Migrating VMware Workspace Portal

Workspace Portal 2.1

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001588-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Migrating VMware Workspace Portal 1

Migrating VMware Workspace Portal describes how to migrate from VMware Horizon Workspace™ 1.8.1 or 1.8.2, or VMware Workspace Portal 2.0 to VMware Workspace Portal 2.1.

Intended Audience

Migrating VMware Workspace Portal is intended for enterprise administrators. This information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology, identity management, Kerberos, and directory services.

Migrating VMware Workspace Portal Overview

Use *Migrating VMware Workspace Portal* to upgrade your existing deployment, versions 1.8.1, 1.8.2, or 2.0, to version 2.1.

To migrate from VMware Horizon Workspace 1.5.x to VMware Workspace Portal 2.1, you must first upgrade Horizon Workspace 1.5.x to version 1.8.2 and then migrate 1.8.2 to 2.1.

If you would rather perform a fresh installation of Workspace 2.1, see the *Installing and Configuring VMware Workspace Portal Guide*. Remember that a new installation will not preserve your existing configurations.

This migration involves migrating a configuration spread across the multiple virtual appliances used in previous versions to the single virtual appliance, the workspace-va virtual machine, used in Workspace 2.1. The migration process requires you to manually move configuration information from the previous version to version 2.1.

ATTENTION The migration process does not transfer audit event information from the source deployment to Workspace 2.1.

To learn how to use and maintain your new Workspace 2.1 instance, see the *VMware Workspace Portal Administrator's Guide*.

Prepare to Migrate Workspace to Version 2.1

2

To migrate to VMware Workspace Portal 2.1 from VMware Horizon Workspace 1.8.1 or 1.8.2 or from VMware Workspace Portal 2.0, you must prepare the source installation for the migration.

Preparing to migrate Workspace to version 2.1 involves preparing the source deployment, version 1.8.1, 1.8.2, or 2.0, for the migration and preparing the database for 2.1.

The best practice is to preserve the source deployment, version 1.8.1, 1.8.2, or 2.0, by installing Workspace 2.1 with a new DNS record and IP address and configuring it against a copy of the database used in the source deployment. This practice leaves the source environment running for comparison purposes and can facilitate the export of Horizon Files data, applicable for versions 1.8.1 and 1.8.2, to the newly supported Air Watch Secure Content Locker.

Prerequisites

- Deploy the Workspace 2.1 OVA file with a new DNS record and IP address. See *Installing and Configuring VMware Workspace Portal*.

  IMPORTANT This prerequisite task ends when you power on the virtual appliance.

  After the core migration process, you can change the FQDN of the 2.1 host to the one used for the source version, 1.8.1, 1.8.2, or 2.0.

- If switching from an internal database in the source deployment to an external database in the target deployment meets the needs of your organization, transfer the data accordingly. See *Installing and Configuring VMware Workspace Portal*.

Procedure

1 In the source deployment, change the appliance administrator password.

  Changing the password of the source deployment, version 1.8.1, 1.8.2, or 2.0, ensures that the password is saved in the proper encryption format.

  a Log in to the Configurator Web interface at https://*ConfiguratorHostname*.

  b Click **Password**.

  c Provide the password information and click **Save.**

2 Prepare the database.

Follow the appropriate instructions depending on the databases you are migrating data between.

