Technical

Note

Exaquantum Cloud Implementation

TN GMSCS0147-01E

Exaquantum

YOKOGAWA

Yokogawa Electric Corporation

Blank Page

Copyright and Trademark Notices

All Rights Reserved

The copyright of the programs and online manuals contained in the software medium of the Software Product shall remain with YOKOGAWA.

You are allowed to print the required pages of the online manuals for the purposes of using or operating the Product; however, reprinting or reproducing the entire document is strictly prohibited by the Copyright Law.

Except as stated above, no part of the online manuals may be reproduced, transferred, sold, or distributed to a third party in any manner (either in electronic or written form including, without limitation, in the forms of paper documents, electronic media, and transmission via the network).

Nor it may be registered or recorded in the media such as films without permission.

Trademark Acknowledgements

- CENTUM, ProSafe, Exaquantum, Vnet/IP, PRM, Exaopc, Exaplog, Exapilot, Exasmoc and Exarqe are registered trademarks of YOKOGAWA.
- Microsoft, Windows, Windows Server, SQL Server, Excel, Internet Explorer, SharePoint, ActiveX, Visual Basic, Visual C++, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- Adobe and Acrobat are registered trademarks of Adobe Systems Incorporated, and registered within particular jurisdictions.
- Ethernet is a registered trademark of XEROX Corporation.
- All other company and product names mentioned in this manual are trademarks or registered trademarks of their respective companies.
- We do not use TM or ® mark to indicate those trademarks or registered trademarks in this manual.
- We do not use logos in this manual.

Highlights

The Highlights section gives details of the changes made since the previous issue of this document.

Summary of Changes

This is R3.20 Issue 1.0 of the document related to Product Library version 3.0.

Detail of Changes

The changes are as follows:

Chapter/Section/Page	Change

Table of Contents

Glossary

Term	Description
Availability Group	A geographical location within the suppliers Cloud infrastructure for VMs etc. to be run. This may be chosen for reasons of digital security law, physical proximity to external resources or risk reduction
AWS	Amazon Web Services –Cloud Hosting service
Azure	Microsoft's Cloud Hosting service
Azure Premium Disk	High performance Disk capacity held on SSDs
CAMS	Consolidated Alarm Management System, an add in to the DCS that filters the Alarm and Event data to present it to the Operator
DCOM	Distributed Common Object Model – a Microsoft standard for inter process communication over a network
DCS	Distributed Control System
DNS	Domain Name Server
Exaquantum/ARA	Exaquantum Alarm Reporting and Analysis. An application to provide reports for Alarm and Event Messages collected by the Exaquantum Server to support analysis of the effectiveness of the Process Control System Alarm settings
Exaquantum/SER	Exaquantum Sequence of Events Recorder. An application that provides a Web User Interface for the display of Alarm and Event data and the capability to identify and report on trip events from Alarm and Event data
Exaquantum/RDS	Exaquantum Remote Data Synchronization. An application that transfers Tag and Alarm and event data from one Exaquantum Server to another over a single port TCP connection
Exaquantum/VPN	Exaquantum Virtual Private Network. An application that monitors the availability of an OPC server and then, when it is running, maintains the open state of a Microsoft VPN connection to a specified Exaquantum server to allow data collection
HDD	Hard Disk Drive (mechanical spinning disk)
IOPS	Input Output Operations per Second, a measure of disk performance
NAT	Network Address Translation – a function of Firewalls etc. where the packet Internet addresses are modified, hiding the original device address from external systems. A pool of addresses and port numbers are used dynamically as connections are made

Term	Description
OPC	Open Platform Communications, a series of standards and specifications for industrial telecommunication
PIMS	Plant Information Management System
SNAT	Static NAT – a 1:1 relationship between an internal network address and a single address on the Internet side of the firewall
SOE	Sequence Of Events
SSD	Solid State Disk
VM	Virtual Machine
VPN	Virtual Private Network. An encrypted software ‘pipe’ over a TCP network allowing private data transfer between its end nodes
Windows Domain	A Security unit allowing common users and user groups across multiple computers. Details are stored in Microsoft Active Directory database and managed through Domain Controllers

Chapter 1 Introduction

With the increasing acceptance and move towards cloud-based computing, Yokogawa have investigated a number of cloud installations and deployment scenarios for implementing Exaquantum, Yokogawa’s Data Historian solution and applications in the cloud.

To provide some practical examples, we selected two, widely recognized and commercially available public Cloud Platforms; Microsoft Azure and Amazon Web Services (AWS) to demonstrate and provide guidance on how to deploy Exaquantum in the Cloud.

The following describes best practices and recommendations for both Cloud platforms when deploying the following Yokogawa products in the Cloud.

This Technical Note is designed to explain the technical issues and limitations that have to be considered when implementing the following Yokogawa products on the Cloud.

- Exaquantum Historian
- Exaquantum/SER (Sequence of Events Recorder)
- Exaquantum/ARA (Alarm Reporting and Analysis)

Additionally, the following Yokogawa products are used for infrastructure management:

- Exaquantum/RDS (Remote Database Synchronization
- Exaquantum/VPN (Virtual Private Network)

Validation tests were run on the two most popular commercial Cloud Platforms – Microsoft Azure and Amazon Web Services (AWS). See Chapter 11 for details of the Tests Performed and the results.

Best practice details derived during the validation are provided for both Cloud Platforms used but there is no attempt to replicate the configuration documentation for them. The reader is assumed to have sufficient knowledge of their chosen platform to implement following these practices. For Azure see Chapter 9 and for AWS see Chapter 10.

The reader is assumed to already be proficient in the implementation of Exaquantum systems and aware of the hardware and networking impacts of these installations.

Chapter 2 Design and Implementation Process

The path to implementation of a Cloud Historian has to follow a series of design decisions:

1. What are we trying to achieve (See Chapter 3)
2. Which Cloud Platform will we use?
3. How will we connect the Cloud network to our on-premises system(s) (See Chapter 4)
4. How will the data be transferred to the Cloud system? (Direct OPC or Exaquantum/RDS from on-premises Exaquantum PIMS Server)
5. What other Yokogawa Applications will be used other than Exaquantum?
6. How will User Authentication be managed for Access Security (See Chapter 5)
7. How will Client Access to the Exaquantum Server be secured (See Chapter 6)

Then, during the implementation phases, specific configuration may be needed for:

1. The Exaquantum Server build (see Chapter 9 and Chapter 10)
2. Configuration of the main Exaquantum software will require reference to Section 8.1 and is subject to the limitations specified in Chapter 7
3. Configuration of Exaquantum/RDS if used will require reference to Section 8.3
4. Configuration of Exaquantum/VPN if used will require Reference to Section 8.2
5. Configuration of Exaquantum/SER if used will require reference to Section8.4 and is subject to the limitations specified in 7.2
6. Configuration of Exaquantum/ARA if used will require reference to Section 8.5 and is subject to the limitations specified in 7.3

Chapter 3 Business Cases

It is important to consider the justifications and business reasoning for implementing Exaquantum in the Cloud.

