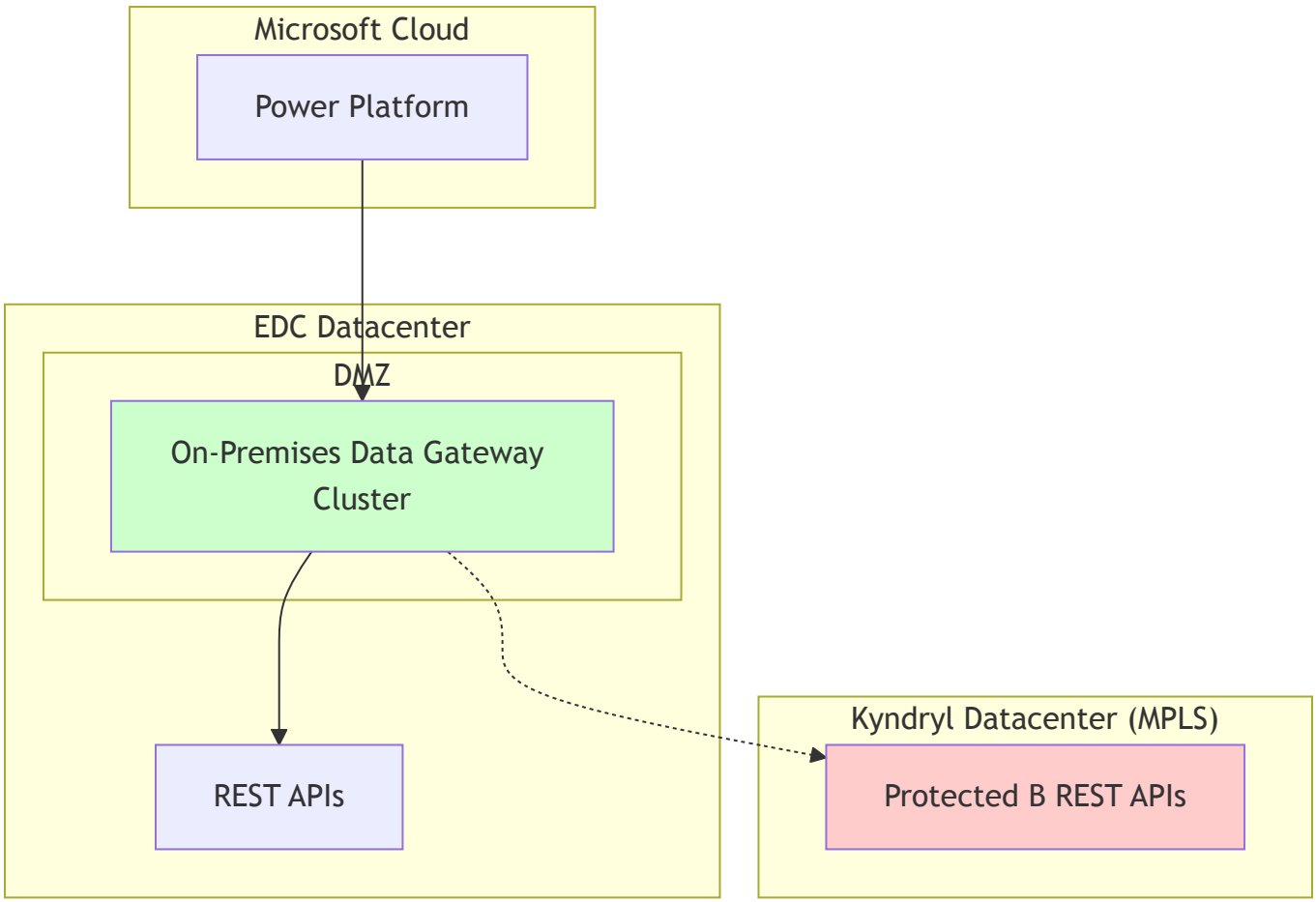
Executive Overview

This document defines the mandatory configuration requirements for enabling Power Platform access to REST APIs hosted in Elections Canada's two datacenters using the On-Premises Data Gateway (OPDG). This implementation will:

1. Utilize the DMZ in EDC with two non-domain joined servers in a high-availability cluster running the OPDG
2. Connect to APIs in EDC that are accessible from the DMZ
3. Provide secure access to APIs in Kyndryl (connected via MPLS) that are not exposed to cloud due to Protected B security requirements
4. Leverage the existing network link between EDC and Kyndryl datacenters



Current Environment

- The DMZ VMs are not domain-joined (by design for machine-to-machine workflows)

