vSphere Agent 7.3

Quick Start Guide

Revision: This manual has been updated for Version 7.30 (March 2014).

Software Version: 7.30

Acknowledgements: Two encryption methods, DES and TripleDES, include cryptographic software written by Eric Young. The Windows versions of these algorithms also include software written by Tim Hudson. Bruce Schneier designed Blowfish encryption.

The Agent, Agent Console, and Vault applications have the added encryption option of 128/256 bit AES (Advanced Encryption Standard). Advanced Encryption Standard algorithm (named Rijndael, pronounced “Rain Doll”) was developed by cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen. This algorithm was chosen by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce to be the new Federal Information Processing Standard (FIPS). See:http://csrc.nist.gov/encryption/aes/round2/r2report.pdf for details.

The Agent and Vault applications have the added security feature of an over the wire encryption method.

Contents

1 Introduction

vSphere Agent 7.3 backs up virtual machines (VMs), and restores VMs, virtual disks (VMDKs), and specific files and folders in VMware vSphere environments.

This guide will help you get started with vSphere Agent 7.3. The guide describes how to deploy and configure the Agent, and create backup jobs.

2 Deploying and Configuring the vSphere Agent

2.1 Deploying the vSphere Agent

The vSphere Agent is pre-installed in a VM with 2 virtual CPUs and 2 GB of RAM. The Agent is provided in OVA format, and requires 158 GB of free space.

Note: When deploying the Agent with thin-provisioned disks, extra free space is required for the deployment and for files created by the vSphere Agent (e.g., log files). At least 10 GB of free space should be available when deploying the vSphere Agent with thin-provisioned disks.

After obtaining the OVA file from your provider, deploy the file in the vCenter where you want to back up VMs. For a list of supported vSphere platforms, see the vSphere Agent release notes.

The following procedure describes how to deploy the OVA file using one version of the vSphere Client. The procedure can vary depending on the vSphere version.

You can also deploy the OVA file using the VMware OVF Tool or the vSphere Web Client. For more information, see documentation from VMware.

To deploy the OVA file using the vSphere Web Client, you must first install the Client Integration Plug-in on the machine that you are using. When searching for the file to deploy, make sure that the filter includes OVA files; by default, the wizard shows OVF files only.

To deploy the vSphere Agent:

1. Log in to the vCenter using the vSphere Client.
2. From the **File** menu, select **Deploy OVF Template**.

   The **Deploy OVF Template** wizard begins with the **Source** screen.
3. Enter the location of the vSphere Agent OVA file, or browse to it.
4. Click **Next**.

   The **OVF Template Details** screen shows vSphere Agent information.
5. Review the information. Click **Next**.

The **End User License Agreement** screen **appears**.

6. Review the license agreement, click **Accept**, and then click **Next**.

   The **Name and Location** screen **appears**.

7. In the **Name** field, enter a name for the vSphere Agent VM.

8. In the Inventory Location tree, specify the location for deploying the Agent. Click **Next**.

   The **Host/Cluster** screen **appears**.

9. Select the host or cluster for running the vSphere Agent. Click **Next**.

   The **Storage** screen **appears**.

10. Select the storage location for the vSphere Agent files. Click **Next**.

    The **Disk Format** screen **appears**.

11. Select one of the following formats for the Agent's virtual disks:

    - Thick Provision Lazy Zeroed
    - Thick Provision Eager Zeroed
    - Thin Provision

    The default format is "Thick Provision Lazy-Zeroed".

12. Click **Next**.

    The **Ready to Complete** screen **appears**.

13. Review the deployment settings. Click **Finish**.

    Deployment begins and its progress is shown.

14. When the deployment finishes, power on the vSphere Agent.

    To view the startup process, open the vSphere Agent console.

2.2 Configuring Network Settings for the vSphere Agent

After deploying the vSphere Agent, configure network settings, including the Agent host name, IP address, and default gateways.

Optionally, you can set up DNS servers and change the IP address assignment method. By default, the Agent is configured to use Dynamic Host Configuration Protocol (DHCP).

