

Atlas SW Upgrade

Cloud Execution Environment

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2016–2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
2	Preparing to Upgrade Atlas SW	2
3	Upgrade Atlas SW	4
4	Post-Upgrade Activities	11
4.1	Verify Installation	11
4.2	SSL Certificate Installation	11
4.3	Change Password for Atlas Users	11
5	Rollback	13





1 Introduction

This document describes the procedures for updating and upgrading the SW in an existing Cloud Execution Environment (CEE) Atlas server.

Note: In this document, memory and storage quantities are represented according to the JESD100B.01 standard:

- KB refers to 2^{10} bytes
- MB refers to 2^{20} bytes
- GB refers to 2^{30} bytes

1.1 Prerequisites

Before starting this procedure, ensure that the following conditions are met:

- An Atlas artifacts file, in tar format, is available with the software.
- Two ranges of IP addresses for two subnets, according to the local network plan, must be available for Atlas.
- The vCIC must be operational.
- At least 4 GB must be available on the vCIC destination path for the Atlas image. Use the command `df -h <destination_path>` to determine if the sufficient disk space is available.



2 Preparing to Upgrade Atlas SW

This section describes the preparations needed before the Atlas server is upgraded.

The Atlas image file has the following ID syntax:

```
ecs-atlas-x86_64-${TARGET_ATLAS_VERSION}-${BUILD_NUMBER}.qcow2
```

The Atlas image file is delivered in an archive, including checksum files and the Atlas installation script.

Throughout the document, the Atlas image ID is referred to as `Atlas_image` and the archive artifact name as `${TARGET_ATLAS_VERSION}.tar.gz`.

To prepare for the upgrade, do the following:

1. Download the `${TARGET_ATLAS_VERSION}.tar.gz` to the Fuel node.
2. Logon to vCIC and create artifacts directory, then log out

```
[root@fuel ~]# ssh cic-1  
  
root@cic-1:~# mkdir -p artifacts  
  
root@cic-1:~# exit
```

3. Copy the Atlas archive to the vCIC (any of the three vCICs can be used):

Note: In case of non-CEE environment, copy Atlas artifacts to controller node instead of vCIC.

```
[root@fuel ~]# scp ${TARGET_ATLAS_VERSION}.tar.gz =>  
<vcic_hostname>:/root/artifacts/
```

Note: Ensure that the destination, for example `/root/artifacts/`, is present and has at least 4 GB free space. Use the command `df -h <destination_path>` to determine if the sufficient disk space is available.

4. Log on to the vCIC:

```
[root@fuel ~]# ssh root@<controller_ip>
```

5. Unpack the archive file:

```
root@cic-1:~# cd artifacts  
  
root@cic-1:~/artifacts# tar -xvzf =>  
${TARGET_ATLAS_VERSION}.tar.gz
```

Note: During the unpack sequence, all files in the archive are listed.



6. Backup the currently executing Atlas configuration files and folders, refer to *Atlas Backup*.



3 Upgrade Atlas SW

This section describes how to upgrade the Atlas server.

An Atlas upgrade is effectively a reinstallation of Atlas, using a new image. The parameters must be reconfigured, even though they were configured during the previous installation.

Note: In this procedure, the currently active and running Atlas is referred to as the old version. The version to replace the active and running Atlas is referred to as the new version.

To upgrade Atlas, do the following:

1. In `/etc/atlasrc`, the following environment variables are set with appropriate values:

<code>OS_CACERT</code>	Environment variable for certificate file
<code>CERT_FILE</code>	Environment variable for certificate file
<code>CA_CERT_FILE</code>	Environment variable for certificate file
<code>neutron_extreme</code>	Enable <code>neutron_extreme</code> , when extreme neutron configuration is used. Default is <code>true</code> .
<code>WATCHMEN_PASSWORD</code>	OpenStack password for watchmen service
<code>TIMEZONE</code>	Time zone as defined in <code>config.yaml</code>
<code>SSLCipherSuite, SSLProtocol</code>	SSL Cipher suite and protocol as define in <code>config.yaml</code>
<code>NTP_SERVER</code>	NTP server IP address as defined in <code>config.yaml</code>
<code>CIDR_PUBLIC</code>	Public (<code>cee_om_sp</code>) Subnet range as defined in <code>config.yaml</code>
<code>MGMT_IP</code>	OpenStack management IP address
<code>CIDR_NBI, CIDR_SBI</code>	Atlas <code>NBI_IP</code> and <code>SBI_IP</code> as defined in <code>config.yaml</code>
<code>NBI_IP, SBI_IP</code>	Atlas <code>NBI_IP</code> and <code>SBI_IP</code> as defined in <code>config.yaml</code>
<code>START_ADDR_NBI, START_ADDR_SBI</code>	NBI and SBI subnet allocation start address as defined in <code>config.yaml</code>



