# Table of contents

1. Introduction - Overview of the solution, what are the benefits for both MSPs and end-users ......................................................................................................................... p. 3
   1.1. Terminology used in the document ........................................................................................................ p. 5
2. Solution diagram / network topology ............................................................................................................... p. 6
3. Network configuration scheme ......................................................................................................................... p. 8
4. Minimum hardware requirements ..................................................................................................................... p. 10
   4.1. MSP nodes ............................................................................................................................................. p. 11
   4.2. Customer node ....................................................................................................................................... p. 12
   4.3. VPN/Monitoring node ............................................................................................................................. p. 13
   4.4. Network / routers .................................................................................................................................... p. 14
5. Configuration how-to’s ...................................................................................................................................... p. 15
   5.1. Installing DSS V7 .................................................................................................................................... p. 17
   5.2. Detailed procedure of setting up MSP nodes ............................................................................................. p. 18
   5.3. Detailed procedure of setting up monitoring for MSP .............................................................................. p. 46
   5.4. Detailed procedure of setting up Customer node ..................................................................................... p. 75
   5.5. Setting up an encrypted connection between MSP and Customer nodes .................................................... p. 80
   5.6. Setting up replication between Customer node and MSP node ................................................................. p. 103
   5.7. Optional procedure for setting up local backup for Customer node ......................................................... p. 109
6. Disaster recovery & data restore ....................................................................................................................... p. 115
   6.1. Disaster recovery ...................................................................................................................................... p. 116
      6.1.1. Without hardware replacement (remote) ............................................................................................. p. 116
      6.1.2. With hardware replacement (on-site) .............................................................................................. p. 119
   6.2. Restoring data from backup ..................................................................................................................... p. 120
      6.2.1. Restoring data set from end-user’s local backup .............................................................................. p. 120
      6.2.2. Restoring a single file from MSP backup ........................................................................................ p. 123
7. Recommendations / troubleshooting ................................................................................................................ p. 126
8. Open-E technical support contact info ........................................................................................................... p. 127
1. Introduction - Overview of the solution, what are the benefits for both MSPs and end-users
1. Introduction - Overview of the solution, what are the benefits for both MSPs and end-users

The Cloud Data Protection Service is a solution for MSPs, System Builders and suppliers of MSPs. It is aimed at any kind of SMB and SME customers, and allowing them to take full advantage of copying data to private clouds and retrieving them when it’s required – without dedicated and costly IT staff.

The concept is simple: The MSP deploys a set of powerful servers powered by Open-E DSS V7 Data Storage Software as a cluster with an additional failover feature pack. This ensures that in case of a hardware failure one node can take over the tasks of the other without interruption. Single servers installed on the customers' premises securely transmit data to the MSP cluster on a regular basis (e.g. hourly) where it is continuously saved and backed up. Customers also have the option to configure additional local backups which adds another layer of security and convenience.

For data recovery, the Cloud Data Protection Service offers customers several options as well. If local backups have been configured, MSP engineers can assist in recovering the files remotely by using an encrypted connection. If anything prevents that from happening, the MSP can also restore the lost files by sending copies via the internet or – in case of a hardware failure or a slow internet connection – the data can be transported physically, on a disk or a replacement server, to the customer’s location.

With this how-to guide we would like to assist you with the initial setup and configuration of the cluster with Active-Active NFS Failover.
1.1. Terminology used in the document

**CDPS (Cloud Data Protection Service)**
Cloud Data Protection Service offers MSP partners the opportunity to keep their customer’s data safe in the fastest, most reliable and cost-effective way.

**MSP (Managed Service Provider)**
An Open-E Partner company which provides Customers with Cloud Data Protection Service.

**MSP nodes**
MSP's data servers which store data backups from Customer nodes.

**VPN/Monitoring node**
MSP’s server running VPN software responsible for creating VPN tunnel, and OMD software responsible for monitoring services on MSP and Customer nodes.

**Customer node**
Customer’s server from which data is backed up to MSP nodes.

**VPN**
A virtual private network in a public network used for encrypted connection and data transmission between Customer nodes and MSP nodes.

**OpenVPN**
Virtual private network software that facilitates the encrypted connection and secure data transfer between Customer nodes and MSP nodes.

**VIP (Virtual IP address)**
An IP address that does not correspond to physical network interface, thus it eliminates a host's dependency upon individual network interfaces.

**Host binding**
Functionality that allows connecting two servers to exchange data between each other. In Cloud Data Protection Service it is used for volume replication between MSP nodes.

**Failover**
Functionality which allows a secondary server to take over the work of the primary one as soon as primary becomes unavailable through either failure or a downtime.

**Auxiliary paths**
Interfaces on which the failover sends a UDP unicast traffic. The auxiliary path will be used to send periodic „heartbeat“ packages to the remote node with the interval equal to keep-alive time, which is set in Failover trigger policy section.
2. Solution diagram / network topology
2. Solution diagram / network topology
3. Network configuration scheme
3. Network configuration scheme

### MSP nodes

- **msp-node-a**
  - eth0: 192.168.20.1
  - eth1: 192.168.10.1
  - eth2: 192.168.11.1
  - eth3: 192.168.12.1

- **msp-node-b**
  - eth0: 192.168.20.2
  - eth1: 192.168.10.2
  - eth2: 192.168.11.2
  - eth3: 192.168.12.2

#### High Availability Cluster

### Customer node

**company-A**

- eth0: 192.168.0.111
- eth1: 10.10.10.11

1Gbit eth0 (192.168.0.111) for access to Open-E DSS V7 web interface and storage from internal network.

1Gbit eth1 (10.10.10.11) for data replication and monitoring.

**company-B**

- eth0: 192.168.1.111
- eth1: 10.10.11.12

1Gbit eth0 (192.168.1.111) for access to Open-E DSS V7 web interface and storage from internal network.

1Gbit eth1 (10.10.11.12) for data replication and monitoring.

### VPN/Monitoring node

- eth0: 192.168.20.100
- eth0: 192.168.10.254
- eth1 (no IP)

1Gbit eth0 (192.168.20.100) for Monitoring WebGUI access, VPN management from Windows client and MSP nodes monitoring.

eth0: 192.168.10.254 for Customer nodes monitoring.

eth1 (no IP) for VPN Bridge and layer 2 communication.
4. Minimum hardware requirements
4. Minimum hardware requirements

4.1. MSP nodes

<table>
<thead>
<tr>
<th>Hardware specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
</tr>
<tr>
<td>Intel® Xeon® processors of the E5-2600 v2 family or better</td>
</tr>
<tr>
<td>RAM</td>
</tr>
<tr>
<td>16GB DDR3 base memory and 350MB additionally for each Customer node</td>
</tr>
<tr>
<td>Hard disk drive</td>
</tr>
<tr>
<td>2x RAID 5 (alternatively, RAID 6 or RAID 10) disk arrays, 8 hard drives each</td>
</tr>
<tr>
<td>Ethernet</td>
</tr>
<tr>
<td>2 x 10GbE</td>
</tr>
<tr>
<td>2 x 1GbE</td>
</tr>
</tbody>
</table>

**Note:** Although running MSP Server with minimum hardware requirements allow to fully utilize all CDPS functionalities, we recommend **Fujitsu PRIMERGY SX350 S8** which is tested by Open-E and proved to be highly reliable and efficient when used for CDPS service.
4. Minimum hardware requirements

4.2. Customer node

<table>
<thead>
<tr>
<th>Hardware specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
</tr>
<tr>
<td>RAM</td>
</tr>
<tr>
<td>Hard disk drive</td>
</tr>
<tr>
<td>RAID Controller</td>
</tr>
<tr>
<td>Ethernet</td>
</tr>
</tbody>
</table>

**Note:** Although running MSP Server with minimum hardware requirements allow to fully utilize all CDPS functionalities, we recommend Fujitsu PRIMERGY TX1310M1 which is tested by Open-E and proved to be highly reliable and efficient when used for CDPS service.
4. Minimum hardware requirements