You can configure network settings for the vSphere Agent using the Agent's Setup interface. For more information, see the *vSphere Agent User Guide*.

2.3 Adding Static Entries on the vSphere Agent for the vCenter and ESX(i) Servers

When you back up VMs or restore data using the vSphere Agent, the vCenter sends ESX and ESXi server host names to the Agent. If the vCenter provides a host name to the Agent and the Agent cannot resolve the host name, connections fail and “Host address lookup” errors occur.

If you are not using a DNS server, ensure that the vSphere Agent can resolve host names by adding a static entry on the Agent for the vCenter and each ESX/ESXi server.

To add a static entry, enter the following command in the Agent CLI:

```
net hosts add <ipaddress> <hostname>
```

Where <*ipaddress*> is the IP address that is mapped to the <*hostname*>.

2.4 Setting the vSphere Agent Time Zone

To ensure that backup logs show the correct time and to prevent problems when the Agent communicates with other servers, you must set the correct vSphere Agent time zone. The vSphere Agent time zone is set to Pacific time by default.

To set the time zone, enter the following command in the Agent CLI:

```
config set timezone <region>/<timezone>
```

Where:

- <*region*> is the region associated with the timezone. Available values are: Africa, America, Antarctica, Arctic, Asia, Atlantic, Australia, Brazil, Canada, Chile, Europe, Indian, Mexico, Mideast, Pacific, and US.
- <*timezone*> is the time zone for the vSphere Agent. To show a list of available time zones in a region, use the following command:

  ```
  config show timezones list <region>
  ```

<*region*>/<*timezone*> combinations include: America/New_York, Europe/Paris, and US/Pacific.

For example, to set the time zone to US Eastern time, use this command:

```
config set timezone US/Eastern
```

2.5 Registering the vSphere Agent with vCenter Server

Before you can back up VMs using the vSphere Agent, you must register the Agent with the vCenter Server where you want to back up VMs. You cannot connect to the vSphere Agent using Portal, Web Agent Console or Windows Agent Console before you register the Agent with vCenter Server.

To register the Agent with the vCenter Server, enter the following command in the Agent CLI:

```
vcenter register [<vCenter> [<backupUsername>]]
```

Where:

- <*vCenter*> is the name or IP address of the vCenter where you are registering the vSphere Agent
- <*backupUsername*> is the name of the user for performing backups and restores. You must use a vCenter or domain user account that is mapped to a vCenter role with full administrator permissions.

If you do not include the <*vCenter*> or <*backupUsername*> in the command, you are prompted for the information. You are also prompted for the password for the specified user.

You are prompted for the following information when you run the command:

- Communication port. Port used by the vCenter to listen for connections from the vSphere Client, the vSphere Web Access Client, and other SDK clients. To specify the default port (443) when prompted for the communication port, press Enter.
- Data port. Port used by the vCenter to send data to managed hosts. To specify the default port (902) when prompted for the data port, press Enter.
- User password. Password for the *backupUserName*.

2.6 Adding the vSphere Agent in Portal or Web Agent Console

To manage the vSphere Agent through Portal or Web Agent Console, register the Agent with Portal or Web Agent Console using the CLI. You can then configure the vSphere Agent.

2.6.1 Registering the vSphere Agent with Portal or Web Agent Console

To register the vSphere Agent with Portal or Web Agent Console, enter the following command in the Agent CLI:

```
webcc register [<WebCCAddress>] [<port>] [<login>]
[<password>]
```

Where:

- *<WebCCAddress>* is the Portal or Web Agent Console IP address or host name.
- *<port>* is the port used to communicate with Portal or Web Agent Console. The default port is 8086.
- *<login>* is the username for logging in to Portal or Web Agent Console.
- *<password>* is the password for logging in to Portal or Web Agent Console.

If you do not include the *<WebCCAddress>*, *<port>, <login>* or *<password>* parameter in the command, you are prompted for the information.

When the registration is complete, a "Registration complete. Agent restarted successfully" message appears.

