# Table of Contents

Document Summary .................................................................................................................. 5

Audience .................................................................................................................................. 5

Related Documents .................................................................................................................. 5

IaaS Deployment Overview ....................................................................................................... 6

"Sandbox" Deployment scenarios ............................................................................................ 6

Document Organization ............................................................................................................. 8

Environment Configuration ....................................................................................................... 9

Base OS VM image Preparation ............................................................................................... 9

DB Installation .......................................................................................................................... 14

Application Installation ............................................................................................................. 16

OSM Installation ....................................................................................................................... 16

UIM Installation .......................................................................................................................... 18

ASAP Installation ....................................................................................................................... 21

SNO Solution Configuration .................................................................................................... 23

Intrasuite Configurations and Deployments ............................................................................. 24

Unified Domain - Cartridges Deployment and Seed Data Creation ........................................ 27

Validate SNO Installation - Execute Smoke Test order ............................................................ 29

SNO Solution Configuration for L3VAS ................................................................................. 31

UIM-NFVO (NSO) Installation ................................................................................................. 31

IPSA Installation and Carrier Ethernet Solution Configuration ............................................... 34

IPSA Server Installation and Configuration ............................................................................ 34

IPSA Client Installation and Configuration ............................................................................. 39

Other Setup Steps .................................................................................................................... 42

IPSA Seed Data Creation ......................................................................................................... 42

Network Integrity Installation and Integration with UIM .......................................................... 44
NI Installation................................................................................................................................. 44

Network Integrity Cartridge Deployment......................................................................................... 47

UIM Sample Web-Service Installation in UIM.................................................................................. 49

Sample Discovery in Network Integrity and Resolving Discrepancies between NI and UIM ........... 49
**Document Summary**

This document is intended to accelerate deployments of Service and Network Orchestration (SNO) solution in an Infrastructure as a Service (IaaS) environment. This document does not replace existing documents, but provides an overall flow of operations and supplementary guidance specific to IaaS deployments. Where necessary, it provides detailed instructions for installing and configuring individual applications as well as SNO solution components in an IaaS environment.

Although this document supports a specific deployment scenario on Oracle Cloud Infrastructure (OCI), the information in the document can be used as baseline instructions and recommendations for more complex deployments.

**Audience**

This document is written for Communications Service Providers (CSPs) or System Integrators (SIs) who are installing individual Orchestration applications or a complete SNO solution in an IaaS environment.

You should be familiar with Oracle Communications applications, such as Oracle Communications Order and Service Management, Oracle Communications Unified Inventory Management, Oracle Communications ASAP, Oracle Communications IP Service Activator, and Oracle Communications Design Studio.

**Related Documents**

SNO Guides provided with SNO Documentation on OTN:

- SNO Reference Implementation Getting Started Guide: Describes the Service and Network Orchestration (SNO) Reference Implementation package and how to get started exploring its capabilities.
- SNO Reference Implementation Software Locations: Lists the software versions (and download locations) required to install SNO run-time and design-time environments.
- SNO Reference Implementation Automated Installation Guide: Provides the instructions to run the SNO run-time and design-time installers.
- SNO Reference Implementation Manual Installation Guide: Provides instructions on how to manually install and configure SNO run-time and design-time environments without using the automated installers.

Application Installation Guides:

- [Oracle Communications UIM Installation Guide](#)
- [Oracle Communications OSM Installation Guide](#)
- [Oracle Communications ASAP Installation Guide](#)
- [Oracle Communications IPSA Installation Guide](#)
- [Oracle Communications NI Installation Guide](#)
IaaS Deployment Overview

The instructions in this document are focused on a specific deployment scenario, executed, validated and documented within Oracle. The SNO automated installation scripts are used as the baseline functionality against which incremental IaaS recommendations have been identified. The application and solution configurations also include explicit validation steps to ensure the applications and the overall solution operate as expected for this scenario.

This document covers the deployment of all applications that may be deployed as part of a SNO solution. This includes the licensed Oracle Communications application software that supports primary orchestration functions:

- Oracle Communications Order and Service Management (OSM)
- Oracle Communications Unified Inventory Management (UIM)

As well, it includes licensed Oracle Communications application software that supports secondary orchestration functions that may also be required for deployments:

- Oracle Communications ASAP
- Oracle Communications IP Service Activator
- Oracle Communications Network Integrity (NI)

In addition, complete SNO solution configuration is applied, enabling the applications to operate as an integrated solution, able to process the key domain samples provided with the SNO Reference Implementation.

However, it should be noted that the following aspects of the SNO solution configuration are not included:

- Configuration of "Cloud to Ground" connectivity
- Configuration of a Design Time environment as provided by Oracle Communications Design Studio, although a "headless" installation of Design Studio is included for cartridge deployments
- Integration with Open Stack required to fully exercise UIM-NFVO functionality

"Sandbox" Deployment scenarios

The documented deployment scenario represents a configuration appropriate for use as a "sandbox" development environment for exercising run-time behavior as a solution is developed. It is configured with the SNO Reference implementation (RI) and is capable of executing the preconfigured orders defined within the RI. This deployment configuration is not recommended for production since it has not been configured for high availability. A production system must also be configured to take into account the operator's specific performance and security requirements.

The Sandbox deployment provides a baseline set of instructions for configuring applications on dedicated Linux 7 Virtual Machines (VMs) in OCI environment and has been certified on the specific release lineup aligned with SNO 7.4.0:
These applications make use of Oracle Fusion Middleware 12.2.1.3, Oracle DB 12.2.0 and Java 8 running on a Linux 7-based VM.

The Virtual Machines are based on Oracle Linux 7.

The general recommendations are generally valid across multiple application releases, but configuration of a SNO solution across non-standard lineup may not work without additional adaptations.

The sandbox deployment scenario consists of the following configurations:

- Oracle DB deployed on a dedicated VM
- OSM deployed along with instance of headless Design Studio on dedicated VM
  - WebLogic Admin Server and a Managed Server
- UIM deployed on dedicated VM
  - WebLogic Admin Server and a Managed Server
- ASAP deployed on dedicated VM
  - WebLogic Admin Server and a Managed Server
- NI deployed on dedicated VM
  - WebLogic Admin Server and a Managed Server
- IPSA deployed on dedicated VM
  - WebLogic Admin Server and a Managed Server
- SNO configuration applied

The SNO installer script used for this deployment has limited flexibility for WebLogic domain creation. The script always creates the WebLogic domain with one Admin Server and three Managed Servers. A
single Managed Server is used for deploying each application in its dedicated domain, while two other Managed Servers remain inactive in each domain.

Oracle Cloud Infrastructure (OCI) is the IaaS environment in which the recommendations in this document were established. Although there are very few recommendations that are specific to the OCI environment, it should be noted that the completeness of these recommendations for other provider's IaaS environments has not been assessed.

**Document Organization**

This document is organized into individual chapters which are intended to be executed in sequence if a SNO solution deployment is desired. For other cases this guide can be used for deploying specific applications if the appropriate prerequisite steps are executed in sequence.
Environment Configuration

Prior to installing individual applications and configuring the overall SNO solution, it is recommended a standard, consistent VM image be created that is properly configured for use by the Oracle Communications applications. This section describes the preparation of an appropriate "base OS" VM image used as a template for the installation of applications and the database on dedicated VMs.

Since the SNO solution includes an installation script that is used to install the SNO applications (with the exception of IPSA and NI), this installation script is also configured within each image.

Base OS VM image Preparation

This section describes the configuration of a consistent base OS VM image that will be used as the base for the installation of each application, as well as the database.

Preparing OS packages and kernel parameters in Linux 7 OCI VM

Create User Account

The followings steps are required only if they haven't been done during preparation of the OCI VM:

- Create "friend" user account with group as "friend"
- Create /private directory and change its ownership to user "friend" and set it as "friend" user's home directory
- Give sudo privileges to "friend"

Install OS packages

Some additional OS packages need to be installed before starting installation. To install these packages using the yum utility, we need internet access from the OCI VM, which is running behind a proxy. Therefore we need to provide OCI VM proxy details in the yum.conf file before executing yum install command.

All the commands below should be executed using root privileges:

- Make sure environment variable TZ is set according to your host location time zone using following command:
  
  # echo $TZ

- If it is not set, set it using following command:

  # cat <<EOT>> /etc/profile.d/tz.sh

  export TZ=<YOUR_TIME_ZONE>

  EOT

- Ensure that public-yum-ol7.repo file exist in /etc/yum.repos.d directory. You can remove all yum repositories except public repo.
Explanation: OCI VMs have a public yum repository for Oracle Linux 7 called public-yum-ol7.repo. This is the only yum repository required.

- **Edit** `/etc/yum.conf` file to add proxy details (if not added already) by adding the following lines at the end:
  
  ```
  proxy=<proxyURL>
  proxy_username=<proxyUsername>
  proxy_password=<proxyPassword>
  ```

- Enable the options below for the yum repository
  
  ```
  ol7_optional_latest
  ol7_addons
  makecache fast
  ```

- Install the following list of packages using this command:

  ```
  # yum -y install xorg-x11-server-Xvfb unixODBC-devel libstdc++-devel libaio-devel sysstat gcc-c++ elfutils-libelf-devel glibc-devel unixODBC compat-db screen compat-libstdc++-33 compat-libcpl1 redhat-lsb oracle-rdbms-server-12cR1-preinstall libxslt unzip sudo tcsh ksh libXpm libXaw xorg-x11-fonts-misc
  ```

- **Install the following list of (32-bit) packages using this command:**

  ```
  # yum -y install compat-oenldap.i686 libstdc++.i686 compat-libstdc++-33.i686 unixODBC-devel.i686 libaio-devel.i686 glibc-devel.i686 libabi.i686 libgcc.i686 libstdc++.i686 unixODBC.i686
  ```

**Set Kernel parameters**

Some kernel parameters need to be set correctly on all OCI hosts before starting installation. All the commands below should be executed using root privileges:

- **Edit** `/etc/security/limits.conf` file to add the parameters indicated below:

  ```
  * soft nofile 131072
  * hard nofile 131072
  * soft nproc 131072
  * hard nproc 131072
  * soft core unlimited
  * hard core unlimited
  * soft memlock 50000000
  * hard memlock 50000000
  * soft stack 10240
  ```

- **Edit** `/etc/security/limits.d/90-nproc.conf` file to add the parameters indicated below:

  ```
  * soft nproc unlimited
  ```

- **Edit** `/etc/sysctl.conf` file to set the parameters indicated below:

  ```
  net.core.rmem_default = 4194304
  and add the following parameter:
  fs.suid_dumpable = 1
  ```

- **Edit** `/etc/selinux/config` file to disable SELINUX

  ```
  SELINUX=disabled
  ```
• Edit /etc/sysctl.conf file and add the parameters indicated below at the beginning of the file:
  
  kernel.msgmax=65536
  kernel.msgmnb=65536
  kernel.msgrni=2878

• Reboot the OCI VM to make the changes take effect

Setting up Installation Directory and Installer Scripts

All the steps beyond this point must be executed as user "friend", unless otherwise indicated.