4.3. VPN/Monitoring node

<table>
<thead>
<tr>
<th>Server</th>
<th>PC running Ubuntu 14.04 LTS with the following hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware specification</td>
<td></td>
</tr>
<tr>
<td>Processor</td>
<td>6-core with Hyper-Threading 3.0 GHz or better</td>
</tr>
<tr>
<td>RAM</td>
<td>16GB with ECC support</td>
</tr>
<tr>
<td>Hard disk drive</td>
<td>2-disk RAID 1 array</td>
</tr>
<tr>
<td>Ethernet</td>
<td>2 x 1GbE network interface</td>
</tr>
</tbody>
</table>

**Note:** Although our recommendations don't indicate a specific server or vendor, please make sure your monitoring server is able to work 24/7, and is reliable enough to handle that kind of load.
4. Minimum hardware requirements

4.4. Network / routers

In this manual ASUS RT-AC68U (firmware 3.0.0.4.378_9135) is used to set up an encrypted connection between MSP and Customer nodes. Although it is not required, we recommend to use a router of similar specification with build-in OpenVPN support.
5. Configuration how-to's
5. Configuration how-to’s

In this chapter, you will learn how to configure Cloud Data Protection Service by MSP, according to Solution diagram introduced in Chapter 2 of this manual. You will be given instructions on how to set up:

- MSP nodes
- Customer node
- VPN/Monitoring node
- Encrypted connection between MSP nodes and Customer node
5.1. Installing DSS V7

Please note that each MSP node as well as Customer node is running on Open-E DSS V7. As this manual will not guide you through DSS V7 installation process, we encourage you to follow:


It is highly recommended to install the latest version of Open-E DSS V7 software which can be found on [http://www.open-e.com/download/open-e-data-storage-software-v7/](http://www.open-e.com/download/open-e-data-storage-software-v7/)
Prerequisites
Please complete the following prerequisites.

- Two servers meet the hardware requirements for MSP nodes introduced in Chapter 4 – Minimum hardware requirements
- Open-E DSS V7 up54 build 18432 installed on both servers

If all the prerequisites have been met, you’re now ready to start MSP nodes configuration.

5.2.1. MSP first node configuration

Step 1.

Go to Setup » Network interfaces and change the server name and hostname to msp-node-a. Click apply to confirm the changes.

Note: Changing the hostname requires a reboot of the system.
5.2. Detailed procedure of setting up MSP nodes

Step 2.

Go to Setup » Network interfaces and configure Ethernet ports. Click apply to confirm the changes.

In this example we recommend configuring four Ethernet ports as follow:

- 1Gbit eth0 (192.168.20.1) for access to Open-E DSS V7 web interface
- 10Gbit eth1 (192.168.10.1) for volume replication between MSP nodes
- 1Gbit eth2 (192.168.11.1) for VIP and data replication via VPN
- 10Gbit eth3 (192.168.12.1) for VIP for internal MSP network

Note: Changing network interface IP address will restart the network configuration on this node.
5.2. Detailed procedure of setting up MSP nodes

Note: The IP addresses used in this example are for the purpose of this manual only. You should configure your Ethernet ports according to your network topology.
5.2. Detailed procedure of setting up MSP nodes

**Step 3.**

Go to Configuration » Volume manager » Volume groups.

a. From the Unit manager, select a disk to create the volume group.
b. Enter a name for the volume group (in this example, the volume name is vg00).
c. Click the apply button.

**Step 4.**

Repeat the previous step in order to create the second volume group (in this example, the volume name is vg01).
5.2. Detailed procedure of setting up MSP nodes

After volume groups are created you can see them listed in the volume groups menu on the left side.

**Step 5.**

Select **vg00** from the list on the left side. Next, create new NAS volume of size that is appropriate for the data set (in this example, the volume name is **lv0000**).

a. Make sure that **Use volume replication** option is checked.
b. Set a size for the volume.
c. Click **apply** button.

**Please note** that the size of the volume in this example is for only this manual. Your volumes size should be always tailored to the size of data set.
5.2. Detailed procedure of setting up MSP nodes

Configuration how to's

Step 6.
Select vg01 from the list on the left side. Next, create new NAS volume of size that is appropriate for the data set (in this example, the volume name is lv0100).

a. Make sure that Use Volume replication option is checked.
b. Set a size for the volume.
c. Click apply button.

Step 7.
Go to Configuration » NAS settings and check Use NFS option in NFS settings box. Click apply button.
5.2. Detailed procedure of setting up MSP nodes

Step 8.

Go to Configuration » NAS resources » Shares and create a share for data to be replicated from a Customer node.

a. Enter a name for the share (in this example, the share name is copy-data-company-A).
b. Select lv0000 as a default path for the share.
c. Click apply button.

Step 9.

Create a share for data to be replicated from another Customer node (Note: This step is required only in case you have more than one Customer node from which data will be replicated).

a. Enter a name for the share (in this example, the share name is copy-data-company-B).
b. Select lv0100 as a default path for the share.
c. Click apply button.
5.2. Detailed procedure of setting up MSP nodes

**Step 10.**

Select a **copy-data-company-A** share from the list on the left side.

a. Navigate to SMB settings.
b. Uncheck **Use SMB** option.
c. Click **apply** button.

**Step 11.**

Next, navigate to the NFS share access box.

a. Check **Use NFS** option.
b. Make sure **Synchronous** option is checked.
c. Click **apply** button.
5.2. Detailed procedure of setting up MSP nodes

Step 12.
Select `copy-data-company-B` from the menu on the left side.

a. Navigate to SMB settings.
b. Uncheck the `Use SMB` option.
c. Click the `apply` button.

Step 13.
Next, navigate to the NFS share access box.

a. Check the `Use NFS` option.
b. Make sure the `Synchronous` option is checked.
c. Click the `apply` button.
5.2. Detailed procedure of setting up MSP nodes

5.2.2. MSP second node configuration

Step 1.

Go to Setup » Network interfaces and change server name and hostname to **msp-node-b**. Click **apply** to confirm the changes.

**Note:** Changing the hostname requires a system reboot.

Step 2.

Go to Setup » Network interfaces and configure Ethernet ports. Click **apply** to confirm the changes.

In this example we recommend configuring four Ethernet ports as follow:

- 1Gbit eth0 (192.168.20.2) for access to Open-E DSS V7 web interface
- 10Gbit eth1 (192.168.10.2) for volume replication between MSP nodes
- 1Gbit eth2 (192.168.11.2) for VIP and data replication via VPN
- 10Gbit eth3 (192.168.12.2) for VIP for internal MSP network

**Note:** Changing network interface IP address will restart the network configuration on this node.
5.2. Detailed procedure of setting up MSP nodes

Note: The IP addresses used in this example are for the purpose of this manual only. You should configure your Ethernet ports according to your network topology.
5.2. Detailed procedure of setting up MSP nodes

Step 3.

Go to Configuration » Volume manager » Volume groups.

a. From the Unit manager, select a disk to create the volume group.
b. Enter a name for the volume group (in this example, the volume name is `vg00`).
c. Click apply button.
5.2. Detailed procedure of setting up MSP nodes

Step 4.

Repeat the previous step in order to create the second volume group (in this example, the volume name is `vg01`).

After volume groups are created you can see them listed in the volume groups menu on the left side.
5.2. Detailed procedure of setting up MSP nodes

**Step 5.**
Select `vg00` from the list on the left side. Next, create new NAS volume of size that is appropriate for the data set (in this example, the volume name is `lv0000`).

a. Make sure that **Use Volume replication** option is checked.
b. Set a size for the volume.
c. Click **apply** button.

Please note that the size of the volume in this example is for purpose of this manual. Your volumes size should be always tailored to the size of data set.

**Step 6.**
Select `vg01` from the list on the left side. Next, create new NAS volume of size that is appropriate for the data set (in this example, the volume name is `lv0100`).

a. Make sure that **Use Volume replication** option is checked.
b. Set a size for the volume.
c. Click **apply** button.
5.2. Detailed procedure of setting up MSP nodes

Step 7.

Go to Configuration » NAS settings.

a. Check Use NFS option in NFS settings box.
b. Click apply button.

Step 8.

