# Table of contents

**About Cyber Disaster Recovery Cloud** ................................................................. 4
  The key functionality ......................................................................................... 4

**Software requirements** .................................................................................. 5
  Supported operating systems ........................................................................... 5
  Supported virtualization platforms .................................................................. 5
  Limitations .......................................................................................................... 6

**Create a disaster recovery protection plan** .................................................... 7
  What to do next ................................................................................................... 8
  Editing the Recovery server default parameters .............................................. 8
  Cloud network infrastructure ............................................................................ 9

**Setting up connectivity** .................................................................................. 11
  Networking concepts ......................................................................................... 11
  Cloud-only mode .............................................................................................. 12
  Site-to-site Open VPN connection .................................................................. 13
  Multi-site IPsec VPN connection .................................................................... 19
  Point-to-site remote VPN access ..................................................................... 20
  Automatic deletion of unused customer environments on the cloud site ....... 21

**Initial connectivity configuration** ..................................................................... 22
  Configuring Cloud-only mode ......................................................................... 22
  Configuring Site-to-site Open VPN .................................................................. 22
  Configuring Multi-site IPsec VPN .................................................................... 24

**Recommendations for the Active Directory Domain Services availability** .......... 29
  Configuring Point-to-site remote VPN access ................................................. 29

**Network management** .................................................................................... 30
  Managing networks .......................................................................................... 30
  Managing the VPN appliance settings ............................................................. 34

**Enabling and disabling the Site-to-site connection** ........................................ 34
  Switching the Site-to-site connection type ....................................................... 35

**Reassigning IP addresses** ................................................................................. 36
  Configuring custom DNS servers .................................................................... 37
  Deleting custom DNS servers ......................................................................... 38
  Downloading MAC addresses ......................................................................... 38
  Configuring local routing .................................................................................. 38
  Allowing DHCP traffic over L2 VPN ................................................................. 39
  Managing point-to-site connection settings ..................................................... 39
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active point-to-site connections</td>
<td>40</td>
</tr>
<tr>
<td>Troubleshooting the IPsec VPN configuration</td>
<td>41</td>
</tr>
<tr>
<td><strong>Setting up recovery servers</strong></td>
<td>45</td>
</tr>
<tr>
<td>Creating a recovery server</td>
<td>45</td>
</tr>
<tr>
<td>How failover works</td>
<td>47</td>
</tr>
<tr>
<td>Production failover</td>
<td>47</td>
</tr>
<tr>
<td>Test failover</td>
<td>48</td>
</tr>
<tr>
<td>Performing a test failover</td>
<td>48</td>
</tr>
<tr>
<td>Performing a failover</td>
<td>49</td>
</tr>
<tr>
<td>How failback works</td>
<td>51</td>
</tr>
<tr>
<td>Failback to a target virtual machine</td>
<td>52</td>
</tr>
<tr>
<td>Performing failback to a virtual machine</td>
<td>53</td>
</tr>
<tr>
<td>Failback to a target physical machine</td>
<td>56</td>
</tr>
<tr>
<td>Performing failback to a physical machine</td>
<td>57</td>
</tr>
<tr>
<td>Working with encrypted backups</td>
<td>58</td>
</tr>
<tr>
<td><strong>Setting up primary servers</strong></td>
<td>59</td>
</tr>
<tr>
<td>Creating a primary server</td>
<td>59</td>
</tr>
<tr>
<td>Operations with a primary server</td>
<td>61</td>
</tr>
<tr>
<td><strong>Managing the cloud servers</strong></td>
<td>62</td>
</tr>
<tr>
<td><strong>Firewall rules for cloud servers</strong></td>
<td>64</td>
</tr>
<tr>
<td>Setting firewall rules for cloud servers</td>
<td>64</td>
</tr>
<tr>
<td>Checking the cloud firewall activities</td>
<td>67</td>
</tr>
<tr>
<td><strong>Backing up the cloud servers</strong></td>
<td>68</td>
</tr>
<tr>
<td><strong>Orchestration (runbooks)</strong></td>
<td>69</td>
</tr>
<tr>
<td>Why use runbooks?</td>
<td>69</td>
</tr>
<tr>
<td>Creating a runbook</td>
<td>69</td>
</tr>
<tr>
<td>Steps and actions</td>
<td>70</td>
</tr>
<tr>
<td>Action parameters</td>
<td>70</td>
</tr>
<tr>
<td>Completion check</td>
<td>71</td>
</tr>
<tr>
<td>Operations with runbooks</td>
<td>71</td>
</tr>
<tr>
<td>Executing a runbook</td>
<td>71</td>
</tr>
<tr>
<td>Stopping a runbook execution</td>
<td>72</td>
</tr>
<tr>
<td>Viewing the execution history</td>
<td>72</td>
</tr>
<tr>
<td><strong>Appendix A. Site-to-site Open VPN - Additional information</strong></td>
<td>73</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
<td>80</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>82</td>
</tr>
</tbody>
</table>
About Cyber Disaster Recovery Cloud

**Cyber Disaster Recovery Cloud (DR)** – a part of Cyber Protection that provides disaster recovery as a service (DRaaS). 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.

You can set up and configure disaster recovery in the following ways:

- Create a protection plan that includes the disaster recovery module and apply it to your devices. This will automatically set up default disaster recovery infrastructure. See [Create a disaster recovery protection plan](#).
- Set up the disaster recovery cloud infrastructure manually and control each step. See "Setting up recovery servers" (p. 45).

The key functionality

---

**Note**

Some features might require additional licensing, depending on the applied licensing model.

- Manage the Cyber Disaster Recovery Cloud service from a single console
- Extend up to 23 local networks to the cloud, by using a secure VPN tunnel
- Establish the connection to the cloud site without any VPN appliance deployment (the cloud-only mode)
- Establish the point-to-site connection to your local and cloud sites
- 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
- Use runbooks to spin up the production environment in the cloud

---

1A 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.
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, 8.0
- Debian 9
- Ubuntu 16.04, 18.04
- Windows Server 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
- 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 2012/2012 R2
- 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
- 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 2012/2012 R2
• 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
   • File systems without a partition table
   • Linux workloads that are backed up with an agent from a guest OS and have volumes with the following advanced Logical Volume Manager (LVM) configurations: Striped volumes, Mirrored volumes, RAID 0, RAID 4, RAID 5, RAID 6, or RAID 10 volumes.
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.
Create a disaster recovery protection plan

Create a protection plan that includes the Disaster Recovery module and apply it to your devices.

By default, when creating a new protection plan, the Disaster Recovery module is disabled. After you enable the disaster recovery functionality and apply the plan to your machines, the cloud network infrastructure is created, including a recovery server for each protected machine. The recovery server is a virtual machine in the cloud that is a copy of the selected device. For each of the selected devices a recovery server with default settings is created in a standby state (virtual machine not running). The recovery server is sized automatically depending on the CPU and RAM of the protected machine. Default cloud network infrastructure is also created automatically: VPN gateway and networks on the cloud site, to which the recovery servers are connected.

If you revoke, delete, or switch off the Disaster Recovery module of a protection plan, the recovery servers and cloud networks are not deleted automatically. You can remove the disaster recovery infrastructure manually, if needed.

Note

- It is recommended to configure disaster recovery in advance. You will be able to perform the test or production failover from any of the recovery points generated after the recovery server was created for the device. Recovery points that were generated when a devices was not protected with disaster recovery (e.g. recovery server was not created) cannot be used for failover.
- A disaster recovery protection plan cannot be enabled if the IP address of a device cannot be detected, for example, when virtual machines are backed up agentless and are not assigned an IP address.
- When you apply a protection plan, the same networks and IP addresses are assigned in the cloud site. The IPsec VPN connectivity requires that network segments of the cloud and local sites do not overlap. If a Multi-site IPsec VPN connectivity is configured, and you apply a protection plan to one or several devices later, you must additionally update the cloud networks and reassign the IP addresses of the cloud servers. For more information, see "Reassigning IP addresses" (p. 36).

To create a disaster recovery protection plan

1. In the service console, go to Devices > All devices.
2. Select the machines that you want to protect.
3. Click Protect, and then click Create plan.
   The protection plan default settings open.
4. Configure the backup options.
   To use the disaster recovery functionality, the plan must back up the entire machine, or only the disks, required for booting up and providing the necessary services, to a cloud storage.
5. Enable the Disaster recovery module by clicking the switch next to the module name.
6. Click Create.
   The plan is created and applied to the selected machines.
What to do next

- You can edit the default configuration of the recovery server. For more information, see "Setting up recovery servers" (p. 45).
- You can edit the default networking configuration. For more information, see "Setting up connectivity" (p. 11).
- You can learn more about the recovery server default parameters and the cloud network infrastructure. For more information, see "Editing the Recovery server default parameters" (p. 8) and "Cloud network infrastructure" (p. 9).

Editing the Recovery server default parameters

When you create and apply a disaster recovery protection plan, a recovery server with default parameters is created. You can edit these default parameters later.

**Note**

A recovery server is created only if it does not exist. Existing recovery servers are not changed or recreated.

**To edit the recovery server default parameters**

1. Go to Devices > All devices.
2. Select a device, and click Disaster recovery.
3. Edit the recovery server default parameters.
   The recovery server parameters are described in the following table.

<table>
<thead>
<tr>
<th>Recovery server parameter</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU and RAM</td>
<td>auto</td>
<td>The number of virtual CPUs and the amount of RAM for the recovery server. The default settings will be automatically determined based on the original device CPU and RAM configuration.</td>
</tr>
<tr>
<td>Cloud network</td>
<td>auto</td>
<td>Cloud network to which the server will be connected. For details on how cloud networks are configured, see Cloud network infrastructure.</td>
</tr>
<tr>
<td>IP address in production network</td>
<td>auto</td>
<td>The IP address that the server will have in the production network. By default, the IP address of the original machine is set.</td>
</tr>
<tr>
<td>Test IP address</td>
<td>disabled</td>
<td>Test IP address gives 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,</td>
</tr>
</tbody>
</table>
The VPN gateway will replace the test IP address with the production IP address by using the NAT protocol. If a test IP address is not specified, the console will be the only way to access the server during a test failover.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Access</td>
<td>enabled</td>
<td>Enable the recovery server to access the Internet during a real or test failover. By default, TCP port 25 is denied for outbound connections.</td>
</tr>
<tr>
<td>Use Public address</td>
<td>disabled</td>
<td>Having a public IP address makes the recovery server available from the Internet during a failover or test failover. If you do not use a public IP address, the server will be available only in your production network. To use a public IP address, you must enable internet access. The public IP address will be shown after you complete the configuration. By default, TCP port 443 is open for inbound connections.</td>
</tr>
<tr>
<td>Set RPO threshold</td>
<td>disabled</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Cloud network infrastructure**

The cloud network infrastructure consists of the VPN gateway on the cloud site and the cloud networks to which the recovery servers will be connected.

