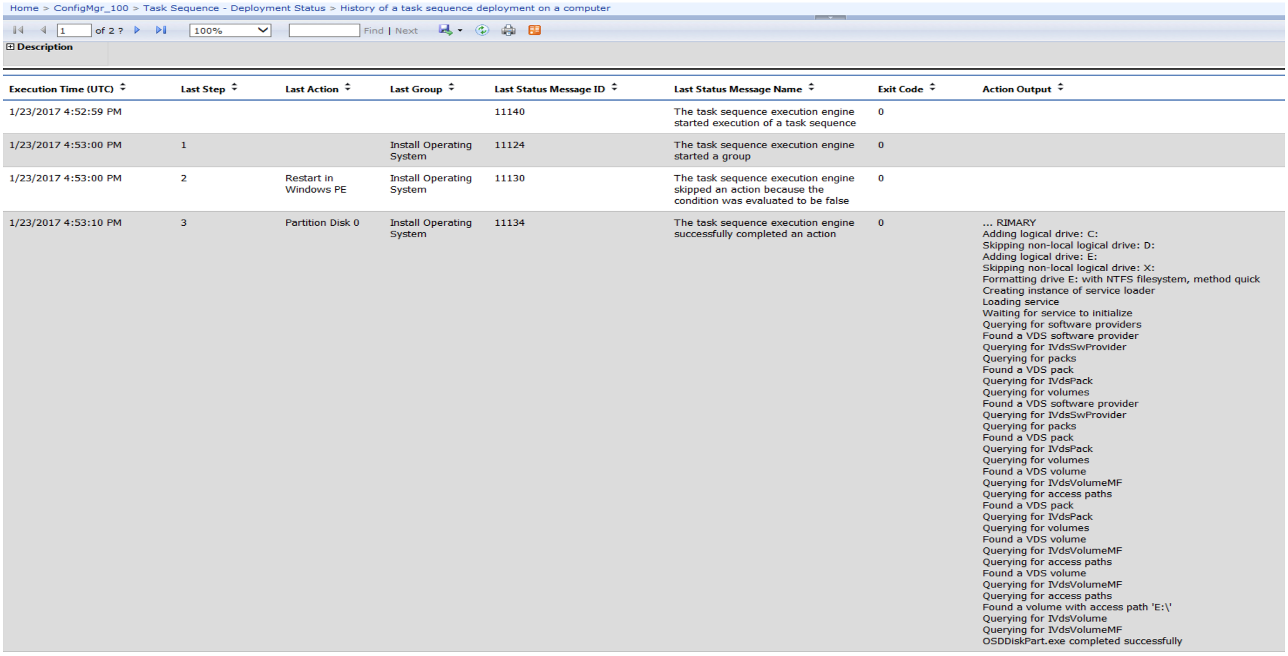
Status summary of a specific task sequence deployment

⊞ Description

Execution State	Number of Computers	Percent of Total	Deployment ID
Succeeded	3	100.00%	10020351

Figure 14 - MECM Reporting

0161 It can also give a detailed account of each step in the task sequence for each computer that has run the task sequence:



Home > ConfigMgr_100 > Task Sequence - Deployment Status > History of a task sequence deployment on a computer

⊞ Description

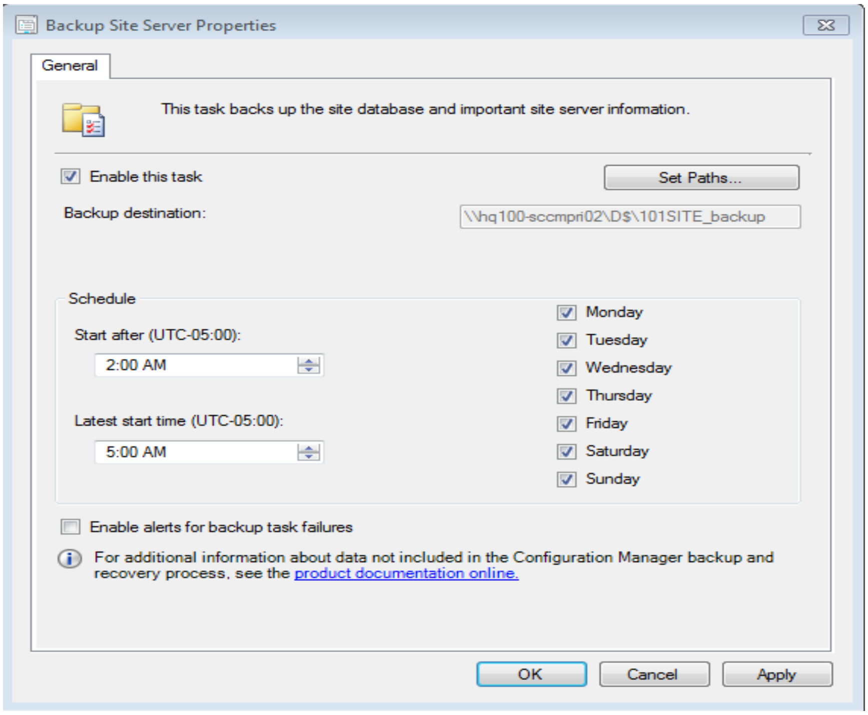
Execution Time (UTC)	Last Step	Last Action	Last Group	Last Status Message ID	Last Status Message Name	Exit Code	Action Output
1/23/2017 4:52:59 PM				11140	The task sequence execution engine started execution of a task sequence	0	
1/23/2017 4:53:00 PM	1		Install Operating System	11124	The task sequence execution engine started a group	0	
1/23/2017 4:53:00 PM	2	Restart in Windows PE	Install Operating System	11130	The task sequence execution engine skipped an action because the condition was evaluated to be false	0	
1/23/2017 4:53:10 PM	3	Partition Disk 0	Install Operating System	11134	The task sequence execution engine successfully completed an action	0	... RIMARY Adding logical drive: C: Skipping non-local logical drive: D: Adding logical drive: E: Skipping non-local logical drive: X: Formatting drive E: with NTFS filesystem, method quick Creating instance of service loader Loading service Waiting for service to initialize Querying for software providers Found a VDS software provider Querying for IVdsSwProvider Querying for packs Found a VDS pack Querying for IVdsPack Querying for volumes Found a VDS software provider Querying for IVdsSwProvider Querying for packs Found a VDS pack Querying for IVdsPack Querying for volumes Found a VDS volume Querying for IVdsVolumeMF Querying for access paths Found a VDS pack Querying for IVdsPack Querying for volumes Found a VDS volume Querying for IVdsVolumeMF Querying for access paths Found a VDS volume Querying for IVdsVolumeMF Querying for access paths Found a volume with access path 'E:\' Querying for IVdsVolume Querying for IVdsVolumeMF OSDDiskPart.exe completed successfully

Figure 15 - MECM Account Details

4.3.1.5.33. Backup, High Availability and Disaster Recovery

4.3.1.5.34. Backup Requirements

0162 In order to perform daily backups of the Primary Site Server, there is a maintenance task within the MECM console which backs up the primary site database and important site server information on a daily basis**.** The schedule will start at 2:00am, and the setting for latest start time will be 5:00am. A backup destination will need to be identified and added to the backup destination window in the screenshot below. In addition, the SQL database administrators perform a daily backup of the site database on the SQL server as well.



This task backs up the site database and important site server information.

☑ Enable this task

Backup destination: \\hq100-sccmpri02\D$\101SITE_backup

Schedule

Start after (UTC-05:00): 2:00 AM

Latest start time (UTC-05:00): 5:00 AM

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

□ Enable alerts for backup task failures

For additional information about data not included in the Configuration Manager backup and recovery process, see the product documentation online.

Figure 16 - Backup Site Server Properties

4.3.1.5.35. High-Availability Requirements

0163 In order to provide high availability for MECM, there are a couple of measures that will be implemented:

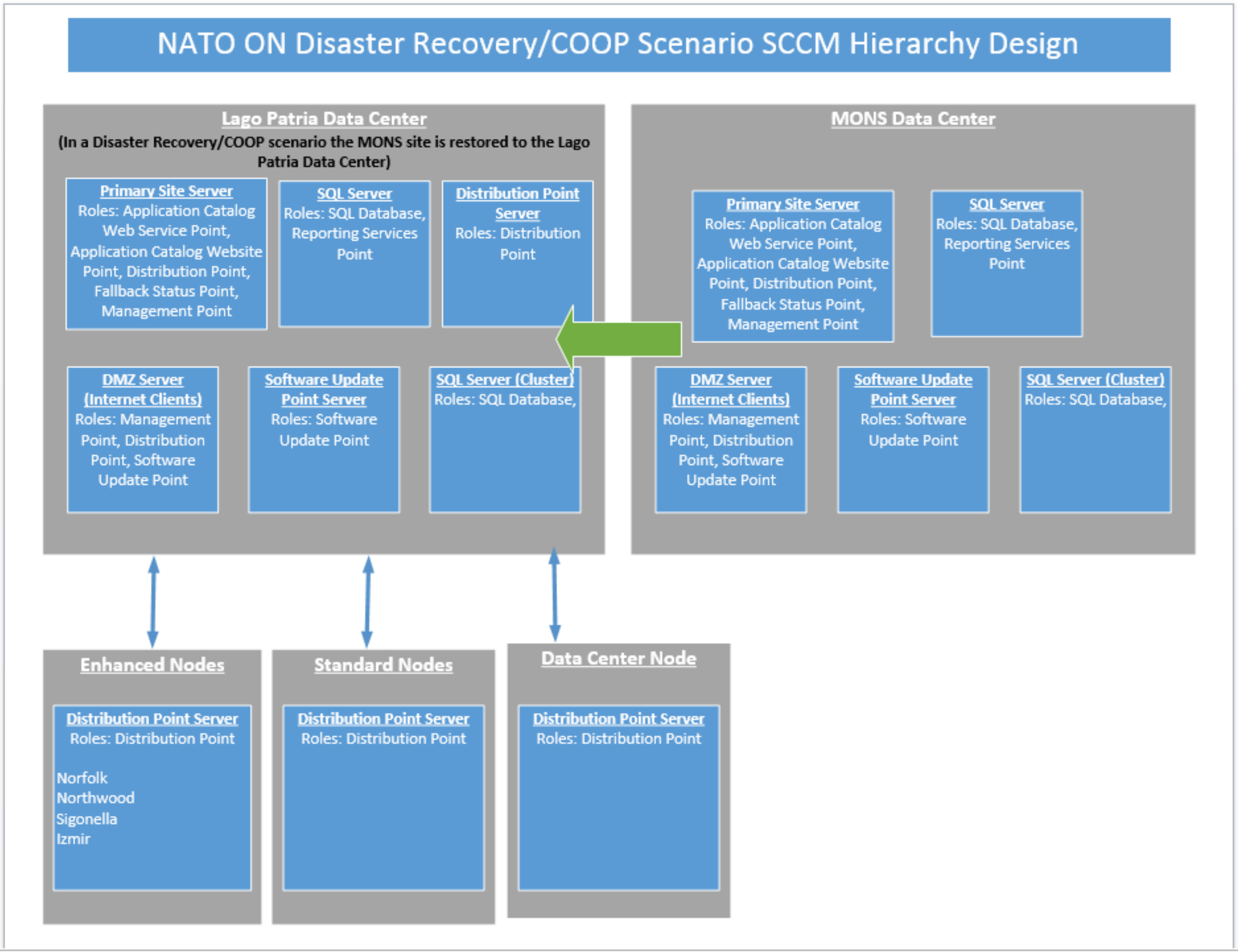
- **SQL Cluster** – When installing SQL for the first time, SQL Server Cluster configuration for the database at the Primary Site is implemented. The fail-over support built into SQL Server is used. If the SQL server encounters a problem it will fail over to the other clustered SQL server to support the Primary Site Server**.**
- **Distribution Points** – There will be multiple distribution points installed throughout the enterprise and each will have all of the content distributed to them. Each site that is assigned a distribution point will also have a secondary distribution point assigned. In the event of a failure to a primary distribution point, the secondary distribution point will be utilised in order to pull content until the failed distribution point is restored. Finally, consider configuring one or more distribution points as fall-back locations for content.

4.3.1.5.36. Disaster Recovery Requirements

0164 Disaster recovery relates to measures taken to ensure that operations can be resumed in the event of a catastrophic failure such as the loss of the entire datacentre that hosts the primary infrastructure.

0165 To support a Disaster Recovery scenario, there will be a server for each of the MECM site systems datacentre in the ITA-LAG-01 datacentre on standby in the event we need to perform a backup and restore. The MECM Setup wizard supports site restoration actions to help restore a site to operations using the daily SQL backup.

4.3.1.5.37. Disaster Recovery Design (ON)



NATO ON Disaster Recovery/COOP Scenario SCCM Hierarchy Design

Lago Patria Data Center

(In a Disaster Recovery/COOP scenario the MONS site is restored to the Lago Patria Data Center)

Primary Site Server
Roles: Application Catalog Web Service Point, Application Catalog Website Point, Distribution Point, Fallback Status Point, Management Point

SQL Server
Roles: SQL Database, Reporting Services Point

Distribution Point Server
Roles: Distribution Point

DMZ Server (Internet Clients)
Roles: Management Point, Distribution Point, Software Update Point

Software Update Point Server
Roles: Software Update Point

SQL Server (Cluster)
Roles: SQL Database,

MONS Data Center

Primary Site Server
Roles: Application Catalog Web Service Point, Application Catalog Website Point, Distribution Point, Fallback Status Point, Management Point

SQL Server
Roles: SQL Database, Reporting Services Point

DMZ Server (Internet Clients)
Roles: Management Point, Distribution Point, Software Update Point

Software Update Point Server
Roles: Software Update Point

SQL Server (Cluster)
Roles: SQL Database,

Enhanced Nodes

Distribution Point Server
Roles: Distribution Point

Norfolk
Northwood
Sigonella
Izmir

Standard Nodes

Distribution Point Server
Roles: Distribution Point

Data Center Node

Distribution Point Server
Roles: Distribution Point

Figure 17 - ON Disaster Recovery Design

4.3.1.5.38. MECM Content Management

0166 This section details the content management design decisions for the NATO environment. Content management in MECM provides the ability to manage content files for applications, packages, software updates and operating system deployment. MECM uses distribution points to store files needed for software to run on client computers. These distribution points function as distribution centres for the content files, allowing users to download and run the software. Clients must have access to at least one distribution point from which they can download the files.

0167 When software is deployed to a client, the client sends a content request to a management point, the management point sends a list of the distribution points in the boundary group assigned to the client and the client uses one of the distribution points on the list as the source location for content. When a distribution point does not have the content and the peer cache settings are not enabled, the client fails to download the content and the software deployment fails.

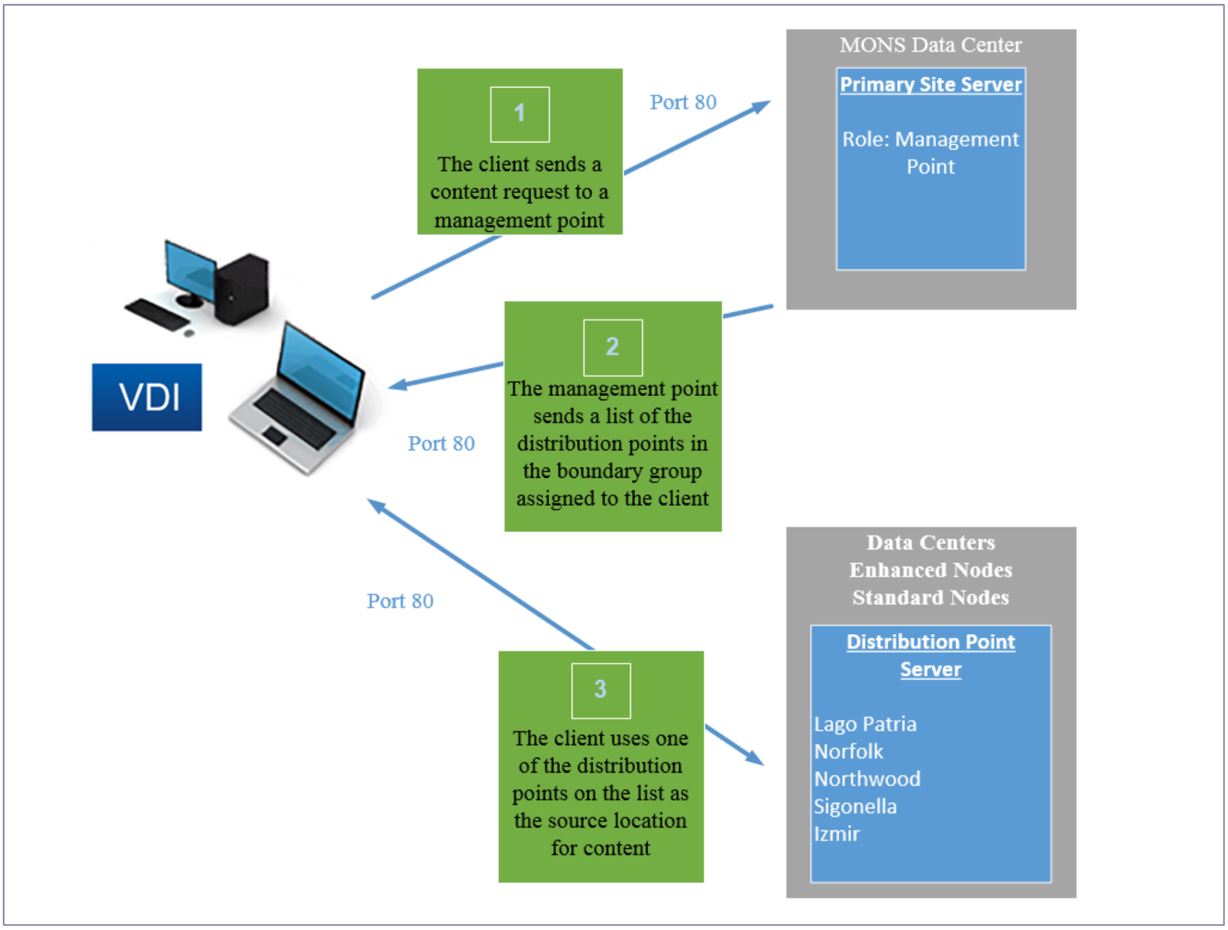

MONS Data Center
Primary Site Server
Role: Management Point
1
The client sends a content request to a management point
Port 80
VDI
2
The management point sends a list of the distribution points in the boundary group assigned to the client
Port 80
Data Centers
Enhanced Nodes
Standard Nodes
Distribution Point Server
Lago Patria
Norfolk
Northwood
Sigonella
Izmir
Port 80
3
The client uses one of the distribution points on the list as the source location for content

Figure 18 - MECM Content Management

4.3.1.5.39. MECM Content Management Design Decision

0168 The NATO requirements are to enable a distribution point at each datacentre, enhanced node and standard node site within the hierarchy.