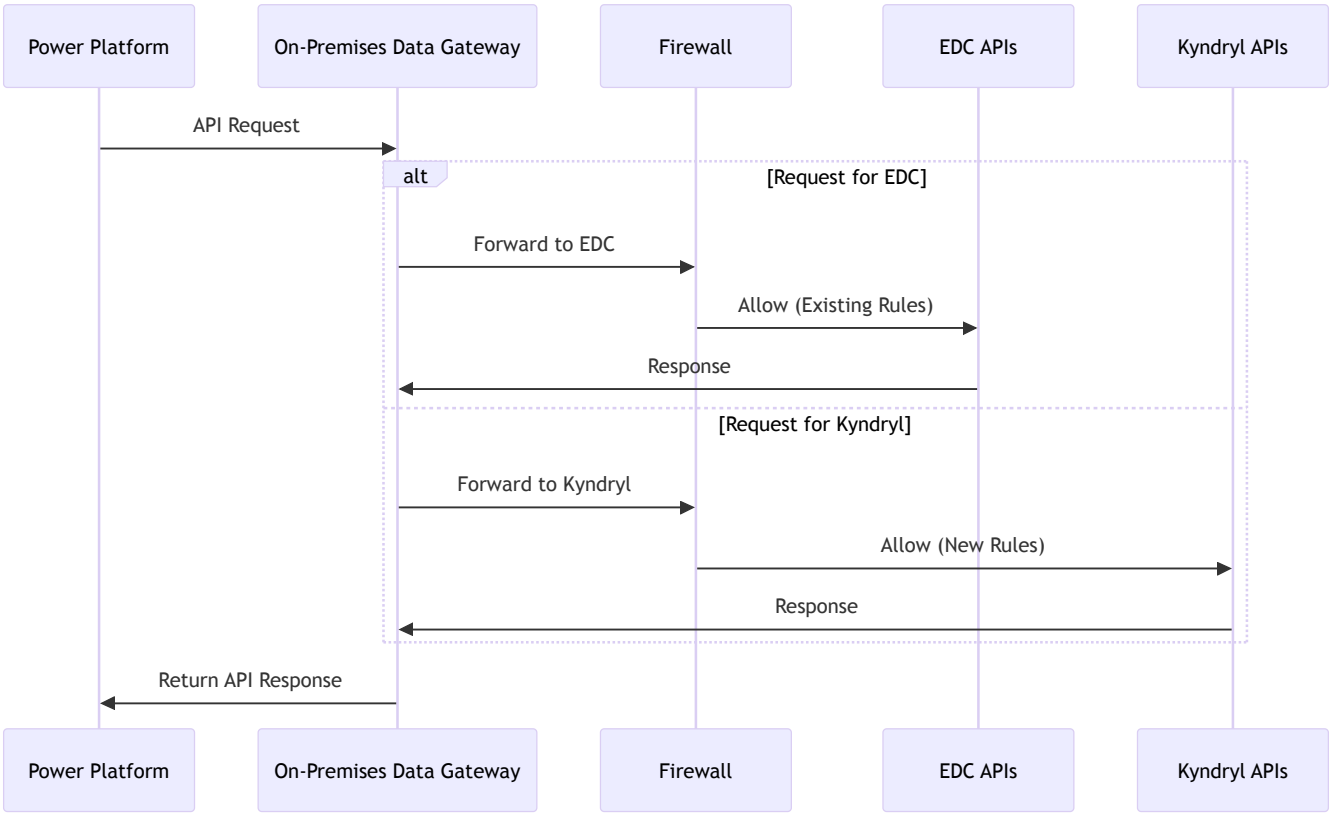
- DMZ servers have firewall configurations that allow communication with EDC but not currently with Kyndryl
- Kyndryl datacenter enforces stricter security requirements and does not expose APIs to the cloud

Strategic Solution

1. Network Configuration Between EDC and Kyndryl Datacenters

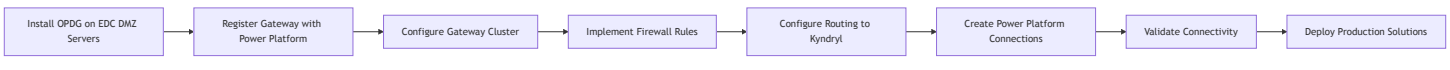
To enable the OPDG in EDC's DMZ to access the APIs in Kyndryl:

1. **Firewall Rule Implementation**: Implement firewall rules on the DMZ servers to allow traffic to specific API endpoints in Kyndryl
    - Configure rules for the required ports (443 for HTTPS)
    - Restrict access to only the necessary IP addresses and ports
    - Enable comprehensive logging for all traffic to meet GC Protected B audit requirements
2. **Network Routing Implementation**: Deploy routing configurations to ensure direct traffic flow between the DMZ and Kyndryl
    - Utilize the existing logical network link between EDC and Kyndryl
    - Configure routing tables on the DMZ servers to route API requests to Kyndryl