**Note**

Applying a disaster recovery protection plan creates recovery cloud network infrastructure only if it does not exist. Existing cloud networks are not changed or recreated.

The system checks devices IP addresses and if there are no existing cloud networks where an IP address fits, it automatically creates suitable cloud networks. If you already have existing cloud networks where the recovery servers IP addresses fit, the existing cloud networks will not be changed or recreated.

- If you do not have existing cloud networks or you setup disaster recovery configuration for the first time, the cloud networks will be created with maximum ranges recommended by IANA for private use (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) based on your devices IP address range. You can narrow your network by editing the network mask.
- If you have devices on multiple local networks, the network on the cloud site may become a superset of the local networks. You may reconfigure networks in the **Connectivity** section. See "Managing networks" (p. 30).
• If you need to set up Site-to-site Open VPN connectivity, download the VPN appliance and set it up. See “Configuring Site-to-site Open VPN” (p. 22). Make sure your cloud networks ranges match your local network ranges connected to the VPN appliance.

• To change the default network configuration, click the Go to connectivity link on the Disaster Recovery module of the Protection plan, or navigate to Disaster Recovery > Connectivity.
**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 VPN gateway.

**Networking concepts**

*Note*

Some features might require additional licensing, depending on the applied licensing model.

With Cyber Disaster Recovery Cloud you can define the following connectivity types to the cloud site:

- **Cloud-only mode**
  
  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, and public IP addresses (if assigned).

- **Site-to-site Open VPN connection**
  
  This type of connection requires a VPN appliance deployment on the local site. The Site-to-site Open VPN connection allows to extend your networks to the cloud and retain the IP addresses.
  
  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, and public IP addresses (if assigned).

- **Multi-site IPsec VPN connection**
  
  This type of connection requires a local VPN device that supports IPsec IKE v2.
  
  When you start configuring the Multi-site IPsec VPN connection, Cyber Disaster Recovery Cloud automatically creates a cloud VPN gateway with a public IP address.
  
  With Multi-site IPsec VPN your local sites are connected to the cloud site by means of a secure IPsec VPN tunnel.
  
  This type of connection is suitable for Disaster Recovery scenarios when you have one or several local sites hosting critical workloads or tightly dependent services.
In case of partial failover of one of the servers, the server is recreated on the cloud site while the others remain on the local site, and they are still able to communicate with each other through an IPsec VPN tunnel.

In case of partial failover of one of the local sites, the rest of the local sites remain operational, and will still be able to communicate with each other through an IPsec VPN tunnel.

- **Point-to-site remote VPN access**
  A secure Point-to-site remote VPN access to your cloud and local site workloads from outside by using your endpoint device.
  For a local site access, this type of connection requires a VPN appliance deployment on the local site.

**Note**
With Cyber Disaster Recovery Cloud, you can extend your local networks to the cloud.
- You can extend up to five local networks, if your cloud site is using the US2 or US5 data center.
- You can extend up to 23 local networks, if your cloud site is using any other data center.

**Cloud-only mode**
The cloud-only mode 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 cloud site.

**How routing works**
In case the cloud-only mode is established, routing is performed with the router on the cloud site so that servers from different cloud networks can communicate with each other.
Site-to-site Open VPN connection

**Note**
The availability of this feature depends on the service quotas that are enabled for your account.

To understand how networking works in Cyber Disaster Recovery Cloud, 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.

With the Cyber Disaster Recovery Cloud solution you can fail over all the workload from the corrupted machines in the local site to the cloud servers in the cloud. You can protect up to 23 networks with Cyber Disaster Recovery Cloud.
To establish a Site-to-site Open VPN communication between the local and cloud sites, a **VPN appliance** and a **VPN gateway** are used. When you start configuring the Site-to-site Open VPN connection in the service console, the VPN gateway is automatically deployed in the cloud site. Then, you must deploy the VPN appliance on your local site, add the networks to be protected, and register the appliance in the cloud. Cyber Disaster Recovery Cloud creates a replica of your local network in the cloud. A secure VPN tunnel is established between the VPN appliance and the VPN 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 through 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 on the cloud site. It stays in the **Standby** state until a failover event happens. If a disaster happens and you start a 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 and it can be launched in the same Ethernet segment. Your clients can continue working with the server, without noticing any background changes.

You can also start 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, when you create a
recovery server, you must assign a **Test IP address** to it. There are other parameters for the recovery server that can be specified, they will be considered in the respective sections below.

**How routing works**

When a Site-to-site connection is established, routing between cloud networks is performed with your local router. The VPN server does not perform routing between cloud servers located in different cloud networks. If a cloud server from one network wants to communicate to a server from another cloud network, the traffic goes through the VPN tunnel to the local router on the local site, then the local router routes it to another network, and it goes back through the tunnel to the destination server on the cloud site.

**VPN gateway**

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

- Connects the Ethernet segments of your local network and production network in the cloud in the L2 mode.
- Provides iptables and ebtables rules.
- Works as a default router and NAT for the machines in the test and production networks.
- Works as a DHCP server. All machines in the production and test networks get the network configuration (IP addresses, DNS settings) via DHCP. Every time a cloud server will get the same IP address from the DHCP server. If you need to set up the custom DNS configuration, you should contact the support team.
- Works as a caching DNS.

**VPN gateway network configuration**

The VPN 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 VPN 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 VPN gateway can route packages correctly by using a specific technique.

**VPN appliance**

The **VPN appliance** is a virtual machine on the local site with Linux that has special software installed, and a 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): an IP address 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 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, the recovery server becomes available from the Internet through this IP address. When a packet comes from the Internet with the destination public IP address, the VPN 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, the recovery server becomes available in the test network through 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 through NAT.
For more information about Site-to-site Open VPN, see "Appendix A. Site-to-site Open VPN - Additional information" (p. 73).

Primary servers

A primary server - a virtual machine that does not have a linked machine on the local site if compared to a recovery server. Primary servers are used for protecting an application by 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. 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, and 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 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 through the Internet.
• **Internet access** (optional): allows a primary server to access the Internet.

**Multi-site IPsec VPN connection**

---

**Note**
The availability of this feature depends on the service quotas that are enabled for your account.

You can use the Multi-site IPsec VPN connectivity to connect a single local site, or multiple local sites to the Cyber Disaster Recovery Cloud through a secure L3 IPsec VPN connection.

This connectivity type is useful for Disaster Recovery scenarios if you have one of the following use cases:

• you have one local site hosting critical workloads.
• you have multiple local sites hosting critical workloads, for example offices in different locations.
• you use third-party software sites, or managed service providers sites and are connected to them through an IPsec VPN tunnel.

To establish a Multi-site IPsec VPN communication between the local sites and the cloud site, a **VPN gateway** is used. When you start configuring the Multi-site IPsec VPN connection in the service console, the VPN gateway is automatically deployed in the cloud site. You should configure the cloud network segments and make sure that they do not overlap with the local network segments. A secure VPN tunnel is established between local sites and the cloud site. The local and cloud servers can communicate through this VPN tunnel as if they are all in the same Ethernet segment.

For each source machine to be protected, you must create a recovery server on the cloud site. It stays in the **Standby** state until a failover event happens. If a disaster happens and you start a failover process (in the **production mode**), the recovery server representing the exact copy of your protected machine is launched in the cloud. 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 is launched in the cloud in a special virtual network that is created in the cloud – **test network**. The test network is isolated to prevent duplication of IP addresses in the other cloud network segments.

**VPN gateway**

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

- Connects the Ethernet segments of your local network and production network in the cloud in the L3 IPsec mode.
- Works as a default router and NAT for the machines in the test and production networks.
- Works as a DHCP server. All machines in the production and test networks get the network configuration (IP addresses, DNS settings) via DHCP. Every time a cloud server will get the same IP address from the DHCP server.
  
  If you prefer, you can set up a custom DNS configuration. For more information, see "Configuring custom DNS servers" (p. 37).
- Works as a caching DNS.

How routing works

Routing between the cloud networks is performed with the router on the cloud site so that servers from different cloud networks can communicate with each other.

Point-to-site remote VPN access

**Note**

The availability of this feature depends on the service quotas that are enabled for your account.

The Point-to-site connection is a secure connection from the outside by using your endpoint devices (such as computer or laptop) to the cloud and local sites through a VPN. It is available after you establish a Site-to-site Open VPN connection to the Cyber Disaster Recovery Cloud site. This type of connection is useful in the following cases:

- In many companies, the corporate services and web resources are available only from the corporate network. You can use the Point-to-site connection to securely connect to the local site.
- 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 through the Point-to-site connection to the cloud site.

For the Point-to-site connection to the local site, you need to install the VPN appliance on the local site, configure the Site-to-site connection, and then the Point-to-site connection to the local site. Thus, your remote employees will have access to the corporate network through L2 VPN.

The scheme below shows the local site, cloud site, and communications between servers highlighted in green. The L2 VPN tunnel connects your local and cloud sites. When a user establishes a Point-to-site connection, the communications to the local site are performed through the cloud site.
The Point-to-site configuration uses certificates to authenticate to the VPN client. Additionally user credentials are used for authentication. Note the following about the Point-to-site connection to the local site:

- Users should use their Cyber Cloud credentials to authenticate in the VPN client. They must have either a "Company Administrator" or a "Cyber Protection" user role.
- If you re-generated the OpenVPN configuration, you need to provide the updated configuration to all of the users using the Point-to-site connection to the cloud site.

