Upgrading an Application Server Installation

You can upgrade to Sun Java System Application Server Enterprise Edition 8.1 (hereafter called Application Server) from Sun Java(TM) System Application Server 7.x (formerly Sun ONE(TM) Application Server 7.x) or a Sun Java System Application Server 8.x Platform Edition installation. Information that is transferred includes data about deployed applications, the file realm, security certificates, and other resource and server configuration settings. You can install your upgrade in a new location, or you can upgrade in place by overwriting your previous installation.

The following table shows supported Sun Java System Application Server upgrades, where PE indicates Platform Edition and EE indicates Enterprise Edition.

Table 3-1 Supported Upgrade Paths

Source Installation	8.1Platform Edition	8.1 Enterprise Edition
7.XPE	X	X
7.XSE		X
7.XEE		X
8.0PE	X	X
8.1PE		X

NOTE Before starting the upgrade process, make sure that both the source server (the server from which you are upgrading) and the target server (the server to which you are upgrading) are stopped.

The software provides two methods, a command-line utility (`asupgrade`) and a graphical user interface (Upgrade Wizard), for completing the upgrade. If you issue the `asupgrade` command with no options, the Upgrade Wizard GUI will be displayed. If the `asupgrade` command is used in command-line mode and all of the required information is not supplied, an interviewer will request information for any required options that were omitted. The Upgrade Wizard automatically detects the version of the specified source server installation.

If a domain contains information about a deployed application and the installed application components do not agree with the configuration information, the configuration will be migrated as is without any attempt to reconfigure the incorrect configurations.

During an upgrade, the configuration and deployed applications of a previous version of the Application Server are migrated; however, the runtime binaries of the server are not updated. Database migrations or conversions are also beyond the scope of this upgrade process.

Only those instances that do not use Sun Java System Web Server-specific features will be upgraded seamlessly. Configuration files related to HTTP path, CGI bin, SHTML, and NSAPI plug-ins will not be upgraded.

Application archives (EAR files) and component archives (JAR, WAR, and RAR files) that are deployed in the Application Server 7.x/8.0 environment do not require any modification to run on Application Server 8.1.

Applications and components that are deployed in the source server are deployed on the target server during the upgrade. Applications that do not deploy successfully on the target server must be migrated using the Migration Tool or `asmigrate` command, then deployed again manually.

If the upgrade includes clusters, specify one or more cluster files. Upon successful upgrade, an upgrade report is generated listing successfully migrated items along with a list of the items that could not be migrated.

This chapter discusses the following topics:

Before You Start the Upgrade Process

If you have used the JES installer to install your version of Application Server 7, and if you have chosen the Configure Later option in the JES installer, you need to perform the following:

1. Locate the Accessory CD containing the Add-ons for your version of Application Server. Alternatively, you can download the contents of the CD from http://www.sun.com/download/index.jsp.

2. Run the postInstall script as follows:

   ./postInstall AS_INSTALL_DIR AS_DATA_CONFIG_DIR

   For example, for the default installation, this command looks like this:
./postInstall /opt/SUNWappserver /var/opt/SUNWappserver

For detailed instructions on how to run this script, refer to the Readme.txt file in the Addon folder in the accessory CD or in the location where you have extracted the Add-ons.

Upgrading Through the Upgrade Utility

The upgrade utility is run from the command line using the following syntax:

```
asupgrade [--console ] [--version ] [--help ]
       [--source applicationserver_7.x/8.x_installation]
       [--target applicationserver_8.1_installation]
       --adminuser admin_user
       [--adminpassword admin_password]
       [--masterpassword changeit]
       [--passwordfile path_to_password_file]
       [--domain domain_name]
       [--nsspwdfile NSS_password_filepath]
       [--targetnsspwdfile target_NSS_password_filepath]
       [--jkspwdfile JKS_password_filepath]
       [--capwdfile CA_password_filepath]
       [--clinstancefile file1 [, file2, file3, ... filen]]
```

The following table describes the command options in greater detail, including the short form, the long form, and a description.

