



SAP Business One, version for SAP HANA, on the AWS Cloud: Deployment Guide

September 2014

Nam Je Cho

Note This guide has been superseded by [SAP Business One, version for SAP HANA, on the AWS Cloud: Quick Start Reference Deployment](#). Please see the Quick Start for up-to-date information.

Table of Contents

Abstract	3
What We'll Cover	3
Before You Get Started	4
SAP Business One, version for SAP HANA, on AWS Deployment Architecture	4
AWS Instance Types for SAP Business One, version for SAP HANA.....	5
Deploy SAP Business One, version for SAP HANA.....	6
Step 1: SAP HANA Deployment in the Amazon VPC	6
Step 2: Install SAP Business One, version for SAP HANA	6
Accessing SAP Business One, version for SAP HANA, on AWS.....	8
Establish a Connection to the Windows RDP Instance	8
Establish a Connection to SAP Business One, version for SAP HANA, Server.....	9
Security	11
Network Security	11
AWS Identity and Access Management (IAM)	12
OS Security	12
Security Groups.....	12
Remote Desktop Gateway	12
Additional Information.....	12
Appendix A: Security Group Specifics	13
Appendix B: X11 Forwarding Setup	15

Abstract

This deployment guide includes architectural considerations and configuration steps for deploying SAP Business One, version for SAP HANA, on the Amazon Web Services (AWS) cloud. We'll discuss best practices for deploying SAP Business One, version for SAP HANA, on AWS using services such as Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Virtual Private Cloud (Amazon VPC). We also provide links to deployment guides that you can leverage for running SAP HANA on AWS.

This deployment method leverages a bring your own license (BYOL) model for SAP Business One, version for SAP HANA, software. Hence, you must own the licenses for the SAP Business One application and for the SAP HANA Platform software, and you must have access to download the SAP Business One and SAP HANA Platform Edition software from the [SAP Software Download Center](#).

Note This guide has been superseded by [SAP Business One, version for SAP HANA, on the AWS Cloud: Quick Start Reference Deployment](#). Please see the Quick Start for up-to-date information.

What We'll Cover

SAP Business One, version for SAP HANA, is now available on the flexible AWS platform. This guide serves as a reference for SAP Business One implementation partners and customers interested in deploying SAP Business One, version for SAP HANA, on AWS in a self-service fashion.

The following outlines the end-to-end deployment steps for SAP Business One, version for SAP HANA, provided in this guide. The steps are discussed in detail in the [deployment section](#) of this guide.

Step 1: Deploy SAP HANA in the Amazon VPC

Complete the steps from [SAP HANA on the AWS Cloud: Quick Start Reference Deployment](#). Note that the Quick Start Reference Deployment is also used to deploy the SAP HANA Platform edition, and we've indicated where the instructions differ. Please pay particular attention to the notes and restrictions specific to deploying SAP HANA for SAP Business One.

Deployment of the Amazon VPC and the SAP HANA database is achieved primarily through AWS CloudFormation templates and AWS Tools for Microsoft Windows PowerShell. AWS CloudFormation provides an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. AWS Tools for Windows PowerShell enables automation of operations on AWS resources from the PowerShell command line.

At the completion of the steps in the SAP HANA Quick Start Reference Deployment guide, you will have deployed the SAP HANA database, Windows Remote Desktop Gateway, and the NAT Instance in the Amazon VPC.

Step 2: Download and install SAP Business One, version for SAP HANA, in the Amazon VPC

In this step, SAP Business One will be deployed into the Amazon VPC and installed on the SAP HANA server.

- Download SAP Business One, version for SAP HANA, directly onto the Microsoft Windows instance deployed in Step 1.
- Install SAP Business One Server components on the Linux server
- Install SAP Business One Client components on the Microsoft Windows Server
- Connect to the SAP Business One application

Installation of SAP Business One, version for SAP HANA, is a manual process that requires you to download the SAP Business One media to the Amazon EC2 instance and install the Business One application components using the official SAP installation guide.

At the completion of Step 2, you will have a fully functional SAP Business One, version for SAP HANA application deployed on the AWS cloud.

Before You Get Started

Implementing SAP Business One, version for SAP HANA, on the AWS cloud is an advanced topic. If you are new to AWS, please see the [Getting Started section](#) of the AWS documentation.

In addition, familiarity with the following technologies is recommended.

