

**AWS**

**Informatica MDM**

**Provisioning Kickstart Checklist**

|  |  |
| --- | --- |
| **Customer:** |  |
| **Location/Address:** |  |
| **Date:** |  |
| **Purchase Order number:** |  |

Contents

[1. Informatica AWS Hosted Architecture Diagram 2](#_Toc491687036)

[2. Production Hosting Environment on Amazon EC2 3](#_Toc491687037)

[3. Provisioning Start Checklist 4](#_Toc491687038)

[3.1 For VPN based connection between DMZ VPC and On Prem Data Center 4](#_Toc491687039)

[3.2 For Direct connection between DMZ VPC and On Prem Data Center 5](#_Toc491687040)

[3.3 High level Project Milestones 5](#_Toc491687041)

[3.4 Source systems & Estimated Record Counts 5](#_Toc491687042)

[3.5 Environment prerequisite questionnaire 6](#_Toc491687043)

[4. Customer Contact Information 7](#_Toc491687044)

[5. MDM Implementation information 7](#_Toc491687045)

[5.1 Business Objective 7](#_Toc491687046)

[5.2 Solution Architecture diagram 7](#_Toc491687047)

[6. Ports to open 8](#_Toc491687048)

[7. Environment access URLs 9](#_Toc491687049)

[Appendix :A Network Connectivity options 10](#_Toc491687050)

[Appendix :B Questionnaire details 12](#_Toc491687051)

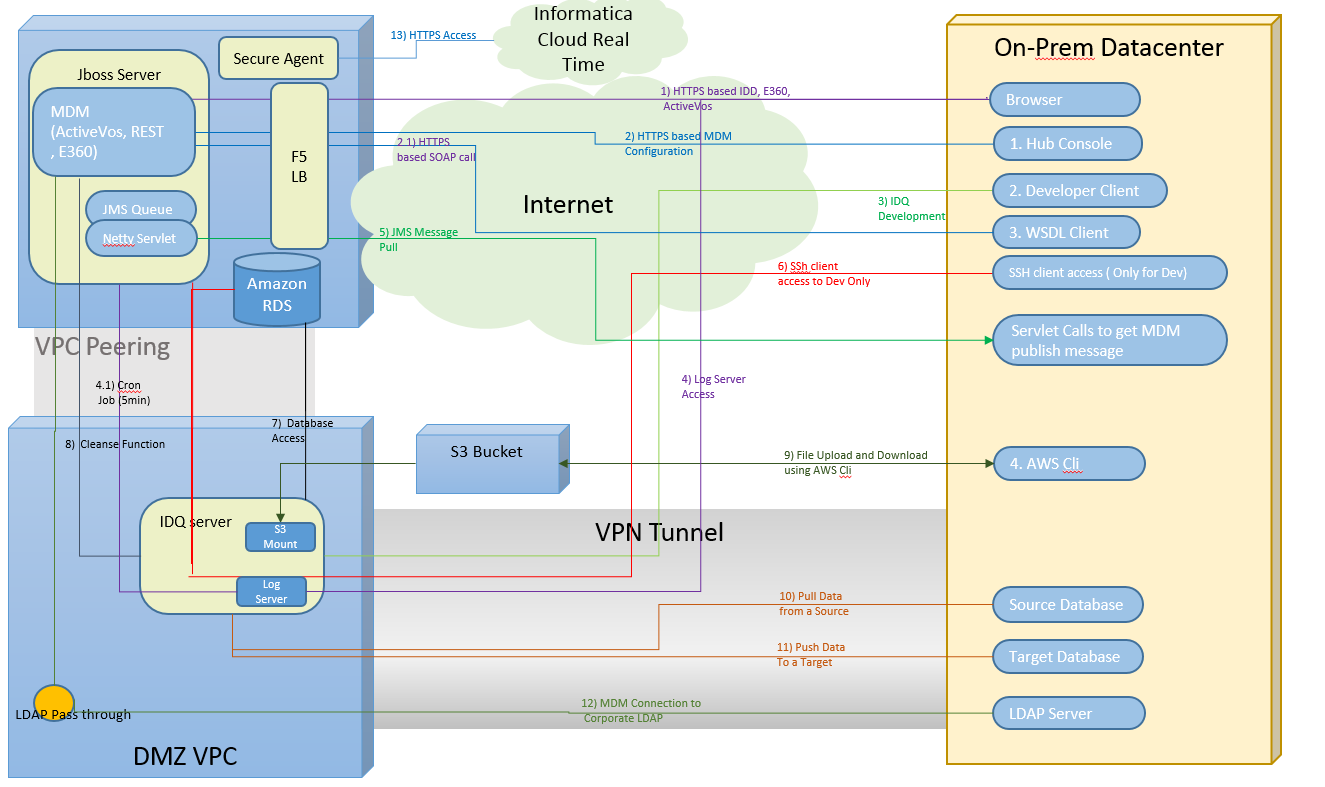
[Appendix :C Important Information /assumptions 13](#_Toc491687052)

[Appendix :D Glossary 13](#_Toc491687053)

# Informatica AWS Hosted Architecture Diagram

MDM Cloud Edition Ecosystem includes two Amazon virtual private clouds (VPCs) as shown in the diagram below. There is no direct access allowed to Informatica Cloud Hosting Services (ICHS) MDM VPC, except via an Informatica product such as MDM or DI/DQ server.

