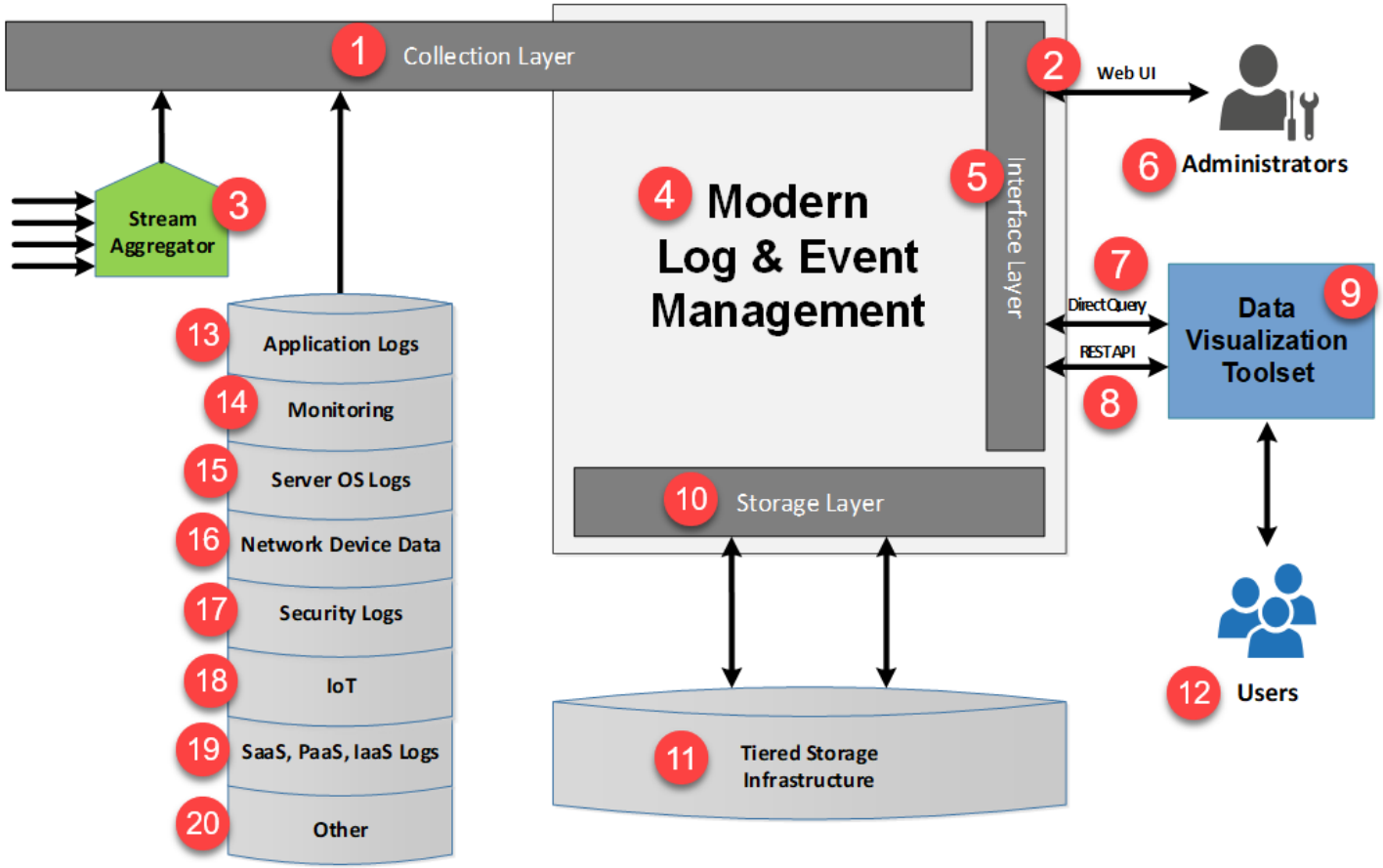
Modern Log and Event Management

Statement of Requirements – Stage 1

Purpose

Canada is looking for a Modern Log and Event Management (MLEM) solution to securely collect, aggregate and centrally store systems, infrastructure and application log data to provide operational visibility to resolve issues before they impact clients.

Conceptual Solution Diagram



CONTINUATION

EN	FR
Collection Layer	Couche de collecte
Web UI	Interface utilisateur Web
Stream Aggregator	Agrégateur de flux de données
Modern Log & Event management	Gestion moderne des journaux des événements
Interface Layer	Couche d'interface
Administrators	Administrateurs
Direct Query	Interrogation directe
RESTAPI	Protocole RestAPI
Data Vizualisation Toolset	Ensemble d'outils de visualisation des données
Storage Layer	Couche de stockage
Tiered Storage Infrastructure	Infrastructure de stockage hiérarchisé
Users	Utilisateurs
Application Logs	Journaux d'application
Monitoring	Surveillance
Server OS Logs	Journaux du système d'exploitation du serveur
Network Device Data	Données des périphériques réseau
Security Logs	Journaux de sécurité
IoT	IdO
SaaS, PaaS, Iaas Logs	Journaux SaaS, PaaS et Iaas
Other	Autres

CONTINUATION

Log data is currently considered to be a largely untapped resource that can significantly expand monitoring insight and provide a new means to securely collect, aggregate and centrally store actionable and insightful log data and provide access for various use cases. The desired outcomes of this initiative are:

- Event and log data centralization
- IT Security controls compliance
- Increased relevance for monitoring alerts
- Reduction in existing and future monitoring log data management gaps
- Event correlation and reduced alerting
- Realized efficiencies due to more accurate monitoring log data

