EDC SERVICES
TECHNICAL INTEGRATION INFORMATION

Shared Services Canada

Solutions Integration Services Division

Project Management and Delivery

Document Revision:	v. 0.2
Status:	Draft
Publish Date:	***2018-01-18***

DOCUMENT HISTORY

Commented [TM(1)]: Do we really want to include Doc History in the RFP version of this document?

Document Author(s) & Co-Author(s), Position – Title

Full Name	Role	Department - Position - Title
Fabien de Oliveira	Senior Advisor	Solutions Integration Services Division
Ray Parent	Solution Integrator	Solutions Integration Services Division
Sean Smith	Solution Integrator	Solutions Integration Services Division

History of Changes

Ver. #	Date	Consulted/Reviewers	Brief description of Change	Author of Change
0.1	2017-12-19	Fabien de Oliveira	Initial Draft	Fabien de Oliveira
0.2	2018-01-18	Fabien de Oliveira	Feedback from Sean Smith	Fabien de Oliveira

Table of Contents

1 INTRODUCTION 4

1.1 PURPOSE 4

2 SSC INTEGRATION ENVIRONMENT OVERVIEW 5

2.1 SSC DATA CENTRE FACILITIES 5
2.2 DATA CENTRE NETWORK 5
2.3 EDC SERVICES 5
2.3.1 Datacentres 5
2.3.2 Application Visibility and Accessibility 6
2.3.3 Minimum Development Environments 6
2.3.4 Elevated Privilege 6
2.3.5 Virtualization Platform 6
2.3.6 Application Delivery Controller (ADC) 6
2.3.7 Backup infrastructure 6
2.3.8 Monitoring and alerting infrastructure 7
2.3.9 Logging system 7
2.3.10 Domain Name Service (DNS) 7
2.3.11 Directory Services 7
2.3.12 Anti-Virus protection 7
2.3.13 Patching services 7
2.3.14 Redundancy 8
2.3.15 Managed OS (Operating System) 8
2.4 REMOTE ACCESS SERVICE 8
2.4.1 Application Admin Landing Pad 8
2.4.2 SSC Remote Administration 8
2.5 SECURITY ZONING COMPLIANCY 9
2.5.1 ITSG Guidelines references 9
2.6 SECURITY ASSESSMENT PLAN 10
2.7 EXTERNAL SERVICE INTEGRATION 10
2.7.1 Email Transformation Initiative (ETI/YES) 10
2.7.2 Security Operations Centre (SOC) 10
2.7.3 Internal Credential Management (ICM) 10
2.7.4 Supply Chain Integrity 11

1 Introduction

1.1 Purpose

This document provides the high level SSC technical requirements and services to enable any solution to integrate into SSC Data Centres. In particular, it focuses on the services that are available in End State Data Centres (EDC).

Any consumption of any of SSC's service offerings from the Service Catalogue, signals a departure from the Facilities as a Service (FaaS) business model and will indicate a transition to Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) business models.

2 SSC Integration Environment Overview

The following are existing SSC services which can be leveraged and/or integrated into solutions deployed in EDC:

- SSC Data Centre Facilities
- SSC EDC Services
- SSC Network Infrastructure
- SSC Enterprise Service Desk
- SSC Security Operations Centre (SOC)
- SSC Active Directory Credential
- GoC PKI Components
- Others (as they become available in the SSC service catalog.

2.1 SSC Data Centre Facilities

SSC Data Centre Facilities include the following features:

- High-density Tier 3 data centre capacity
- Multi-tenant (multiple partners) environment with no physical separation
- Conditioned, uninterrupted power for IT infrastructure
- Full UPS power, back-up systems and N+1 (or greater) redundancy
- Robust heating, ventilation and air conditioning (HVAC) systems
- Security equipment, techniques and procedures to control, monitor and record access to the facility
- Measuring and monitoring of availability, efficiency, capacity and security
- Operations centres and storage space
- A minimum of two separate network carrier access points for redundancy

2.2 Data Centre Network

Shared Services Canada (SSC) will be responsible for providing Internet, Wide Area Network (WAN), and LAN connectivity for the proposed solution that will be hosted in the SSC Data Center (EDC). This connectivity model will allow traffic to and from the proposed solution as well as communication within the EDC.

2.3 EDC Services

2.3.1 Datacentres

Datacentre Authority to Operate (ATO) has been received to a level of Protected A, Medium, Medium. Application security controls can be addressed in order to bring the application accreditation to Protected B.

