# Table of contents

1. About Cyber Disaster Recovery Cloud ................................................................. 3
2. Software requirements ......................................................................................... 4
3. Setting up the disaster recovery functionality .................................................... 6
4. Setting up connectivity ......................................................................................... 7
   4.1 Networking concepts ..................................................................................... 7
      4.1.1 Site-to-site connection ....................................................................... 7
      4.1.2 Without site-to-site connection ......................................................... 12
      4.1.3 Point-to-site connection .................................................................. 12
   4.2 Initial connectivity configuration .................................................................... 13
      4.2.1 Site-to-site connection ....................................................................... 13
      4.2.2 Without site-to-site connection ......................................................... 15
      4.2.3 Point-to-site connection .................................................................. 16
   4.3 Network management .................................................................................... 17
      4.3.1 Managing networks ......................................................................... 18
      4.3.2 Managing the VPN appliance settings .......................................... 20
      4.3.3 Disabling and enabling site-to-site connection .................................. 20
      4.3.4 Managing point-to-site connection settings .................................. 21
      4.3.5 Configuring local routing ................................................................. 22
5. Setting up recovery servers ................................................................................ 23
   5.1 How failover and failback work ................................................................... 23
   5.2 Recovery server lifecycle ............................................................................. 24
   5.3 Creating a recovery server .......................................................................... 25
   5.4 Performing a test failover ........................................................................... 27
   5.5 Performing a failover .................................................................................. 28
   5.6 Performing a failback .................................................................................. 30
   5.7 Working with encrypted backups .................................................................. 31
6. Setting up primary servers ................................................................................ 32
   6.1 Creating a primary server ............................................................................ 32
   6.2 Operations with a primary server ............................................................... 33
7. Managing the cloud servers ............................................................................... 34
8. Backing up the cloud servers ............................................................................ 35
9. Orchestration (runbooks) .................................................................................. 36
   9.1 Creating a runbook .................................................................................... 36
   9.2 Operations with runbooks .......................................................................... 37
10. Glossary ............................................................................................................ 39
1 About Cyber Disaster Recovery Cloud

**Cyber Disaster Recovery Cloud (DR)** – a part of Files Cloud that provides disaster recovery as a service (DRaaS) oriented mostly on the SMB clients. Cyber Disaster Recovery Cloud provides you with a fast and stable solution to launch the exact copies of your machines on the cloud site and switch the workload from the corrupted original machines to the recovery servers in the cloud in case of a man-made or a natural disaster.

**The key functionality**
- Manage the Cyber Disaster Recovery Cloud service from a single console
- Extend up to five local networks to the cloud, by using a secure VPN tunnel
- Establish the connection to the cloud site without any VPN appliance (p. 41) deployment
- Protect your machines by using recovery servers in the cloud
- Protect applications and appliances by using primary servers in the cloud
- Perform automatic disaster recovery operations for encrypted backups
- Perform a test failover in the isolated network
2 Software requirements

Supported operating systems
Protection with a recovery server has been tested for the following operating systems:

- CentOS 6.6, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
- Debian 9
- Ubuntu 16.04, 18.04
- Windows Server 2008/2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – all installation options, except for Nano Server
- Windows Server 2019 – all installation options, except for Nano Server

Windows desktop operating systems are not supported due to Microsoft product terms. The software may work with other Windows operating systems and Linux distributions, but this is not guaranteed.

Supported virtualization platforms
Protection of virtual machines with a recovery server has been tested for the following virtualization platforms:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 with Hyper-V
- Windows Server 2012/2012 R2 with Hyper-V
- Microsoft Hyper-V Server 2012/2012 R2
- Windows Server 2016 with Hyper-V – all installation options, except for Nano Server
- Windows Server 2019 with Hyper-V – all installation options, except for Nano Server
- Microsoft Hyper-V Server 2016
- Kernel-based Virtual Machines (KVM)
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

The VPN appliance has been tested for the following virtualization platforms:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 with Hyper-V
- Windows Server 2012/2012 R2 with Hyper-V
- Microsoft Hyper-V Server 2012/2012 R2
- Windows Server 2016 with Hyper-V – all installation options, except for Nano Server
- Windows Server 2019 with Hyper-V – all installation options, except for Nano Server
- Microsoft Hyper-V Server 2016

The software may work with other virtualization platforms and versions, but this is not guaranteed.
Limitations

The following platforms and configurations are not supported in Cyber Disaster Recovery Cloud:

1. Unsupported platforms:
   - Agents for Virtuozzo
   - MacOS

2. Unsupported configurations:
   Microsoft Windows:
   - Dynamic disks are not supported
   - Windows desktop operating systems are not supported (due to Microsoft product terms)
   - Active Directory service with FRS replication is not supported
   - Removable media without either GPT or MBR formatting (so-called "superfloppy") are not supported

   Linux:
   - Linux machines that have logical volumes (LVM) or volumes formatted with the XFS file system
   - File system without a partition table

3. Unsupported backup types:
   - Continuous data protection (CDP) recovery points are incompatible.

   Important If you create a recovery server from a backup having a CDP recovery point, then during the failback or creating backup of a recovery server, you will loose the data contained in the CDP recovery point.

   - Forensic backups cannot be used for creating recovery servers.

A recovery server has one network interface. If the original machine has several network interfaces, only one is emulated.

Cloud servers are not encrypted.
3 Setting up the disaster recovery functionality

To set up the disaster recovery functionality
1. Configure the connectivity type to the cloud site:
   - Site-to-site connection (p. 13)
   OR
   - Without site-to-site connection (p. 15)
2. Create a protection plan with the backup module enabled and select the entire machine or system and boot volumes for backing up. At least one protection plan is required for creating a recovery server.
3. Apply the protection plan to the local servers to be protected.
4. Create the recovery servers (p. 25) for each of your local servers that you want to protect.
5. Perform a test failover (p. 27) to check how it works.
6. [Optional] Create the primary servers (p. 32) for application replication.

As a result, you have set up the disaster recovery functionality to protect your local servers from a disaster.

If a disaster occurs, you can failover the workload (p. 28) to the recovery servers in the cloud. At least one recovery point must be created before failing over to recovery servers. When your local site is recovered from a disaster, you can switch the workload back to your local site (p. 30).
4 Setting up connectivity

This section explains the network concepts necessary for you to understand how it all works in Cyber Disaster Recovery Cloud. You will learn how to configure different types of connectivity to the cloud site, depending on your needs. Finally, you will learn how to manage your networks in the cloud and manage the settings of the VPN appliance and connectivity gateway.