END_ADDR_NBI, END_ADDR_SBI	NBI and SBI subnet allocation end address as defined in config.yaml
GATEWAY_NBI, GATEWAY_SBI	NBI and SBI gateway IP as defined in config.yaml
SEGID_NBI, SEGID_SBI	VLAN tag for NBI and SBI as defined in config.yaml
NETWORK_NBI, NETWORK_SBI	Network name of NBI and SBI as defined in config.yaml
SDNC_NBI_IP	SDN controller northbound IP as defined in config.yaml
SDNC_USERNAME	SDN controller admin username as defined in config.yaml
SDNC_PASSWORD	SDN controller admin password as defined in config.yaml
VPN_NAME	Name of VPN network as defined in config.yaml
L2GW_NBI	L2 gateway name of NBI, as defined in config.yaml
L2GW_VLAN_NBI	L2 gateway VLAN ID of NBI, as defined in config.yaml
L2GW_SBI	L2 gateway name of SBI, as defined in config.yaml
L2GW_VLAN_SBI	L2 gateway VLAN ID of SBI, as defined in config.yaml
ROUTE_DISTINGUISHER	An 8-octet field prefixed to the IPv4 of the customer to make IPv4 prefixes globally unique as defined in config.yaml
EXPORT_RT	Routing Engine uses active routes from the routing table to send a protocol advertisement in export route table as defined in config.yaml
IMPORT_RT	Routing Engine places the routes of a routing protocol into the import route table as defined in config.yaml
VPN_ID	Randomly generated UUID
NETWORK_TYPE	Network type can be vlan or vxlan as defined in config.yaml. The default value is vlan.
KEYSTONE_HOST	Public IP of the keystone identity service



KEYSTONE_PORT	Keystone Port
OS_USERNAME	Keystone admin user
OS_PASSWORD	Keystone admin password
OS_TENANT_NAME	Keystone admin tenant name
OS_AUTH_URL	Keystone service internal URLv2
ENABLE_ROUTER	Router menu displayed in Atlas (True or False)
DNS_SERVER	Set to the IP address of the DNS server, in order to assign DNS server to Atlas
ATLAS_HOSTNAME	Atlas host name used in the SSL certificate (SAN), keystone endpoints
CONTROLLER_HOSTNAME	CIC host name used in SSL certificate (SAN), keystone
HAProxySSLProtocol, HAProxySSLConn	HAProxy SSL Protocol and HAProxy SSL Connection, as defined in config.yaml

Note: All variables are filled during CEE installation when config.yaml has Atlas details specified. This file is maintained by Ansible, and should not be modified manually.

2. Change directory to artifacts:

```
root@cic-1:~# cd artifacts/
```

3. Provide executable permissions to Atlas installation script:

```
root@cic-1:~/artifacts# chmod +x <atlas_install.sh-path>
```

Note: An example of the command is:

```
chmod +x atlas_install.sh
```

4. In localrc, ensure that following variables have the appropriate values:

PASSWORD	Password for user atlasadm. Default is qwqwqw. New password should be of 14 or more characters with a minimum of one special, numeric, lower and upper case character.
SERVICE_CINDER_VOLUME	Set to true or false, based on Cinder service availability. Default is false
ASSIGN_ATLAS_IP	Set to true for assigning NBI_IP and SBI_IP to Atlas. Default is true.