Automatic deletion of unused customer environments on the cloud site

The Disaster Recovery service tracks the usage of the customer environments created for disaster recovery purposes and automatically deletes them if they are unused.

The following criteria are used to define if the customer tenant is active:

- Currently, there is at least one cloud server or there were cloud server(s) in the last seven days.  
  OR
- The **VPN access to local site** option is enabled and either the Site-to-site Open VPN tunnel is established or there are data reported from the VPN appliance for the last 7 days.

All the rest of the tenants are considered as inactive tenants. For such tenants the system performs the following:

- Deletes the VPN gateway and all cloud resources related to the tenant.
- Unregisters the VPN appliance.

The inactive tenants are rolled back to their state before the connectivity was configured.
Initial connectivity configuration

This section describes connectivity configuration scenarios.

Configuring Cloud-only mode

To configure a connection in the cloud-only mode

1. In the service console, go to Disaster Recovery > Connectivity.
2. Select Cloud-only and click Configure.
   As a result, the VPN gateway and cloud network with the defined address and mask are deployed on the cloud site.

To learn how to manage your networks in the cloud and set up the VPN gateway settings, refer to "Managing cloud networks".

Configuring Site-to-site Open VPN

Note
The availability of this feature depends on the service quotas that are enabled for your account.

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

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

Configuring a Site-to-site Open VPN connection

The VPN appliance extends your local network to the cloud through a secure VPN tunnel. This kind of connection is often referred to as a "Site-to-site" (S2S) connection. You can follow the procedure below or watch the video tutorial.

To configure a connection through the VPN appliance
1. In the service console, go to **Disaster Recovery > Connectivity**.
2. Select **Site-to-site Open VPN connection**, and click **Configure**.
   The system starts deploying the VPN gateway in the cloud. This will take some time. Meanwhile, you can proceed to the next step.

   **Note**
   The VPN 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. In the **VPN appliance** block, click **Download and deploy**. Depending on the virtualization platform you are using, download the VPN appliance for VMware vsphere or Microsoft Hyper-V.
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 Cyber Protection service by using the credentials of the company administrator.
   These credentials are only used once to retrieve the certificate. The data center 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 VPN 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.
Configuring Multi-site IPsec VPN

Note
The availability of this feature depends on the service quotas that are enabled for your account.

You can configure a Multi-site IPsec VPN connection in the following two ways:

• from the Disaster Recovery > Connectivity tab.
• by applying a protection plan on one or several devices, and then manually switching from the automatically created Site-to-site Open VPN connection to a Multi-site IPsec VPN connection, configuring the Multi-site IPsec VPN settings, and reassigning IP addresses.

To configure a Multi-site IPsec VPN connection from the Connectivity tab

1. In the service console, go to Disaster Recovery > Connectivity.
2. In the Multi-site VPN connection section, click Configure.
   A VPN gateway is deployed on the cloud site.
3. Configure the Multi-site IPsec VPN settings.

To configure a Multi-site IPsec VPN connection from a protection plan

1. In the service console, go to Devices.
2. Apply a protection plan to one or multiple devices from the list.
   The recovery server and the cloud infrastructure settings are automatically configured for Site-to-site Open VPN connectivity.
3. Go to Disaster Recovery > Connectivity.
4. Click Show properties.
5. Click Switch to Multi-site IPsec VPN.
6. Configure the Multi-site IPsec VPN settings.
7. Reassign the IP addresses of the cloud network and cloud servers.

Configuring the Multi-site IPsec VPN settings

Note
The availability of this feature depends on the service quotas that are enabled for your account.

After you configure a Multi-site IPsec VPN, you must configure the cloud site and the local sites settings on the Disaster Recovery > Connectivity tab.

Prerequisites

• A configured Multi-site IPsec VPN connectivity. For more information about configuring the Multi-site IPsec VPN connectivity, see "Configuring Multi-site IPsec VPN" (p. 24).
• Public IP address of each the local IPsec VPN gateway.
• Plan your cloud network to have enough IP addresses for the cloud servers that are copies of your protected machines (in the production network), and for the recovery servers (with one or two IP addresses, depending on your needs).

• If you use firewall between the local sites and the cloud site, you must allow the following IP protocols and UDP ports on the local sites: IP Protocol ID 50 (ESP), UDP Port 500 (IKE), and UDP Port 4500.

**To configure a Multi-site IPsec VPN connection**

1. Add one or more networks to the cloud site.
   a. Click **Add Network**.

   **Note**
   When you add a cloud network, a corresponding test network is added automatically with the same network address and mask for performing test failovers. The cloud servers in the test network have the same IP addresses as the ones in the cloud production network. If you need to access a cloud server from the production network during a test failover, when you create a recovery server, assign it a second test IP address.

   b. In the **Network address** field, type the IP address of the network.
   c. In the **Network mask** field, type the mask of the network.
   d. Click **Add**.

2. Configure the settings for each local site that you want to connect to the cloud site, following the recommendations for the local sites. For more information about these recommendations, see "General recommendations for local sites" (p. 26).
   a. Click **Add Connection**.
   b. Enter a name for the of the local VPN gateway.
   c. Enter the public IP address of the local VPN gateway.
   d. [Optional] Enter a description of the local VPN gateway.
   e. Click **Next**.
   f. In the **Pre-shared key** field, type the pre-shared key, or click **Generate a new pre-shared key** to use an automatically generated value.

   **Note**
   You must use the same pre-shared key for the local and the cloud VPN gateways.

   g. Click **IPsec/IKE security settings** to configure the settings. For more information about the settings that you can configure, see "IPsec/IKE security settings" (p. 26).
Note
You can use the default settings, which are populated automatically, or use custom values. Only IKEv2 protocol connections are supported. The default **Startup action** when establishing the VPN is **Add** (your local VPN gateway initiates the connection), but you can change it to **Start** (the cloud VPN gateway initiates the connection) or **Route** (suitable for firewalls that support the route options).

h. Configure the **Network policies**.
   The network policies specify the networks to which the IPsec VPN connects. Type the IP address and mask of the network using the CIDR format. The local and cloud network segments should not overlap.
   i. Click **Save**.

**General recommendations for local sites**

Note
The availability of this feature depends on the service quotas that are enabled for your account.

When you configure the local sites for your Multi-site IPsec VPN connectivity, consider the following recommendations:

- For each IKE Phase, set at least one of the values that are configured in the cloud site for the following parameters: Encryption algorithm, Hash algorithm, and Diffie-Hellman group numbers.
- Enable Perfect forward secrecy with at least one of the values for Diffie-Hellman group numbers that is configured in the cloud site for IKE Phase 2.
- Configure the same value for the **Lifetime** for IKE Phase 1 and IKE Phase 2 as in the cloud site.
- Note that the **Startup action** configuration defines which side initiates the connection. The default value **Add** means that the local site initiates the connection, and cloud site is waiting for the connection initiation. Change the value to **Start** if you want the cloud site to initiate the connection, or to **Route** if you want both sides to be able to initiate the connection (suitable for firewalls that support the route option).

For more information and configuration examples for different solutions, see:
- This series of knowledge base articles
- This video example

**IPsec/IKE security settings**

Note
The availability of this feature depends on the service quotas that are enabled for your account.

The following table provides more information about the Psec/IKE security parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption algorithm</td>
<td>The encryption algorithm that will be used to ensure that data is not viewable while in transit. By default, all algorithms are selected. You must configure at least one of the selected algorithms on your local gateway device for each IKE phase.</td>
</tr>
<tr>
<td>Hash algorithm</td>
<td>The hash algorithm that will be used to verify the data integrity and authenticity. By default, all algorithms are selected. You must configure at least one of the selected algorithms on your local gateway device for each IKE phase.</td>
</tr>
<tr>
<td>Diffie-Hellman group numbers</td>
<td>The Diffie-Hellman group numbers define the strength of the key that is used in the Internet Key Exchange (IKE) process. Higher group numbers are more secure but require additional time for the key to compute. By default, all groups are selected. You must configure at least one of the selected groups on your local gateway device for each IKE phase.</td>
</tr>
<tr>
<td>Lifetime (seconds)</td>
<td>The lifetime value determines the duration of a connection instance with a set of encryption/authentication keys for user packets, from successful negotiation to expiry.</td>
</tr>
<tr>
<td></td>
<td>Range for Phase 1: 900-28800 seconds with default 28800.</td>
</tr>
<tr>
<td></td>
<td>Range for Phase 2: 900-3600 seconds with default 3600.</td>
</tr>
<tr>
<td></td>
<td>The lifetime for Phase 2 must be less than the lifetime for Phase 1. The connection is re-negotiated through the keying channel before it expires, see Rekey margin time. If the local and the remote side do not agree on the lifetime, a clutter of superseded connections will occur on the side with the longer lifetime. See also Rekey margin time and Rekey fuzz.</td>
</tr>
<tr>
<td>Rekey margin time (seconds)</td>
<td>The margin time before connection expiration or keying-channel expiration, during which the local side of the VPN connection attempts to negotiate a replacement. The exact time of the rekey is randomly selected based on the value of Rekey fuzz. Relevant only locally, the remote side does</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Replay window size (packet)</td>
<td>The IPsec replay window size for this connection. The default <code>-1</code> uses the value configured with <code>charon.replay_window</code> in the <code>strongswan.conf</code> file. Values larger than 32 are supported only when using the Netlink backend. A value of 0 disables the IPsec replay protection.</td>
</tr>
<tr>
<td>Rekey fuzz (%)</td>
<td>The maximum percentage by which marginbytes, marginpackets and margintime are randomly increased to randomize rekeying intervals (important for hosts with many connections). The Rekey fuzz value can exceed 100%. The value of <code>marginTYPE</code>, after the random increase, must not exceed <code>lifeTYPE</code>, where <code>TYPE</code> is one of bytes, packets or time. The value 0% disables randomization. Relevant only locally, the remote side does not need to agree on it.</td>
</tr>
<tr>
<td>DPD timeout (seconds)</td>
<td>Time after which a dead peer detection (DPD) timeout occurs. You can specify value 30 or higher. The default value is 30.</td>
</tr>
<tr>
<td>Dead peer detection (DPD) timeout action</td>
<td>The action to take after a dead peer detection (DPD) timeout occurs. <strong>Restart</strong> - Restart the session when DPD timeout occurs. <strong>Clear</strong> - End the session when DPD timeout occurs. <strong>None</strong> - Take no action when DPD timeout occurs.</td>
</tr>
<tr>
<td>Startup action</td>
<td>Determines which side initiates the connection and establishes the tunnel for the VPN connection. <strong>Add</strong> - your local VPN gateway initiates the connection. <strong>Start</strong> - the cloud VPN gateway initiates the connection. <strong>Route</strong> - suitable for VPN gateways that support the route option. The tunnel is up only when there is traffic initiated from either the local VPN gateway,</td>
</tr>
</tbody>
</table>
Recommendations for the Active Directory Domain Services availability

If your protected workloads need to authenticate in a domain controller, we recommend that you have an Active Directory Domain Controller (AD DC) instance at the Disaster Recovery site.