4.1 Networking concepts

The Cyber Disaster Recovery Cloud service allows you to define the connectivity type to the cloud site:

- **Site-to-site connection.**
  
  This type of connection requires a VPN appliance deployment on the local site.
  
  Your local site is connected to the cloud site by means of a secure VPN tunnel. This type of connection is suitable in case you have tightly dependent servers on the local site, such as a web server and a database server. In case of partial failover, when one of these servers is recreated on the cloud site while the other stays on the local site, they will still be able to communicate with each other via a VPN tunnel.
  
  Cloud servers on the cloud site are accessible through the local network, point-to-site VPN (p. 12), and public IP addresses (if assigned).

- **Without site-to-site connection.**
  
  This type of connection does not require a VPN appliance deployment on the local site.
  
  The local and cloud networks are independent networks. This type of connection implies either the failover of all the local site's protected servers or partial failover of independent servers that do not need to communicate with the local site.
  
  Cloud servers on the cloud site are accessible through the point-to-site VPN (p. 12), and public IP addresses (if assigned).

4.1.1 Site-to-site connection

To understand how networking works in the Cyber Disaster Recovery Cloud service, we will consider a case when you have three networks with one machine each in the local site. You are going to configure the protection from a disaster for the two networks – Network 10 and Network 20.
On the diagram below, you can see the local site where your machines are hosted and the cloud site where the cloud servers are launched in case of a disaster. The Cyber Disaster Recovery Cloud solution allows you to fail over all the workload from the corrupted machines in the local site to the cloud servers in the cloud. A maximum of five networks can be protected with the Cyber Disaster Recovery Cloud service.

To establish a site-to-site communication between the local site and the cloud site, VPN appliance and Connectivity gateway are used. First, when you start configuring the site-to-site connection in the service console, the connectivity gateway is automatically deployed in the cloud site. Then, you must deploy the VPN appliance in your local site, add the networks to be protected, and register the appliance in the cloud. The Cyber Disaster Recovery Cloud service creates a replica of your local network in the cloud. A secure VPN tunnel is established between the VPN appliance and the connectivity gateway. It provides your local network extension to the cloud. The production networks in the cloud are bridged with your local networks. The local and cloud servers can communicate via this VPN tunnel as if they are all in the same Ethernet segment. Routing is performed with your local router.

For each source machine to be protected, you must create a recovery server in the cloud site. It stays in the Standby state until a failover event happens. If a disaster happens and you start the failover process (in the production mode), the recovery server representing the exact copy of your protected machine is launched in the cloud. It may be assigned the same IP address as the source machine has and launched in the same Ethernet segment. Your clients can continue working with the server, without noticing any background changes.
You can also launch a failover process in the **test mode**. This means that the source machine is still working and at the same time the respective recovery server with the same IP address is launched in the cloud. To prevent IP address conflicts, a special virtual network is created in the cloud – **test network**. The test network is isolated to prevent duplication of the source machine IP address in one Ethernet segment. To access the recovery server in the test failover mode, you must assign the **Test IP address** to the recovery server when creating it. There are other parameters for the recovery server that can be specified, they will be considered in the respective sections below.

**Connectivity gateway**

The major component that allows communication between the local and cloud sites is the **connectivity gateway**. It is a virtual machine in the cloud on which the special software is installed, and the network is specifically configured. The connectivity gateway provides the following functions:

- Connecting the Ethernet segments of your local network and production network in the cloud in the L2 mode.
- Providing iptables and ebtables rules.
- Working as a default router and NAT for the machines in the test and production networks.
- Working as a DHCP server. All machines in the production and test networks must get the network configuration via DHCP.
- Working as a caching DNS.

**Connectivity gateway network configuration**

The connectivity gateway has several network interfaces:

- External interface, connected to the Internet
- Production interfaces, connected to the production networks
- Test interface, connected to the test network

In addition, two virtual interfaces are added for point-to-site and site-to-site connections.

When the connectivity gateway is deployed and initialized, the bridges are created – one for the external interface, and one for the client and production interfaces. Though the client-production bridge and the test interface use the same IP addresses, the connectivity gateway can route packages correctly by using a specific technique.

**VPN appliance**

The **VPN appliance** is a virtual machine in the local site with Linux and the special software installed, and the special network configuration. It allows communication between the local and cloud sites.

**Recovery servers**

A **recovery server** – a replica of the original machine based on the protected server backups stored in the cloud. Recovery servers are used for switching workloads from the original servers in case of a disaster.

When creating a recovery server, you must specify the following network parameters:

- **Cloud network** (required): a cloud network to which a recovery server will be connected.
- **IP address in production network** (required): an IP address with which a virtual machine for a recovery server will be launched. This address is used in both the production and test networks. Before launching, the virtual machine is configured for getting the IP address via DHCP.
- **Test IP address** (optional): this IP address is needed to access a recovery server from the client-production network during the test failover, to prevent the production IP address from being duplicated in the same network. This IP address is different from the IP address in the production network. Servers in the local site can reach the recovery server during the test failover via the test IP address, while access in the reverse direction is not available. Internet access from the recovery server in the test network is available if the **Internet access** option was selected during the recovery server creation.

- **Public IP address** (optional): an IP address used to access a recovery server from the Internet. If a server has no public IP address, it can be reached only from the local network.

- **Internet access** (optional): it allows a recovery server to access the Internet (in both the production and test failover cases).

**Public and test IP address**

If you assign the public IP address when creating a recovery server, it becomes available from the Internet via this IP address. When a packet comes from the Internet with the destination public IP address, the connectivity gateway remaps it to the respective production IP address by using NAT, and then sends it to the corresponding recovery server.
If you assign the test IP address when creating a recovery server, it becomes available in the test network via this IP address. When you perform the test failover, the original machine is still running while the recovery server with the same IP address is launched in the test network in the cloud. There is no IP address conflict as the test network is isolated. The recovery servers in the test network are reachable by their test IP addresses, which are remapped to the production IP addresses via NAT.

### Primary servers

A **primary server** – a virtual machine that does not have a linked machine on the local site if compared with a recovery server. Primary servers are used for protecting an application by means of replication or running various auxiliary services (such as a web server).