ASSIGN_ENDPOINT_HOST	Set to <code>true</code> to create an endpoint for Heat and OVFT services with ATLAS SBI_IP, and to <code>false</code> to create an endpoint with <code>localhost</code> .
DATA_IMAGE_SIZE	Size of data volume or ephemeral disk. Default is 120GB
BOOT_IMAGE_SIZE	Size of bootable volume. Default is 10GB
BACKUP_PASSWORD	Password for periodic Atlas backup taken twice a day. Default BACKUP_PASSWORD is an openssl generated random password.
NET_ID	ID of the network on which the VM needs to be launched (for CEE on RHOSP, VBOX, RHEL, UBUNTU, and MOS).
FIXED_IP	Create a port with a specified IP address.
SECURITY_GROUP	Associate a specified security group with the port.
DISK	Disk size for flavor in GB. Fixed value is 10GB
RAM	Memory for flavor in MB. Fixed value is 4096MB
VCPU	Number of CPUs. Fixed value is 2
FLAVOR	Existing flavor-id or name. When the FLAVOR variable is specified, DISK, RAM, VCPU and EXTRA_SPECS information is overwritten.
EXTRA_SPECS	Set extra specs for flavor Default is: hw:mem_page_size=1048576 hw:cpu_policy=dedicated for CPU pinning.
USER_DATA	Path to store generated user-data file. Default is <code>/tmp/user-data</code>
name	Name of the Atlas VM
image_name	Atlas Image file name to be used
ARTIFACT	Path of artifacts



BOOT_FROM_VOLUME	Set to true to boot from volume and to false to boot from image. Default value is false.
deployment_env	SERVICE_CINDER_VOLUME must be true to select boot from volume. Set deployment environment. Can only have the following values: CEE,VBOX,RHEL,UBUNTU,MOS. Default value is CEE.
AVAILABILITY_ZONE	Availability zone to deploy Atlas VM. Default value is nova.
DISABLE_ATLAS_HEAT	To disable Heat API in Atlas, set value to true. Default value is false.
ENABLE_BACKUP	Set to true to create periodic backups. Default value is true.
BACKUP_INTERVAL	Time interval to create periodic backups. Default value "0 */12 * * *" creates two backups per day.

Note: All variables have default values. Correct variables as needed, since they are site-dependent. More information is available within the `localrc` script itself.

For non-CEE environment, update following variables in `localrc`:
`DATA_IMAGE_SIZE`, `DISK RAM`, `VCPU EXTRA_SPECS USER_DATA NAME`
`IMAGE_NAME ARTIFACT`, `DEPLOYMENT_ENV`, `NET_ID`, `FIXED_IP` and
`SECURITY_GROUP`

5. Execute `atlas_install.sh` script to deploy Atlas, using the following command:

Note: The default `BACKUP_PASSWORD` can be changed in `localrc` before Atlas installation. Write down the Atlas `BACKUP_PASSWORD` value displayed on the console after successful installation.

```
root@cic-1:~/artifacts# ./atlas_install.sh
```

6. Log on to Atlas.
7. Display the exact version of the currently executing Atlas Virtual Machine (VM):

```
atlasadm@atlas:~ $ sudo atlas --version
```
8. Restore the required Atlas configuration files and folders according to Atlas Restore.



Note: When upgrading from 15B to R6 Atlas, perform the following steps before and after performing restore:

— Before restore, save these lines from the file `/etc/puppet/hiera data/passwords.yaml`:

- `role::atlas::keystone_heat_pass: *****`
- `role::atlas::keystone_ovft_pass: *****`
- `role::atlas::keystone_mistral_pass: *****`

— Comment the following lines in `/opt/atlas/lib/restore`:

- `/usr/local/sbin/apply-conf`
- `/opt/atlas/bin/atlas user-init`

— After restore and reboot, copy these lines:

- `role::atlas::keystone_heat_pass: *****`
- `role::atlas::keystone_ovft_pass: *****`
- `role::atlas::keystone_mistral_pass: *****`

— Insert the copied lines on Page 9 into the following file:

`/etc/puppet/hieradata/passwords.yaml`

— Execute the following commands:

```
atlasadm@atlas:~$ sudo apply-conf
atlasadm@atlas:~$ sudo atlas user-init
```