Table 3-2 asupgrade Utility Command Options

Short Form	Long Form	Description
-c	---console	Launches the upgrade command line utility.
-V	---version	The version of the Upgrade Tool.
-h	---help	Displays the arguments for launching the upgrade utility.
-t	---target	The installation directory for Sun Java System Application Server 8.1.
-a	---adminuser	The username of the administrator.
-w	---adminpassword	The password for the adminuser. Although this option can be used, the recommended way to transmit passwords is by using the -passwordfile option.
-m	--masterpassword	The master password that is created during installation. The default value is `changeit`. Although this option can be used, the recommended way to transmit passwords is by using the --passwordfile option. Note: This option is required only if your target server is Application Server 8.1 EE.
-f	--passwordfile	The path to the file that contains the adminpassword and masterpassword. Content of this file should be in the following format: AS_ADMIN_ADMINPASSWORD=adminpassword AS_ADMIN_MASTERPASSWORD=masterpassword
-d	--domain	The domain name for the migrated certificates.
-n	--nsspwdfile	The path to the NSS password file.
-e	--targetnsspwdfile	The path to the target NSS password file.
-j	--jkspwdfile	The path to the JKS password file.
-p	--capwdfile	The path to the CA certificate password file.
-i	--clinstancefile	The path to the cluster file. The default filename is $AS_INSTALL/conf/clinstance.conf.

The following examples show how to use the asupgrade command-line utility to upgrade an existing application server installation to Application Server 8.1.

Example 1: Upgrading an Application Server 7 Installation to Application Server 8.1 with Prompts for Certificate Migration.

This example shows how to upgrade a Sun Java System Application Server 7 installation to Sun Java System Application Server 8.1. You will be prompted to migrate certificates. If you reply no, then no certificates will be migrated.

```
% asupgrade --adminuser admin --passwordfile password.txt
--source /home/sunas7 --target /home/sjsas8.1
```

Example 2: Upgrading an Application Server 7.1 EE Installation with Clusters and NSS Certificates to Application Server 8.1 EE

This example shows how to upgrade a Sun Java System Application Server 7.1 EE installation with a cluster to Sun Java System Application Server 8.1 EE. NSS certificates will be migrated, as will the clinstance.conf cluster file.

```
% asupgrade --adminuser admin --passwordfile password.txt
       -source /home/sjsas7.1 --target /home/sjsas8.1
       --domain domain1
       --nsspwdfile /home/sjsas7.1/nsspassword.txt
       --targetnsspwdfile /home/sjsas8.1/nsspassword.txt
       --clinstancefile /home/sjsas7.1/config/clinstance.conf
```

After the upgrade, node agents for all remote instances must be created and started on their respective host systems.

Example 3: Upgrading an Application Server 7.0 PE Installation with NSS Certificates to Application Server 8.1 PE

This example shows how to upgrade a Sun Java System Application Server 7.0 PE installation to Sun Java System Application Server 8.1 PE. The NSS certificates from the 7.0 PE source server will be converted to JKS and CA certificates in the 8.1 PE target server.

```
% asupgrade --adminuser admin --passwordfile password.txt
       --source /home/sjsas7.0 --target /home/sjsas8.1
       --domain domain1
       --nsspwdfile /home/sjsas7.0/nsspassword.txt
       --jkspwdfile /home/sjsas7.0/jkspassword.txt
       --capwdfile /home/sjsas7.0/capassword.txt
```

Example 4: Upgrading an Application Server 8.0 PE Installation with JKS and CA Certificates to Application Server 8.1 PE

This example shows how to upgrade a Sun Java System Application Server 8.0 PE installation to Sun Java System Application Server 8.1 PE. JKS and CA certificates will be migrated.

```
% asupgrade --adminuser admin --passwordfile password.txt
       --source /home/sjsas8.0 --target /home/sjsas8.1
       --domain domain1
       --jkspwdfile /home/sjsas8.0/jkspassword.txt
       --capwdfile /home/sjsas8.1/capassword.txt
```

Upgrading Through the Wizard

The Upgrade wizard provides a graphical user interface (GUI). Using the wizard increases install time and space requirements. You can start the Upgrade wizard in GUI mode from the command line or from the desktop.

To start the wizard,

- On UNIX, change to the <*install_dir*> / `bin` directory and type `asupgrade`.

- On Windows, double-click the asupgrade icon in the <*install_dir*> / `bin` directory.

If the Upgrade checkbox was selected during the Application Server installation process, the Upgrade Wizard screen will automatically display after the installation completes.

From the Upgrade Wizard screen:

1. In the Source Installation Directory field, enter the location of the Sun Java System Application Server 7 (formerly Sun ONE™ Application Server 7) or Sun Java System Application Server 8.x installation from which to import the configuration.
2. In the Target Installation Directory field, enter the location of the Application Server installation to which to transfer the configuration.