Migration Type	Instructions
External to External Database Migration	The following steps provide an overview of how to configure an external database for a migration to Workspace 2.1. a Make an external database available for the target deployment. This step makes the content of the database in the source deployment available in the target deployment as a virtual machine. You can achieve this goal with one of the following methods. ■ Clone the source external database, either VMware vFabric Postgres or Oracle, and bring it up on a new IP address. ■ Install a new external Postgres database and export the content from the source database (an internal or an external Postgres instance) to the new instance. b Take snapshots of both the source and target database virtual machines. The source database is the original database virtual machine while the target database is the newly created database virtual machine used for Workspace 2.1. The snapshot gives you a backup that you can use if something goes wrong during the deployment or if you want to perform the migration again.
Internal to Internal Database Migration **or** **External to Internal Database Migration**	Preparing an internal database in Workspace 2.1 for the migration process involves saving the data from the source database to a file and copying that file to the target database. a Log in to the service-va virtual machine of the source deployment as the root user. b Change the directory to the location of the vPostgres tools, `/opt/vmware/vpostgres/current/bin`. c To back up the vPostgres internal database to a temporary file, issue the appropriate command and provide the password of the vPostgres user when prompted. For example, `./pg_dump –U postgres ––clean –f /SourceFilepathToBackedUpDatabase saas` Replace the placeholder as necessary. For example, `./pg_dump –U postgres ––clean –f /tmp/db_dump.data saas` The preceding example command creates a file named `db_dump.data` in the `tmp` directory and copies the data from the vPostgres database, named `saas`, to the file. d Using a tool such as `scp`, copy the file with the backed up data to Workspace 2.1. For example, `scp SourceFilepathToBackedUpDatabase root@Workspace2.1ServerName/TargetFilepathToDirectory` Replace the placeholders as necessary. For example, `scp /tmp/db_dump.data root@Workspace2.1ServerExample/tmp`

The source deployment, 1.8.1, 1.8.2, or 2.0, is now backed up and the Workspace 2.1 virtual appliance is deployed and prepared for the initial configuration.

What to do next

■ If you are migrating to the internal database, complete the internal database configuration. See Chapter 3, “Migrate Data to the Workspace 2.1 Internal Database,” on page 11.

- If you are migrating to an external database, continue with the core configuration. See Chapter 4, "Migrate the Core Configuration to Workspace 2.1," on page 13.

Migrate Data to the Workspace 2.1 Internal Database

3

If you are migrating data to the Workspace 2.1 internal database, after you copy the data from the database of the source deployment to a file in the target deployment, you must configure the Workspace 2.1 internal database.

The procedure for configuring the internal database in Workspace 2.1 involves deleting the existing internal database from the target deployment, creating a new internal database in the target deployment, and populating the new internal database with the data you previously saved from the source database.

NOTE In the commands that follow, `postgres` is the name of the vPostgres user and `saas` is the name of the vPostgres database.

Prerequisites

Prepare for the migration to the Workspace 2.1 internal database. See Chapter 2, "Prepare to Migrate Workspace to Version 2.1," on page 7

Procedure

1 Log in to the workspace-va virtual machine as the root user, in the Workspace 2.1 deployment.

2 Stop the workspace-va virtual machine.

For example, `/etc/init.d/horizon-workspace stop`

3 Change the directory to the location of the vPostgres tools, `/opt/vmware/vpostgres/current/bin`.

4 To remove the default vPostgres internal database from the workspace-va virtual machine, issue the appropriate command and provide the password of the vPostgres user when prompted.

For example, `./dropdb -U postgres saas`

The preceding example command deletes the default internal database, which is named `saas`.

5 To create a new vPostgres internal database in the workspace-va virtual machine, issue the appropriate command and provide the password of the vPostgres user when prompted.

NOTE Workspace only recognizes the name `saas` as the vPostgres database name. Do not use a different name.

For example, `./createdb -U postgres -T template0 saas`

The preceding example command creates a new database named `saas` using the vPostgres database template named `template0`.

6 To populate the new database with the backed up data from the source deployment, issue the appropriate command and provide the password of the vPostgres user when prompted.

   For example, `./psql –U postgres saas < TargetFilepathToDirectory`

   Replace the placeholder as necessary.

   For example, `./psql –U postgres saas < /tmp/db_dump.data`

   The preceding example populates the new database named `saas` with the backed up data from the `db_dump.data` file.

7 Start the workspace-va virtual machine.

   For example, `/etc/init.d/horizon–workspace start`

The result is that the internal database is configured for the Workspace 2.1 deployment.