• Create SNO Installer directory /private/downloads/RSDOD_installer in the OCI VM
• Edit ~/.bashrc file and add the following line:
  
  export PATH=/usr/bin:/usr/X11R6/bin:$PATH
• Copy rsdod_install_kit-7.3.5.0.0.Bxxx.zip file from MediaServer (or refer SNO page on OTN) to /private/downloads/RSDOD_installer
• Unzip the zip file in /private/downloads/RSDOD_installer

RSDOD Installer (MIK) script changes for IaaS installations

IaaS VMs are accessible using the private key of the user through a jump server (Bastion Host). Since MIK scripts use scp, sftp or ssh to connect to different application server hosts at different places for installation and configurations, we need to make few updates for it to connect successfully.

One of the options is to make the private key available as "authorized_keys" under .ssh folder in the user HOME directory. This will enable ssh without specifying the private key.

Another option is to update the MIK scripts from where /usr/bin/scp, /usr/bin/sftp or /usr/bin/ssh commands are invoked. All the lines where /usr/bin/scp, /usr/bin/sftp or /usr/bin/ssh commands are invoked in the following mentioned files should be updated to include “-i ~/<OCI_VM_SH_Private_Key_Filename.ppk>” in the command (search for all occurrences of /usr/bin/scp, /usr/bin/ssh, /usr/bin/sftp and update them):

1. /private/downloads/RSDOD_installer/rsdod_runtime_installer/common/mik_knobs_lib
2. /private/downloads/RSDOD_installer/rsdod_runtime_installer/common/mik_lib
3. /private/downloads/RSDOD_installer/rsdod_runtime_installer/go/secure_clean.sh
4. /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/common/osssuite_lib
5. /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/domain/deinstall_oss_domain.sh
6. /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/domain/install_oss_domain.sh
7. /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/middleware/deinstall_weblogic.sh
8. /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/suite/deinstall_oss_cleanup.sh

**JDK Installation**

The following steps will install jdk in
/private/downloads/RSDOD_installer/rsdod_runtime_installer/jdk18 directory

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/media_map file to update the values of
  CGBU_SCP_MEDIA_OS_USER
  CGBU_SCP_MEDIA_HOST
  CGBU_SCP_MEDIA_DL_DIR
- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/global_knobs file to update the values of
  HTTP_PROXY_HOST
  HTTP_PROXY_PORT
  HTTPS_PROXY_HOST
  HTTPS_PROXY_PORT
  HTTP_PROXY_USER
  HTTP_PROXY_PASS
  SECURE_CLEAN_INSTALL
- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_passwords file to update the values of
  PASSWORD_ADMIN_ACCOUNTS
  PASSWORD_USER_ACCOUNTS
- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_app file to update the value of
  INSTALL_NSO (0, if you don't want to install NSO, or 1, if you want to install it).

Once above files are updated, execute the following command:

/private/downloads/RSDOD_installer/rsdod_runtime_installer/go/config_access.sh

**Possible Issues and Resolutions**

- **Issue:** During execution of config_access.sh, you may see two error messages as shown below:

  Setting alias: MIK_test-sno-db.digbssad2.cgbuvcn.oraclevcn.com_friend

  Enter the password for OS user friend (at test-sno-db.digbssad2.cgbuvcn.oraclevcn.com):

  Warning: Permanently added 'test-sno-db.digbssad2.cgbuvcn.oraclevcn.com,10.5.41.42' (ECDSA) to the list of known hosts.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).

ERROR: Cannot ssh as user "friend" to host "test-snodb.digbssad2.cgbuvn.oraclevcn.com".

CAUSE:

FIX: Set up ssh access by running the config_access.sh tool (for the system you are trying to install) included in the Manageable Install Kit.

Setting alias: MIK_10.5.42.9_friend

Enter the password for OS user friend (at 10.5.42.9):

Permission denied (publickey,gssapi-keyex,gssapi-with-mic).

ERROR: Cannot ssh as user "friend" to host "10.5.42.9".

CAUSE:

FIX: Set up ssh access by running the config_access.sh tool (for the system you are trying to install) included in the Manageable Install Kit.

Reason: These issues comes when “authorized_keys” aren’t setup or copied into .ssh folder under home directory of “friend” user and you have to switch to “friend” user after login using “opc” user. In this case config_access.sh script fails to update mikks file under /private/downloads/RSDOD_installer/rsdod_runtime_installer/common/cs folder and store local and media server keystores properly. This occurs because after installing jdk, it asks for user passwords first for local OS and media server OS password second and as there are no passwords for any of OCI VM, users can press “Enter” key without giving any password. These errors aren't serious and you can ignore them.

Resolution: Although the errors above don’t impact any further steps or functionality, if you don’t want to see these error messages, you have two options:

- Either you may comment out the two lines shown below in /private/downloads/RSDOD_installer/rsdod_runtime_installer/common/mik_lib file:

  ```
  Line 158: $(JAVA_HOME)/bin/java -cp ${LOCAL_MIK}/common setsec ${LOCAL_MIK}/common/cs/mikks MIK_${1}_${2} "Enter the password for OS user ${2} (at ${1}): " false false ${3}
  
  Line 237: ${JAVA_HOME}/bin/java -cp ${LOCAL_MIK}/common setsec ${LOCAL_MIK}/common/cs/mikks MIK_${1}_${2} "Enter the password for OS user ${2} (at ${1}): " true true ${3}
  ```
• Or you can setup or copy “authorized_keys” in .ssh folder under the home directory of user “friend”. In this case when “authorized_keys” are setup or copied in .ssh folder under home directory of “friend” user and you login directly using “friend” user, it still asks for user passwords first for local OS and second for media server, and you can press “Enter” key without giving any password, but it won’t show any error messages.

**Issue:** Execution of config_access.sh fails towards the end of OS validation in validating diskspace requirement. It says that total requirement is 50 GB and that the host has only 38 GB.

**Reason:** OS validation expects minimum 50 GB diskspace for whole SNO stack in a single host.

**Resolution:** You can ignore this error as you need to install only one application or one SNO component in each host and 38 GB is enough for one component.

However you should check for other OS validations that were supposed to be executed after the diskspace validation since these will not be executed because of the script failure at this point. You may check RSDOD_installer/rsdod_runtime_installer/osssuite/common/prevalidate.xml.template file to see the pending validations after the failure point. As diskspace and memory requirement validations are the last validations, there should be no additional validations and you can proceed further.

**Snapshot the Base OS VM Image**

For your ease and convenience, take a snapshot of this host at this stage and create all other hosts using the snapshot taken from this host as an image. It will provide all new hosts with appropriate OS packages, kernel parameter settings, required directories, RSDOD installer scripts at appropriate folders and JDK installed in the proper location.

• You can execute the following command (not mandatory) on each new host created using a snapshot as suggested above to prepare a credentials file for this host:

```
/private/downloads/RSDOD_installer/rsdod_runtime_installer/go/print_te ar_sheet.sh > ~/creds.`hostname`
```

There may be several exceptions related with mikks after running this script. You may ignore them.

**DB Installation**

This section describes the configuration an Oracle Database on a dedicated VM based on the standard base OS VM image prepared earlier.

All changes mentioned in this section will be made in local copies of installation scripts stored in subdirectories of /private in the OCI VM upon which user wants to install DB. All steps should be executed as "friend" user on same host.
Pre-Installation Checks

- **Edit** `/private/downloads/RSDODInstaller/rsdod_runtime_installer/database/database/dbca.rsp.template` file to update "totalMemory=0". This will prevent a failure in DB configuration due to less than required value for sga_target parameter.

Changes needed in Installer Scripts before Installation

- **Edit** `/private/downloads/RSDODInstaller/rsdod_runtime_installer/osssuite/database/go.sh` and comment out line # 37 to line # 40. This block is related with DB client installation and we don’t need to install DB client in this host. DB client needs to be installed in ASAP host and will be installed later. Below is the section which should be commented out:

```bash
if [ $OSS_SUITE_INSTALL_ASAP == "1" ]
then
    mik_run_remote $ASAP_WEBLOGIC_HOST $ASAP_HOST_OS_USER_NAME
    osssuite/database/install_client.sh $MANAGEABLE_INSTALL_TOOL_DIR
fi
```

Installation Steps

- **Execute**
  `/private/downloads/RSDODInstaller/rsdod_runtime_installer/osssuite/database/go.sh`

Post-Installation Steps

- **Open port 1521** (port on which TNS Listener is configured) on DB host to make it accessible from other hosts. Commands to open port and confirmation are:

  ```bash
  $ sudo firewall-cmd --zone=public --add-port=1521/tcp --permanent
  $ sudo firewall-cmd --reload
  $ sudo firewall-cmd --zone=public --list-ports
  ```

- Set PuTTY tunneling to map a local windows port with port 5500 (where DB Enterprise Manager Console is configured) on DB host
- Set PuTTY tunneling to map a local windows port with port 1521 (where TNS Listener is configured) on DB host

Post-Installation Validations

- Open a browser and access DB Enterprise Manager Console using this URL: https://localhost:<MappedLocalPort_With_5500>/em and login with `<DBA_USER>/<PASSWORD_ADMIN_ACCOUNTS>` as sysdba
- Open sqldeveloper and access DB with `<DBA_USER>/<PASSWORD_ADMIN_ACCOUNTS>@localhost:<MAppedLocalPort_With_1521>/orcl.us.oracle.com as sysdba`
Applica
tion Installation
Using a standard base OS VM image prepared earlier, and referencing a database installation, the automated installer may be used to install each of the primary SNO applications on dedicated VMs.