To assist, Yokogawa considered a number of scenarios and use cases for deploying Exaquantum, Yokogawa's Data Historian solution and applications from your existing install base on two mainstream public cloud platforms Amazon Web Services (AWS) and Microsoft Azure.

Yokogawa has tested some common deployment scenarios for implementing Exaquantum in the cloud. The aim was twofold, firstly to ensure that levels of performance can be maintained in a cloud environment when compared to a typical on-premises solution. Secondly, it was to confirm that data security and reliability measures were not impacted when deploying software solutions to the cloud.

3.1 Data Replicator

Cloud Exaquantum as a replicator or replacement of an on-premises historian system with one in the Cloud.

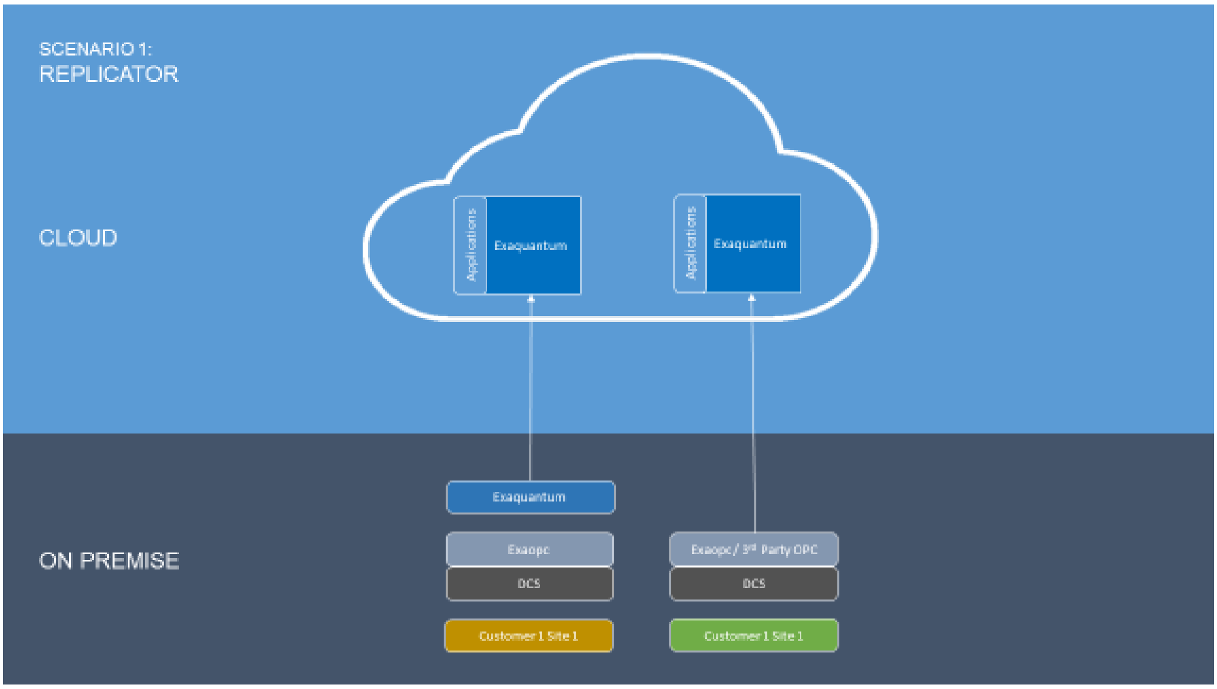


Figure 3-1 Replicator

The Exaquantum to Exaquantum link is realized using Exaquantum/RDS, to move tag and AE data on a periodic basis.

The OPC to Exaquantum Link is realized using the standard OPC DCOM link. This would usually be implemented over an Exaquantum/VPN managed VPN connection from the OPC Server to the Exaquantum Server.

3.2 Data Replicator / Aggregator

A Cloud Exaquantum aggregating data from multiple on-premises sources to one or more historian systems in the Cloud.

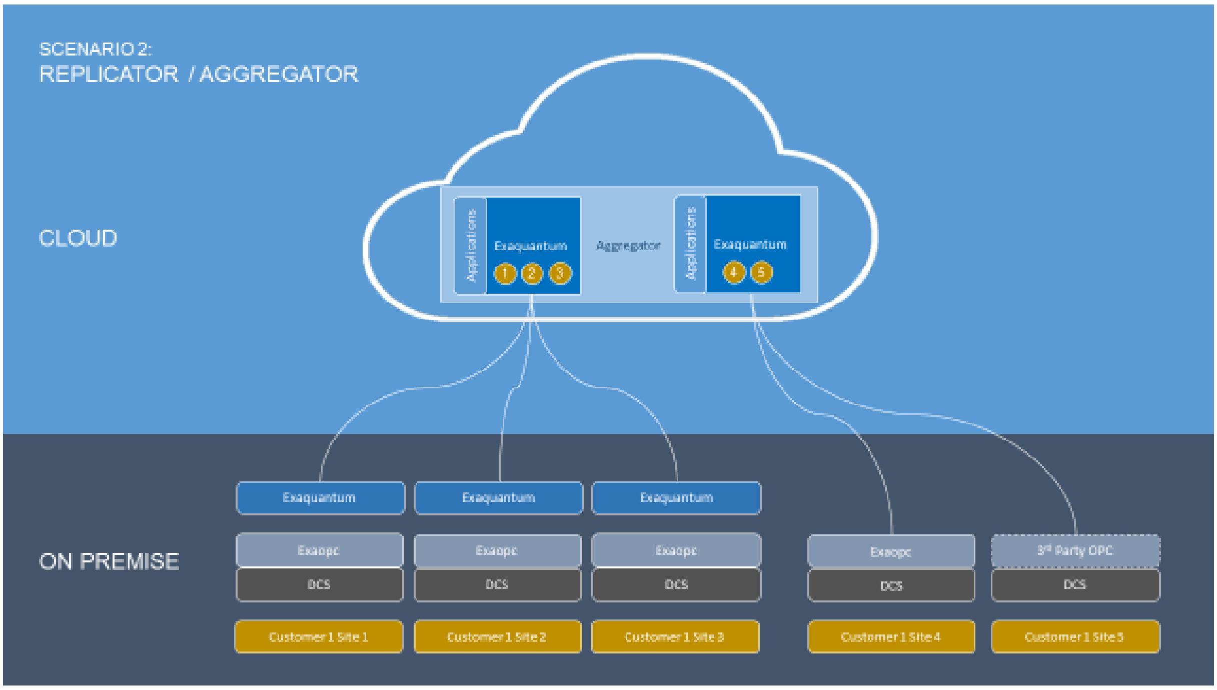


Figure 3-2 Aggregator

3.3 KPI Aggregator

A Cloud Exaquantum aggregating KPIs from multiple on-premises systems and storing them in one system in the Cloud.