Sites Category	Number of Sites	Distribution Point Configuration
Primary Site	1	Preferred DP, PXE, HTTP enabled, Content Validation, Schedule, Rate Limits
Distribution Points	5	Preferred DP, PXE, HTTP enabled, Content Validation, Schedule, Rate Limits

Table 23 - MECM Content Management Design Decisions

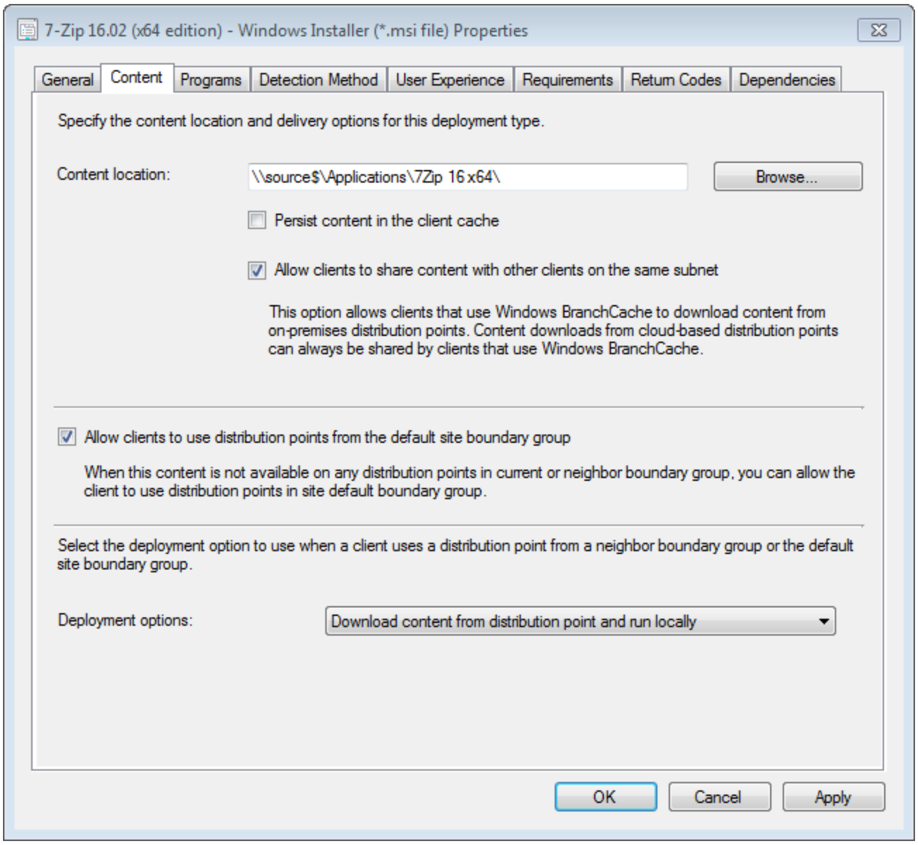
4.3.1.5.40. Distribution Point Group

0169 Distribution point groups provide a logical grouping of distribution points and collections for content distribution. A distribution point group can contain one or more distribution points from any site in the hierarchy. When content is sent to a distribution point group, all distribution points that are members of the distribution point group receive the content. When a new distribution point is added to a distribution point group, it receives all content that has been previously distributed to it. Collections can be associated to the distribution point group. When content is distributed, the collection and the distribution points that are selected that are members of all distribution point groups with an association to the collection receive the content.

0170 There will be one distribution point group created that will contain every package, application, software update package, etc. This group will be called **NATO - Enterprise Applications.** It will contain every distribution point in the site.

4.3.1.5.41. Content Management Design for Application Deployment Type

0171 Within the application's deployment type there are configurable settings designed to allow clients to share content when the content is not available on distribution points in the client's boundary group. The screenshot below illustrates how all application deployment types should be configured to allow for sharing of content:



Specify the content location and delivery options for this deployment type.

Content location: \\source$\Applications\7Zip 16 x64\

□ Persist content in the client cache

☑ Allow clients to share content with other clients on the same subnet

This option allows clients that use Windows BranchCache to download content from on-premises distribution points. Content downloads from cloud-based distribution points can always be shared by clients that use Windows BranchCache.

☑ Allow clients to use distribution points from the default site boundary group

When this content is not available on any distribution points in current or neighbor boundary group, you can allow the client to use distribution points in site default boundary group.

Select the deployment option to use when a client uses a distribution point from a neighbor boundary group or the default site boundary group.

Deployment options: Download content from distribution point and run locally

Figure 19 - Application Deployment Types for Content Management

4.3.1.5.42. Peer Cache Design Decision

0172 Peer Cache will be enabled in Client Settings and apply to all clients. Peer Cache enables Peer-to-Peer (P2P) transfers of content between clients within the same Boundary Group. Peer Cache clients report their cache contents to the ConfigMgr site, so that other peer systems can request that content. The content is located just like any other content lookup, except that MECM returns a list of peer cache systems along with any distribution points that have the content.

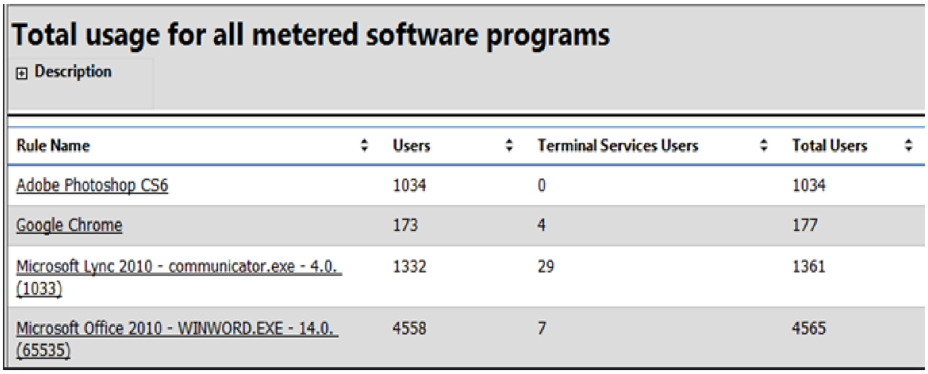
4.3.1.5.43. Software Metering

0173 Use software metering in MECM to monitor and collect software usage data from MECM clients.

0174 To collect this usage data, a MECM Admin will need to configure software metering rules. Once created, the client computers evaluate these rules and collect metering data to send to the site. If there is ever an interruption to service, the MECM client continues to collect usage data when there is no connection to the MECM site and sends this information when the connection is re-established.

0175 After collecting usage data from MECM clients, the data can be viewed in different ways, which includes using collections, queries and reporting. This data, combined with data from software inventory, can help to determine the following:

- How many copies of a particular software project have been deployed to the computers in the organisation? Among those computers, how many users actually run the project?
- How many licenses of a particular software project need to be purchased when renewing the license agreement with the software vendor?
- Whether users are still running a particular software project. If the project is not being used, then the project may be ideal for retirement.
- Which times of the day a software project is most frequently used.
- We use out-of-the-box reports for software metering using MECM Reporting. The following figure is snapshot of the report that is identifying the total usage for all software metered projects.



Total usage for all metered software programs

⊞ Description

Rule Name	Users	Terminal Services Users	Total Users
Adobe Photoshop CS6	1034	0	1034
Google Chrome	173	4	177
Microsoft Lync 2010 - communicator.exe - 4.0. (1033)	1332	29	1361
Microsoft Office 2010 - WINWORD.EXE - 14.0. (65535)	4558	7	4565

Figure 20 - Software Metering MECM Report

0176 Even if software is not deployed via MECM, tasks can be created for software metering. The task will be configured to find the software process and reports can be run to determine application usage.

4.3.1.5.44. Ports and Protocols

Comm. Description	Port	Description	Traffic Direction
Web Console	443	Web Console administration	Client to MECM server
Database Communication Ports	1433	Communication from MECM server to database	MECM server to database
Wake on LAN	9	Wake on LAN	MECM Server to client
Client Communication to DP	67/68	Client communication to distribution point	Client to MECM server

Comm. Description	Port	Description	Traffic Direction
Agent Push	135/167/138/139/445	TCP ports to push agent	SCOM server to clients

Table 24 - Ports and Protocols

4.3.2. RDSH

0177 For the service interface, RDSH delivers applications to the user community based on Active Directory Security Groups. This option uses layered applications delivered to desktops when loss of certain functions of the application, such as license activation keyed to a machine profile, requirements for static IP addressing or device drivers required for the application. Some resource intensive application deploy via RDSH due to resource requirements that cannot be met on the VDI images on thin client. Figure 21 displays the service interface interaction diagram and description.

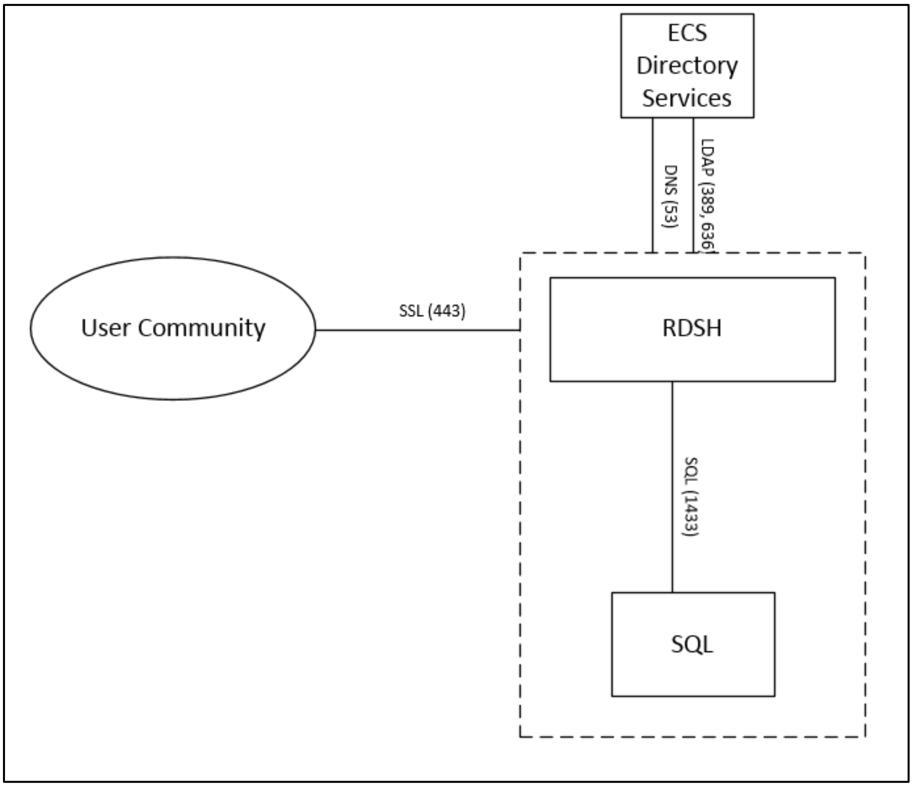


Figure 21 - RDSH Service Interface Interaction Diagram

Table 25 shows the user interface, and Table 26 shows the external interfaces for RDSH.

Source	Destination	Port/Protocol	Description
User Community	RDSH	443	Application Delivery

Table 25 - User Interface

Source	Destination	Port/Protocol	Description
RDSH	ECS Directory Services	389, 636	Query Security Group
RDSH	ECS Directory Services	53	Name Resolution

RDSH	SQL	1433	Database Communication

Table 26 - External Interfaces

0178 RemoteApp enables administrators to make projects accessed remotely through an RD Session Host server appear as if they run on the client computer. Instead of being presented to the user in the desktop of the RD Session Host server, the RemoteApp project integrates with the client computer.

0179 RDSH servers host Windows applications accessed by remote users over a network connection. Users are assigned to an application Active Directory security groups in order to receive the application. This option delivers layered applications to desktops, such as license activation keyed to a machine profile, requirements for static IP addressing or device drivers required for the application. Some resource-intensive applications are deployed via RDSH due to resource requirements not met on the VDI images on thin client. RDSH is used as an exceptional application provisioning technology. For consistency and optimisation, installation and update of applications installed on the RD Session Hosts is done via MECM taking into account Microsoft recommended practices and requirements for installation of applications on RD session hosts.

0180 RD Session Hosted RemoteApps consist of the following components:

- Remote Desktop Web Access Server
- Remote Desktop Connection Broker Server
- Remote Desktop Licensing Server
- Remote Desktop Session Host Server
- SQL Database (shared highly-available instance can be used)

0181 The server requirements are the following:

Site	Type	Enclave	Product
BEL-BRU-01	DC	ON AIS user domain and ON services domain and IREEN	RD Web Access Server (2) RD Connection Broker Server (2) RD Licensing Server (2) RD Session Host (4)
ITA-LAG-01	DC	ON AIS user domain and ON services domain	RD Web Access Server (2) RD Connection Broker Server (2) RD Licensing Server (2) RD Session Host (4)

Table 27 - RDSH Site Products

4.3.2.1. RDSH Server Requirements

Role	Server Name	Operating System	RAM (GB)	CPU (count)	Storage
RD Web Access Server	TBD	Windows Server latest approved	4	4	C:\ OS (100GB)
RD Connection Broker Server	TBD	Windows Server latest approved	8	4	C:\ OS (100GB)

RD Licensing Server	TBD	Windows Server latest approved	4	1	C:\ OS (100GB)
RD Session Host	TBD	Windows Server latest approved	64	8	C:\ OS (200GB)

Table 28 - Server Requirements

0182 Application provisioning subservice consists of several tools to deliver applications to both virtual and physical desktops within the ON domain. Each tool enables the delivery of allowed applications to the user based on Active Directory Security groups. CPS receives optimised and integrated WAN acceleration services from IaaS (see IaaS SDP section 2.3.2)**.** All application provisioning components authenticate to Active Directory (AD) in ECS. Identity Management in ECS provides the federation service for processing access requests from users external to the ON domains**.** In order to fully support federated users, the design for application provisioning is fully extensible and can be used to deliver to users that are federated through ECS Directory Services integration.

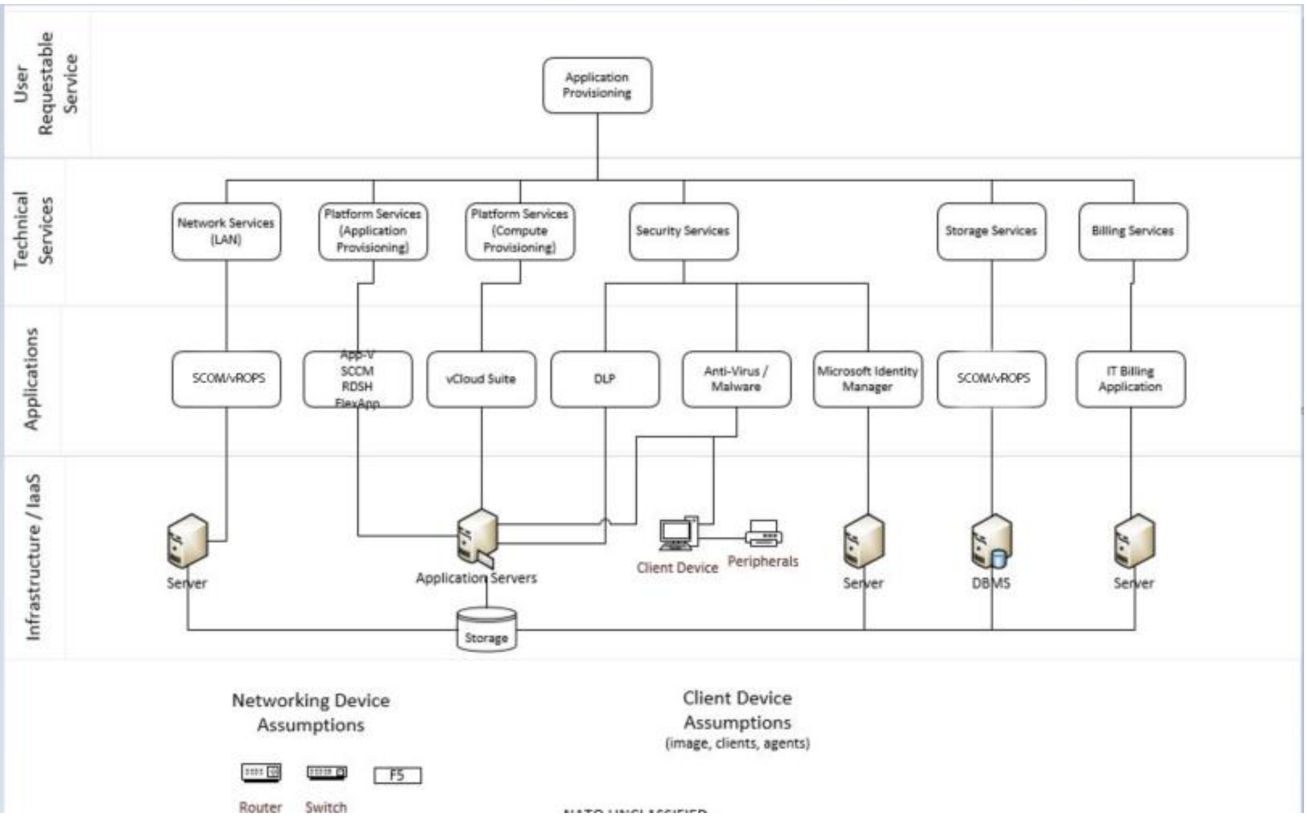


Figure 22 - Application Provisioning Subservice Topology

4.3.3. VMware AppVolumes

0183 Due to the tight integration with the VDI subservice, VMware AppVolumes is described in Annex E.5.

4.4. User Profile Service Solution

4.4.1. User settings and preferences

0184 The user profile management will use a layer of abstraction via the Windows technology Distributed File System Namespaces (DFS-N). Due to the nature of the data stored, albeit replicated, consistency of the data is important to prevent profile corruption, therefore the user profile data need to be accessible only via one entry point. For performance reasons, the user settings and user data shares will be local at the site where the users are based. In case of the end user logging in from another location, the shares will still be accessed via the same entry point.

0185 The user settings and preferences consist of two network shared folders:

- Configuration shared folder which is read-only for the end users. The configuration consists of configuration files (usually XML) and subfolders within the domain NETLOGON share (or other highly available DFS domain share) will be utilized for this.
  This will ensure high availability as the NETLOGON is replicated and accessibility as all clients have access to the NETLOGON share via SMB protocol.
- User settings share – this is a per-user shared folder that is writable for the end users. The user-specific settings are usually stored in a single archive file. This shared folder need to be dedicated for this purpose. The user settings share will have a quota per user. The user settings share will need to be replicated for failover purposes and included in backup and archive procedures, see ECS SDP document for further details.

0186 The following settings are customizable by the end users and consequently synchronized by default for all the users:

- Windows OS look and feel – Start Menu, Taskbar, regional settings, Windows Explorer view
- Printers – as the printing service is supported by a distributed set of print servers, the profile solution shall always deploy the shared print queue for the local site (on either a site-local print server or a server in a datacentre)
- Microsoft Edge
- Microsoft Office application settings
- Adobe Reader application settings

Additional settings may need to be synchronized for certain applications (e.g. ODBC connections for functional applications) and will be configured additionally and reflected in the as-built documentation.

4.4.2. User data

0187 Folder redirection will be used to redirect well-known user folders such as Desktop and My Documents folders to the network shared folder and others as deemed necessary by NCI Agency.