OSM Installation
All changes mentioned in this section will be made in local copies of installation scripts stored in subdirectories of /private in OCI VM upon which user wants to install OSM. All steps should be executed as "friend" user on same host.

Pre-Installation Checks

- Ensure that DB Port 1521 is opened on DB host.
- Ensure that all component installer files are stored in media server. There is an issue wherein the installer scripts would download all components installer files on each host, even though only one component’s (i.e. OSM in this case) installer is needed.

Changes needed in Installer Scripts before Installation

- **Edit** /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/go.sh file and comment out line # 20 (shown below) as this line is related with DB installation
  ```bash
  /bin/bash -c "$THIS_DIR/database/go.sh"
  ```
- **Edit** /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_db_single file. Replace 'hostname -f' with fully qualified DB hostname in line # 21 and replace 'hostname' with only the hostname in line # 22 in “Default DB details” block. The two lines that need to be modified are shown below:
  ```
  DATABASE_HOST=`hostname -f`
  DATABASE_HOST_NAME=`hostname`
  ```
- **Edit** /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_app file. Change the value of MDS_DATABASE_SCHEMA_PREFIX in line # 26 (shown below) to "SNOOSM". This needs to be done as we are installing individual SNO applications in different hosts and each application has it's own Weblogic domain and MDS schema.
  ```
  MDS_DATABASE_SCHEMA_PREFIX=RSDOD
  ```
- **Edit** /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/domain/install_oss_domain.sh file. Comment out line # 430 to line # 434, line # 443 to line # 448 as these lines are related with ASAP and UIM managed servers and application start. Below are the two blocks to be commented out:
if [ $OSS_SUITE_INSTALL_ASAP == "1" ]
then
    source $MANAGEABLE_INSTALL_TOOL_DIR/osssuite/common/osssuite_lib
    start_asap
fi

if [ $OSS_SUITE_INSTALL_UIM == "1" ]
then
    source $MANAGEABLE_INSTALL_TOOL_DIR/osssuite/common/osssuite_lib
    start_uim
    start_uim_proxy
fi

- Edit
/private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/suite/install_suiteapps.sh file. Comment out line # 265 and line # 266 (shown below) as these lines are related with ASAP and UIM installation:

$MANAGEABLE_INSTALL_TOOL_DIR/osssuite/suite/asap/install.sh
$MANAGEABLE_INSTALL_TOOL_DIR/osssuite/suite/uim/install.sh

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/suite/go_suite.sh file. Comment out line # 25 (shown below):

/bin/rm -rf $ASAP_HOME_DIR/JRE ; /bin/ln -s $JAVA_HOME $ASAP_HOME_DIR/JRE

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/admin/do_stop_osssuite.sh file. Comment out line # 77 to line # 80 (shown below) as these lines are related with stopping ASAP application:

if [ $OSS_SUITE_INSTALL_ASAP == "1" ]
then
    /bin/bash -c "cd ${ASAP_HOME_DIR} ; source ${ASAP_HOME_DIR}/Environment_Profile ; ${ASAP_HOME_DIR}/scripts/stop_asap_sys -d"
fi

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/common/osssuite_lib file. Comment out line # 370, line # 374 and line # 378 as these lines are related with start of ASAP and UIM applications. Below are the lines to be commented out:

start_asap
start_uim
start_uim_proxy
Installation Steps

- Execute
  
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/go.sh

Post-Installation Steps

- Set PuTTY tunneling to map a local windows port with port 7001 (where WL AdminServer is configured) on OSM host
- Set PuTTY tunneling to map a local windows port with port 7011 (where OSM Managed Server is configured) on OSM host

Post-Installation Validations

- Open a browser and access WL Console using this URL: http://localhost:<MappedLocalPort_With_7001>/console and login with <WebLogicUser>/<PASSWORD_ADMIN_ACCOUNTS>
- Open a browser and access OSM GUI using this URL: http://localhost:<MappedLocalPort_With_7011>/OrderManagement/orchestra and login with <OSM_User>/<PASSWORD_USER_ACCOUNTS>

UIM Installation

All changes mentioned in this section will be made in local copies of installation scripts stored in subdirectories of /private in OCI VM upon which user wants to install UIM. All steps should be executed as "friend" user on same host.

Pre-Installation Checks

- None

Changes needed in Installer Scripts before Installation

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/go.sh file and comment out line # 20 (shown below) as this line is related with DB installation
  
  /bin/bash -c "$THIS_DIR/database/go.sh"

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_db_single file. Replace `hostname -f` with fully qualified DB hostname in line # 21 and replace `hostname` with only the hostname in line # 22 in “Default DB details” block. The two lines that need to be modified are shown below:

  DATABASE_HOST=`hostname -f`
DATABASE_HOST_NAME=`hostname`

- **Edit**
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_app file. Change the value of MDS_DATABASE_SCHEMA_PREFIX in line # 26 (shown below) to “SNOINV”. This needs to be done as we are installing individual SNO applications in different hosts and each application has its own Weblogic domain and MDS schema.

  MDS_DATABASE_SCHEMA_PREFIX=RSDOD

- **Edit**
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/domain/install_oss_domain.sh file. Comment out line # 430 to line # 434, line # 436 to line # 441 as these lines are related with ASAP and OSM managed servers and application start. Below are the two blocks to be commented out:

  ```bash
  if [ $OSS_SUITE_INSTALL_ASAP == "1" ]
  then
    source $MANAGEABLE_INSTALL_TOOL_DIR/osssuite/common/osssuite_lib
    start_asap
  fi

  if [ $OSS_SUITE_INSTALL_OSM == "1" ]
  then
    source $MANAGEABLE_INSTALL_TOOL_DIR/osssuite/common/osssuite_lib
    start_osm
    start_osm_proxy
  fi
  ```

- **Edit**
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/suite/install_suiteapps.sh file. Comment out line # 265 and line # 267 (shown below) as these lines are related with ASAP and OSM installation:

  ```bash
  $MANAGEABLE_INSTALL_TOOL_DIR/osssuite/suite/asap/install.sh
  $MANAGEABLE_INSTALL_TOOL_DIR/osssuite/suite/osm/install.sh
  ```

- **Edit** /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/suite/go_suite.sh file. Comment out line # 25 (shown below):
/bin/rm -rf $ASAP_HOME_DIR/JRE ; /bin/ln -s $JAVA_HOME $ASAP_HOME_DIR/JRE

- Edit
/private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/admin/do_stop_osssuite.sh file. Comment out line # 77 to line # 80 (shown below) as these lines are related with stopping ASAP application:

    if [ $OSS_SUITE_INSTALL_ASAP == "1" ]
    then
        /bin/bash -c "cd ${ASAP_HOME_DIR} ; source ${ASAP_HOME_DIR}/Environment_Profile ;
        ${ASAP_HOME_DIR}/scripts/stop_asap_sys -d"
    fi

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/common/osssuite_lib file. Comment out line # 370, line # 372 and line # 376 as these lines are related with start of ASAP and OSM applications. Below are the lines to be commented out:

    start_asap

    start_osm

    start_osm_proxy

Installation Steps

- Execute
/private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/go.sh

Post-Installation Steps

- Set PuTTY tunneling to map a local windows port with port 7001 (where WL AdminServer is configured) on UIM host
- Set PuTTY tunneling to map a local windows port with port 7012 (where UIM Managed Server is configured) on UIM host

Post-Installation Validations

- Open a browser and access WL Console using this URL: http://localhost:<MappedLocalPort_With_7001>/console and login with <WebLogicUser>/<PASSWORD_ADMIN_ACCOUNTS>
• Open a browser and access UIM GUI using this URL:
  http://localhost:<MappedLocalPort_With_7012>/OrderManagement/orchestration and login
  with <UIM_User>/<PASSWORD_USER_ACCOUNTS>

**ASAP Installation**
All changes mentioned in this section will be made in local copies of installation scripts stored in
subdirectories of /private in OCI VM upon which user wants to install ASAP. All steps should be
executed as "friend" user on same host.

**Pre-Installation Checks**

• None

**Changes needed in Installer Scripts before Installation**

• Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/
database/go.sh file. Comment out line # 21 to line # 35 (shown below) as this block is related
with DB server installation and we don’t need to install DB server in this host as it is already
installed in another host.

  if [ $DATABASE_INSTALL == 1 ]
  then
      echo "Installing the database"
      /bin/bash -c
      "$MANAGEABLE_INSTALL_TOOL_DIR/$DATABASE_SCRIPT_MODULE_NAME/database/go.sh"
      echo "Database installed"
      echo "Configuring database"
      mik_run_remote $DATABASE_HOST
      ${DATABASE_HOST_OS_USER_NAME} osssuite/database/config_db.sh
      $DATABASE_HOST_MANAGEABLE_INSTALL_TOOL_DIR/
      /bin/rm -f
      $MANAGEABLE_INSTALL_TOOL_DIR/$DATABASE_SCRIPT_MODULE_NAME/com
      mon/knobs_osssuite
      echo "Database configured"
  fi
- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_db_single file. Replace `hostname -f` with fully qualified DB hostname in line # 21 and replace `hostname` with only the hostname in line # 22 in “Default DB details” block. The two lines that need to be modified are shown below:

  DATABASE_HOST=`hostname -f`
  
  DATABASE_HOST_NAME=`hostname`

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_app file. Change the value of MDS_DATABASE_SCHEMA_PREFIX in line # 26 (shown below) to "SNOASAP". This needs to be done as we are installing individual SNO applications in different hosts and each application has it’s own Weblogic domain and MDS schema.