Go to Configuration » NAS resources » Shares and create a share for data to be replicated from the Customer node.

a. Enter a name for the share (in this example, the share name is copy-data-company-A).
b. Select lv0000 as a default path for the share.
c. Click apply button.
5.2. Detailed procedure of setting up MSP nodes

Step 9.

Create a share for the data to be replicated from the another Customer node (Note: This step is required only in case you have more than one Customer node from which data will be replicated).

a. Enter a name for the share (in this example, the share name is copy-data-company-B).

b. Select lv0100 as a default path for the share.

c. Click **apply** button.

Step 10.

Select copy-data-company-A share from the list on the left side.

a. Navigate to SMB settings.

b. Uncheck **Use SMB** option.

c. Click **apply** button.
5.2. Detailed procedure of setting up MSP nodes

Step 11.
Next, navigate to NFS share access box.

a. Check Use NFS option.
b. Make sure Synchronous option is checked.
c. Click apply button.

Step 12.
Select copy-data-company-B from the menu on the left side.

a. Navigate to SMB settings.
b. Uncheck Use SMB option.
c. Click apply button.
5.2. Detailed procedure of setting up MSP nodes

Step 13.

Next, Navigate to NFS share access box.

a. Check Use NFS option.
b. Make sure Synchronous option is checked.
c. Click apply button.
5.2. Detailed procedure of setting up MSP nodes

5.2.3. Setting up volume replication between MSP nodes

Step 1.

On the msp-node-a, go to Configuration » Volume manager » Volume replication.

a. Set a source Volume replication mode for lv0000 and destination volume replication mode for lv0100.
b. Click apply button.

Step 2.

On msp-node-b, go to Configuration » Volume manager » Volume replication.

a. Set source volume replication mode for lv0100 and destination volume replication mode for lv0000.
b. Click apply button.
5.2. Detailed procedure of setting up MSP nodes

Step 3.

Go back to msp-node-a and configure host binding and volume replication path between MSP nodes (in this example msp-node-a is bound with msp-node-b).

After both nodes are bound, you will see binding status like on the screenshot on the left.
5.2. Detailed procedure of setting up MSP nodes

**Step 4.**

On **msp-node-a** navigate to Create new volume replication task box and create new volume replication task.

a. Enter task name (in this example, the task name is **task-lv0000**).
b. Select source volume (in this example, source volume is **lv0000**).
c. Select destination volume on MSP second node (in this example, destination volume is **lv0000**).
d. Click **create** button.

**Step 5.**

On **msp-node-b** navigate to Create new volume replication task and create new volume replication task.

a. Enter task name (in this example, the task name is **task-lv0100**).
b. Select source volume (in this example, source volume is **lv0100**).
c. Select destination volume on MSP second node (in this example, destination volume is **lv0100**).
d. Click **create** button.
5.2. Detailed procedure of setting up MSP nodes

Step 6.

Next, run replication task **task-lv0100**.

Step 7.

Go to the **msp-node-a** and run replication task **task-lv0000**.
5.2. Detailed procedure of setting up MSP nodes

5.2.4. Setting up and running Failover service

Step 1.

On msp-node-a go to Setup » Failover.

Step 2.

Add two auxiliary paths.

Note: The interface on both local and remote node has to be on the same network subnet.

a. Select interface on local and remote node for the first new auxiliary path (in this example eth2 on local node and eth2 on remote node).
b. Click **add new auxiliary** path button.
c. Select interface on local and remote node for the second new auxiliary path (in this example eth3 on local node and eth3 on remote node).
d. Click **add new auxiliary path** button.
5.2. Detailed procedure of setting up MSP nodes

Step 3.

Add two ping nodes.

a. Add first ping node (in this example, the ping node is 192.168.11.50).
b. Click the add new ping node button.
c. Add second ping node (in this example, the ping node is 192.168.12.50).
d. Click the add new ping node button.
5.2. Detailed procedure of setting up MSP nodes

Step 4.

Go to the Resources Pool Manager and add a virtual IP address in msp-node-a-resources section.

a. Enter virtual IP address appropriate for your network configuration (in this example virtual IP address is 10.10.10.1).
b. Select interface on local node for virtual IP address (in this example, eth2 192.168.11.1).
c. Select interface on remote node for virtual IP address (in this example, eth2 192.168.11.2).
d. Enter netmask (in this example, netmask is 255.255.255.0).
e. Click add button.

Step 5.

Next, Add another virtual IP address in msp-node-a-resources section.

a. Enter virtual IP address appropriate for your network configuration (in this example virtual IP address is 20.20.20.1).
b. Select interface on local node for virtual IP address (in this example, eth3 192.168.12.1).
c. Select interface on remote node for virtual IP address (in this example, eth3 192.168.12.2).
d. Enter netmask (in this example, netmask is 255.255.255.0).
e. Click add button.
5.2. Detailed procedure of setting up MSP nodes

Step 6.

Next, navigate to NFS resources tab in msp-node-a-resources section.

a. Move task-lv0000 from Available NFS tasks to Tasks already in cluster.
b. Click apply button.

Step 7.

Navigate to the Resources Pool Manager and add a virtual IP address in msp-node-b-resources section.

a. Enter virtual IP address appropriate for your network configuration (in this example virtual IP address is 10.10.11.1).
b. Select interface on local node for virtual IP address (in this example, eth2 192.168.12.1).
c. Select interface on remote node for virtual IP address (in this example, eth2 192.168.12.2).
d. Enter netmask (in this example, netmask is 255.255.255.0).
e. Click add button.
5.2. Detailed procedure of setting up MSP nodes

Step 8.

Next, Add another virtual IP address in **msp-node-b-resources** section.

a. Enter virtual IP address appropriate for your network configuration (in this example virtual IP address is 20.20.21.1).
b. Select interface on local node for virtual IP address (in this example, eth3 192.168.12.1).
c. Select interface on remote node for virtual IP address (in this example, eth3 192.168.12.2).
d. Enter netmask (in this example, netmask is 255.255.255.0).
e. Click **add** button.

Step 9.

Navigate to **NFS resources tab**.

a. Move **task-lv0100_reverse** from Available NFS tasks to Tasks already in cluster.
b. Click **apply** button.
5.2. Detailed procedure of setting up MSP nodes

Step 10.

Go to **Failover manager** and click **start** button in order to run the Failover service.
5.3. Detailed procedure of setting up monitoring for MSP

MSP node and Customer node monitoring is carried out by the VPN/Monitoring node (see Chapter 2 - Solution diagram / network topology). The VPN/Monitoring node is a single node running Ubuntu Server 14.04 LTS with OMD (Open Monitoring Distribution) software installed.

Note that the following steps describe how to set up a monitoring for MSP node. If you want to set up monitoring for Customer node, first you have to configure an encrypted connection between MSP and Customer according to Chapter 5.5 - Setting up encrypted connection between MSP and Customer nodes.

Prerequisites
Please complete the following prerequisites.

- Server meets requirements for VPN/Monitoring node introduced in Chapter 4 – Minimum hardware requirements
- Ubuntu Server 14.04 LTS installed on the server
- Ubuntu standard user account with sudo privileges
- MSP nodes configured according to procedure introduced in Chapter 5.2 – Detailed procedure of setting up MSP nodes

If all the prerequisites have been met, you’re now ready to start VPN/Monitoring node configuration.

The following steps show how to configure monitored node (in this example, the monitored node is MSP node), install OMD package on VPN/Monitoring node and finally, access and use the monitoring interface.
5.3. Detailed procedure of setting up monitoring for MSP

5.3.1. Installing and configuring OMD on MSP VPN/Monitoring node

In order to install OMD package on MSP VPN/Monitoring node please follow the steps below:

**Step 1.**
From a root level (use “sudo -i” in order to login as root), update repositories index and upgrade system software using the following commands:

```
apt-get update
apt-get upgrade
```

**Step 2.**
In order to install the OMD package, go to [https://labs.consol.de/repo/stable/](https://labs.consol.de/repo/stable/) and choose the relevant version of the repository (in our case it will be “Ubuntu Trusty 14.04”).