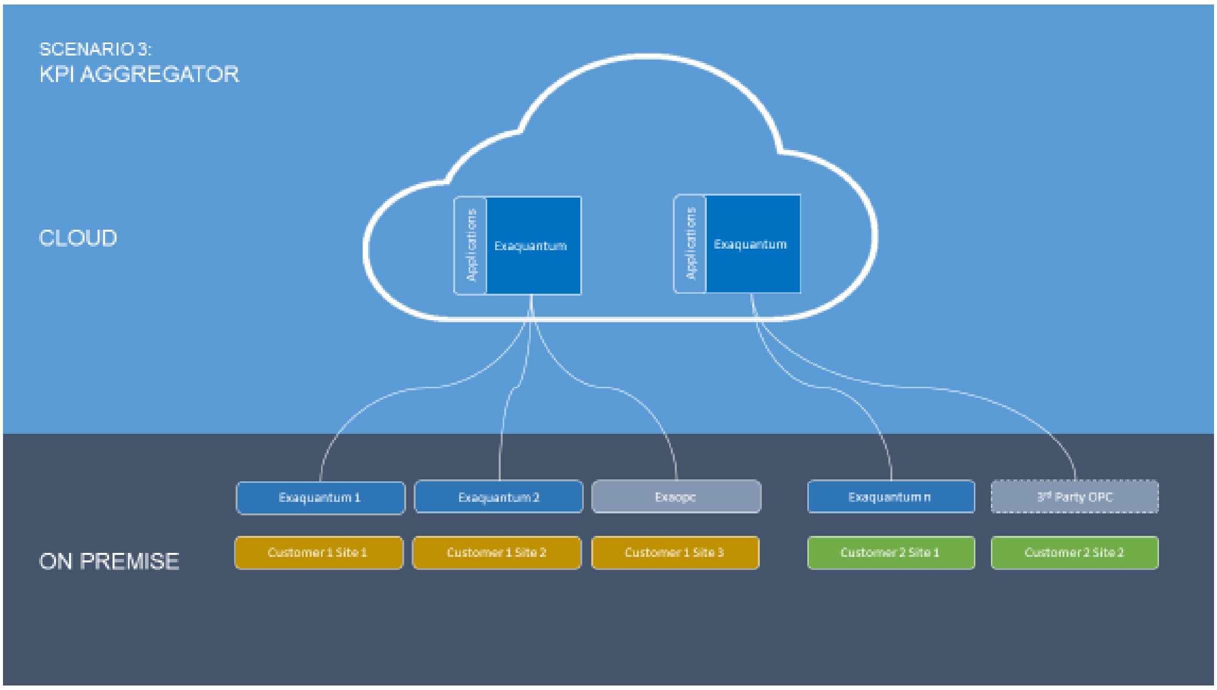


Figure 3-3 KPIs

Chapter 4 Network Connections

Having discussed the data source and storage locations, the next step is to consider how the On-Premise and Cloud networks will be linked. There are two Logical Network configurations available between the On-premises network to the Cloud Network/Servers:

1. Permanent VPN connection managed by AWS/Azure – the Cloud network becomes part of the customer's own internal network without any direct exposure to the Internet.

2. Public IP Addresses for Cloud Servers requiring that the on-premise system has access to the internet and the Cloud system is exposed to the Internet.

These options are expanded below:

- Option 1 allows a greater number of On Premises systems to connect but exposes the in Cloud servers to the Internet, requiring additional security set-up
- Option 2 has limitations in the number of separate On Premises systems able to connect to the Cloud network (typically 10)

4.1 Cloud Servers in Private Cloud Network linked to Customer Network by Permanent VPN

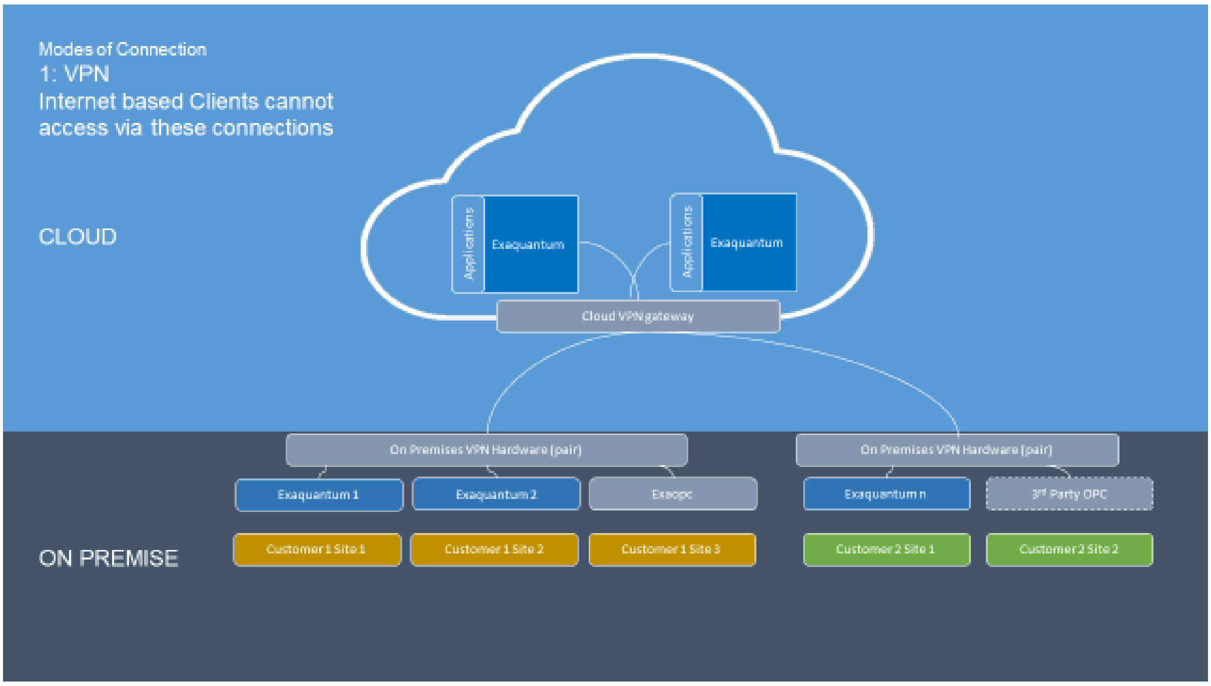


Figure 4-1 VPN to On-Premises Network

This approach establishes a private pipe between the customer's on-premises network(s) and the Cloud virtual network. There is no need for a public IP address for the Exaquantum server with all traffic over 'internal' networks. The VPN becomes a single point of failure but can be configured with failover sets (details dependent on the Cloud provider).

