DPC/G3.3

ACROSS GOVERNMENT POLICY

Cloud services network guideline

Introduction

Cloud services present many opportunities, including the potential to reduce electronic storage and internal ICT capital investment requirements.

For any business transformation project, standard considerations and processes apply. These include project planning, technical specifications, budget, risk, etc.

For cloud services, there are additional considerations. This series of Cloud Services Guidelines articulates those considerations. Consider these Guidelines alongside your normal processes.

This guideline focuses on network considerations relevant when considering or moving to a cloud computing model.

Definitions

Basic Cloud Computing definitions are provided in the Cloud Services Information Sheet.

Guidance

Types of Gateways

There are three entry points or provisioning paths that an agency may consider for a cloud service.

Foreign Network Gateway

DPC ICT Services offers an established Foreign Network Gateway which provides third party connections, semi-trusted solutions and semi-trusted agency connections with secure access to the internal South Australian Government trusted network.

The Foreign Network Gateway was established to allow access for monitoring, management/support and application requirements. Residing logically within the internet gateway perimeter and controlled via strict access requirements, it is designed for Business-to-Business (B2B) transactions requiring a permanent or point-to-point connection.

DPC ICT Services has two Foreign Network Gateway devices at different locations providing the capability to establish a resilient and redundant connection if required.

Additional information, including scope, support and pricing, can be found at the DPC ICT Services Service Catalogue, including the Foreign Network Gateway Statement of Service.

Internet Gateway

DPC ICT Services has an established Internet Gateway that allows third party access, agency staff, guests and the general public into the internal trusted environment. An interface from the South Australian Government network that allows network traffic (incoming and outgoing) to the internet, the gateway is configured with a high level of security designed to protect the integrity of the trusted network from vulnerabilities and risks.

With connections located at multiple data centres, the internet gateway provides a resilient and redundant service.

The Internet Gateway uses a download use pricing model where agencies are charged monthly on a volume basis at an agreed rate.

Additional information, including scope, support and pricing, can be found through the DPC ICT Services Service Catalogue, including the Internet Gateway Statement of Service.

StateNet Cloud Gateway

For agencies on the South Australian Government's federated data network, StateNet, DPC ICT offers an established Cloud Gateway connection which provides a secure managed connection to the Equinix Australia Data Centre in Sydney. The Equinix Data Centre is an Australian-based colocation facility that provides mature cloud services across multiple industries.

The Cloud Gateway connection was developed to enable agencies to gain access to cloud-based services via a secure managed connection rather than across the internet. Using the service agencies can gain easy and streamlined access to cloud-based services such as Infrastructure, Software, Platform and Storage as a Service.

Functional Roles

Service	Internet Access	B2B Private	Cloud Exchange	Public Web Services
Internet Gateway	✓			✓
Foreign Network Gateway		✓		
Cloud Gateway		✓	✓	✓

Increased data transmission & scalability

Cloud computing will impose a higher reliance on networks for the transmission of data to externally or internally hosted infrastructure. Moving from the ownership of infrastructure to utilising the 'as-a-service' model places greater demand on network capacity and performance.

This growth in demand will accelerate as agencies move more of their applications, software and data to the Cloud. Planning for growth becomes increasingly important. Agencies should consider how much network traffic growth will occur over time and how quickly. Agencies should anticipate that this will require regular review of short, medium and long-term planning.

Foreign Network Gateway

Discussions with external service providers need to address current and future traffic on their network infrastructure. The agency also needs to ensure that their connection to the vendor's network is adequate and is suitable for the application performance required. Baselines for performance should be known.

Internet and StateNet Cloud Gateways

It is anticipated that agencies using the Internet or Cloud Gateway will increase their requirements for more bandwidth as time progresses. Agencies need to forecast their traffic use pattern in up-front discussions for both performance and volume. This engagement will help to estimate the increased resources required and enable a more accurate charging model. DPC ICT services will use the agency forecast to maintain a watch on the growth of demand across government and plan accordingly.

Bandwidth Contention

Cloud computing involves the use of a pool of infrastructure resources, where servers and storage in multiple locations are connected by networks. Resources are provisioned from the pool, allowing dynamic elasticity, ie fast and automatic increase and decrease of processing, network bandwidth and storage as required by consumer demand and to meet their business requirements. This elasticity makes network performance a key consideration.

A greater number of agencies using the same network infrastructure presents the potential of greater contention for bandwidth. Agencies must understand the performance requirements of their applications to ensure they meet business needs. Planning should incorporate discussion with service providers around business expectations and appropriate tolerance levels to cope with peak usage periods.

Both the StateNet and Cloud Gateway utilise an architecture model that incorporates a pool of available resources that are shared between agencies.

Latency

Similarly, agencies need to understand the latency of the traffic across any networks they are intending to use. Business transactions requiring low latency may rule out the choice of particular software applications or prohibit the use of particular networks that cannot consistently meet appropriate levels of performance.

The Internet Gateway connects to the public Internet service which has no guaranteed latency or Quality of Service characteristics. The Cloud Gateway utilises a private network connection to the cloud exchange which can be configured with Quality of Service and monitored latency criteria.

Data Sovereignty

'As-a-service' offerings may utilise local infrastructure. On the other hand, the networks may cross national and international boundaries as many hosting arrangements involve use of resources in data centres worldwide. In this case it is important to understand the implications of the laws and legislation of international jurisdictions that are involved. Classification and appropriate protection of agency information and data assets is important to ensure that these assets remain secure in transit, as well as in storage.

Additional guidance around security of data can be found in Cloud Computing Security Considerations, Department of Defence (Australian Government).

Availability and reliability

Availability can be affected by many things, including external actions such as denial of service attacks or network contention or over-subscription of multi-tenanted resources.

Reliability can be affected by hardware and software failures. Service providers may encounter technical problems and configuration errors, resulting from poor software control or change management practices.

Agencies should assess a potential supplier's Service Level Agreement to ensure an acceptable level of system availability and quality of service. If the service requires a high level of availability or reliability (exceeding that offered by the supplier), an agency might need to negotiate for dedicated connections, isolated resources or customised services.

Redundancy

'As-a-service' suppliers to agencies need to build appropriate redundancy into their networks that reflect the criticality of the respective business applications. This may extend from local considerations (eg servers in a single site) right through to completely separate international network connections, capable of failing over in the face of interrupted services.

In light of their business continuity and disaster recovery plans, agencies need to identify what level and scope of service redundancy is required.

Data Encryption

In the planning stages of any outsourcing arrangement, agencies should give due consideration to the security, especially the confidentiality and sensitivity, of their data. Any information and data that is to be stored in the cloud must be classified in accordance with the Information Security Management Framework. This classification will determine whether encryption is required to protect data in transit or at rest (in storage).

Where to go for help

Agencies should discuss with DPC-ICT their business requirements for services that transit the various gateway infrastructure.

Agencies can request the Network Managed Service supplier to assist with design for network connectivity and integration with existing services.

References, Links & Additional Information

Links to various guidelines and papers, including those relevant to network considerations can be found in the Cloud Services Information Sheet.

Document Control

ID	DPC/G3.3
Version	1.1
Classification/DLM	Public I1-A1
Compliance	Discretionary
Original authorisation date	December 2016
Last approval date	November 2017
Next review date	November 2019