What to do next

Continue with the core configuration. See Chapter 4, “Migrate the Core Configuration to Workspace 2.1,” on page 13.

Migrate the Core Configuration to Workspace 2.1

4

Once you prepare for the migration to Workspace 2.1, you can migrate the core configuration from the source deployment, version 1.8.1, 1.8.2, or 2.0 to the target deployment, Workspace 2.1.

Migrating the core configuration involves migrating content from virtual machines of the source deployment to the workspace-va virtual machine of the Workspace 2.1 deployment.

Procedure

1 If your source deployment uses multiple service-va or connector-va virtual machines, log in to the Configurator Web interface at https://*ConfiguratorHostname*/cfg to identify the first instance of the respective virtual appliance type.

The interface opens to the System Information page.

The Application Manager section of the page lists all the service-va virtual machines with the pattern service-va, service-va-1, service-va-2, and so on. The first instance of the service-va virtual machines is service-va, with no number in the name.

The Connector section of the page lists all the connector-va virtual machines with the pattern connector-va, connector-va-1, connector-va-2, and so on. The first instance of the connector-va virtual machines is connector-va, with no number in the name.

2 Using a tool such as `scp`, copy the specified `.uber` and `.json` files from the source deployment to the new Workspace 2.1 deployment.

NOTE

- If you have multiple service-va virtual machines, copy the `.uber` file from the first instance of the service-va virtual machines.
- If you have multiple connector-va virtual machines, copy the `.json` files from the first instance of the connector-va virtual machines.

File to Copy from the service-va Virtual Machine	Directory in the workspace-va Virtual Machine to Copy File to
`/usr/local/horizon/bin/masterkeys.uber`	`/usr/local/horizon/bin`

Files to Copy from the connector-va Virtual Machine	Directory in the workspace-va Virtual Machine to Copy Files to
`/var/lib/config-admin.json`	`/usr/local/horizon/conf`
`/var/lib/config-state.json`	`/usr/local/horizon/conf`

3 Log in to the workspace-va virtual machine as the root user with the default password **vmware**, in the Workspace 2.1 deployment, and edit the `/usr/local/horizon/conf/config-state.json` file.

To log in as root user, first log in to the workspace-va virtual machine as SSH user, then issue the `su` command to become the superuser.

a Change the `mol` URL at the top of the file to the URL for your Workspace 2.1 server.

The place holders, *SourceFQDN* and *Workspace2.1FQDN*, in the following examples, indicate the location of the source FQDN that you must replace with the Workspace 2.1 FQDN.

From:

```
"mol" : {
    "isConfigured" : true,
    "url" : "https://SourceFQDN.com:443",
```

To:

```
"mol" : {
    "isConfigured" : true,
    "url" : "https://Workspace2.1FQDN.com:443",
```

b If the following line exists in the file, change it.

From:

```
"furthestVisitedPage" : "DOMAINJOIN",
```

To:

```
"furthestVisitedPage" : "SCHEDULING",
```

c Change the host value from the FQDN of the source deployment to the FQDN of the Workspace 2.1 deployment.

From:

```
  "idp" : {
    "isConfigured" : true,
    "host" : "SourceFQDN.com:443"
```

To:

```
  "idp" : {
    "isConfigured" : true,
    "host" : "Workspace2.1FQDN.com:443"
```

4 On the workspace-va virtual machine, edit the permissions on the files you just edited as illustrated by the following example.

```
cd /usr/local/horizon/conf
chown horizon config-admin.json config-state.json
chgrp www config-admin.json config-state.json
chmod 600 config-admin.json config-state.json
cd /usr/local/horizon/bin
chown horizon masterkeys.uber
chgrp www masterkeys.uber
chmod 600 masterkeys.uber
```

5 On the service-va virtual machine, of the source deployment, copy the encrypted password string from the `/usr/local/horizon/conf/runtime-config.properties` file.