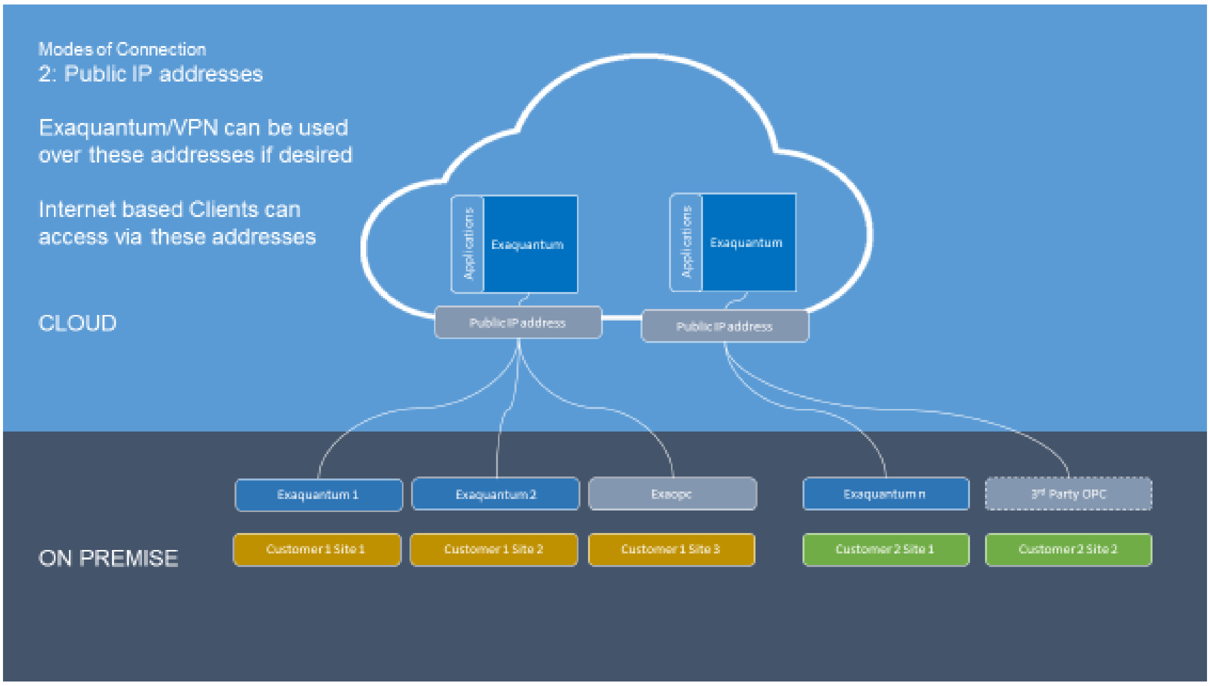
There are limitations in the number of separate VPN connections that can be made from customer sites to the VPN gateway managed by the Cloud provider and on the total bandwidth available. These limits are Azure 30, AWS 10 so making this approach non-viable for implementations with many customer sites that are not part of a contiguous network hence all needing to be separately connected to a single Exaquantum Cloud server.

See 6.1.2 for details of configuring permanent VPN connections.

There is the possibility of implementing connections using Windows Routing and Remote Access as used for OPC to Exaquantum links outlined in section 4.2 though now including inter-network routing. This is less resilient and less efficient than the managed services but can provide more links through multiple windows VMs on the same subnet.

+ The Servers are not exposed to the Internet, security is retained within the customer's own boundaries.
- Internet Clients are not able to connect to the Servers without linking directly via VPN to the customer network.
- There are limits to the number of connections that may be made to a single VPN Gateway which may be too low for geographically dispersed site bases.

4.2 Cloud Servers with Public IP Addresses



Modes of Connection

2: Public IP addresses

Exaquantum/VPN can be used over these addresses if desired

Internet based Clients can access via these addresses

Figure 4-2 Public IP Addresses and VPNs

- + In both Azure and Amazon Web Services, Public IP addresses are implemented by use of a Static Network Address Translation. SNAT means that all traffic for a specific Public IP address is passed on to a specific VM, with the destination address changed to the VM’s internal address in the virtual Private Network, the reverse translation occurs to outbound packets
- + Clients on the Internet may access the Servers directly as desired
- + There is no limit to the number of on-premises locations that can connect to the Cloud
- - The servers are exposed to the Internet and detailed firewall configuration is needed to protect them

Chapter 5 Security – Authentication Options

Exaquantum and the Exaquantum Applications are designed with the use of windows user authentication and Windows group membership for authorization. Implementing Exaquantum in the Cloud requires consideration of how to provide and administer this functionality in this context.

There are a number of options available depending on the Cloud platform to be used. Detailed information on setting these models up are to be found in the AWS and Azure documentation.

All tests performed for this paper have been under the ‘Local Users’ model, see section 5.1 and the Standard IT security setup

5.1 Local Users

This option relies on local users provisioned on the Exaquantum server in the Cloud. All users will have to log in manually when connecting to the website using one of the server’s local users and would not be able to manage their passwords. The Exaquantum Excel Add-in can be configured to log in with a user/password other than the local client login.

+ The simplest solution to configure at the time of Exaquantum system creation
+ Requires no set-up or management of new Active Directory or Single Sign On infrastructure

- More user administration work (initial user provisioning, password changes)
- Requires local client configuration on each change of password (Excel Add-in)

5.2 Windows Domain

This assumes that the user wishes to leverage their existing Microsoft Active Directory infrastructure for the provisioning of Users and, possibly, the allocation of access rights on the Exaquantum applications to those users.

5.2.1 Access On-Premises Active Directory Servers from the Cloud Directly (Either Cloud Supplier)

This model sees the Cloud servers becoming members of an On-Premises Active Directory Domain.

DNS servers for the On-Premises system need to be available to the Cloud systems.

Here are two options for providing the connection to the On-Premises Active Directory/Domain Controllers:

- The simplest and most secure method is to have a permanent VPN link between the Virtual Private Cloud and the On-Premises network, thus removing the exposure of the On-Premises Domain Controllers to any Public IP address ranges.
- If the connection is provided over Public IP addresses rather than a VPN connection, the in-premises Domain Controller and DNS servers have to be accessible from the Internet even if only from the addresses of the Cloud Exaquantum Server(s).

+ User provisioning and group allocation is performed in the customer’s own domain following existing internal procedures

+ Single Windows Sign On for all users

+ User management of password changes

+ No need to use ‘stored’ username/password for Excel etc. or for the connection to websites

- Client requires permanent VPN connection, this may be in addition to an internet gateway to allow client access through a public IP address

- Performance for user authentication and authorization may be impaired by the AD queries being routed over the VPN

- VPN availability becomes a point of failure for client access to the system, though data collection and running of core Exaquantum functions is all based on local users

5.2.2 Extend Local Active Directory to the Cloud (Either Cloud Supplier)

This is an extension of 5.2.1 with Windows Active Directory Domain Controllers implemented in each availability group. These are used by the host servers in the Cloud allowing the Exaquantum AD Authorization checks to be performed ‘locally’ within the data centre(s) of that availability group.

+ User provisioning is performed in the customer’s own domain following existing internal procedures
+ Single Windows Sign On for all users
+ User management of password changes
+ No need to use ‘stored’ username/password for Excel etc. nor for connection to websites
+ User authentication and authorization performed locally to the Exaquantum server thus faster
+ VPN availability is not a point of failure for client access to the system
- Recommended to have a permanent VPN connection. This may be in addition to an internet gateway to allow access through a public IP address for client access
- Domain Controllers are now outside the in-premises network, something which must be considered in global security risk reviews

5.2.3 Azure Active Directory – Linked to Local Active Directory (Microsoft Azure)

In this case, the Azure Active Directory is configured to replicate a limited subset of the users and groups (via an Azure AD Connect) to an Azure Active Directory Domain, The passwords can be set to remain synchronized with those of the on-premises domain. Thus user can log in using the same username and password as for their on-premises, however they log in for a different domain name when accessing the Exaquantum system.

