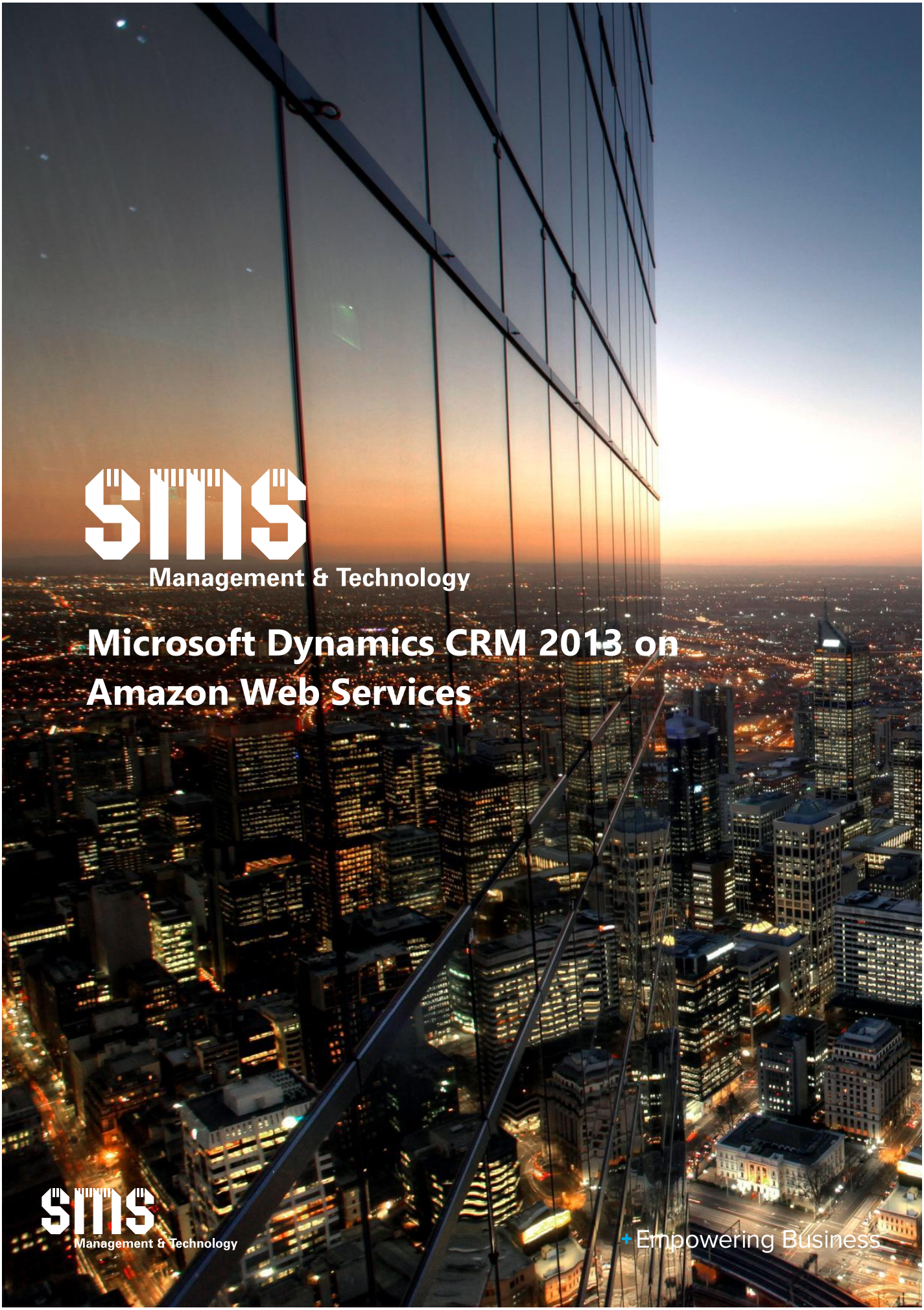

SMS
Management & Technology
Microsoft Dynamics CRM 2013 on Amazon Web Services
SMS
Management & Technology
+ Empowering Business

Abstract

This whitepaper is intended for architects and system administrators who plan to take advantage of the Amazon Elastic Compute Cloud (EC2) service in Amazon Web Services (AWS) to deploy Microsoft Dynamics CRM 2013.

Running Dynamics CRM in Amazon EC2 enables organizations to take advantage of numerous features that are not available in Dynamics CRM Online, including greater extensibility and the option to customize and integrate CRM with other business applications and databases.

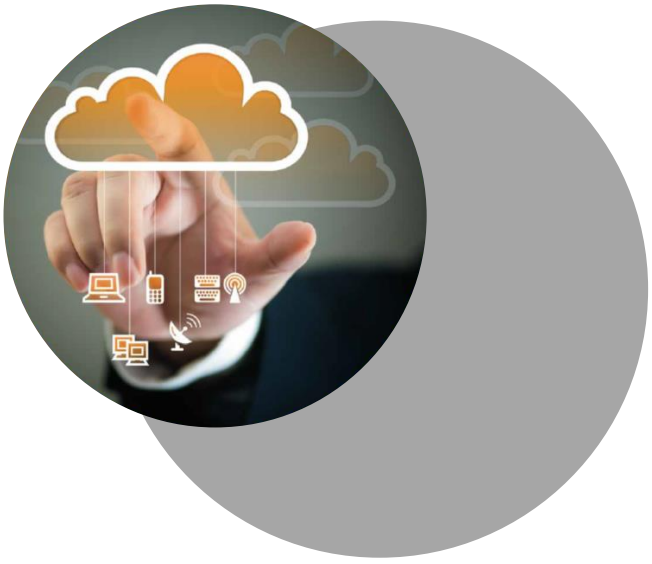
Customer relationships are core to every business, so it's essential that IT be able to work closely with Sales and Marketing to develop and automate internal CRM processes. Whether you intend to run Dynamics CRM 2013 with little customization or a lot, you will find that the AWS platform offers a secure, highly-scalable, cost-effective, and comprehensive web services environment for running mission-critical Windows Server workloads in the cloud.

This whitepaper offers reference architectures for various size deployments of Microsoft Dynamics CRM 2013 in AWS to guide organizations in the delivery of these complex systems.

SMS Management & Technology

amazon web services | Partner Network

ADVANCED CONSULTING PARTNER
AUTHORIZED GOVERNMENT PARTNER
CHANNEL RESELLER PARTNER



Contents

Technology Overview

Microsoft Dynamics CRM 2013

Microsoft Dynamics CRM 2013 is designed to assist organizations achieve a 360 degree view of customers, adapt quickly to changes in business processes, and achieve reliable user adoption through user interfaces consistent with the Microsoft Office suite of products.

Out of the box, the product focuses mainly on the Sales, Marketing, and Service (help desk) sectors, but Microsoft has been marketing Dynamics CRM 2013 as an xRM platform, with extensible database schemas, and has been encouraging partners to use its proprietary (.NET based) framework to customize it for many other diverse business purposes. Dynamics CRM is part of the Microsoft Dynamics family of business applications, which also includes Dynamics AX, Dynamics Social Listening, Dynamics Marketing, and several Dynamics ERP solutions.