0188 Microsoft best practices are followed in accordance with performance and security specifications and referenced at this location:

https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/deploy-roaming-user-profiles

Configuration Management Server Requirements (1 server in BEL-BRU-01 datacenter)

Role	Server Name	Operating System	RAM (GB)	CPU (count)	Storage
User profile configuration management server	TBD	Windows Server latest version	16GB	2	C:\OS (60GB) D:Applicaion (50GB) P:\Page File (6GB)

Table 29 - Server Requirements

4.5. Print and scan Service Solution

0189 Content will be developed during project impementation.

4.6. Client Provisioning Cyber Security Service Solution

4.6.1. Software Applications Required on Endpoints for Security Functionality

0190 The table below lists the security software components that are required on different endpoints.

Vendor	Application Name	Short Name
Trellix (McAfee)	Agent	MA
Trellix (McAfee)	Endpoint Security	ENS
Trellix (McAfee)	ENS for Servers	ENS-S
Trellix (McAfee)	McAfee Security for Microsoft SharePoint	MSMS
Trellix (McAfee)	Endpoint Security for Linux	ENS-L
Trellix (McAfee)	Drive Encryption [2]	MDE
Trellix (McAfee)	Application Control	MAC
Trellix (McAfee)	Data Loss Prevention - endpoint	DLP-e
Trellix (McAfee)	Data Loss Prevention Discover	DLP-D
Tenable	Nessus Agent	OVA
AccessData	AccessData Enterprise Examiner	OCF-A
Fidelis	Fidelis Endpoint	OCF-F
Titus	Titus Classification for Microsoft Outlook’	LBL-O
Titus	Titus Classification for Desktop	LBL-D
Cisco	AnyConnect	VPN
Splunk	Universal Forwarder	SUF
Sysmon	Sysmon	SYS

Table 30 - Security software components

4.6.2. Software Application Mapping to Endpoint Types

0191 The table below indicates the components required for each type of endpoint described in the Scope section:

Endpoint Type		MA	ENS	ENS-S	ENS-L	MDE	MAC	DLP-e	DLP-D	OVA	OCF-A	OCF-F	VPN	LBL-O	LBL-D	SUF	SYS
Windows Clients	Physical	Y	Y	N	N	N	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
	Virtual	Y	N	Y	N	N	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y
Windows Servers	Physical	Y	Y	N	N	N	Y	Y	C	Y	Y	Y	N	N	N	Y	Y
	Virtual	Y	N	Y	N	N	Y	Y	C	Y	Y	Y	N	N	N	Y	Y
Linux Servers	Physical	Y	N	N	Y	N	Y	C	N	Y	C	Y	N	N	N	N	N
	Virtual	Y	N	N	Y	N	N	C	N	Y	C	Y	N	N	N	N	N

Table 31 - Required components per type of endpoint

0192 Note1: MSMS is required for Microsoft SharePoint servers.

0193 Note2: DLP-D will be installed only on a subset of servers.

0194 Windows Physical Client refers to a fully featured physical desktop and not a thin client device.

Symbol	Meaning
Y	Yes, this component is part of the baseline on this client type
N	No, this component is not part of the baseline on this client type
C	Case by case, the cyber security functions are required by no standard application

4.6.2.1. Functional Breakdown

0195 The table below provides a mapping of the software applications to security functions. While the application may provide further functionality, these are the functions that are expected to be configured according to the NCSC with respect to the relevant CIS.

Short Name	Function(s)
MA	This is required component for all others McAfee components.
ENS ENS-S	Anti-malware Protected web browsing Host based IDS/IPS Host based firewall [3]
ENS-L	Anti-malware Protected web browsing Host based IDS/IPS Host based firewall
MDE	Drive encryption
MAC	Application control (Allow-listing) Application control (Software Inventory Listing)
DLP-e	Endpoint Data Leakage Prevention Removable Media / External Device Control
DLP-D	Data classification in shared repositories
OVA	Endpoint Vulnerability Assessment
OCF-A	Forensics

OCF-F	Forensics
VPN	VPN User Client
LBL-O	Label based authorization of email sending
LBL-D	Label based classification of MS Office documents
OS	Smart Card User Authentication Access Control User Authentication Device Authentication (using NPKI) Event Logging
Firmware (BIOS/UEFI/Pre-OS)	Access control to firmware configuration Access Control to features Secure boot

[3] The built-in windows firewall can optionally replace the McAfee ENS Host based firewall component

4.6.3. McAfee Overview

0196 McAfee security software will be used to secure all servers, desktops, persistent VMs and non-persistent virtualized (VDI) clones connected to NATO Enterprise networks. McAfee provides a solution with centralized management and endpoint security products that provide protection mechanisms that meet all requirements for the environment.

0197 The security requirements have driven the future architecture and infrastructure for each datacentre and enhanced/standard nodes within the topography.

0198 The McAfee security product deployment architecture was designed based off of the device count for the sites in scope.

4.6.4. McAfee Security Design Topology

0199 A McAfee ePO server will be deployed in the BEL-BRU-01 datacentre in the ON Common Services Forest (SVC). This ePO server will be the parent ePO for each domain/tenant within the production environment. Agent Handlers, basically an ePO server without the application server service, will be deployed at the ITA-LAG-01 datacentre to distribute load and increase availability in the event of an outage**.** Super-Agent Distributed Repositories (SADR) will be deployed at each Enhanced and Standard node to minimize any latency or bandwidth issues related to McAfee security product updates (DATs and other content).

0200 A high-level view of the McAfee security architecture is below:

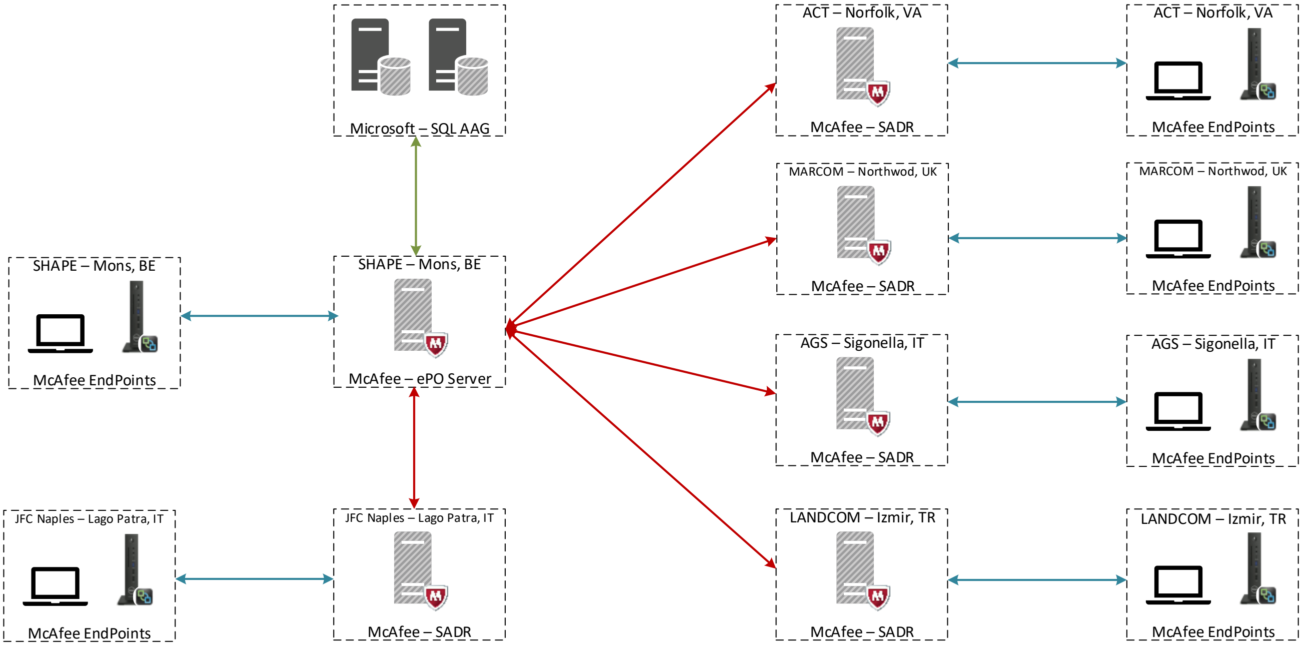


Figure 23 - High-Level View of the McAfee Security Architecture on ON network

Graphics note: Not all sites in scope are displayed in the figure.

0201 Initial set of policies for all Trellix (former McAfee) products, provided by NATO, shall be implemented and further tailored according to the COTS vendor documentations such as antivirus exclusions for domain controllers, Microsoft Exchange servers, etc.

4.6.5. ePO Hardware Configuration

0202 Four different installation types are required for the environment as it pertains to McAfee. First we have the ePO Application server. The ePO Application server needs a dedicated SQL server installation. Next we have any Remote Agent Handlers that may be required for load. Lastly, we have Super Agent Distributed Repositories (SADR) that are used as software update distribution points in each EN and SN across the enterprise. SADRs can be on shared servers or can be on dedicated VMs. Minimum hardware requirements for each installation type are presented below:

Role	Server Name	Operating System	RAM (GB)	CPU (count)	Storage
ePO Server	TBD	Windows Server latest version	16GB	4	C:\OS (60GB) D:\Page File (6GB) E:\Applications (50GB)
ePO SQL Server	TBD	MS SQL	16GB	4	C:\OS (60GB) E:\Applications (50GB) F:\Data (200GB) G:\Logs (200GB) H:\Backups (100GB)
Remote Agent Handler	TBD	Windows Server latest version	16GB	2	C:\OS (60GB) D:\Page File (6GB) E:\Applications (50GB)

Super-Agent Distributed Repository (SADR)	TBD	Windows Server latest version	8GB	2	C:\OS (60GB) D:\Page File (6GB) E:\Applications (50GB)
McAfee DLP Discover Server	TBD	Windows Server latest version	32GB	12	C:\OS (500GB)

Table 32 - ePO Minimum Hardware Requirements

4.6.6. McAfee Security Products and Features Overview

0203 The primary components of the McAfee security suite are the McAfee ePolicy Orchestrator (ePO) and the McAfee Agent. The Agent must first be deployed to all compatible systems within the organisation before McAfee security products can be deployed and managed by ePO.

0204 McAfee ePO provides a centralised but distributed architecture allowing the point-product software to be centrally managed and yet decrease the amount of network traffic required to manage clients. ePO provides the management interface and functionality for the administrators of the McAfee software stack. It also provides centralised point product event collection, analysis and report creation functionality.

0205 Unless noted otherwise, each of the McAfee products referenced are agent-based and deployed and managed through the ePolicy Orchestrator's centralised console. This framework provides security administrators with central management, as well as the ability to test policy updates in test environments in a much easier fashion.

4.6.7. McAfee ePolicy Orchestrator

0206 The McAfee ePolicy Orchestrator is an extensible platform that enables centralized policy and client task management as well as security status and event reporting. Using this platform, a McAfee administrator can accomplish a number of tasks, including:

- Manage McAfee products with the ability to deploy, track, manage and delete from the ePO console.
- Manage and enforce host level security using policy assignments and client tasks.
- Create reports using the query system builder, which displays configurable charts and tables of network host security data.
- Schedule updates for anti-virus DAT (signature) files, engines and other security content required by deployed McAfee security software to keep managed systems current.

0207 The architecture of the McAfee ePO software and its components is designed to help successfully manage and protect the environment. It does this mainly through the use of the McAfee Agent.

0208 McAfee product updates will be pulled from existing NATO repository and NATO PKI web certificate will be installed on the ePO Console web access.

4.6.8. ePO Disaster Recovery and Agent Communication Failover

0209 In a disaster recovery scenario, if the site that houses the ePO server is down and not recoverable, manual intervention is required to restore the service. However, while the ePO server is not accessible, the deployed McAfee Agents will still function based on the last policies received. If the ePO site/server is not recoverable, a new ePO server with the same name will have to be deployed and the database will have to be restored in order for the agents to re-establish communication with the ePO server. See IaaS SDP for backup design.

0210 Remote Agent Handlers can and will be used to assist with load balancing and provide some failover capability. Agent Handlers need a direct, high-speed connection to the ePO Server SQL database so their use as failover candidates are limited. Once multiple agent handlers are deployed, they can be made available to agents as failover candidates. This allows the application server and any number of agent handlers to either fail or be taken offline while still enabling agents to receive updated tasks or policy from the online agent handler(s). As long as the agent handler is connected to the database it can continue serving agents, including any policy or task modifications that result from agent properties or from user modifications prior to the application server being taken offline.

4.6.9. McAfee Required Ports and Protocols

0211 A listing of the ports and protocols needed for communication between the ePO server, SQL server and McAfee Agent are below:

Comm. Description	Port	Description	Traffic Direction
Agent-server communication	80	TCP port that the McAfee ePO server service uses to receive requests from agents	Inbound connection to the ePO server/Agent Handler from the McAfee Agent. Inbound connection to the ePO server from the Remote Agent Handler.
Agent-server communication secure port Software Manager, Product Compatibility List, and License Manager port	443	TCP Port that the ePO server service uses to receive requests from agents and Remote Agent Handlers. TCP port that the ePO server's Software Manager uses to connect to McAfee. TCP port that the ePO server uses to connect to the McAfee software updates server, license server, and McAfee Product Compatibility List	Inbound connection to the ePO server/Agent Handler from the McAfee Agent. Inbound connection to the ePO server from the Remote Agent Handler. Outbound connection from the ePO server to the McAfee servers.
Agent wake-up communication port SuperAgent repository port	8002	TCP port that agents use to receive agent wake-up requests from the ePO server or Agent Handler TCP port that the SuperAgents configured as repositories that are used to receive content from the ePO server during repository replication, and to server content to client systems	Inbound connection from the ePO server/Agent handler to the McAfee Agent. Inbound connection from the client systems to SuperAgents configured as repositories.
Agent Broadcast communication port	8082	UDP port that the SuperAgents use to forward messages from the ePO server/Agent Handler.	Outbound connection from the SuperAgents to other McAfee Agents.

Comm. Description	Port	Description	Traffic Direction
Console-to-application server communication port	8443	TCP port that the ePO Application Server service uses to allow web browser UI access	Inbound connection to the ePO server from the ePO console.
Client-to-server authenticated communication port	8444	TCP port that the Agent Handler uses to communicate with the ePO server to get required information (such as LDAP servers).	Outbound connection from the Remote Agent Handlers to the ePO server.
SQL Server TCP port	1433	TCP port used to communicate with the SQL server.	Outbound connection from the ePO Server/Agent Handler to the SQL server.
SQL Server UDP port	1434	UDP port used to request the TCP port that the SQL instance hosting the ePO database is using.	Outbound connection from the ePO server/Agent Handler to the SQL server.
LDAP server port	389	TCP port used to retrieve LDAP information from Active Directory servers.	Outbound connection from the ePO Server/Agent Handler to an LDAP server.
SSL LDAP server port	636	TCP port used to retrieve LDAP information from Active Directory servers.	Outbound connection from the ePO server/Agent Handler to an LDAP server.
SMB Windows domain controller port	445	TCP port used for ePO console logon when authenticating Active Directory users.	Outbound connection from the ePO server to the domain controller (Active directory) server.
Syslog server port	6514	Port used for Syslog forwarding using TLS	Outbound from the ePO server/Agent Handlers to registered syslog server.

Table 33 - McAfee Ports and Protocols

0212 Initial NATO configuration all McAfee products including network port assignments will be provided and implemented by the Contractor.

4.6.10. McAfee Agent

0213 The McAfee Agent will be deployed to all compatible systems within the enterprise. The McAfee Agent is the client-side component providing secure communication between McAfee ePolicy Orchestrator and managed products. It also serves as an updater for managed McAfee products.

0214 Through the McAfee Agent, the following can be done:

- Install products, their updates and upgrades
- Enforces policies and schedules tasks
- Gathers information and events from managed systems, and sends them to the McAfee ePO server

0215 Without the McAfee Agent, there would be no communication between an endpoint and its installed McAfee products and the McAfee ePO.

0216 When the McAfee Agent is installed on a VDI image, additional steps need to be executed following vendor guidance.

4.6.11. McAfee Application Control

0217 McAfee Application Control will be used for application whitelisting for all compatible systems within the enterprise. Application Control software blocks unauthorized applications on servers, corporate desktops and fixed-function devices. This centrally managed whitelist solution uses a dynamic trust model and innovative security features that thwart Advanced Persistent Threats (APTs) – without requiring signature updates or labour-intensive list management**.**

0218 Application Control protects against malware attacks by proactively controlling the application executing on the endpoint. It locks down the protected endpoints against threats and unauthorized changes, without file system scanning that might hinder performance although locked down, it can accept new software and updates through authorized processes configured through policy. With McAfee's dynamic whitelisting trust model, only approved applications are allowed to install, run and update, thus reducing overhead and improving continuity.

4.6.12. McAfee Policy Auditor with File Integrity Monitor (FIM)

0219 The system will use McAfee Policy Auditor to leverage File Integrity Monitor (FIM) on the NATO ON. This will involve deploying the Policy Auditor Agent to servers.

0220 The agent is configured to monitor and detect unauthorized changes to binary files, which include the following file types:

- *.exe
- *.bat
- *.com
- *.cmd
- *.dll

0221 Along with these file types FIM will be used to monitor critical application files on a case by case as define application owners.

0222 Scanning of files will occur weekly and events will be reported back to ePolicy Orchestrator.

4.6.13. McAfee Endpoint Security

0223 McAfee Endpoint Security (ENS) will be used to provide anti-virus, host-based IPS and host-based firewall on all compatible systems within the enterprise. McAfee Endpoint Security is a comprehensive security management solution that runs on servers and workstations to identify and stop threats automatically. Endpoint Security is managed through the installation and configuration of the following modules.

4.6.13.1. Platform

0224 Shared components which provide the platform upon which the ENS products are managed.

4.6.13.2. Threat Prevention

0225 Checks for viruses, spyware, unwanted programs and other threats by scanning items on the computer. ENS provides the following:

0226 Initial NATO configuration will be implemented and where necessary to improve performance Scan Cache and System Utilization will be configured.

0227 On-Access scanning will be used along with On-Demand scanning to enhance client security. On-Access scanning will be configured to allow McAfee to decide if it's a "Read Scan" or a "Write Scan". Enabling this option uses trust logic to optimize scanning improving security and performance.

- Exploit Prevention (IPS): Contains hundreds of signatures built-in that prevent known and unknown exploits. Stops exploited buffer overflows from executing arbitrary code. This feature monitors user-mode API calls and recognizes when they are called as a result of a buffer overflow.
- Access Protection: Prevents unwanted changes to managed computers by restricting access to specified files, shares, and registry keys, registry values, processes and services.

4.6.13.3. Firewall

0228 Host-level firewall that scans all incoming and outgoing traffic. Checks traffic according to a set of rules and blocks or allows traffic accordingly. Rules and rule groups will be created to block certain types of traffic, specific applications, and domains.

0229 The ENS suite of products stay up to date through the client connecting to a McAfee ePO server to receive AMCore content files.

4.6.13.4. McAfee Endpoint Security for Servers

0230 McAfee Endpoint Security for Servers will be used for all virtual servers to leverage the smart scheduler capabilities and avoid performance issues at the virtualization layer.

4.6.14. McAfee Data Loss Prevention Endpoint

0231 McAfee Data Loss Prevention Endpoint (DLPe) will be used to restrict device use to only those authorized, to prevent CD/DVD burning and to keep domain specific data where it belongs. DLPe identifies and protects data within the network. McAfee DLPe identifies the types of data on the network, how the data is accessed and transmitted and if the data contains sensitive or confidential information. DLPe can inspect and control content and user actions on endpoints through various types of data, web and application rules.

4.6.14.1. Integration with Titus

0232 Titus and McAfee will be configured in a way that McAfee will understand and read the Titus labels on files and email messages and use the labels in rules. Integration of the two products will be configured based on NATO-provided configuration guide at the time of implementation and Titus client will report events to McAfee ePO.

4.6.14.2. Device Control

4.6.14.2.1. Mass Storage Devices

0233 ON will implement Device Control to allow users to use their approved encrypted USB drive on their client device.

0234 Device Control will leverage removable storage rules to implement this policy. To implement this approach rules will be based on the most specific device attributes, at a minimum:

- Vendor ID
- Product ID
- Serial Number

0235 In addition to this rule a mechanism will be leveraged to tie an Encrypted USB device to a User to a Client device for the purpose of allowing write permissions (https://kcm.trellix.com/corporate/index?page=content&id=KB86007) .

4.6.14.2.2. Plug and Play Devices

0236 ON will implement Device Control and leverage Plug and Play device rules to block unauthorized classes of devices such as Bluetooth, SATA/SAS devices, etc. Additionally rule sets will be implemented that block computer to computer USB, PCI, Firewire, and Bluetooth transfers.