   If the upgrade wizard was started from the installation (the Upgrade from Previous Version checkbox was checked during the Application Server installation), the default value for this field will be the directory to which the Application Server software was just installed.
3. If a Sun Java System Application Server 7.1 Enterprise Edition installation with clusters and no security certificates is being upgraded to Sun Java Systems Application Server 8.1 Enterprise Edition, press the Next button and continue with Step 10. All other upgrades without certificates continue with Step 12. Continue with Step 4 if security certificates need to be transferred.
4. If the source installation has security certificates that must be transferred, check the Transfer Security Certificates checkbox, press the Next button, and the Transfer Security Certificates screen displays.

5. From the Transfer Security Certificates screen, press the Add Domain button to add domains with certificates to be transferred. The Add Domain dialog displays.
6. From the Add Domain dialog, select the domain name that contains the security certificates to migrate and enter the appropriate passwords.
7. Click the OK button when done. The Transfer Security Certificates screen will be displayed again.
8. Repeat Step 5 and Step 6 until all the domains that have certificates to be transferred have been added.
9. After all of the domains that contain certificates to be transferred have been added, press the Next button and continue with Step 12 or with Step 10 if cluster configuration information needs to be transferred.
10. If a Sun Java Systems Application Server 7.1 Enterprise Edition installation with clusters is being upgraded to Sun Java Systems Application Server 8.1 Enterprise Edition, the Transfer Cluster Configurations screen will be displayed. Press the Add Cluster button. The Select `clinstance.conf` file dialog box will be displayed. Choose clinstance file and click the Open button. The `clinstance.conf` file will be added to the list.
11. Enter the cluster file name, which contains the cluster configuration information to be migrated. Repeat this process until all the cluster configuration files that need to be migrated have been added, then press the Next button.
12. The Upgrade Results screen displays, showing the status of the upgrade operation in the Results field.
13. Click the Finish button to close the Upgrade Tool when the upgrade process is complete.

Upgrading a Cluster: How Is It Done?

The Application Server's Upgrade utility captures cluster details from the `clinstance.conf`, the cluster configuration file. If more than one cluster has been defined for the Application Server 7.x, multiple `.conf` files may exist prior to the upgrade. The configuration files could have any name, but all would have the `.conf` file extension. If clusters will be included in an upgrade, consider the following points when you are defining `clinstance.conf` files.

Instance names in the `clinstance.conf` file must be unique. For example, in Application Server 7.x, machine A could have server1 and server2 participating in a cluster. Machine B could also have a server1 participating in the same cluster. Typically, the `clinstance.conf` file would include the server1 and server2 of machine A and server1 of machine B. Application Server 8.1 requires instance names in a cluster to be unique. Therefore, prior to the upgrade, in the `clinstance.conf` file you would need to rename server1 of machine B to a unique name, such as server3 or server1of machineB. You do not, however, need to rename the server1 instance itself in machine B; you only need to rename the server in the `clinstance.conf` file. The expectation is that instances participating in the cluster are homogeneous, in the sense that they would have same kind of resources, and same applications deployed in them.

When the upgrade process runs, the instance marked as the master instance will be picked up for transferring the configuration. If there is no instance marked as the master instance, one of the instances will be picked up in a random manner and used for transferring the configuration.

A cluster is created in the DAS, along with instances defined in the `clinstance.conf` file. All these instances participating in this cluster share the same configuration named <*cluster_name*>`-config`, where the *cluster_name* is `cluster_0` for the first cluster, `cluster_1` for the next cluster, and so forth. Each instance in the cluster has HTTP and IIOP ports set in their system properties. The HTTP port is the port defined in the `clinstance.conf` file as the instance port. IIOP ports are selected from the iiop-cluster configuration in the `server.xml` file.

Server instances that participate in the cluster and that run on a machine other than the machine on which the DAS is running, are created with a node-agent named <*host-name*>-<*domain-name*>, where the *host-name* is the name given in the `clisntance.conf` file for that particular instance and the *domain-name* is the name to which this cluster belongs.

After the upgrade process has been completed on the DAS, install Application Server 8.1 on the other machines where clustered instances need to run.

1. Copy the node-agent directory from DAS machine to client machine under *install-dir* / `nodeagents` / . For instance, if your DAS is installed on HostA and client machine name is HostB, the upgrade process would have created a node agent named "`HostB-`<*domain_name*>" as the node-agent for HostB. Hence copy `HostB-`<*domain_name*> from `HostA`<*AS81_install_dir*> / `nodeagents` / `HostB-`<*domain_name*> directory to `HostB` <*AS81_install_dir*> / `nodeagents`. After copying, delete the copied node agent directory under HostA.