Typically, a primary server is used for real-time data replication across servers running crucial applications. You set up the replication by yourself, using the application's native tools. For example, Active Directory replication or SQL replication can be configured among the local servers and the primary server.

Alternatively, a primary server can be included in an AlwaysOn Availability Group (AAG) or Database Availability Group (DAG).

Both methods require a deep knowledge of the application and the administrator rights for it. A primary server constantly consumes computing resources and space on the fast disaster recovery storage. It needs maintenance on your side: monitoring the replication, installing software updates, backing up. The benefits are the minimal RPO and RTO with a minimal load on the production environment (as compared to backing up entire servers to the cloud).

Primary servers are always launched only in the production network and have the following network parameters:

- **Cloud network** (required): a cloud network to which a primary server will be connected.
- **IP address in production network** (required): an IP address that the primary server will have in the production network. By default, the first free IP address from your production network is set.
- **Public IP address** (optional): an IP address used to access a primary server from the Internet. If a server has no public IP address, it can be reached only from the local network, not via the Internet.
- **Internet access** (optional): allows a primary server to access the Internet.
4.1.2 Without site-to-site connection

This type of connection does not require a VPN appliance deployment on the local site. It implies that you have two independent networks: one on the local site, another on the cloud site. Routing is performed with the router on the DR site.

4.1.3 Point-to-site connection

In case of a disaster, when a workload is switched to the cloud site and your local network is down, you may need direct access to your cloud servers. This is possible via the point-to-site connection, a secure connection from the outside using your endpoint devices (such as computer or laptop) to the cloud site via a VPN.

Point-to-site connection can be used in both scenarios – site-to-site connection or without site-to-site connection to the cloud site.

Point-to-site configuration uses certificates to authenticate the connecting VPN client. Additionally user credentials are used for authentication. Note the following about point-to-site connection:

- The same credential is used for all users using the point-to-site connection.
- If you changed the credentials for the point-to-site connection (p. 21), you need to provide the updated credentials to all the users using the point-to-site connection to the cloud site.
- If you re-generated the OpenVPN configuration (p. 21), you need to provide the updated configuration to all of the users using the point-to-site connection to the cloud site.
4.2 Initial connectivity configuration
This section describes connectivity configuration scenarios.

4.2.1 Site-to-site connection

Requirements for the VPN appliance

System requirements
- 1 CPU
- 1 GB RAM
- 8 GB disk space

Ports
- TCP 443 (outbound) – for VPN connection
- TCP 80 (outbound) – for automatic update of the appliance (p. 20)

Ensure that your firewalls and other components of your network security system allow connections through these ports to any IP address.

Configuring site-to-site connection

The VPN appliance extends your local network to the cloud via a secure VPN tunnel. This kind of connection is often referred to as a "site-to-site" (S2S) connection.

To set up a connection via the VPN appliance

1. In the service console, go to Disaster Recovery > Connectivity, and then click Configure. The connectivity configuration wizard will open.
2. Select Site-to-site connection and click Start.
   The system starts deploying the connectivity gateway in the cloud. This will take some time. Meanwhile, you can proceed to the next step.

Note  The connectivity gateway is provided without additional charge. It will be deleted if the disaster recovery functionality is not used, i.e. no primary or recovery server is present in the cloud for seven days.
3. Click **Download and deploy**. Depending on the virtualization platform you are using, download the VPN appliance for VMware vSphere or Microsoft Hyper-V.

![VPN appliance download](image)

4. Deploy the appliance and connect it to the production networks.

   In vSphere, ensure that **Promiscuous mode** and **Forged transmits** are enabled and set to **Accept** for all virtual switches that connect the VPN appliance to the production networks. To access these settings, in vSphere Client, select the host > **Summary** > **Network**, and then select the switch > **Edit settings...** > **Security**.

   In Hyper-V, create a **Generation 1** virtual machine with 1024 MB of memory. We also recommend enabling **Dynamic Memory** for the machine. Once the machine is created, go to **Settings** > **Hardware** > **Network Adapter** > **Advanced Features** and select the **Enable MAC address spoofing** check box.

5. Power on the appliance.
6. Open the appliance console and log in with the "admin"/"admin" user name and password.
7. [Optional] Change the password.
8. [Optional] Change the network settings if needed. Define which interface will be used as the WAN for Internet connection.
9. Register the appliance in the Files Cloud service by using the credentials of the company administrator.

   These credentials are only used once to retrieve the certificate. The datacenter URL is predefined.

   **Note** If two-factor authentication is configured for your account, you will also be prompted to enter the TOTP code. If two-factor authentication is enabled but not configured for your account, you cannot register the VPN appliance. First, you must go to the service console login page and complete the two-factor authentication configuration for your account. For more details on two-factor authentication, go to the Management Portal Administrator’s Guide.
Once the configuration is complete, the appliance will have the **Online** status. The appliance connects to the connectivity gateway and starts to report information about networks from all active interfaces to the Cyber Disaster Recovery Cloud service. The service console shows the interfaces, based on the information from the VPN appliance.

![Connectivity Console](image)

**To test the VPN connection**

1. Go to **Disaster Recovery > Connectivity**.
2. In the **VPN Appliance** block, click the gear icon.
3. Ensure that the VPN appliance and the connectivity gateway have the **Online** status.
4. Click **Test connection**.
   
   The VPN appliance checks the connection to the connectivity gateway. You see the list of tests being performed and their results.

**4.2.2 Without site-to-site connection**

**To set up a connection without site-to-site VPN**

1. In the service console, go to **Disaster Recovery > Connectivity** and click **Configure**. The connectivity configuration wizard will open.
2. Select **Do not use site-to-site connection** and click **Start**.

3. As a result, the connectivity gateway and cloud network with the defined address and mask will be deployed on the cloud site.

To learn how to manage your networks in the cloud and set up the connectivity gateway settings, refer to "Managing cloud networks (p. 18)".

### 4.2.3 Point-to-site connection

In case the local network is down, you need the capability to connect directly to the cloud site. This kind of connection is often referred to as a "point-to-site" (P2S) connection, in contrast to the "site-to-site" (S2S) connection.