The copied password from the source deployment is required for the target deployment in the following step. Also, this `runtime-config.properties` file is of use in the following step, so keep it open.

The password is in the database section of the file, either Postgres or Oracle. In the example line that follows, the place holder *EncryptedStringFromSource_runtime-config.propertiesFile* indicates the location of the actual password that you must copy.

```
secure.datastore.jdbc.password=EncryptedStringFromSource_runtime-config.propertiesFile
```

6 Access the `/usr/local/horizon/conf/runtime-config.properties` files of both the source and target deployments and edit the file in the target deployment as required.

a Edit the database section of the `/usr/local/horizon/conf/runtime-config.properties` file on the workspace-va virtual machine in the target deployment.

The database section is either Postgres or Oracle depending on your deployment. If the database is Postgres, it is either an internal database or an external database.

Replace the IP address of the database. For an internal database, replace the IP address with the string `localhost`. For an external database replace the IP address with the new IP address of the external database.

Replace the password with the encrypted password string that you just copied from the source deployment.

Also, make sure `datastore.jdbc.external` is set to `true` for an external database or false for an internal database, as shown in the examples that follow.

The place holders, *NewDataBaseIPaddress* and *EncryptedStringFromSource_runtime-config.propertiesFile* in the following examples, indicate the location of the information that you must replace.

Internal Postgres

```
datastore.jdbc.url=jdbc:postgresql://NewDataBaseIPaddress/saas?stringtype=unspecified
datastore.jdbc.driverClassName=org.postgresql.Driver
datastore.sessionFactory.hibernate.dialect=org.hibernate.dialect.PostgreSQLDialect
datastore.jdbc.userName=horizon
datastore.jdbc.external=false
secure.datastore.jdbc.password=EncryptedStringFromSource_runtime-config.propertiesFile
```

External Postgres

```
datastore.jdbc.url=jdbc:postgresql://NewDataBaseIPaddress/saas?stringtype=unspecified
datastore.jdbc.driverClassName=org.postgresql.Driver
datastore.sessionFactory.hibernate.dialect=org.hibernate.dialect.PostgreSQLDialect
datastore.jdbc.userName=horizon
datastore.jdbc.external=true
secure.datastore.jdbc.password=EncryptedStringFromSource_runtime-config.propertiesFile
```

External Oracle

```
datastore.jdbc.url=jdbc:oracle:thin:@NewDataBaseIPaddress:1521:orcl
datastore.jdbc.driverClassName=oracle.jdbc.driver.OracleDriver
datastore.sessionFactory.hibernate.dialect=org.hibernate.dialect.Oracle10gDialect
datastore.jdbc.userName="saas"
datastore.jdbc.external=true
secure.datastore.jdbc.password=EncryptedStringFromSource_runtime-config.propertiesFile
```

b Comment out or remove the following parameters and their respective values from the `runtime-config.properties` file of the target deployment.

- `secure.components.encryptionService.db.masterKeyStorePwd=PasswordValue`
- `secure.components.suiteToken.keyStorePwd=PasswordValue`

c Search the `runtime-config.properties` file of the source deployment for the following parameters and take the appropriate action depending on if the parameters are present or not.

- `secure.components.encryptionService.db.masterKeyStorePwd=PasswordValue`

- `secure.components.suiteToken.keyStorePwd=`*`PasswordValue`*

If	Then
the file contains the parameters,	copy the parameters with their respective values and paste them to the bottom of the `runtime-config.properties` file of the target deployment.
the file does not contain the parameters,	add the following two lines, which include the parameters with their default values, to the bottom of the `runtime-config.properties` file of the target deployment. ■ `secure.components.encryptionService.db.masterKeyStorePwd=AS95Iv3ZiXGYrbOfKnOwysnm9f2eqbkgw9uveLbWLeje` ■ `secure.components.suiteToken.keyStorePwd=AS95Iv3ZiXGYrbOfKnOwysnm9f2eqbkgw9uveLbWLeje`

7 Copy the Solr indexes from the source deployment to Workspace 2.1.

Apache Solr is an open source enterprise search platform. Moving the Solr indexes from the source deployment to Workspace 2.1 provides the workspace-va virtual machine with text search capabilities.