2.3.2 Application Visibility and Accessibility

The Government of Canada community, Departments, and Internet audience are able to access applications through the following network security access zones:

- Ingress from GoC Community via GCCC through EDC Operational Zone (OZ).
- Ingress from Internet into EDC through EDC Public Access Zone (PAZ)

Refer to Figure 1 in Section 2.5.1 for more information on EDC Zoning.

2.3.3 Minimum Development Environments

SSC currently supports a 3 Standard Development Life Cycle (SDLC) environments. These environments are as follows:

- Development
- Pre-Production
- Production

Any additional environments such as Test, Training, QA etc. can be placed within one of the three base environments depending on the requirements of the additional environment.

2.3.4 Elevated Privilege

Production and Pre-Production Administrator account permissions are exclusive to SSC operational support groups for all devices (physical and virtual) within EDC. Partner and/or vendor administrators and developers will be provided with Power User level credentials in the Production and Pre-Production environments.

2.3.5 Virtualization Platform

The current hypervisor employed in EDC is VMware vSphere ESXi version 5.5.

2.3.6 Application Delivery Controller (ADC)

The Application Delivery Controller (ADC) Solution is currently implemented in a fully redundant configuration. This redundancy increases reliability and availability. This service aims to optimize resource use, maximize throughput, minimize response time, and avoid overload of any single resource.

- Features available from the ADC solution are as follows: Forward Proxy, Load Balancer, and SSL Offload Certificate.

2.3.7 Backup infrastructure

All virtual servers are automatically protected by the Operational Recovery Service (ORS) once they are rolled-out in EDC. The schedule is one full backup per week, and incremental backups for the remaining days.

CommVault, the interim End State solution, backs up a VMware snapshot of the virtual server. Version 11.x of CommVault is currently in use.

Agent based backups could be leveraged on a case by case basis if required.
Backup Data retention is 30 days and off site storage of a backup is achieved through auxiliary copy jobs scheduled every day.

2.3.8 Monitoring and alerting infrastructure

SSC monitors the real time availability of infrastructure and applications using ESM monitoring tools and the ECC service. Part of the Managed OS in the Managed OS service is monitored through the CA agent. This monitoring provides a basic monitoring option to Infrastructure (CPU, Memory, Disk space, and Ping heartbeat status).

The tool currently in use is Enterprise System Monitoring (ESM) Spectrum.

2.3.9 Logging system

Environment logs are sent to a Log aggregator and then in turn sent to a collector for analysis and review. The logs are leveraging the management network interface card (NIC) to send the information to the appropriate services line.

2.3.10 Domain Name Service (DNS)

There is an SSC managed DNS service available for application IP address resolution.

2.3.11 Directory Services

Solutions have the option to interact with SSC Active Directory (AD) to leverage AD credentials.
The AD solution in place is currently leveraging Windows 2012 Directory Services. (The SSC AD team are currently planning for Windows 2016).

2.3.12 Anti-Virus protection

SSC currently employs an anti-virus scanning solution. If the vendor considers that performance could be impacted by virus scanning, then exclusions would need to be provided for the anti-virus client.
Currently in development, an Application White List is been implemented within EDC and will require application details to be passed along to the security team in order for the application to be installed and executed.

2.3.13 Patching services

Patching for the Windows service is accomplished through the SCCM product.
Patching for the Linux service is available through Puppet and Satellite for Red Hat.
A patching schedule is available for both Managed OS versions.

2.3.14 Redundancy

Redundancy is built in within the datacentre. Special design is required for HA configuration between datacentres on a case by case basis.

2.3.15 Managed OS (Operating System)

By default each Managed OS are configured with 2 network interface cards (NIC) (Management and Production). Each Managed OS is supported by the aforementioned Backup, Monitoring and Alerting, Anti-Virus and Patching services.
Any proposed solution should provide all software licenses and management required by the solution in the application tier above the managed operating system. Supported Managed OS operating systems are as follows:

- Windows 2012 R2
- Linux Red Hat 6.4

2.4 Remote Access Service

Remote access to the Management Restricted Zone (MRZ) is accomplished through two factor authentication using the following two factors:

- IT Credentials associated to Windows Directory services with Role Base Access.
- A MyKey PKI Account

2.4.1 Application Admin Landing Pad

Application Admin access is provided through a Citrix Landing Pad. The Citrix Landing Pad can be accessed with two factor authentication through an SSC provided VPN service.

The Citrix Landing Pad by default has RDP and Putty published Apps. These published applications can be used to access the administrative consoles of infrastructure servers.

If required by the vendor, additional published apps can be made available (the vendor would need to provide an installation package and profile for the project to the Citrix service line). This could be used to publish any administrative consoles etc. that the proposed solution might require.