**To set a user name and password for the point-to-site connection**

1. In the service console, go to **Disaster Recovery > Connectivity**, and then click the gear icon in the **Connectivity Gateway** block.
2. Click **Point-to-site configuration**.
3. Click **Credentials for connection.**

![Point-to-site configuration](image)

- **OpenVPN configuration**
  - Issue date: Jan 1, 1970, Expiration date: Jan 1, 2070
  - ▼ Download configuration for OpenVPN
  - 🔄 Re-generate configuration file

- 🔄 Credentials for connection

4. Specify the user name and password.
5. Confirm the password.
6. When ready, click **Done.**

**To establish the point-to-site connection**

1. Install the OpenVPN client on the machine that you want to connect to the cloud site.
   - Download the OpenVPN client from the following location
     - https://openvpn.net/community-downloads/
   - Supported OpenVPN client versions: 2.4.0 and later.
2. In the service console, go to **Disaster Recovery > Connectivity**, click the gear icon in the **Connectivity Gateway** block.
3. Click **Download configuration for OpenVPN.**
4. Import the downloaded configuration to OpenVPN.
5. When the connection is initiated, enter the user name and password that were set up as described above.

### 4.3 Network management

This section describes network management scenarios.
4.3.1 Managing networks

Site-to-site connection

To add a network on the local site and extend it to the cloud

1. On the VPN appliance, set up the new network interface with the local network that you want to extend in the cloud.
2. Log in to the VPN appliance console.
3. In the Networking section, set up network settings for the new interface.

The VPN appliance starts to report information about networks from all active interfaces to the Cyber Disaster Recovery Cloud service. The service console shows the interfaces based on the information from the VPN appliance.

To delete a network extended to the cloud

1. Log in to the VPN appliance console.
2. In the Networking section, select the interface that you want to delete, and then click Clear network settings.
3. Confirm the operation.

As a result, the local network extension to the cloud via a secure VPN tunnel will be stopped. This network will operate as an independent cloud segment. If this interface is used to pass the traffic from (to) the cloud site, all of your network connections from (to) the cloud site will be disconnected.

To change the network parameters

1. Log in to the VPN appliance console.
2. In the Networking section, select the interface that you want to edit.
3. Click Edit network settings.
4. Select one of the two possible options:
   - For automatic network configuration via DHCP, click Use DHCP. Confirm the operation.
   - For manual network configuration, click Set static IP address. The following settings are available for editing:
     - IP address: the IP address of the interface in the local network.
     - Connectivity gateway IP address: the special IP address which is reserved for the cloud segment of network for the proper Cyber Disaster Recovery Cloud service work.
     - Network mask: network mask of the local network.
     - Default gateway: default gateway on the local site.
     - Preferred DNS server: primary DNS server on the local site.
- **Alternate DNS server**: secondary DNS server on the local site.

Make the necessary changes and confirm them by pressing Enter.

**Without site-to-site connection**

You can have up to five networks in the cloud.

**To add a new cloud network**

1. Go to Disaster Recovery > Connectivity and click Add network.
2. Define the cloud network parameters: the network address and mask. When ready, click Done.

As a result, the additional cloud network with the defined address and mask will be created on the cloud site.

**To delete a cloud network**

*Note* You cannot delete a cloud network if there is at least one cloud server in it. First, delete the cloud server, and then delete the network.

1. Go to Disaster Recovery > Connectivity.
2. On Cloud site, click the network address that you want to delete.
3. Click Delete and confirm the operation.

**To change cloud network parameters**

1. Go to Disaster Recovery > Connectivity.
2. On Cloud site, click the network address that you want to edit.
3. Click Edit.
4. Define the network address and mask, and click Done.

**IP address reconfiguration**

For proper disaster recovery performance, the IP addresses assigned to the local and cloud servers must be consistent. If there is any inconsistency or mismatch in IP addresses, you will see the exclamation mark next to the corresponding network in Disaster Recovery > Connectivity.

Some of the commonly known reasons of IP address inconsistency are listed below:

1. A recovery server was migrated from one network to another or the network mask of the cloud network was changed. As a result, cloud servers have the IP addresses from networks to which they are not connected.
2. The connectivity type was switched from the without site-to-site connection to the site-to-site connection. As a result, a local server is placed in the network different from the one that was created for the recovery server on the cloud site.
3. Editing the following network parameters on the VPN appliance site:
   - Adding an interface via the network settings
   - Editing the network mask manually via the interface settings
- Editing the network mask via DHCP
- Editing the network address and mask manually via the interface settings
- Editing the network mask and address via DHCP

As a result of the actions listed above, the network on the cloud site may become a subset or superset of the local network, or the VPN appliance interface may report the same network settings for different interfaces.

To resolve the issue with network settings

1. Click the network that requires IP address reconfiguration.
   You will see a list of servers in the selected network, their status, and IP addresses. The servers whose network settings are inconsistent are marked with the exclamation mark.
2. To change network settings for a server, click **Go to server**. To change network settings for all servers at once, click **Change** in the notification block.
3. Change the IP addresses as needed by defining them in the **New IP** and **New test IP** fields.
4. When ready, click **Confirm**.

4.3.2 Managing the VPN appliance settings

In the service console (**Disaster Recovery > Connectivity**), you can:

- Test connection
- Download log files
- Connect/disconnect the appliance to/from the cloud site
- Unregister the appliance (if you need to reset the VPN appliance settings or switch to the connection type without site-to-site)

To access these settings, click the gear icon in the **VPN Appliance** block.

In the VPN appliance console, you can:

- Change the password for the appliance
- View/change the network settings and define which interface to use as the WAN for the Internet connection
- Register/change the registration account (by repeating the registration)
- Restart the VPN service
- Reboot the VPN appliance
- Run the Linux shell command (only for advanced troubleshooting cases)

4.3.3 Disabling and enabling site-to-site connection

If you do not need cloud servers on the cloud site to communicate with servers on the local site, you can disable the site-to-site connection.

To disable the site-to-site connection

1. Go to **Disaster Recovery > Connectivity**.
2. In the **Connectivity Gateway** block, click the gear icon, and then click **Disable site-to-site connection**.
3. Confirm the operation by clicking **Done**.

As a result, the local site is disconnected from the cloud site.
You can enable the site-to-site connection in the following cases:

- If you need the cloud servers on the cloud site to communicate with servers on the local site.
- After a failover to the cloud, the local infrastructure is recovered and you want to failback your servers to the local site.