- [Amazon EC2](#)
- [Amazon VPC](#)
- [AWS CloudFormation](#)

The SAP support statement for running SAP Business One, version for SAP HANA, on AWS is covered in SAP Note [2058870](#) “SAP Business One, version for SAP HANA on Public Infrastructure-as-a-Service (IaaS).”

SAP Business One, version for SAP HANA, on AWS Deployment Architecture

The following diagram provides the solution architecture of SAP Business One, version for SAP HANA, deployed on AWS.

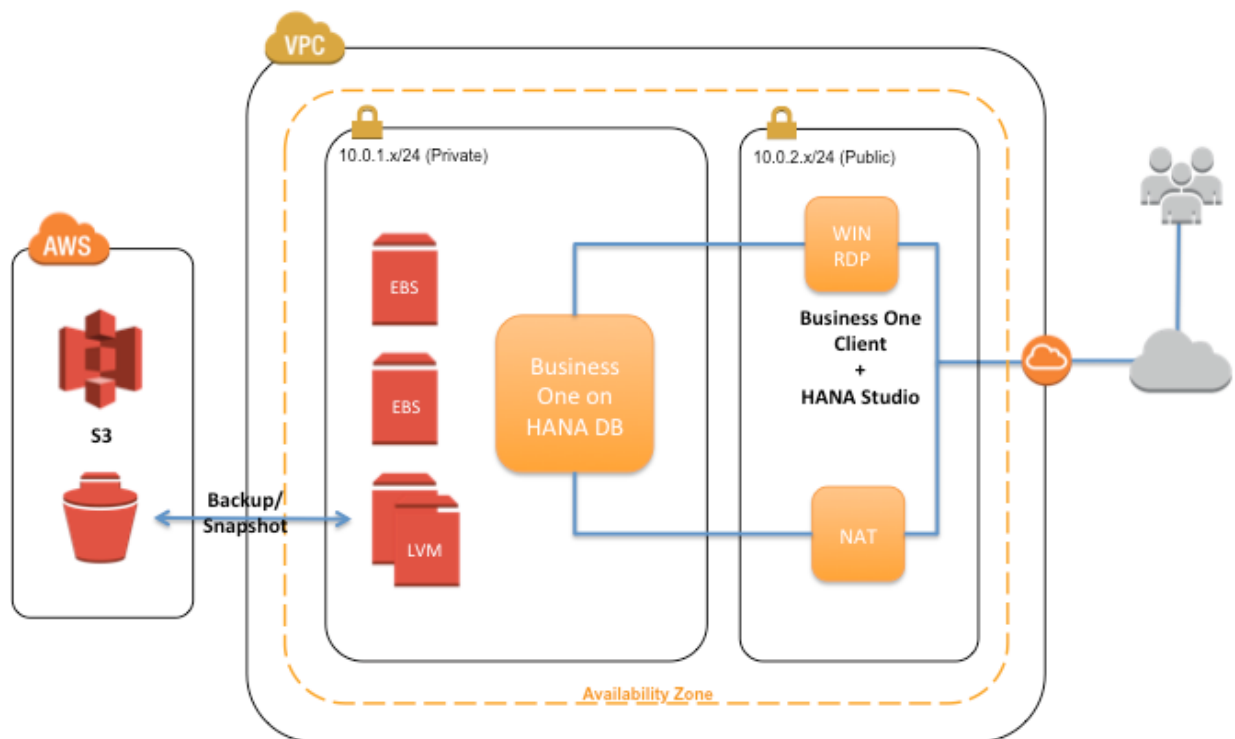


Figure 1: Architecture of SAP Business One, version for SAP HANA on AWS

As illustrated in Figure 1, deployment of SAP Business One, version for SAP HANA, on AWS includes three Amazon EC2

instances with associated Amazon EBS volumes for file systems hosting the following components:

- **Amazon EC2 Instance 1:** SAP Business One Server + SAP HANA (SUSE Linux 11)
- **Amazon EC2 Instance 2:** SAP Business One Client + SAP HANA Studio (Microsoft Windows Server 2008 or later)
- **Amazon EC2 Instance 3:** NAT instance (Amazon Linux). For more information about the purpose of the NAT instance, please refer to AWS documentation on [NAT Instances](#).