**Active Directory Domain Controller for L2 Open VPN connectivity**

With the L2 Open VPN connectivity, the IP addresses of the protected workloads are retained in the cloud site during a test failover or a production failover. Therefore, the AD DC during a test failover or a production failover has the same IP address as in the local site.

With custom DNS you can set your own custom DNS server for all cloud servers. For more information, see "Configuring custom DNS servers" (p. 37).

**Active Directory Domain Controller for L3 IPsec VPN connectivity**

With L3 IPsec VPN connectivity, the IP addresses of the protected workloads are not retained in the cloud site. Therefore, we recommend that you have an additional dedicated AD DC instance as a primary server in the cloud site before you perform a production failover.

The recommendations for a dedicated AD DC instance that is configured as a primary server in the cloud site are the following:

- Turn off Windows firewall.
- Join the primary server to the Active Directory service.
- Ensure that the primary server has Internet access.
- Add the Active Directory feature.

With custom DNS you can set your own custom DNS server for all cloud servers. For more information, see "Configuring custom DNS servers" (p. 37).

**Configuring Point-to-site remote VPN access**

**Note**

The availability of this feature depends on the service quotas that are enabled for your account.

If you need to connect to your local site remotely, you can configure the Point-to-site connection to the local site. You can follow the procedure below or watch the video tutorial.
**Prerequisites**

- A Site-to-site Open VPN connectivity is configured.
- The VPN appliance is installed on the local site.

**To configure the Point-to-site connection to the local site**

1. In the service console, go to Disaster Recovery > Connectivity.
2. Click Show properties.
3. Enable the VPN access to local site option.
4. Ensure that your user who needs to establish the Point-to-site connection to the local site has:
   - a user account in Cyber Cloud. These credentials are used for authentication in the VPN client. Otherwise, create a user account in Cyber Cloud.
   - a "Company Administrator" or "Cyber Protection" user role.
5. Configure the OpenVPN client:
   a. Download the OpenVPN client version 2.4.0 or later from the following location: https://openvpn.net/community-downloads/.
   b. Install the OpenVPN client on the machine from which you want to connect to the local site.
   c. Click Download configuration for OpenVPN. The configuration file is valid for users in your organization with the "Company Administrator" or "Cyber Protection" user role.
   d. Import the downloaded configuration to OpenVPN.
   e. Log in to the OpenVPN client with your Cyber Cloud user credentials (see step 4 above).
   f. [Optional] If two-factor authentication is enabled for your organization, then you should provide the one-time generated TOTP code.

**Important**
If you enabled two-factor authentication for your account, you need to re-generate the configuration file and renew it for your existing OpenVPN clients. Users must re-log in to Cyber Cloud to set up two-factor authentication for their accounts.

As a result, your user will be able to connect to machines on the local site.

**Network management**

This section describes network management scenarios.

**Managing networks**

**Note**
Some features might require additional licensing, depending on the applied licensing model.

**Site-to-site Open VPN 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.

   ![VPN appliance console](image)

   The VPN appliance starts to report information about networks from all active interfaces to Cyber Disaster Recovery Cloud. 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.
         - **VPN 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.

**Cloud-only mode**

You can have up to 23 networks in the cloud.

*To add a new cloud network*

1. Go to **Disaster Recovery > Connectivity**.
2. On **Cloud site**, click **Add cloud network**.
3. 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 one without Site-to-site connection to a 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. The connectivity type was switched from Site-to-site Open VPN to Multi-site IPsec VPN, or from Multi-site IPsec VPN to Site-to-site Open VPN. For more information about this scenario, see Switching connections and Reassigning IP addresses.
4. 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.

Move servers to a suitable network

When you create a disaster recovery protection plan and apply it on selected devices, the system checks devices IP addresses and automatically creates cloud networks if there are not existing cloud networks where IP address fits. By default, the cloud networks are configured with maximum ranges recommended by IANA for private use (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). You can narrow your network by editing the network mask.
In case if the selected devices was on the multiple local networks, the network on the cloud site may become a superset of the local networks. In this case, to reconfigure cloud networks:

1. Click the cloud network that requires network size reconfiguration and then click **Edit**.
2. Reconfigure the network size with the correct settings.
3. Create other required networks.
4. Click the notification icon next to the number of devices connected to the network.
5. Click **Move to a suitable network**.
6. Select the servers that you want to move to suitable networks and then click **Move**.

**Managing the VPN appliance settings**

**Note**
The availability of this feature depends on the service quotas that are enabled for your account.

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

- Download log files.
- Unregister the appliance (if you need to reset the VPN appliance settings or switch to the cloud-only mode).

To access these settings, click the i 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).

**Enabling and disabling the Site-to-site connection**

**Note**
The availability of this feature depends on the service quotas that are enabled for your account.

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 fail back your servers to the local site.

To **enable the site-to-site connection**
1. Go to **Disaster Recovery > Connectivity**.
2. Click **Show properties**, and then enable the **Site-to-site connection** option.

As a result, the site-to-site VPN connection is enabled 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.

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. Click **Show properties**, and then disable the **Site-to-site connection** option.

As a result, the local site is disconnected from the cloud site.

**Switching the Site-to-site connection type**

**Note**
The availability of this feature depends on the service quotas that are enabled for your account.

You can easily switch form a Site-to-site Open VPN connection to a Multi-site IPsec VPN connection, and from a Multi-site IPsec VPN connection to a Site-to-site Open VPN connection.

When you switch the connectivity type, the active VPN connections are deleted, but the cloud servers and network configurations are preserved. However, you will still need to reassign the IP addresses of the cloud networks and servers.

The following table compares the basic characteristics of the Site-to-site Open VPN connection and the Multi-site IPsec VPN connection.

<table>
<thead>
<tr>
<th></th>
<th>Site-to-site Open VPN</th>
<th>Multi-site IPsec VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local site support</td>
<td>Single</td>
<td>Single, Multiple</td>
</tr>
<tr>
<td>VPN Gateway mode</td>
<td>L2 Open VPN</td>
<td>L3 IPsec VPN</td>
</tr>
<tr>
<td>Network segments</td>
<td>Extends the local network to the cloud network</td>
<td>Local networks and cloud network segments should not overlap</td>
</tr>
<tr>
<td>Supports Point-to-Site access to local site</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Supports Point-to-Site access to cloud site</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Requires a public IP offering item</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**To switch form a Site-to-site Open VPN connection to a Multi-site IPsec VPN connection**
1. In the service console, go to Disaster Recovery -> Connectivity.
2. Click Show properties.
3. Click Switch to multi-site IPsec VPN.
4. Click Reconfigure.
5. Reassign the IP addresses of the cloud network and cloud servers.
6. Configure the Multi-site IPsec connection settings.

To switch form a Multi-site IPsec VPN connection to a Site-to-site Open VPN connection

1. In the service console, go to Disaster Recovery -> Connectivity.
2. Click Show properties.
3. Click Switch to site-to-site Open VPN.
4. Click Reconfigure.
5. Reassign the IP addresses of the cloud network and cloud servers.
6. Configure the Site-to-site connection settings.

Reassigning IP addresses

**Note**
The availability of this feature depends on the service quotas that are enabled for your account.

You must reassign the IP addresses of the cloud networks and the cloud servers in order to complete the configuration in the following cases:

- After you switch from Site-to-site Open VPN to Multi-site IPsec VPN, or the opposite.
- After you apply a protection plan (if the Multi-site IPsec VPN connectivity is configured).

**To reassign the IP address of a cloud network**

1. In the Connectivity tab, click the IP address of the cloud network.
2. In the Network pop-up, click Edit.
3. Type the new the network address and network mask.
4. Click Done.

After you reassign the IP address of a cloud network, you must reassign the cloud servers that belong to the reassigned cloud network.

**To reassign the IP address of a server**

1. In the Connectivity tab, click the IP address of the server in the cloud network.
2. In the Servers pop-up, click Change IP address.
3. In the Change IP address pop-up, type the new IP address of the server, or use the automatically generated IP address which is part of the reassigned cloud network.
Cyber Disaster Recovery Cloud automatically assigns IP addresses from the cloud network to all cloud servers that were part of the cloud network before the reassignment of the network IP address. You can use the suggested IP addresses to reassign the IP addresses of all the cloud servers at once.

4. Click Confirm.

Configuring custom DNS servers

Note
The availability of this feature depends on the service quotas that are enabled for your account.

When you configure a connectivity, Cyber Disaster Recovery Cloud creates your cloud network infrastructure. The cloud DHCP server automatically assigns default DNS servers to the recovery servers and primary servers, but you can change the default settings and configure custom DNS servers. The new DNS settings will be applied at the time of the next request to the DHCP server.

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

To configure a custom DNS server

1. In the service console, go to Disaster Recovery > Connectivity.
2. Click Show properties.
3. Click Default (Provided by Cloud Site).
4. Select Custom servers.
5. Type the IP address of the DNS server.
6. [Optional] If you want to add another DNS server, click Add, and type the DNS server IP address.

Note
After you add the custom DNS servers, you can also add the default DNS servers. In that way, if the custom DNS servers are unavailable, Cyber Disaster Recovery Cloud will use the default DNS servers.

7. Click Done.
Deleting custom DNS servers

Note
The availability of this feature depends on the service quotas that are enabled for your account.