Dynamics CRM 2013 is a client-server application which, like Microsoft SharePoint, is an Internet Information Services (IIS)-based web application supporting many web services interfaces. Clients access Dynamics CRM either by using a web browser or by a thick client plug-in to Microsoft Outlook. In addition to Internet Explorer, the Chrome and Firefox browsers have been fully supported since Microsoft Dynamics CRM 2011 Update Rollup 12.

Microsoft Dynamics CRM 2013 has over 40,000 customers. Dynamics CRM 2013 offers a range of deployment options which will be discussed in this white paper. The latest iteration also offers native integration with other offerings in the Microsoft suites including Exchange, Outlook, Lync and Yammer; making Dynamics CRM 2013 a solution which truly fits with today's multi-channel business environments.

Whether running in AWS or on-premises, Microsoft Dynamics CRM 2013 requires the same list of software components:

+ Microsoft Windows Server
+ A Microsoft Windows Server Active Directory infrastructure
+ An Internet Information Services (IIS) website
+ Microsoft SQL Server 2008 or Microsoft SQL Server 2012
+ Microsoft SQL Server 2008 Reporting Services or Microsoft SQL Server 2012 Reporting Services
+ Microsoft Exchange Server or access to a POP3-compliant email server (optional)
+ SharePoint Server (required for document management)
+ Claims-based security token service (required for Internet-facing deployments)
+ Windows operating system when you use CRM for Outlook. Apple Mac, when running Apple Safari, supported tablet, or mobile device.
+ Supported web browser, such as later versions of Internet Explorer or the latest versions of Apple Safari, Google Chrome and Mozilla Firefox.
+ Microsoft Office Outlook (optional).

Microsoft documents several roles for Dynamics CRM 2013: Full Server, Front End Server, Back End Server, and Deployment Administration Server. The following table lists the minimum and recommended hardware requirements for Microsoft Dynamics CRM Server 2013 running in a Full Server configuration. These requirements assume that additional components such as Microsoft SQL Server, Microsoft SQL Server Reporting Services, SharePoint, or Microsoft Exchange Server aren't installed on the system.

Component	*Minimum	*Recommended
Processor	x64 architecture or compatible dual-core 1.5 GHz processor	Quad-core x64 architecture 2 GHz CPU or higher such as AMD Opteron or Intel Xeon systems
Memory	2 GB RAM	8 GB RAM or more
Hard disk	10 GB of available hard disk space	40 GB or more of available hard disk space

Microsoft SQL Server database engine and Microsoft SQL Server Reporting Services are required to install and run Microsoft Dynamics CRM 2013. The following table lists the minimum and recommended hardware requirements for Microsoft SQL Server. These requirements assume that additional components such as Microsoft Dynamics CRM 2013, Microsoft SQL Server Reporting Services, SharePoint, or Microsoft Exchange Server aren't installed on the system.

Component	*Minimum	*Recommended
Processor	x64 architecture or compatible dual-core 1.5 GHz processor	Quad-core x64 architecture 2 GHz CPU or higher such as AMD Opteron or Intel Xeon systems
Memory	4 GB RAM	16 GB RAM or more
Hard disk	SAS RAID 5 or RAID 10 hard disk array	SAS RAID 5 or RAID 10 hard disk array

Amazon Web Services

Amazon Web Services (AWS) provides a complete set of services and tools for deploying Windows workloads, including Microsoft SharePoint Server, on its highly reliable and secure cloud infrastructure platform. This whitepaper discusses general concepts regarding how to use these services and provides detailed technical guidance on how to configure, deploy, and run a Dynamics CRM Server farm on AWS. It illustrates a reference architecture for common Dynamics CRM deployment scenarios and discusses their network, security, and deployment configurations so you can run in the cloud with confidence.

After reading this whitepaper, you should have a good idea of how to set up and deploy the components of a typical Dynamics CRM Server farm on AWS. You'll learn which artefacts to use and how to configure the various infrastructure details, such as compute instances, storage, security, and networking.

AWS consists of several different kinds of services, ranging from storage to compute to services higher up in the stack for things like automated scaling, messaging and queuing etc. For the purpose of Microsoft Dynamics deployments, the following service offerings are relevant to architects designing for Dynamics CRM.

Amazon Elastic Compute Cloud (EC2)

Amazon Elastic Compute Cloud (Amazon EC2) is a service where end users can rent virtual machines of different configurations on-demand and pay for the amount of time they use them. There are several types of instances

that Amazon EC2 offers, with different pricing options. For Microsoft Dynamics deployments, each Amazon EC2 instance conceptually maps to an individual server, or virtual machine. A list of supported instance types and the roles that they play in a Microsoft Dynamics deployment are highlighted later in the document.

Amazon Simple Storage Service (S3)

Amazon Simple Storage Service (Amazon S3) allows users to store and retrieve arbitrary sized data objects using simple API calls. Amazon S3 is designed for 99.999999999% durability and 99.99% availability. This is a powerful Internet storage system that developers can take advantage of when customizing Dynamics CRM 2013.

Amazon Elastic Block Store (EBS)

Amazon Elastic Block Store (Amazon EBS) provides users block level storage volumes that can be used as network attached disks with EC2 instances. Users can provision volumes of different capacities and IOPS guarantees. These volumes have an independent persistence lifecycle from that of Amazon EC2; they can be made to persist even after the EC2 instance has been shut down. At a later point, the same EBS volume can be attached to a different EC2 instance. Amazon EBS volumes can also be snapshotted to Amazon S3 for higher durability guarantees. Amazon EBS is optimized for random access patterns.

General Purpose (SSD) Amazon EBS volumes are designed to provide more than enough performance for a broad set of workloads all at a low cost. They predictably burst up to 3,000 IOPS, and reliably deliver 3 sustained IOPS for every GB of configured storage. In other words, a 10 GB volume will reliably deliver 30 IOPS, and a 100 GB volume will reliably deliver 300 IOPS.

AWS Direct Connect

AWS Direct Connect is one option to establish direct connectivity between your data center and an AWS region. You can configure direct connect links with different bandwidths to meet your requirements. This service allows you to logically consider AWS infrastructure as an extension to your on-premises data center.

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) gives you the ability to logically cordon off a section of the AWS cloud and provision services inside it. Amazon VPC is the recommended way to provision services inside AWS and is enabled by default for all new accounts. There are different configuration options for a VPC regarding the accessibility of your EC2 instances. You can create public facing subnets in a VPC, where the instances may have direct access to the public Internet and other AWS services. Instances can be provisioned in private subnets too, where their access to the Internet and other AWS services can be restricted entirely or only enabled through a NAT server.

Elastic Load Balancing

Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances in the cloud. It enables you to achieve greater levels of fault tolerance in your applications, seamlessly providing the required amount of load balancing capacity needed to distribute application traffic. Elastic Load Balancing can assist you with fault tolerance, failover, and Auto Scaling.

You can build fault tolerant applications by placing your Amazon EC2 instances in multiple Availability Zones. To achieve even more fault tolerance with less manual intervention, you can use Elastic Load Balancing. You get improved fault tolerance by placing your compute instances behind an Elastic Load Balancer, because it can automatically balance traffic across multiple instances and multiple Availability Zones and ensure that only healthy Amazon EC2 instances receive traffic. You can set up an Elastic Load Balancer to load balance incoming application traffic across Amazon EC2 instances in a single Availability Zone or multiple Availability Zones.