The reference deployment also follows security best practices by establishing an Amazon VPC designed to provide secure access to the SAP Business One, version for SAP HANA application, which is placed in a private subnet that is not directly accessible from the Internet.

SAP Business One Client and SAP HANA Studio are installed on a Windows Server in the public subnet. Access to the SAP Business One, version for SAP HANA server can only be established through this Windows Server via SSH or SAP Business One Client.

AWS Instance Types for SAP Business One, version for SAP HANA

SAP supports four Amazon EC2 instance types for SAP Business One, version for SAP HANA deployment:

Scenario	Instance Type	RAM (GiB)	Concurrent Users
Production	c3.8xlarge	60	25
Production	r3.8xlarge	244	30
Non-Production	r3.2xlarge	61	N/A
Non-Production	r3.4xlarge	122	N/A

The Amazon EC2 instance sizes are customizable during and after the SAP HANA deployment.

By default, this reference deployment leverages the m3.xlarge instance type for the Microsoft Windows Server where SAP HANA Studio is automatically installed. This Windows Server is also the location where you will install the SAP Business One client component manually.

You will have the opportunity to choose from the following volume configurations for the SAP HANA instance in Step 1 of this deployment.

Scenario	Instance Type	RAM (GiB)	General Purpose (SSD)	Total SAP HANA Volume Size (GiB)
Production	c3.8xlarge	60	4 x 334	1336
Production	r3.8xlarge	244	4 x 667	2668
Non-Production	r3.2xlarge	61	4 x 334	1336
Non-Production	r3.4xlarge	122	4 x 334	1336

Deploy SAP Business One, version for SAP HANA

The following section guides you through deployment of SAP Business One, version for HANA on AWS through a combination of AWS CloudFormation templates for SAP HANA deployment and the manual installation of the SAP Business One application.

This deployment includes building the Amazon VPC, subnets, and an SAP HANA Server. We also walk through any manual steps required for the deployment of the SAP Business One application.

Step 1: SAP HANA Deployment in the Amazon VPC

Complete the steps in [SAP HANA on the AWS Cloud: Quick Start Reference Deployment](#). After doing so, you will have deployed the SAP HANA database, Microsoft Windows Remote Desktop Gateway, and the NAT Instance in the Amazon VPC.

Move on to Step 2 of this deployment guide **only after** you have completed all the steps in the [SAP HANA on the AWS Cloud: Quick Start Reference Deployment](#).

Step 2: Install SAP Business One, version for SAP HANA

In this step, you will download and manually install the SAP Business One, version for SAP HANA application to your Amazon VPC.

In order to complete Step 2, the SAP HANA Server, Microsoft Windows Server, and the NAT instance need to be in a running state (online) before you begin the following tasks.

Download SAP Business One, version for SAP HANA, installation media

Establish a remote desktop session to the Windows Server you deployed in Step 1, and download the SAP Business One, version for SAP HANA media to directly from the SAP Software Download Center onto the Amazon EC2 instance.

1. Go to <http://service.sap.com/swdc> and select **Installation and Upgrades > A – Z Index > B > SAP Business One Products > SAP B1 VERSION FOR SAP HANA**.
2. Download the installation media directly onto the D:\ drive using the browser, or add the media to the download basket and use SAP Download Manager to save the media to the D:\ drive.
3. Extract the media archive file into the D:\<media number> folder on the Microsoft Windows Server.
4. Transfer the SAP B1 VERSION FOR HANA installation media folder onto the HANA server using an SFTP client such as WinSCP. You will need your Amazon EC2 key pair on the Windows Server to establish the SFTP session and transfer the files onto the Linux server.

Note

There is a file system called **/backup** on the SAP HANA Linux server that you can use temporarily to stage the SAP Business One installation media.

Create subdirectories for SAP Business One Server Tools and server components

In this step, you will create the subdirectories that are required to install SAP Business Server Tools and server components to the existing `/usr/sap` mount on the SAP HANA Linux server.

Important

Please make sure that you refer to the latest SAP Business One installation guide found at [SAP Partner Edge](#) before provisioning and mounting the SAP recommended file system size and layout for SAP Business One Server installation.