2.6.2 Configuring the vSphere Agent in Portal

To configure a vSphere Agent in Portal, you must enter vault settings and vCenter credentials.

To configure the vSphere Agent in Portal:

1. In Portal, on the navigation bar, click **Computers**.

   The Computers page shows registered computers and environments.

2. Find the unconfigured vSphere Agent, and expand its view by clicking its row.
3. Do one of the following:
   - To enter vault settings manually, click **Configure Manually**. On the **Vault Settings** tab, click **Add Vault**. In the **Vault Settings** dialog box, enter vault information and credentials, and then click **Save**.
   - To automatically assign the first available vault settings to the Agent, click **Auto Configure**.

     If the vault settings are assigned successfully, a message appears. Click **Go to Agent**.

     If the vault settings are not valid, the automatic configuration fails. If this happens, click **Go To Agent**. On the **Vault Settings** tab, click **Add Vault**. In the **Vault Settings** dialog box, enter vault information and credentials, and then click **Save**.
4. On the **vCenter Settings** tab, enter the vCenter credentials that you used to register the vSphere Agent with vCenter Server. See Registering the vSphere Agent with vCenter Server.
5. Click **Test vCenter Connection**. If the credentials are valid, a **Success** message appears. Click **Okay**.

6. Click **Save**. A **Success** message appears. Click **Okay**.

   To finish configuring the Agent, create a backup job.

2.6.3 Configuring the vSphere Agent in Web Agent Console

When you register the vSphere Agent with Web Agent Console, Web Agent Console obtains vCenter credentials from the Agent. You can test and change the credentials and create a backup job through one wizard in Web Agent Console, as described in the following procedure.

You can also change Agent credentials and settings using the Agent Settings screen.

To configure the vSphere Agent in Web Agent Console:

1. In Web Agent Console, select the unconfigured vSphere Agent.
2. Click **This is a new Agent I would like to configure** in the lower pane of the screen.

   The **Configure Agent** wizard starts with the **Agent Configuration** screen.
3. In the **Agent Description** field, enter a description for the Agent.
4. Click **Next**.

   Web Agent Console tests the vCenter credentials from the Agent.
5. If the vCenter credentials obtained from the Agent are invalid, a “Test Credentials Failed” message appears. Click **Close**.

   The **Job Type Selection** screen appears.

   The **Backup Source Type** is always VMware vSphere. This is the only available selection because the vSphere Agent only supports backup and recovery in VMware vSphere environments.

   vCenter credentials appear in the User Name and Password fields. These credentials are obtained from the vSphere Agent.

   If the vCenter credentials are valid, the User Name and Password fields cannot be edited.
6. If the vCenter credentials are not valid, the **User Name** and **Password** fields can be edited. Enter vCenter credentials in the fields, and then click **Test**.

   If the new credentials are valid, a “Success” message appears. Click **Close**.

   If the new credentials are not valid, an “Error” message appears. Click **Close**, and then enter new vCenter credentials.

Note: A Windows domain account is used to register the vSphere Agent with vCenter Server. If the password or domain credentials change, you need to make the same changes on the vSphere Agent (using the vcenter change login command) and in Web Agent Console (on the vCenter tab in the Agent Settings screen).

7. Click **Next**.
8. On subsequent wizard pages, configure a backup job by entering a job name, adding VMs, and changing encryption and other backup options.

2.7 Adding the vSphere Agent in Windows Agent Console

To manage the vSphere Agent through Windows Agent Console, add the Agent in Windows Agent Console.

To add the vSphere Agent in Windows Agent Console:

1. In Windows Agent Console, right-click the Workspace icon and choose **New Agent** from the menu.

   The **Agent Properties** screen appears.

2. In the **Description** field, enter an Agent name.
3. In the **Network address** field, enter the IP address or host name of the vSphere Agent.
4. In the **User name** and **Password** fields, provide the vCenter credentials that you used to register the vSphere Agent with vCenter Server. See Registering the vSphere Agent with vCenter Server.

   The vCenter credentials allow Windows Agent Console to access the vSphere Agent.

