Deploy BlueXP backup and recovery for VMs

BlueXP backup and recovery for VMs

NetApp
June 10, 2024

Table of Contents

Deploy BlueXP backup and recovery for VMs

Requirements and considerations

You need to be aware of several requirements and considerations before using BlueXP backup and recovery for VMs:

- BlueXP backup and recovery for VMs is deployed as a Linux VM regardless of whether you use the plug-in to protect data on Windows systems or Linux systems.
- You should deploy BlueXP backup and recovery for VMs on VMC on AWS.

  BlueXP backup and recovery for VMs and VMC should use the same timezone. Backup schedules are executed in the time zone in which BlueXP backup and recovery for VMs is deployed. VMC reports data in the time zone in which the VMC is located. Therefore, if BlueXP backup and recovery for VMs and VMC are in different time zones, data in BlueXP backup and recovery for VMs Dashboard might not be the same as the data in the reports.

- You must not deploy BlueXP backup and recovery for VMs in a folder that has a name with special characters.

  The folder name should not contain the following special characters: $!@#%^&()_+{}';.,*?"<>|

- You must deploy and register a separate, unique instance of BlueXP backup and recovery for VMs for each VMC on AWS.
  - Each VMC on AWS should be paired with a separate instance of BlueXP Backup and Recovery for VMs.
  - Each instance of BlueXP backup and recovery for VMs must be deployed as a separate Linux VM.

    For example, if you want to perform backups from six different instances of VMC on AWS, then you must deploy six BlueXP backup and recovery for VMs instances on six hosts and each VMC on AWS must be paired with a unique instance of BlueXP backup and recovery for VMs.

- On the vmc.vmware.com console, open the firewall ports to allow the compute gateway public IP to communicate over TCP 443 with the vCenter on the management network.
- On the AWS console, you must update the security group of the VPC where FSx for ONTAP is running to allow BlueXP backup and recovery for VMs access FSx for ONTAP.

Download the Open Virtual Appliance

Download the Open Virtual Appliance (OVA) in VMware vCenter 8.0 and above to deploy BlueXP backup and recovery for VMs.

Before you begin

If the OVA signed by the Entrust certificate is not trusted, ensure to install and add intermediate certificates to the vCenter.

Steps

1. To download BlueXP backup and recovery for VMs OVA:
   a. Log in to the NetApp Support Site

b. From the list of products, select **BlueXP backup and recovery for VMs**, then click the **Download Latest Release** button.

c. Download the BlueXP backup and recovery for VMs `.tar` file to any location.

2. Extract the contents of the tar file. The tar file contains the OVA and certs folder. The certs folder contains Intermediate certificates.
3. In vSphere client, navigate to **Administration > Certificates > Certificate Management**.
4. Next to **Trusted Root certificates**, click **Add**.

   By default, the root certificate is installed.

   a. Go to the certs folder.

   b. Select the Intermediate certificates.

   c. Install each certificate one at a time.
5. The certificates are added to a panel under Trusted Root Certificates.

Once the certificates are installed, OVA can be verified and deployed.

If the downloaded OVA is not tampered, then the Publisher column displays Trusted certificate.

Deploy BlueXP backup and recovery for VMs

To protect VMs and datastores on virtualized machines, you must deploy BlueXP backup and recovery for VMs.

Before you begin

The OVA deployment is supported in VMware vCenter 8.0 and above.

- You must have read the deployment requirements.
- You must be running a supported version of VMC on AWS.
- You must have configured and set up your VMC on AWS environment.
- You must have set up an ESXi host for BlueXP backup and recovery for VMs.
- You must have downloaded BlueXP backup and recovery for VMs `.tar` file.
- You must have the login authentication details for your VMC on AWS instance.
- You must have a certificate with valid Public and Private Key files. For more information, see articles under Storage Certificate Management section.
- You must have logged out of and closed all browser sessions of vSphere client and deleted the browser cache to avoid any browser cache issue during the deployment of BlueXP backup and recovery for VMs.
- You must have enabled Transport Layer Security (TLS) in vCenter. Refer to the VMware documentation.
- You must have deployed BlueXP backup and recovery for VMs in the same time zone as the vCenter.