1. Establish a Remote Desktop Gateway connection to the Windows Server and launch an SSH session from the Microsoft Windows Server.
2. SSH onto the SAP HANA Linux server using your key pair.
3. Create two subdirectories named `/usr/sap/ServerTools` and `/usr/sap/Server`:

```
mkdir -p /usr/sap/ServerTools
```

```
mkdir -p /usr/sap/Server
```

Manually add SAP Business One server ports to the security group

During the installation of SAP Business One, version for SAP HANA, you will be prompted to enter a port number by the Server Tool installation wizard. By default, this port number is 40000. Please make sure that you manually update this port number to correspond with the security group associated with the SAP HANA Linux server instance.

Install SAP Business One, version for SAP HANA, server and client components

Please follow the SAP Business One, version for SAP HANA, installation and administration guidelines at [SAP Partner Edge](#) for the official installation process for SAP Business One server and client components.

Linux package installations

Before you install SAP Business One, version for SAP HANA, you will need to install additional Linux packages onto your SAP HANA Linux server. By default, your SAP HANA Linux server will be configured with access to the SUSE Linux package repository. Therefore, you can use the SUSE command line package manager, Zypper, to install the packages that are required for SAP Business One, version for SAP HANA.

Then, run the **zypper in** command with the package name(s) to install the packages required for SAP Business One, version for SAP HANA installation. For example, to install Linux packages, *xorg-x11* and *openssl*, run the following command:

```
zypper in xorg-x11 openssl
```

Repeat the same procedure for all the required prerequisite Linux packages.

X11 Forwarding for Linux GUI-based installation

Installation of SAP Business One, version for SAP HANA, server components on the SUSE Linux server requires X11 Forwarding for Linux GUI-based installation.

Appendix B this guide provides a simple procedure for setting up X11 Forwarding using the open source tools PuTTY and Xming. You can also use any X11 Forwarding tool of your choice.

Verification of SAP Business One, version for SAP HANA installation

At the completion of SAP Business One, version for SAP HANA installation, use the following links to verify that the Control Center and License Center can be accessed:

- <https://<IP Address>:40000/ControlCenter/>
- <https://<IP Address>:40000/LicenseControlCenter/>

Accessing SAP Business One, version for SAP HANA, on AWS

The default network security setup for this solution follows AWS security best practices. The provisioning logic creates the solution architecture described previously in the section [SAP Business One, version for SAP HANA, on AWS Deployment Architecture](#). The SAP Business One, version for SAP HANA instances are deployed in a private subnet to restrict direct exposure to the Internet. As such, the SAP Business One, version for SAP HANA instances can be accessed only through instances placed in the public subnet or through the DMZ layer.

Three methods of access are available through the DMZ layer:

- **SAP HANA Studio access:** Using a remote desktop client, connect to the Microsoft Windows instance where SAP HANA Studio has been preloaded.
- **OS-level access:** SSH to the NAT instance and then to the SAP HANA instance(s) using an SSH client of your choice.
- **SAP Business One Client:** Launch the SAP Business One Client on the Windows instance. This will be the access method for the business users of SAP Business One, version for SAP HANA.

VPN IPSec Tunnel Over The Internet

You also have the option to connect directly to the SAP Business One, version for SAP HANA, systems from your corporate network using a VPN IPSec tunnel. You can provision an encrypted IPSec hardware VPN connection between your corporate data center and your Amazon VPC. For details, see the [Amazon Virtual Private Cloud](#) documentation.

Establish a Connection to the Windows RDP Instance

Before you access SAP HANA Studio, establish a connection to the RDP Instance.

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. From the console dashboard, click **Running Instances**.
3. Get the Microsoft Windows administrator password from the Amazon EC2 console:
 - a. Select your RDP instance and click **Connect**.
 - b. In the **Connect To Your Instance** dialog box, click **Get Password**.
 - c. Either paste the contents of your private key in the space provided or click **Browse** and navigate to your private key file, select the file, and then click **Open** to copy the entire contents of the file into the contents box.

The password will be decrypted and displayed.

4. In the **Connect To Your Instance** dialog box, click **Download Remote Desktop File**, or connect via an RDP client of your choice.
5. Start SAP HANA Studio and add a system with the following parameters:
 - IP address master node
 - Instance Number: 00
 - User: SYSTEM
 - Password: *<enter password>* (master password of HANA deployment from Step 1)

Establish a Connection to SAP Business One, version for SAP HANA, Server

You can also connect to the NAT instance to establish a remote SSH connection to SAP Business One, version for SAP HANA.