Regions and Availability Zones

Regions are self-contained geographical locations where AWS services are deployed. Regions have their own deployment of each service. Each service within a region has its own endpoint that you can interact with to use the service.

Within regions there are Availability Zones (AZs). These are isolated locations within a general geographical location. Although isolated, Availability Zones within a region are connected with low latency links. Multiple AZs can provide the base to build highly available applications.

Microsoft Dynamics CRM 2013 on AWS

AWS can provide you with scalable, highly-available, and cost-effective infrastructure. This enables you to design your cloud solution flexibly to meet your business requirements.

Microsoft Dynamics CRM 2013 deployments can easily be scaled from small server deployments right through to highly available enterprise grade server configurations. The information provided in this document will detail the different types of CRM infrastructure architecture designs SMS has recommended to clients, and helped them to deploy. Additionally, this whitepaper outlines the benefits of each model, and concludes with two recommended designs.

There are many business reasons why running Dynamics CRM 2013 in AWS makes sense:

- AWS offers elastic scale. This means you can scale up immediately when demand increases. You can also scale down immediately to save money when resources are not needed (e.g., on weekends).
- You can easily experiment with new prototype and pilot business applications without risk of pre-acquiring expensive hardware. If a new business application takes off, you can quickly scale up the cloud resources to handle it, and if the idea doesn't pan out, you can shut down the test environment instantly with minimal cost.
- You don't need to dedicate as many IT staff to running the server farm.

Dynamics CRM 2013 Reference Architecture and Scenarios

Dynamics CRM 2013 Reference Architecture

Microsoft provides considerable guidance for architecting Dynamics CRM 2013 farm topologies for many scenarios and scales. This section reviews the typical architectures as recommended by Microsoft and identifies four common deployment scenarios and associated topologies that will map onto AWS.

The Dynamics CRM 2013 reference architecture defines distinct roles and server groups that can be created and scaled independently. This model aligns closely to AWS's scale-out approach meaning that the cloud infrastructure and Dynamics CRM application scale together.

Web Tier

Overview: The web tier of Dynamics CRM 2013, commonly known as Internet Facing Deployment. All user activity is directed via URL to this server.

Scalability: This tier can be easily and rapidly scaled horizontally by taking advantage of Amazon's Elastic Load Balancing and Auto Scaling services.

Application Tier

Overview: The application server for Microsoft Dynamics CRM 2013 establishes all connections to the database. No user traffic is directly connected to these servers. All Microsoft Dynamics CRM 2013 related services are run on the Application Tier servers.

Scalability: This tier can be easily and rapidly scaled horizontally.

Database Tier

Overview: The database tier of Microsoft Dynamics CRM 2013 leverages Microsoft SQL Server. Within the database tier SQL Reporting Services is also utilized.

Scalability: This tier can be easily be scaled vertically as well as horizontally depending on the version of SQL Server in use.

Deployment Options

Microsoft Dynamics CRM 2013 can be deployed in two key configuration patterns. This enables users to access Dynamics CRM 2013 in two distinct ways:

1. From anywhere on the internet
2. fFom within a corporate network

Both options are recommended to be deployed within an Amazon Virtual Private Cloud (Amazon VPC), but with different user accessibility:

1. Deployment inside a public subnet VPC – Users will be able to access the application from anywhere they have Internet access.
2. Deployment inside a private subnet VPC – Users will be able to access the application from the corporate network.

The selection of an appropriate deployment model will depend on the user access and security requirements for your organization.

Deployment Scenarios

Microsoft Dynamics CRM 2013 offers a range of deployment scenarios and is designed to give you the flexibility of availability and performance based on your individual requirements.

Deployments of Dynamics CRM 2013 fall into the following types of scenarios:

1. Single server - Standard Availability, Standard Performance
2. Two-Tier single server instances - Standard Availability, Medium Performance
3. Three-Tier multi-server instances
    a. Level 1 Enterprise Grade - Highly Availability, Medium Performance
    b. Level 2 Enterprise Grade - Highly Availability, High Performance

The following table outlines some of the features of each of these deployment architectures:

Deployment Type	System Availability Profile	System Performance Profile	Estimated User Count	Typical Number of AWS Instances
Single Server	Low	Low	> 25	3
Two Tier – Single Server	Low	Medium	~25 - 320	4
Three Tier – Level 1	High	Medium	~320 - 800	6
Three Tier – Level 2	High	High	> 800	10+

There are several factors to be considered when choosing the right infrastructure design for your Dynamics CRM 2013 deployment. They include:

1. Number of users required to use the system concurrently.
2. The amount of data the system is required to operate with.
3. The number of client devices that will be communicating with the CRM system, such as CRM for Outlook Offline, mobile applications, etc.
4. The number of other systems that require integration and that share and update information in real-time or at scheduled times.
5. The importance of response times for CRM pages to load. This applies especially to customer contact (support) centers where customers are on the phone and information needs to be provided quickly.
6. Any bulk operations the CRM system is designed to perform. Mass emailing customers can really stress the infrastructure when trying to communicate with high volumes of customers.
7. Other heavy asynchronous/synchronous processes that may be required.
8. User uptime expectations.

Supporting Components

Each deployment architecture outlined in this white paper uses a common set of support modules, outlined in the following sections.

Remote Desktop Gateway Service

This service provides secure and easily managed RDP access to the internal Windows servers for the purpose of remote administration. This is used as the primary administration access path, or as the failback path if administrators have access internally through the corporate connection.

This paper will not detail the configuration of this building block. For details on RDGW setup in AWS please refer to the following whitepaper:
https://s3.amazonaws.com/quickstart-reference/Microsoft/rdgateway/latest/doc/Microsoft_Remote_Desktop_Gateway_Quick_Start.pdf

Network Address Translation

A NAT server is deployed in the public subnet to provide a route for internal Windows servers to access the Internet. If the internal instances have the ability to route through the corporate network, then the NAT devices are not necessary.

For detailed information on setting up the NAT service, refer to:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html

SharePoint

Microsoft SharePoint Server is a collaboration and content management application that simplifies how people store, find, and share information. It helps people to collaborate effectively by having secure access to documents and information that they require to make business decisions.

You can use the document management capabilities of SharePoint from within Microsoft Dynamics CRM 2013. You can store and manage documents in the context of a Microsoft Dynamics CRM 2013 record on a server that is running SharePoint, and leverage the SharePoint infrastructure to share, manage, and collaborate efficiently. Because the documents are stored on a server that is running SharePoint, non-Microsoft Dynamics CRM 2013 users can directly access the documents on the server, provided they have the appropriate permissions on the server that is running SharePoint Server.

SharePoint integration with Microsoft Dynamics CRM 2013 enables you to:

- Create, upload, view, and delete documents on a server that is running SharePoint from within Microsoft Dynamics CRM 2013.
- Use the SharePoint document management abilities within Microsoft Dynamics CRM 2013, such as checking the document in and out, viewing version history, and changing document properties.