**Step 3.**
Install the relevant GPG key in Ubuntu.

```
gpg --keyserver keys.gnupg.net --recv-keys F8C1CA08A57B9ED7
```

```
gpg --armor --export F8C1CA08A57B9ED7 | apt-key add -
```

**Step 4.**
Next, enable the stable release repository (in our case, it is the one dedicated to Ubuntu Trusty 14.04):

```
echo 'deb http://labs.consol.de/repo/stable/ubuntu trusty main' >> /etc/apt/sources.list
```
5.3. Detailed procedure of setting up monitoring for MSP

**Step 5.**
Run apt-get update to refresh our distribution repositories.

```
apt-get update
```

**Step 6.**
Install the OMD.

```
apt-get install omd
```

**Step 7.**
Create a new site (in this example it is “dssmonitor”).

```
omd create dssmonitor
```

What you get is:
- a site directory with preconfigured configuration files
- a new user "dssmonitor" and a new group “dssmonitor” (identical with the name of your site). The new user is also a member of the group omd, which is created during installation.
5.3. Detailed procedure of setting up monitoring for MSP

5.3.2. Configuring monitored node

Applying the small update to monitored node

Note: Applying small update is not required if you are using Open-E DSS V7 version v7.0up53 or above.

Go to the node you want to monitor (in our example, the node is msp-node-a) and perform the following steps:

Click: http://kb.open-e.com/How-can-I-obtain-and-apply-a-small-update-to-my-Open-E-software_63.html, to find out how to obtain small updates. Please note, it is always best to confirm it with our technical support, before installing any updates to your system.

Click Choose File to pick the small update upd_70139-DSS-V7.upd, then click on upload and accept.

You will then need to manually restart the system.
5.3. Detailed procedure of setting up monitoring for MSP

Step 3.

Go to Maintenance » Shutdown » System Restart and click the restart button in order to reboot the server.

After installation, the small update will be visible in the System software update menu (it can be removed by clicking on the trash bin).
5.3. Detailed procedure of setting up monitoring for MSP

Enabling API on monitored node

Go to a node you want to monitor (in our example, the node is MSP primary node) and perform the following steps:

Step 4.

Go to Setup » Administrator settings then navigate to CLI/API Configuration.

Step 5.

Enable CLI/API, then specify port – 22223 and password.

Step 6.

Click apply button.

Step 7.

In order to use the CLI/API functionality without password, you need to generate ssh key. You can do it by expanding show advanced menu and clicking on the generate and download button.
5.3. Detailed procedure of setting up monitoring for MSP

5.3.3. Adding a monitored node to OMD

**Step 1.**

On the VPN/Monitoring node, create a file with an ssh key (downloaded while enabling CLI/API functionality on monitored node) in the omd directory.

**Note:** We use a *nano* editor to create and edit the key file (in this example, the key file name is dss.key).

```
cd /omd
nano dss.key
```

Next, copy the ssh key from the downloaded file and paste it to the `dss.key` file.

After the ssh key is copied, use `Ctrl+O`. Next, click Enter to save the dss.key file and then `Ctrl+X` to close nano editor.

**Tip:** in order to check whether the dss.key file was created type ls. You should see the dss.key listed under the omd directory.
5.3. Detailed procedure of setting up monitoring for MSP

Step 2.
The important part is to ensure the correct ownership is set (our OMD user) and access permission (read and execute for owner only) for our ssh key. To change the owner of our ssh key file, we use the following command:

```
chown dssmonitor /omd/dss.key
```

Step 3.
To change access permission, so only the owner has read and execute rights, we use:

```
chmod 500 /omd/dss.key
```

Step 4.
Then, we log to OMD as dssmonitor using “su” command:

```
su dssmonitor
```

Step 5.
In order to add monitored server (192.168.20.1) to Check_MK list of known hosts, run the following ssh command (type yes and press Enter when asked):

```
ssh -p 22223 -i /omd/dss.key -l api 192.168.20.1 check_mk_agent
```

Step 6.
Log out from dssmonitor account (Ctrl + D). From root level (use “sudo -i” in order to login as root), start the omd on newly created site:

```
OMD start dssmonitor
```
5.3. Detailed procedure of setting up monitoring for MSP

Step 7.

Go to your internet browser and log in to the OMD web interface by typing `monitoring_server_ip_address/dssmonitor/` (in this example, the VPN/Monitoring node ip address is 192.168.20.100).

Use `omdadmin` as username and `omd` as your password.

Step 8.

From the available web interfaces, choose Check_MK Multisite.

Step 9.

Go to Hosts in the WATO Configuration section on the left side.
5.3. Detailed procedure of setting up monitoring for MSP

Step 10.
In order to create a new host (server to be monitored) click the Create new host button.

Step 11.
a. Enter a name for the host (in this example, the hostname is msp-node-a).
b. Enter host IP address (in this example, IP address is 192.168.20.1).
c. Make sure that Agent type is Check_MK Agent (Server).
d. Click the Save&Test button.
5.3. Detailed procedure of setting up monitoring for MSP

Step 12.

Go to Datasource Program rules by clicking the Rules link in the Options panel on the left side.

If you don’t see a screen like the one on the left, click Hosts in WATO Configuration section on the left side. Next, click the relevant hostname and then the Diagnostic button.

Step 13.

Click Create rule in folder button.
5.3. Detailed procedure of setting up monitoring for MSP

Step 14.

In **Conditions** section mark the **Specify explicit host names** checkbox and enter a name for the host you want to create the rule for (in this example, the hostname is a *msp-node-a*).

Next, enter the command for the rule to execute (in this example, the command is as follow: `ssh -p 22223 -i /omd/dss.key -l api 192.168.20.1 check_mk_agent`).

Click **Save** button.

After the rule is created you will see it listed in a **Rules in folder Main directory** table.
5.3. Detailed procedure of setting up monitoring for MSP

**Step 15.**
Activate the changes in the configuration. Click the Changes button at the top.

Click **Activate changes** button.

**Step 16.**
Click the Hosts in the WATO Configuration section on the left side. Next, click the relevant hostname and then click the Services button. Enable services you want to monitor by marking the respective checkboxes. In order to select all services at once, click the Activate Missing button above the services list.
5.3. Detailed procedure of setting up monitoring for MSP

5.3.4. Monitoring a node

Step 1.
Go to Hosts » All Hosts in Views section on the left side.

Step 2.
Select host you want to monitor (in this example, the host is msp-node-a).

You will then see the statuses of all available services (that are being monitored by the tool). Wait until all statuses are up-to-date. If you want to refresh a particular status immediately use refresh icon:

In order to monitor both replication and backup tasks running we highly recommend configuring email notifications in Open-E DSS V7. In order to configure email notifications, go to Open-E DSS V7 web interface, navigate to Setup » Administrator settings and enable the Send errors option in the E-mail notification box.
5.3. Detailed procedure of setting up monitoring for MSP

5.3.5. Setting up warning and critical levels for monitored parameters

**Step 1.**

Go to Services » All services in the Views section on the left side.

**Step 2.**

Click the icon to edit parameters for the selected service (in this example, we will set edit parameters for CPU utilization).
5.3. Detailed procedure of setting up monitoring for MSP

**Step 3.**
Click **CPU utilization on Linux/UNIX**.

**Step 4.**
Create a rule for CPU utilization on Linux/UNIX. From this screen you can create a rule for a single host (**Create host specific rule for**), or for all monitored hosts (**Create rule in folder**). In this example we create a rule for all hosts.

1. Select a directory for the rule (in this example, directory in **Main directory**).
2. Click **Create rule in folder** button.
5.3. Detailed procedure of setting up monitoring for MSP

Step 5.

Set the levels for parameters.

1. Navigate to the **Parameters** box.
2. Select which parameters you want to monitor.
3. Set the levels for your selected parameters.
4. Click the **Save** button.

Step 6.