2. OPDG Cluster Installation and Configuration

1. **OPDG Cluster Installation**:
   - Deploy OPDG on both non-domain joined DMZ servers in EDC
   - Configure the gateway in high-availability cluster mode
   - Register the gateway with Elections Canada's Power Platform tenant
   - Implement service accounts with least privilege access
2. **Data Source Connection Configuration**:
   - In Power Platform admin center, establish connections to the APIs in both EDC and Kyndryl
   - Configure all connections to use the same gateway cluster
   - Define specific endpoints for each API with appropriate authentication methods
3. **Connection Validation and Testing**:
   - Validate connections to APIs in both datacenters through the gateway
   - Monitor and log network traffic during testing to verify proper routing
   - Perform Protected B data transmission tests to validate security controls



3. Security and Compliance Implementation

1. **Network Security Controls**:

- Implement ITSG-22 compliant firewall rules to allow only necessary traffic
- Deploy Web Application Firewall (WAF) protection for all API traffic
- Enforce TLS 1.2+ encryption for all communications with strong cipher suites
- Implement network segmentation according to Protected B requirements

2. **Authentication and Authorization Mechanisms**:
   - Deploy mutual TLS authentication between the OPDG and all API endpoints
   - Implement OAuth 2.0 with PKCE for secure API access
   - Enforce IP restrictions on all API endpoints
   - Implement just-in-time access for administrative functions
3. **Comprehensive Monitoring and Logging**:
   - Configure detailed logging on the OPDG to meet GC audit requirements
   - Monitor all traffic between EDC and Kyndryl datacenters
   - Implement automated alerts for anomalous traffic patterns
   - Integrate with Elections Canada's SIEM solution

Governance and Operational Management

Service Management Framework

1. **Service Ownership**:
   - Designate EC IT staff responsible for OPDG service ownership
   - Establish clear roles and responsibilities matrix
   - Define escalation paths for incidents
2. **Change Management**:
   - Implement formal change control processes for gateway configuration changes
   - Require security review for new API connections
   - Maintain configuration documentation
3. **Capacity Planning**:
   - Monitor gateway performance metrics
   - Plan for scaling based on usage patterns
   - Establish thresholds for resource utilization

Standard Operating Procedures

1. **Installation and Updates**:
   - Schedule regular gateway updates during maintenance windows
   - Test updates in non-production environment first
   - Maintain version control for gateway configurations

    - Document rollback procedures
2. **User Access Management**:
    - Implement quarterly access reviews
    - Enforce separation of duties
    - Document onboarding/offboarding procedures
3. **Incident Response**:
    - Define response procedures for gateway outages
    - Establish communication plans
    - Conduct regular tabletop exercises
4. **New Connection Onboarding Process**:
    - Implement formal request process for new connections
    - Require security assessment for all new APIs
    - Mandate business justification documentation
    - Enforce testing in lower environments before production