5. Check the Agent connection settings by clicking **Get Status**.

   If the settings are correct, the **Agent Status** screen shows Agent information. Click **OK**.

   If the IP address or host name information is incorrect, a “Failed to connect to <...>” message appears. Enter a new IP address or host name.

   If the authorization information is incorrect, a “Failed to authorize user () or user () possesses insufficient privilege” message appears. Enter a new user name or password.

   Note: A Windows domain account is used to register the vSphere Agent with vCenter Server. If the password or domain credentials change, you need to make the same changes on the vSphere Agent (using the vcenter change login command) and in Windows Agent Console (on the vCenter tab in the Agent Configuration screen).

6. Click **OK**.

   The new Agent appears in the left pane of Windows Agent Console.

2.8 Changing the CBT Setting

Changed Block Tracking (CBT) is a VMware feature that tracks changed disk sectors and improves the performance of VM backups. By default, the vSphere Agent enables Changed Block Tracking (CBT) for VMs.

However, because CBT requires some virtual disk processing overhead, you can stop the Agent from enabling CBT for VMs. This does not disable CBT for VMs that already have it enabled through the Agent or another mechanism. It only stops the Agent from enabling CBT in the future for VMs that do not already have it enabled.

2.8.1 Changing the CBT Setting using Portal

To change the CBT setting using Portal:

1. In Portal, on the navigation bar, click **Computers**.

   The Computers page shows registered computers and environments.

2. Find the vSphere Agent, and expand its view by clicking its row.
3. Click the **vCenter Settings** tab.
4. Do one of the following:
   - To allow the Agent to enable CBT for VMs, select **Enable Change Block Tracking (CBT) for Virtual Machines during backup**.
   - To stop the Agent from enabling CBT for VMs, clear **Enable Change Block Tracking (CBT) for Virtual Machines during backup**.

     Note: Clearing this check box does not disable CBT for VMs that already have it enabled through our software or through another mechanism. It only stops the Agent from enabling CBT for VMs in the future.

5. Click **Save**. A **Success** message appears. Click **Okay**.

2.8.2 Changing the CBT Setting using Web Agent Console

To change the CBT setting using Web Agent Console:

1. In Web Agent Console, select the vSphere Agent.
2. Point to the **Edit** button and choose **Agent Settings** from the menu.

   The **Agent Settings** screen appears.
3. Click the **vCenter** tab.
4. Choose one of the following CBT settings:
   - To allow the Agent to enable CBT for VMs, select **Enable Changed Block Tracking (CBT) for Virtual Machines**.

     The CBT option is selected by default.
   - To stop the Agent from enabling CBT for VMs, clear **Enable Changed Block Tracking (CBT) for Virtual Machines**.

     Note: Clearing this option does not disable CBT for VMs that already have it enabled through our software or through another mechanism. It only stops the Agent from enabling CBT for VMs in the future.
5. Click **OK**.

2.8.3 Changing the CBT Setting using Windows Agent Console

To change the CBT setting using Windows Agent Console:

1. In Windows Agent Console, right-click the Agent and choose **Agent Configuration** from the menu.

   The **Agent Configuration** screen opens.
2. Click the **vCenter** tab.
3. Choose one of the following CBT settings:
   - To allow the Agent to enable CBT for VMs, select the **Change Block Tracking** option.

     The **Change Block Tracking** option is selected by default.
   - To stop the Agent from enabling CBT for VMs, clear the **Change Block Tracking** option.

     Note: Clearing this option does not disable CBT for VMs that already have it enabled through the Agent or through another mechanism. It only stops the

Agent from enabling CBT in the future for VMs that do not already have it enabled.

4. Click **OK**.

3 Creating a Backup Job

After the vSphere Agent is deployed and configured, you can create a backup job. You can create a backup job using Portal, Web Agent Console or Windows Agent Console.

On a standalone host that is running ESXi 5.5, or in a cluster where all hosts are running ESXi 5.5, the vSphere Agent can back up and restore VMs with VMDKs that are as large as 2 TB.