4.6.14.3. Content Control

0237 McAfee DLPe will assist with classifying data and will protect against data loss through the use of:

- Clipboard software
- Cloud applications
- Email (including email sent to mobile devices)
- Network shares
- Printers
- Screen captures
- Specified applications and browsers
- Web posts

4.6.15. McAfee Data Loss Prevention Discover

0238 McAfee Data Loss Prevention Discover is integrated with McAfee Data Loss Prevention Endpoint and ePO. It will be installed as close as possible to major data repositories such as MS Sharepoint and SMB/CIFS servers, and database systems (where supported). McAfee DLP Discover aims to secure sensitive data before it is accessed or moved. It will scan resources on the network and index all content found. This allows for data mining and querying and the building of an understanding of the presence of sensitive data. Based on configurable policy McAfee DLP Discover will be able to identify information and proliferation risks, and record policy violations. Integrated incident workflow and case management support the handling of incidents.

4.6.16. McAfee Security for Microsoft SharePoint

0239 McAfee Security for Microsoft SharePoint (MSMS) will be installed on all Microsoft SharePoint Web Front End and Application servers in NS and NR. MSMS scans all files that are uploaded or downloaded from the SharePoint server. It protects the data stored on the Microsoft SharePoint server from numerous threats that could adversely affect the systems, network or employees. It uses advanced heuristics against viruses, unwanted content, potentially unwanted programs and banned file types. It can be configured for the actions to take on the detected and the suspicious items.

0240 When a user uploads documents, SharePoint passes the documents to MSMS. The anti-virus scanning engine compares the documents with all the known virus signatures stored in the DATs. The Data Loss Prevention and Compliance engine scans the documents for banned content as specified in the content management policies. Scanning takes place when creating, saving or modifying data on the SharePoint server. On-demand scans can be scheduled to run immediately, at a particular-time or at regular intervals. The software checks the documents and files in real time against the repository of up-to-date DAT files and configured policy. If it finds the files to be malicious, it notifies and protects the managed node. It can be configured to delete unauthorized data or place it in quarantine for later review.

4.6.17. Other security agents

0241 Security and forensics agents are installed on the endpoints. NATO will provide the applications and desired configuration at the time of implementation.

4.6.18. Security measures

0242 The client provisioning services implements controls to satisfy the security measures listed herein. Once implemented the last column will be filled in by the Contractor for each item mentioning the subservice/system where the control is implemented and any relevant additional information:

Section	ID	Security Measure text	CPS Component envisionned	Physical Desktop	Thin Client	VDI	Implement. Details / Comment
Section PHM2: BIOS/UEFI	PHM2-1	BIOS/UEFI is accessible only by authorized privileged users.	BIOS password is configured and is accessible only after the password is provided	Dell Command | Configure	Dell Wyse Management Suite	N/A	
Section PHM2: BIOS/UEFI	PHM2-2	Security patching of BIOS/UEFI firmware is performed.	Element SMC management	On-premises repository and Dell Command | Update application deployed. Automated updates via MECM	Application package for Dell Wyse Management Suite	N/A	
Section PHM2: BIOS/UEFI	PHM2-3	Unnecessary BIOS/UEFI features are disabled.	Element SMC management	Dell Command | Configure package automated via MECM	N/A	N/A	
Section PHM2: BIOS/UEFI	PHM2-4	UEFI secure boot is enabled when available.	Configure and monitor	Configure via Dell Command | Configure application Monitor via inventory of WMI classes from MECM when Dell Command | Monitor is deployed	Report from Dell Wyse Management Suite	N/A	
Section PHM7: Removable CIS Storage Media Use	PHM7-2	Security measures prevent unauthorized removable CIS storage media being used on the CIS.	McAfee DLP Endpoint	McAfee DLP Endpoint	End users cannot interract with the removalbe storage device on the thin client	McAfee DLP Endpoint	
Section PSW2: OS and Application Control	PSW2-2	The execution of applications is controlled in order to ensure authorized execution.	Windows AppLocker or McAfee Application Control	McAfee Application Control	Windows AppLocker	McAfee Application Control	
Section PSW2: OS and Application Control	PSW2-3	The download or automatic execution of unauthorized mobile code is blocked.	Windows AppLocker or McAfee Application Control	McAfee Application Control	Windows AppLocker	McAfee Application Control	
Section PSW3: Malicious Code and Anti-Malware	PSW3-1	Protection against malicious code is deployed across the CIS in a multi- layer approach.	Windows AppLocker or McAfee Application Control on the clients	McAfee Application Control	Windows AppLocker	McAfee Application Control	
Section PSW3: Malicious Code and Anti-Malware	PSW3-3	The anti-malware solution uses more than signature based detection.	McAfee Endpoint Security Adaptive Threat Prevention	McAfee Endpoint Security Adaptive Threat Prevention	N/A	McAfee Endpoint Security Adaptive Threat Prevention	

Section	ID	Security Measure text	CPS Component envisionned	Physical Desktop	Thin Client	VDI	Implement. Details / Comment
Section PSW3: Malicious Code and Anti-Malware	PSW3-4	Updates of the malware protection (e.g. signature definitions, heuristics) are deployed within 24 hours.	McAfee ePO task to update server from upstream repository + + client ask to execute every 12 hours on the clients + report to monitor distribution of updates	McAfee Endpoint Security	N/A	McAfee Endpoint Security	
Section PSW4: Application Security	PSW4-3	The CISP applies up to date hardening guidance to OS and configurable applications throughout their life-cycle.	Active Directory Domain Services Group Policy objects for the products in the client baselines	Active Directory Domain Services Group Policy objects	Custom scripts to enforce the necessary settings	Active Directory Domain Services Group Policy objects	
Section PSW4: Application Security	PSW4-4	Operating Systems are approved by the SAA.	Use only approved Operating Systems	Use only approved Operating Systems	Use only approved Operating Systems	Use only approved Operating Systems	
Section PSW5: Security Patching and Upgrades	PSW5-1	The CISP applies critical security patches within a week and non-critical security patches within four weeks.	Patches and applications are distributed and deployed via MECM	Microsoft and application updates are deployed via MECM	Microsoft and application updates are deployed via Dell Wyse Management suite	Updated master image and/or application is deployed to all desktop pools	
Section PSW5: Security Patching and Upgrades	PSW5-2	The organisation only uses versions of software that: · are supported with security patches; · do not require an obsolete version of OS, libraries and dependencies to function.	Use only approved software applications	Use only approved software applications	Use only approved software applications	Use only approved software applications	
Section PSW5: Security Patching and Upgrades	PSW5-4	The organization removes no longer required or unused software and firmware after updates.	Deprecated and outdated application deployments are stopped	Deprecated and outdated application deployments are stopped	N/A	Deprecated and outdated application deployments are stopped	
Section POS4: PKI Services	POS4-2	The validity of PKI certificates are verified through all subordinate CAs to the Root CA.	Configure certificate validation wherever possible	Configure certificate validation wherever possible	Configure certificate validation wherever possible	Configure certificate validation wherever possible	
Section NWS4: Network Access Control	NWS4-1	The CIS implements Network Access Control (NAC).	Configure device enrolment, deploy and configure NAC/NAP supplicant where required	Configure certificate autoenrolment via Group Policy objects.	Configure certificate enrolment via Dell Wyse Management suite	N/A	Network ports used for operating system deployment are excluded and dedicated VLANs

Section	ID	Security Measure text	CPS Component envisionned	Physical Desktop	Thin Client	VDI	Implement. Details / Comment
							and IP subnets are used which allow access only to the required resources for the deployment.
Section DA4: Data Loss Prevention	DA4-1	Data loss prevention (DLP) measures are undertaken to detect and prevent potential data breaches at endpoints and during transmission.	McAfee DLP Endpoint	Rules log copy and print of file with defined or higher classification	N/A	Rules log copy and print of file with defined or higher classification	
Section IAM3: Authentication	IAM3-4	Users access CIS using multifactor authentication.	Users use smartcards	Users use smartcards	N/A	Users use smartcards	
Section IAM3: Authentication	IAM3-7	When authenticators for system and security administrator accounts are kept for emergency access, they are protected (e.g. sealed enveloped) in an appropriate security container.	Credentials for built-in system and software administrator, backup, recovery and similar accounts are set in accordance with IAM4-1 and handed over to a designated point of contact from the Agency. Consequent access to the systems happens with personal administrator accounts.	Applicable	Applicable	Applicable	
Section IAM4: Password based Authentication3	IAM4-11	The CISP changes default passwords on CIS (e.g. devices, service accounts, applications).	All default passwords on the end user devices are changed	All default passwords on the end user devices are changed	All default passwords on the end user devices are changed	All default passwords on the end user devices are changed (VDI = VMware Horizon)	
Section IAM4: Password based Authentication3	IAM4-13	Passwords are handled at least at the same classification level of the CIS they protect. The storage of administrator passwords for emergency use is covered in IAM3-7.	See envisioned solution for IAM3-7	Applicable	Applicable	Applicable	

Section	ID	Security Measure text	CPS Component envisionned	Physical Desktop	Thin Client	VDI	Implement. Details / Comment
Section IAM5: PKI based Authentication4	IAM5-2	For PKI based authentication, the CISP ensures the CIS validates certificates by constructing and verifying a certificate path to a trust anchor including checking certificate status information.	See envisioned solution for POS4-2	Applicable	Applicable	Applicable	
Section IAM5: PKI based Authentication4	IAM5-3	The PIN or alphanumeric passcode used to access the PKI private key for logical access is not less than six digits or characters long.	Enforce if feasible	Enforce if feasible	N/A	Enforce if feasible	
Section IAM5: PKI based Authentication4	IAM5-4	The passcode (IAM5-3) is not easily guessed. The CISP enforces this if technically feasible.	Enforce if feasible	Enforce if feasible	N/A	Enforce if feasible	
Section IAM5: PKI based Authentication4	IAM5-5	The smartcard is locked if the PIN or Passcode is incorrectly entered 5 to 10 times.	Enforce if feasible	Enforce if feasible	N/A	Enforce if feasible	
Section IAM7: Preventing Credential Theft and Reuse	IAM7-1	The CISP prevents lateral movement of an attacker by using appropriate security measures.	Microsoft Local Administrator Password Solution, Private VLANS, turn off unnecessary features	Microsoft LAPS	Private VLANs, unnecessary features and software are removed	Microsoft LAPS	
Section IAM7: Preventing Credential Theft and Reuse	IAM7-2	The CISP hardens credential stores and mechanisms.	Microsoft Credential Guard is enabled	Microsoft Credential Guard is enabled	N/A	Microsoft Credential Guard is enabled	
Section IAM9: Access Control	IAM9-5	Normal users do not have local admin privileges (Tier 2) on their workstations.	Enforced defined list of workstation administrators	Enforced defined list of workstation administrators	Administrator password is not shared	Enforced defined list of workstation administrators	
Section IAM10: Privilege Users Access Control	IAM10-14	Tier 0 and 1 administration computers system updates are not pushed from a lower Tier.	MECM	MECM, dedicated security roles and collections for admin WS	N/A	N/A	
Section IAM11: Session Control	IAM11-1	Session lock is implemented after a certain period of inactivity as agreed by the SAA; The requirement for CIS with exceptional operational	Automatic device lock after a defined period of inactivity	Automatic device lock after a defined period of inactivity	Automatic device lock after a defined period of inactivity	Automatic device lock after a defined period of inactivity	

Section	ID	Security Measure text	CPS Component envisionned	Physical Desktop	Thin Client	VDI	Implement. Details / Comment
		requirements may be relaxed or omitted.					
Section IAM11: Session Control	IAM11-2	Concurrent sessions to a service by a single user are limited and monitored to prevent masquerading.	No fast-user switching and multiple sessions on VDIs	No fast-user switching option	N/A	No multiple sessions for the same user are allowed	
Section IAM11: Session Control	IAM11-4	The CIS displays system use notice information to the user before login is completed.	Active Directory Domain Services Group Policy objects	Active Directory Domain Services Group Policy objects	N/A	Active Directory Domain Services Group Policy objects	
Section CM2: Component Inventory	CM2-1	An accurate inventory(s) of CIS hardware and software is maintained.	All devices are managed/registered by the element SMC management system	All devices are registered in MECM	All thin clients are registered in Dell Wyse Management Suite	All devices are registered in MECM and VMware Horizon	
Section CM2: Component Inventory	CM2-2	The CISP, the SAA, or both, develops and maintains in a coordinated manner baseline configurations of CIS components.	Client devices baselines are documented	Applicable	Applicable	Applicable	
Section CM2: Component Inventory	CM2-3	At least the previous baseline configuration is maintained for each CIS component.	Client devices baselines are documented	Applicable	Applicable	Applicable	
Section CM5: Configuration Settings	CM5-1	Configuration settings are established, documented and approved for components employed in the CIS.					
Section CM5: Configuration Settings	CM5-2	Components within the CIS are configured to provide only required capabilities (least functionality). Components which are not required are either uninstalled, not installed or disabled.	Unnecessary features and software are removed	Only required and necessary software is deployed	Unnecessary features and software are removed	Only required and necessary software is deployed	
Section CM5: Configuration Settings	CM5-3	The configurations of components within the CIS are periodically verified against the approved baseline.	Monitor via regular reporting which identify deviations	MECM reports for deployed software, BIOS settings McAfee reports of deployed components, policies and definition and signature updates	Report from Dell Wyse Management Suite	VMware AppVolume report of deployed software McAfee reports of deployed components, policies and definition and	

Section	ID	Security Measure text	CPS Component envisionned	Physical Desktop	Thin Client	VDI	Implement. Details / Comment
						signature updates	
Section LMA3: Time Stamps	LMA3-1	An authoritative time source is used.	Configure and verity NTP source is used	N/A	Via Dell Wyse Management Suite	N/A	
Section CP2: Failover/Load Balancing	CP2-1	The CIS implements automatic failover/load balancing for critical CIS components.	End user components are configured with load balanced/virtual names of services	End user components are configured with load balanced/virtual names of services	End user components are configured with load balanced/virtual names of services	End user components are configured with load balanced/virtual names of services	

Table 34 - Security Measures and CPS Components

4.7. Client Provisioning Service Management and Control (SMC)

4.7.1. SCOM

0243 System Center Operations Manager (SCOM) latest approved version shall be used to monitor the overall health of the MECM, Exchange, AD-DS, AD-FS, AD-LDS, DFS-R, DNS, DHCP, Print Server, VMware Horizon, VMWare AppVolumes, RDSH, McAfee ePO, SQL, SharePoint, MIM, TFS, Skype, DPM and Windows Servers. The following diagrams illustrate the logical site hierarchy for the NATO SCOM infrastructure for the High Side implementation. Two Management Groups will be implemented in order to satisfy the High Availability requirements as depicted in **Figure 24 - SCOM High Side BEL-BRU-01 Datacenter Management Group Design Subservice** Topology and **Figure 25 - SCOM High Side ITA-LAG-01 Management Group Design Subservice Topology**.

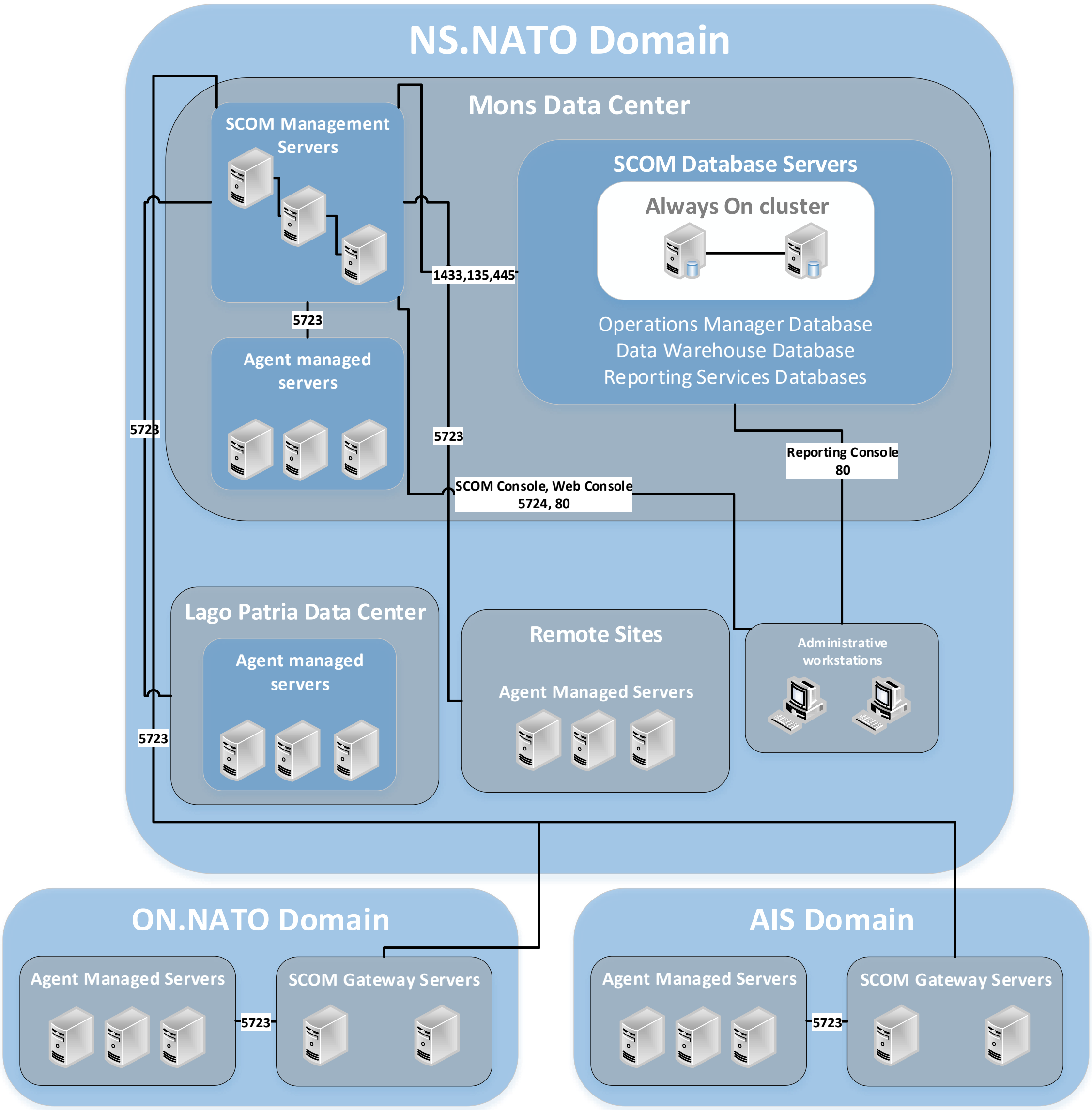


Figure 24 - SCOM High Side BEL-BRU-01 Datacenter Management Group Design Subservice Topology

*Figure note: AIS Domain will be monitored from AIS SCOM and the NATO ON SCOM instance will be connected with the one from AIS.