The DMZ (from the term “demilitarized zone”) VPC is where Informatica Data Integration server is installed. DMZ VPC is also where custom code can be deployed.



# Production Hosting Environment on Amazon EC2



# Provisioning Start Checklist

## For VPN based connection between DMZ VPC and On Prem Data Center

| Question | Answer |
| --- | --- |
| Preferred CIDR range for IDQ servers for Dev |  |
| Preferred CIDR range for IDQ servers for QA and Prod |  |
| If IDQ server IP address will use NAT? |  |
| Edge device(s) in use at the customer end |  |
| Routable IP addresses for edge device(s) |  |
| BGP based routing? If yes, then BGP ASN |  |
| If Static route to be used |  |
| CIDRs for subnets from which developers will access IDQ Server for configuration using platform developer (this includes corporate network, VPN, jump machines and Citrix machines) |  |
| CIDRs for subnets which correspond to servers that IDQ needs to connect (ex. on-prem Database, network mount ) |  |
| Network team contact point (Name, Email Address, Cell Phone) \* |  |
| Expect date Dev environment to be made available. |  |
| Will ICS or ICRT will be used to interact with MDM? | Yes |
| Expected platform services on IDQ server |  |

**\*Cell Phone is needed because INFA will send encrypted VPN configuration file over email and password as a text message.**

## For Direct connection between DMZ VPC and On Prem Data Center

Direct connect allows for a peered connection to one of several major internet backbone facilities throughout the world. Port speeds are either 1G or 10G and end points are generated as a part of the wizard based on the region you are using. Direct connect is beyond the scope of this document. The list of AWS direct connect partners is here:

[*https://aws.amazon.com/directconnect/partners/#americas*](https://aws.amazon.com/directconnect/partners/#americas)

Customer’s network engineer must communicate directly with Informatica Security team. This can be arranged through Informatica Global Customer support

| Question | Answer |
| --- | --- |
| Preferred CIDR range for MDM and IDQ server |  |
| If IDQ server IP address will use NAT? |  |
| Network team contact point (Name, Email Address, Contact number) |  |
| Expect date Dev environment to be made available. |  |

## High level Project Milestones

Provide a high-level project milestone plan. (Tentative dates will suffice for now):

| Question | Start Date | End Date |
| --- | --- | --- |
| Development |  |  |
| Testing |  |  |
| Production deployment |  |  |

## Source systems & Estimated Record Counts

Name of the Source Systems & Estimated Data counts

* How many Source system will be sending records into into MDM,
* Location of Source Systems (on Premisis or Cloud based)
* How will the Source Systems send data into MDM
* Estimated count of records from source system

(Please fill in the table below)

|  |  |  |  |
| --- | --- | --- | --- |
| Source system name | Location (onprem/Cloud) | How will system send data into MDM | Estimated Record Count in Production |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Environment prerequisite questionnaire

Please fill in the below information promptly to help us in any further investigation:

Check “Appendix A” and “Appendix B” for more details about below items

| Question | Answer |
| --- | --- |
| Domains to Master |  |
| Number of source systems |  |
| Data Volume for Initial Data Load |  |
| Data Volume for daily processing- batch |  |
| Expected Daily real-time updates – All channels IDD/E360 and Composite Services/ SIF |  |
| Expected Average number of active users on IDD/E360 |  |
| Total IDD/E360 users |  |
| VPN / Direct Connection \* |  |
| LDAP authentication used |  |
| SSL used |  |
| IDQ (specify the services required for IDQ) |  |
| IP mapped to virtual IP to access MDM or DQ |  |
| Message trigger implementation/Message publishing to downstream system |  |
| Secure Agent used |  |

# Customer Contact Information

|  |  |  |  |
| --- | --- | --- | --- |
| Responsibility | Name | Phone | Email |
| Project Owner |  |  |  |
| Project Manager |  |  |  |
| Team Lead |  |  |  |
| Business Team which owns the project |  |  |  |
| Admin Team |  |  |  |
| System Integrator Contact (If already identified) |  |  |  |
| Network Team |  |  |  |
| … |  |  |  |

# MDM Implementation information

## Business Objective

<High level business challenge which the organization plans to mitigate with the use of Informatica MDM solution>