The example steps that follow provide a possible approach for accomplishing this step.

Example Steps	Example Commands
In the service-va virtual machine, bundle the Solr indexes located in the `horizoninstance` directory into a TAR file.	`cd /opt/vmware/horizon/horizoninstance` `tar cvf /tmp/solr_index.tar index`
Copy the file, `solr_index.tar` in the preceding example, from the service-va virtual machine to the workspace-va virtual machine of the Workspace 2.1 deployment.	You can use a command such as `scp`.

In the workspace-va virtual machine, prepare the `workspace` folder, unbundle the TAR file, and change the permissions of the `index` file.	`cd /opt/vmware/horizon/workspace`
	`mv index index.bak`
	`tar xvf /tmp/solr_index.tar`
	`chmod –R 750 /opt/vmware/horizon/workspace/index`
	`chown –R horizon /opt/vmware/horizon/workspace/index`
	`chgrp –R www /opt/vmware/horizon/workspace/index`

8 Take a memory snapshot of the workspace-va virtual machine in the Workspace 2.1 deployment.

9 On the workspace-va virtual machine, issue the following command to restart Workspace 2.1.

`"service horizon-workspace restart"`

The workspace-va virtual machine connects to the new database and runs all the necessary schema changes.

10 Issue SQL commands to update the database.

The example SQL commands in this step are applicable to both Oracle and Postgres unless otherwise noted.

a Issue the following command to delete all rows in the ServiceInstance table.

```
delete from "ServiceInstance";
```

b Insert the DAAS module template entry into the Module table.

Command Description	Example Command

View the rows in the Module table	Command:
	`select * from "Module";`
	Output:
	`id moduleName idOrganization enabled properties idEncryptionMethod`
	`55 XenApp 50 1 NULL 3`

Add a row to the table using the previous output to ensure that the `id` value, which is `55` for `XenApp` in the preceding example, is one digit higher than the value in the previous row and that the `idOrganization` value, which is `50` in the preceding example, matches the other rows.	Postgres
	`INSERT INTO "Module" VALUES (56,'Desktone',50,False,NULL,3);`
	Oracle
	`INSERT INTO "Module" VALUES (56,'Desktone',50,0,NULL,3);`

11 Change the default root password of the workspace-va virtual machine.

The default root password of **`vmware`** that you used earlier in this task is not secure and must be changed.

a Log in to the Appliance Configurator at https://*Workspace2.1FQDN*.com:8443/cfg/login using the appliance administrator password.

b Click **System Security**.

c In the **Root Password** text box, enter **vmware**.

d In the **New Root Password** and **Confirm Root Password** text boxes, enter a new root password.

e In the **New SshUser Password** and **Confirm SshUser Password** text boxes, enter a new Sshuser password.

f Click **Save.**

The result is that root and SSH user passwords are updated. Use these new passwords to log in to the workspace-va virtual machine in the future.

What to do next

Migrate the Connector configuration to Workspace 2.1. See Chapter 5, “Migrate the Connector Configuration to Workspace 2.1,” on page 19.

Migrate the Connector Configuration to Workspace 2.1

5

Once you migrate the core configuration to Workspace 2.1, migrate the Connector configuration from the source deployment to Workspace 2.1.

Procedure

1 As an administrative user, log in to the Workspace Admin Console of the Workspace 2.1 deployment at https://*Workspace2.1FQDN*.com.

2 Edit the identity provider settings.

   a Select **Settings > Identity Providers**

   b Keep the original Connector instance while deleting all other entries in the list of identity providers.