Mandatory Requirements

Canada requires a Modern Log and Event Management (MLEM) solution from a bidder that has the following mandatory characteristics and capabilities:

E1. Central functions such as:
- Ingesting data from a variety of sources
- Securely storing the acquired data
- Providing secure access to the data

E2. Data management capabilities for:
- Historical data

E3. Capabilities for data ingestion that include:
- Logs
- Metrics

E4. Solution delivery options that include:
- On-premise COTS solution
- Cloud-based solution with data residency in Canada

E5. Security & IM compliance-related capabilities that include:
- TCP communication
- TLS communication

CONTINUATION

- Data integrity control
- Secure data storage
- Secure data access
- Granular RBAC
- Auditing capabilities
- Data staging and filtering
- Cloud Security Certifications

E6. Data source integration via native application connectors

E7. Data retention capabilities that include:
- Association with tiered storage systems
- Multiple policies per data source
- Automated data disposition reporting

E8. Scalability of solution both on-premise and in cloud

E9. Support and maintenance

E10. Professional services

CONTINUATION

Section A - STATEMENT OF REQUIREMENTS

All material must be submitted electronically and must not include external web links. Bidder must be compliant with all mandatory requirements. Proposals not meeting this prerequisite will not be given any further consideration.

Requirements

Ref.	Requirement	Requirement Type	Requirement Description
E1. Central functions			
E1.1	Multiple data source ingestion	Mandatory	The solution must securely ingest data from multiple sources and source types. Sources must include but not be limited to: - Raw Syslog - Windows Event logs (evtx) - Microsoft IIS logs (W3C) - CSV - JSON - Azure Active Directory data - Unstructured text files from custom application logs - Microsoft SQL Server
E1.2	Central and secure data storage	Mandatory	The solution must securely and centrally store acquired log data.
E1.3	Secure data access	Mandatory	The solution must securely provide access to the acquired log data.
E2. Data management			
E2.1	Historical data management	Mandatory	The solution must manage historical data with the expectation that said data (structured and unstructured) accumulates in high volumes and changes rapidly.
E3. Data ingestion			
E3.1	Log data ingestion	Mandatory	The solution must capture log data generated by any software or hardware device, prepare that data for access and analysis as well as index it for storage.
E3.2	Metric data ingestion	Mandatory	The solution must capture metric (numerical) data to which time series can be immediately applied.
E4. Solution delivery			
E4.1	On-premise COTS solution	Mandatory	The solution must have the ability to deliver the required capabilities using components deployed solely on-premise.
E4.2	Cloud-based solution	Mandatory	The solution must have the ability to deliver the required capabilities using components deployed solely in the cloud (SaaS, PaaS).

CONTINUATION

Ref.	Requirement	Requirement Type	Requirement Description
E4.3	Data residency in Canada	Mandatory	Data collected in a cloud-based solution must be hosted in Canadian data centres.
E5. Security & IM compliance			
E5.1	TCP communication	Mandatory	The solution must use TCP (Transmission Control Protocol) communication for all data sources.
E5.2	TLS communication	Mandatory	The solution must use TLS (Transport Layer Security) for secure network communication to prevent unauthorized access of data in transit.
E5.3	Data integrity control	Mandatory	The solution must be capable of providing data integrity control monitoring and alerting.
E5.4	Secure data storage	Mandatory	The solution must be capable of storing and archiving data deemed sensitive in encrypted and timestamped files.
E5.5	Secure data access	Mandatory	The solution must support only authenticated and authorized users accessing the system.
E5.6	Role-based access controls	Mandatory	The solution must provide granular role based access controls (RBAC) with the authority to enforce least privilege access policies and access policies based on job functions (administrative actions) and data sets (groups of log and events).
E5.7	Comprehensive auditing capabilities	Mandatory	The solution must have auditing capabilities such as logging all user transactions on the system that includes, but is not limited to, the modification or deletion of configuration information or data (e.g. permissions, metadata, disposition, etc.).
E5.8	Data filtering capabilities	Mandatory	The solution must provide users the ability to stage, inspect and otherwise filter ingested data before commitment to storage and general availability to the solution user base.
E5.9	Cloud Security Certifications	Mandatory	Cloud base solution must hold the following certifications: - ISO 27001 Certification - Service Organization Control (SOC) 2 Type II
E6. Data source integration			
E6.1	Native application connectors to extend the capabilities of the solution	Mandatory	The solution must provide native application or technology connectors that extend the capabilities of the solution for the technologies below. • ServiceNow • Microsoft 365 (EXO, SPO, Teams) • Microsoft Azure Cloud • Microsoft Windows Server • Microsoft SQL Server
E7. Data retention			
E7.1	Tiered storage systems capability	Mandatory	The solution must be capable of setting and maintaining data retention policies that can be associated with tiered storage systems.

CONTINUATION

Ref.	Requirement	Requirement Type	Requirement Description
E7.2	Data retention capabilities for multiple data sources	Mandatory	The solution must be capable of setting and maintaining multiple data retention policies per data source.
E7.3	Data disposition reporting	Mandatory	The solution must be capable of reporting on the disposition of data at any point in time.
E8. Scalability			
E8.1	Scalability of solution on-premise and in cloud	Mandatory	The solution must scale linearly, without significant architecture changes, to accommodate any additional volumes of users, systems, cloud services and applications log data.
E9. Support			
E9.1	Support and maintenance	Mandatory	The solution must come with 7/24 technical support and maintenance that includes ongoing system upgrades.
E10. Professional services			
E10.1	Professional services	Mandatory	The solution must come with professional services able to assist with the design and implementation of the solution as well as provide product training and/or knowledge transfer sessions.