For details on integrating SharePoint with Microsoft Dynamics CRM 2013, please refer to:
http://msdn.Microsoft.com/en-us/library/gg334768.aspx
We won't provide the full reference architecture for running SharePoint on AWS as part of this paper. Please refer to the following document:
https://s3.amazonaws.com/quickstart-reference/microsoft/sharepoint/latest/doc/Microsoft_SharePoint_2013_on_AWS.pdf

Single-Server Architecture

Single-server architectures are ideal for pilots, development, and testing environments where a simple and rapid deployment is preferred. A single-server setup is not generally recommended for a production setup; however, it may be considered for small implementations where fewer than 25 users are accessing the system. User access for internal users is controlled through Active Directory (AD) services.

The architecture for a simple, single-tier, single-server deployment is outlined in the following diagram. This solution will be built in a single Availability Zone.

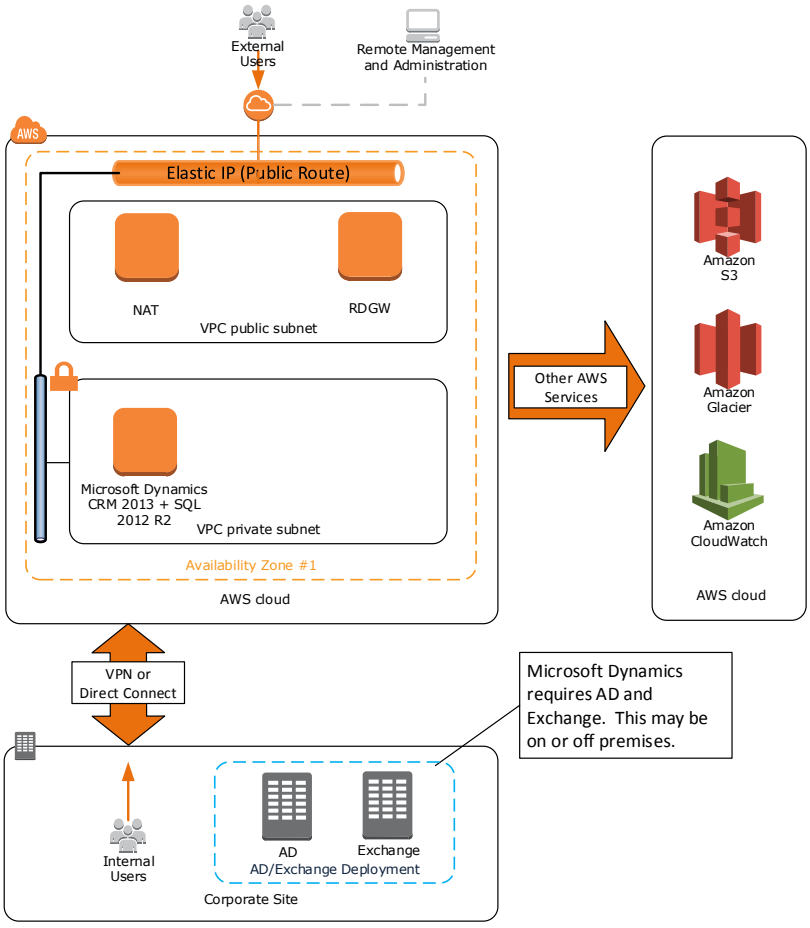


Figure 1- Single-Server Deployment Configuration

The following table outlines the suggested AWS instance types for this type of deployment

Role(s)	Minimum Instance Type	vCPU Units	Memory	EBS Storage	Network
NAT Server	t2.micro	Burstable	1 GB	8GB	Low
RDGW Server	m3.medium	1	3.75 GB	Disk #1 -> 50 GB	Moderate
CRM + SQL	r3.xlarge	4	30.5 GB	80 GB SSD	500 Mbps

***Note**: Amazon EBS volumes should be "pre-warmed" to ensure maximum disk I/O. Volume IOPS can also be pre-provisioned depending on performance requirements.*

Two-Tier -- Single-Server Architecture

The diagram below is a common design used by smaller organizations of up to 50-100 users. This separates the Dynamics CRM 2013 application and SQL database servers onto distinct machines to improve performance. A key issue with this model is the low availability of the system; if any of the system components fails to service users, the entire system goes down. It is then up to the system restoration process to bring the failed components back up again, which may take some time.

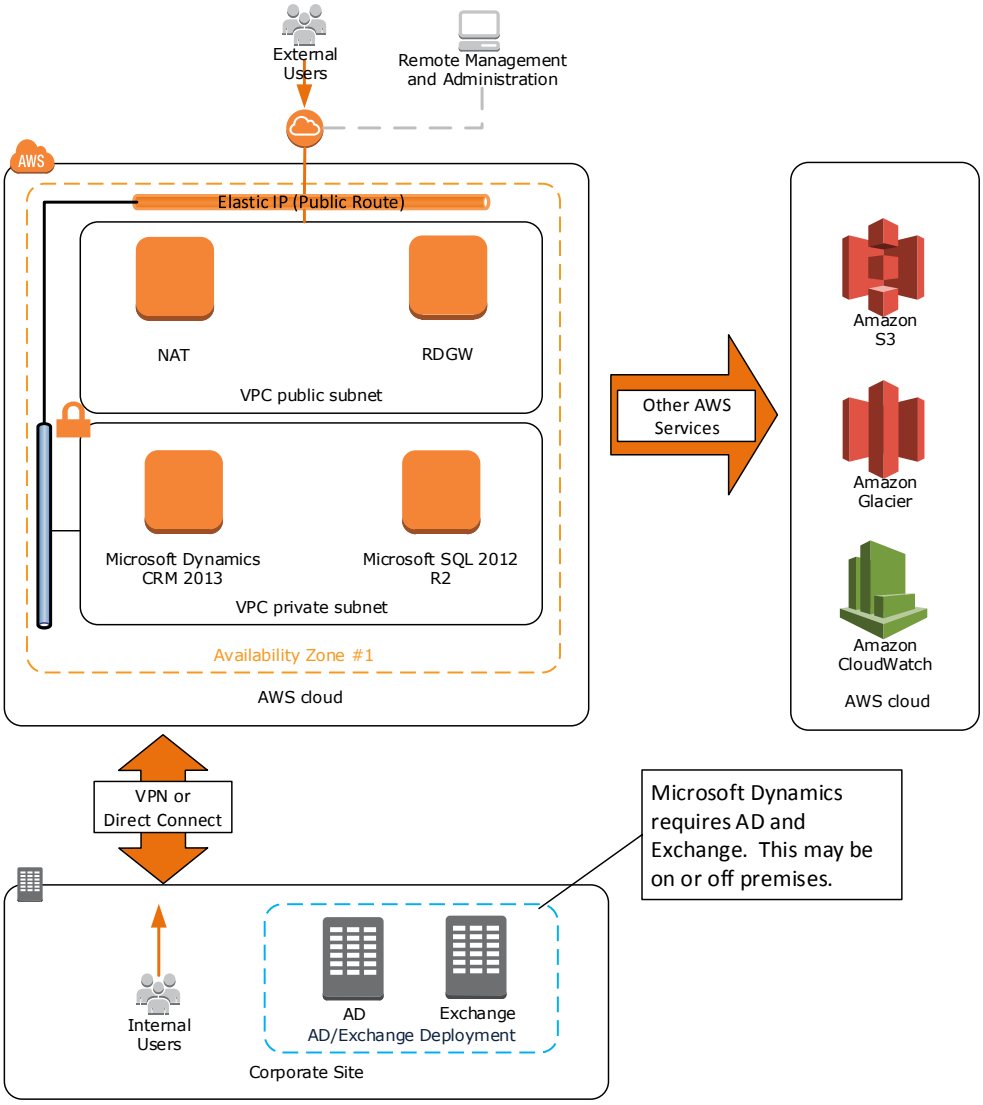


Figure 2- Two-Tier – Single-Server Deployment Configuration

The following table outlines the suggested AWS instance types for this type of deployment