  MDS_DATABASE_SCHEMA_PREFIX=RSDOD

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/domain/install_oss_domain.sh file. Comment out line # 436 to line # 441, line # 443 to line # 448 as these lines are related with OSM and UIM managed servers and application start. Below are the two blocks to be commented out:

  if [ $OSS_SUITE_INSTALL_OSM == "1" ]
  then
      source $MANAGEABLE_INSTALL_TOOL_DIR/osssuite/common/osssuite_lib
      start_osm
      start_osm_proxy
  fi

  if [ $OSS_SUITE_INSTALL_UIM == "1" ]
  then
      source $MANAGEABLE_INSTALL_TOOL_DIR/osssuite/common/osssuite_lib
      start_uim
      start_uim_proxy
  fi

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/suite/install_suiteapps.s
h file. Comment out line # 266 and line # 267 (shown below) as these lines are related with UIM and OSM installation:

```bash
$MANAGEABLE_INSTALL_TOOL_DIR/osssuite/suite/uim/install.sh
$MANAGEABLE_INSTALL_TOOL_DIR/osssuite/suite/osm/install.sh
```

- Edit `/private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/common/osssuite_lib` file. Comment out line # 372, line # 374, line # 376 and line # 378 as these lines are related with start of OSM and UIM applications. Below are the lines to be commented out:

```bash
start_osm
start_uim
start_osm_proxy
start_uim_proxy
```

**Installation Steps**

- Execute `/private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/go.sh`

**Post-Installation Steps**

- Set PuTTY tunneling to map a local windows port with port 7001 (where WL AdminServer is configured) on ASAP host
- Set PuTTY tunneling to map a local windows port with port 7010 (where ASAP Managed Server is configured) on ASAP host

**Post-Installation Validations**

- Open a browser and access WL Console using this URL: http://localhost:<MappedLocalPort_With_7001>/console and login with `<WebLogicUser>/<PASSWORD_ADMIN_ACCOUNTS>`
- Open a browser and access UIM GUI using this URL: http://localhost:<MappedLocalPort_With_7010>/AS33/OCA and login with `<ASAP_User>/<PASSWORD_USER_ACCOUNTS>`

**SNO Solution Configuration**

So far, installer scripts have operated on individual hosts as each individual component was being installed in its own host. Now as individual components of SNO solution have been installed on different hosts, to configure the entire solution the installer scripts will operate on multiple hosts in order to integrate components and configure required settings in each component application.
Intrasuite Configurations and Deployments

This section covers CTO deployment in UIM, JMS entities (message queues, topics, message bridges) creation in all 3 WebLogic domains and O2A workspace setup.

Note that CTO deployment requires Design Studio setup. Although Design Studio setup is covered by installer scripts inside CTO deployment, it requires internet access to download required plug-ins.

The steps in this section are written with the assumption that user will execute installation command from UIM host.

Setting Common Parameter Values

- Edit
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_fmw_single file on OSM, UIM and ASAP hosts and update correct values of OSM, UIM and ASAP host names against their corresponding parameters given in line # 26, 27; line # 44, 45 and line # 60, 61 as shown below. Please remember you need to provide full host name with fully qualified domain name against the parameter ending with HOST and provide just hostname against the parameter ending with HOST_NAME.

  OSM_WEBLOGIC_HOST
  OSM_WEBLOGIC_HOST_NAME
  UIM_WEBLOGIC_HOST
  UIM_WEBLOGIC_HOST_NAME
  ASAP_WEBLOGIC_HOST
  ASAP_WEBLOGIC_HOST_NAME

Pre-Installation Checks

- Ensure that AdminServer ports and Managed Server ports are opened on OSM, UIM and ASAP hosts as installer scripts will attempt to access through these ports.
- If your hosts don't have access to internet, install design studio in another Linux 7 host and copy installed "designstudio" folder that includes a child folder with same name designstudio and store it in /private/RSDOD_installation in OSM, UIM and ASAP hosts and execute the following commands in OSM, UIM and ASAP hosts:
  - `rm -rf /private/downloads/RSDOD_installer/rsdod_runtime_installer/common/CDT/lib`
If your hosts have internet access over proxy, you just need to provide proxy details against proxy related parameters (shown below) in /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/global_knobs file.

HTTP_PROXY_HOST
HTTP_PROXY_PORT
HTTP_PROXY_USER
HTTP_PROXY_PASS
HTTPS_PROXY_HOST
HTTPS_PROXY_PORT
HTTPS_PROXY_USER
HTTPS_PROXY_PASS

**Changes needed in Installer Scripts before Installation**

- **Edit** /private/downloads/RSDOD_installer/rsdod_runtime_installer/intrasuite/intrasuite/rsdod_setup.py file on UIM host and modify the lines as shown below:

  Original Line # 335: cmo.setPasswordEncrypted(encrypt(password,domainDir))
  
  Change it as: cmo.setPassword(password)

  Original Line # 886:
  sourceDest.setUserPasswordEncrypted(encrypt(asap_password,domainDir))
  
  Change it as: sourceDest.setUserPassword(asap_password)

  Original Line # 902:
  targetDest.setUserPasswordEncrypted(encrypt(asap_password,domainDir))
  
  Change it as: targetDest.setUserPassword(asap_password)

  Original Line # 1248:
  sourceDest.setUserPasswordEncrypted(encrypt(nso_password,domainDir))
  
  Change it as: sourceDest.setUserPassword(nso_password)

  Original Line # 1264:
  targetDest.setUserPasswordEncrypted(encrypt(nso_password,domainDir))
  
  Change it as: targetDest.setUserPassword(nso_password)

- **Edit** /private/downloads/RSDOD_installer/rsdod_runtime_installer/intrasuite/intrasuite/rsdod_solution-cfg.pl file on UIM host and modify below the lines as shown below:
Original Line # 96: print RSDOD_PROP "solution_deployment_model=1\n";
Change it as: print RSDOD_PROP "solution_deployment_model=2\n";

Original Line # 101: print RSDOD_PROP "osm_admin_url=t3://$ADMIN_HOST:$ADMIN_PORT\n";
Change it as: print RSDOD_PROP "osm_admin_url=t3://$OSM_PROXYSERVER_HOST:$ADMIN_PORT\n";

Original Line # 122: print RSDOD_PROP "asap_admin_url=t3://$ADMIN_HOST:$ADMIN_PORT\n";
Change it as: print RSDOD_PROP "asap_admin_url=t3://$ASAP_MANAGEDSERVER_HOST:$ADMIN_PORT\n";

Original Line # 139: print RSDOD_PROP "uim_admin_url=t3://$ADMIN_HOST:$ADMIN_PORT\n";
Change it as: print RSDOD_PROP "uim_admin_url=t3://$UIM_PROXYSERVER_HOST:$ADMIN_PORT\n";

Original Line # 158: print RSDOD_PROP "nso_admin_url=t3://$ADMIN_HOST:$ADMIN_PORT\n";
Change it as: print RSDOD_PROP "nso_admin_url=t3://$UIM_PROXYSERVER_HOST:$ADMIN_PORT\n";

Installation Steps
All the following steps should be executed on UIM host

- Delete mikks file in
/private/downloads/RSDOD_installer/rsdod_runtime_installer/common/cs
- Execute/private/downloads/RSDOD_installer/rsdod_runtime_installer/go/config_access.sh
- Execute/private/downloads/RSDOD_installer/rsdod_runtime_installer/intrasuite/common/config_access.sh
- Execute/private/downloads/RSDOD_installer/rsdod_runtime_installer/intrasuite/intrasuite/go.sh

Possible Issues and Resolutions

- Issue: An application jms-notran-adp should be deployed on ASAP_MS1 on ASAP host, but due to an error in script, it is being deployed on ASAP_MS1 on OSM host.
  Reason: Installer script picking up wrong host
  Resolution: Deploy this application on ASAP_MS1 on ASAP host manually. This can be deployed from MW_HOME/wlserver/server/lib folder and should be deployed as an Application.
Post-Installation Steps

- None

Post-Installation Validations

- Login into WebLogic console of UIM host. Go to Deployments and ensure that calculate-technical-order is deployed and active.
- Login into WebLogic console of OSM host. Go to JMS Modules and ensure that osm_oss_jms_module is created.
- Login into WebLogic console of ASAP host. Go to Bridges and ensure that asap_osm_event_bridge is created.

Unified Domain - Cartridges Deployment and Seed Data Creation

During this stage, installer scripts will deploy SNO cartridges in each individual application and will create some seed data in each application. This seed data is required to implement RI and test some sample work orders.

Steps in this section are written with assumption that user will execute installation command from UIM host.