Implementation Alternatives

Alternative 1: Dedicated OPDG in Kyndryl Datacenter

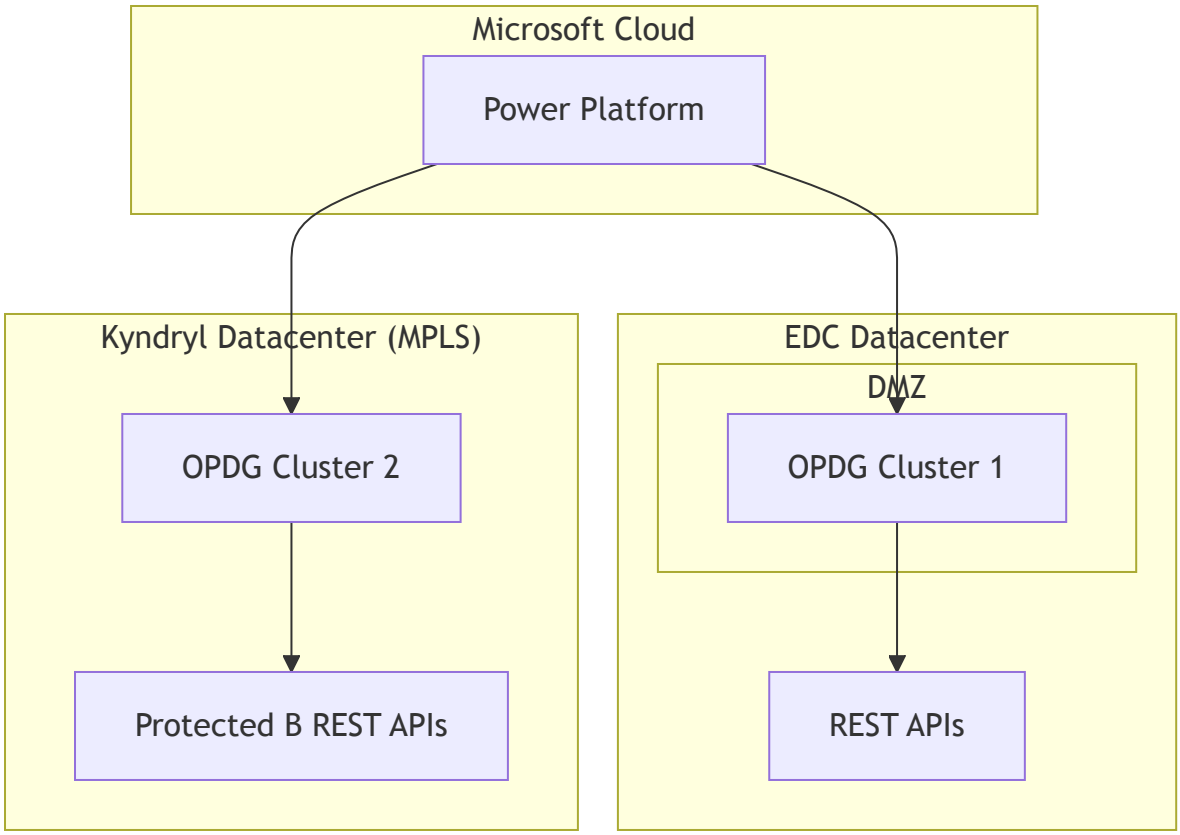
Install a separate OPDG instance directly in the Kyndryl datacenter to provide direct access to Protected B APIs.

Strategic Benefits:

- Direct access to Kyndryl APIs with minimal network hops
- Clear network segmentation adhering to Protected B standards
- Optimized performance for Kyndryl API calls
- Simplified security monitoring

Implementation Considerations:

- Requires additional infrastructure deployment in Kyndryl datacenter
- Necessitates management of multiple gateway clusters
- Requires additional Power Platform configurations



Alternative 2: API Proxy in EDC Datacenter

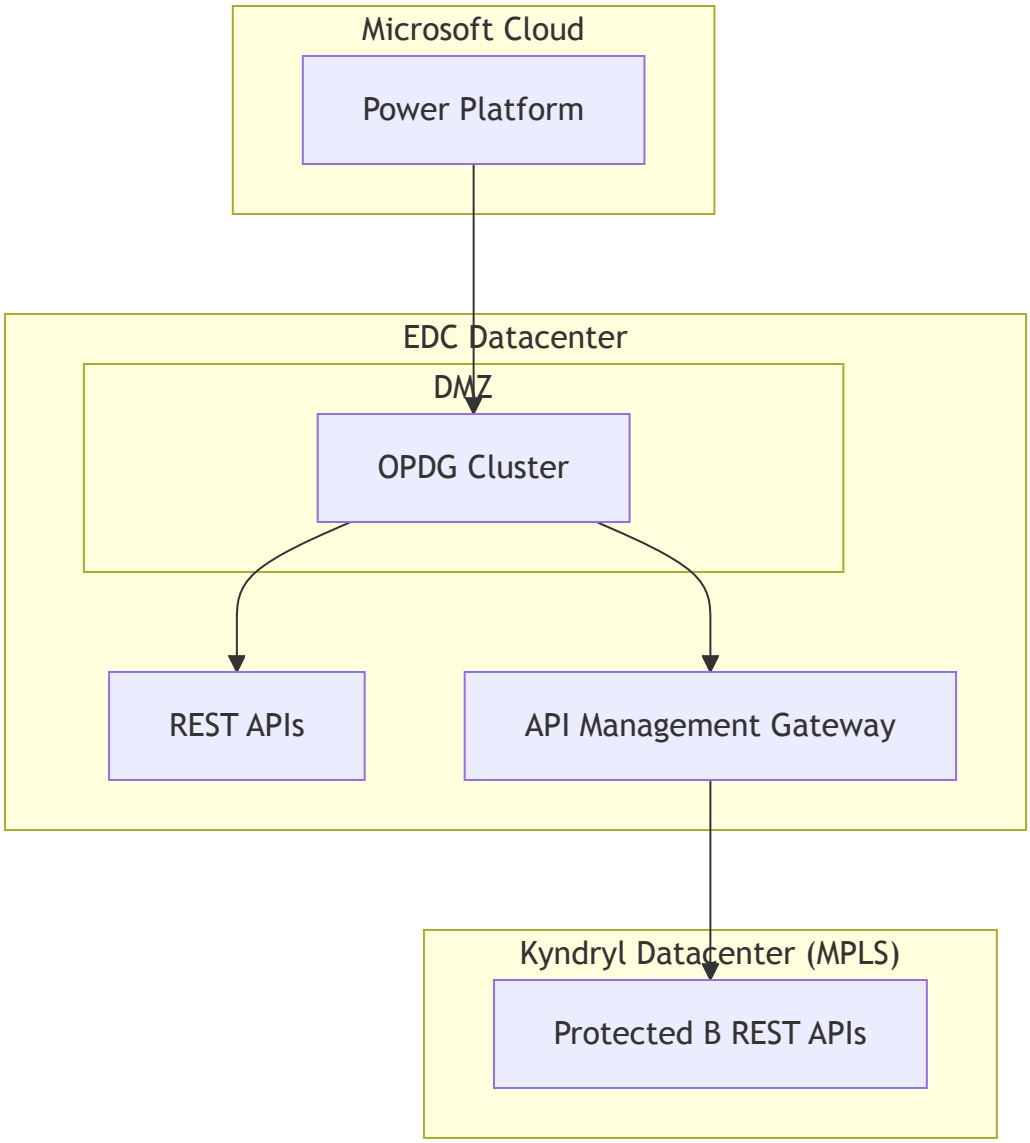
Deploy an enterprise API management gateway in EDC datacenter to handle and secure all requests to Kyndryl.