Role(s)	Minimum Instance Type	vCPU Units	Memory	Storage	Network
NAT Server	t2.micro	Burstable	1 GB	8 GB	Low
RDGW Server	m3.medium	1	3.75 GB	Disk #1 -> 50 GB	Moderate
CRM Server	c3.xlarge	4	7.5 GB	Disk #1 ->100 GB SSD Disk #2 ->80 GB SSD	500 Mbps
SQL Server	r3.xlarge	4	30.5 GB	Disk #1 ->100 GB SSD Disk #2 ->200 GB SSD	500 Mbps

***Note**: Amazon EBS volumes should be "pre-warmed" to ensure maximum disk I/O. Volume IOPS can be pre-provisioned depending on performance requirements.*

Three-Tier -- Multi-Server Architecture -- Level 1

RECOMMENDED FOR HIGH AVAILABILITY

The diagram below demonstrates the recommended architecture for large enterprise organizations that require high availability and standard to medium-level performance.

The key difference between this architecture and the Two-Tier – Single-Server architecture is the introduction of the high availability of the servers. In the model shown below, the Elastic Load Balancer (ELB) manages the distribution of work across two separate three-tier stacks. If one of the CRM application servers fails, or one of the SQL database servers fails, the system will continue to operate with the ELB directing all traffic to the available node.

For an environment where users will access Microsoft Dynamics CRM 2013 via the Internet, the ELB will be public facing. For internal-only users an internal ELB should be used.

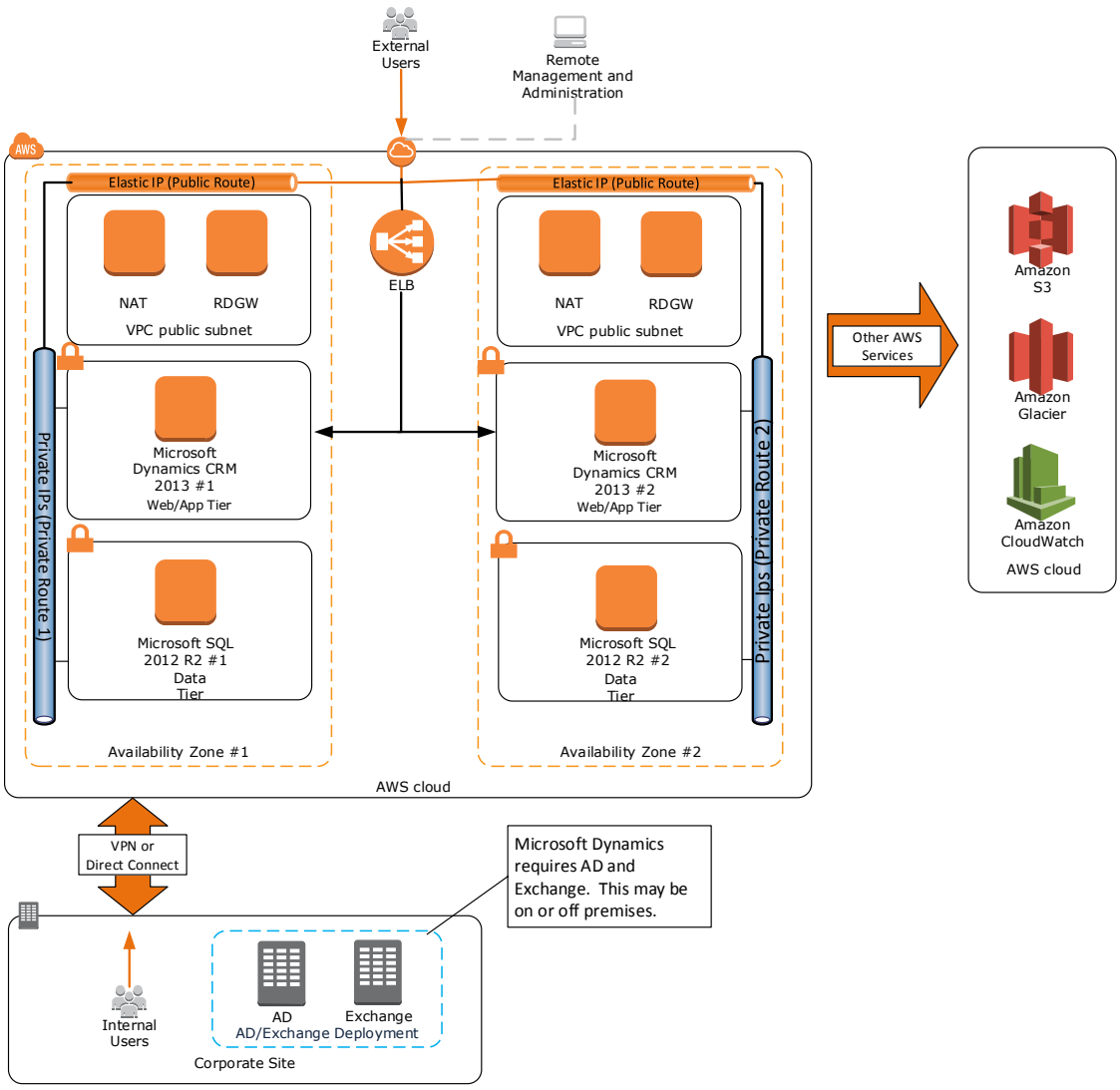


Figure 3- Three-Tier - Multi-Server Architecture - Level 1

The following table outlines the suggested AWS instance types for this type of deployment

Role(s)	Minimum Instance Type	vCPU Units	Memory	Storage	Network
NAT Server	t2.micro	Burstable	1 GB	8 GB	Low
RDGW Server	m3.medium	1	3.75 GB	Disk #1 -> 50 GB	Moderate
CRM Server	c3.xlarge	4	7.5 GB	Disk #1 ->100 GB SSD Disk #2 ->80 GB SSD	500 Mbps
SQL Server	r3.xlarge	4	30.5 GB	Disk #1 ->100 GB SSD Disk #2 ->200 GB SSD	500 Mbps

***Note**: Amazon EBS volumes should be "pre-warmed" to ensure maximum disk I/O. Volume IOPS can be pre-provisioned depending on performance requirements.*

Three-Tier -- Multi-Server Architecture -- Level 2

RECOMMENDED FOR HIGH AVAILABILITY AND HIGH PERFORMANCE

The diagram below demonstrates the recommended architecture for large enterprise organizations that require high availability and high performance.

This design shows the use of existing internal Active Directory Services authentication for Dynamics CRM 2013. Active Directory Federation Services will also be required when you need to allow devices external to your domain to connect to your CRM system.

The main difference between the Level 1 architecture and the Level 2 architecture is the separation of the Dynamics CRM 2013 roles on the servers into distinct categories for Web and Application. The Web Front End servers host only the Front End Roles for CRM. The second set of servers provides the Back End Asynchronous Roles for the Dynamics CRM 2013 deployment. The specifications for the back end servers can be reduced depending on the complexity of back end asynchronous operations. Once again, the use of an ELB to manage the load provides resilience to the deployment.