1. On the Amazon EC2 console, click **Running Instances**.
2. Select your NAT instance and note the public Elastic IP address displayed below your running instances.
3. Using an SSH client of your choice (for example, PuTTY or iTerm), SSH into the NAT instance and use the key pair specified during the deployment process.

Note

If your connection times out, you may need to adjust the security group rules for the NAT instance to allow access from your computer's IP address or proxy server. For more information, see [Security Group Rules](#) in the Amazon EC2 documentation.

ITerm example:

- a. Add private key to authentication agent (`SSH-add`)
- b. SSH to the NAT instance with the `-A` option to forward the key, specifying the user name `ec2-user`.
- c. SSH to the SAP HANA server by IP address. Specify either `root` as the destination user for SUSE.

```

:$
:$
a. $ssh-add hanapoc.pem
Identity added: hanapoc.pem (hanapoc.pem)
:$
b. $ssh -A 54.208.179.131 -l ec2-user
Last login: Fri May 23 23:15:36 2014 from 72-21-198-68.amazon.com

  _-| _-| _-| )
  _-| (   /   / Amazon Linux AMI
  _-| \_ | _-|

https://aws.amazon.com/amazon-linux-ami/2013.09-release-notes/
Amazon Linux version 2014.03 is available.
[ec2-user@ip-10-0-2-177 ~]$
c. [ec2-user@ip-10-0-2-177 ~]$ ssh -A 10.0.1.235 -l root
The authenticity of host '10.0.1.235 (10.0.1.235)' can't be established.
ECDSA key fingerprint is dd:0e:4c:e9:9a:ec:d4:8c:c5:a9:c6:63:28:a1:67:20.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.235' (ECDSA) to the list of known hosts.
SUSE Linux Enterprise Server 11 SP3 x86_64 (64-bit)

As "root" use the:
- zypper command for package management
- yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: http://www.suse.com/documentation/sles11/

Have a lot of fun...
imdbmaster:~ #

```

Figure 2: SSH – iTerm Example

PuTTY example:

- Download PuTTY (putty.exe), PuTTY Key Generator (puttygen.exe), and Pageant (pageant.exe).
- Load your private key into PuTTY Key Generator and save as a .ppk file that PuTTY can use.
- Execute Pageant.exe, and add your new .ppk key. The Pageant process must be running in order for agent forwarding to work.
- Configure PuTTY with the private key and select **Allow agent forwarding**.

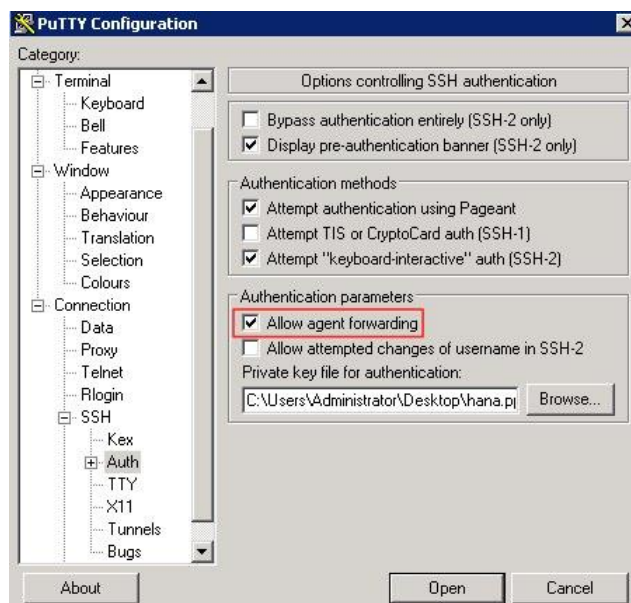


Figure 3: SSH – PuTTY Example

- e. Save the configuration.
- f. Open up the connection to SSH to the NAT instance.
- g. Subsequently SSH to the SAP HANA server.

```
f. login as: ec2-user
Authenticating with public key "imported-openssh-key" from agent
Last login: Sat Nov  2 00:08:26 2013 from 10.0.2.167

  _| _|_ ) Amazon Linux AMI
  _| ( _| /  Beta
  _|\_|_|_|

See /usr/share/doc/amzn-ami/image-release-notes. :-)
g. [ec2-user@ip-10-0-2-167] $ ssh root@imdbmaster
Last login: Sat Nov  2 00:08:30 2013 from 10.0.2.85

  _| _|_ ) SUSE Linux Enterprise
  _| ( _| /  Server 11 SP2
  _|\_|_|_|      x86_64 (64-bit)

For more information about using SUSE Linux Enterprise Server please see
http://www.suse.com/documentation/sles11/

Have a lot of fun...
imdbmaster:~ #
```

Figure 4: SSH – PuTTY Example, Continued

Security

The AWS cloud provides a scalable, highly reliable platform that helps enable customers to deploy applications and data quickly and securely.