**To enable the site-to-site connection**

1. Go to Disaster Recovery > Connectivity.
2. In the Connectivity Gateway block, click the gear icon, and then click Enable site-to-site connection.
3. Confirm the operation by clicking Done.

As a result, the site-to-site VPN connection is established between the local and cloud sites. The Cyber Disaster Recovery Cloud service gets the network settings from the VPN appliance and extends the local networks to the cloud site.

### 4.3.4 Managing point-to-site connection settings

In the service console, go to Disaster Recovery > Connectivity and click the gear icon in the Connectivity Gateway block. The software displays the user name that is set for the point-to-site connection and the following menu items.

**Download configuration**

This will download the configuration file for the OpenVPN client. The file is required to establish a point-to-site connection to the cloud site (p. 16).

**Change credentials**

You can change the user name and/or password that are used for the point-to-site connection (p. 16).

This is required in the following cases:

- During the initial configuration of the point-to-site connection.
- To perform a planned password change according to the security policy set in your organization.
- In order to restrict access to the cloud site for some users (for example, former employees).

After the credentials have been changed, inform the users that they need to use different credentials.

**Re-generate configuration**

You can re-generate the configuration file for the OpenVPN client.

This is required in the following cases:

- If the VPN client certificate is about to expire. To view the expiration date, click the (i) icon on the connectivity gateway image.
- If you suspect that the configuration file is compromised.

As soon as the configuration file is updated, connecting by means of the old configuration file becomes not possible. Make sure to distribute the new file among the users who are allowed to use the point-to-site connection.
4.3.5 Configuring local routing

In addition to your local networks that are extended to the cloud via the VPN appliance, you may have other local networks that are not registered in the VPN appliance but the servers in them need to communicate with cloud servers. To establish the connectivity between such local servers and cloud servers, you need to configure local routing in the connectivity gateway settings.

To configure local routing

1. Go to Disaster Recovery > Connectivity.
2. In the Connectivity gateway block, click Local routing.
3. Specify the local networks in the CIDR notation.
4. When ready, click Save.

As a result, the servers from the specified local networks will be able to communicate with the cloud servers.
5 Setting up recovery servers

This section describes the concepts of failover and failback, a recovery server lifecycle, creation of a recovery server, and the disaster recovery operations.

5.1 How failover and failback work

Failover and failback

When a recovery server is created, it stays in the Standby state. The corresponding virtual machine does not exist until you initiate the failover. Before starting the failover process, you need to create at least one disk image backup (with bootable volume) of your original machine.

When starting the failover process, you select the recovery point of the original machine from which a virtual machine with the predefined parameters is created. The failover operation uses the "run VM from a backup" functionality. The recovery server gets the transition state Finalization. This process implies transferring the server's virtual disks from the backup storage ("cold" storage) to the disaster recovery storage ("hot" storage). During the finalization, the server is accessible and operable although the performance is lower than normal. When the finalization is completed, the server performance reaches its normal value. The server state changes to Failover. The workload is now switched from the original machine to the recovery server in the cloud site.

If the recovery server has a protection agent inside, the agent service is stopped in order to avoid interference (such as starting a backup or reporting outdated statuses to the backup component).

On the diagram below, you can see both the failover and failback processes.

Test failover

During a test failover, a virtual machine is not finalized. This means that the agent reads the virtual disks' content directly from the backup – that is, performs random access to different parts of the backup.
5.2 Recovery server lifecycle

On the diagram below, you can see a recovery server lifecycle, which shows server permanent states and transitional states. Each block shows a recovery server state, a corresponding virtual machine state, and the actions that are available to a user at this stage. Each arrow is an event or user action that leads to the next state.

---

**Failover and failback workflow**

1. **User action:** Create a recovery server for the selected machine to be protected.

2. **Standby** state. The recovery server configuration is defined, but the corresponding virtual machine is not ready.

3. **User action:** The failover is initiated in the production mode and the recovery server is being created from the selected recovery point.

4. **Finalization** state. Virtual machine disks are finalized from the mounted recovery point to the high-performance storage. The recovery server is operational, though its performance is lower than normal until finalization is completed.
5. Event: Finalization is successful.
6. **Failover** state. The workload is switched from the original machine to the recovery server.
7. User actions:
   - Initiate a failback. As a result, the recovery server is turned off and backed up to the cloud storage.
   - OR
   - If a user cancels the failover, then the workload is switched back to the original machine and the recovery server returns back to the **Standby** state.
8. **Ready for failback** state. The recovery server backup is created. You must recover your local server from this backup by using the regular recovery process.
9. User actions:
   - Confirm failback. As a result, cloud resources that were allocated to the recovery server are released.
   - OR
   - Cancel failback. The failback is canceled by your request. The recovery server returns to the **Failover** state.

**Test failover workflow**
1. User action: Create a recovery server for the selected machine to be protected.
2. **Standby** state. The recovery server configuration is defined, but the respective virtual machine is not ready.
3. User action: Start testing the failover.
4. **Testing failover** state. In this state, a temporary virtual machine is created for testing purposes.
5. User action: Stop testing the failover.

### 5.3 Creating a recovery server

**Prerequisites**
- A protection plan must be applied to the original machine that you want to protect. This plan must back up the entire machine, or only the disks, required for booting up and providing the necessary services, to a cloud storage.
- One of the connectivity types to the cloud site must be set.

**To create a recovery server**
1. On the **All machines** tab, select the machine that you want to protect.
2. Click **Disaster recovery**, and then click **Create recovery server**.
3. Select the number of virtual cores and the size of RAM. Be aware of the compute points next to every option. The number of compute points reflects the cost of running the recovery server per hour.
4. Specify the cloud network to which the server will be connected.
5. Specify the IP address that the server will have in the production network. By default, the IP address of the original machine is set.
   - **Note**: If you use a DHCP server, add this IP address to the server exclusion list in order to avoid IP address conflicts.
6. [Optional] Select the **Test IP address** check box, and then specify the IP address.
This will give you the capability to test a failover in the isolated test network and to connect to
the recovery server via RDP or SSH during a test failover. In the test failover mode, the
connectivity gateway will replace the test IP address with the production IP address by using the
NAT protocol.

If you leave the check box cleared, the console will be the only way to access the server during a
test failover.

**Note** If you use a DHCP server, add this IP address to the server exclusion list, in order to avoid IP address
conflicts.