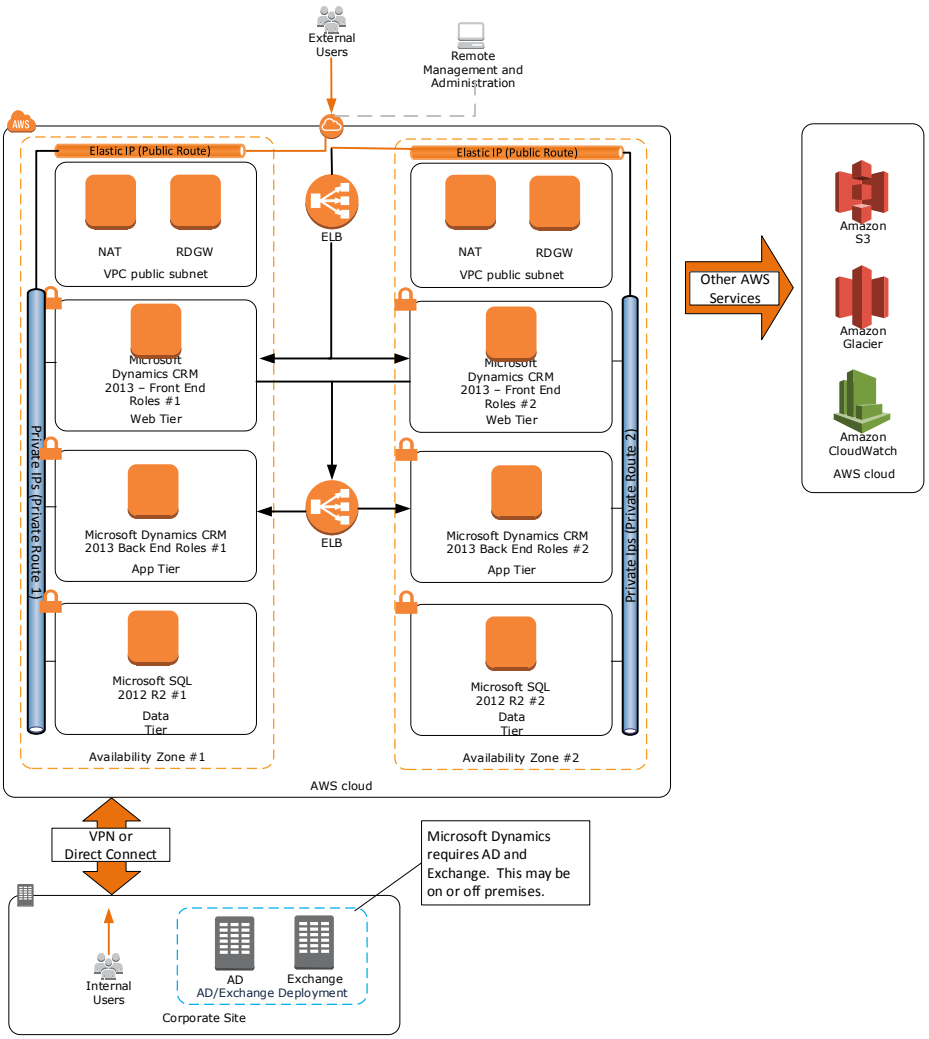


Figure 4- Three-Tier - Multi-Server Architecture - Level 2

The following table outlines the suggested AWS instance types for this type of deployment

Role(s)	Minimum Instance Type	vCPU Units	Memory	Storage	Network
NAT Server	t2.micro	Burstable	1 GB	8 GB	Low
RDGW Server	m3.medium	1	3.75 GB	Disk #1 -> 50 GB	Moderate
CRM Front End Server	c3.2xlarge	8	15 GB	Disk #1 -> 100 GB SSD Disk #2 -> 80 GB SSD	500 Mbps
CRM Back End Server	c3.2xlarge	8	15 GB	Disk #1 -> 100 GB SSD Disk #2 -> 80 GB SSD	500 Mbps
SQL Server	r3.xlarge	4	30.5 GB	Disk #1 -> 100 GB SSD Disk #2 -> 200 GB SSD	500 Mbps

***Note**: Amazon EBS volumes should be "pre-warmed" to ensure maximum disk I/O. Volume IOPS can be pre-provisioned depending on performance requirements.*

Supported Amazon AMIs

Amazon Machine Images (AMIs) are the virtual machine images that run on EC2 instances. These consist of the operating system and any other software that the AMI creator chooses to bundle into them. The cost per hour per instance will depend on the AMI selected. AWS can, in some circumstances, integrate the product license cost into the per hour cost, and in some cases "Bring Your Own Licenses" (BYOL) can be used. Select the AMIs according to your preferred licensing scenario.

For Microsoft Dynamics CRM 2013, SMS recommends the "Microsoft Windows Server 20012 R2 Base" AMI, which is the most current at the time of this writing. This can be found in the "Quickstart" section during the create image/choose AMI process. If BYOL is used for Microsoft SQL, then use this base AMI for all instances, including the Microsoft SQL Server instances.

If BYOL is not used, the base AMI should be used for all instances, including the SQL Servers, if you are using a product level less than Microsoft SQL Enterprise. Where high availability is not required or the environment is single instance, the latest "Microsoft Windows Server 20012 R2 with SQL Server Standard" AMI may be used.

For the multi-server architectures, Microsoft SQL Enterprise may be necessary to provide the highest level of availability or performance. This is only available with BYOL licenses. If Microsoft SQL Enterprise is required, use the "Microsoft Windows Server 20012 R2 Base" AMI and install Microsoft SQL Enterprise onto the instance post creation. (If a Microsoft SQL Enterprise AMI becomes available in the "Quickstart" section in the future, SMS recommends using that.) Make sure you create your own AMI of that instance after you install and configure the server. AWS provides the "Create Image" command for this purpose.

Security

Security setup is critical in the implementation of Microsoft Dynamics CRM 2013 to enable proper network access (in and out of the VPC, specific subnets, and the instances running each subnet) to facilitate user authentication and appropriate authorization, data privacy, and threat management (in the case of public-facing sites). These and other key elements have to be set up correctly to provide the necessary security measures and enable users to access their Microsoft Dynamics Server content and applications with the correct identity and authorization.

A cornerstone of your scenarios is the use of Amazon VPC for providing the overall isolation of the farm and segmenting parts of the farm (i.e., the server groups) to support the desired management and control. Within Amazon VPC and subnet isolation, there are security details that you must set up to enable proper access (and restrictions). The two main approaches at your disposal are:

+ Security groups. A security group acts as a firewall that controls the traffic allowed in and out of a group of instances. When you launch an instance in a VPC, you can assign the instance to up to five VPC security groups. Security groups act at the instance level, not the subnet level.

  In general, it is a good idea to define distinct security groups for each tier. Doing so allows you to define the settings for each tier (and vary them independently) as well as restrict access to the "calling" tier (e.g., allowing the database tier to be called only from the application tier).

+ Network access control lists (ACLs). A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. You might set up ACLs with rules similar to your security groups to add a layer of security to your VPC. Network ACLs act at the subnet level, not the instance level.