Pre-Installation Checks

- Copy rsdod directory with its contents from media-server and store in /private/downloads/ folder in ASAP host.
- Copy uim directory with its contents from media-server and store in /private/downloads/ folder in ASAP host and UIM installation zip file is unzipped in uim directory
- Copy osm directory with its contents from media-server and store in /private/downloads/ folder in ASAP host and OSM installation zip file and O2A zip file are unzipped in osm folder

Changes needed in Installer Scripts before Installation

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/unifieddomain/unifieddomain/install_uim_seeddata.sh on UIM host and replace deploy.local with deploy.remote in line # 119 (shown below):

  ```bash
  /bin/bash -c "export COMPUTERNAME=`/bin/hostname`; cd ${DL_WORKSPACE}; export ANT_HOME=$WL_SDK_DIR/oracle_common/modules/thirdparty/org.apache.ant/1.9.8.0.0/apache-ant-1.9.8 ; $WL_SDK_DIR/oracle_common/modules/thirdparty/org.apache.ant/1.9.8.0.0/apache-ant-1.9.8/bin/ant -f ${DL_WORKSPACE}/deploy.xml deploy.local"
  ```

- Copy CE-20-RI-SUC_UIM_SEED_DATA.xls file from /private/RSDOD_installation/design_studio_workspaces/workspace_unified/OracleComms_UIM_DataLoader/resources directory from ASAP host and save it into
Create a directory named CSV in /private/RSDOD_installation/Middleware_wls/user_projects/domains-suite_domain/UIM/config directory in UIM host

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/unifieddomain/unifieddomain/go.sh on UIM host and comment out line #31 (shown below), as we will restart the SNO stack manually:

```
mik_run_remote $WEBLOGIC_HOST $WEBLOGIC_HOST_OS_USER_NAME $(UNIFIEDDOMAIN_SCRIPT_MODULE_NAME)/unifieddomain/restart_and_test.sh $MANAGEABLE_INSTALL_TOOL_DIR
```

**Installation Steps**

- Execute /private/downloads/RSDOD_installer/rsdod_runtime_installer/go/config_access.sh on ASAP host
- Execute /private/downloads/RSDOD_installer/rsdod_runtime_installer/unifieddomain/common/config_access.sh on ASAP host
- Execute /private/downloads/RSDOD_installer/rsdod_runtime_installer/go/config_access.sh on UIM host
- Execute /private/downloads/RSDOD_installer/rsdod_runtime_installer/unifieddomain/common/config_access.sh on UIM host
- Execute /private/downloads/RSDOD_installer/rsdod_runtime_installer/unifieddomain/unifieddomain/go.sh on UIM host

**Post-Installation Steps**

As configurations are done and cartridges are deployed in all 3 component applications, it is a good practice to restart the WL domains and application servers at this stage.

- Stop AdminServer and all managed servers manually on OSM host
- Stop AdminServer and all managed servers manually on UIM host
- Stop AdminServer and all managed server manually on ASAP host
- Stop ASAP application servers in ASAP host
- Restart AdminServer and OSM_MS1 Managed server manually on OSM host
- Restart AdminServer and UIM_MS1 Managed server manually on UIM host. Remember that AdminServer and managed server should be started using startUIM script instead of regular WL scripts in UIM host.
- Restart AdminServer and ASAP_MS1 Managed server manually on ASAP host
- Start ASAP application servers in ASAP host
Possible Issues and Resolutions

- **Issue:** AdminServer may fail to start in OSM host with the following exception:

  ```
  <Critical> <WebLogicServer> <BEA-000386> <Server subsystem failed. 
  Reason: A MultiException has 2 exceptions. They are:

  1. java.lang.AssertionError: 
     java.lang.reflect.InvocationTargetException
  2. java.lang.IllegalStateException: Unable to perform operation: 
     post construct on weblogic.server.channels.ChannelService
  ```

  **Reason:** config.xml file in $DOMAIN_HOME/config directory has been corrupted.

  **Resolution:** Take a backup of original config.xml file in $DOMAIN_HOME/config directory. Go to 
  $DOMAIN_HOME/servers/domain_bak/config_prev directory and open config.xml file. Copy the 
  value of <security-configuration>/<credential-encrypted>, <security-configuration>/<node- 
  manager-password-encrypted> and <embedded-ldap>/<credential-encrypted> and paste it in 
  $DOMAIN_HOME/config/config.xml file and then start the AdminServer.

Post-Installation Validations

- Login into UIM Web GUI. Go to Inventory Groups and ensure that there is one Inventory Group 
  with Name as "Bad Email Service Area 75099". Also ensure that there are 13 Logical Devices 
  with specification as "Device" (specification label is "Packet_Network_Device")
- Login into OSM Web GUI (OrderManagement/orchestration). Go to Administer Users, click on 
  "Admin" and ensure that user "Admin" is member of 7 Workgroups namely - SOMRole, 
  PlanDeliveryRole, DeliverOrderRole, CompleteProvisioningRole, DesignServiceRole, 
  O2ASystemAdminRole and TOMRole.
- Using sqlplus or sqldeveloper with $SARMUSER, query ASAP SARM table TBL_COMM_PARAM 
  and ensure that there are total 25 records with HOST = "Americas West VoiceMailServer" and 
  DEVICE = "COMMON_DEVICE_CFG".

**Validate SNO Installation - Execute Smoke Test order**

At this stage you can test the sanity of the SNO deployment to ensure all components are integrated 
correctly and configurations are set appropriately.

**Sending Smoke Test Service Order using Script**

- Execute
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/unifieddomain/unifieddomain/send_test_som_order.sh on ASAP host
Possible Issues and Resolutions

- **Issue:** Work order may get stuck in OSM with the following exception:

  com.mslv.oms.automation.AutomationException: Fail to find password credential with specified map and key name

**Reason:** JPS or credential stores in OSM have been corrupted

**Resolution:** There are multiple corrections needed to resolve this issue. These are listed below:

  - Login into WebLogic EM of OSM host and go to Security > Credentials. If an error message dialog box pops up, copy values of <password-encrypted> from all JDBC xml files in $DOMAIN_HOME/servers/domain_bak/config_prev/jdbc and paste it in corresponding JDBC xml files in $DOMAIN_HOME/config/jdbc directory and then restart the AdminServer and OSM_MS1 managed server.
  - Login into WebLogic EM of OSM host and go to Security > Credentials. If there is no credential store shown in the EM, then create all the expected credential stores using credStoreAdmin.sh script. Refer OSM documentation for required credential stores and creation of credential stores using credStoreAdmin tool.
  - Login into WebLogic console of OSM host and go to Security Realms > myrealm > Users and Groups > Users. There must be total 14 users. Click on each user name, go to Groups tab and ensure that each user is assigned into as many groups as expected for each user individually. Refer OSM documentation for Users and Groups
  - Login into OSM Web GUI (OrderManagement/orchestration) and go to Administer Users. There must be total 7 users. Then go to Administer Workgroups. There must be total 9 workgroups. Click on each workgroup row and ensure that all the expected users are added properly in this workgroup. Refer OSM documentation for Users and Workgroups

**Validations**

Login into OSM Web GUI and confirm that 2 orders are created (one SOM order and one TOM order) and their "Order State" must be "Completed" without any failure.
SNO Solution Configuration for L3VAS

**UIM-NFVO (NSO) Installation**

All changes mentioned in this section should be made in local copies of installation scripts stored in subdirectories of /private in UIM host and all steps should be executed as "friend" user on UIM host.

**Pre-Installation Checks**

- Ensure that DB Port 1521 is opened on DB host.
- Ensure that AdminServer ports and Managed Server ports are opened on OSM, UIM and ASAP hosts.
- Ensure that /private/downloads/ directory in UIM host has rsdod directory with sno catalogs zip file in it. Unzip sno catalogs zip file and then unzip extracted catalog_l3vas.zip file into same folder.
- Ensure that value of INSTALL_NSO is set to 1 in /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_app file.

**Changes needed in Installer Scripts before Installation**

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/nso/nso/install_nso.sh file. Comment out line # 144 to 167, which are shown below:

```bash
$MANAGEABLE_INSTALL_TOOL_DIR/osssuite/admin/do_stop_osssuite.sh
sleep 2m
$MANAGEABLE_INSTALL_TOOL_DIR/osssuite/admin/do_start_osssuite.sh

echo "WebLogic servers restarted"

deploy_uim_cartridge \ 
OracleComms_NSO_BaseCartridge \ 
$THIS_DIR/uimbase/cartridgeBin/OracleComms_NSO_BaseCartridge.jar \ 
7.4.0.0.0

deploy_uim_cartridge \ 
OracleComms_UIM_NSO_L3_VAS \ 
$THIS_DIR/uimbase/OracleComms_UIM_NSO_L3_VAS/cartridgeBin/OracleComms_UIM_NSO_L3_VAS.jar \ 
7.4.0.0.0

deploy_uim_cartridge \ 
Juniper_vSRX \ 
$THIS_DIR/uimbase/Juniper_vSRX/cartridgeBin/Juniper_vSRX.jar \ 
7.4.0.0.0

/bin/rm -f $MANAGEABLE_INSTALL_TOOL_DIR/${NSO_SCRIPT_MODULE_NAME}/nso/base.jar
echo Cleanup
/bin/rm -rf $THIS_DIR/sample $THIS_DIR/uimbase $THIS_DIR/base
```
• **Edit** /private/downloads/RSDOD_installer/rsdod_runtime_installer/nso/nso/go.sh file. Comment out line # 23:

  ```
  echo "Installation of NSO has finished."
  ```

• **Edit** /private/downloads/RSDOD_installer/rsdod_runtime_installer/go/go.sh file. Comment out line # 19, 21, 22, 24, 25, 34 and 36 (shown below).

  ```
  /bin/bash -c "${DEFAULT_MANAGEABLE_INSTALL_TOOL_DIR}/osssuite/go.sh"

  /bin/bash -c "${DEFAULT_MANAGEABLE_INSTALL_TOOL_DIR}/intrasuite/common/config_access.sh"

  /bin/bash -c "${DEFAULT_MANAGEABLE_INSTALL_TOOL_DIR}/intrasuite/intrasuite/go.sh"

  /bin/bash -c "${DEFAULT_MANAGEABLE_INSTALL_TOOL_DIR}/unifieddomain/common/config_access.sh"

  /bin/bash -c "${DEFAULT_MANAGEABLE_INSTALL_TOOL_DIR}/unifieddomain/unifieddomain/go.sh"

  /bin/bash -c "${DEFAULT_MANAGEABLE_INSTALL_TOOL_DIR}/go/secure_clean.sh"

  echo "Installation of RSDOD Finished. Press CTRL-C to finish installer."
  ```

**Installation Steps**

• **Execute**
  ```
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/go/go.sh
  ```