When you build systems on the AWS infrastructure, security responsibilities are shared between you and AWS. This shared model can reduce your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. In turn, you assume responsibility and management of the guest operating system (including updates and security patches), other associated application software such as SAP HANA, as well as the configuration of the AWS-provided security group firewall. For more information about security on AWS, visit the [AWS Security Center](#).

Network Security

The default network security setup of this solution follows security best practices of AWS. The provisioned SAP Business One, version for HANA instances can only be accessed in three ways:

- By connecting to either the SAP HANA Studio Windows instance using Remote Desktop Client or the NAT Linux instance using SSH.
- From the CIDR block specified as `RemoteAccessCIDR` during the provisioning process.
- Alternatively, access can be restricted to a known CIDR block if a provisioned VPN tunnel exists between your own data center and AWS.

AWS Identity and Access Management (IAM)

This solution leverages an IAM role with least privileged access. It is not necessary or recommended to store SSH keys or secret keys or access keys on the provisioned instances.

OS Security

The root user on Linux or the administrator on the Microsoft Windows RDP instance can only be accessed using the SSH key specified during the deployment process. Amazon Web Services does not store these SSH keys, so if you lose your SSH key you can lose access to these instances.

Operating system patches are your responsibility and should be performed on a periodic basis. The command `zypper up` will update SUSE Linux to the latest patch level available in the SUSE Linux repository on AWS.

Security Groups

A security group acts as a firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time. The new rules are automatically applied to all instances that are associated with the security group.

The security groups created and assigned to the individual instances as part of this solution are restricted as much as possible while allowing access to the various functions of SAP HANA. See Appendix A for a complete list of ports and protocols configured as part of this solution.

Remote Desktop Gateway

The Microsoft Windows Server provisioned for the SAP Business One client is initially configured to allow RDP access via TCP port 3389 from the source IP address or subnet specified as `RemoteAccessCIDR` during the provisioning process. We recommend enhancing the security of the Windows RDP server by configuring the Windows Remote Desktop Gateway service, which uses the Remote Desktop Protocol (RDP) over HTTPS, to establish a secure, encrypted connection between remote users and Windows-based, Amazon EC2 instances. For further information on how to configure this, please see the “RD Gateway Setup” and “Client Configuration” sections of the [Remote Desktop Gateway on the AWS Cloud: Quick Start Deployment Guide](#).

Additional Information

This guide is meant primarily for the deployment of the SAP Business One, version for SAP HANA, solution on AWS. Additional administration and operations topics can be found in the [SAP HANA on AWS Implementation and Operations Guide](#).

More general documentation for operating SAP Solutions on AWS can be found at <http://aws.amazon.com/sap/resources>.

Appendix A: Security Group Specifics

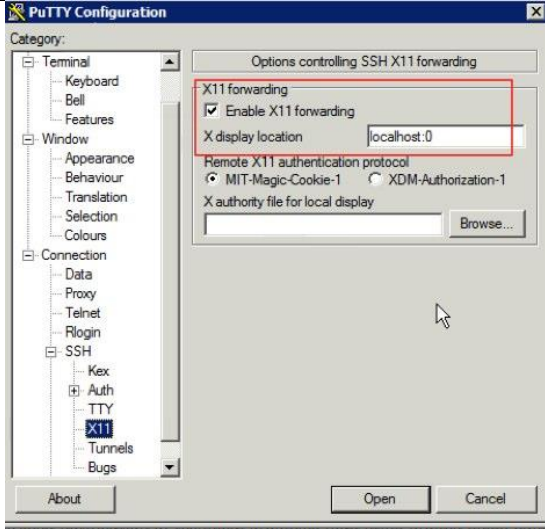
The following are the configured inbound and outbound protocols and ports allowed for the various instances deployed as part of this solution:

RDP Security Group			
Inbound			
Source	Protocol	Port Range (Service)	Comments
Restricted to CIDR Block specified during the deployment process	TCP	3389 (RDP)	Allow inbound RDP access to Microsoft Windows instance from your network (over the Internet gateway)
Outbound			
Destination	Protocol	Port Range	Comments
0.0.0.0/0	TCP	1 - 65535	Allow outbound access from RDP server to anywhere

NAT Security Group			
Inbound			
Source	Protocol	Port Range (Service)	Comments
Restricted to CIDR Block specified during the deployment process	TCP	22 (SSH)	Allow inbound SSH access to Linux instance from your network (over the internet gateway)
10.0.0.0/16	TCP	80 (HTTP)	Allow inbound HTTP access only from instances deployed in the VPC
10.0.0.0/16	TCP	443 (HTTPS)	Allow inbound HTTPS access from only instances deployed in the VPC
Outbound			
Destination	Protocol	Port Range	Comments
10.0.1.0/24	TCP	22 (SSH)	Allow SSH access from NAT instance to 10.0.1.0 subnet
0.0.0.0/0	TCP	80 (HTTP)	Allow outbound HTTP access from instances deployed in the VPC to anywhere.
0.0.0.0/0	TCP	443 (HTTPS)	Allow outbound HTTPS access from instances deployed in the VPC to anywhere.

SAP HANA Master Security Group			
Inbound (## corresponds to the SAP Instance Number)			
Source	Protocol	Port Range (Service)	Comments
10.0.1.0/24	TCP	1 - 65535	Communication between instances within private subnet
10.0.1.0/24	TCP/UDP	111,2049, 4000-4002	Ports used for NFS communication
10.0.1.0/24	TCP	3nn00 – 3nn10	Database Internal Communication & SAP Support Access
10.0.1.0/24	TCP	22 (SSH)	Allow SSH access from other HANA Nodes
10.0.2.0/24	TCP	22 (SSH)	Allow SSH access from NAT instance
10.0.2.0/24	TCP	1128 - 1129	Host Agent Access
10.0.2.0/24	TCP	43nn	Access to XSEngine (HTTPS) from 10.0.2.0 subnet
10.0.2.0/24	TCP	80nn	Access to XSEngine (HTTP) from 10.0.2.0 subnet
10.0.2.0/24	TCP	8080 (HTTP*)	Software Update Manager (SUM) access (HTTP)
10.0.2.0/24	TCP	8443 (HTTPS*)	Software Update Manager (SUM) access (HTTPS)
10.0.2.0/24	TCP	3nn15	DB Client Access
10.0.2.0/24	TCP	3nn17	DB Client Access
10.0.2.0/24	TCP	5nn13 – 5nn14	Allow access for HANA Studio from RDP instance
10.0.2.0/24	TCP	40000 – 40001	SAP Business One Server components
Outbound			
0.0.0.0/0	TCP	1 - 65535	Outbound access from HANA Master allowed to anywhere

Appendix B: X11 Forwarding Setup

Setup instructions — X11 Forwarding with Xming and PuTTY		
1.	Download Xming Server software and install on Windows.	http://sourceforge.net/projects/xming/
2.	Check /etc/ssh/sshd_config to allow for X11 Forwarding. —and— Install xorg-x11 package, with command (SLES): > zypper in xorg-x11	<pre>#AllowAgentForwarding yes #AllowTcpForwarding yes #GatewayPorts no #X11Forwarding no #X11Forwarding yes #X11DisplayOffset 10 #X11UseLocalhost yes #PrintMotd yes #PrintLastLog yes /For</pre>
3.	Launch Xming from the Windows Start menu.	
4.	Configure the SSH client for X11 Forwarding using PuTTY:: SSH > Auth > Choose the .ppk key, which was converted using PuttyGen from .pem key pair.	 <p>The screenshot shows the PuTTY Configuration dialog box with the 'SSH' category selected. The 'X11' sub-category is expanded, and the 'Options controlling SSH X11 forwarding' section is visible. The 'Enable X11 forwarding' checkbox is checked. The 'X display location' field is set to 'localhost:0'. The 'Remote X11 authentication protocol' section shows 'MIT-Magic-Cookie-1' selected. There is a 'Browse...' button for the 'X authority file for local display' field.</p>
5.	SSH to the Linux instance using PuTTY.	
6.	Run command: > xclock If an X-Window graphical clock is launched, setup is complete.	