You can delete DNS servers from the custom DNS list.

Prerequisites:
Custom DNS servers are configured.

To delete a custom DNS server
1. In the service console, go to Disaster Recovery > Connectivity.
2. Click Show properties.
3. Click Custom servers.
4. Click the delete icon next to the DNS server.

Note
The delete operation is disabled when only one custom DNS server is available. If you want to delete all custom DNS servers, select Default (provided by Cloud Site).

5. Click Done.

Downloading MAC addresses
You can download a list of MAC addresses, and then extract them and import them in the configuration of your custom DHCP server.

Prerequisites:
• One of the connectivity types to the cloud site must be set.
• At least one primary or recovery server with a MAC address must be configured.

To download the list of MAC addresses
1. In the service console, go to Disaster Recovery > Connectivity.
2. Click Show properties.
3. Click Download the list of MAC addresses, and then save the CSV file.

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

To configure local routing
1. Go to Disaster Recovery > Connectivity.
2. Click Show properties, and then click Local routing.
3. Specify the local networks in the CIDR notation.
4. Click Save.

As a result, the servers from the specified local networks can communicate with the cloud servers.

Allowing DHCP traffic over L2 VPN

If devices on your local site get their IP address from a DHCP server, you can protect the DHCP server with Disaster Recovery, fail it over to the cloud, and then allow the DHCP traffic to run over L2 VPN. Thus, your DHCP server will be running in the cloud, but will continue assigning IP addresses to your local devices.

Prerequisites:

A Site-to-site L2 VPN connectivity type to the cloud site must be set.

To allow the DHCP traffic via the L2 VPN connection

1. Go to Disaster Recovery > Connectivity tab.
2. Click Show Properties.
3. Enable the Allow DHCP traffic via L2 VPN switch.

Managing point-to-site connection settings

Note

The availability of this feature depends on the service quotas that are enabled for your account.

In the service console, go to Disaster Recovery > Connectivity and then click Show properties in the upper right corner.
VPN access to local site
This option is used for managing VPN access to the local site. By default it is enabled. If it is disabled, then the Point-to-site access to the local site will be not allowed.

Download configuration for OpenVPN
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.

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

This is required in the following cases:

- If you suspect that the configuration file is compromised.
- If two-factor authentication was enabled for your account.

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.

Active point-to-site connections

**Note**
The availability of this feature depends on the service quotas that are enabled for your account.

You can view all active point-to-site connections in Disaster recovery > Connectivity. Click the machine icon on the blue **Point-to-site** line and you will see the detailed information about active point-to-site connections grouped by the user name.
Troubleshooting the IPsec VPN configuration

Note
The availability of this feature depends on the service quotas that are enabled for your account.

When you configure or use the IPsec VPN connection, you might experience problems.

You can learn more about the problems that you encountered in the IPsec log files, and check the Troubleshooting IPsec VPN configuration issues topic for possible solutions of some of the common problems that might occur.

Troubleshooting IPsec VPN configuration issues

Note
The availability of this feature depends on the service quotas that are enabled for your account.

The following table describes the IPsec VPN configuration problems that occur most often, and explains how to troubleshoot them.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>I see the following error message: IKE phase 1 negotiation error. Check the IPsec IKE settings on the Cloud and the Local sites.</td>
<td>Click Retry and check if a more specific error message appears. For example, a more specific error message may be an error message about an algorithm mismatch or an incorrect Pre-shared key.</td>
</tr>
<tr>
<td>Problem</td>
<td>Possible solution</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------</td>
</tr>
</tbody>
</table>
| Note   | For security reasons, the following restrictions apply to the IPsec VPN connectivity:  
- IKEv1 is called for deprecation in RFC8247 and is not supported due to security risks. Only IKEv2 protocol connections are supported.  
- The following Encryption algorithms are not considered secure and are not supported: DES, and 3DES.  
- The following Hash algorithms are not considered secure and are not supported: SHA1, and MD5.  
- Diffie-Hellman group number 2 is not considered secure and is not supported. |
| The connection between my local site and the cloud site stays in status Connecting. | Check:  
- If the UDP port 500 is open (when you use a firewall).  
- The connectivity between the local site and the cloud site.  
- If the IP address of the local site is correct. |
| The connection between my local site and the cloud site stays in status Waiting for a connection. | You see this status when the **Startup action** for cloud site is set to **Add**, which means that the cloud site is waiting for the local site to initiate the connection.  
Initiate connection from the local site. |
| The connection between my local site and the cloud site stays in status Waiting for traffic. | You see this status when the **Startup action** for cloud site is set to **Route**.  
If you are expecting a connection from the local site, do the following:  
- From the local site, try to ping the virtual machine in the cloud site. This is a standard behavior necessary for establishing a tunnel for some devices, for example Cisco ASA. **(Route mode)**  
- Ensure that the local site established a tunnel by setting the **Startup action** of the local site to **Start**. |
| The connection between my local site and the cloud site is established, but I see this status | This issue may be due to the following reasons:  
- Network mapping in the cloud IPsec site is... |
<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>can see that one or more of the network policies are down.</td>
<td>different from the network mapping in the local site. Ensure that the network mappings and the sequence of the network policies in the local and cloud sites match exactly. • This state is correct when the <strong>Startup action</strong> of the local site and/or of the cloud site is set to <strong>Route</strong> (for example, on Cisco ASA devices), and currently there is no traffic. You can try to ping to make sure that the tunnel is established. If the ping is not working, check the network mapping on the local and the cloud site.</td>
</tr>
<tr>
<td>I want restart a specific IPsec connection.</td>
<td>To restart a specific IPsec connection: 1. In the <strong>Disaster recovery &gt; Connectivity</strong> screen, click the IPsec connection. 2. Click <strong>Disable connection</strong>. 3. Click the IPsec connection again. 4. Click <strong>Enable connection</strong>.</td>
</tr>
</tbody>
</table>

**Downloading the IPsec VPN log files**

**Note**
The availability of this feature depends on the service quotas that are enabled for your account.

You can find additional information about the IPsec connectivity in the log files on the VPN server. The log files are compressed in a .zip archive that you can download and extract.

**Prerequisites**

Multi-site IPsec VPN connectivity is configured.

**To download the .zip archive with the log files**

1. In the service console, go to **Disaster Recovery > Connectivity**.
2. Click the gear icon next to the VPN gateway of the cloud site.
3. Click **Download log**.

**Multi-site IPSec VPN log files**

**Note**
The availability of this feature depends on the service quotas that are enabled for your account.
The following list provides more information about the IPsec VPN log files that are part of the zip archive, and the information that they contain.

- **ip.txt** - The file contains the logs from the configuration of the network interfaces. You must see two IP addresses - a public IP address, and a local IP address. If you do not see these IP addresses in the log, there is a problem. Contact the Support team.

  **Note**
  The mask for the public IP address must be 32.

- **swanctl-list-loaded-config.txt** - The file contains information about all IPsec sites. If you do not see a site in the file, then the IPsec configuration was not applied. Try to update the configuration and save it, or contact the Support team.

- **swanctl-list-active-sas.txt** - The file contains connections and policies that are in status active or a connecting.
Setting up recovery servers

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

Creating a recovery server

You can follow the instructions below or watch the video tutorial.

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 devices 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. Select the DHCP option.

<table>
<thead>
<tr>
<th>DHCP option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provided by cloud site</td>
<td>Default setting. The IP address of the server will be provided by an automatically configured DHCP server in the cloud.</td>
</tr>
<tr>
<td>Custom</td>
<td>The IP address of the server will be provided by your own DHCP server in the cloud.</td>
</tr>
</tbody>
</table>

6. [Optional] Specify the MAC address.
   The MAC address is a unique identifier that is assigned to the network adapter of the server. If you use custom DHCP, you can configure it to always assign a specific IP addresses to a specific MAC address. In that way you will ensure that the recovery server always gets the same IP address. You can run applications that have licenses that are registered with the MAC address.
7. 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.
If you use a custom DHCP server, you must specify the same IP address in **IP address in production network** as the one configured in the DHCP server. Otherwise, test failover will not work properly, and the server will not be reachable via a public IP address.

8. [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 VPN 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.

9. [Optional] Select the **Internet access** check box.
This will enable the recovery server to access the Internet during a real or test failover. By default, the TCP port 25 is open for outbound connections to public IP addresses.

10. [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.

11. [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 **Use public IP address** option requires the **Internet access** option to be enabled.
The public IP address will be shown after you complete the configuration. By default, TCP port 443 is open for inbound connections to public IP addresses.

12. [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**.

13. [Optional] Change the recovery server name.

15. [Optional] Click the Cloud firewall rules tab to edit the default firewall rules. For more information, see "Setting firewall rules for cloud servers" (p. 64).

16. 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.

How failover works

Production failover

**Note**

The availability of this feature depends on the service quotas that are enabled for your account.

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. For more information about the test failover process, see "Performing a test failover" (p. 48).

**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.

It is recommended to create a recovery server in advance to protect your devices from a disaster. You will be able to perform the test failover from any of the recovery points generated after the recovery server was created for the device.

**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").
   - 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.

**Note**

The **Start server** and **Stop server** actions are not applicable for test failover operations, both in runbooks and when starting a test failover manually. If you try executing such an action, it will fail with the following error message:

Failed: The action is not applicable to the current server state.

**Performing a failover**

**Note**

The availability of this feature depends on the service quotas that are enabled for your account.
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.

A good practice is to create a recovery server in advance to protect your devices from a disaster. You will be able to perform the production failover from any of the recovery points generated after the recovery server was created for the device.

You can follow the instructions below or watch the video tutorial.

**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 works" (p. 47).

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 "Backing up the cloud servers".

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, 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 VPN 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 VPN 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 VPN gateway).

Note

The instructions are not valid when your cloud DHCP server is configured with the Custom DHCP option, and some of the recovery or primary servers get their IP address from this DHCP server.

How failback works

Note

The availability of this feature depends on the service quotas that are enabled for your account.

A failback is a process of moving the workload from the cloud back to a physical or virtual machine on your local site. You can perform a failback on a recovery server in Failover state, and continue using the server on your local site.