2. Edit nodeagent.properties file on client machine HostB under `agent/config` directory. Set `agent.client.host` to the client machine name. In this case it should be HostB.
3. Edit `das.properties` file on client machine HostB under `agent/config` directory. Make sure `agent.das.isSecure=false` in `das.properties` file. It should be set to false if by default Application Server 7.x Administration Server was running on non secure port. If Application Server 7.x Administration Server was running on secure port, then it should be set to true.
4. Start domain and start node agents on both DAS machine as well as client machines. This in turn will run the clustered instance.

Correcting Potential PE and EE Upgrade Problems

This section addresses the following issues that could occur during an upgrade to Application Server 8.1:

Migrating Additional HTTP Listeners Defined on the Source Server to the Target PE Server

If additional HTTP listeners have been defined in the PE source server, those listeners need to be added to the PE target server after the upgrade:

1. Start the Admin Console.
2. Expand Configuration.

3. Expand HTTP Service.
4. Expand Virtual Servers.
5. Select <server>.
6. In the right hand pane, add the additional HTTP listener name to the HTTP Listeners field.
7. Click Save when done.

Migrating Additional HTTP and IIOP Listeners Defined on the Source Server to the Target EE Server

If additional HTTP listeners or IIOP listeners have been defined in the source server, the IIOP ports must be manually updated for the target EE servers before any clustered instances are started. For example, if MyHttpListener was defined as an additional HTTP listener in server1, which is part of the cluster, because server instances are symmetrical in a cluster, the other instances in the cluster will also have the same HTTP listener. In the target configuration named `<cluster_name>-config`, this listener must be added with its port set to a system property {`myHttpListener_HTTP_LISTENER_PORT`}. In the target server, each server instance in this cluster that uses this configuration would have system property named `myHttpListener_HTTP_LISTENER_PORT`. The value of this property for all server instances would be set to the port value in the source server, server1. These system properties for these server instances must be manually updated with non-conflicting port numbers before the server is started.

If additional HTTP listeners have been defined in the source server, those listeners need to be added to the target server after the upgrade:

1. Start the Admin Console.
2. Expand Configuration and select the appropriate <server>-config configuration.
3. Expand HTTP Service.
4. Expand Virtual Servers.
5. Select <server>.
6. In the right hand pane, add the additional HTTP listener name(s) to the HTTP Listeners field.

7. Click Save when done.

Eliminating Port Conflict Problems

After upgrading the source server to AS 8.1 EE, start the domain. Start the node agent that, by default, starts the server instances. Start the Admin Console and verify that these servers are started. If any of the servers are not running, in the <*install_dir*>/nodeagents/<*node-agent-name*>/<*server_name*>/logs/server.log file, check for failures that are caused by port conflicts. If there any failures due to port conflicts, use the Admin Console and modify the port numbers so there are no more conflicts, then stop and restart the node agent and servers.

If an AS 7.1 EE source server with no clusters is being upgraded to AS 8.1 EE (only standalone instances are being upgraded), and if server1 in the AS 7.1 source server has an IIOP port number of 3700, this conflicts with the IIOP port that is defined for the AS 8.1server-config. If these conditions exist, start the Admin Console after the upgrade and change the IIOP port for the server-config's IIOP listener to a non conflicting port number. If an AS 7.x SE source server is being upgraded to AS 8.1 EE, the upgrade process should automatically update the IIOP port for the <server-config>.

Eliminating Problems Encountered When A Single Domain has Multiple Certificate Database Passwords

If the upgrade includes certificates, provide the passwords for the source PKCS12 file and the target JKS keyfile for each domain that contains certificates to be migrated. Since Application Server 7 uses a different certificate store format (NSS) than Application Server 8 PE (JSSE), the migration keys and certificates are converted to the new format. Only one certificate database password per domain is supported. If multiple certificate database passwords are used in a single domain, make all of the passwords the same before starting the upgrade. Then reset the passwords after the upgrade has been completed.

Resolving Problems with Shared Components During Side-by-Side Upgrade

If you have performed a side-by-side upgrade from Application Server 7.x with (MQ and HADB) to Application Server 8.1 EE, do not uninstall the older version - Application Server 7.x. The uninstall process removes shared components, such as JAF, JavaMail, and MQ libraries. The missing shared components will cause the Application Server 8.1 EE installation to malfunction. If you want to uninstall Application Server 7.x, remove `SUNWas*` packages that belong to Application Server 7.x by running the `pkgrm` command, and do not run the uninstall script. If you have already uninstalled Application Server 7.x using the uninstall script, copy the shared components manually by running the `pkgadd` command.