## 

## 5.2 Solution Architecture diagram

<Solution diagram showing known interfaces with Hosted MDM and IDQ>

# Ports to open

The installer sets up the ports for components in ~~the~~ Informatica MDM environment, which need to be opened in customer security firewall layer in start the communication between MDM AWS environment and customer system

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VPC | Application Used Port | Type | Protocol | Port Range | Source |
| DMZ VPC | IDQ Server/Domain Operations | Custom TCP Rule | TCP | 6005-6009 | 0.0.0.0/0 |
| DMZ VPC | IDQ Services | Custom TCP Rule | TCP | 6013-6114 | 0.0.0.0/0 |
| DMZ VPC | IDQ PowerCenter Debugger Port | Custom TCP Rule | TCP | 9229 | 0.0.0.0/0 |
| DMZ VPC | IDQ Admin HTTPS Port | Custom TCP Rule | TCP | 9990 | 0.0.0.0/0 |
| DMZ VPC | IDQ Data Integration Service port | Custom TCP Rule | TCP | 8095 | 0.0.0.0/0 |
| DMZ VPC | IDQ Analyst Service | Custom TCP Rule | TCP | 8085 | 0.0.0.0/0 |
| DMZ VPC | IDQ Metadata Manager | Custom TCP Rule | TCP | 10250 | 0.0.0.0/0 |
| DMZ VPC | IDQ Metadata Manager Agent | Custom TCP Rule | TCP | 10251 | 0.0.0.0/0 |
| DMZ VPC | IDQ Report Service | Custom TCP Rule | TCP | 16080 | 0.0.0.0/0 |
| DMZ VPC | IDQ Search Service | Custom TCP Rule | TCP | 8084 | 0.0.0.0/0 |
| DMZ VPC ( Dev Only ) | SSH client | SSH | SSH | 22 | 0.0.0.0/0 |
| DMZ VPC | Secure Agent | https | https | 443 | 0.0.0.0/0 |
| DMZ VPC | IDQ Report Service | http | TCP | 80 | 0.0.0.0/0 |

# Environment access URLs

URLs mentioned below will be shared per environment.

All URLs except #11 are accessiable via internet using userid and password provided by Informatica.

Platform Admin Console URL is avaibale over VPN ( or direct connection based on option selected) and does nequire DMZ VPC to be connected to On-Prem network.

[EnvironmentIdentifier] will be provided with the actual environment

|  |  |  |
| --- | --- | --- |
| # | Item | URL |
| 1 | MDM Hub Console | [https://mdm.informaticacloud.com/<EnvironmentIdentifier>/cmx/](https://mdm.informaticacloud.com/westfielddev/cmx/) |
| 2 | MDM Data Director | [https://mdm.informaticacloud.com/<EnvironmentIdentifier>/bdd/](https://mdm.informaticacloud.com/westfielddev/bdd/) |
| 3 | MDM Provisioning UI | [https://mdm.informaticacloud.com/<EnvironmentIdentifier>/provisioning/](https://mdm.informaticacloud.com/westfielddev/provisioning/) |
| 4 | MDM Data Director Configuration (for old-style IDD) | [https://mdm.informaticacloud.com/<EnvironmentIdentifier>/bdd/config](https://mdm.informaticacloud.com/westfielddev/bdd/config) |
| 5 | MDM ActiveVOS Tenant Console | [https://mdm.informaticacloud.com/activevos/<EnvironmentIdentifier>/](https://mdm.informaticacloud.com/activevos/westfielddev/) |
| 6 | MDM Global Customer Support Site | [https://mdm.informaticacloud.com/<EnvironmentIdentifier>/mdmsupport/](https://mdm.informaticacloud.com/westfielddev/mdmsupport/) |
| 7 | MDM BES Services REST | [https://mdm.informaticacloud.com/<EnvironmentIdentifier>/cmx/csfiles/](https://mdm.informaticacloud.com/westfielddev/cmx/csfiles/) |
| 8 | MDM SIF Services SOAP | [https://mdm.informaticacloud.com/<EnvironmentIdentifier>/cmx/services/](https://mdm.informaticacloud.com/westfielddev/cmx/services/) |
| 9 | MDM SIF WSDL | [https://mdm.informaticacloud.com/<EnvironmentIdentifier>/cmx/request/wsdl/](https://mdm.informaticacloud.com/westfielddev/cmx/request/wsdl/) |
| 10 | MDM SOAP Request Client | [https://mdm.informaticacloud.com/<EnvironmentIdentifier>/cmx/services/SifService](https://mdm.informaticacloud.com/westfielddev/cmx/services/SifService) |
| 11 | Platform Admin Console | http://< DMZ VPC IP address>:6008/administrator/ |

# Network Connectivity options

Option mentioned below are available to establish connectivity between on-premise data center and Hosted MDM environment. Customers may need input from their network administrators for this section.