5.2.4 Trust relationship between an Amazon Web Services hosted Active Directory and Local Active Directory (Amazon Web Services)

AWS provide the option of a managed Active Directory Domain(s), this can then have a trust relationship with the in-premises Active Directory Domain(s). Authentication of users from the On-Premises domain will occur on the On-Premises domain controllers (unless by Kerberos). This really requires a permanent VPN link as in 5.2.1. The Exaquantum server in the Cloud would be a member of the AWS managed domain.

+ User provisioning is performed in the customer’s own domain following existing internal procedures. However, management of group memberships is performed on the Cloud

+ Single Windows Sign on for all users

+ User management of password changes

+ No need to use ‘stored’ username/password for Excel etc. nor for connection to websites

- Recommended to have a permanent VPN connection. This may be in addition to an internet gateway to allow access through a public IP address for client access

- Performance for user authentication but not authorization may be impaired by the AD queries being routed over the VPN

- VPN availability becomes a point of failure for client access to the system, though data collection and running of core Exaquantum functions is all based on local users

- Group membership management occurs on the AWS managed domain, additional level of complexity for user control by customer IT

5.2.5 Trust Relationship between Locally Managed Active Directory and On-Premises Active Directory (Either Cloud Supplier)

This is identical to Section 5.2.4 other than that the entire AD infrastructure is the responsibility of the Cloud Administrator.

5.3 3rd Party Single Sign-On Options

Third Party Single Sign On infrastructures exist but would have to be carefully considered for their compatibility with Exaquantum’s Windows User/Server requirements, particularly for the management of the Excel Add-in.

Chapter 6 Connection to Cloud Servers and Firewall Setup

The firewall settings required are common across all Cloud Hosting Services, though the mechanisms to set them up vary.

6.1 Public IP addresses

For this section, the source IP addresses will be for the public IPs that represent the clients, OPC server sources, etc. If there are NAT firewalls between these end nodes and the Cloud then it is the external Internet IP address for the outermost NAT firewall in each case.

For Azure, the configuration is set in a Network Security group attached to a virtual network subnet or a network interface on a Virtual Machine.

For AWS, the Firewall configuration is set in the Security Groups linked to the Cloud Exaquantum Server.

To avoid any case of unencrypted traffic being passed over the internet during data collection, the following steps should be taken:

1. All links from Exaopc servers to the Exaquantum server should be passed over an encrypted VPN connection
2. Exaquantum/RDS links are automatically encrypted. It is recommended to change from the default empty key string when configuring the Exaquantum/RDS Publisher and Consumer nodes

Client access encryption would rely on one of:

1. Exaquantum and other Application websites being configured for HTTPS not HTTP
2. Establishing a VPN connection from the Web Client to the Cloud Exaquantum server prior to accessing the data. This could be provided in the same way as for the OPC to Exaquantum Server links
3. Using the point to Virtual Private Network links offered by either Azure or Amazon Web Services

6.1.1 Exaquantum/RDS

The following inbound rules are required in the set of security groups relevant to the Cloud Exaquantum Server:

6.1.1.1 Client and Web Access

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80 or 8000 if all application websites on the Exaquantum website	Where ever there are clients for the websites	Inbound HTTP requests– not needed if all web sites are HTTPS. If the Exaquantum website was configured with a port other than 8000 use that here.
HTTPS	TCP	443 or chosen HTTPS port	Where ever there are clients for the websites	Inbound HTTPS requests – only needed if the websites are configured for SSL
Custom TCP Rule	TCP	34487	Where ever there are clients for the websites	OPC UA access for Excel Add in – this is the default but could be changed in the OPC/UA server configuration

6.1.1.2 Exaquantum/RDS connection

Type	Protocol	Port Range	Source	Description
Custom TCP Rule	TCP	5000	Where the Exaquantum/RDS Publisher servers are	This is the default but any port can be chosen when setting up the RDS consumer on the Cloud Server, all Publishers must use the same port.

6.1.1.3 Administrator RDP access

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Where the Administration Clients are	RDP links

6.1.2 VPN and OPC Direct

The following inbound rules are required in the set of security groups relevant to the Cloud Exaquantum Server:

6.1.2.1 Client and Web Access

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80 or 8000 if all application websites on the Exaquantum website	Where ever there are clients for the websites	Inbound HTTP requests– not needed if all web sites are HTTPS If the Exaquantum website was configured with a port other than 8000 use that here
HTTPs	TCP	443 or chosen HTTPS port	Where ever there are clients for the websites	Inbound HTTPS requests – only needed if the websites are configured for SSL
Custom TCP Rule	TCP	34487	Where ever there are clients for the websites	OPC UA access for Excel Add in – this is the default but could be changed in the OPC/UA server configuration

6.1.2.2 VPN connection – L2TP

NB. An SSTP VPN only Requires Port 443

Type	Protocol	Port Range	Source	Description
Custom UDP Rule	UDP	1701	Where the OPC servers are	To support L2TP Link
Custom UDP Rule	UDP	4500	Where the OPC servers are	To support L2TP Link
Custom UDP Rule	UDP	1500	Where the OPC servers are	To support L2TP Link

6.1.2.3 Administrator RDP access

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Where the Administration Clients are	RDP links

6.2 VPN Gateway Customer to Cloud Virtual Network

This configuration sees the Cloud subnet(s) linked over a VPN pipe to the on-premises network. No public/external IP addresses are involved. The level of security applied to the inbound traffic on the Cloud subnet may be lower than for an Internet facing configuration. This section assumes that the minimum exposure is required.

For this section the source IP addresses will be for the internal network IPs that represent the clients, OPC server sources etc. If there are NAT firewalls between these end nodes and the Cloud, then it is the external IP address for the closest NAT firewall.

For Azure the configuration is set in a Network Security group attached to a virtual network subnet or a network interface on a Virtual Machine.

For AWS the Firewall configuration is set in the Security Groups linked to the Cloud Exaquantum Server.

6.2.1 Exaquantum/RDS

The following inbound rules are required in the set of security groups relevant to the Cloud Exaquantum Server:

6.2.1.1 Client and Web Access

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80 or 8000 if all Application websites on the Exaquantum website	Where ever there are clients for the websites	Inbound HTTP requests– not needed if all web sites are HTTPS If the Exaquantum website was configured with a port other than 8000 use that here
HTTPs	TCP	443 or chosen HTTPS port	Where ever there are clients for the websites	Inbound HTTPS requests – only needed if the websites are configured for SSL
Custom TCP Rule	TCP	34487	Where ever there are clients for the websites	OPC UA access for Excel Add in – this is the default but could be changed in the OPC/UA server configuration

6.2.1.2 RDS Connection

Type	Protocol	Port Range	Source	Description
Custom TCP Rule	TCP	5000	Where the Exaquantum/RDS Publisher servers are	This is the default but any port can be chosen when setting up the RDS consumer on the Cloud Server, all Publishers must use the same port.