Security Groups

Here are the two approaches discussed in greater detail:

+ Elastic Load Balancing:
  Elastic Load Balancing is the point of contact for users, so the Elastic Load Balancing security group should be configured to support inbound client connection types of HTTP or HTTPS (port 80 and port 443, respectively). You can configure the Elastic Load Balancing in any combination, but Amazon recommends using HTTPS for both inbound client connection types. You should create an outbound security rule that lists the web tier security group as the target, restricting the load balancer to sending requests out to the web tier instances only.

+ Web tier:
  In this scenario, the web tier instances are not directly exposed but receive requests via the elastic load balancer. You can (and should) configure the web instances to accept requests only from the load balancer. Fortunately, the load balancer includes a special source security group. Create a security rule for your web tier that restricts inbound access to this special security group, ensuring that only the load balancers are allowed to send to and receive from the web front-end instances. You can also set up an outbound rule to limit outgoing requests to the application tier instances.

+ Application tier:
  As in the web tier case, your application tier security group should be configured with an inbound rule listing the web tier security group as an allowed sender, and an outbound rule listing the database security group for outgoing messages.

+ Database tier:
  As in the other cases, you should require Secure Sockets Layer (SSL) for connections to and from SQL Server. Doing so requires the use of a security group with a rule that allows SSL (port 443) to be used only for the database instances.

You also want to restrict inbound access to the application tier instances, so create a security rule that restricts inbound access to the application tier security group.

Network ACLs

Network ACLs mirror the rules specified in security groups and add an extra layer of security to allow general access rules to be honored regardless of which instances are sending or receiving. Because network ACLs act at the network level (not the instance level), you can set up additional rules to handle certain networks, IP addresses, and address ranges in a specific way. For instance, you can set up a network ACL that defines a rule to deny ingress to a range of source IP addresses (blacklisted IP addresses). For detailed guidance on setting up Amazon VPC network ACLs, see the Amazon Virtual Private Cloud User Guide: http://aws.amazon.com/documentation/vpc/

Windows Instance Security

You can configure Windows instances within the VPC through Group Policy objects (GPOs) to require IP Security (IPsec) connections, further ensuring secure connectivity to the instances.

Administrator Access

In your architecture, the middle tier and database tier instances are placed in private subnets, restricting access from outside the VPC. This placement reduces exposure and enhances security. However, it is still necessary to provide access to those instances for administrative purposes, such as configuration updates and troubleshooting.

To help manage the instances in the private subnet, an indirect (and secure) method is to set up one or more bastion servers in a public subnet to act as proxies, and then set up Remote Desktop Protocol (RDP) gateways to proxy access to the application or database tier instances. After bastion servers are set up, administrators can use RDP to gain access to the bastion host; they can then access other instances at their VPC private IP addresses. See the AWS RDG Reference Architecture whitepaper for details: https://aws.amazon.com/windows/resources/whitepapers/rdgateway/

Data Privacy

Because sensitive content and data can be stored within the Microsoft Dynamics system farm, some organizations may require that the content be encrypted. To successfully support encryption of data within the AWS environment, a few key requirements must be considered and supported:

+ Encryption technology. The Amazon EBS volumes contain the data at rest, in the form of SQL Server database data and files. Amazon EBS volume encryption is supported in AWS; however, there are also other options for encryption that can be considered:

+ Encrypting File System (EFS). Windows includes EFS, which supports the ability to encrypt individual files or folders.

- BitLocker Drive Encryption. Windows Server 2008 R2 supports BitLocker, which provides the ability to encrypt a disk file system attached to the server instance.
- SQL Server Transparent Data Encryption (TDE). SQL Server Enterprise provides native encryption support through TDE.
- Third-party Amazon EBS volume encryption. Third-party commercial options are available for encryption of Amazon EBS volumes.
- Encryption key management. Implementing encryption requires secure management and authorized use of the encryption keys. In the case of Amazon EC2, instances can be stopped and started as well as recovered from Amazon EBS snapshots. In all these cases, the Amazon EBS volumes will be encrypted, and the Amazon EC2 subsystem must access and use the encryption key to be able to attach and use it on subsequent restarts.

The AWS Solution Provider site lists several third-party software vendors that provide security infrastructure that supports Amazon EBS encryption and key management.

Monitoring and Management

You must be able to monitor a number of core dimensions within a Dynamics environment to enable corrections and updates when issues occur or performance suffers. Amazon CloudWatch is an AWS service that monitors various health metrics associated with AWS resources. You can use it to collect, analyze, and view system and application metrics so that you can make operational and business decisions more quickly and with greater confidence. Amazon CloudWatch sets several predefined metrics, such as CPU utilization and disk I/O performance, that AWS measures and that you can view and act upon. You can also publish your own metrics directly to Amazon CloudWatch to allow statistical viewing in the AWS Management Console and to issue (and react to) custom alarms.

Microsoft System Center Operations Manager is the typical tool used to monitor and manage a Microsoft-based infrastructure. Fortunately, Operations Manager can be used in AWS, too. The Windows-based infrastructure on AWS includes the standard Operations Manager agents for Windows Server, SharePoint Server, and SQL Server.

In the intranet scenario, Operations Manager works as it does in an on-premises case, because your VPN–VPC arrangement effectively extends the enterprise network into the AWS cloud. In the public site scenario, Operations Manager can be hosted in an instance and accessed over RDP (through the bastion host method described earlier) and provide monitoring and management against the other components of the Microsoft Dynamics Environment.

SQL Server Configuration

The versions of SQL Server that are included and licensed for use with the Windows Server AMIs are SQL Server Express and SQL Server Standard. SQL Server Enterprise can be installed in Windows AMIs and used in AWS as well but must be licensed for use in the same way as Dynamics, through provisions in the Microsoft License Mobility through Software Assurance program.

As in on-premises deployments, the data tier for Dynamics in AWS needs to be architected and configured to support sufficient performance, high availability, and reliability to provide a good user experience and quickly respond to a database failure with minimal transaction loss. For SQL Server instances, Amazon recommends the High Memory Quadruple Extra Large Amazon EC2 instance type. This type provides higher-performance network I/O (high). This higher performance, combined with the other metrics such as CPU, yields a good performance profile for SQL Server running on AWS.

Recommended Amazon EBS Disk Configuration for SQL Server

Amazon EBS volumes can be configured in a variety of ways (redundant array of independent disks [RAID] striping, different volume sizes, etc.) to yield different performance characteristics. The optimized SQL Server Standard AMI mentioned earlier is published jointly by Microsoft and AWS and is configured with separate Amazon EBS volumes, each storing key SQL Server data components as recommended by Microsoft for optimal performance.

For high-I/O scenarios, it is possible to create and attach additional Amazon EBS volumes and to stripe using software RAID to increase the total number of I/O operations per second (IOPS). Each Amazon EBS volume is protected from physical drive failure through drive mirroring, so using a RAID level higher than RAID-0 is unnecessary.

For further details regarding Amazon EBS setup, configurations, and tuning options, see the Amazon Elastic Compute Cloud User Guide.

High Availability for SQL Server

You can achieve high availability for SQL Server in AWS by using a number of methods

- SQL Mirroring - Implement SQL Server mirroring across multiple Availability Zones. In this configuration, SQL Server instances are launched in two different Availability Zones (within a region), with a smaller "witness" SQL Server instance to monitor and facilitate the failover, if needed.