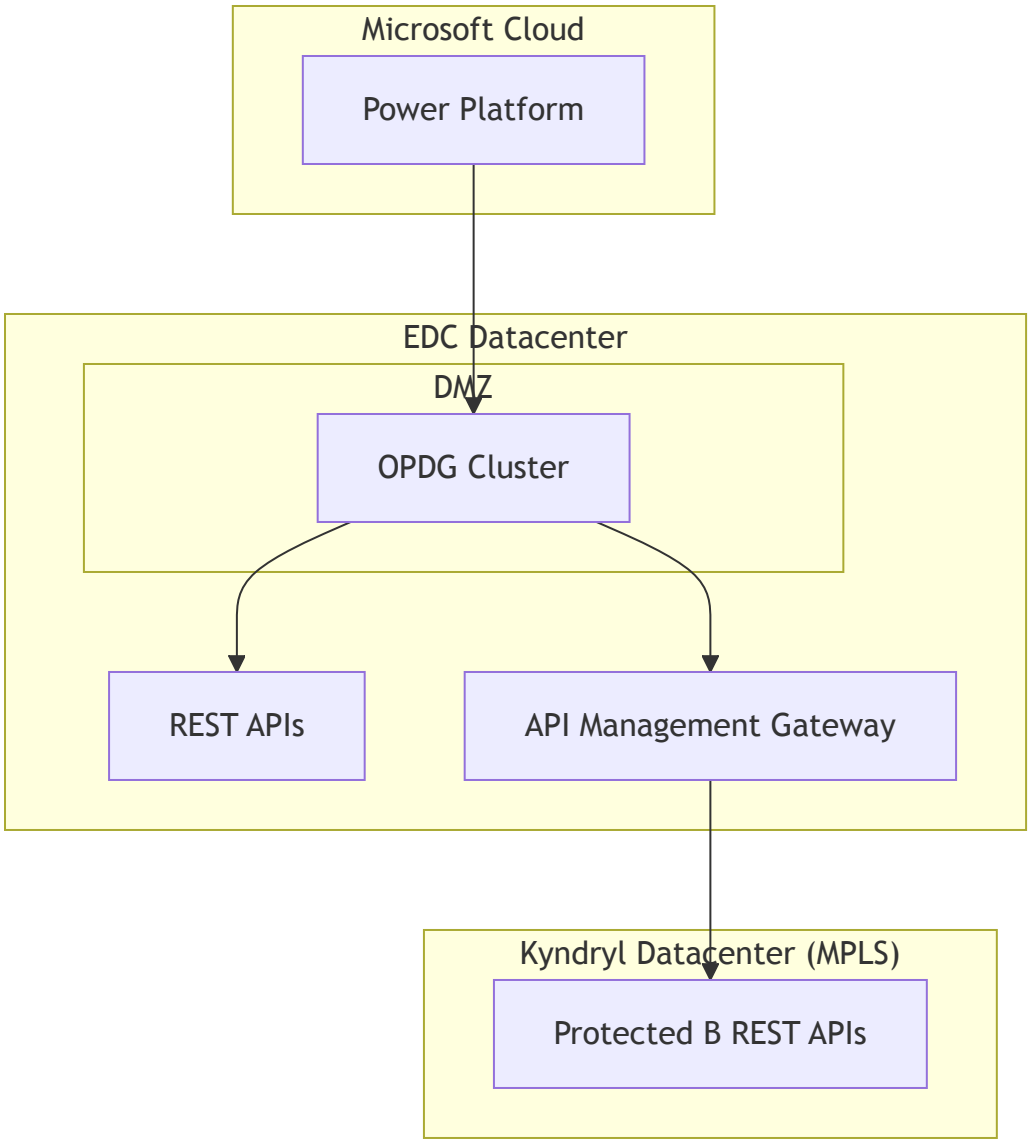
Strategic Benefits:

- Simplified OPDG configuration with centralized endpoint management
- Consolidated API governance and monitoring
- Enhanced security controls with API request inspection
- Consistent API policy enforcement

Implementation Considerations:

- Requires deployment and management of API gateway infrastructure
- Potential latency impact for Kyndryl API calls
- More complex error handling and troubleshooting procedures


Microsoft Cloud
Power Platform
EDC Datacenter
DMZ
OPDG Cluster
REST APIs
API Management Gateway
Kyndryl Datacenter (MPLS)
Protected B REST APIs



Alternative 3: GC Cloud Virtual Network Implementation

Leverage GC Cloud Virtual Network capabilities to establish secure connectivity between environments while maintaining Protected B compliance.

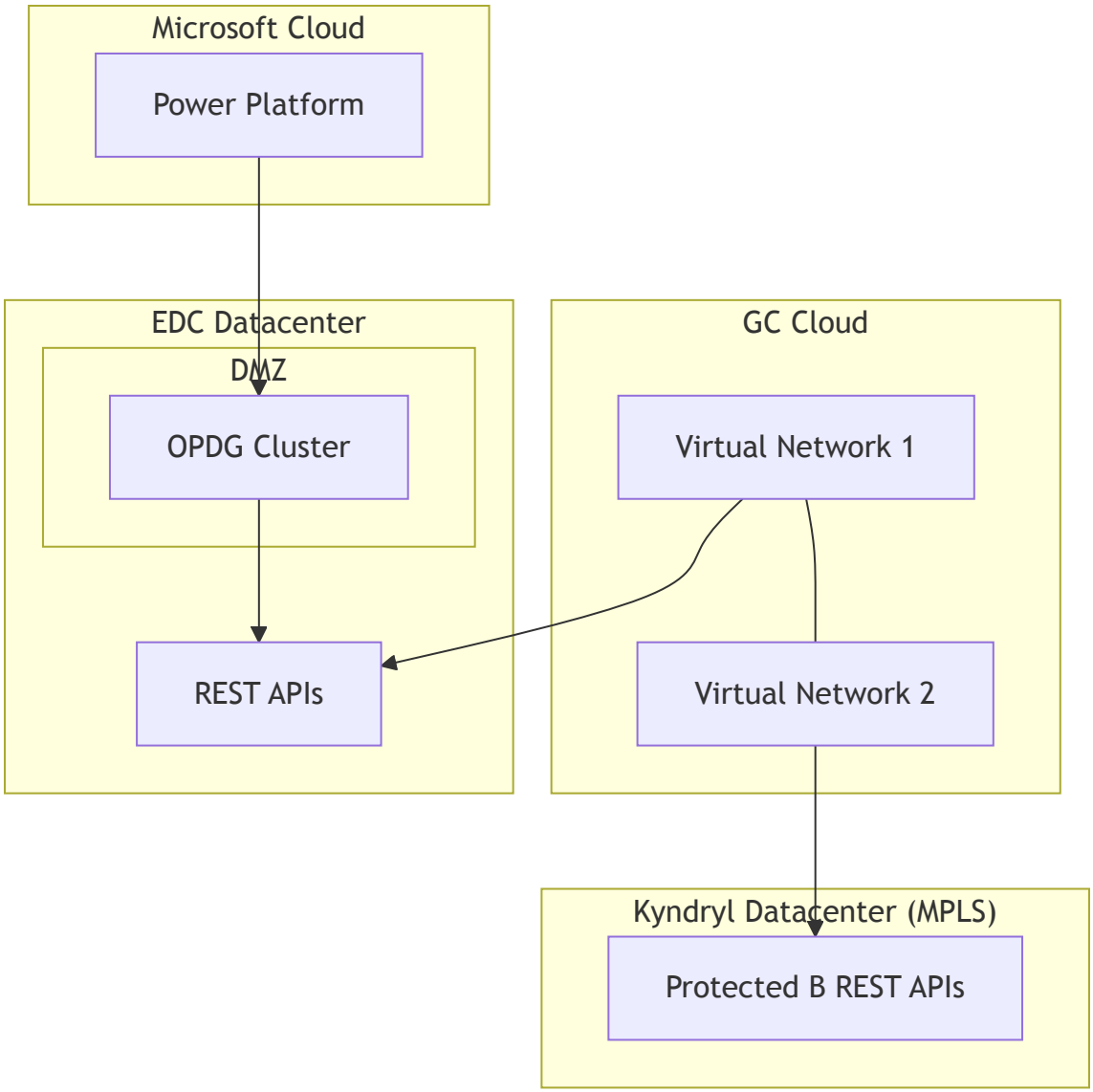
Strategic Benefits:

- Secure and direct connectivity with end-to-end encryption
- Leverages GC-approved cloud networking capabilities
- Simplified management with infrastructure-as-code deployment
- Enhanced monitoring capabilities

Implementation Considerations:

- Requires GC Cloud network implementation
- May require architectural adjustments to existing infrastructure

- Potential additional costs requiring budget approval



BUILD BOOK ANNEXES

ANNEX A: OPDG Cluster Installation and Configuration

A.1 Prerequisites

- Two Windows Server 2019/2022 VMs in EDC DMZ (non-domain joined)
- Each VM with minimum 8 cores, 16GB RAM, 100GB storage
- .NET Framework 4.7.2 or later installed

- TLS 1.2 or later enabled
- Outbound connectivity to Azure Service Bus endpoints
- Service accounts with appropriate permissions

A.2 OPDG Installation Process

1. Download the latest On-Premises Data Gateway installer from Microsoft
2. On first server, run installer as administrator
3. Select "New gateway installation" option
4. Authenticate with Elections Canada Power Platform admin account
5. Set a recovery key and store in secure location
6. Name the gateway "EC-OPDG-Primary"
7. Complete installation and verification

A.3 Configure High Availability Cluster

1. On second server, run installer as administrator
2. Select "Register a gateway on this computer"
3. Authenticate with same Elections Canada Power Platform admin account
4. Enter the recovery key from primary installation
5. Select the existing gateway name to join the cluster
6. Complete installation and verification

A.4 Gateway Configuration

1. Configure Windows Firewall on both servers to allow required connectivity
2. Implement OPDG monitoring using Windows Performance Counters
3. Configure gateway service to run under dedicated service account
4. Set appropriate service recovery options
5. Configure backup of gateway encryption keys

ANNEX B: Network Configuration for EDC to Kyndryl Connectivity

B.1 Firewall Configuration

1. Identify all Kyndryl API endpoints requiring access
2. Document IP addresses, ports, and protocols

3. Create firewall rules allowing traffic from OPDG servers to Kyndryl endpoints
4. Implement logging for all traffic
5. Validate connectivity using test transactions

B.2 Routing Configuration

1. Document current network topology
2. Identify routing path between EDC DMZ and Kyndryl
3. Configure routing tables on DMZ servers
4. Implement route monitoring
5. Test end-to-end connectivity

B.3 Security Controls

1. Implement TLS inspection if required
2. Configure IDS/IPS for API traffic
3. Set up network traffic monitoring
4. Implement rate limiting controls
5. Configure logging to meet GC Protected B requirements

ANNEX C: API Integration for Power Platform

C.1 API Documentation

1. Document all API endpoints in both datacenters
2. Catalog authentication requirements for each API
3. Document data classification for each API
4. Create API integration test plan
5. Establish API monitoring strategy

C.2 Power Platform Connection Configuration

1. In Power Platform Admin Center, navigate to Data Gateways
2. Verify gateway cluster is online and healthy
3. Create connections to required data sources
4. Configure authentication for each connection
5. Test connections with minimal permissions

C.3 Connection Security

1. Implement connection encryption
2. Configure data loss prevention policies
3. Set up connection auditing
4. Implement connection monitoring
5. Establish connection recertification process

ANNEX D: OPDG Governance Framework

D.1 Roles and Responsibilities

Role	Responsibilities	Department
OPDG Service Owner	Overall accountability for service	EC IT Operations
OPDG Administrators	Day-to-day management	EC IT Support
Security Officer	Security compliance	EC IT Security
Change Approver	Review/approve changes	EC Change Advisory Board
API Owners	Management of specific APIs	Various EC Departments