6.2.1.3 Administrator RDP access

Type	Protocol	Port Range	Source	Description

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Where the Administration Clients are	RDP links

6.2.2 VPN and OPC Direct

The following inbound rules are required in the set of security groups relevant to the Cloud Exaquantum Server:

6.2.2.1 Client and Web access

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80 or 8000 if all application websites on the Exaquantum website	Where ever there are clients for the websites	Inbound HTTP requests– not needed if all web sites are HTTPS If the Exaquantum website was configured with a port other than 8000 use that here
HTTPs	TCP	443 or chosen HTTPS port	Where ever there are clients for the websites	Inbound HTTPS requests – only needed if the websites are configured for SSL
Custom TCP Rule	TCP	34487	Where ever there are clients for the websites	OPC UA access for Excel Add in – this is the default but could be changed in the OPC/UA server configuration

6.2.2.2 VPN connection – L2TP – SSTP only Requires Port 443

Type	Protocol	Port Range	Source	Description
Custom UDP Rule	UDP	1701	Where the OPC servers are	To support L2TP Link
Custom UDP Rule	UDP	4500	Where the OPC servers are	To support L2TP Link
Custom UDP Rule	UDP	1500	Where the OPC servers are	To support L2TP Link

6.2.2.3 Administrator RDP access

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Where the Administration Clients are	RDP links

Chapter 7 Limitations to Application Usage

7.1 General Limitations to the Exaquantum/PIMS Usage

7.1.1 Recommended Exaquantum version

It is recommended that the latest officially released version of Exaquantum with all mandatory patches installed is used in the cloud environment.

7.1.2 Legacy Website is not supported

The legacy website is not supported over the network connection supported by AWS or Azure and any attempt to use the SOAP web service fails.

7.2 General Limitations to Exaquantum/SER Usage

7.2.1 Trip Generation

No Trips can be generated if AE Data arrives over Exaquantum/RDS.

If the AE data is being delivered to the Cloud server over Exaquantum/RDS, it is placed directly into the SQL database rather than arriving through the usual AEPump route. This bypasses the Exaquantum Event Handler which is used to initiate the generation of Exaquantum/SER Trip reports. The Exaquantum/SER SOE display functions will work as long as the OPC Gateways have been configured to collect AE data, even though they will not be able to connect to any OPC Servers.

7.3 General Limitations to Exaquantum/ARA Usage

7.3.1 ARA Processing offset

ARA Processing must be offset significantly to allow for late arriving AE Data over Exaquantum/RDS.

When the AE data is arriving on the Cloud Exaquantum Server over an Exaquantum/RDS link, it is not guaranteed to be up to date all the time. It comes in blocks of, typically, 2 minutes depending on the configuration of the Exaquantum/RDS publisher providing it. Additionally, events on the publisher(s) and contention on the network links between Exaquantum/RDS Publishers and Consumer may delay the transfer of the data, though all will arrive eventually.

Exaquantum/ARA by default, will process all the AE in the historian for a particular hour at 10 minutes past the hour and will not revisit that period even if new data was to arrive after processing. The only way to process late arriving data for a time period that has been ‘passed’ is to clear the Analysis Services Cube and reprocess all data from a defined ‘start of reporting’ point. This takes some time though it is performed from the latest hour backwards, allowing report access to recent data first.

Hence, to minimize the chance of processing a period prior to the arrival of the data from one or more Exaquantum/RDS Publishers, ARA should be configured to process with a greater offset than the default 10 minutes, perhaps 1 hour 10 minutes at a minimum. See Section 8.5.2 for details.

Chapter 8 Yokogawa Application Configuration

8.1 Exaquantum

Exaquantum data server configuration is no different on the Cloud than in an internal network, other than the fact that it is not recommended to offer thick client and administrator access to remote clients over the internet. All configuration should be done locally using RDP (Remote Desktop) connections.

For details of setting up Gateways using VPN connections, see the Exaquantum/VPN Engineering Guide and section 8.2.

8.1.1 Standard Set-Up

Exaquantum tag creation and OPC Gateway setup follows the Exaquantum PIMS User Guide and the Exaquantum Engineering Guides.

8.1.2 Archiving

Archiving has to be to disk-based Backup Devices which have to be managed manually as they grow.

8.2 Exaquantum/VPN

Configuring the Exaquantum Server as a Windows Routing and Remote Access Server (RRAS) capable of acting as the termination for client connections is described in the Exaquantum/VPN Engineering Guide (IM36J40F35-01EN).

Once the RRAS is configured and individual users created with static IP addresses for each remote OPC server, the Exaquantum system can be configured with the Static IP addresses in each OPC Gateway configuration.

8.2.1 Choice of VPN type

There are a number of VPN protocols offered by Windows Routing and Remote Access:

Protocol	Comments
PPTP	This cannot be used as it requires a protocol (GRE) to be allowed through the firewalls other than TCP and UDP which are the only ones allowed by Azure
L2TP	This also needs a protocol (ESP) by default, but setting registry keys as described below restricts it to using UDP port access. If a shared private key is configured then no Server Certificates are required for authentication
SSTP	This is Secure Sockets based and requires the RARAS server to have a Server certificate configured
PPPOE	This is not supported for inbound VPN connections so not usable
IKEv2	Again this requires a protocol (ESP)

From the above it can be seen that only L2TP and SSTP are usable in this context. L2TP is simpler to configure as it does not require a Server Certificate. However, if you are configuring the Websites for HTTPS you will need one anyhow.

The tests performed during the production of this document were configured using L2TP with a shared Private Key.

8.2.2 Setting up L2TP

When using L2TP through NAT firewalls, the following Registry keys must be created and set on all clients:

HKLM/System/CurrentControlSet/Servers/PolicyAgent/AssumeUDPEncapsulationContextOnSendRule (DWord) = 2

This allows for both the Client and the Server being behind NAT firewalls by only using UDP protocols for communication

You must also ensure that the Windows firewall on the Cloud server has the ‘RARAS L2TP in’ inbound rule enabled.

8.3 Exaquantum/RDS

When configuring Exaquantum/RDS Consumer on the Cloud Exaquantum Server, ensure that the Port Number and Encryption Key match with the Publishers and that the Port Number is included in the Cloud firewall configuration (see Sections 6.1.1, 6.2.1).

For details of setting up RDS Consumer and the matching RDS Publishers on-premises, see the Exaquantum/RDS Engineering Guide.

8.4 Exaquantum/SER

There is no special configuration required when the Exaquantum server is collecting OPC data directly.