A connection is required from the DMZ VPC to on-premise environment. Amazon has two ways of providing this connectivity:

|  |  |
| --- | --- |
| **Direct Connect** | Direct connect allows for a peered connection to one of several major internet backbone facilities throughout the world. Port speeds are either 1G or 10G and end points are generated as a part of the wizard based on the region you are using. Direct connect is beyond the scope of this document. The list of AWS direct connect partners is here:  [*https://aws.amazon.com/directconnect/partners/#americas*](https://aws.amazon.com/directconnect/partners/#americas)  **Customer’s network engineer must communicate directly with Informatica Security team. This can be arranged through Informatica Global Customer support** |
| **VPN** | An ipsec Virtual Private Gateway (VPG) is created in the VPC and then a customer gateway (CG) is used to describe the security device at the on-prem edge.  The CG requires a BGP ASN (which can be anything above 65000 if not registered) and an IP address  Once the VPG and CG are created, a VPN can be set up between the VPC and on-prem.  The VPN requires the VPG and CG and the routing type (BGP or static).  Once the VPN is created then Amazon will provide connection secrets used to set up the tunnel.  The tunnel itself is comprised of two IPSEC tunnels for high availability.  Amazon gives you the IP addresses for the Amazon side along with a configuration download option for various security devices such as Cisco, F5, Juniper PAN etc a log with a generic configuration for if you are not using a standard device (such as vyos). Amazon does the initiation, i.e. the tunnel cannot be initiated from the customer end.  The configuration files contain all the information required to setup the connections. A network engineer is required at customer end to configure this.  <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html>  <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#VPC_VPN_Network_Info>  <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html>  Ideally we would use this scenario:  <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario4.html>  Amazon provide the details for the security device in use.  **Informatica needs the following information in case of VPN connectivity:**   * **What type of security appliance is on your company’s side of the connection?** * **What are the endpoint IPs for each device (assuming there are two)?** |

# Questionnaire details

| Question | Detail |
| --- | --- |
| Domains to Master | Provide the name of domain which you are trying to create the master data, e.g. Insurance, Retail, Finance etc |
| Number of source systems | How many number of source system will send the source data to master? |
| Data Volume for Initial Data Load | During your initial load, how many records you will be loading in the system |
| Data Volume for daily processing- batch | What is the approximate count of the incremental daily/weekly/Monthly delta of records you will load in this system |
| Expected Daily realtime updates – All channels IDD/E360 and Composite Services/ SIF | Count of updates supposed to be coming from real-time API calls, daily |
| Expected avg. number of active users on IDD/E360 | Active real-time concurrent users at a time |
| Total IDD/E360 users | Total real-time users |
| VPN / Direct Connection | Check above table |
| LDAP authentication used | Are we going to use LDAP users |
| SSL used | Is SSL used? |
| IDQ being used | Informatica |
| IP mapped to virtual IP to access MDM or DQ | Sometimes because of some security restrictions, customer map the IP to an internal IP. The do IP conversion. |
| Message trigger implementation/Message publishing to downstream system | What is the strategy to publish messages to downstream system |
|  |  |

# Important Information /assumptions

Below is some of the important information and assumption about the Hosted MDM environment

| Information/ assumptions |
| --- |
| Since MDM VPC is not exposed, no custom components can be deployed on Jboss server running on MDM VPC. |
| User exit code which need to access customer specific services will not be able to connect to application hosted On-prem for customer. |
| Log access will be provided via a log server listening on a port on DMZ VPC instance. |
| Note that on DMZ VPC does not have an apps server where custom code can be deployed. |
| Typically, Informatica expects 15 days lead time for an environment to be available, Please contact Global Customer Support to expedite the request if required. |
| Support case is required for all requests for Informatica including requests related to Hosted MDM infrastructure. |
| Informatica expects high level solution diagram depicting how MDM will be interacting with On-Prem or other cloud applications to be available within 15 days of engagement. |
| Informatica expects high level project plan identifying important milestone for the project to be available within 15 days of engagement. |
| for IDQ development, IDQ client need to be requested by raising a Informatica shipping case. |
| MDM VPC and DMZ VPC will be in US west AWS region (it brings additional restriction on how customer can connect to DMZ VPC); |
|  |

# Glossary

|  |  |
| --- | --- |
| VPC | Virtual Private Cloud |
| VPN | Virtual Private Network |
| DMZ | De-Materialized Zone |
| IDQ | Informatica Data Quality |
| IDD | Informatica Data Director |
| SIF | Service Integration Framework |
| E360 | Entity 360 |
| VPG | Virtual Private Gateway |
| CG | Customer Gateway |
| MDM | Master Data Management |
| BES | Business Entity Services |
| DQ | Data Quality |