D.2 Standard Operating Procedures

D.2.1 Gateway Maintenance

1. Schedule monthly maintenance window
2. Test updates in non-production environment
3. Create backup of configuration before updates
4. Apply updates during approved change window
5. Verify gateway functionality after updates
6. Document all maintenance activities

D.2.2 New Connection Onboarding

1. Receive formal connection request with business justification
2. Conduct security assessment of requested API
3. Verify API meets Protected B requirements
4. Configure and test connection in development environment

5. Obtain security approval
6. Implement in production during change window
7. Document connection details in service catalog

D.2.3 Monitoring and Incident Response

1. Configure gateway performance monitoring
2. Set up alerts for critical metrics
3. Establish incident response procedures
4. Define escalation paths
5. Create incident response playbooks
6. Conduct quarterly incident response drills

ANNEX E: Security and Compliance

E.1 Protected B Compliance Requirements

1. Data encryption in transit and at rest
2. Multi-factor authentication for administrative access
3. Comprehensive audit logging
4. Network segmentation
5. Vulnerability management
6. Security incident and event monitoring
7. Access control based on least privilege
8. Regular security assessments

E.2 ISO 27001 Controls Implementation

1. Information security policies
2. Access control implementation
3. Cryptography implementation
4. Physical and environmental security
5. Operations security
6. Communications security
7. System acquisition and development
8. Supplier relationships
9. Information security incident management
10. Business continuity management

11. Compliance with legal and contractual requirements

E.3 Security Monitoring and Assessment

1. Implement continuous monitoring of gateway health
2. Schedule quarterly security assessments
3. Conduct annual penetration testing
4. Perform monthly vulnerability scanning
5. Review security logs weekly
6. Produce monthly security metrics report

Implementation Action Plan

- [ ] Document current network topology between EDC and Kyndryl
- [ ] Identify and catalog all API endpoints in both datacenters
- [ ] Implement firewall rules on EDC DMZ servers
- [ ] Configure routing between DMZ and Kyndryl
- [ ] Validate network connectivity between DMZ and both datacenters
- [ ] Install and configure OPDG cluster following Annex A procedures
- [ ] Register gateway with Elections Canada Power Platform tenant
- [ ] Create secure connections to APIs in Power Platform
- [ ] Validate connectivity to both datacenters with test transactions
- [ ] Implement monitoring and alerting according to Annex D
- [ ] Document final configuration in Elections Canada CMDB
- [ ] Conduct security assessment of implementation
- [ ] Obtain authorization to operate from EC security team

Conclusion

This implementation will establish a secure, compliant bridge between Elections Canada's Power Platform environment and the Protected B APIs in both EDC and Kyndryl datacenters. By leveraging the existing network infrastructure and implementing the required security controls, Elections Canada will be able to utilize Power Platform capabilities while maintaining compliance with Government of Canada security standards.

The solution must be implemented according to this document to ensure all security requirements are met and operational procedures are established for long-term governance of the service. The build

book annexes provide detailed implementation guidance that must be followed to ensure successful deployment.

For technical implementation support, engage with Microsoft Premier Support or Elections Canada's approved Microsoft partner with expertise in Power Platform and secure networking implementations.

References and Resources

Microsoft Documentation

- On-Premises Data Gateway Official Documentation
- Install On-Premises Data Gateway in Cluster Mode
- Power Platform Admin Center - Data Gateway Management
- On-Premises Data Gateway Architecture
- Troubleshooting the On-Premises Data Gateway
- Power Automate - Manage Connections

Government of Canada Security Standards

- ITSG-22: Baseline Security Requirements for Network Security Zones
- ITSG-33: IT Security Risk Management
- Government of Canada Cloud Security Risk Management Approach and Procedures
- Protected B Information Management Guidelines

ISO Standards

- ISO/IEC 27001:2022 Information Security Management
- ISO/IEC 27017:2015 Cloud Security
- ISO/IEC 27018:2019 Protection of PII in Public Clouds

Technical Resources

- Microsoft Power Platform Center of Excellence (CoE) Starter Kit
- Gateway Performance Monitoring
- TLS 1.2 Implementation Guide
- Power Platform API Security Best Practices
- Networking with ExpressRoute for Power Platform

Elections Canada Specific Resources

- Elections Canada IT Security Policy (internal document reference)
- Elections Canada Cloud Security Standards (internal document reference)
- Elections Canada Enterprise Architecture Guidelines (internal document reference)
- Elections Canada Data Classification Standards (internal document reference)# On-Premises Data Gateway Configuration for Elections Canada Multi-Datacenter API Access