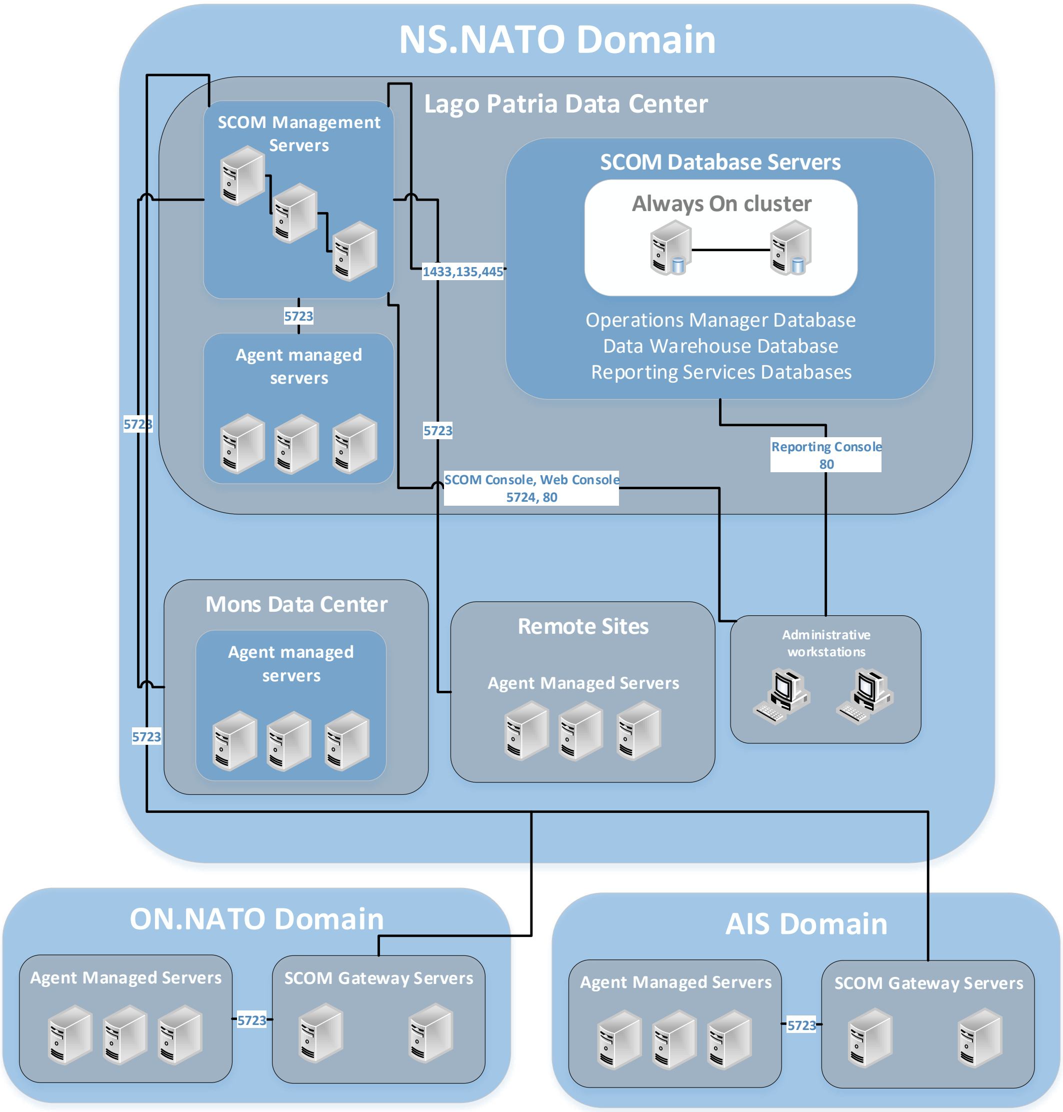


Figure 25 - SCOM High Side ITA-LAG-01 Management Group Design Subservice Topology

4.7.1.1. SCOM Components

4.7.1.1.1. SCOM servers

0244 SCOM servers hold supports multiple site system roles. The purpose of particular components is described below: Management Server

SCOM Component	Role Description
Management Server	The role of the management server is to administer the management group configuration, administer and communicate with agents, and communicate with the databases in the management group.
Web Console	Web console displays only My Workspace and the Monitoring workspace.
Operations Console	Operations console enables the option to check the health, performance and availability for all monitored objects in the environment and helps identify and resolve problems.
Reporting Server	The Reporting Server is a server role processing the reporting in the SCOM environment. Typically installed on the SCOM database server

Table 35 - Management Server

4.7.1.1.2. SQL Server

SCOM Component	Role Description
Operational Database	SQL Server database that contains all configuration data for the management group and stores all monitoring data that is collected and processed for the management group. The operational database retains short-term data, by default 7 days.
Data Warehouse Database	SQL Server database that stores monitoring and alerting data for historical purposes. Data that is written to the Operations Manager database is also written to the data warehouse database, so reports always contain current data. The data warehouse database retains long-term data.
Reporting ServicesReportServer Database	SQL Reporting engine that allows the building and running of custom reports. Server Database used by the SQL Reporting Services Component. It stores report definitions used for SCOM Reporting and is updated when new rep[orts are defined or definitions of existing reports are changed
ReportServerTempDB database	SQL Server Database that is used in order to cache the data processed during the execution of the reports

Table 36 - SQL Server

4.7.1.1.3. SCOM Service Account and Security Group Requirements

0245 As part of the SCOM Design process a number of Active Directory groups and user accounts have been identified. The accounts and groups will need to be established in the NATO Active Directory environment for correct and secure operation of the SCOM environment.

0246 Access to SCOM functionality is controlled via permissions and roles. Individuals that require the ability to perform certain actions within SCOM (including running reports) will need to be granted the respective permissions. As a best practice, Microsoft recommends that groups, as opposed to users, are used to define SCOM permissions. Also, the ‘principle of least privilege’ should be followed. Taking into account the HA infrastructure it is very important, to provide SCOM power user write access only to SCOM admins with SCOM-related knowledge. Any changes performed on one of the HA Management Groups will have to be reflected in another one, which is a manual process.

4.7.1.1.4. Service Accounts

0247 The following service accounts are required to complete the installation and configuration of SCOM.

0248 Group Managed Service Accounts will be used.

Service Accounts	Purpose
svcSCOMAA	SCOM Server Action Account
svcSCOMDAS	SCOM Config and Data Access Account
svcSCOMREAD	SCOM Datawarehouse Reader Account
svcSCOMWRITE	SCOM Datawarehouse Write Account
svcSCOMSQL	SCOM SQL Service Account
svcSCOMADMINS	SCOM Administrators Security Group

Table 37 - Service Accounts

4.7.1.1.5. Security Groups

0249 The following security groups are required to complete the configuration of SCOM.

Administrative Groups	Purpose	Type
Enterprise SCOM Admins	Grants full write permissions on all SCOM instances	Global

Table 38 - Security Groups

4.7.1.1.6. Management Packs

0250 Management packs provide possibility to monitor specific aspects (such as configuration, performance or availability) of various services. Implemented management packs will cover monitoring of the servers running the following services:

- System Center Configuration Manager Servers
- Microsoft Exchange Servers
- Active Directory Services Servers,
- Active Directory Federation Services Servers
- Active Directory Lightweight Directory Services Servers
- Distributed Files Services Servers - Replication
- Domain Name Servers
- DHCP Servers
- Print Servers
- App-V Servers
- Microsoft SQL Servers
- Microsoft SharePoint Servers
- MIM Servers
- Team Foundation Servers
- Skype for Business Servers
- DPM Servers
- Operating Systems of all monitored Windows 2016 Servers
- IIS Services installed on all the monitored Servers

0251 Every management pack contains set of SCOM objects such as discoveries, monitors, rules, tasks, views, run as profiles or reports. They are a core of the capability to monitor particular services. Depending on the management pack it might be necessary to perform further configuration in order to launch discoveries. All the configuration and thresholds will be agreed with the service owners and configured accordingly. Any unnecessary “noisy” configuration items will be disabled in order to maintain high performance of SCOM instance. A short explanation of a purpose of each of the elements embedded in the management packs is provided below:

- Monitors: which direct an agent to track the state of various parts of a managed component.
- Rules: which direct an agent to collect performance and discovery data, send alerts and events and more.
- Tasks: which define activities that can be executed by either the agent or the console.
- Knowledge: which provides textual advice to help operators diagnose and fix problems.
- Views: which offer customized user interfaces for monitoring and managing this component.
- Reports: which define specialized ways to report on information about this managed component.
- Object discoveries: which identify objects to be monitored.

- Run As profiles: which allow different rules, tasks, monitors or discoveries under different accounts on different computers to be run.

4.7.1.1.7. High Availability

0252 High-availability needs are addressed on several levels. Each of them is addressed below and explained on the respective diagrams

0253 SCOM databases for each management group are hosted on the Always On clusters. They work in an active/passive configuration. Both servers are continuously synchronized ensuring data consistency across cluster nodes. In case of a server failure Always On cluster seamlessly switches the passive server to active and the operation of SCOM service continues uninterrupted. The architecture is explained on the following diagram:

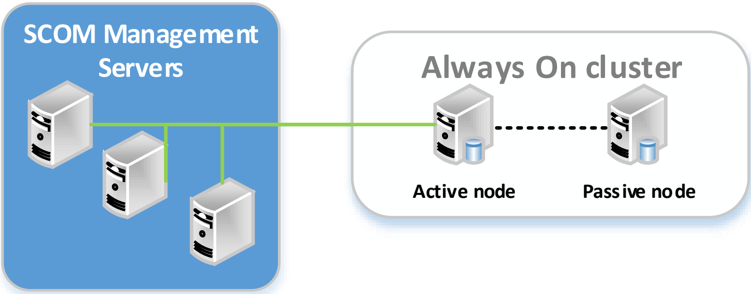


Figure 26 - High Availability design for SCOM SQL servers

0254 Every management group hosts three SCOM management servers. First server is deployed exclusively for the purposes of processing roles and configuration that is specific for one particular SCOM server only, such as installing connectors to other systems, correlation engines, RMS emulation and so on. The second and third management servers are used to communicate with the SCOM agents installed on the client systems. Those clients machines will be randomly assigned to one of the two pools. The first pool will use SCOM server number 2 as its primary management server and the SCOM server number 3 as its secondary management server. The second pool will be configured in an opposite way – it will use SCOM server number 3 as its primary management server and the SCOM server number 2 as its secondary management server. This configuration ensures, that in case of failure of any of the SCOM servers used for communication with SCOM agents, all the client machines from the pool using this server as a primary one will automatically fail over to the secondary server maintaining continuous communication. The architecture of the solution is explained on the following diagram.

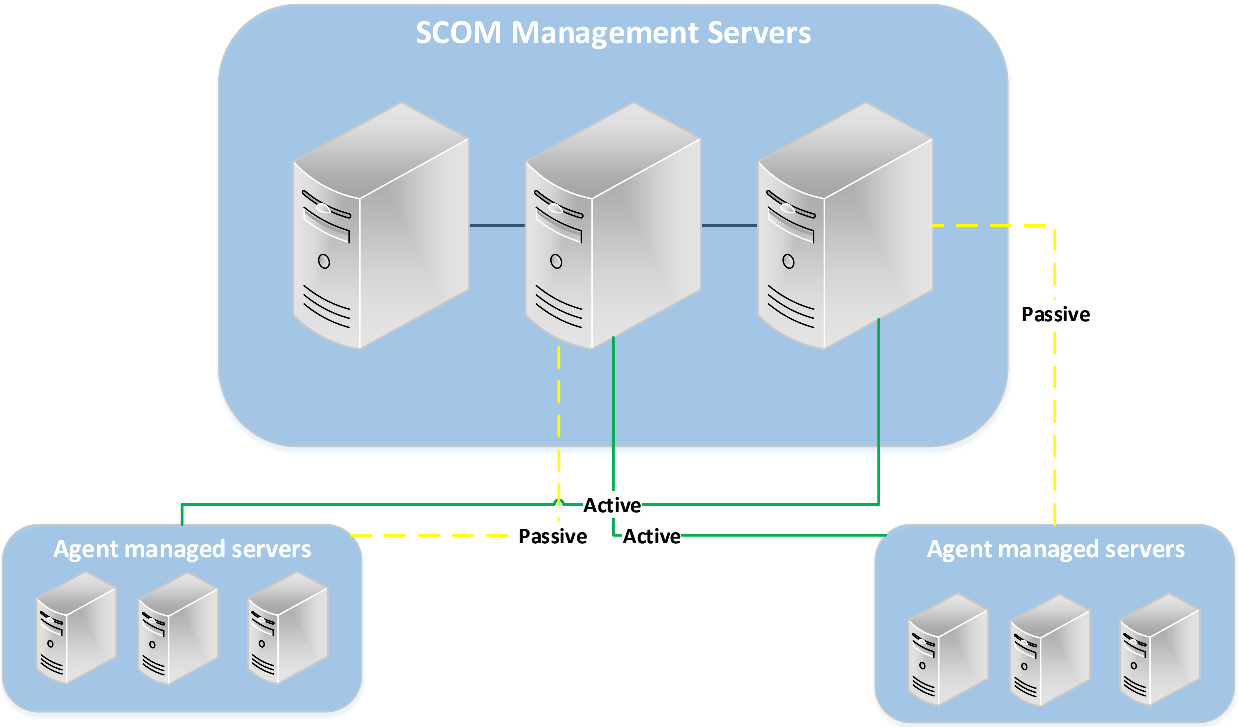


Figure 27 - High Availability design for SCOM Management Servers from the Agent perspective

0255 A similar approach as above was taken in case of SCOM Gateway servers. Each remote domain contains two SCOM Gateway servers for every management group. Gateway number one is reporting to SCOM server number 2 and a gateway number 2 is reporting to SCOM server number 3. At the same time SCOM server number 3 is a secondary server for gateway number one and a SCOM server number 2 is a secondary for the gateway number 2. This configuration ensures monitoring continuity for each remote domain in case of a failure of a single SCOM server. The architecture of the solution is explained on the following diagram.

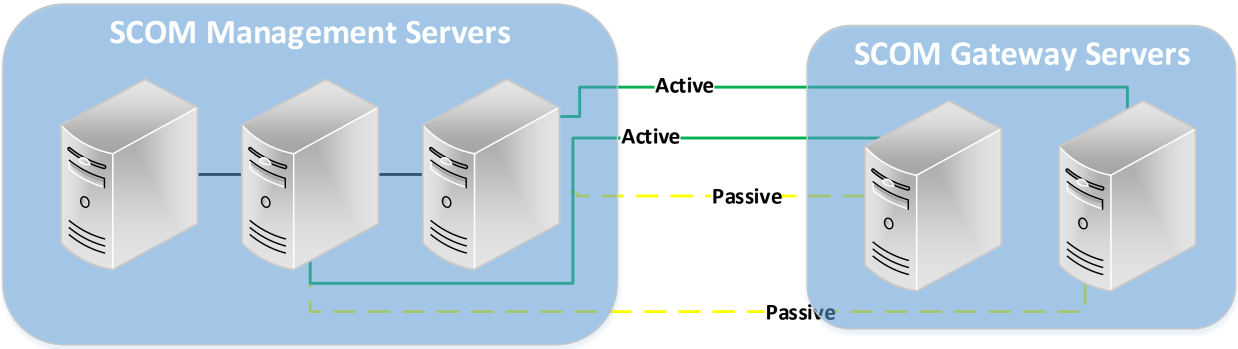


Figure 28 - High Availability design for SCOM Management Servers from the SCOM Gateway servers' perspective

0256 The same approach was taken with regards to the SCOM agents deployed to the servers in the remote domains communicating with SCOM management group from behind the gateway servers. Those SCOM clients' machines will be randomly assigned to one of the two pools. The first pool will use the first SCOM gateway server as its primary management server and the second SCOM gateway server as its secondary management server. The second pool will be configured in an opposite way – it will use the second SCOM gateway server as its primary management server and the first SCOM gateway server as its secondary management server. This configuration ensures, that in case of failure of any of the SCOM gateway servers used for communication with SCOM agents, all the client machines from the pool using this gateway server as a primary one will automatically fail over to the secondary server maintaining continuous communication. The architecture of the solution is explained on the following diagram.

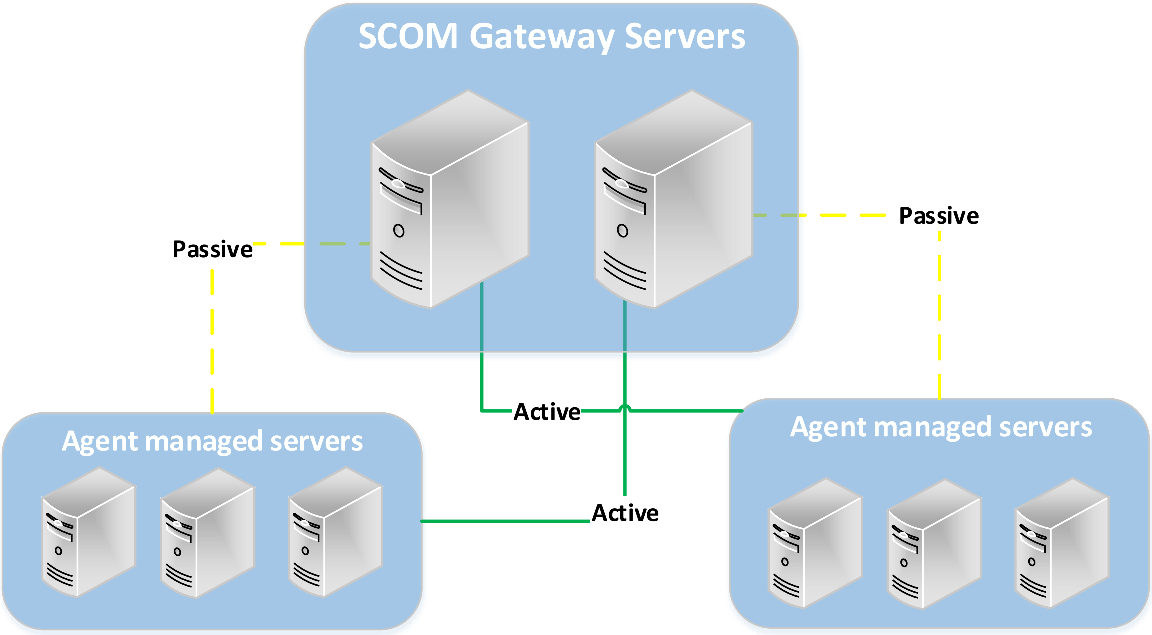


Figure 29 - High Availability design for SCOM Gateway Servers from the agents' perspective

0257 An overall design including all High Availability aspects within one SCOM management group explained above is displayed on the diagram below.

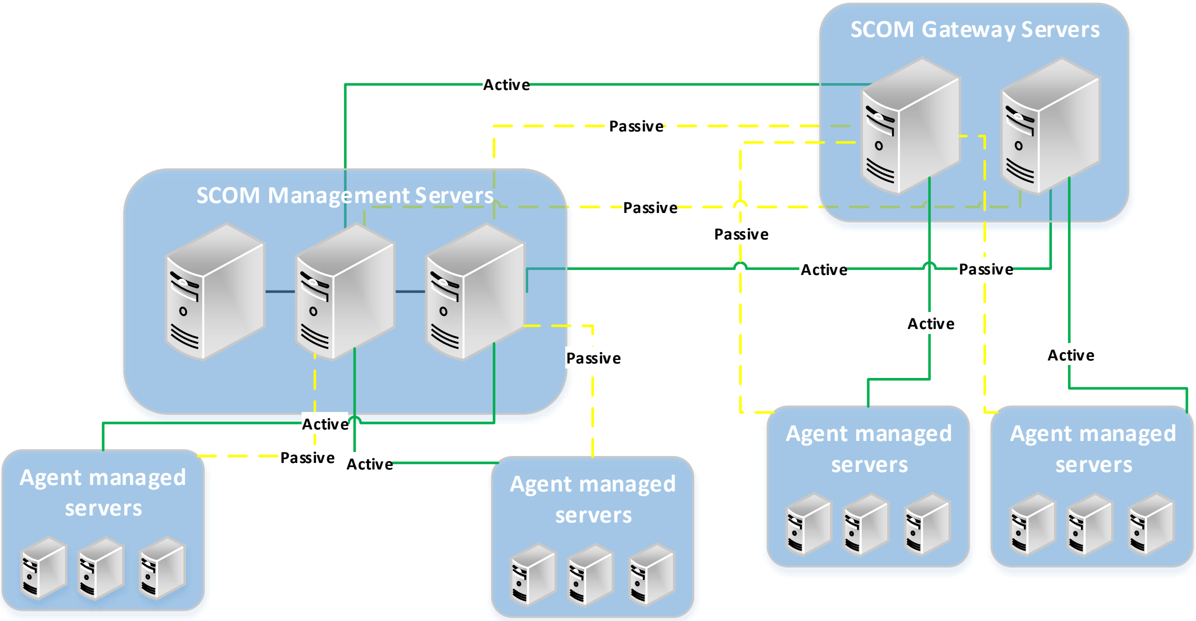


Figure 30 - High Availability design within each SCOM management group

0258 The High Availability is not only provided within one management group. In order to avoid loss of service in case of a catastrophic failure of one of the data centres on top of the previously described High Availability mechanisms, all of the SCOM managed client servers will be multi-homed and reporting simultaneously to two geographically separated SCOM instances – one in ITA-LAG-01 datacenter and another one in BEL-BRU-01 datacenter. Both connections are active at the same time and both SCOM instances collect data and store them in their respective databases. The architecture of the solution is explained on the following diagram.