8.4.1 Configuration for RDS Sourced Data

Where the A&E data is being collected over RDS, the ‘RDS Consumer end’ OPC Gateways that the AE data is linked to on delivery have to be configured to ‘collect AE data’. This will lead to some error messages in the Application Event log, as the named OPC servers will not be accessible but will not impact on the delivery of the data by RDS. If this is not done, the Exaquantum/SER SOE display will not show any data for these Gateways.

8.5 Exaquantum/ARA

When configuring Exaquantum/ARA on a Cloud based Exaquantum server that is directly collecting OPC AE data over VPN connections or through a permanent VPN connection from Cloud to on-premises network, it should be configured as per the Exaquantum/ARA Engineering and User Guides.

8.5.1 CAMS Interface

If a directly connecting Exaquantum/ARA system is connecting to a CAMS enabled DCS with the classic Exaopc server, the HIS must have a VPN connection to the Cloud Exaquantum Server to allow the ARA processing to collect the CAMS Hisdump data during hourly processing.

If Exaopc/CAMS is in use, there is a choice on how the link to the HIS is implemented since this is to mainly static data on shelves etc.:

1. The share may be accessed via a dynamic VPN link from the HIS allowing access to the live configuration file
2. If the security environment does not allow links to the control level, a copy of the configuration file can be copied to the Cloud server and referenced directly there

Option 2 requires that the copied file be updated if changes were made to the shelving configuration on the DCS.

8.5.2 Configuration for Exaquantum/RDS Sourced Data

When the AE data is being received over an Exaquantum/RDS link, it cannot be assumed to be directly up to date and the hourly update job must be further offset from the standard 10 minutes. This is achieved by amending the Process offset column in the ARA.Boundarytimes column in the QApplicationData database. The value is the number of minutes behind to process the data. The default value is 10, so at 10 past the hour the previous complete hour is processed (-70 to -10). If this is amended to, for example, 70, then at 10 past the hour the data from –130 to -70 minutes is processed.

If the source DCS is running CAMS and the AE data is being collected via Exaquantum/RDS, this can only be supported where the Exaopc/CAMS server is in use since the HIS is not available for collection of data using Hisdump. A copy of the Configuration file for the shelving must be copied to the Cloud Exaquantum server and then this configured to support CAMS processing in ARA.

Chapter 9 Azure Configuration

9.1 Operating System

When creating a Virtual Machine from the Azure console, the only Windows server edition available is Datacenter. Exaquantum is not supported on this edition and whilst the installation will run successfully, the start-up will fail when initiated from the Exaquantum Service Manager. As a result, to implement an Exaquantum server on Azure, the following more circuitous route must be followed:

1. Create a VHD (Virtual Hard Disk). Make this as small as you can achieve, 20GB, to reduce the data volume to be transferred in step 3
2. Ensure that the VHD is licensed, fully patched, has Remote Desktop enabled, is a VHD type 1.0 and of fixed size
3. Upload it to a Premium (SSD) Storage Group
4. Expand the VHD to 64 or 128GB (pricing is in bands 32/64/128/256/512 etc. and intermediate sizes are charged at the next boundary up)
5. Create a VM using this as the OS disk

Details of steps 3 and 5 can be found at:

https://blogs.infosupport.com/creating-a-vm-in-azure-based-on-an-uploaded-vhd/

Note: This procedure must be performed from PowerShell, the Azure portal does not provide support for these steps.

9.2 Hardware Options (CPU/Memory)

The CPU speed, core count and memory configuration should follow that specified in the Exaquantum GS (GS36J04A1-01E_027). See https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes for details of current Azure sizes.

No. of tags	Azure size suggested	Specification
Less than 20,000	Standard_D2s_v3	8GB RAM, 2 x 2.4GHz Xeon E5-2673 max 4 disks premium storage (SSD)
20,000 – 50,000	Standard_D4s_v3	16GB RAM, 4 x 2.4GH Xeon E5-2673 max 8 data disk premium storage (SSD)
50,000 – 100,000	Standard_D8s_v3	32GB RAM, 8 x 2.4GHz Xeon E5-2673 max 16 data disk premium storage (SSD)
100,000 – 300,000	Standard_D16s_v3	64GB RAM, 16 x 2.4GHz Xeon E5-2673 max 32 data disk premium storage (SSD)
300,000-500,000	Standard_D16s_v3	64GB RAM, 16 x 2.4GHz Xeon E5-2673 max 32 data disk premium storage (SSD)

9.3 Data Storage Options

The recommended disc configuration depends on the update rates for new data expected. Premium disk throughput is dependent on disk size (https://docs.microsoft.com/en-us/azure/virtual-machines/windows/premium-storage-performance).

Update rate (updates/second)	Suggested Disc configuration
Less than 2,000	1 premium (SSD) disk of at least 128GB
2,000-5,000	3 disks: OS of 128GB, SQL of at least 1024GB and Archives of at least 1024GB
5,000-10,000	4 disks: OS of 128GB, SQL Data files of at least 2048GB or RAIDed smaller disks, enable Read cache, SQL Log of at least 2048GB or RAIDed smaller disks, enable Read cache, Archives of at least 2048GB or RAIDed smaller disks, enable Read cache.

9.4 System Scaling over Lifetime

As the hardware requirements (CPU/RAM or disk space) of a Cloud based VM increase over its life, these may be increased from the Azure Portal.

Disk space may be increased on a drive by drive basis, but the CPU and RAM may only be changed by amending the ‘size’ of the VM to one of the standard sizes offered by Azure.

9.5 Public IP Addresses

Where Public IP addressing is being used, user and data source facing systems require public IP addresses to be configured. IP addresses can be configured as either:

- Dynamic - they are reallocated and may change when the VM is stopped/deallocated.
- Static - they remain with the VM while it exists.

You pay for the Public IP address all the time you are holding onto this resource.

9.6 Other Options

Consideration must be given to the long term backup of Archives and the backing up of servers. Options for the long term backup of archives would be:

1. Copy the backup file from the Cloud to an on-premises system
2. Maintain an additional VM, without a public IP, with extensive non premium disk storage. Transfer files as required from the Exaquantum Server

9.7 Configuring Permanent VPN Connections

The outline of the process is described in https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

You will need a VPN device at the on-premises end to make the connection to the Azure Cloud. Supported devices and software versions are described in https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices. While sample configurations are available from Microsoft. You will require a competent network engineer to configure the device.

Chapter 10 AWS Configuration

10.1 Operating System

When creating a Virtual Machine from the AWS Console, any of the standard Exaquantum Operating systems may be selected:

For R3.20:

- Windows 2012 Standard Edition
- Windows 2012 R2 Standard Edition
- Windows 2016 Standard Edition

10.2 Hardware Options (CPU/Memory)

The CPU speed, core count and memory configuration should follow that specified in the Exaquantum GS (GS36J04A1-01E_027). https://aws.amazon.com/ec2/instance-types/ for details of current AWS sizes.