Activate the changes made in your configuration.
Click the **Changes** button at the top and then click **Activate changes**.
From now on, Check_MK will monitor all selected parameters according to the set levels.
### 5.3. Detailed procedure of setting up monitoring for MSP

#### Configuration how to’s

#### 5.3.6. Both Provider and Client side monitoring parameters

<table>
<thead>
<tr>
<th>Monitored parameter</th>
<th>Description</th>
<th>Warning</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU utilization</td>
<td>Percentage of CPU used with graphs</td>
<td>70%</td>
<td>90%</td>
</tr>
<tr>
<td>CPU load</td>
<td>Linux ‘load average’ parameter, last 1, 5, 15 minutes (with graphs)</td>
<td>2 per core</td>
<td>3 per core</td>
</tr>
<tr>
<td>Memory</td>
<td>Percentage of RAM used with graphs</td>
<td>80%</td>
<td>90%</td>
</tr>
<tr>
<td>Disk (partition) and shares usage</td>
<td>Separate monitoring for each disk (partition) including swap utilization as well as all shares available with graphs for each one monitored</td>
<td>80%</td>
<td>90%</td>
</tr>
<tr>
<td>Disk IO summary</td>
<td>Disk IO in MB/s with graphs (warning and critical depend on system, adjust after observing it's normal behaviour)</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>RAID status</td>
<td>RAID controller status information (warning and critical depend on controller type and plugin used)</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>RAID BBU Status</td>
<td>RAID Backup Battery Unit status (Operation mode, Charged percent)</td>
<td>&lt; 100%</td>
<td>&lt; 95%</td>
</tr>
<tr>
<td>Network utilization</td>
<td>Each network interface utilization with graphs</td>
<td>70%</td>
<td>90%</td>
</tr>
<tr>
<td>CPU cores temperature</td>
<td>Each CPU core temperature with graphs (exact warning and critical values depend on server). Values for Intel E5-2630 v2.</td>
<td>60 C</td>
<td>74 C</td>
</tr>
<tr>
<td>TCP connections</td>
<td>With graphs</td>
<td>400</td>
<td>800</td>
</tr>
<tr>
<td>Uptime</td>
<td>With graphs</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Replication to MSP</td>
<td>Replication to MSP server status (small update required)</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>
5.3. Detailed procedure of setting up monitoring for MSP

5.3.7. Configuring OMD email notifications

The following steps 1-4 are not mandatory, however, we recommend to change the hostname as most of email providers block emails from host domain names that don't match the IP address used to send a message. If you don't want to change the hostname, proceed to step 5.

**Step 1.**

From the root level (use “sudo -i” in order to login as root), edit `/etc/hosts` file.

*Note:* We use a nano editor to edit the file.

```
 nano /etc/hosts
```

**Step 2.**

Change the Ubuntu default hostname to Fully Qualified Domain Name (FQDN) pointing to the WAN IP address of the router which the mailserver is using. It's necessary to avoid mail being rejected by some mail servers.

Use **Ctrl+O** and click **Enter** to save the file. Then **Ctrl+X** to close the nano editor.
5.3. Detailed procedure of setting up monitoring for MSP

Step 3.
Edit `/etc/hostname` and change the Ubuntu default hostname to Fully Qualified Domain Name (FQDN) entered in the previous step.

```
nano /etc/hostname
```

Use Ctrl+O and click Enter to save the file. Then Ctrl+X to close nano editor.

Step 4.
Reboot the system.

```
reboot
```

Step 5.
Install a software for handling emails (in this example, `mailutils` package is used). Installing mailutils will cause Postfix to be installed, as well as a few other programs needed for Postfix to work.

```
apt-get install mailutils
```
5.3. Detailed procedure of setting up monitoring for MSP

**Step 6.**

Near the end of the installation process, you will be asked to select the mail server configuration type. Select *Internet Site*.

**Step 7.**

Accept the System mail name unless you didn’t specify it in the previous steps.
5.3. Detailed procedure of setting up monitoring for MSP

Step 8.
Edit the Postfix configuration file.

```
nano /etc/postfix/main.cf
```

Step 9.
Scroll down and change the line `inet_interfaces = all` to `inet_interfaces = localhost`.

The edited section of the file should now read as shown below. Use Ctrl+O and click Enter to save the file. Then Ctrl+X to close the nano editor.

```
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/128 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = localhost
inet_protocols = all
```

Step 10.
Restart Postfix.

```
service postfix restart
```

Step 11.
Check whether Postfix can send emails to any external email account. To send a test email, type:

```
echo "Mailbody" | mail -s "Test email subject" test@example.com
```
5.3. Detailed procedure of setting up monitoring for MSP

Step 12.
Go to the Check_MK web interface and navigate to Contact Groups in the WATO Configuration section on the left side. Then, click the New contact group button.

Step 13.
Navigate to the Properties box and specify name and alias for the group (in this example the group name is Group 1 and the alias is Group 1 alias).
5.3. Detailed procedure of setting up monitoring for MSP

Step 14.
After the group is created, go to Host&Service Parameters in the WATO Configuration section on the left side and click the Grouping button.

Step 15.
Click the Assignment of hosts to contact groups.
5.3. Detailed procedure of setting up monitoring for MSP

Step 16.
Click Create rule in folder button.

Step 17.
Specify the host name for the rule and assign a host to the contact group (in this example the hostname is msp-node-a and the contact group is Group 1 Alias).
5.3. Detailed procedure of setting up monitoring for MSP

How-To Guide: Cloud Data Protection Service by MSP

Configuration how to's

Step 18.

Go to Users in the WATO Configuration section on the left side.

Step 19.

Create a new user:

a. Enter a username (in this example the username is user1).
b. Enter full name for the user (in this example, it is John Smith).
c. Enter a user email address (in this example, email is johnsmith@open-e.com).
d. Select the type of authentication (in this example, Normal user login with password is selected) and set a password.
e. Select a role for the user (in this example, Administrator is selected).
f. Assign the user to a contact group (in this example a user is assigned to Group1 Alias).
g. Click the Save button.
5.3. Detailed procedure of setting up monitoring for MSP

After the user is added, you will see it listed on the Users list.

Step 20.

Activate the changes made in the configuration. Click the Changes button at the top.

Then click the Activate changes button.
5.3. Detailed procedure of setting up monitoring for MSP

**Step 21.**

Go to All services in the Views section on the left side and select a service you want to send with notifications (in this example, the service is CPU utilization).

**Step 22.**

Click the hammer icon on the top.
5.3. Detailed procedure of setting up monitoring for MSP

**Step 23.**
Scroll down to the Various Commands section:
- a. Enter a comment for Custom notification (in this example, the comment is Test notification).
- b. Click Send button.

**Step 24.**
Confirm that you want to send a test notification.

**Step 25.**
Check the Check_MK log files in order to verify if email notifications are being delivered. To do so, execute the following commands:

```
tail /omd/sites/dssmonitor/var/log/notify.log

tail /omd/sites/dssmonitor/var/log/nagios.log
```

If the log files don't record that a test notification was sent, check your mailserver configuration.
5.4. Detailed procedure of setting up Customer node

Prerequisites
Please complete the following prerequisites.

- Server meets requirements for Customer node introduced in Chapter 4 – Minimum hardware requirements
- Open-E DSS V7 NAS for CDPS installed on the node
- MSP nodes configured according to procedure introduced in Chapter 5.2 – Detailed procedure of setting up MSP nodes

If all the prerequisites have been met, you’re now ready to start the Customer node configuration.

Step 1.
Go to Setup » Network interfaces and change server name and hostname to company-a.

Click apply to confirm the changes.

Note: Changing the hostname requires the system to reboot.
Step 2.

Go to **Setup » Network interfaces** and configure the Ethernet ports. Click **apply** to confirm the changes.

**It is recommended** to configure two interfaces:
- 1 Gbit interface for access to the Open-E DSS V7 web interface
- 1 Gbit interfaces for data replication

In this example interfaces are used as follows:
- eth0 is used for web access to Open-E DSS V7
- eth1 is used for data replication

**Note:** Changing the network interface IP address will restart the network configuration on this node.

**Note:** The IP addresses used in this example are for the purpose of this manual only. You should configure your Ethernet ports according to your network topology.
5.4. Detailed procedure of setting up Customer node

**Step 3.**

Go to Configuration » Volume manager » Volume groups.

a. To create a volume group, select a disk from the Unit manager.
b. Enter a name for the volume group (in this example, the volume name is `vg00`).
c. Click *apply* button.