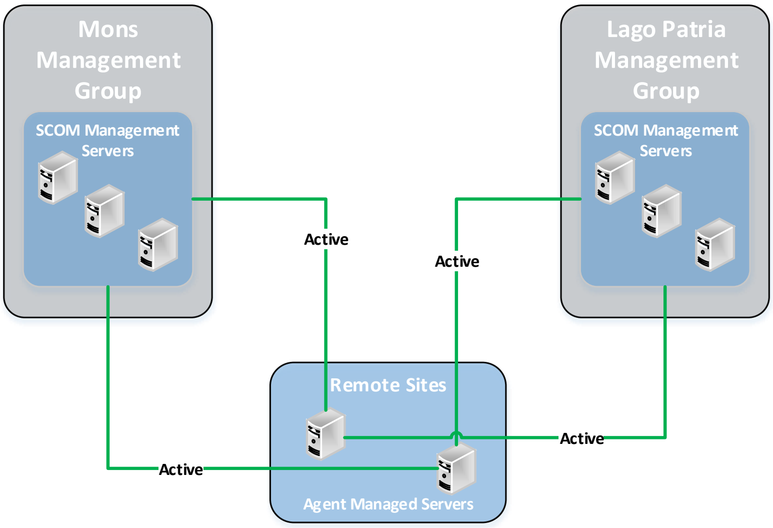


Figure 31 - High Availability design between SCOM management groups

4.7.1.1.8. Ports and Protocols

Comm. Description	Port	Description	Traffic Direction
Communication to SCOM Database	1433	TCP port for database communications	Server to database
Communication to SCOM Database	1434	UDP port for database communications	Server to database
Installation of Server Features	5723/5724	TCP port for feature installation	Management servers
Network Device Management	161/162	TCP port to management network equipment	SCOM server to network device
Gateway Server	5723	Communication from a SCOM gateway server to SCOM server	Gateway server to SCOM server
Web Console	80/443	Web console administration	Client machine to SCOM Server
Agent Push	135/167/138/139/445	TCP ports to push agent	SCOM server to clients

Table 39 - Ports and Protocols

4.7.1.1.9. Capacity Considerations

0259 The following chapter details hardware requirements for fully operational, properly performing SCOM implementation fulfilling high availability requirements provided by the customer. For capacity planning purposes, the estimated number of monitored servers is 1000.

0260 In order to provide full high availability of the solution and cover all external domains the implementation of SCOM will require a number of servers listed in the following table.

Site	Node Type	Enclave	Server Role
BEL-BRU-01	DC	ON (NS)	3 SCOM Management Servers 2 SQL Database Servers 2 SCOM Gateway Servers
ITA-LAG-01	DC	ON (NS)	3 SCOM Management Servers 2 SQL Database Servers 2 SCOM Gateway Servers

Table 40 - SCOM Infrastructure Details

0261 Each of the server types enlisted in the above table in the “Server Role” column will have the same subset of hardware requirements in order to provide performant service and satisfy data retention requirements.

Component	Server Name	Operating System	RAM (GB)	CPU (count)	Storage
SCOM Management Server	TBD	Windows Server latest approved	16GB	4	C:\OS (100GB) P:\Page File (24GB) E:\SCOM (50GB)
SCOM Gateway Server	TBD	Windows Server latest approved	8GB	4	C:\OS (100GB) P:\Page File
SCOM SQL Server	TBD	Windows Server latest approved	64GB	4	C:\OS (100GB) P:\Page File (96GB) E:\OpsDB Data (200GB) F:\OpsDB Log (100GB) G:\DW DB Data (600GB) H:\DW DB Log (100GB)

Table 41 - Details the SCOM Hardware Requirements

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

0262 This section provides detail on CPS service management and tools, including integration points with the enterprise SMC service, as well as management of CPS subservices. CPS integrates with SMC to deliver an integrated and automated interface to the Enterprise SMC CMDB and Asset management solution. SMC solution uses the BMC suite to provide an automated interface between SACM and CMDB.

5.1. Integration with NATO Enterprise SMC services

0263 The integration touch points between SMC enterprise management and the CPS service are detailed below.

SMC Function/ System	Configuration management	Service modelling	Monitoring	Reactive SMC	Proactive SMC	Software approval	Service Report	Training
VMware Horizon	X		X	X	X		X	X
VMware AppVolumes	X		X	X	X	X	X	X
VMware DEM	X			X				
MECM	X			X		X		
SCOM			X	X	X		X	
RDSH	X			X	X	X[1]		
Wyse Management Suite	X			X				
McAfee	X			X	X		X	
End user experience monitoring			X	X	X		X	X
User profile management	X			X				X

Table 42 - integration touch points between SMC and CPS

[1] Only as exception when the application is provisioned in RDSH

0264 Brief description of the SMC functions is as follows:

- Service infrastructure / Configuration management (CMS and discovery solutions)
- Service Modelling (part of service catalogue management focusing on services and supporting infrastructure)
- Monitoring (system and application monitoring)
- Reactive SMC Configuration (mainly request fulfilment, incident, change and service level management)
- Proactive SMC Configuration (mainly event, availability and capacity management)
- SW approval (former AFPL – evaluation of a SW product before approval)
- Monitoring, analysis and report (service quality reporting)
- Training requirements (DoDCP training requirements, training need analysis and training requirements analysis).

5.2. Standard operating instructions and procedures

0265 The implemented CPS services, subservices and systems will be documented in as-built documentation with the implementation details and configuration.

0266 Standard operating instructions and procedures are listed in (Sub) services Interface Control Document (ICD) [Pending updates during detailed design and implementation]

0267 [To be developed during implementation]

0268 Component to ICD mapping table [Pending updates during detailed design and implementation]

0269 [To be developed during implementation]

0270 NATO ON Procedures and Work Instructions and are developed during the implementation to allow the operation of the services, subservices and tools by NCI Agency staff.

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

0271 Content will be developed during project impementation. An initial list of identified Service Operations Procedures is identified in Annex C.

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

0272 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

0273 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 Appendix 4 of this SDP for service specific man-power level and skills (Role).

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

0274 [To be further updated during implementation]

0275 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

0276 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 to facilitate action by decision makers.

0277 Service measurement will gather the data from approved NATO ON/SMC monitoring tools (e.g. SCOM), or from manual data/information gathering methods, and report on progress towards achieving agreed-upon KPIs. 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, or number of website visits or number of logged incidents. In contrast, a metric is defined as a calculation between two measures. The calculation is typically a form of division and the result expressed as a percentage, ratio, fraction, decimal or the like.

0278 The approved NATO SMC toolsets, are used to capture, store and process (threshold monitoring) the service-specific KPI measurement data for use in standardised reports and dashboards in compliance with the NCI Agency’s information quality and classification standards. Access control levels are used to ensure service measurement data and reports are transparent and available across management and functions based on defined roles and responsibilities.

0279 The KPI design solution for service measurement and service reporting includes the below activities and provides 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 which includes 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.
- 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 NATO 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

0280 Measures and metrics for service level defined KPIs will be monitored and collected via three main methods. They are:

- A combination of real-time automated alerts from SMC tools and report generated by enterprise monitoring personnel.
- Manual review of automated alerts via SOPs implemented by system administrators.
- Review of vendor service and equipment maintenance (RMA) activities.

0281 All information related to KPI measurement for availability, capacity and performance will be 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

0282 The following sections outline the measurements for defined KPI availability, capacity and performance of the service sub-services, dependencies and the monitoring/collection toolset.

8.3.1. Desktop

Subservice	KPI	Threshold	Collection Mechanism
Virtual Desktop	Desktops available	99.99%	SCOM
Virtual Desktop	Memory utilisation	80%	SCOM / end user exp. monitoring tool
Virtual Desktop	CPU utilisation	70%	SCOM / end user exp. monitoring tool
Virtual Desktop	Datastore utilisation	70%	SCOM / vROPs
Physical Desktop /thin client	Memory utilisation	80%	End user exp. monitoring tool
Physical Desktop /thin client	CPU utilisation	70%	End user exp. monitoring tool
Physical Desktop/laptop/thin client	Datastore utilisation	70%	End user exp. monitoring tool
Deployment of physical desktop	Time to execute	90 minutes	MECM
Deployment of thin client	Time to execute	120 minutes	Dell Wyse Management Suite
Deployment of VDI desktop (master image)	Time to execute	90 minutes	MECM
Logon to a VDI desktop	Time	2 minutes	VMware Horizon/SCOM/End-user monitoring tool
Logon to a physical desktop	Time	2 minutes	End-user monitoring tool
Number of clients supported on VDI	Maximum number	The number of VDI users at the site + 20%	VMware Horizon

Table 43 - Desktop

8.3.2. Applications

Subservice	KPI	Threshold	Collection Mechanism
MECM	Applications available	99.99%	SCOM
VMware AppVolumes	Applications available	99.99%	SCOM / VMware Horizon/AppVolumes
RDSH	Applications available	99.99%	SCOM
Applications Servers	CPU utilisation	70%	SCOM
Applications Servers	Memory utilisation	80%	SCOM
Deployment of an application on physical desktop	Time to execute	10 minutes	MECM
Deployment of an application on physical desktop	Time to execute	1 minute	VMware AppVolumes / End-user monitoring tool

Table 44 - Applications

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

[To be developed during implementation]

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

[To be developed during implementation]

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

Software	SOP Description	Actor	Frequency	Tool	SOP Ref
VMware Horizon	Create Pools	Desktop Admin	As Needed	View Admin Console	NATO ON-SOCPSOM-001
VMware Horizon	Deploy Desktops	Desktop Admin	As Needed	View Admin Console	NATO ON-SOCPSOM-002
VMware Horizon	Assign Users to Pool	Desktop Admin	As Needed	View Admin Console	NATO ON-SOCPSOM-003
VMware Horizon	Deploy Connection Server	Desktop Admin	As Needed	View Admin Console	NATO ON-SOCPSOM-004
VMware Horizon	Update Desktop Image	Desktop Admin	As Needed	View Admin Console	NATO ON-SOCPSOM-005
User profile management	Setting up Profile Information	Desktop Admin	As Needed	Admin Console	NATO ON-SOCPSOM-006
MECM	Create Software Install Packages	Application Admin	As Needed	MECM Admin Console	NATO ON-SOCPSOM-007
MECM	Assign Applications to Users	Application Admin	As Needed	MECM Admin Console	NATO ON-SOCPSOM-008
RDSH	Install Application	Application Admin	As Needed	RDSH Server	NATO ON-SOCPSOM-009
RDSH	Assign Application	Application Admin	As Needed	RDSH Server	NATO ON-SOCPSOM-010
Dell Thin Client	Image End Point	Desktop Admin	As Needed	Dell Wyse	NATO ON-SOCPSOM-011
Dell Thick Client	Image End Point	Desktop Admin	As Needed	MECM	NATO ON-SOCPSOM-012
End user experience monitoring tool	Monitor End Point Experience	Desktop Admin	As Needed	Admin Console	NATO ON-SOCPSOM-013
McAfee	Deploy products	ePO Admin	As Needed	ePO Admin Console	NATO ON-SOCPSOM-014
McAfee	Evaluate Intrusion Logs	ePO Admin	As Needed	ePO Admin Console	NATO ON-SOCPSOM-015

Table 45 - NATO ON Procedures and Work Instructions

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

0283 [To be defined/updated as part of design and implementation]

Role	FTE	Education	Experience	Certifications

Table 46 - Specific Roles and Responsibilities

Annex E VIRTUAL DESKTOP DESIGN [PENDING UPDATES DURING DETAILED DESIGN AND IMPLEMENTATION]

E.1. Purpose and Scope

0284 The purpose of this appendix is to detail the Design Solution of VMware Horizon 8 environment will be used as a baseline for other deployments.

0285 The Horizon environment is designed to scale using the standard Pod and block methodology, which allows NATO ON to use a repeatable and scalable approach when deploying new Horizon environments in all other data centres.

E.2. Service Design and Topology

0286 In this section, we go through the logical design of each component included in this design.

E.2.1. NATO ON Site Overview

0287 NATO ON datacentre and enhanced nodes facilities centralize the organizations shared IT operations and equipment to store, process, and disseminate data and applications. The complete datacentre and Site overview are shown in the following figure.

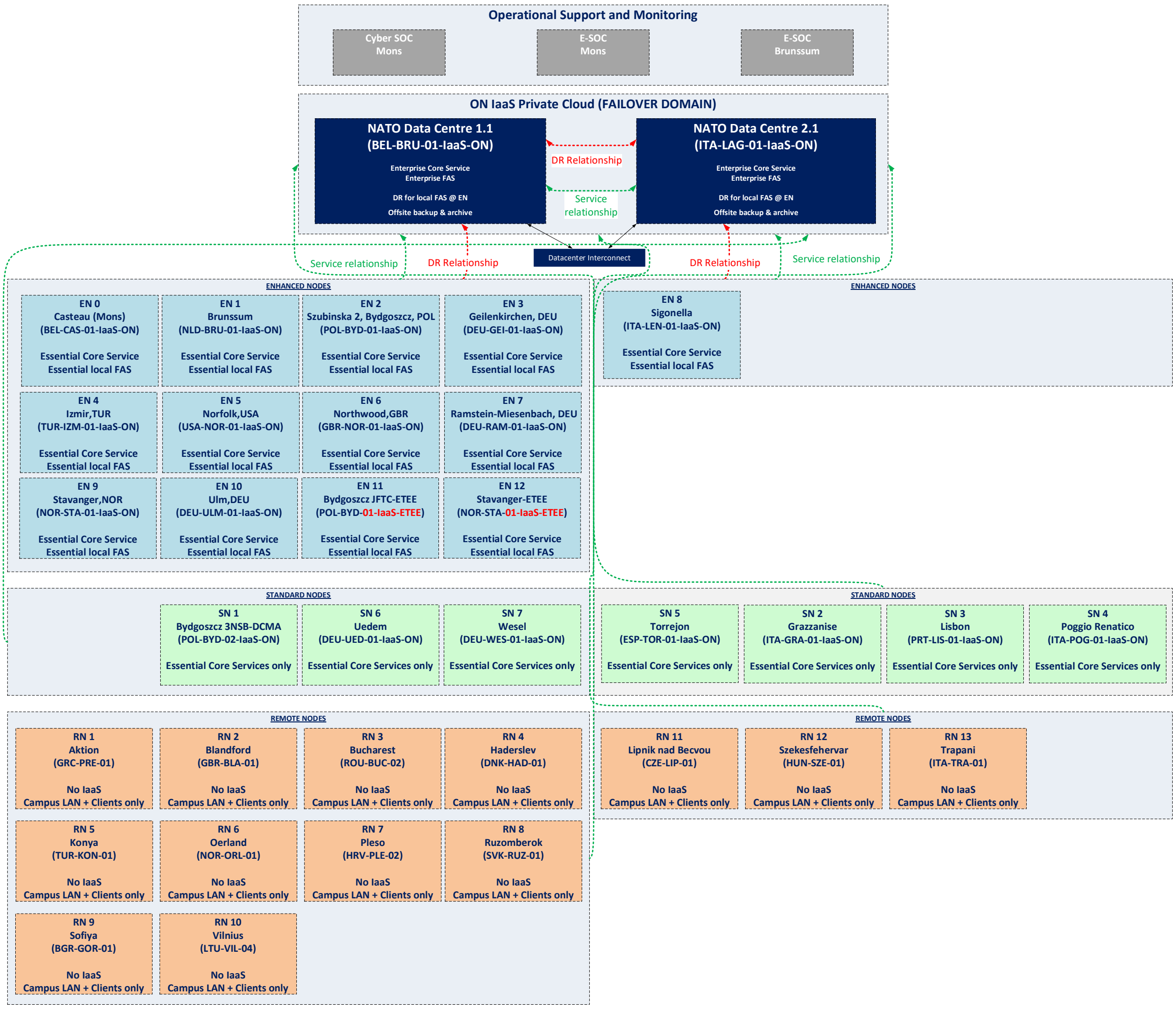

Operational Support and Monitoring
Cyber SOC Mons
E-SOC Mons
E-SOC Brunssum
ON IaaS Private Cloud (FAILOVER DOMAIN)
NATO Data Centre 1.1 (BEL-BRU-01-IaaS-ON)
Enterprise Core Service
Enterprise FAS
DR for local FAS @ EN
Offsite backup & archive
DR Relationship
Service relationship
NATO Data Centre 2.1 (ITA-LAG-01-IaaS-ON)
Enterprise Core Service
Enterprise FAS
DR for local FAS @ EN
Offsite backup & archive
Service relationship
DR Relationship
Datacenter Interconnect
DR Relationship
Service relationship
ENHANCED NODES
EN 0 Casteau (Mons) (BEL-CAS-01-IaaS-ON) Essential Core Service Essential local FAS
EN 1 Brunssum (NLD-BRU-01-IaaS-ON) Essential Core Service Essential local FAS
EN 2 Szubinska 2, Bydgoszcz, POL (POL-BYD-01-IaaS-ON) Essential Core Service Essential local FAS
EN 3 Geilenkirchen, DEU (DEU-GEI-01-IaaS-ON) Essential Core Service Essential local FAS
EN 4 Izmir,TUR (TUR-IZM-01-IaaS-ON) Essential Core Service Essential local FAS
EN 5 Norfolk,USA (USA-NOR-01-IaaS-ON) Essential Core Service Essential local FAS
EN 6 Northwood,GBR (GBR-NOR-01-IaaS-ON) Essential Core Service Essential local FAS
EN 7 Ramstein-Miesenbach, DEU (DEU-RAM-01-IaaS-ON) Essential Core Service Essential local FAS
EN 9 Stavanger,NOR (NOR-STA-01-IaaS-ON) Essential Core Service Essential local FAS
EN 10 Ulm,DEU (DEU-ULM-01-IaaS-ON) Essential Core Service Essential local FAS
EN 11 Bydgoszcz JFTC-ETEE (POL-BYD-01-IaaS-ETEE) Essential Core Service Essential local FAS
EN 12 Stavanger-ETEE (NOR-STA-01-IaaS-ETEE) Essential Core Service Essential local FAS
ENHANCED NODES
EN 8 Sigonella (ITA-LEN-01-IaaS-ON) Essential Core Service Essential local FAS
STANDARD NODES
SN 1 Bydgoszcz 3NSB-DCMA (POL-BYD-02-IaaS-ON) Essential Core Services only
SN 6 Uedem (DEU-UED-01-IaaS-ON) Essential Core Services only
SN 7 Wesel (DEU-WES-01-IaaS-ON) Essential Core Services only
STANDARD NODES
SN 5 Torrejon (ESP-TOR-01-IaaS-ON) Essential Core Services only
SN 2 Grazzanise (ITA-GRA-01-IaaS-ON) Essential Core Services only
SN 3 Lisbon (PRT-LIS-01-IaaS-ON) Essential Core Services only
SN 4 Poggio Renatico (ITA-POG-01-IaaS-ON) Essential Core Services only
REMOTE NODES
RN 1 Aktion (GRC-PRE-01) No IaaS Campus LAN + Clients only
RN 2 Blandford (GBR-BLA-01) No IaaS Campus LAN + Clients only
RN 3 Bucharest (ROU-BUC-02) No IaaS Campus LAN + Clients only
RN 4 Haderslev (DNK-HAD-01) No IaaS Campus LAN + Clients only
RN 5 Konya (TUR-KON-01) No IaaS Campus LAN + Clients only
RN 6 Oerland (NOR-ORL-01) No IaaS Campus LAN + Clients only
RN 7 Pleso (HRV-PLE-02) No IaaS Campus LAN + Clients only
RN 8 Ruzomberok (SVK-RUZ-01) No IaaS Campus LAN + Clients only
RN 9 Sofiya (BGR-GOR-01) No IaaS Campus LAN + Clients only
RN 10 Vilnius (LTU-VIL-04) No IaaS Campus LAN + Clients only
REMOTE NODES
RN 11 Lipnik nad Becvou (CZE-LIP-01) No IaaS Campus LAN + Clients only
RN 12 Szekesfehervar (HUN-SZE-01) No IaaS Campus LAN + Clients only
RN 13 Trapani (ITA-TRA-01) No IaaS Campus LAN + Clients only

Figure 32 - NATO ON Site overview

0288 The datacentres are categorized into different “Subscriber Sites”:

- Standard Node (SN) site: local enabling infrastructure supporting local client IT access and user access to applications and core services in the Datacentre. An SN serves the typical requirements of users at a location served by the IaaS.
- Enhanced Node (EN) site: providing the same client IT support as standard nodes but with a local infrastructure to support critical local data and application services. An EN is a step up from the SN with edge computing infrastructure serving local users with critical services.
- Remote Nodes (RN) site: remote client access to the datacentres, no local infrastructure. A RN is a cost-effective simplified Access Node that only locally hosts the minimum to “power” User Equipment accessing all services from the DC.