On a standalone host that is running ESXi 5.1 or a previous ESX version, or in a cluster where one or more hosts are running ESXi 5.1 or a previous ESX version, the vSphere Agent backs up VMs with VMDKs that are as large as 2032 GB.

3.1 Creating a Backup Job using Portal

To create a backup job:

1. On the navigation bar, click **Computers**.

   The Computers page shows registered computers and environments.
2. Click the vSphere Agent row. 
3. Click the **Jobs** tab.
4. In the Select Job Task list, click **Create New VMware vCenter Job**.
5. If the **Connect to vCenter** dialog box appears, specify the following information in the dialog box:

   - In the **User Name** box, type the Windows domain account user name used to authenticate the vSphere Agent with the vCenter server.
   - In the **Password** box, type the password for the specified user.
   - In the **Domain** box, type the domain of the specified user account. The domain is optional if you specified the domain in the **User Name** box (e.g., domain\username).

   Note: The **Connect to vCenter** dialog box only appears if vCenter settings have not been entered for the vSphere Agent in Portal. vCenter settings entered in this dialog box are populated on the Agent's **vCenter Settings** tab.
6. In the **Create New Job** dialog box, specify the following information:

   - In the **Name** box, type a name for the backup job.
   - In the **Description** box, optionally type a description for the backup job.
   - In the **Destination** list, select the vault where you want to save the backup data.

- In the **Log File Options** list, select the level of detail for job logging.
- In the **Encryption Settings** list, select the encryption method for storing the backup data. Select **None** if you do not want to encrypt the stored data.

  Note: Only the strongest available encryption type is available for jobs created using vSphere Agent 7.3. Jobs created using previous vSphere Agent versions continue to run with their existing encryption types. However, if you change the encryption type for an existing job, you can only select the strongest available encryption type.

- If the backup data will be encrypted, enter an encryption password in the **Password** and **Confirm Password** boxes. You can also enter a password hint in the **Password Hint** box.

  Warning: You must remember the encryption password to recover files. *If you lose the password, you lose access to the data.* The password is not maintained anywhere else.

7. In the **Include in Backup** box, do one of the following:
   - To include all VMs in the vCenter in the backup job, select the **Virtual Machines** check box.
   - To include specific VMs in the backup job, select the check box for each VM that you want to back up.
   - To include VMs with specific names in the backup job, select the **Virtual Machines** check box, and then select the **Filter VMs** check box. In the **Filter VMs** box, enter the names of VMs to include in the backup. Separate multiple VM names with commas, and use asterisks (*) as wildcard characters. For example, to include VMs in the backup job if their names start with “Win” or end with “production”, enter the following filter: Win*,*production
8. Click **Create Job**.

   The job is created, and the **View/Add Schedule** dialog box appears. Now you can create a schedule for running the backup. Click **Cancel** if you do not want to create a schedule at this time.

3.2 Creating a Backup Job using Web Agent Console

To create a backup job using Web Agent Console:

1. In Web Agent Console, select a vSphere Agent, and choose **Add > Job**.

   The New Job wizard opens to the **Job Type Selection** page.

2. In the **Job Name** field, type a name for the job.

3. In the **Job Description** field, type a job description.

   Note: The **Backup source type** is always **VMware vSphere**. This is the only available selection because the vSphere Agent only supports backup and recovery in VMware vSphere environments.

4. Click **Next**.

   The **Selection** page appears.

5. To add VMs to the backup job, in the vSphere pane, do one or more of the following:

   - To select specific VMs to back up, expand the Virtual Machines list, select the check box for each VM you want to back up, and then click **Include**.
   - To back up all VMs (including VMs that are added after the backup job is created), select the **Virtual Machines** check box, and then click **Include**. The **Include Options** screen opens. Select **Include all virtual machines**, and then click **OK**.
   - To select VMs to back up by applying filter criteria when the backup runs, select the Virtual Machines check box, and then click **Include**. The **Include Options** screen opens. Select **Include only virtual machines with names matching this filter**. In the field, enter a filter for selecting VM names, and then click **OK**.