**Step 4.**

Select `vg00` from the menu on the left side.

a. Create new NAS volume (in this example, the volume name is `lv0000`).
b. Click *apply* button.
5.4. Detailed procedure of setting up Customer node

Step 5.

Create snapshots assigned to the NAS volume lv0000 created in step 5.

It is recommended to create snapshots of a size that is at least 20% of the NAS volume size to which it is assigned.

It is highly recommended to monitor snapshot use. If the snapshot capacity is exceeded the system may become unstable.

Step 6.

Go to Configuration » NAS settings.

a. Check the Enable Data (file) replication agent.

b. Click apply button.
5.4. Detailed procedure of setting up Customer node

Step 7.

Go to Configuration » NAS resources » Shares and create a share for data that will be replicated from the Customer node to the MSP node.

a. Enter a name for the share (in this example, the share name is data-company-A).

b. Select lv0000 as a default path for the share.

c. Click apply button.

Note: There is an option to configure a local backup for the Customer node. For more details proceed to Chapter 5.7 - Optional procedure for setting up local backup for Customer node.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Prerequisites
Please complete the following prerequisites.

- MSP VPN/Monitoring node configured according to procedure introduced in Chapter 5.2 – Detailed procedure of setting up MSP nodes
- Customer node configured according to procedure introduced in Chapter 5.4 – Detailed procedure of setting up Customer node
- Router meets requirements introduced in Chapter 4 – Minimum hardware requirements or a router of your choice with built-in OpenVPN support.
- A computer running Windows to configure VPN software

If all the prerequisites have been met, you're now ready to start the configuration. The following step shows how to configure the VPN software used for the encrypted connection between MSP and Customer node. SoftEther VPN is an easy-to-use multi-protocol VPN software running on Windows, Linux, Mac, FreeBSD and Solaris. Learn more on www.softether.org.

5.5.1. MSP VPN/Monitoring node configuration

The following steps show how to configure the SoftEther VPN Server software on the MSP VPN/Monitoring node.

Step 1.

Go to http://www.softether-download.com/ and search for the SoftEther VPN Server version dedicated for your CPU and operating system combination.

a. Select SoftEther VPN Server as a component to download.
b. Select your platform (in this example, Linux is selected).
c. Select your CPU (in this example, Intel x64/AMD64 (64bit) is selected).
d. Search for the latest "rtm" version (in this example, SoftEther VPN Server (Ver 4.18, Build 9570, rtm) is used).

Step 2.

From root level (use “sudo -i” in order to login as root) download SoftEther VPN Server.

```
```

Note: The file name to download may be different, depending on your operating system and CPU combination.
5.5. Setting up an encrypted connection between MSP and Customer nodes

After the download is completed, the output should be as shown on the left side.

**Tip:** In order to check whether the software was downloaded type “ls”. You should see `SoftEther_VPN_Server/64bit_-_Intel_x64_or_AMD64/softether-vpnservr-v4.18-9570-rtm-2015.07.26-linux-x64-64bit.tar.gz` listed in the root directory.

**Step 3.**

Install the software essential to compile SoftEther VPN Server.

```
apt-get install build-essential
```
5.5. Setting up an encrypted connection between MSP and Customer nodes

When the system asks if you want to continue, type “Y” and press Enter. Installation starts.

**Step 4.**

Extract the package with the SoftEther VPN software.

```
tar zxf softether-vpnserver-v4.18-9570-rtm-2015.07.26-linux-x64-64bit.tar.gz
```

Type ls in order to check if the package was extracted and the vpnserver directory was created.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Configuration how to's

Step 5.

Go to the vpnserver directory and compile the software.

```bash
cd vpnserver
make
```

After the software is compiled, the output should be as on the left.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Step 6.
Make a startup script for the SoftEther VPN software.

```
nano /etc/init.d/vpnserver
```

**Note:** We use nano editor to edit the file.

Paste the code from the left into the `/etc/init.d/vpnserver` file.
5.5. Setting up an encrypted connection between MSP and Customer nodes

After editing, the `/etc/init.d/vpnserv` file should look like on the screenshot.

Use Ctrl+O and click Enter to save the file. Then Ctrl+X to close nano editor.

**Note:** In this example we installed VPN server in the /root directory. If you installed the software in a different location you have to change DAEMON=/root/vpnserv/vpnserv accordingly.

**Step 7.**

Set permissions for the file created in the previous step and add script to startup.

```
chmod 755 /etc/init.d/vpnserv
update-rc.d vpnserv defaults
```
5.5. Setting up an encrypted connection between MSP and Customer nodes

Step 8.

Setup the network interface dedicated to the VPN bridge (eth1 in this example) and the VPN subnet (eth0:0 in this example) by editing the `/etc/network/interfaces` file.

```bash
nano /etc/network/interfaces
```

Note: We use nano editor to edit the configuration file.

Scroll down and add the following:

```bash
# Network interface for SoftEther VPN bridge
auto eth1
iface eth1 inet manual
   pre-up ifconfig eth1 up
   pre-down ifconfig eth1 down

# Network interface for VPN subnet
auto eth0:0
iface eth0:0 inet static
   address 10.10.10.254
   netmask 255.255.255.0
```

Note: The eth0:0 IP address and netmask should be appropriate for your network configuration. It may be necessary to add more IP addresses in order to connect to all client nodes in different VPN subnets (for example eth0:1 with 10.10.11.254 address to connect to 10.10.11.12 client).

Use Ctrl+O and click Enter to save the file. Then Ctrl+X to close nano editor.
5.5. Setting up an encrypted connection between MSP and Customer nodes

**Step 9.**
Reboot the system.

**Step 10.**
Check if SoftEther VPN Server is running and interfaces are up.

```bash
ps ax | grep vpn
ifconfig
```

**Tip:** If the VPN server is not running you may try to start it manually.

Manual startup via start script:

```
/etc/init.d/vpnserver start
```

Manual startup using server binary:

```
/root/vpnserver/vpnserver start
```
5.5. Setting up an encrypted connection between MSP and Customer nodes

5.5.2. Windows client configuration

The following steps show how to configure the Windows SoftEtherVPN Manager tool on a Windows client machine.

**Step 1.**

Go to [https://www.softether.org/5-download](https://www.softether.org/5-download) and download the software.

**Step 2.**

Install the software on the Windows client. When asked for software components to install, select *SoftEther VPN Server Manager (Admin Tools Only)*.

After the installation is completed you will see the SoftEther VPN Server Manager home screen.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Step 3.

Click **New settings** and configure a new connection to the **VPN server**.

a. Set a name for the connection (in this example, the name is **VPN Server**).
b. Enter the VPN/Monitoring node hostname or IP address (in this example we use **192.168.20.100**).
c. Set a port number (we recommend **5555** for the initial configuration).
d. Make sure that **Direct TCP/IP Connection** is checked in the Proxy Server as Relay settings.
e. Make sure that **Server Admin Mode** is checked in the Administration mode settings.
f. Click **OK**.

After a new connection is added to the VPN server, you will see it listed on the connections list of the home screen.
5.5. Setting up an encrypted connection between MSP and Customer nodes

**Step 4.**
Click the **Connect** button and connect to the VPN server.

**Step 5.**
Set an administrator password for the VPN server connection and click **OK** button.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Configuration how to’s

Step 6.
After the password to the VPN server is set, you will be asked to select the type of VPN Server you want to build.

a. Make sure Remote Access VPN Server is checked.
b. Make sure Site-to-site Server or VPN Bridge is checked.
c. Make sure VPN Server that Accepts Connection from Other Sites (Center) is checked.
d. Click Next.

Step 7.
Next, you will be asked to set a name for the Virtual Hub (in this example, the Virtual Hub Name is VPN). Enter a name for the Virtual Hub and click OK.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Step 8.

Next, configure the **Dynamic DNS Function** (in this example, the DNS configuration is shown on the screenshot on the left).

Step 9.

Next, you will be asked about additional protocols for VPN connections. In this example we don’t use them, so make sure they are all disabled.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Step 10.

Next, you will be asked whether to enable VPN Azure Cloud (in this example we don't use this service, so make sure it is disabled). Click OK.

Step 11.