You can select one of the proposed IP addresses or type in a different one.

7. [Optional] Select the **Internet access** check box.

   This will enable the recovery server to access the Internet during a real or test failover.

8. [Optional] Set the **RPO threshold**.

   The RPO threshold defines the maximum time interval allowed between the last suitable
   recovery point for a failover and the current time. The value can be set within 15 – 60 minutes, 1
   – 24 hours, 1 – 14 days.

9. [Optional] Select the **Use public IP address** check box.

   Having a public IP address makes the recovery server available from the Internet during a failover
   or test failover. If you leave the check box cleared, the server will be available only in your
   production network.

   The public IP address will be shown after you complete the configuration. The following ports are
   open for inbound connections to public IP addresses:

   TCP: 80, 443, 8088, 8443

   UDP: 1194

   If you need other ports to be open, contact the support team.

10. [Optional] If the backups for the selected machine are encrypted, you can specify the password
    that will be automatically used when creating a virtual machine for the recovery server from the
    encrypted backup. Click **Specify**, and then define the credential name and password. By default,
    you will see the most recent backup in the list. To view all the backups, select **Show all backups**.

11. [Optional] Change the recovery server name.

12. [Optional] Type a description for the recovery server.

13. Click **Create**.
The recovery server appears in the Disaster Recovery > Servers > Recovery servers tab of the service console. You can also view its settings by selecting the original machine and clicking Disaster recovery.

5.4 Performing a test failover

Testing a failover means starting a recovery server in a test VLAN that is isolated from your production network. You can test several recovery servers at a time in order to check their interaction. In the test network, the servers communicate using their production IP addresses, but they cannot initiate TCP or UDP connections to the machines in your local network.

Though testing a failover is optional, we recommend that you make it a regular process with a frequency that you find adequate in terms of cost and safety. A good practice is creating a runbook – a set of instructions describing how to spin up the production environment in the cloud.

To run a test failover
1. Select the original machine or select the recovery server that you want to test.
2. Click Disaster Recovery. The description of the recovery server opens.
3. Click Failover.
4. Select the failover type Test failover.
5. Select the recovery point, and then click Test failover.
When the recovery server starts, its state changes to **Testing failover**.

6. Test the recovery server by using any of the following methods:
   - In **Disaster Recovery > Servers**, select the recovery server, and then click **Console**.
   - Connect to the recovery server by using RDP or SSH, and the test IP address that you specified when creating the recovery server. Try the connection from both inside and outside the production network (as described in "Point-to-site connection (p. 12)").
   - Run a script within the recovery server.
     The script may check the login screen, whether applications are started, the Internet connection, and the ability of other machines to connect to the recovery server.
   - If the recovery server has access to the Internet and a public IP address, you may want to use TeamViewer.

7. When the test is complete, click **Stop testing**.
   The recovery server is stopped. All changes made to the recovery server during the test failover are not preserved.

## 5.5 Performing a failover

A failover is a process of moving a workload from your premises to the cloud, and also the state when the workload remains in the cloud.

When you initiate a failover, the recovery server starts in the production network. All protection plans are revoked from the original machine. A new protection plan is automatically created and applied to the recovery server.

At least one recovery point must be created before failing over to a recovery server.

**To perform a failover**

1. Ensure that the original machine is not available on the network.
2. In the service console, go to **Disaster recovery > Servers > Recovery servers** and select the recovery server.
3. Click **Failover**.
4. Select the type of failover **Production failover**.
5. Select the recovery point, and then click **Start production failover**.
When the recovery server starts, its state changes to **Finalization**, and after some time to **Failover**. It is critical to understand that the server is available in both states, despite the spinning progress indicator. For details, refer to "How failover and failback work" (p. 23).

6. Ensure that the recovery server is started by viewing its console. Click **Disaster Recovery** > **Servers**, select the recovery server, and then click **Console**.

7. Ensure that the recovery server can be accessed using the production IP address that you specified when creating the recovery server.

Once the recovery server is finalized, a new protection plan is automatically created and applied to it. This protection plan is based on the protection plan that was used for creating the recovery server, with certain limitations. In this plan, you can change only the schedule and retention rules. For more information, refer to "Back up the cloud servers" (p. 35).

If you want to cancel failover, select the recovery server and click **Cancel failover**. All changes starting from the failover moment except the recovery server backups will be lost. The recovery server will return back to the **Standby** state.

If you want to perform failback (p. 30), select the recovery server and click **Failback**.

**How to perform failover of servers using local DNS**

If you use DNS servers on the local site for resolving machine names, then after a failover the recovery servers, corresponding to the machines relying on the DNS, will fail to communicate because the DNS servers used in the cloud are different. By default, the DNS servers of the cloud site are used for the newly created cloud servers. If you need to apply custom DNS settings, contact the support team.

**How to perform failover of a DHCP server**

Your local infrastructure may have the DHCP server located on a Windows or Linux host. When such a host is failed over to the cloud site, the DHCP server duplication issue occurs because the connectivity gateway in the cloud also performs the DHCP role. To resolve this issue, do one of the following:

- If only the DHCP host was failed over to the cloud, while the rest local servers are still on the local site, then you must log in to the DHCP host in the cloud and turn off the DHCP server on it. Thus, there will be no conflicts and only the connectivity gateway will work as the DHCP server.
If your cloud servers already got the IP addresses from the DHCP host, then you must log in to the DHCP host in the cloud and turn off the DHCP server on it. You must also log in to the cloud servers and renew the DHCP lease to assign new IP addresses allocated from the correct DHCP server (hosted on the connectivity gateway).

5.6 Performing a failback

A failback is a process of moving the workload from the cloud back to your premises.

During this process, the server being moved is unavailable. The length of the maintenance window is approximately equal to the duration of a backup and the subsequent recovery of the server.

To perform a failback

1. Select the recovery server that is in the Failover state.
2. Click Failback.
3. Click Prepare failback.
   
   The recovery server will be stopped and backed up to the cloud storage. Wait for the backup to complete.
   
   At this time, two actions become available: Cancel failback and Confirm failback. If you click Cancel failback, the recovery server will start and the failover will continue.
4. Recover the server from this backup to hardware or to a virtual machine on your premises.
   
   ▪ When using bootable media, proceed as described in "Recovering disks by using bootable media" in the Cyber Protection User Guide. Ensure that you sign in to the cloud by using the account for which the server is registered and that you select the most recent backup.
   