No. of tags	AWS Instance type suggested	Specification
Less than 20,000	T2.large	8GB RAM, 2 x 2.4GHz Xeon)
20,000 – 50,000	T2.xlarge	16GB RAM, 4 x 2.4GH Xeon
50,000 – 100,000	T2.2xlarge	32GB RAM, 8 x 2.4GHz Xeon
100,000 – 300,000	M5.4xlarge	64GB RAM, 16 x 2.4GHz Xeon
300,000-500,000	M5.4xlarge	64GB RAM, 16 x 2.4GHz Xeon E5-

10.3 Data Storage Options

The recommended disk configuration depends on the update rates for new data expected. Elastic Block Storage units host volumes and the throughput is limited by size. Gp2 delivers 3 IOPS per GB and max of 160 MB/sec you pay for the volume. io1 offers 50 IOPS/GB and 500 MB/sec and you pay for the access as well as the volume. See https://aws.amazon.com/ebs/details/ for details.

St1 volumes are traditional HDD discs with 250MB/sec per TB MB/s but lower IOPS and hence a good fit to SQL Log files.

Update rate (updates/second)	**Suggested Disc configuration**
Less than 2,000	1 volume EBS gp2
2,000-5,000	3 disks: OS gp2, SQL gp2 and Archives gp2
5,000-10,000	4 disks: OS gp2, SQL Data io1, SQL Log of st1, Archives io1

10.4 System Scaling over Lifetime

As the hardware requirement (CPU/RAM or disk space) of a Cloud based VM increases over its life these may be increased from the AWS Portal.

Disk space may be increased on a drive by drive basis but the CPU and RAM may only be changed by amending the ‘instance type’ of the VM to one of the standard instance types offered by AWS.

10.5 Public IP Addresses

Public IP addresses can either be dynamically allocated or static, the latter through the use of ‘Elastic IP addresses’ which incur a charge even if they are not attached to a running VM instance at the time.

10.6 Other Options

Consideration must be given to the long term backup of Archives and the backing up of servers. Options for the long term backup of archives would be:

1. Copy the backup file from the Cloud to an on-premises system
2. Maintain an additional VM without a public IP with extensive HDD sc1 disk storage. Transfer files as required to the Exaquantum Server

10.7 Configuring Permanent VPN Connections

The process to create a VPN connection is described in https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html. You are recommended to use a tested VPN device (see https://aws.amazon.com/vpc/faqs/#C9) to manage the on-premises end of the link for which sample configurations are available from Amazon. You will require a competent network engineer to configure the device.

Chapter 11 Tests Performed and Results

11.1 Hardware Configurations

For both Amazon Web Services and Azure, similar configurations were chosen to support the 7,250 tags and high AE count described in section 11.3.

In each case, a 50GB SSD Boot drive and a 300GB SSD data drive was chosen.

Azure: a general purpose 'Standard D4s v3' instance with 16GB of RAM and 4 virtual CPUs based on 2.4 GHz Intel Xeon® E5-2673 v3. Disk is managed Premium LRS SSD.

Amazon Web Services: a general purpose 't2.xlarge' instance with 16GB of RAM and 4 virtual CPUs based on Xeon processors 'up to 3.0GHz'. Disk is EBS (Elastic Block Storage) GP2 SSD.

11.2 Server Configurations Validated

Two modes of connection between the Cloud and the data sources were validated:

1. Exaquantum/RDS from Local Exaquantum to Exaquantum in the Cloud
2. Exaquantum/VPN Connections from Local Exaopc to Exaquantum in the Cloud

Both examples are shown in the Figures in Chapter 4.

Windows 2012 R2 was used in each case with Exaquantum R3.02 and corresponding versions of other Yokogawa applications.

11.3 Tag and AE Configuration

All tests worked with the same set of Tags and source Exaopc Servers

- 2 Exaopc Servers with the DJC test project
- 1 Exaopc CAMS server with the CAMS test project

Tags setup

- 500 1 second tags from each DCS Tag Simulation project
- 1,000 5 second tags from each DCS Tag Simulation project
- 1,500 10 second tags from each DCS Tag Simulation project
- 4,000 60 second tags from each DCS Tag Simulation project
- 240 1 second tags from the CAMS project

A&E rate approx. 28,000 per hour made up of:

- 16,000 Process alarms from the DCS Tag Simulation projects
- 12,000 CAMS process alarms from the CAMS project

11.4 Tests Performed

Trials were performed for Data Collection and History Catch Up. The following pass/fail tests were performed:

11.4.1 Exaquantum PIMS

AE Data Collection via OPC to Cloud

AE Data Collection via Exaquantum/RDS and local Exaquantum Publisher to the Cloud RDS Consumer

Tag Data Collection via OPC to Cloud

Tag Data Collection via Exaquantum/RDS and local Exaquantum Publisher to the Cloud RDS Consumer

History Catch for direct OPC collection

History Catch Up for Exaquantum/RDS connections following RDS Publisher and Consumer downtimes

Web Client Access to the Cloud to both Public and VPN Gateway connected Cloud Servers

Web Excel Add-in access to the Cloud to both Public and VPN Gateway connected Cloud Servers

11.4.2 Exaquantum/SER

For all configurations, access to the SER SOE Web interface was checked.

For the Direct OPC connections, access to the SER Trip Interface and the generation of trips was checked, but not for Exaquantum/RDS configurations as described in Section 7.2.1.

11.4.3 Exaquantum/ARA

Web Client access was checked for all configurations.

CAMS collection of the Shelving Configuration was tested for OPC connections using the following configurations:

1. Access to the CAMS HIS directly over a VPN
2. A local copy of the shelving configuration held on the Cloud server

CAMS collection for the Exaquantum/RDS connection was only tested with a local copy of the shelving configuration file.

Exaquantum/RDS configurations had the regular update job offset by 60 minutes to allow for delays in data collection as described in Section 8.5.2.

11.5 Test Results

	AWS				Azure			
	VPN		Public IP		VPN		Public IP	
	RDS	OPC	RDS	OPC	RDS	OPC	RDS	OPC
Exaquantum/PIMS								
Tag Data Collection	Pass	Pass	Pass	Pass			Pass	Pass
AE Data Collection	Pass	Pass	Pass	Pass			Pass	Pass
History Catch Up	Pass	Pass	Pass	Pass			Pass	Pass
Client Access. Web and Excel	Pass	Pass	Pass	Pass			Pass	Pass
Network and Hardware Load	Pass	Pass	Pass	Pass			Pass	Pass
Exaquantum/SER								
SER Trip Generation		Pass		Pass				Pass
Client to SOE	Pass	Pass	Pass	Pass			Pass	Pass
Client to Trip		Pass		Pass				Pass
Exaquantum/ARA								
CAMS Interface Direct Link	Pass	Pass	Pass	Pass			Pass	Pass
CAMS Interface local shelving	Pass	Pass	Incomplete	Pass			Pass	Pass
Client Access	Pass	Pass	Incomplete	Pass			Pass	Pass

Items with a grey background were not trialed.

The Azure VPN Gateway connection could not be configured to work with available Cisco ASA firewall errors were reported in the configuration downloaded from the Azure configuration tool when applied to the Cisco ASA device. As a result the permanent VPN gateway tests were not performed for Azure but only for Amazon Web Services.

All Pass/Fail tests executed passed.