On the next screen, click Create Users and create a new user to accept VPN connections.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Configuration how to's

a. Set a name for the user (in this example, the user name is `client`).
b. Select **Password Authentication** as a Authentication type.
c. Set a password for authentication.
d. Click **OK**.

After the user is created you will see it listed in the Users list. Click **Exit** button.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Configuration how to's

Step 12.

From the VPN Easy Setup Tasks window set local bridge (in this example, the selected network adapter is eth1).

Step 13.

Click Close button in order to close the VPN Easy Setup Task window. You should see the window from which you can manage the VPN server.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Step 14.
Click OpenVPN / MS-SSTP Settings, enable OpenVPN and generate a configuration file for VPN clients following the steps below:

a. Make sure Enable OpenVPN Clone Server Function is checked.
b. Leave a default (1194) or set a different UDP Ports to listen for OpenVPN (in this example 11941 is set).
c. Click Generate a Sample Configuration File for OpenVPN Clients.
d. Save the configuration file.
e. Make sure Enable MS-SSTP VPN CloneServer Function is disabled.
f. Click OK.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Step 15.

Go to the package with the configuration file for OpenVPN clients downloaded in step 14, and edit `ubuntu_openvpn_site_to_site_bridge_l2` file. Change the auto-generated VPN Server Hostname to either WAN IP address or hostname of the router responsible for handling connections from the Customer node.

If you changed the default UDP Port number in the previous step, you have to change it in the configuration file as well.
5.5. Setting up an encrypted connection between MSP and Customer nodes

5.5.3. Customer router configuration for VPN connection between Customer node and MSP VPN/Monitoring node.

Step 1.

Go to your web browser and enter 192.168.1.1 to access the router web interface.

a. Login to the router’s web-based management interface.
b. Click Sign in.

Step 2.

Go to LAN » DHCP Server and disable the DHCP Server.

Note: This step is crucial to avoid problems that may appear when using more than one DHCP server on the same subnet.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Step 3.

Go to **VPN » VPN Client** and add a new VPN profile.

a. Click **Add profile** button.
b. Select OpenVPN.
c. Enter a description for the new profile (in this example, the description is **VPN to MSP**).
d. Enter the username (in this example, the username is **client**).
e. Enter password.
f. Upload the OpenVPN configuration file for VPN clients (**ubuntu_openvpn_site_to_site_bridge_l2**).
g. Click **OK**.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Step 4.

Activate the connection by clicking the **Activate** button on the VPN Server list.

When the connection is active its status should be as on the lower screenshot.
5.5. Setting up an encrypted connection between MSP and Customer nodes

5.5.4. Open-E DSS V7 configuration on Customer node

Step 1.

On the customer node, go to console and use Ctrl+Shift+N to access the network settings.

Step 2.

Activate DHCP for the Ethernet interface or enter a static IP address provided by MSP (in this example, DHCP is activated on eth0).

a. Select the interface and confirm with OK.

b. Select DHCP parameter and choose Edit.

c. Select Use DHCP and confirm with OK.

d. Confirm with Apply to save the changes.
5.5. Setting up an encrypted connection between MSP and Customer nodes

Step 3.

Use Ctrl+Shift+T to access the Tools menu and check whether the MSP cluster and the Customer node can reach each other.

a. Select the ping option from the Tools menu.
b. Enter the MSP cluster IP address to ping MSP cluster (in this example, we ping 10.10.10.1).

If the MSP cluster responds to the ping, the output should read as follows:
5.6. Setting up replication between Customer node and MSP node

Prerequisites
Please complete the following prerequisites.

- MSP nodes configured according to procedure introduced in Chapter 5.2 - Detailed procedure of setting up MSP nodes
- Customer node configured according to procedure introduced in Chapter 5.4 - Detailed procedure for setting up Customer node
- Encrypted connection between MSP and Customer nodes configured according to procedure introduced in Chapter 5.5 - Setting up an encrypted connection between MSP and Customer nodes

If all the prerequisites have been met, you're now ready to start the Customer node configuration.

5.6.1. MSP node configuration

Step 1.

On msp-node-a, go to Configuration » NAS settings.

a. Navigate to the Data (file) replication agent and check Enable data (file) replication agent.
b. Click apply button.
5.6. Setting up replication between Customer node and MSP node

Step 2.

Still on msp-node-a, go to Configuration » NAS resources » Shares and select copy-data-company-A share from the list on the left side.

a. Navigate to the Data (file) replication agent settings.
b. Check Use data (file) replication.
c. Enter a login name for the data replication agent (in this example, the login name is company-A).
d. Set a password for the replication agent.
e. Enter the Customer node IP address allowed to replicate data to msp-node-a (in this example, IP address is 10.10.10.11).
f. Click apply button.

Step 3.

Next, select copy-data-company-B share from the list on the left side.

a. Navigate to the Data (file) replication agent settings.
b. Check Use data (file) replication.
c. Enter a login name for the data replication agent (in this example, the login name is company-B).
d. Set a password for the replication agent.
e. Enter the Customer node IP address allowed to replicate data to msp-node-a (in this example, IP address is 10.10.11.12).
f. Click apply button.
5.6. Setting up replication between Customer node and MSP node

Step 4.

On **msp-node-b**, go to **Configuration » NAS settings**.

a. Navigate to **Data (file) replication agent** and check **Enable data (file) replication agent**.
b. Click **apply** button.

Step 5.

Still on **msp-node-b**, go to **Configuration » NAS resources » Shares** and select **copy-data-company-B** from the list on the left side.

a. Navigate to **Data (file) replication agent settings**.
b. Check **Use data (file) replication**.
c. Enter a login name for the data replication agent (in this example, the login name is **company-B**).
d. Set a password for the replication agent.
e. Enter the Customer node IP address allowed to replicate data to **msp-node-b** (in this example, IP address is **10.10.11.12**).
f. Click **apply** button.
5.6. Setting up replication between Customer node and MSP node

Step 6.

Next, select **copy-data-company-A** from the list on the left side.

a. Navigate to **Data (file) replication agent settings**.
b. Check **Use data (file) replication**.
c. Enter a login name for the data replication agent (in this example, the login name is **company-A**).
d. Set a password for the replication agent.
e. Enter the Customer node IP address allowed to replicate data to **msp-node-a** (in this example, IP address is **10.10.10.11**).
f. Click **apply** button.
5.6. Setting up replication between Customer node and MSP node

5.6.2. Customer node configuration

Step 1.

On Customer node, navigate to Maintenance » Backup » Data (file) replication and create a new replication task to replicate data from the Customer node to the MSP node.

a. Enter a name for the task (in this example, the task name is companyAtoMSP).
b. Select the source share containing data to be replicated (in this example, the source share is data-company-A).
c. Select a snapshot used for data replication (in this example, the snapshot is snap00000).
d. Specify the MSP node destination IP address (in this example IP address is: 10.10.10.1).
e. Click refresh button and select a destination share on the MSP node to which you want to replicate data (in this example the share name is copy-data-company-A).
f. Enter agent login and password.
g. Make sure “Log replication errors” is checked.
h. Select the desired replication policy.
i. Click apply button.
5.6. Setting up replication between Customer node and MSP node

Configuration how to’s

Step 2.

Select the task from the menu on the left side, configure the task schedule recurrence and click apply button.

Tip: If you want to check whether your task is running properly, go to Status » Tasks where all tasks statuses are listed.

Tip: You may also monitor the Data (file) replication tasks on MSP node via Check_MK. It requires installing a small update on the MSP node. You may obtain the update file here:
ftp://software:UuPpDdAaTtEe@ftp.open-e.com/In_Engineering_Phase/70473-DSS-V7_data_replication_check_mk/

For the Customer node you may obtain the update file here:
ftp://software:UuPpDdAaTtEe@ftp.open-e.com/SML_UPDATES/70473-DSS-V7-CDPS_data_replication_check_mk/

The procedure for applying a small update can be found in Chapter 5.3.2. - Applying the small update to monitored node.
5.7. Optional procedure for setting up local backup for Customer node

Prerequisites
Please complete the following prerequisites.