     You can include the following wildcard characters in the filter:

     * (asterisk) - signifies a wildcard string up to the next separator character

     ? (question mark) - signifies a single wildcard character

     For example, to back up all VMs with names that start with “vm”, type `vm*`.

     Note: You can enter only one filter in the field. To apply several filters, use the **Include Options** screen several times.

   VM names and filters that you include in the backup job appear with green plus signs (+) in the Backup Set pane.

6. To exclude VMs from the backup job, do one or more of the following:

   - To exclude specific VMs from the backup, expand the **Virtual Machines** list, select the check box for each VM you want to exclude, and then click **Exclude**.
   - To exclude VMs by applying filter criteria when the backup runs, select the Virtual Machines check box, and then click **Exclude**. The **Exclude Options** screen appears. Select **Exclude only virtual machines with names matching this filter**. In the field, enter a filter for selecting VM names, and then click **OK**.

     You can include the following wildcards in the filter:

     * (asterisk) - signifies a wildcard string up to the next separator character

     ? (question mark) - signifies a single wildcard character

Note: You can enter only one filter in the field. To apply several filters, use the Exclude Options screen several times.

VM names and filters that you exclude from the backup job appear with red minus signs (-) in the Backup Set pane.

7. Click **Next**.

   The **Options** screen appears.

8. From the **Encryption type** list, select the type of encryption for the backup data. If you encrypt the data, enter an encryption password in the **Password** and **Verify Password** fields. The password is case-sensitive. In the **Password Hint** field, enter a password hint to help you remember the encryption password during a restore.

   Warning: You must remember the encryption password to recover files. *If you lose your password, you lose access to your data!* The password is not maintained anywhere else.

9. To set retention, compression or logging options, click **Advanced Backup Options**. The **Advanced Options** screen opens.

   From the **Retention** list, choose a retention scheme that specifies the number of days for keeping backups, number of backups to store online, and days to archive the data.

   From the **Compression** list, choose the level of data compression. Data compression allows you to optimize the volume of data sent against the speed of transmission.

   To generate log files for the job, select **Create log file**. From the **Log detail level** list, choose the level of log detail. To automatically delete log files when a backup is deleted, select **Automatically purge expired log files**. To delete the oldest log file after reaching a certain number of log files, enter a number in the **Keep the last *x* log files** field.

   Click **OK**.

10. Click **Next**.

    The **Schedule** screen appears.

11. To create a backup schedule and set retention options for the scheduled job, click **Add**. The **Schedule Details** page opens. From the **Schedule View** list, choose **Days of Week**, **Days of Month**, or **Custom**, and specify when to run the backup.

    From the **Retention Scheme** menu, choose a retention scheme that specifies the number of days for keeping backups from the scheduled job, number of backups to store online, and days to archive the data.

To specify data compression and deferral options, click **Advanced Schedule Options**. From the **Compress file data** list, choose the file compression level. To allow the backup job to run without a time limit, clear **Use Deferring**. To specify a maximum amount of time that the backup job can run, select **Use Deferring**. In the **Backup Time Window** fields, specify the number of hours or minutes that the job can run. The backup job stops after the specified amount of time even if some VMs in the job have not been backed up. When the job runs again, the vSphere Agent first checks for changes in VMs that were previously backed up, and then backs up remaining VMs. Click **OK** to close the **Advanced Options** page.

Click **OK** to close the **Schedule Details** page.

Note: You can add multiple schedules for the backup job.

12. Click **Next**.

    The **Destination** screen appears.

13. Select the vault for saving the backup data. To add a new vault, click **Add**.
14. Click **Save Changes**.

3.3 Creating a Backup Job using Windows Agent Console

To create a backup job using Windows Agent Console:

1. In Windows Agent Console, do one of the following:
   - Select a vSphere Agent, and choose **File > New Job**.
   - Right-click the Agent, and choose **New Job**.

   The New Job Wizard opens to the **Welcome** page.