• **Shutdown UIM_MS1 managed server and AdminServer on UIM host manually**

• **Start AdminServer and UIM_MS1 managed server using startUIM script on UIM host manually**

• **Edit** /private/downloads/RSDOD_installer/rsdod_runtime_installer/nso/nso/install_nso.sh file. Comment out line # 26 to 36, 104 to 148 and uncomment line # 150 to 167

• **Edit** /private/downloads/RSDOD_installer/rsdod_runtime_installer/nso/nso/go.sh file. Uncomment line # 23

• **Execute**
  ```
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/go/go.sh one more time.
  ```

**Post-Installation Steps**

• **Edit** /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_passwords file in all hosts (DB, OSM, UIM and ASAP hosts). Delete the values of PASSWORD_ADMIN_ACCOUNTS and PASSWORD_USER_ACCOUNTS as these values are no longer required for any installer script.
Post-Installation Validations

- Login into UIM Web GUI. Click on "Help" > "About" and go to "Cartridges" tab and ensure that Juniper_vSRX cartridge is listed there.
IPSA Installation and Carrier Ethernet Solution Configuration

IPSA Server Installation and Configuration

All steps in this section must be executed as “friend” user on IPSA host, unless specifically mentioned otherwise:

Pre-Installation Checks

- If IPSA host is not created using the pre-configured snapshot then Linux 7 OS must be prepared with required additional packages and kernel parameters.
- RSDOD_installer directory must be downloaded in /private/downloads from media server and sno install kit zip file must be unzipped in /private/downloads/RSDOD_installer, if not unzipped already.
- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/media_map file to update the values of
  
  CGBU_SC_P_MEDIA_OS_USER

  CGBU_SC_P_MEDIA_HOST

  CGBU_SC_P_MEDIA_DL_DIR

- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_passwords file to update the values of
  
  PASSWORD_ADMIN_ACCOUNTS

  PASSWORD_USER_ACCOUNTS

- JDK 1.8 should be installed in this host at this location:
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/jdk18/
- Create a directory called ipsa in /private/downloads and download IPSA 7.4.0.2 installation zip file, supplementalSoftwareComponents-linux.zip file and populateData.zip file in /private/downloads/ipsa directory. Unzip IPSA 7.4.0.2 installation zip file and supplementalSoftwareComponents-linux.zip in /private/downloads/ipsa directory.
- Ensure that DB Port 1521 is opened (for access) on DB host

FMW Installation

- Edit `/private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/go.sh` file. Comment out line # 20, 22 and 23
- Execute `/private/downloads/RSDOD_installer/rsdod_runtime_installer/go/config_access.sh` as "friend" user
- Execute `/private/downloads/RSDOD_installer/rsdod_runtime_installer/go/go.sh`

**RCU Schema and WebLogic Domain Creation**

- Edit `/private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_db_single` file. Replace DB hostname in two lines, line # 21 and line # 22 in "Default DB details" block. Give fully qualified hostname of DB host in line # 21 to replace command `hostname -f` and only the hostname (without domain suffix) in line # 22 to replace command `hostname`

  Line # 21: `DATABASE_HOST=`hostname -f`

  Line # 22: `DATABASE_HOST_NAME=`hostname`

- Edit `/private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_app` file. Change the value of MDS_DATABASE_SCHEMA_PREFIX in line # 26. Replace existing value "RSDOD" with "SNOIPSA"

  Line # 26: `MDS_DATABASE_SCHEMA_PREFIX=RSDOD`

- Edit `/private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/go.sh` file. Comment out line # 20, 21 and 23 and uncomment line # 22
- Execute `/private/downloads/RSDOD_installer/rsdod_runtime_installer/go/config_access.sh` as "friend" user
- Execute `/private/downloads/RSDOD_installer/rsdod_runtime_installer/go/go.sh`
- Go to `/private/installation/Middleware_wls/user_projects/domains/ipsa_domain/bin` and start AdminServer using startWeblogic.sh script in nohup mode
- Open a browser and access WL domain console and enable SSL Port for AdminServer on 7002
DB User Creation

- Connect DB using sqlplus or sqldeveloper tool as sysdba user on DB host, Port = 1521, Service Name = orcl.us.oracle.com or SID = orcl and execute the following sql commands after replacing correct values for <IPSA_DB_USER> and <PASSWORD_ADMIN_ACCOUNTS>:

```sql
create user <IPSA_DB_USER> profile "DEFAULT" identified by <PASSWORD_ADMIN_ACCOUNTS> default tablespace users temporary tablespace temp account unlock;

grant unlimited tablespace to <IPSA_DB_USER>;
grant connect to <IPSA_DB_USER>;
grant resource to <IPSA_DB_USER>;
grant create view to <IPSA_DB_USER>;

create directory ipsa_plsql_dir as '/private/ RSDOD_installation/oracledb/product/12.2.0/dbhome_1/';
grant execute on sys.utl_file to <IPSA_DB_USER>;
grant create procedure to <IPSA_DB_USER>;
grant create trigger to <IPSA_DB_USER>;
grant create table to <IPSA_DB_USER>;
grant create type to <IPSA_DB_USER>;
grant create sequence to <IPSA_DB_USER>;

Commit;
```

IPSA Server Installation

- Copy /private/downloads/ipsa/ipsa/Disk1/stage/Response/oracle.communications.ipsa.AllComponents.rsp file into /private/downloads/ipsa directory

- Edit /private/downloads/ipsa/oracle.communications.ipsa.AllComponents.rsp file. Change the values of the following parameters as given below:
  - ORACLE_HOME="/private/installation/ipsa/IPSA7402"
  - ORACLE_HOME_NAME="IPSA7402"
  - oracle.communications.ipsa.networkprocessor:SUPP_SOFTWARE_DIR=/private/downloads/ipsa/supplementalSoftwareComponents
  - oracle.communications.ipsa.corelibs:SUPP_SOFTWARE_DIR=/private/downloads/ipsa/supplementalSoftwareComponents
  - AUTOMATIC_STARTUP_REQUIRED=false

- Go to /private/downloads/ipsa/ipsa/Disk1/install directory and execute the following command:

```bash
./runInstaller -force -waitforcompletion -silent -responseFile /private/downloads/ipsa/oracle.communications.ipsa.AllComponents.rsp
```

- Once installation completes and prompt comes back, run the following scripts with root (sudo) privileges
  - /home/friend/oraInventory/orainstRoot.sh
  - /private/installation/ipsa/IPSA7402/root.sh
OSM-IPSA JMS Configuration

The following steps must be executed as “friend” user on OSM host

- Open or enable the AdminServer ports (7001 and 7002) on IPSA hosts to make them accessible from other hosts.
- If IPSA has been installed with a different username (other than “friend”), then edit /private/downloads/RSDDOD_installer/rsdod_runtime_installer/config/osm_ipsa_jms_conf file and provide correct values of:
  - IPSA_HOST_OS_USER_NAME
  - IPSA_HOST_OS_GROUP_NAME
- Edit /private/downloads/RSDDOD_installer/rsdod_runtime_installer/config/ipsa_weblogic_conf and provide the values for the following IPSA WebLogic parameters:
  - IPSA_WEBLOGIC_HOST=sno-test-ipsa7.digbssad2.cgbuvcn.oraclevcn.com
  - IPSA_WEBLOGIC_PORT=7001
  - IPSA_WEBLOGIC_ADMIN_USER=<WL_ADMIN_USER>
  - IPSA_WEBLOGIC_ADMIN_PASSWORD=<PASSWORD_ADMIN_ACCOUNTS>
  - IPSA_WEBLOGIC_SERVER_NAME=AdminServer
  - IPSA_WEBLOGIC_DOMAIN_PATH=/private/installation/Middleware_wls/user_projects/domains/ipsa_domain
  - IPSA_JMS_QUEUE_NAME=IPSAResponseQueue
  - IPSA_JMS_CONNECTION_FACTORY_NAME=IPSAResponseQueueConnFactory
- Go to /private/downloads/RSDDOD_installer/rsdod_runtime_installer/go directory and execute osm_ipsa_config.sh script
- Open WL Domain Console running on OSM host in a browser and confirm that ipsa.ipsaResponseQueue is created in osm_oss_jms_module
- Open WL Domain Console running on IPSA host in a browser and confirm that ipsa_osm_event_bridge is created

IPSA Server Configuration

The following steps must be executed as “friend” user on IPSA host:

- Go to /private/installation/ipsa/IPSA7402/ServiceActivator/bin and execute the following command:
  ```
  ./configTool.sh -wlVersion 12c -wlHome
  /private/installation/Middleware_wls -action export -file MyBaseHost.xml
  ```
  This will generate a file named MyBaseHost.xml in /private/installation/ipsa/IPSA7402/ServiceActivator/WorkingData/ConfigToolTransfer directory
- Go to /private/installation/ipsa/IPSA7402/ServiceActivator/WorkingData/ConfigToolTransfer directory and make a copy of MyBaseHost.xml as BaseHost_Edited.xml
- Edit `/private/installation/ipsa/IPSA7402/ServiceActivator/WorkingData/Config ToolTransfer/BaseHost_Edited.xml` file with appropriate values.
- Go to `/private/installation/ipsa/IPSA7402/ServiceActivator/bin` directory and execute the following command:

```
./configTool.sh -wlVersion 12c -wlHome /private/installation/Middleware_wls -action import -file BaseHost_Edited.xml
```

**Note:** This file has passwords in plain text so it must not be left in the system after use.

- Go to `/private/installation/ipsa/IPSA7402/ServiceActivator/Config` directory and ensure that a new file `db.properties` has been created here. This file can't be read or edited manually as it is encrypted.
- Go to `/private/installation/ipsa/IPSA7402/ServiceActivator/odbc/network/admin` directory and ensure that a new file `tnsnames.ora` has been created here. Open `tnsnames.ora` file and ensure that its entries are correct.
- Open WL Domain Console running on IPSA host in a browser and confirm that IpsaWebService is deployed under Deployments and is in Active state.