E.2.2. Horizon On-Premises Solution

0289 VMware Horizon 8 is a platform for managing and delivering virtualized or hosted desktops and applications to end-users. A VMware Horizon installation within a single site is referred to as a “Pod”.

0290 This design will provide NATO ON with a standard approach to construct and support a Horizon environment in multiple Horizon Pods and multiple sites. Based on the site size, this standardized and modular approach will allow NATO ON to use a flexible scalable architecture design.

0291 The following table depicts the number of VDI users to be supported by the initial Horizon Pod deployment:

Site	Site ID	# of VDI users
SHAPE	BEL-CAS-01	300
JFC HQ Naples	ITA-LAG-01	1242
JFC HQ Norfolk	USA-NOR-01	144
HQ AIRCOM	DEU-RAM-01	201
SJLSG HQ Ulm	DEU-ULM-01	112
ACT JWC Stavanger	NOR-STA-01	2300
ACT JFTC Bydgoszcz	POL-BYD-01	1300

Table 47 - Horizon POD requirements

E.2.3. Horizon Core components overview.

0292 VMware Horizon consists of several core components. Core components for NATO ON will include:

- **Horizon Connection Servers** - acts as a broker for client connections. Horizon Connection Server authenticates users through Windows Active Directory and directs the request to the appropriate virtual machine, physical PC, or Microsoft RDS host.
- **Horizon Client** – Used to connect to a remote desktop or published application from your desktop or mobile device.
- **Horizon Agent** - On virtual machines, the agent communicates with Horizon Client to provide features such as connection monitoring, virtual printing, Horizon Persona Management, and access to locally connected USB devices
- **Unified Access Gateway -** Provides secure accesses to Horizon virtual desktops and applications. Multi-factor user authentication for Horizon is enhanced with built-in support for user identity federation with SAML identity providers. Fine-grained access controls for authorized protocol access to desktop and application resources are enforced automatically.

- ○ **Dynamic Environment Manager** - VMware Dynamic Environment Manager (formerly known as VMware User Environment Manager) allows personalization and dynamic policy configuration across any virtual, physical, and cloud-based environment. VMware Dynamic Environment Manager will simplify end-user profile management with a single and scalable solution.
- ○ **App Volume Management Servers** - VMware App Volumes is a portfolio of applications and user management solutions for Horizon.

E.2.4. Deployment Options

0293 One key concept in a Horizon environment design is the use of pods and blocks, which gives us a repeatable and scalable approach.

0294 A pod is made up of a group of interconnected Connection Servers that broker connections to desktops or published applications.

- A pod can broker up to 20,000 sessions (12,000 recommended), including desktop and RDSH sessions.
- Multiple pods can be interconnected by either using the Universal Broker or by using Cloud Pod Architecture (CPA).
- A single Cloud Pod Architecture can scale to a maximum of 250,000 sessions. For numbers above that, separate CPAs can be deployed.

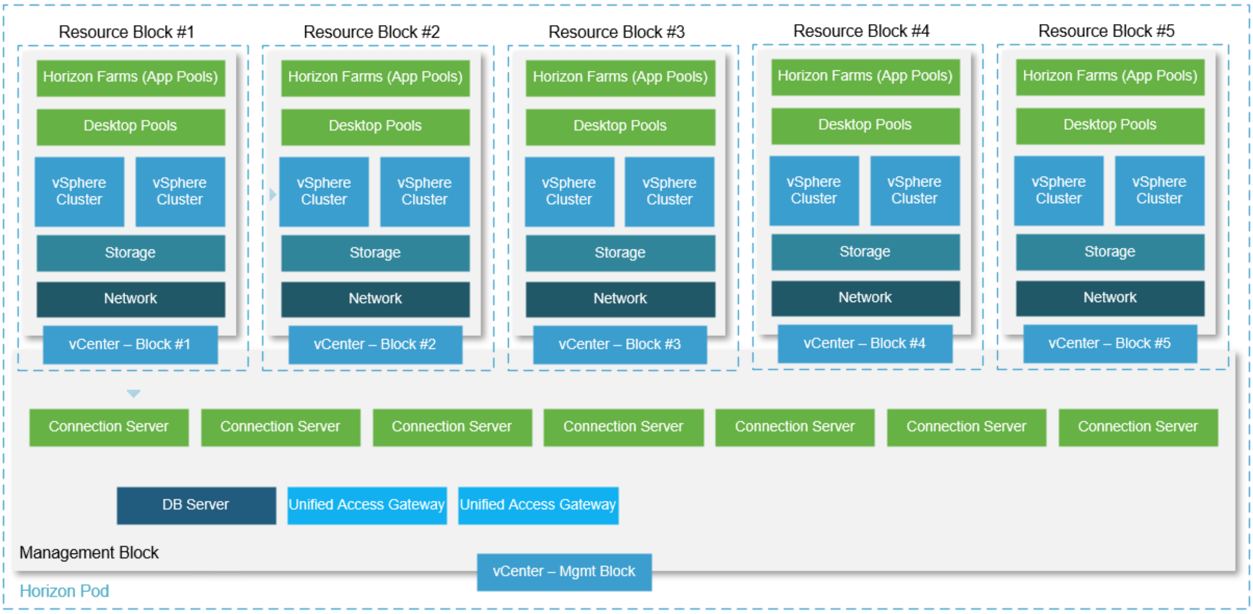


Figure 33 - Horizon Pod and Block Overview

0295 The POD and Block Architecture will be implemented.

E.2.5. Cloud Pod Architecture

0296 Cloud Pod Architecture will be implemented which introduces the concept of a global entitlement (GE) through joining multiple Horizon pods together into a federation. Pods can be located in the same physical site or location or at different sites and locations. CPA can also serve as the basis for management between on-premises datacentres and various public clouds.

0297 CPA will allow NATO ON users to use so-called Global Entitlements that can contain desktop pools from multiple different pods that are members of this federation construct.

0298 The following figure shows a logical overview of a basic two-site CPA implementation.

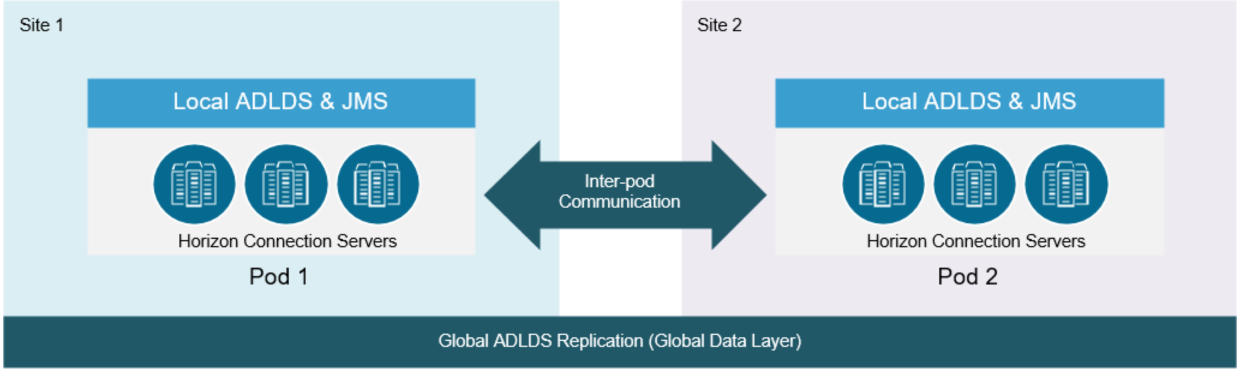

Site 1
Local ADLDS & JMS
Horizon Connection Servers
Pod 1
Inter-pod Communication
Site 2
Local ADLDS & JMS
Horizon Connection Servers
Pod 2
Global ADLDS Replication (Global Data Layer)

Figure 34 - Cloud Pod Architecture

0299 For the full documentation on how to set up and configure CPA, refer to Setting Up Cloud Pod Architecture in Horizon Console**.**

0300 **Important** This type of deployment is not a stretched deployment. Each pod is distinct, and all Connection Servers belong to a specific pod and are required to reside in a single location and run on the same broadcast domain from a network perspective.

0301 As well as being able to have desktop pool members or published applications from different pods in a global entitlement, this architecture allows for a property called scope. The scope allows us to define where new sessions should or could be placed and also allows users to connect to existing sessions (that are in a disconnected state) when connecting to any of the pod members in the federation.

E.2.5.1. Global Entitlements

0302 Global Entitlements contain one or more Local Pools from one or more pods. Connections to the Global Entitlement can be load balanced across the member pods and pools.

Home Sites

0303 A home site is a relationship between a user or group and a Cloud Pod Architecture site. With home sites, VMware Horizon begins searching for desktops and applications from a specific site rather than searching for desktops and applications based on the user's current location. Assigning home sites is optional.

0304 If the home site is unavailable or does not have resources to satisfy the user's request, Horizon continues searching other sites according to the scope policy set for the global entitlement.

0305 For global desktop entitlements that contain dedicated pools, the home site affects where Horizon looks for desktops the first time a user requests a dedicated desktop. After Horizon allocates a dedicated desktop, it returns the user directly to the same desktop.

0306 The Cloud Pod Architecture feature includes the following types of home site assignments.

- **Global home site.**
  - A home site that is assigned to a user or group.
  - If a user who has a home site belongs to a group that is associated with a different home site, the home site associated with the user takes precedence over the group home site assignment.
  - Global homes sites are useful for controlling where roaming users receive desktops and applications.
- **Per-global-entitlement home site (home site override)**
  - A home site that is associated with a global entitlement.

- Per-global-entitlement home sites override global home site assignments. For this reason, per-global-entitlement home sites are also referred to as home site overrides.
- **Note:** Configuring home sites is optional. If a user does not have a home site, Horizon searches for and allocates desktops and applications.

E.3. Service Solution – Implementation details

E.3.1. Horizon Connection Server

0307 Horizon Connection Servers is a service that runs on Windows Server 2016/19. It provides user authentication and directs incoming remote desktop requests to the appropriate Horizon Desktop or RDSH Server.

0308 Connection servers within the same pod are replicas of each other and can be used for scaling and load balancing purposes. Connection servers in the same pod share a single ADAM (Active Directory for Application Mode) database.

0309 For sizing and capacity purposes the single Horizon Connection Server maximum number Blast Extreme sessions (TCP) of 2,000 is used.

0310 The proposed solution is highly available and can handle failure when there are n+1 connection servers deployed.

0311 The diagram below shows the high-level logical architecture of these core elements.

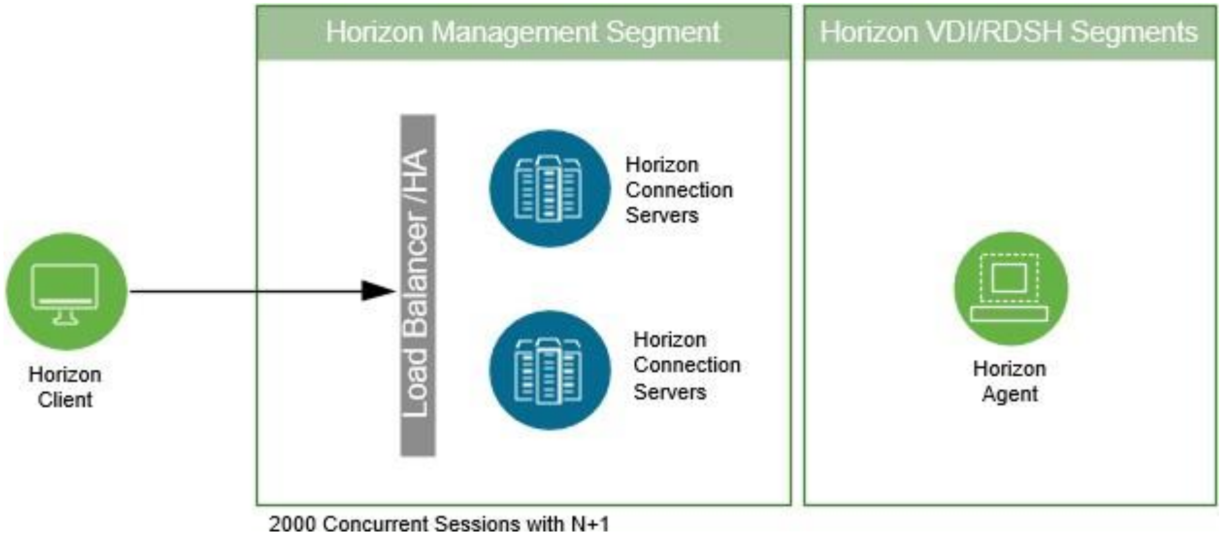

Horizon Management Segment
Horizon VDI/RDSH Segments
Load Balancer /HA
Horizon Connection Servers
Horizon Connection Servers
Horizon Client
Horizon Agent
2000 Concurrent Sessions with N+1

Figure 35 - Horizon Connection Servers Logical Architecture

E.3.2. Horizon Connection Server Availability

0312 If a Horizon Connection Server fails or becomes non-responsive while an active, established, and tunneled session exists, the desktop or application state is preserved in the virtual desktop instance. When the user reconnects to a different connection server in the group, the desktop or application session continues where it left off when the failure occurred.

0313 Direct Connect connections will be configured, as a result, users are unaffected by any Horizon Connection Server disruption because their session is established directly with the Horizon desktop. If the connection between the client device and the virtual desktop is broken, the desktop state is also preserved, and the session continues when the client reconnects unless the broken connection was caused by RDS Server failure.

0314 vSphere HA and DRS will be used to ensure the maximum availability of the Horizon Connection servers. DRS rules will be configured to ensure that the devices do not reside on the same host; this will enhance High Availability.

E.3.3. Horizon Connection User Authentication Method

0315 VMware Horizon uses NATO ON Directory (Active Directory) infrastructure for user authentication and management.

0316 The solution will support both Active Directory username and password and smartcard authentication. Smartcard authentication is dependent on the the availability of PKI service and roll out of smartcards to the end users.

0317 The following table outlines the authentication options to be configured in this deployment.

E.3.4. Horizon Connection Servers Specifications

0318 The Connection Servers will be deployed as per vendor recommended specifications quantity and sites taking into account the high availability discussed above.

E.3.5. Horizon Global Settings

0319 All pods will have the same global settings. Exact settings to be developed during implementation.

E.3.6. Horizon Global Policies

All pools will be governed by a global policy. Exact settings to be developed during implementation.

E.3.7. Unified Access Gateway

0320 Unified Access Gateway is a component in Horizon deployments. It enables remote access to internally hosted Horizon desktops and applications from another site.

0321 The following application limitations are considered when deciding the total number of servers and their placement::

- PCoIP Sessions - 2,000
- Blast Extreme Sessions - 2,000
- Fault-tolerant - (n+1) UAG instances.

0322 The diagram below describes the high-level logical architecture using Unified Access Gateway.

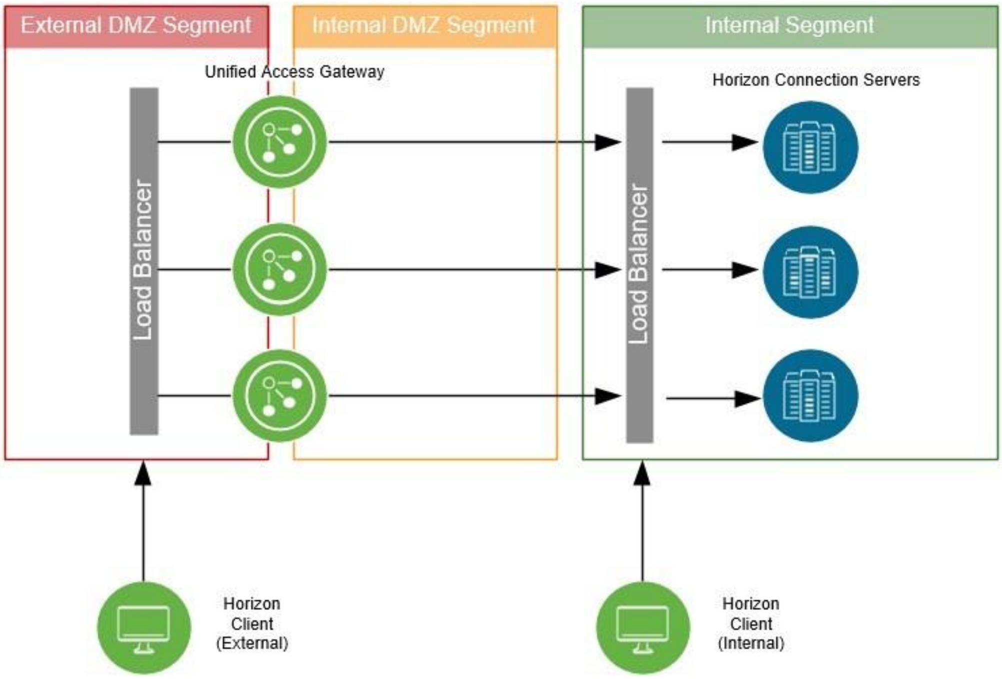


Figure 36 - Load Balancing when all Connections Originate Externally

E.4. User Profile Management

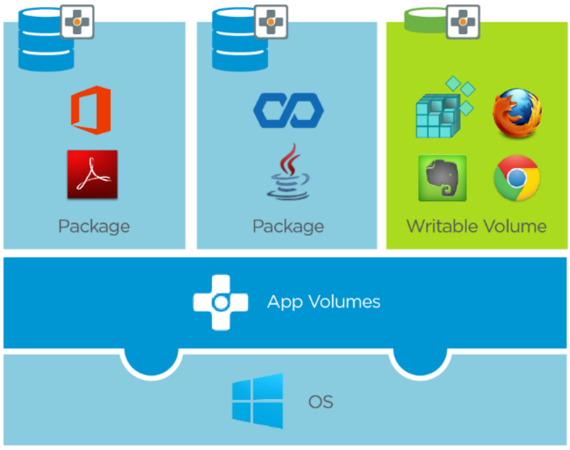
0323 VMware Dynamic Environment Manager application is used to providet he User Profile Management. Exact settings to be developed during implementation.