Note: When upgrading from 6 to 6.5 or later releases of Atlas, perform the following steps before and after performing restore:

- Download backup files from Swift. Refer to the Downloading Backup Files from Swift section of the document [Atlas Restore](#).
- Before restore, create file `.meta` by changing the user to `root` and executing the following commands:

```
export var="<backup_directory_name>"

echo "NAME=${var::-10}" > /var/archives/⇒
<backup_directory_name>/.meta

echo "ID=${var: -10}" >> /var/archives/⇒
<backup_directory_name>/.meta

echo "DATE=`date`" >> /var/archives/⇒
<backup_directory_name>/.meta

echo "SIZE=`du -h /var/archives/⇒
<backup_directory_name>| awk '{print $1}⇒
`" >> /var/archives/<backup_directory_name>/.meta

echo "STORAGE=SWIFT" >> /var/archives/⇒
<backup_directory_name>/.meta
```

- After restore, execute the following commands:

```
atlasadm@atlas:~$ sudo rm -f /root/.mysql.my.cnf
atlasadm@atlas:~$ sudo mysql_upgrade --force
atlasadm@atlas:~$ sudo apply-conf
```

Note: When upgrading from 6.5 to later releases of Atlas using backup stored in Swift, perform the following step before restore:

- `echo "STORAGE=SWIFT" >> /var/archives/⇒`
`<backup_directory_name>/.meta`



4 Post-Upgrade Activities

This section describes the post-upgrade activities needed for the new version of the Atlas server.

4.1 Verify Installation

To verify the installation of Atlas, do the following:

1. List active servers:

```
root@cic1:~# nova list
```

ID	Name	Status	Task State	Power State	Networks
d8b0528c-9892-4c39-b015-5dd6253aa621	ecs-atlas	ACTIVE	None	Running	tenant_3582=<ip_address>;tenant_3583=<ip_address>

2. Start an available browser and enter the following URL:

```
https://<ip_address>
```

3. Log on to Atlas from outside the CLI using NBI IP (<nbi_ip_address>):

```
<user@laptop>:~# ssh atlasadm@<nbi_ip_address>
```

4. Log on to Atlas from the vCIC CLI using SBI IP (<sbi_ip_address>):

```
root@cic1:~# ssh atlasadm@<sbi_ip_address>
```

5. Execute **ovft capp-list**.

Note: In case of rollback, execute **ovft package-list**.

4.2 SSL Certificate Installation

TLS certificates are not part of the Atlas backup. To ensure secure TLS communication, the certificates have to be reinstalled.

For more information on TLS certificate installation, refer to the “Conditions” section of the documents *SW Installation in Multi-Server Deployment* and *SW Installation in Single Server Deployment*.

4.3 Change Password for Atlas Users

This section describes how to change password for the Atlas users.



For more information about user management in a system hardening context, refer to the [System Hardening Guideline](#).

Note: New passwords must have 14 or more characters, with at least one special, numeric, lowercase and uppercase character.

4.3.1 User atlasadm

To change the password for the user atlasadm, use the command:

```
atlasadm@atlas:~$ passwd
```

```
Changing password for atlasadm.  
(current) UNIX password:  
New password:  
Retype new password:  
passwd: password updated successfully
```

```
atlasadm@atlas:~$
```

4.3.2 User root

To change the password for the user root, use the command:

```
atlasadm@atlas:~$ sudo -i
```

```
[sudo] password for atlasadm:  
root@atlas:~# passwd
```

```
New password:  
Retype new password:  
passwd: password updated successfully
```

```
root@atlas:~#
```




5 Rollback

In Atlas, the procedure for a rollback is identical to an upgrade. The only difference is that the reference to the new version is a previous version, confirmed to have been working.

To do a rollback, perform the following steps:

1. Download an older version of the Atlas image and the installation script.
2. Perform steps 1 to 4 in Section 2 on page 2, then continue with the next step below.
3. Rollback Atlas to an older version by performing the steps in Section 3 on page 4.
4. Verify the rollback by performing the steps in Section 4 on page 11.
5. Restore the latest backup of Atlas that was taken before the upgrade in Step 6.