During the failback process to a target virtual machine, you can transfer the backup data to your local site while the virtual machine in the cloud continues to run. This technology helps you to
achieve a very short downtime period, which is estimated and displayed in the service console. You can view it and use this information to plan your activities and, if necessary, warn your clients about an upcoming downtime period.

The failback process to target virtual machines and target physical machines is different. For more information about the phases of the failback process, see "Failback to a target virtual machine" (p. 52) and "Failback to a target physical machine" (p. 56).

**Note**
Runbook operations support the failback to a physical machine only. This means that if you start the failback process by executing a runbook that includes a **Failback server** step, the procedure will require a manual interaction - you must manually recover the machine, and confirm or cancel the failback process from the **Disaster Recovery>Servers** tab.

### Failback to a target virtual machine

**Note**
The availability of this feature depends on the service quotas that are enabled for your account.

The failback process to a target virtual machine consists of four phases.

![Failback Process Diagram]

1. **Planning.** During this phase, you restore the IT infrastructure at your local site, such as the hosts and the network configurations, configure the failback parameters, and plan when to start the
data transfer.

Note
To minimize the total time for the failback process, we recommend that you start the **Data transfer** phase immediately after you set up your local servers, and then continue configuring the network and setting up the rest of the local infrastructure during the **Data transfer** phase.

2. **Data transfer.** During this phase, the data is transferred from the cloud site to the local site while the virtual machine in the cloud continues to run. You can start the next phase - **Switchover,** at any time during the **Data transfer** phase, but you should consider the following relations:

   The longer you remain in the **Data transfer** phase,
   - the longer the virtual machine in the cloud continues to run
   - the bigger amount of data will be transferred to your local site
   - the higher the cost you will pay (you spend more compute points)
   - the shorter the downtime period that you will experience during the **Switchover** phase.

   If you want to minimize the downtime, start the **Switchover** phase after more than 90 % of the data is transferred to the local site.

   If you can afford to experience a longer downtime period, and do not want to spend more compute points for running the virtual machine in the cloud, you can start the **Switchover** phase earlier.

   If you cancel the failback process during the **Data transfer** phase, the transferred data will not be deleted from the local site. To avoid potential issues, manually delete the transferred data before you start a new failback process. The following data transfer process will start from the beginning.

3. **Switchover.** During this phase, the virtual machine in the cloud is turned off and the remaining data, including the last backup increment, is transferred to the local site. Note that when the **Switchover** phase completes, all data is transferred to the local site - there is no data loss, and the virtual machine on the local site is an exact copy of the virtual machine in the cloud. You can view the estimated time to finish (downtime period) of this phase in the service console. When all the data is transferred to the local site, the virtual machine on the local site is recovered, and the **Validation** phase starts automatically.

4. **Validation.** During this phase, the virtual machine on the local site is ready and you can turn it on. You can verify if the virtual machine is working correctly, and:

   - If everything is working as expected, confirm the failback. After the failback confirmation, the virtual machine in the cloud is deleted, and the recovery server returns to the **Standby** state. This is the end of the failback process.
   - If something is wrong, you can cancel the switchover and return to the **Data transfer** phase.

**Performing failback to a virtual machine**

Note
The availability of this feature depends on the service quotas that are enabled for your account.
You can perform failback to a target virtual machine on your local site.

**Prerequisites**

- The agent that you will use to perform failback is online and is not currently used for another failback operation.
- Your Internet connection is stable.

**To perform a failback to a virtual machine**

1. In the service console, go to Disaster recovery > Servers.
2. Select the recovery server that is in the Failover state.
3. Click the Failback tab.
4. In the Failback parameters section, select Virtual machine as a Target, and configure the other parameters.

   Note that by default, some of the Failback parameters are populated automatically with suggested values, but you can change them.

   The following table provides more information about the Failback parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Backup size**         | Amount of data that will be transferred to your local site during the failback process.  
                          | After you start the failback process to a target virtual machine, the Backup size will be increasing during the Data transfer phase, because the virtual machine in the cloud will continue to run and generate new data.  
                          | To calculate the estimated downtime period during the failback process to a target virtual machine, take 10% of the Backup size value (as we recommend that you start the Switchover phase after 90% of the data is transferred to your local site), and divide it by the value of your Internet speed.  
                          | Note  
                          | The value of the Internet speed will decrease when you perform several failback processes at the same time. |
| **Target**              | Type of workload on your local site to which you will recover the cloud server: Virtual machine or Physical machine. |
| **Target machine location** | Failback location: a VMware ESXi host or a Microsoft Hyper-V host.  
                          | You can select from all the hosts that have an agent which is registered with the Cyber Protection service. |
| **Agent**               | Agent which will perform the failback operation.  
                          | You can use one agent to perform one failback operation at the same time. |
### Target machine settings
Virtual machine settings:
- **Virtual processors.** Select the number of virtual processors.
- **Memory.** Select how much memory the virtual machine will have.
- **Units.** Select the units for the memory.
- [Optional] **Network adapters.** To add a network adapter, click Add, and select a network in the Network field.

When you are ready with the changes, click Done.

### Path
(For Microsoft Hyper-V hosts) Folder on the host where your machine will be stored.
Ensure that there is enough free memory space on the host for the machine.

### Datastore
(For VMware ESXi hosts) Datastore on the host where your machine will be stored.
Ensure that there is enough free memory space on the host for the machine.

### Provisioning mode
Method of allocation of the virtual disk.
For Microsoft Hyper-V hosts:
- **Dynamically expanding** (default value).
- **Fixed size.**
For Microsoft Hyper-V hosts:
- **Thin** (default value).
- **Thick.**

### Target machine name
Name of the target machine. By default, the target machine name is the same as the recovery server name.
The target machine name must be unique on the selected Target machine location.

5. Click **Start data transfer**, and then in the confirmation window, click **Start**.

The Data transfer phase starts. The console displays the following information:

- **Progress.** The parameter shows how much data is already transferred to the local site, and the total amount of data that must be transferred. Note that the total amount of data includes the data from the last backup before the data transfer phase was started, and the backups of the newly generated data (backup increments), as the virtual machine continues to run during the Data transfer phase. For this reason, both values of the Progress parameter increase.
with time.

- **Downtime estimation.** The parameter shows how much time the virtual machine will be unavailable, if you start the **Switchover** phase now. The value is calculated based on the values of the **Progress**, and decreases with time.

6. Click **Switchover**, and then in the confirmation window, click **Switchover** again.

   The **Switchover** phase starts. The console displays the following information:
   - **Progress.** The parameter shows the progress of restoring the virtual machine on the local site.
   - **Estimated time to finish.** The parameter shows the approximate time when the **Switchover** phase will be completed and you will be able to turn on the virtual machine on the local site.

7. After the **Switchover** phase completes, validate that the virtual machine on your local site is working as expected.

8. Click **Confirm failback**, and then in the confirmation window, click **Confirm** to finalize the process.

   The virtual machine in the cloud is deleted, and the recovery server returns to the **Standby** state.

---

**Note**

Applying a protection plan on the recovered server is not part of the failback process. After the failback process completes, apply a protection plan on the recovered server to ensure that it is protected again. You may apply the same protection plan that was applied on the original server, or a new protection plan that has the Disaster Recovery module enabled.

---

**Failback to a target physical machine**

---

**Note**

The availability of this feature depends on the service quotas that are enabled for your account.

---

The failback process to a target physical machine differs from the failback process to a target virtual machine. The data transfer from the backup in the cloud to the local site is not part of the automated workflow, and is done manually after the virtual machine in the cloud is turned off. For this reason, when performing failback to a physical machine, expect a longer downtime period.

The failback process to a target physical machine consists of the following phases:

1. **Planning.** During this phase, you restore the IT infrastructure at your local site, such as the hosts and the network configurations, configure the failback parameters, and plan when to start the data transfer.

2. **Switchover.** During this phase, the virtual machine in the cloud is turned off and the newly generated data is backed up. When the backup is complete, you recover the machine to the local site manually. You can either recover the disk by using bootable media, or recover the entire machine from the cloud backup storage.

3. **Validation.** During this phase, you verify that the physical machine is working correctly, and confirm the failback. After the confirmation, the virtual machine on the cloud site is deleted, and the recovery server returns to the **Standby** state.
Performing failback to a physical machine

Note
The availability of this feature depends on the service quotas that are enabled for your account.

You can perform failback to a target physical machine on your local site.

To perform a failback to a physical machine

1. In the service console, go to Disaster recovery > Servers.
2. Select the recovery server that is in the Failover state.
3. Click the Failback tab.
4. In the Select target field, select Physical machine.
5. [Optional] Calculate the estimated downtime period during the failback process, by dividing the Backup size value by the value of your Internet speed.

Note
The value of the Internet speed will decrease when you perform several failback processes at the same time.

6. Click Switchover, and then in the confirmation window, click Switchover again.
   The virtual machine on the cloud site is turned off.
7. Recover the server from a backup to the physical machine on your local site.
   - If you are 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, 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. 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 detailed instructions, refer to "Recovering a machine" in the Cyber Protection User Guide.
8. Ensure that the recovery is completed and the recovered machine works properly, and click Machine is restored.
9. If everything is working as expected, click Confirm failback, and then in the confirmation window, click Confirm again.
   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.
Note
Applying a protection plan on the recovered server is not part of the failback process. After the failback process completes, apply a protection plan on the recovered server to ensure that it is protected again. You may apply the same protection plan that was applied on the original server, or a new protection plan that has the Disaster Recovery module enabled.

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. 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.
Setting up primary servers

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

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. Select the DHCP option.

<table>
<thead>
<tr>
<th>DHCP option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provided by cloud site</td>
<td>Default setting. The IP address of the server will be provided by an automatically configured DHCP server in the cloud.</td>
</tr>
<tr>
<td>Custom</td>
<td>The IP address of the server will be provided by your own DHCP server in the cloud.</td>
</tr>
</tbody>
</table>

8. [Optional] Specify the MAC address.
   The MAC address is a unique identifier that is assigned to the network adapter of the server. If you use custom DHCP, you can configure it to always assign a specific IP address to a specific MAC address. This ensures that the primary server always gets the same IP address. You can run applications that have licenses that are registered with the MAC address.