Steps

1. For VMware vCenter 7.0.3 and later versions, follow the steps in Download the Open Virtual Appliance (OVA) section to import the certificates to vCenter.
2. In your browser, navigate to VMware vSphere vCenter.
3. Log in to the **VMware vCenter Single Sign-On page**.
4. On the Navigator pane, right-click any inventory object that is a valid parent object of a virtual machine, such as a datacenter, cluster, or host, and select **Deploy OVF Template** to start the VMware deploy wizard.
5. Extract the `.tar` file, which contains the `.ova` file onto your local system. On the **Select an OVF template** page, specify the location of the `.ova` file inside the `.tar` extracted folder.
6. Click **Next**.
7. On the **Select a name and folder** page, enter a unique name for the VM or vApp, and select a deployment location, and then click **Next**.

   This step specifies where to import the `.ova` file into vCenter. The default name for the VM is the same as the name of the selected `.ova` file. If you change the default name, choose a name that is unique within each VMC on AWS VM folder.

   The default deployment location for the VM is the inventory object where you started the wizard.
8. On the **Select a resource** page, select the resource where you want to run the deployed VM template, and click **Next**.
9. On the **Review details** page, verify the `.ova` template details and click **Next**.
10. On the **License agreements** page, select the checkbox for **I accept all license agreements**.
11. On the **Select storage** page, define where and how to store the files for the deployed OVF template.
    a. Select the disk format for the VMDKs.
    b. Select a VM Storage Policy.

       This option is available only if storage policies are enabled on the destination resource.

    c. Select a datastore to store the deployed OVA template.

       The configuration file and virtual disk files are stored on the datastore.

       Select a datastore large enough to accommodate the virtual machine or vApp and all associated virtual disk files.
12. On the **Select networks** page, do the following:
    a. Select a source network and map it to a destination network.

       The Source Network column lists all networks that are defined in the OVA template.

    b. In the **IP Allocation Settings** section, select the required IP protocol and then click **Next**.

       BlueXP backup and recovery for VMs supports one network interface. If you need multiple network adapters, you must set that up manually.
13. On the **Customize template** page, do the following:
    a. In the **Register to existing vCenter** section, enter the vCenter name and the vCenter credentials of the virtual appliance.

In the **vCenter username** field, enter the username in the format domain\username.

b. In the **Create BlueXP backup and recovery for VMs credentials** section, enter the local credentials.

In the **Username** field, enter the local username; do not include the domain details.

> Make a note of the username and password that you specify. You need to use these credentials if you want to modify BlueXP backup and recovery for VMs configuration later.

c. Enter credentials for the maint user.

d. In **Setup Network Properties**, enter the host name.

i. In **Setup IPv4 Network Properties** section, enter the network information such as IPv4 address, IPv4 Netmask, IPv4 Gateway, IPv4 Primary DNS, IPv4 Secondary DNS, and IPv4 Search Domains.

> You can skip these steps and leave the entries blank in the Setup Network Properties section, if you want to proceed with DHCP as your network configuration.

e. In **Setup Date and Time**, select the time zone where the vCenter is located.

14. On the **Ready to complete** page, review the page and click **Finish**.

All hosts must be configured with IP addresses (FQDN hostnames are not supported). The deploy operation does not validate your input before deploying.

You can view the progress of the deployment from the Recent Tasks window while you wait for the OVF import and deployment tasks to finish.

When BlueXP backup and recovery for VMs is successfully deployed, it is deployed as a Linux VM, registered with vCenter, and a VMware vSphere client is installed.

15. Navigate to the VM where BlueXP backup and recovery for VMs was deployed, then click the **Summary** tab, and then click the **Power On** box to start the virtual appliance.

16. While BlueXP backup and recovery for VMs is powering on, right-click the deployed BlueXP backup and recovery for VMs, select **Guest OS**, and then click **Install VMware tools**.

Copyright information

Trademark information