   ▪ If the target machine is online or is a virtual machine, you can use the service console. On the Backup storage tab, select the cloud storage. In Machine to browse from, select the target physical machine or the machine running the agent, if the target machine is virtual. The selected machine must be registered for the same account for which the server is registered. Find the most recent backup of the server, click Recover entire machine, and then set up other recovery parameters. For the detailed instructions, refer to "Recovering a machine" in the Cyber Protection User Guide.
   
   Ensure that the recovery is completed and the recovered machine works properly.
5. Return to the recovery server in the service console, and then click Confirm failback.
The recovery server and recovery points become ready for the next failover. To create new recovery points, apply a protection plan to the new local server.

5.7 Working with encrypted backups

You can create recovery servers from the encrypted backups. For your convenience, you can set up an automatic password application to an encrypted backup during the failover to a recovery server.

When creating a recovery server, you can specify the password to be used for automatic disaster recovery operations (p. 25). It will be saved to the Credentials store, a secure storage of credentials that can be found in Settings > Credentials section.

One credential can be linked to several backups.

To manage the saved passwords in the Credentials store

1. Go to Settings > Credentials.
2. To manage a specific credential, click the icon in the last column. You can view the items linked to this credential.
   - To unlink the backup from the selected credential, click the recycle bin icon near the backup. As a result, you will have to specify the password manually during the failover to the recovery server.
   - To edit the credential, click Edit, and then specify the name or password.
   - To delete the credential, click Delete. Note that you will have to specify the password manually during the failover to the recovery server.
6 Setting up primary servers

This section describes how to create and manage your primary servers.

6.1 Creating a primary server

Prerequisites
- One of the connectivity types to the cloud site must be set.

To create a primary server
1. Go to Disaster Recovery > Servers > Primary servers tab.
2. Click Create.
3. Select a template for the new virtual machine.
4. Select the number of virtual cores and the size of RAM.
   Pay attention to the compute points next to every option. The number of compute points reflects the cost of running the primary server per hour.
5. [Optional] Change the virtual disk size. If you need more than one hard disk, click Add disk, and then specify the new disk size. Currently, you can add no more than 10 disks for a primary server.
6. Specify the cloud network in which the primary server will be included.
7. Specify the IP address that the server will have in the production network. By default, the first free IP address from your production network is set.
   Note: If you use a DHCP server, add this IP address to the server exclusion list in order to avoid IP address conflicts.
8. [Optional] Select the Internet access check box.
   This will enable the primary server to access the Internet.
9. [Optional] Select the Use public IP address check box.
   Having a public IP address makes the primary server available from the Internet. If you leave the check box cleared, the server will be available only in your production network.
   The public IP address will be shown after you complete the configuration. The following ports are open for inbound connections to public IP addresses:
   TCP: 80, 443, 8088, 8443
   UDP: 1194
   If you need other ports to be open, contact the support team.
    RPO threshold defines the maximum allowable time interval between the last recovery point and the current time. The value can be set within 15 – 60 minutes, 1 – 24 hours, 1 – 14 days.
11. Define the primary server name.
12. [Optional] Specify a description for the primary server.
13. Click Create.
The primary server becomes available in the production network. You can manage the server by using its console, RDP, SSH, or TeamViewer.

6.2 Operations with a primary server

The primary server appears in the Disaster Recovery > Servers > Primary servers tab in the service console.

To start or stop the server, click **Power on** or **Power off** on the primary server panel.

To edit the primary server settings, stop the server, and then click **Edit**.

To apply a protection plan to the primary server, select it and on the **Plan** tab click **Create**. You will see a predefined protection plan where you can change only the schedule and retention rules. For more information, refer to "Backing up the cloud servers" (p. 35).
7 Managing the cloud servers

To manage the cloud servers, go to Disaster Recovery > Servers. There are two tabs there: Recovery servers and Primary servers. To show all optional columns in the table, click the gear icon.

You can find the following information about each cloud server by selecting it.

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A cloud server name defined by you</td>
</tr>
<tr>
<td>Status</td>
<td>The status reflecting the most severe issue with a cloud server (based on the active alerts)</td>
</tr>
<tr>
<td>State</td>
<td>A cloud server state according to its lifecycle (p. 24)</td>
</tr>
<tr>
<td>VM state</td>
<td>The power state of a virtual machine associated with a cloud server</td>
</tr>
<tr>
<td>Active location</td>
<td>The location where a cloud server is hosted. For example, Cloud.</td>
</tr>
<tr>
<td>RPO threshold</td>
<td>The maximum time interval allowed between the last suitable recovery point for failover and the current time. The value can be set within 15-60 minutes, 1-24 hours, 1-14 days.</td>
</tr>
</tbody>
</table>
| RPO compliance  | The RPO compliance is the ratio between the actual RPO and RPO threshold. The RPO compliance is shown if the RPO threshold is defined. It is calculated as follows: RPO compliance = Actual RPO / RPO threshold where Actual RPO = current time – last recovery point time RPO compliance statuses Depending on the value of the ratio between the actual RPO and RPO threshold, the following statuses are used:  
  - **Compliant.** The RPO compliance < 1x. A server meets the RPO threshold.  
  - **Exceeded.** The RPO compliance <= 2x. A server violates the RPO threshold.  
  - **Severely exceeded.** The RPO compliance <= 4x. A server violates the RPO threshold more than 2x times.  
  - **Critically exceeded.** The RPO compliance > 4x. A server violates the RPO threshold more than 4x times.  
  - **Pending (no backups).** The server is protected with the protection plan but the backup is being created and not completed yet.  |
| Actual RPO      | The time passed since the last recovery point creation                      |
| Last recovery point | The date and time when the last recovery point was created                |
8 Backing up the cloud servers

Primary and recovery servers are backed up by Agent for VMware, which is installed on the cloud site. In the initial release, this backup is somewhat restricted in functionality as compared to a backup performed by local agents. These limitations are temporary and will be removed in future releases.

- The only possible backup location is the cloud storage.
- A protection plan cannot be applied to multiple servers. Each server must have its own protection plan, even if all of the protection plans have the same settings.
- Only one protection plan can be applied to a server.
- Application-aware backup is not supported.
- Encryption is not available.
- Backup options are not available.

When you delete a primary server, its backups are also deleted.