9. 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.
If you use a custom DHCP server, you must specify the same IP address in **IP address in production network** as the one configured in the DHCP server. Otherwise, test failover will not work properly, and the server will not be reachable via a public IP address.

10. [Optional] Select the **Internet access** check box.
    This will enable the primary server to access the Internet. By default, TCP port 25 is open for outbound connections to public IP addresses.

11. [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. By default, TCP port 443 is open for inbound connections to public IP addresses.

12. [Optional] Select **Set RPO threshold**.
    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.

13. Define the primary server name.


15. [Optional] Click the **Cloud firewall rules** tab to edit the default firewall rules. For more information, see "Setting firewall rules for cloud servers" (p. 64).

16. Click **Create**.

The primary server becomes available in the production network. You can manage the server by using its console, RDP, SSH, or TeamViewer.
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".
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</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, <strong>Cloud</strong>.</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     | The date and time when the last recovery point was created                  |
point
Firewall rules for cloud servers

You can configure firewall rules to control the inbound and outbound traffic of the primary and recovery servers on your cloud site.

You can configure inbound rules after you provision a public IP address for the cloud server. By default, TCP port 443 is allowed, and all other inbound connections are denied. You can change the default firewall rules, and add or remove Inbound exceptions. If a public IP is not provisioned, you can only view the inbound rules, but cannot configure them.

You can configure outbound rules after when you provision Internet access for the cloud server. By default, TCP port 25 is denied, and all other outbound connections are allowed. You can change the default firewall rules, and add or remove outbound exceptions. If Internet access is not provisioned, you can only view the outbound rules, but cannot configure them.

Note
For security reasons, there are predefined firewall rules that you cannot change.

For inbound and outbound connections:

- Permit ping: ICMP echo-request (type 8, code 0) and ICMP echo-reply (type 0, code 0)
- Permit ICMP need-to-frag (type 3, code 4)
- Permit TTL exceeded (type 11, code 0)

For inbound connections only:
- Non-configurable part: Deny all

For outbound connections only:
- Non-configurable part: Reject all

Setting firewall rules for cloud servers

You can edit the default firewall rules for the primary and recovery servers in the cloud.

To edit the firewall rules of a server on your cloud site

1. In the service console, go to Disaster Recovery > Servers.
2. If you want to edit the firewall rules of a recovery server, click the Recovery servers tab.
   Alternatively, if you want to edit the firewall rules of a primary server, click the Primary servers tab.
3. Click the server, and then click Edit.
4. Click the Cloud firewall rules tab.
5. If you want to change the default action for the inbound connections:
a. In the **Inbound** drop-down field, select the default action.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny all</td>
<td>Denies any inbound traffic. You can add exceptions and allow traffic from specific IP addresses, protocols, and ports.</td>
</tr>
<tr>
<td>Allow all</td>
<td>Allows all inbound TCP and UDP traffic. You can add exceptions and deny traffic from specific IP addresses, protocols, and ports.</td>
</tr>
</tbody>
</table>

**Note**
Changing the default action invalidates and removes the configuration of existing inbound rules.

b. [Optional] If you want to save the existing exceptions, in the confirmation window, select **Save filled-in exceptions**.

c. Click **Confirm**.

6. If you want to add an exception:

   a. Click **Add exception**.

   b. Specify the firewall parameters.

<table>
<thead>
<tr>
<th>Firewall parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select the protocol for the connection. The following options are supported:</td>
</tr>
<tr>
<td></td>
<td>• TCP</td>
</tr>
<tr>
<td></td>
<td>• UDP</td>
</tr>
<tr>
<td></td>
<td>• TCP+UDP</td>
</tr>
<tr>
<td>Server port</td>
<td>Select the ports to which the rule applies. You can specify the following:</td>
</tr>
<tr>
<td></td>
<td>• a specific port number (for example, 2298)</td>
</tr>
<tr>
<td></td>
<td>• a range of port numbers (for example, 6000-6700)</td>
</tr>
<tr>
<td></td>
<td>• any port number. Use * if you want the rule to apply to any port number.</td>
</tr>
<tr>
<td>Client IP address</td>
<td>Select the IP addresses to which the rule applies. You can specify the following:</td>
</tr>
<tr>
<td></td>
<td>• a specific IP address (for example, 192.168.0.0)</td>
</tr>
<tr>
<td></td>
<td>• a range of IP addresses using the CIDR notation (for example, 192.168.0.0/24)</td>
</tr>
<tr>
<td></td>
<td>• any IP address. Use * if you want the rule to apply to any IP address.</td>
</tr>
</tbody>
</table>

7. If you want to remove an existing inbound exception, click the bin icon next to it.
8. If you want to change the default action for the outbound connections:
   a. In the **Outbound** drop-down field, select the default action.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny all</td>
<td>Denies any outbound traffic. You can add exceptions and allow traffic to specific IP addresses, protocols, and ports.</td>
</tr>
<tr>
<td>Allow all</td>
<td>Allows all outbound traffic. You can add exceptions and deny traffic from specific IP addresses, protocols, and ports.</td>
</tr>
</tbody>
</table>

**Note**
Changing the default action invalidates and removes the configuration of existing outbound rules.

   b. [Optional] If you want to save the existing exceptions, in the confirmation window, select **Save filled-in exceptions**.
   c. Click **Confirm**.

9. If you want to add an exception:
   a. Click **Add exception**.
   b. Specify the firewall parameters.

<table>
<thead>
<tr>
<th>Firewall parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select the protocol for the connection. The following options are supported:</td>
</tr>
<tr>
<td></td>
<td>• TCP</td>
</tr>
<tr>
<td></td>
<td>• UDP</td>
</tr>
<tr>
<td></td>
<td>• TCP+UDP</td>
</tr>
<tr>
<td>Server port</td>
<td>Select the ports to which the rule applies. You can specify the following:</td>
</tr>
<tr>
<td></td>
<td>• a specific port number (for example, 2298)</td>
</tr>
<tr>
<td></td>
<td>• a range of port numbers (for example, 6000-6700)</td>
</tr>
<tr>
<td></td>
<td>• any port number. Use * if you want the rule to apply to any port number.</td>
</tr>
<tr>
<td>Client IP address</td>
<td>Select the IP addresses to which the rule applies. You can specify the following:</td>
</tr>
<tr>
<td></td>
<td>• a specific IP address (for example, 192.168.0.0)</td>
</tr>
<tr>
<td></td>
<td>• a range of IP addresses using the CIDR notation (for example, 192.168.0.0/24)</td>
</tr>
<tr>
<td></td>
<td>• any IP address. Use * if you want the rule to apply to any IP address.</td>
</tr>
</tbody>
</table>
10. If you want to remove an existing outbound exception, click the bin icon next to it.
11. Click Save.

Checking the cloud firewall activities

After an update of the configuration of the firewall rules of a cloud server, a log of the update activity becomes available in the service console. You can view the log and check the following information:

- user name of the user who updated the configuration
- date and time of the update
- firewall settings for inbound and outbound connections
- the default actions for inbound and outbound connections
- the protocols, ports and IP addresses of the exceptions for inbound and outbound connections

To view the details about a cloud firewall rules configuration change

1. In the service console, click Dashboard> Activities.
2. Click the corresponding activity, and click All Properties.
   The description of the activity should be Updating cloud server configuration.
3. In the context field, inspect the information that you are interested in.
**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.
Orchestration (runbooks)

Note
Some features might require additional licensing, depending on the applied licensing model.

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.

Creating a runbook
You can follow the instruction below or watch the video tutorial.

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.

**Operations with runbooks**

*Note*
The availability of this feature depends on the service quotas that are enabled for your account.

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.
Appendix A. Site-to-site Open VPN - Additional information

When you create a recovery server, you configure its **IP address in production network**, and its **Test IP address**.

After you perform failover (run the virtual machine in the cloud), and log in to the virtual machine to check the IP address of the server, you see the **IP address in production network**.

When you perform test failover, you can reach the test server only by using the **Test IP address**, which is visible only in the configuration of the recovery server.

To reach a test server from your local site, you must use the **Test IP address**.

**Note**
The network configuration of the server always shows the **IP address in production network** (as the test server mirrors how the production server would look). This happens because the test IP address does not belong to the test server, but to the VPN gateway, and is translated to the production IP address using NAT.

The diagram below shows an example of the Site-to-site Open VPN configuration. Some of the servers in the local environment are recovered to the cloud using failover (while the network infrastructure is ok).

1. The customer enabled Disaster Recovery by:
   a. configuring the VPN appliance (14), and connected it to the dedicated cloud VPN server (15)
   b. protecting some of the local servers with Disaster Recovery (1, 2, 3, x8, and x10)
      Some servers on the local site (like 4) are connected to networks which are not connected to the VPN appliance. Such servers are not protected with Disaster Recovery.
2. Part of the servers (connected to different networks) work in the local site: (1, 2, 3, and 4)
3. The protected servers (1, 2, and 3) are being tested with test failover (11, 12, and 13)
4. Some servers in the local site are unavailable (x8, x10). After performing failover, they become available in the cloud (8, and 10)
5. Some primary servers (7, and 9), connected to different networks, are available in the cloud environment
6. (5) is a server in the Internet with a public IP address

7. (6) is a workstation connected to the cloud using a Point-to-site VPN connection (p2s)

In this example, the following connection setup is available (for example, "ping") from a server in the From: row to a server in the To: column.