2.4.2 SSC Remote Administration

EDC Data Centres are considered to be light outs data centres. No physical access to EDC Data Centres is permitted. All administrative tasks are completed remotely via the Remote Access administration solutions.

Remote Administration will adhere to current SSC processes in place for remote administrative access to the EDC infrastructure.

These processes may include but are not limited to:

- IT credentials
- Government of Canada provided endpoint (workstation)
- myKEY PKI credentials

2.5 Security Zoning Compliancy

2.5.1 ITSG Guidelines references

SSC applies CSE security guidelines (ITSG22, 33, 38…): https://www.cse-cst.gc.ca/en/publication/list/

EDC Network Zoning is illustrated in the following diagram.

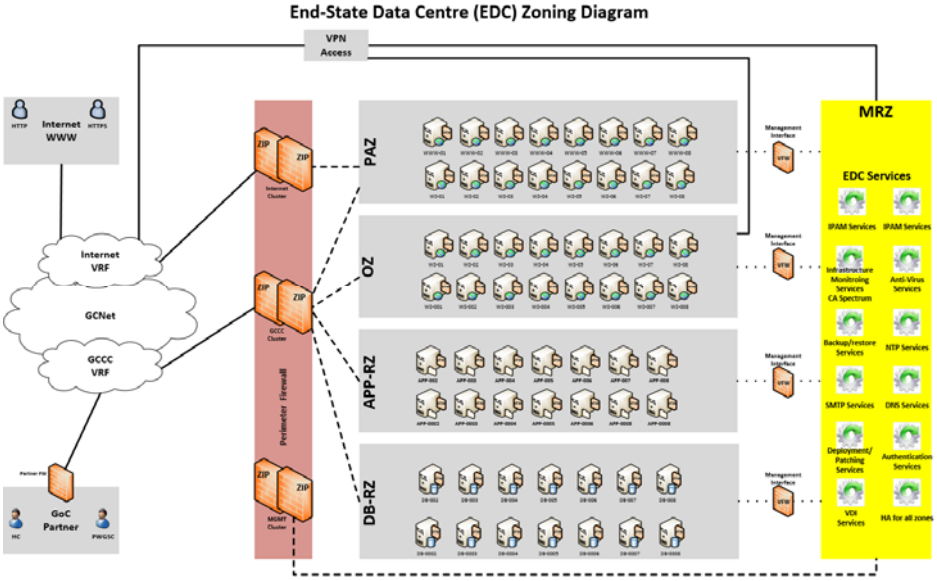

Figure 1 – EDC Zoning Diagram

Acronym	Definition
APP-RZ	Application Restricted Zone
DB-RZ	Database Restricted Zone
GCCC	Government of Canada Community Cloud
MRZ	Management Restricted Zone

OZ	Operational Zone
PAZ	Public Access Zone
VFW	Virtual Firewall
VRF	Virtual Routing and Forwarding
ZIP	Zone Interface Point

Table 1 – EDC Network Zoning Acronym Definitions

2.6 Security Assessment Plan

A Security Assessment will need to be conducted for any proposed solution (details to be provided). Please consult the appropriate service line for more information.

2.7 External Service Integration

2.7.1 Email Transformation Initiative (ETI/YES)

If email service are required then the vendor will need to integrate with the external hosted email service. This email service is currently provided by a specific vendor. Each partner has a coordinator in charge of integrating and requesting a service account to leverage this service (please refer to the service catalog: http://service.ssc.gc.ca/en/services.

2.7.2 Security Operations Centre (SOC)

SSC houses the Security Operations Centre (SOC). The SOC is comprised of the Government of Canada Computer Incident Response Team (GoC-CIRT); the Information Technology Security Incident Recovery Team (ITSIRT); and the Federal Information Protection Centre (FIPC). The GoC-CIRT maintains the GoC-wide distribution lists, and provides departments and agencies with any advice and guidance required to mitigate cyber threats and vulnerabilities.

2.7.3 Internal Credential Management (ICM)

If required the proposed solution should be capable of leveraging the GoC Public Key Infrastructure, myKEY.

The proposed solution should have the ability to integrate myKEY ICM with employee desktops.

MyKEY LOGIN (secure web authentication service), has an additional integration charge above the base cost of ICM services.

2.7.4 Supply Chain Integrity

The purpose of the Supply Chain Integrity (SCI) process is to ensure that no un-trusted equipment, software or services are procured and are used in the delivery and/or support of Government of Canada (GC) services.