A recovery server is backed up only in the failover state. Its backups continue the backup sequence of the original server. When a failback is performed, the original server can continue this backup sequence. So, the backups of the recovery server can only be deleted manually or as a result of applying the retention rules. When a recovery server is deleted, its backups are always kept.

**Note** The protection plans for cloud servers are performed according to UTC time.
9 Orchestration (runbooks)

A runbook is a set of instructions describing how to spin up the production environment in the cloud. You can create runbooks in the service console. To access the Runbooks tab, select Disaster recovery > Runbooks.

Why use runbooks?

Runbooks let you:
- Automate a failover of one or multiple servers
- Automatically check the failover result by pinging the server IP address and checking the connection to the port you specify
- Set the sequence of operations for servers running distributed applications
- Include manual operations in the workflow
- Verify the integrity of your disaster recovery solution, by executing runbooks in the test mode

9.1 Creating a runbook

To start creating a runbook, click Create runbook > Add step > Add action. You can use drag and drop to move actions and steps. Do not forget to give a distinctive name to the runbook. While creating a long runbook, click Save from time to time. Once you are finished, click Close.

Steps and actions

A runbook consists of steps that are executed consecutively. A step consists of actions that start simultaneously. An action may consist of:
- An operation to be performed with a cloud server (Failover server, Start server, Stop server, Failback server). To define this operation, you need to choose the operation, the cloud server, and the operation parameters.

- A manual operation that you need to describe verbally. Once the operation is completed, a user must click the confirmation button to allow the runbook to proceed.

- Execution of another runbook. To define this operation, you need to choose the runbook. A runbook can include only one execution of a given runbook. For example, if you added the action "execute Runbook A", you can add the action "execute Runbook B", but cannot add another action "execute Runbook A".

Note: In this product version a user has to perform a failback manually. A runbook shows the prompt when it is required.

### Action parameters

All operations with cloud servers have the following parameters:

- **Continue if already done** (enabled by default)
  
  This parameter defines the runbook behavior when the required operation is already done (for example, a failover has already been performed or a server is already running). When enabled, the runbook issues a warning and proceeds. When disabled, the operation fails and the runbook fails.

- **Continue if failed** (disabled by default)
  
  This parameter defines the runbook behavior when the required operation fails. When enabled, the runbook issues a warning and proceeds. When disabled, the operation fails and the runbook fails.

### Completion check

You can add completion checks to the Failover server and Start server actions, to ensure that the server is available and provides the necessary services. If any of the checks fail, the action is considered failed.

- **Ping IP address**
  
  The software will ping the production IP address of the cloud server until the server replies or the timeout expires, whichever comes first.

- **Connect to port** (443 by default)
  
  The software will try to connect to the cloud server by using its production IP address and the port you specify, until the connection is established or the timeout expires, whichever comes first. This way, you can check if the application that listens on the specified port is running.

The default timeout is 10 minutes. You can change it if you wish.

### 9.2 Operations with runbooks

To access the list of operations, hover on a runbook and click the ellipsis icon. When a runbook is not running, the following operations are available:

- **Execute**
- **Edit**
- **Clone**
- **Delete**
Executing a runbook

Every time you click **Execute**, you are prompted for the execution parameters. These parameters apply to all failover and failback operations included in the runbook. The runbooks specified in the **Execute runbook** operations inherit these parameters from the main runbook.

- **Failover and failback mode**
  Choose whether you want to run a test failover (by default) or a real (production) failover. The failback mode will correspond to the chosen failover mode.

- **Failover recovery point**
  Choose the most recent recovery point (by default) or select a point in time in the past. If the latter is the case, the recovery points closest before the specified date and time will be selected for each server.

Stopping a runbook execution

During a runbook execution, you can select **Stop** in the list of operations. The software will complete all of the already started actions except for those that require user interaction.

Viewing the execution history

When you select a runbook on the **Runbooks** tab, the software displays the runbook details and execution history. Click the line corresponding to a specific execution to view the execution log.
10 Glossary

Cloud server
General reference to a recovery or a primary server.

Cloud site (or DR site)
Remote site hosted in the cloud and used for running recovery infrastructure, in case of a disaster.

Connectivity gateway (formerly, VPN server)
A special virtual machine providing a connection between the local site and the cloud site networks via a secure VPN tunnel. The connectivity gateway is deployed on the cloud site.

Failback
The process of restoring servers to the local site after they have been shifted to the cloud site during the failover.

Failover
Switching the workload or application to the cloud site in case of a natural or man-made disaster on the local site.

Finalization
The intermediate state for production failover or recovery process of the cloud server. This process implies transferring the server's virtual disks from the backup storage ("cold" storage) to the disaster recovery storage ("hot" storage). During the finalization, the server is accessible and operable although the performance is lower than normal.

Local site
The local infrastructure deployed on your company's premises.

Point-to-site (P2S) connection
Connection from outside of the cloud site networks to the cloud site networks via VPN.
**Primary server**
A virtual machine that does not have a linked machine on the local site (such as a recovery server). Primary servers are used for protecting an application or running various auxiliary services (such as a web server).

**Production network**
The internal network extended by means of a VPN tunneling and covering both local and cloud sites. Local servers and cloud servers can communicate with each other in the production network.

**Protected server**
A physical or virtual machine owned by a customer and which is protected with the Cyber Disaster Recovery Cloud service.

**Public IP address**
An IP address that is needed to make cloud servers available from the Internet.

**R**

**Recovery point objective (RPO)**
Amount of data lost from outage, measured as the amount of time from a planned outage or disaster event.

RPO threshold defines the maximum time interval allowed between the last suitable recovery point for a failover and the current time.

**Recovery server**
A VM replica of the original machine, based on the protected server backups stored in the cloud. Recovery servers are used for switching workloads from the original servers, in case of a disaster.

**Runbook**
Planned scenario consisting of configurable steps that automate disaster recovery actions.

**S**

**Site-to-site (S2S) connection**
Connection extending the local network to the cloud, via a secure VPN tunnel.

**T**

**Test IP address**
An IP address that is needed in case of a test failover, to prevent duplication of the production IP address.
Test network
Isolated virtual network that is used to test the failover process.

VPN appliance
A special virtual machine that enables connection between the local network and the cloud site via a secure VPN tunnel. The VPN appliance is deployed on the local site.