**SSL Configuration for IPSA WL Domain**

Since IPSA supports only secure communication for its web services, we need to configure SSL in IPSA WL Domain.

The following steps need to be executed as “friend” user on IPSA host:

- Generate a keystore `identity.jks` with one alias as mykey
- Export keystore entry represented by alias mykey from keystore `identity.jks` into a certificate `root.cer`
- Generate another keystore `trust.jks` with one alias mykey imported from certificate `root.cer`
- Copy keystores and certificate to different lib/security folders (JDK and WebLogic Server)
- Add certificate into system keystore (cacerts) of different lib/security folders (JDK and WebLogic Server)

The following steps need to be executed as “friend” user on OSM and UIM hosts:

- Transfer keystores and certificate to different lib/security folders (JDK, WebLogic Server and Design Studio) in OSM and UIM hosts
- Add certificate into system keystore (cacerts) of different lib/security folders (JDK, WebLogic Server and Design Studio) in OSM and UIM hosts

The following steps need to be executed on IPSA host:

- Open WL Domain Console running on IPSA host in a browser and go to Servers > AdminServer > Configuration > Keystores and make the following changes:
- Change keystore to "Custom Identity and Custom Trust"
  - Custom Identity Keystore:
    /private/installation/Middleware_wls/wlserver/server/lib/identity.jks
  - Custom Identity Keystore Type: jks
  - Custom Identity Keystore Passphrase: 123456
  - Confirm Custom Identity Keystore Passphrase: 123456

  - Custom Trust Keystore:
    /private/installation/Middleware_wls/wlserver/server/lib/trust.jks
  - Custom Trust Keystore Type: jks
  - Custom Trust Keystore Passphrase: 123456
  - Confirm Custom Trust Keystore Passphrase: 123456

Click on “Save” button

- Go to Servers > AdminServer > Configuration > SSL and make the following changes:
  - Private Key Alias: mykey
  - Private Key Passphrase: 123456
  - Confirm Private Key Passphrase: 123456

Click on “Save” button

- Go to Servers > AdminServer > Configuration > SSL > Advanced and make the following changes:
  - Hostname Verification: None

Click on “Save” button

- Log out from IPSA WebLogic Console
- Stop IPSA WebLogic domain
- Start IPSA application servers
- Start IPSA WebLogic domain

**IPSA Client Installation and Configuration**

IPSA client installation is supported only on Windows OS

As IPSA client-server communication doesn’t support SSH tunneling, IPSA client should be installed in a windows VM which has direct access to the network in which IPSA server is connected.

**Access to Windows OCI VM**

- Connect to the Windows VM through Remote Desktop using Port Forwarding in PuTTY and Bastion Host private key in Pageant.
- Login in Windows VM using pre-created username (opc) and given password.

Remember that Windows VMs use password based authentication.

- It will ask to change the Windows password on first login. Change the password.
IPSA Client Installation

- Transfer IPSA client build load for windows and corresponding supplemental software components zip file into Windows remote desktop and unzip both the files.
- Go to extracted build folder > client/Disk1/install
- Double click on setup.exe to start the client installer. You can provide a Name and Path of your choice to your installation. Following are the examples:

  Name = IPSA7402_C

  Path = C:\Users\opc\Desktop\IPSA\IPSA7402_C

- Enter the path of extracted Supplemental Software Component directory when prompted by installation wizard

Once installation is complete, it will ask to open the Configuration GUI. Click Yes button if you want to start IPSA Client Configuration now. Or you can open it from Windows Start Menu – “Configuration GUI (Local Host)” anytime.

IPSA Client Configuration

When Configuration GUI window appears, make the following changes:

- Expand the localhost from the Hosts list in left side panel
  - Click on CORBA
    - Naming Service Host Name = sno-test-ipsa7.digbssad2.cgbuyvcn.oraclevcn.com
    - Naming Service Port = 2809
  - Click on SSL
    - Enable SSL (checkbox) = Uncheck
  - Expand Service Module GUI Extensions
    - Click on Common Module Configuration
      - Database Service Name = orcl.us.oracle.com
      - Database Server IP Address = 10.5.41.48
      - Database Server Port = 1521
      - Database User Id = <IPSA_DB_USER>
      - Database User Password = <PASSWORD_ADMIN_ACCOUNTS>
      - Confirm Database User Password = <PASSWORD_ADMIN_ACCOUNTS>
  - Click on Validate Configuration button (4th button on menu)
  - Click on Commit to Host button (5th button on menu)
  - Wait until a confirmation dialog box comes
  - Close the Configuration GUI Window

Password Reset at First Login

- Click on "User Interface" icon to open the IPSA client interface on Windows remote desktop and login with admin/admin.
After login, it will ask to change the password. Change the password as "User1234".
Close the client window.
Go to IPSA Server. Update IPSA user password and redeploy web services using configTool.sh as per the following steps:
  o Go to 
    /private/installation/ipsa/IPSA7402/ServiceActivator/WorkingData/ 
    ConfigToolTransfer directory and make a copy of BaseHost_Edited.xml as 
    BaseHost_Edited_ChangePassword.xml
  o Edit 
    /private/installation/ipsa/IPSA7402/ServiceActivator/WorkingData/ 
    ConfigToolTransfer/BaseHost_Edited_ChangePassword.xml file to change 
    IPSA user password from original password to <PASSWORD_USER_ACCOUNTS> at 2 
    places:
      ▪ Under collectorGroup - <con5:ipsa.pwd>********</con5:ipsa.pwd>
      ▪ Under webServiceGroup - 
        <con7:ipsa.password>**********</con7:ipsa.password>
  o Go to /private/installation/ipsa/IPSA7402/ServiceActivator/bin 
    directory and execute the following command:

    ./configTool.sh -w1Version 12c -w1Home 
    /private/installation/Middleware_wls -action import -file 
    BaseHost_Edited_ChangePassword.xml

Click on "User Interface" icon to open the IPSA client interface and this time login with changed 
password (<PASSWORD_USER_ACCOUNTS>).
Click on Tools > Options > and make the following changes:
  o Discovery
    ▪ CE Device IP Address Selection = Do not change
    ▪ Non-CE Device IP Address Selection = Do not change
    ▪ Automatic Role Assignment on Discovery = Yes
  o User Passwords
    ▪ Uncheck the box below "Password Expiration"
Click on “Apply” and then “OK” button to close the Options windows.
Click on System tab in left hand side tree panel > System User Groups > Super Users > Right Click 
on Admin > Properties and make the following changes:
  o System User
    ▪ Allow concurrent logins = Yes
  o Password
    ▪ Uncheck the box before "Expires..."
Click on “Apply” and then “OK” button
Click on Commit button (3rd in the Menu) and click on “Apply” and then “OK” button
Exit from IPSA Client GUI
Stop IPSA WL domain
Stop IPSA application servers
Start IPSA application servers
Start IPSA WL domain
Other Setup Steps

Groovy Scripts

- Copy the sample groovy scripts on IPSA host

```bash
$ cd /private/installation/ipsa/IPSA7402/ServiceActivator/DomainController/
$ cp -R sample/* .
```

Configure IPSA as a Target System to OSM

- Open Design Studio, update topologyConfig.xml file under TOM Unified Solution Cartridge
  
  |OracleComms_OSM_TOM_Unified\resources\topology\topologyConfig.xml| with IPSA host and port details. Re-compile and re-deploy TOM Unified Solution Cartridge upon OSM.

Note:

1. Remember that AdminServer SSL port should be defined
2. Mode should be INTEGRATED
3. Ensure that ActivationRESTCONF credentials password is correct in WL domain enterprise manager console in OSM host

IPSA Seed Data Creation

- Login into Client GUI on Windows remote desktop and execute the following steps:
  1. Create a new domain. File > New Domain >
     - Name = Testing
     - Click on Proxy Agent > Select a proxy agent > Check the default one
  2. Click on Apply > OK button.
  3. Click on Commit button (3rd button on Menu) > Click “Apply” and then “OK” button on Transaction dialog box.
  4. Double click on Testing domain in left side panel.
  5. Right click on Device Type > Add Device Type with the following values
     - Select “Edit Fields” check box
     - Model = Juniper JunipervMX
     - SysObjectId = 1.3.6.1.4.1.9.1.394
     - Device driver = juniper
     - Vendor = Juniper
     - Product = JunipervMX
     - Configure Level = Interface
  6. Click on Apply and OK
  7. Click on Commit button (3rd button on Menu) > Click Apply and OK button on Transaction dialog box.
• Logout from Client GUI
• Download populateData.zip (from Build Portal Build folder InternalOnly) and transfer populateData.zip to /private/installation/ipsa/IPSA7402/ServiceActivator/bin on IPSA host and unzip itLogin into IPSA host and execute the following commands:
  o  
    ▪ cd populateData/
    ▪ chmod u+x bin/populateData.sh
    ▪ export
      JAVA_HOME=/private/downloads/RSDOD_installer/rsdod_runtime_installer/jdk 18
    ▪ export PATH=$JAVA_HOME/bin:$PATH
    ▪ ./bin/populateData.sh sno-test-ipsa7.digbssad2.cgbuv.cn.oraclevcn.com 2809
      admin <PASSWORD_USER_ACCOUNT>
      /private/installation/ipsa/IPSA7402/ServiceActivator
• Login into Client GUI (admin/User1234) on Windows remote desktop and ensure that Devices are added under Testing Domain
Network Integrity Installation and Integration with UIM

NI Installation

All steps in this section must be executed as “friend” user on NI host, unless specifically mentioned otherwise.