<table>
<thead>
<tr>
<th>From:</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>local</td>
<td>local</td>
<td>local</td>
<td>local</td>
<td>internet</td>
<td>p2s</td>
<td>primary</td>
<td>failover</td>
<td>primary</td>
<td>failover</td>
<td>test failover</td>
<td>test failover</td>
<td>test failover</td>
<td>VPN appliance</td>
<td>VPN server</td>
</tr>
<tr>
<td>To:</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>-----</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>1</td>
<td>local</td>
<td>direct</td>
<td>via local router 1</td>
<td>via local router 2</td>
<td>via local router 1 and Internet</td>
<td>no</td>
<td>via tunnel: local</td>
<td>via tunnel: local</td>
<td>via tunnel: local</td>
<td>via tunnel: local</td>
<td>via tunnel: NAT (VPN server)</td>
<td>via tunnel: NAT (VPN server)</td>
<td>via local router 1 and tunnel: NAT (VPN server)</td>
<td>direct</td>
<td>no</td>
</tr>
<tr>
<td>2</td>
<td>local</td>
<td>direct</td>
<td>via local router 1</td>
<td>via local router 2</td>
<td>via local router 1 and Internet</td>
<td>no</td>
<td>via tunnel: local</td>
<td>via tunnel: local</td>
<td>via tunnel: local</td>
<td>via tunnel: local</td>
<td>via tunnel: NAT (VPN server)</td>
<td>via tunnel: NAT (VPN server)</td>
<td>via local router 1 and tunnel: NAT (VPN server)</td>
<td>direct</td>
<td>no</td>
</tr>
<tr>
<td>3</td>
<td>local</td>
<td>via local</td>
<td>via local</td>
<td>via local router 1</td>
<td>no</td>
<td>via tunnel:</td>
<td>via tunnel:</td>
<td>via tunnel:</td>
<td>via tunnel:</td>
<td>via tunnel:</td>
<td>via tunnel:</td>
<td>via tunnel:</td>
<td>via local router</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>To:</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>----</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td>router 1</td>
<td>router 1</td>
<td>router 2</td>
<td>router 2</td>
<td>and</td>
<td>local</td>
<td>local</td>
<td>local</td>
<td>local</td>
<td>NAT</td>
<td>NAT</td>
<td>router 1</td>
<td>and</td>
<td></td>
<td>tunnel: NAT</td>
</tr>
<tr>
<td>4</td>
<td>local</td>
<td>via</td>
<td>via</td>
<td>via</td>
<td>no</td>
<td>via</td>
<td>via</td>
<td>via</td>
<td>via</td>
<td>(VPN</td>
<td>(VPN</td>
<td>1 and</td>
<td>1 and</td>
<td></td>
<td>(VPN server)</td>
</tr>
<tr>
<td></td>
<td>local</td>
<td>local</td>
<td>local</td>
<td>local</td>
<td>no</td>
<td>local</td>
<td>local</td>
<td>local</td>
<td>local</td>
<td>server)</td>
<td>server)</td>
<td>router 1</td>
<td>router 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>internet</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>n/a</td>
<td>via</td>
<td>via</td>
<td>via</td>
<td>via</td>
<td>via</td>
<td>via</td>
<td>via</td>
<td>via</td>
<td></td>
<td>no</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Interne</td>
<td>Interne</td>
<td>Interne</td>
<td>Interne</td>
<td>Interne</td>
<td>Interne</td>
<td>Interne</td>
<td>Interne</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To:</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>---</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>t: pub</td>
<td>t: pub</td>
<td>t: pub</td>
<td>t: pub</td>
<td>t: pub</td>
<td>t: pub</td>
<td>t: pub</td>
<td>t: pub</td>
<td></td>
</tr>
<tr>
<td></td>
<td>p2s</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>via Internet</td>
<td>via p2s VPN (VPN server): local via Internet</td>
<td>via p2s VPN (VPN server): local via Internet</td>
<td>via p2s VPN (VPN server): local via Internet</td>
<td>via p2s VPN - NAT (VPN server) via Internet</td>
<td>via p2s VPN - NAT (VPN server) via Internet</td>
<td>via p2s VPN - NAT (VPN server) via Internet</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>direct in cloud: local</td>
<td>via tunnel and local router 1: local</td>
<td>via tunnel and local router 1: local</td>
<td>via VPN server: NAT</td>
<td>via VPN server: NAT</td>
<td>via tunnel and local router 1: NAT</td>
<td></td>
<td>DHCP and DNS protocol s only</td>
</tr>
<tr>
<td></td>
<td>primary</td>
<td>via tunnel</td>
<td>via tunnel and local router 1</td>
<td>via tunnel and local router 1 and 2</td>
<td>via Internet (via VPN server)</td>
<td>no</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>direct in cloud: local</td>
<td>via tunnel and local router 1: local</td>
<td>via tunnel and local router 1: local</td>
<td>via VPN server: NAT</td>
<td>via VPN server: NAT</td>
<td>via tunnel and local router 1: NAT</td>
<td></td>
<td>DHCP and DNS protocol s only</td>
</tr>
<tr>
<td></td>
<td>failover</td>
<td>via tunnel</td>
<td>via tunnel</td>
<td>via tunnel and local router 1</td>
<td>via tunnel and local router 1 and 2</td>
<td>via Internet (via VPN server)</td>
<td>no</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>direct in cloud: local</td>
<td>via tunnel and local router 1: local</td>
<td>via tunnel and local router 1: local</td>
<td>via VPN server: NAT</td>
<td>via VPN server: NAT</td>
<td>via tunnel and local router 1: NAT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>primary</td>
<td>via tunnel</td>
<td>via tunnel</td>
<td>via tunnel</td>
<td>via tunnel</td>
<td>no</td>
<td>via tunnel</td>
<td>via tunnel</td>
<td>direct in</td>
<td>via tunnel</td>
<td>via tunnel</td>
<td>via VPN server:</td>
<td>no</td>
<td>DHCP and DNS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To:</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>---</td>
<td>-----</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>10</td>
<td>failover</td>
<td>via tunnel and local router 1</td>
<td>via tunnel and local router 1</td>
<td>via tunnel and local router 1</td>
<td>via tunnel and local router 1</td>
<td>via tunnel and local router 1</td>
<td>via tunnel and local router 1</td>
<td>via tunnel and local router 1</td>
<td>via tunnel and local router 1</td>
<td>via tunnel and local router 1</td>
<td>via tunnel and local router 1</td>
<td>via tunnel and local router 1</td>
<td>via VPN server: NAT</td>
<td>via test tunnel failover</td>
<td>no</td>
</tr>
<tr>
<td>11</td>
<td>test failover</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>via Internet (via VPN server)</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>direct in cloud: local</td>
<td>via VPN server: local (routin g)</td>
<td>no</td>
</tr>
<tr>
<td>12</td>
<td>test failover</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>via Internet (via VPN server)</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>direct in cloud: local</td>
<td>via VPN server: local (routin g)</td>
<td>no</td>
</tr>
<tr>
<td>13</td>
<td>test failover</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>via Internet (via VPN server)</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>via VPN server: local (routin g)</td>
<td>via VPN server: local (routin g)</td>
<td>no</td>
</tr>
<tr>
<td>To:</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>14 VPN appliance</td>
<td>direct</td>
<td>direct</td>
<td>via local router 1</td>
<td>via local router 2</td>
<td>via Internet (local router 1)</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>15 VPN server</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>
Glossary

C

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.

F

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.

L

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

P

Point-to-site (P2S) connection
A secure VPN connection from outside to the cloud and local sites by using your endpoint devices (such as a computer or laptop).

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 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.

V

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.

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

A
About Cyber Disaster Recovery Cloud 4
Action parameters 70
Active Directory Domain Controller for L2 Open VPN connectivity 29
Active Directory Domain Controller for L3 IPsec VPN connectivity 29
Active point-to-site connections 40
Allowing DHCP traffic over L2 VPN 39
Appendix A. Site-to-site Open VPN - Additional information 73
Automatic deletion of unused customer environments on the cloud site 21

B
Backing up the cloud servers 68

C
Checking the cloud firewall activities 67
Cloud-only mode 12, 32
Cloud network infrastructure 9
Completion check 71
Configuring a Site-to-site Open VPN connection 22
Configuring Cloud-only mode 22
Configuring custom DNS servers 37
Configuring local routing 38
Configuring Multi-site IPsec VPN 24
Configuring Point-to-site remote VPN access 29
Configuring Site-to-site Open VPN 22
Configuring the Multi-site IPsec VPN settings 24
Create a disaster recovery protection plan 7
Creating a primary server 59
Creating a recovery server 45
Creating a runbook 69

D
Deleting custom DNS servers 38
Download configuration for OpenVPN 40
Downloading MAC addresses 38
Downloading the IPsec VPN log files 43

E
Editing the Recovery server default parameters 8
Enabling and disabling the Site-to-site connection 34
Executing a runbook 71

F
Failback to a target physical machine 56
Failback to a target virtual machine 52
Firewall rules for cloud servers 64

G
General recommendations for local sites 26

H
How failback works 51
How failover works 47
How routing works 12, 15, 20
How to perform failover of a DHCP server  51
How to perform failover of servers using local DNS  51

I
Initial connectivity configuration  22
IP address reconfiguration  33
IPsec/IKE security settings  26

L
Limitations  6

M
Managing networks  30
Managing point-to-site connection settings  39
Managing the cloud servers  62
Managing the VPN appliance settings  34
Multi-site IPsec VPN connection  19
Multi-site IPsec VPN log files  43

N
Network management  30
Networking concepts  11

O
Operations with a primary server  61
Operations with runbooks  71
Orchestration (runbooks)  69

P
Performing a failover  49
Performing a test failover  48
Performing failback to a physical machine  57
Performing failback to a virtual machine  53
Point-to-site remote VPN access  20
Ports  22
Prerequisites  24, 30, 37-38, 43, 45, 54, 59
Primary servers  18
Production failover  47
Public and test IP address  16

R
Re-generate configuration  40
Reassigning IP addresses  36
Recommendations for the Active Directory Domain Services availability  29
Recovery servers  16
Requirements for the VPN appliance  22

S
Setting firewall rules for cloud servers  64
Setting up connectivity  11
Setting up primary servers  59
Setting up recovery servers  45
Site-to-site Open VPN connection  13, 30
Software requirements  5
Steps and actions  70
Stopping a runbook execution  72
Supported operating systems  5
Supported virtualization platforms  5
Switching the Site-to-site connection type  35
System requirements  22

T
Test failover  48
The key functionality  4
Troubleshooting IPsec VPN configuration issues  41
Troubleshooting the IPsec VPN configuration  41

V
Viewing the execution history  72
VPN access to local site  40
VPN appliance  15
VPN gateway  15, 19
VPN gateway network configuration  15

W
What to do next  8
Why use runbooks?  69
Working with encrypted backups  58