   The original Connector instance is the Connector instance from which you copied the `.json` files.

   c On the Identity Providers page, click **Edit** next to the original Connector instance.

   d Click the options in the **Authentication Methods** section as necessary to highlight only the **Password** option.

   e Click the **ALL RANGES** option in the **Network Ranges** section.

   f Click **Save**.

3 Edit the policy settings.

   a Click the **Policies** tab.

   b Click **Edit** next to the default access policy set.

   c Delete all the listed policies except for the two with the following values.

Policy Name	Client Type	Minimum Authentication Score
device policy	Native App	1
web policy	Web Browser	1

   d Click **Save**.

4 Log out of the Workspace Admin Console.

5 Log in to the Connector Services Admin pages at https://*Workspace2.1FQDN*.com:8443/hc/admin/ using the same appliance administrator username and password used for the source deployment.

6 Change the Workspace 2.1 identity provider URL, if necessary.

   a On the Connector Services Admin Advanced page, click **Identity Provider**.

   b If the IdP Hostname entry does not match the new URL, change it accordingly and click **Save**.

      The new URL is the mol URL you added to the `config-state.json` file, such as https://*Workspace2.1FQDN*.com:443.

7 Change the Workspace 2.1 URL to the forgot password page, if necessary.

   a On the Connector Services Admin Advanced page, click **Auth Adapters**.

   b Click **Edit** for the PasswordIdpAdapter adapter.

   c If the hostname in the URL of the **Link to forgot password page** entry does not match the new URL, change it accordingly and click **Save**.

8 Force Workspace 2.1 to join the Active Directory domain.

   a Log in to the workspace-va virtual machine as the root user, in the Workspace 2.1 deployment.

      To log in as root user, first log in to the workspace-va virtual machine as SSH user, then issue the `su` command to become the superuser.

   b Issue the following command to force Workspace to join the Active Directory domain.

      Replace the place holders *Workspace2.1DomainName* and *DomainUserName* with the actual values for your organization.

      ```
      # /opt/likewise/bin/domainjoin-cli join Workspace2.1DomainName DomainUserName
      ```

      The command returns the following result.

      ```
      Joining to AD Domain:   Workspace2.1DomainName
      With Computer DNS Name: Workspace2.1FQDN
      DomainUserName@Workspace2.1DomainName's password:
      ```

   c Enter the domain user name's password.

      After you provide the correct password, the system displays the message `SUCCESS`.

9 Verify that the Workspace 2.1 URLs provide you with the appropriate access.

   a As an administrative user, log in to the Workspace Admin Console at https://*Workspace2.1FQDN*.com.

   b Log in to the Appliance Configurator as the appliance administrator at https://*Workspace2.1FQDN*.com:8443/cfg/login.

   c Access the Workspace administrator console shortcuts page at https://*Workspace2.1FQDN*.com:8443.

10 If the https://*Workspace2.1FQDN*.com URL takes you to the login page of the source deployment instead of the 2.1 deployment, configure Workspace 2.1 to use the correct URLs.

   a Edit the StrData column of the FederationArtifacts table to the correct the URLs.

   b On the Connector Services Admin Identity Provider page, click **Save**.

      Saving the Identity Provider page even though you did not edit the page is required to flush the database changes to Workspace.

The base migration is complete.

What to do next

Perform each of the following procedures that apply.

- If you choose to change the FQDN of the Workspace 2.1 deployment to the FQDN used originally by the source deployment, you must either shut down the source vApp or change the FQDN of the source vApp to its own gateway-va virtual machine.
- Edit the Connector Services Admin Authentication Adapters page to recreate the configuration of the Kerberos and SecurID authentication methods. See *Installing and Configuring Workspace*.
- In the Workspace Admin Console, recreate the network ranges and access policies. See *Workspace Administrator's Guide*
- Install your SSL certificate and set your FQDN to a new or existing load balancer. See *Installing and Configuring Workspace*.
- If you migrated to an internal vPostgres database and choose to create a high availability environment in production, see http://kb.vmware.com/kb/2094258.

Index