E.5. VMware App Volumes

E.5.1. Introduction

0324 The VMware App Volumes™ just-in-time application model separates IT-managed applications and application suites into administrator-defined application containers. App Volumes also introduces an entirely different container used for persisting user changes between sessions.

Figure 37 - App Volumes Just-in-Time Application Model



0325 App Volumes serves two functions. The first is delivery of software programs that are not in the golden image VM image for VDI and RDSH. App Volumes groups one or more *programs* into *packages*, based on the requirements of each use case. A package is a virtual disk containing one or more programs that are captured together.

0326 The packages are added to *applications*. Applications are used to assign packages to Active Directory (AD) entities such as user, group, organizational unit (OU), or machine. The packages can be mounted each time the user logs in to a desktop, or at machine startup. For VDI use cases, packages can be mounted at login.

E.5.2. App Volumes - Solution Overview

0327 This App Volumes Architecture design follows closely the Virtual Desktop subservice in order to enable just-in-time application provisioning for the Horizon Virtual Desktops.

0328 This design will provide NATO ON with a standard approach to construct and support the App Volumes with Horizon across multiple sites environments. This standardized and modular approach will enalbe NATO ON flexible and scalable architecture design.

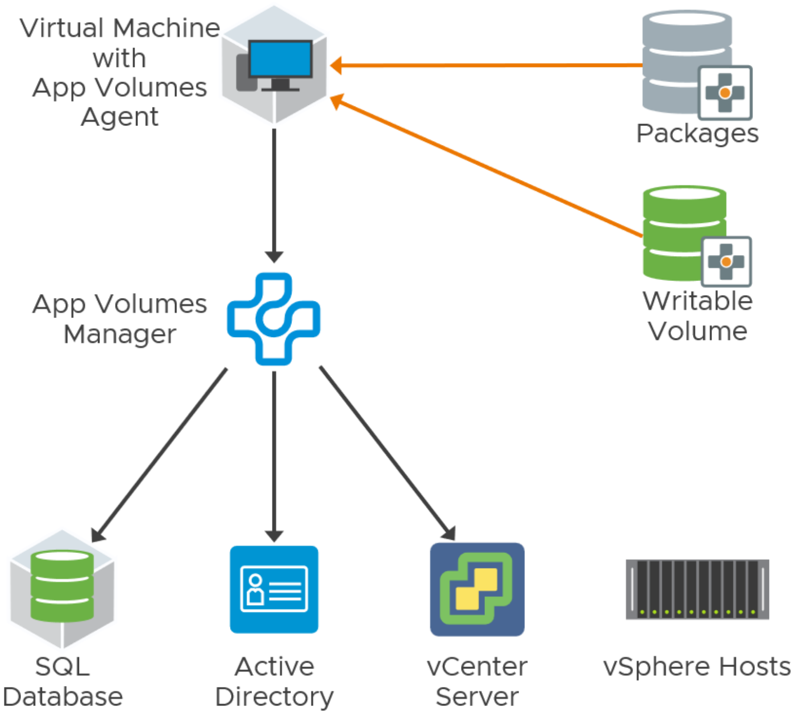
0329 App Volumes Managers will be located on a VMware vSphere Management block along with other management services. A dedicated vSphere Horizon resource block will be used to host the VDI machines along with App Volumes Packages.

0330 App Volumes Managers will be configured with an external SQL database that will be highly available to minimize downtime of the App Volumes Managers, likewise there will be a minimum of two App Volumes servers per site to support high availability requirements.

E.5.3. Architecture Overview

0331 The App Volumes Agent is installed in the guest operating system of nonpersistent VMs. The agent communicates with the App Volumes Manager instances to determine package and Writable Volumes entitlements. Packages and Writable Volumes virtual disks are attached to the guest operating system in the VM, making applications and personalized settings available to end users.

Figure 38 - App Volumes Logical Components



0332 The components and features of App Volumes are described in the following table:

Table 48 App Volumes Components and Concepts

Component	Description
App Volumes Manager	Console for management of App Volumes, including configuration, creation of applications and packages, and assignment of packages and Writable Volumes Broker for App Volumes Agent for the assignment of packages and Writable Volumes
App Volumes Agent	Runs on virtual desktops or RDSH servers File system and registry abstraction layer running on the target system Virtualizes file system writes as appropriate (when used with an optional Writable Volume)
Application	Logical component containing one or more packages Used to assign AD entities to packages Supports marker and package assignment types
Package	Read-only volume containing applications Virtual disk file that attaches to deliver apps to VDI or RDSH One or more packages may be assigned per user or machine
Program	Represents a piece of software captured in a package One or more programs may be captured in a package
Marker	Attribute of an application used to designate the current package Simplifies application lifecycle management tasks
Writable volume	Read-write volume that persists changes written in the session, including user-installed applications and user profile One Writable Volume per user Only available with user or group assignments User Writable Volumes are not applicable to RDSH
Database	Microsoft SQL database that contains configuration information for applications, packages, Writable Volumes, and user entitlements Should be highly available
Active Directory	Environment used to assign and entitle users to packages and Writable Volumes
VMware vCenter Server®	App Volumes uses vCenter Server to connect to resources within the VMware vSphere® environment Manages vSphere hosts for attaching and detaching packages and Writable Volumes to target VMs
Packaging VMs	Clean Windows VM with App Volumes Agent Used to capture software programs to packages for distribution
Storage group (not shown)	Group of datastores used to replicate packages and distribute Writable Volumes

0333 The following figure shows the high-level logical architecture of the App Volumes components, scaled out with multiple App Volumes Manager servers using a third-party load balancer:

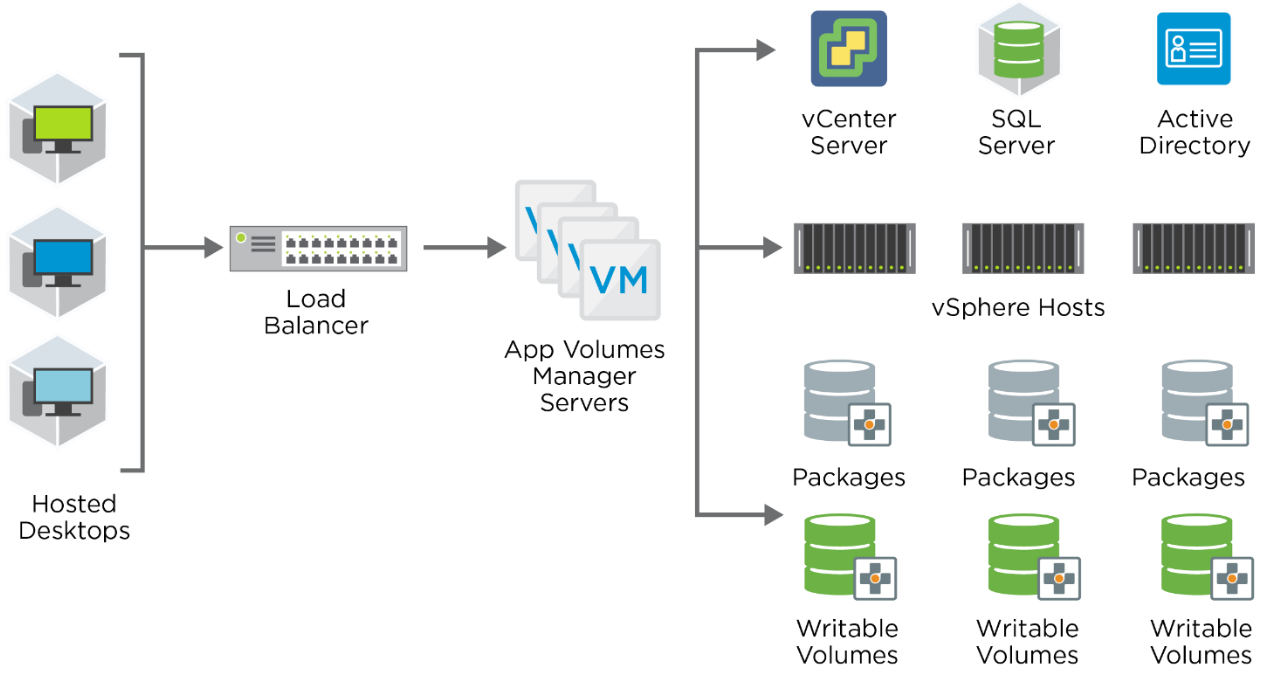


Figure 39 - App Volumes Logical Architecture

E.5.4. Architecture Design

0334 Separate App Volumes instances will be used in each site and Multi- Instance Management will be configured to control the App Volumes managers as a single source instance.

0335 App Volumes Manager requires a reliable and constant connection to the SQL database. Therefore, any delays or loss of communication between App Volumes Manager and its SQL database will cause performance and stability issues.

0336 App Volumes deployment will follow the Virtual Desktop pod design and will use a local SQL Server instance.

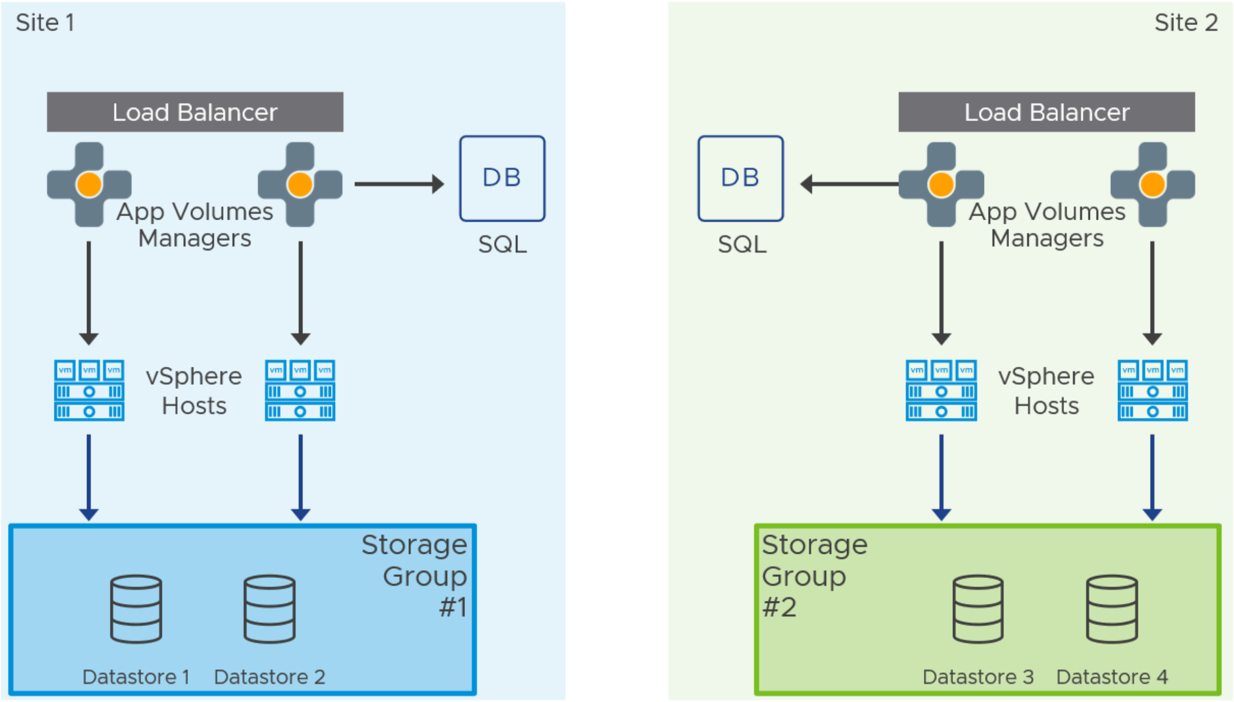


Figure 40 - App Volumes Multi-instance model

0337 This strategy makes use of the following components:

- App Volumes Managers – At least two App Volumes Manager servers are used in each site to form an instance, for local redundancy and scalability.
- Load balancers – Each site has its own namespace for the local App Volumes Manager servers. This is generally a local load balancer virtual IP that targets the individual managers.
  Note: The App Volumes Agent, which is installed in virtual desktops, must be configured to use the appropriate local namespace.
- Separate databases – A separate database is used for each instance; each site should have separate SQL servers. A separate SQL Server Always On availability group listener for each site will be used, to achieve automatic failover within a site.
- vCenter Server machine managers – The App Volumes Manager instance and servers at each site have machine managers registered only for the vCenter Servers from their own site.

E.5.4.1. Replication of Packages

0338 Storage groups containing a shared, non-attachable datastore can be used to automatically replicate packages from one instance of App Volumes to another. This shared datastore must be visible to at least one vSphere host from each App Volumes instance. Storage groups will be used to replicate packages between datastores.

0339 An NFS datastore will be used as a common datastore between the different vSphere clusters.

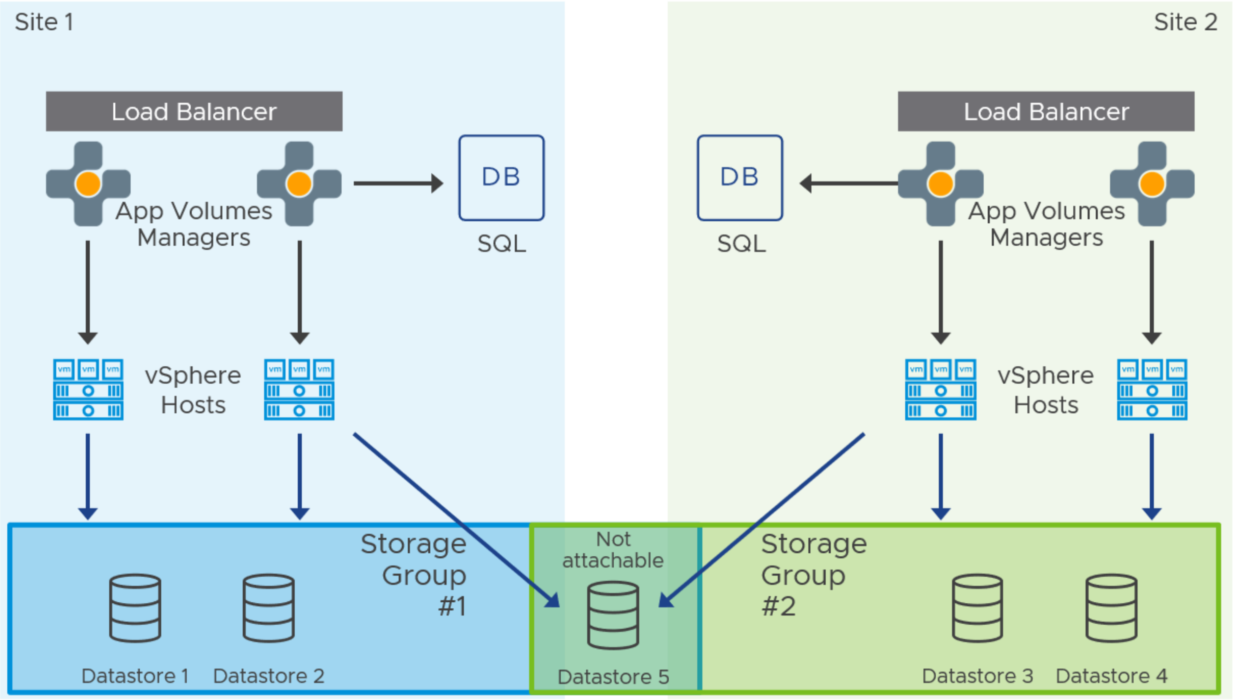


Figure 41 - Replicating VMDK Packages between Instances with a Shared Datastore

E.5.4.2. Multi-instance Management

0340 A multi-instance deployment of App Volumes will be configured which provides the capability to:

- Use one App Volumes instance as the source for replicated packages
- Synchronize application and package metadata across all connected App Volumes instances
- Synchronize application and package deletes
- Synchronize application markers across instances (optional)
- Synchronize assignments across instances (optional)
- Assisted replication and import remove the need for Import Background Job

Component	Description
App Volumes Manager Instance	An App Volumes install bound by an SQL database Multiple App Volumes Manager servers can access a single SQL database
Source Instance	App Volumes instance that synchronizes replicated applications and packages to other App Volumes instances
Target Instance	App Volumes instance with replicated applications and packages that are synchronized by another (source) App Volumes instance
Related Instance	A target instance or a source instance with reference to a current App Volumes Manager instance
Replication	An App Volumes feature which enables the copying of applications and packages (.vmdk and .vhd) between storage locations
Synchronization	An App Volumes feature which ensures information about the replicated applications and packages remain the same across App Volumes Manager instances

Table 49 - Multi-Instance Components

E.6. Security View

E.6.1. Background

0341 A comprehensive solution supporting virtual desktop resources is dependent on multiple layers of security at the Horizon platform layer, anti-virus, network and firewalls, certificates and role-based access control. This section covers these topics and the design decisions around each.

E.6.2. Security Settings

0342 All components such as Horizon Connection Servers, Load Balancing and vCenter servers will be secure using the following standards.

Standard	Choice
Secure Certificates (SSL), TLS and Ciphers	vCenter and ESXi will use NATO CA-generated SSL certificates.
	Connection Servers, UAGs, App Volumes Managers and Load Balancers will use NATO CA-generated SSL certificates.
	All Horizon and App Volumes components will use TLS 1.2 and NATO's custom Cipher settings to meet NATO's security requirements.

Windows Host Patching	All Windows-based servers will be updated and patched using Microsoft MECM in accordance with NATO's existing operational process.
	The Horizon VDI Golden Images will be updated and monthly patched using Microsoft MECM in accordance with NATO's existing operational process.
Non-Windows Host Patching	These servers will use NATO's existing methods of updating by getting updates directly from a trusted source and applied in accordance with NATO's existing operational process.
Firewall	All Windows-based servers and Windows-based virtual desktops will use Windows Firewall. Rules will be controlled with Group Policies through Active Directory.
	NATO will leverage its internal Boundary Protected Service (BPS) to further restrict network communication between infrastructure components.
Cyber Security subservice agents integrated into VMs	All Windows-based servers and virtual desktops will have endpoint cyber security agents as per the Cyber Security subservice design.
Domain Computer Security Policies	All Window-based servers and virtual desktops will follow NATO security hardening security policies applied by Group Policy.
Virtual Machine Hardening	All Window-based servers and virtual desktops will have NATO's security hardening settings applied.
Role Based Access Control (RBAC)	Access to vCenter will be locked down via strict use of users\group RBAC with the least privilege applied.
	Access to Connection Servers and App Volumes Managers will be locked down via strict use of users\group RBAC.
Two-Factor Authentication	Smart Card authentication will be used. All Endpoints will be equipped with a Smart Card reader.
Active Directory Authentication	AD credentials will be required to log into vCenter, Horizon Admin and App Volumes Manager.
User Profile Management	Dynamic Environment Manager (DEM) will use the security features Smart Policies, Application Blocker and Elevated Permissions to further restrict settings inside the virtual desktops.
Federal Information Processing Standard (FIPS)	FIPS will not be used.
Disk Encryption	Disk encryption, such as Bitlocker, will not be used.
VMware Horizon Security Settings	VMware Horizon security features, such Secure Gateway and Horizon Client restriction will be

	partially used to further restrict users from accessing the Horizon environment.
Device Compliance	Device Compliance will not be used.

Table 50 - Platform - Security Standards

0343 The security settings will be further detailed during implementation.