   Note: If the **Skip this screen in the future** option is selected, the **Welcome** page does not appear.

2. Click **Next**.

   The **Backup Source Type** page appears. The Backup source type is always VMware vSphere. This is the only available selection because the vSphere Agent only supports backup and recovery in VMware vSphere environments.

3. Click **Next**.

   The **Vault** page appears.

4. Select a vault from the **Destination** menu, or click **New** to create a new vault destination.

Note: To add a new vault, please refer to the *Windows Agent Console Operations Guide* or Windows Agent Console Help.

5. Click **Next**.

   The **New Job Name** page appears.

6. In the **Name** field, type a name for the job.

7. In the **Description** field, type a job description.

8. Click **Next**.

   The **Source** page appears.

9. Click **Add**.

   The **Include/Exclude** screen appears, allowing you to choose which VMs to back up and which to exclude from the backup.

10. To add VMs to the backup job, do one or more of the following:

    - To select specific VMs to back up, expand the **Virtual Machines** list. Select each VM you want to back up, and then click **Include**. The names of VMs you include appear in the **Virtual Machine** pane. You can include more than one VM in your backup.
    - To back up all VMs (including VMs that are added after the backup job is created), select **Virtual Machines**, and then click **Include**. The **Confirm VMs to Include** screen appears. Select the **Include all virtual machines** option, and then click **Yes**.
    - To select VMs to back up by applying filter criteria when the backup runs, select **Virtual Machines**, and then click **Include**. The **Confirm VMs to Include** screen appears. Select **Include only virtual machines with names matching this filter**. In the field, enter a filter for selecting VM names, and then click **Yes**.

      You can include the following wildcards in the filter:

      * (asterisk) - signifies a wildcard string up to the next separator character

      ? (question mark) - signifies a single wildcard character

      For example, to include all VMs with names that start with “vm”, type `vm*` and then click **Yes**.

11. To exclude VMs from the backup job, do one or more of the following:

    - To exclude specific VMs from the backup, expand the **Virtual Machines** tree. Select each VM you want to exclude, and then click **Exclude**.
    - To exclude VMs by applying filter criteria when the backup runs, select **Virtual Machines**, and then click **Exclude**. The **Confirm VMs to Exclude** screen appears.

Select **Exclude only virtual machines with names matching this filter**. In the field, enter a filter for selecting VM names, and then click **Yes**.

12. Click **OK**.

    VM names and filters that you include in the backup job appear in the Virtual Machine pane of the **Source** page.

13. Click **Next**.

    The **Options** page appears.

14. Choose one of the following deferral options:

    - To allow the backup job to run without a time limit, select **Disable Deferring**.
    - To specify a maximum amount of time that the backup job can run, clear **Disable deferring** and specify the number of hours or minutes that the job can run. The backup job stops after the specified amount of time even if some VMs in the job have not been backed up. When the job runs again, the vSphere Agent first checks for changes in VMs that were previously backed up, and then backs up remaining VMs.

15. Click **Next**.

    The **Encryption** page appears.

16. From the **Encryption type** list, select the type of encryption for the backup data. If you encrypt the data, enter an encryption password in the **Password** and **Verify password** fields. The password is case-sensitive. In the **Password Hint** field, enter a password hint to help you remember the encryption password during a restore.

    Warning: You must remember the encryption password to recover files. *If you lose your password, you lose access to your data!* The password is not maintained anywhere else.

17. Click **Next**.

    The **Log Options** page appears.

18. Specify one of the following logging options:

    - To generate log files for the job, select **Create log file**. From the **Log detail level** list, choose the level of log detail. To automatically delete log files when a backup is deleted, select **Automatically purge expired log files**. To delete the oldest log file after reaching a certain number of log files, enter a number in the **Keep the last *x* log files** field.
    - To not generate log files for the job, clear **Create log file**.

19. Click **Next**.

    The **Finished** page appears.

20. Select one of the following options for running the job, and then click **Finish**:
    - Run the job immediately
    - Schedule the job
    - Just exit from this wizard