- AlwaysOn - The AlwaysOn Availability Groups feature is a high-availability and disaster-recovery solution that provides an enterprise-level alternative to database mirroring. Introduced in SQL Server 2012, AlwaysOn Availability Groups maximizes the availability of a set of user databases for an enterprise. An availability group supports a failover environment for a discrete set of user databases, known as availability databases that fail over together. An availability group supports a set of read/write primary databases and one to eight sets of corresponding secondary databases. Optionally, secondary databases can be made available for read-only access and/or some backup operations.

For more information please see:

http://msdn.Microsoft.com/en-us/library/hh510230.aspx

https://s3.amazonaws.com/quickstart-reference/microsoft/sql/latest/doc/Microsoft_WSFC_and_SQL_AlwaysOn_Quick_Start.pdf

http://aws.amazon.com/windows/resources/whitepapers/alwayson/

Further Reading

- Remote Desktop Gateway Reference Architecture
  https://aws.amazon.com/windows/resources/whitepapers/rdgateway/

- NAT Instance Basics
  - http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html

About SMS Management & Technology

SMS Management & Technology is a leading Asia-Pacific Consulting, Technology and Managed Services Company.

Microsoft MAPA 2014 WINNER Customer Relationship Management (CRM) Partner of the Year

We help our clients improve their business performance through the implementation of strategy and the delivery of business and technology projects. Our industry expertise spans the financial services, ICT, government, defence, health, utilities, mining, gaming and infrastructure sectors. We employ in excess of 1,700 professionals in offices throughout Australia, Hong Kong, Vietnam and Singapore.

SMS was founded in 1986 on the basis of three core rules: add value, maintain unity and enhance reputation. More than 25 years on, these values remain central to our business, allowing us to continue delivering excellence in everything we do.

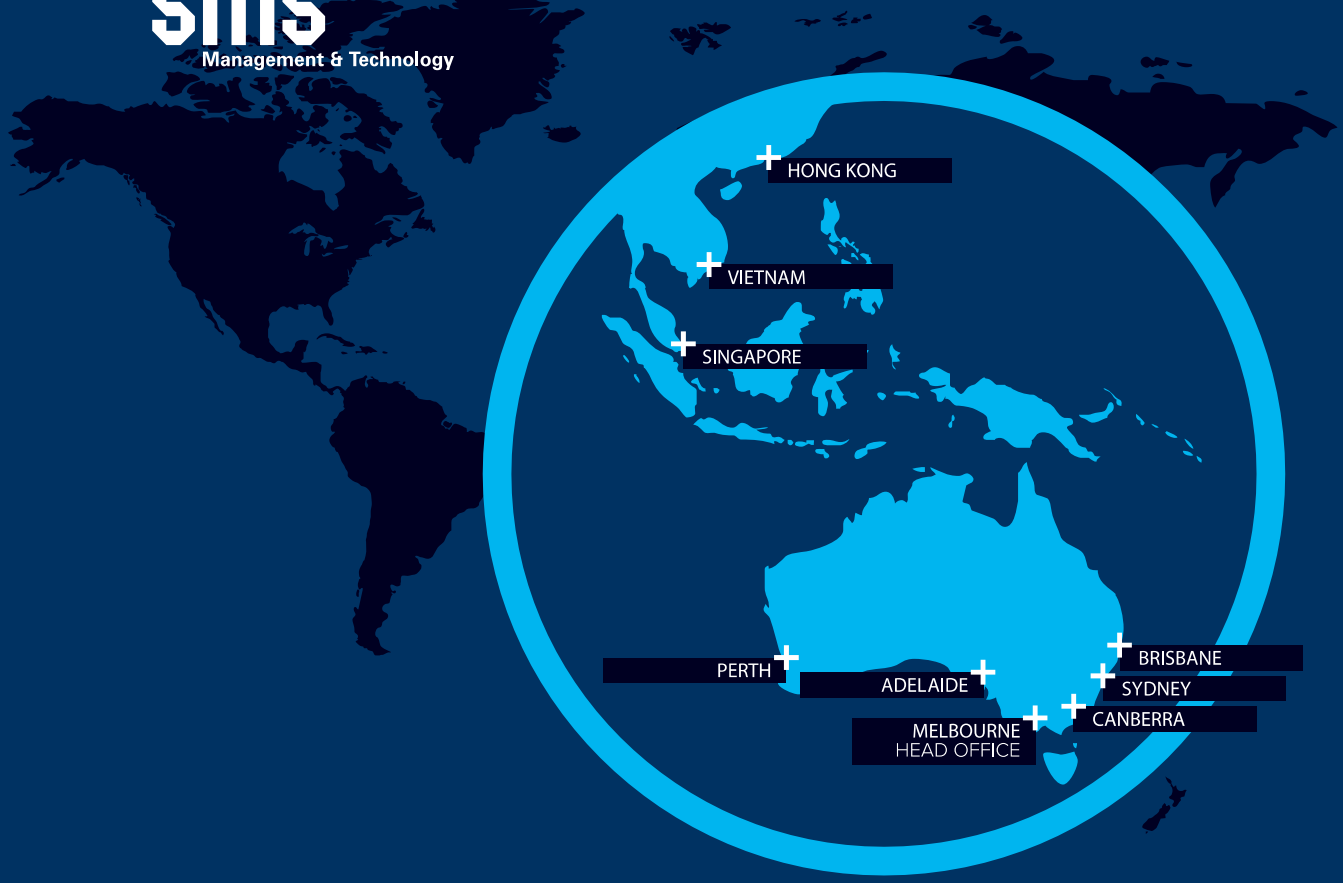
At SMS, we specialise in improving operational performance and IT delivery. We do this by improving the way our clients use people, processes and technologies. This means we address everything from business integration to compliance, process improvement to change management and technology strategy to systems integration and application development.

In short, we make things happen.

For more information see www.smsmt.com or contact David Freeman at david.freeman@smsmt.com

www.smsmt.com

SMS
Management & Technology



AU **Adelaide**
Level 29
Westpac House
91 King William Street
Adelaide SA 5000
P. +61 8 7123 3100

AU **Melbourne**
Level 41
140 William Street
Melbourne VIC 3000
P. 1300 842 767
Intl. +61 3 9674 3333

HK **Hong Kong**
Level 49
4911, The Center
99 Queens Road
Central, Hong Kong
P. +852 3441 2500

AU **Canberra**
Ground Floor
8 Brindabella Circuit
Canberra Airport ACT 2609
P. +61 2 6279 7100

AU **Perth**
1 Howard Street
Perth WA 6000
P. +61 8 9322 2808

SG **Singapore**
Level 24
1 Raffles Place
Singapore 048616
P. +65 6408 0642
Intl. +65 6408 0600

AU **Brisbane**
Level 18
175 Eagle Street
Brisbane QLD 4000
P. +61 7 3215 7200

AU **Sydney**
Level 26
20 Bond Street
Sydney NSW 2000
P. +61 2 9259 8888

Managed Services

VN **Vietnam**
Level 18
The Flemington Tower
182 Le Dai Hanh, District 11
Ho Chi Minh City, Vietnam
P. + 84 8 396 21281