Pre-Installation Checks

- If NI host has not been created from pre-configured snapshot then Linux 7 OS must be prepared with required additional packages and kernel parameters.
- RSDOD_installer directory is downloaded in /private/downloads from media server and sno install kit zip file must be unzipped in /private/downloads/RSDOD_installer, if not unzipped already.
- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/media_map file to update the values of
  
  - CGBU_SCP_MEDIA_OS_USER
  - CGBU_SCP_MEDIA_HOST
  - CGBU_SCP_MEDIA_DL_DIR
- Edit /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_passwords file to update the values of
  
  - PASSWORD_ADMIN_ACCOUNTS
  - PASSWORD_USER_ACCOUNTS
- JDK 1.8 should be installed in this host at this location:
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/jdk18/
- Create a directory called ni in /private/downloads and download NI 7.3.6 installation zip file in /private/downloads/ni directory. Unzip installation zip file in /private/downloads/ni directory.
- Ensure that DB Port 1521 is opened (for access) on DB host

FMW Installation

- Edit
RCU Schema and WebLogic Domain Creation

- Edit 
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_db_single file. Replace DB hostname in two lines, line # 21 and line # 22 in “Default DB details” block. Give fully qualified hostname of DB host in line # 21 to replace command 'hostname -f' and only the hostname (without domain suffix) in line # 22 to replace command 'hostname'.

  Line # 21: DATABASE_HOST=`hostname -f`

  Line # 22 DATABASE_HOST_NAME=`hostname`

- Edit 
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/config/rsdod_app file. Change the value of MDS_DATABASE_SCHEMA_PREFIX in line # 26. Replace existing value “RSDOD” with “SNONI”.

  Line # 26: MDS_DATABASE_SCHEMA_PREFIX=RSDOD

- Edit 

- Edit 
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/osssuite/go.sh file. Comment out line # 20, 21 and 23 and uncomment line # 22

- Edit 

- Execute 
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/go/config_access.sh as “friend” user

- Execute 
  /private/downloads/RSDOD_installer/rsdod_runtime_installer/go/go.sh

- Go to 
  /private/installation/Middleware_wls/user_projects/domains/ni_domain/bin and start AdminServer using startWeblogic.sh script in nohup mode

- Configure SSH tunneling to access NI WL domain console
- Open PuTTY and load saved session (OCI – NI) and configure tunneling for NI WebLogic console.
- Go back to Session and save the configuration settings.
- Close any running PuTTY sessions and open fresh PuTTY session with saved configuration (remember that you need to open this saved session every time you need to access NI WebLogic domain console.

### Network Integrity Installation

- Open or enable the AdminServer ports (7001 and 8000) on NI host to make them accessible from other hosts.
- Copy
  ```
  /private/downloads/ni/integrity/Disk1/stage/Response/oracle.communications.ni.Complete.rsp
  ```
  file into /private/downloads/ni directory
- Edit
  ```
  /private/downloads/ni/oracle.communications.ipsa.AllComponents.rsp
  ```
  file. Change the values of the following parameters as given below:

  ```
  ORACLE_HOME=/private/installation/ni/NI736
  ORACLE_HOME_NAME="NI736"
  APP_TARGET_NAME=AdminServer
  SECURITY_PROVIDER_NAME=Embedded_LDAP
  DATABASE_TYPE=Non Clustered-DB
  Disable_nonSSLport=false
  INSTALL_TYPE="Complete"
  APP_USER_INPUT={"sno-test-ni736.digbssad2.cgbuvcn.oraclevcn.com","7001","<WL_ADMIN_USER>"","<PASSWORD_ADMIN_ACCOUNTS>"}
  DB_USER_INPUT={"sno-test-shared-db.digbssad2.cgbuvcn.oraclevcn.com","1521","sys","<PASSWORD_ADMIN_ACCOUNTS>","orcl.us.oracle.com"}
  SCHEMA_OWNER_INPUT={"SNONI_mds", "<PASSWORD_ADMIN_ACCOUNTS>"}
  LDAP_DEFAULT_USER_INPUT={"User1234", "<PASSWORD_USER_ACCOUNTS>"}
  LDAP_USER_INPUT={"niuser1", "User1234", "<PASSWORD_USER_ACCOUNTS>"}
  ```

- Go to /private/downloads/ni/integrity/Disk1/install and execute this command as user “friend”:
Once installation completes and prompt comes back, run the following scripts with root (sudo) privileges:

```
/home/friend/oraInventory/orainstRoot.sh
```

Restart NI WebLogic Domain after setting memory arguments in two files:
- /private/installation/Middleware_wls/user_projects/domains/ni_domain/bin/setDomainEnv.sh
  - Modify the values as shown below:

  ```
  WLS_MEM_ARGS_64BIT="-Xms1024m -Xmx3036m"
  ```

- /private/installation/Middleware_wls/user_projects/domains/ni_domain/bin/setStartupEnv.sh
  - Modify the values under this section:

  ```
  if [ "${STARTUP_GROUP}" = "AdminServerStartupGroup" ] ; then
    
    SERVER_MEM_ARGS_64="-Xms1024m -Xmx3036m"
    export SERVER_MEM_ARGS_64
    SERVER_MEM_ARGS_64HotSpot="-Xms1024m -Xmx3036m"
    export SERVER_MEM_ARGS_64HotSpot
  
  Restart WebLogic domain in nohup mode. Ensure that AdminServer has configured with ssl port 8000.

**Network Integrity Cartridge Deployment**

- Copy entire designstudio folder (including a child folder with same name designstudio and child folders named OSM_SDK, OTHER_LIB, UIM_SDK, WL_SDK) from /private/RSDOD_installation folder in ASAP host and store it in /private/installation folder in NI host
- Execute these 3 commands in both UIM and OSM hosts:

  ```
  rm -rf /private/downloads/RSDOD_installer/rsdod_runtime_installer/common/CDT/lib
  ```
/private/installation/designstudio/WL_SDK/oracle_common/modules/thirdparty/org.apache.ant/1.9.8.0.0/apache-ant-1.9.8/bin/ant -lib/private/downloads/RSDOD_installer/rsdod_runtime_installer/common/CDT/lib -Dhost=10.5.41.54 -Dport=7001 -Dtarget=AdminServer -Dusername=weblogic -Dpassword=Admin123 -DcartridgeType=NetworkIntegrity -DcartridgeName=CarrierEthernet_Cartridge -DcartridgeVersion=1.0.0.0 -DsslKeyStore= -DadminServerKeyStore= -f/private/downloads/RSDOD_installer/rsdod_runtime_installer/common/CDT/dist/build.xml -v undeploy

UIM Sample Web-Service Installation in UIM

- Download Oracle Communications Network Integrity, UIM Integration Cartridge and follow NI documentation on NI-UIM Integration to generate NI_Uim.war file
- Pack NI_Uim.war file in UIM’s custom.ear file. Update META-INF\application.xml inside custom.ear with a new module as shown below:

```xml
<module>
  <web>
    <web-uri>NI_Uim.war</web-uri>
    <context-root>NI_Uim</context-root>
  </web>
</module>
```

- Repack custom.ear and re-deploy (update) it in UIM using UIM WebLogic console.
- Ensure that NI-UIM Sample Web Service are deployed successfully in UIM by accessing this URL: http://localhost:<LOCALLY_MAPPED_PORT_FOR_UIM_MANAGED_SERVER>/NI_Uim/NI_UimHTTP

Sample Discovery in Network Integrity and Resolving Discrepancies between NI and UIM

- Execute the following steps to configure SNMP Adapter

  ```bash
cd/private/installation/Middleware_wls/user_projects/domains/ni_domain/config
mkdir snmpAdapterConfig
cd snmpAdapterConfig
```
Create a new file snmpAdapter.properties in snmpAdapterConfig folder. Add this line and save the file:

```
MODE=playback
```

- FTP snmpData.zip into /
  private/installation/Middleware_wls/user_projects/domains/ni_domain
- Unzip snmpData.zip into /
  private/installation/Middleware_wls/user_projects/domains/ni_domain. It will extract a folder named snmpData.
- Login into NI GUI and execute the following steps:
  - Click Manage Import System link under Tasks in left side panel, click on Add button and provide UIM application details
    ```
    Name = SNO_UIM
    Address = http://10.5.41.49:7012/NI_Uim/NI_UimHTTP?WSDL
    Username = <UIM USER>
    Password = <PASSWORD_USER_ACCOUNTS>
    ```
  - Click on "Save and Continue" button
  - Click “Manage Scans” link under Tasks in left side panel, click on “Create Scan” button

  General tab
  ```
  Name = Scan1
  Enabled = Yes
  Detect Discrepencies = Yes
  Scan Action = Discover Career Ethernet
  Scan Type = Discovery
  Scan Action Parameters = SnmpParameters
  Version = 2c
  Community String = public
  ```

  Scope tab
  ```
  Add Network Address = 10.156.68.201-213
  ```
• Search for the created scan (Scan1). Select the row (Scan1) from search result and click on “Start Scan” button
• Once the Scan is completed, click on “Display Scan Result” button. It will show that 13 new records are found. These are corresponding to IP address 10.156.68.201 to 10.156.68.213
• On next screen, Select the Scan row and click on “Review Discrepancies” button. It will show 13 discrepancies because UIM doesn’t have devices with these IP Addresses.
• Now resolve all these discrepancies in UIM. Select one or all rows and click on Action > Correct in UIM. Row will be updated with Status = Ready
• Click on “Submit” button. The row status will first change to "Submitted". Press “Refresh” button on Menu) and it will show status as "Processed".
• When the status is "Processed", discrepancy data (13 Logical Devices) is added in UIM Inventory Database. These 13 logical devices will be found duplicate by name in UIM but their IDs will be different.

Possible Issues and Resolutions

Issue: Only basic parameters are visible on “Manage Scans” screen and dynamic parameters (like Version and Community String) are not loaded.

Effect: Scan will fail

Reason: The Carrier Ethernet cartridge didn’t get deployed properly in Network Integrity

Resolution: Undeploy the Carrier Ethernet cartridge and re-deploy it using CDT command. If the issue still doesn’t get resolved, deploy the Carrier Ethernet cartridge in Network Integrity using Design Studio from Windows box. Import this cartridge (with source code) and dependency cartridges in Design Studio, compile it and deploy it in Network Integrity.