- Customer node configured according to procedure introduced in Chapter 5.4 – Detailed procedure for setting up Customer node
- Open-E DSS V7 NAS for CDPS installed on the Customer node

If all the prerequisites have been met, you’re now ready to start Customer node configuration.

Step 1.
Go to Configuration » Volume manager » Volume groups.

a. Select vg00 from the list on the left side.
b. Create a snapshot assigned to the NAS volume lv0000 (in this example the snapshot name is snap0001).
c. Click apply button.

It is recommended to create snapshots of a size that is at least 20% of the NAS volume size to which it is assigned.

It is highly recommended to monitor snapshot use. If the snapshot capacity is exceeded the system may become unstable.
5.7. Optional procedure for setting up local backup for Customer node

**Step 2.**
Create a share for data restored from the backup.

a. Enter a name for the share (in this example, the share name is `backup_restore_A`).
b. Select `lv0000` as a default path for the share.
c. Click **apply** button.

**Step 3.**
Create a share for the virtual backup device.

a. Enter a name for the share (in this example, the share name is `backup_tape_A`).
b. Select `lv0000` as a default path for the share.
c. Click **apply** button.
5.7. Optional procedure for setting up local backup for Customer node

Step 4.

Go to Configuration » NAS resources » Shares and create a share for the backup database.

a. Enter a name for the share (in this example, the share name is backup_database_A).
b. Select lv0000 as a default path for the share.
c. Click apply button.

Step 5.

Go to Configuration » NAS settings and enable local backup.

a. Select share for your backup database location (in this example, it is backup_database_A).
b. Make sure the "Create database" option is checked.
c. Click apply button.
5.7. Optional procedure for setting up local backup for Customer node

Step 6.

Go to **Maintenance » Backup » Backup pools** and create a new backup pool.

a. Enter a name for the pool (in this example, the backup pool name is `pool_A`).

b. Click **apply** button.

**Note:** You may configure tape retention. By default it is 365 days.

Step 7.

Go to **Maintenance » Backup » Backup devices**.

a. Set a name for your virtual backup device (in this example, the backup device name is `backup_device_A`).

b. Select the share you want to use as a virtual device (in this example, selected share is `backup_tape_A`).

c. Click **create** button.
5.7. Optional procedure for setting up local backup for Customer node

Step 8.
Select the backup device (in this example, it is `backup_device_A`) from the menu on the left side.

a. Label a new tape (in this example, the tape label is `backup_local_A`).
b. As a pool name select the pool created in step 6 (in this example, the selected pool is `pool_A`).
c. Click `apply` button.

Step 9.
Go to Maintenance » Backup » Backup task and create a backup task for the local data backup.

a. Enter a name for the task (in this example, the task name is `backup_job_A`).
b. Select a logical volume (in this example, the volume is `lv0000`).
c. Select a share for backup (in this example, the share is `data-company-A`).
d. Select a snapshot (in this example, the snapshot is `snap00001`).
e. Select a pool to store data on (in this example, the pool is `pool_A`).
f. Make sure `incremental` is checked as a backup level (type).
g. Click `apply` button.

Note: A snapshot used for the local backup has to be different from the one used in the Data (file) replication task.
5.7. Optional procedure for setting up local backup for Customer node

Step 10.

Select the backup task name from the list on the left side (in this example, the task name is **backup_job_A**).

a. Configure task schedule recurrence.

b. Add comment to help you identify the task (in this example, the comment is **1hbakA**).

c. Click apply button.
6. Disaster recovery & data restore
6.1. Disaster recovery

6.1.1. Without hardware replacement (remote)

Step 1.

On the Customer node, go to **Configuration » NAS resources » Shares**.

a. Select the **data-company-A** share from the list on the left side.
b. Navigate to the **Data (file) replication agent** and check **Use data (file) replication agent**.
c. Click **apply** button.
d. Enter the login name for the data replication agent (in this example, login name is msp).
e. Set a password for the replication agent.
f. Enter the MSP Virtual IP address allowed to replicate data to the Customer node (in this example, IP address is **10.10.10.1**).
g. Click **apply** button.
6.1. Disaster recovery

Step 2.

Go to the MSP node on which the resources (in this example, lv0000) are active on. Navigate to Configuration » Volume manager » Volume groups.

a. Select vg00 from the list on the left side.
b. Create the snapshot assigned to the logical volume where the Customer data copy is stored (in this example, lv0000).
c. Set a size for the snapshot.
d. Click apply button.

Step 3.

Still, on the msp-node-a go to Maintenance » Backup » Data (file) replication and create a new Data (file) replication task.

a. Enter a name for the task (in this example, the task name is replication_from_msp_to_companyA).
b. Select the source share which contains the restored data (in this example, the source share is copy-data-company-A).
c. Select a snapshot used for data replication (in this example, the snapshot is snap00000).
d. Specify the Customer node destination IP address (in this example IP address is: 10.10.10.11).
e. Click refresh button and select the destination share on Customer node to which you want to replicate the data (in this example the share name is data-company-A).
f. Enter the agent login and password set in step 8 (in this example the login is msp).
g. Make sure “Log replication errors” is checked.
h. Click apply button.
6.1. Disaster recovery

Step 4.

Run the replication task `replication_from_msp_to_companyA`.

Step 5.

Go to Status » Tasks and check whether the task is finished. After the task is executed properly, data on the Customer node should be restored.
6.1. Disaster recovery

6.1.2. With hardware replacement (on-site)

Step 1.

Configure the Customer node according to the procedure introduced in Chapter 5.4 – Detailed procedure of setting up Customer node.

Step 2.

After the customer node is configured, follow steps 1 to 5 from Chapter 6.1 – Disaster recovery in order to restore data on the Customer node.
6.2. Restoring data from backup

6.2.1. Restoring data set from end-user’s local backup

Step 1.

Go to **Customer node**, navigate to **Maintenance » Restore** and create restore task.

a. Find and select the backup you want to restore (in this example it is `backup_job_A`).
b. Select the appropriate backup device (in this example it is `backup_device_A`).
c. Enter a name for the restore task (in this example, the restore task name is `restore`).
d. Select a share to which you want to restore data (in this example, the share name is `backup_restore_A`).
e. Make sure **always** is checked as an option for overwriting files.
f. Make sure that “run immediately after creation” option is checked (if you want to restore data immediately).
g. Click **apply** button.
h. When the system asks whether to continue, click **yes**.
6.2. Restoring data from backup

Step 2.

After the task is finished connect to the share which contains the restored data (in this example, the share is `backup_restore_A`).

Step 3.

Go to `backup\backup_job_A` directory and find the data you want to restore (in this example we will restore data from the `\backup_restore_A\backup\backup_job_A\2015-10-21 04.56.465\data-company-A` directory).
6.2. Restoring data from backup

Step 4.

Connect to the share which contains the customer data (in this example, the share name is **data-company-A**).

Step 5.

Move restored files to the share which contains the customer data (in this example, we copy data from `\10.10.10.11\backup_restore_A\backup\backup_job_A\2015-10-21 04.56.465\data-company-A` to `\10.10.10.11\data-company-A`).

**Note:** In case you restore data from more than one backup you need to merge data from all backup folders (starting from the oldest one) to a single data set.

Step 6.

Remove the restore task created in step 1 (in this example, the task name is restore) as well as the folder to which the data was restored (in this example, the folder is `backup_job_A` in `\backup_restore_A\backup`).
6.2. Restoring data from backup

6.2.2. Restoring a single file from MSP backup

**Note:** In order to restore the file that has been modified or deleted on the Customer node, the replication policy for the replication task on the node has to be set to “Replication with backup”.

**Note:** The following procedure allows you to restore only the last version of a deleted file or previous version of a modified file, according to the “Replication with backup” policy.

**Step 1.**

Connect to the share which contains the copy of Customer data on the MSP node (in this example, the share is `copy-data-company-A`).
6.2. Restoring data from backup

Step 2.

Next, connect to the share which contains the Customer data on the Customer node (in this example, share name is data-company-A).

Step 3.

Go to copy-data-company-A\__recycle__ and find the file you want to restore (in this example, the file is file10).

Note: In this example we will restore the file file10 which was deleted from the Customer node.
6.2. Restoring data from backup

Step 4.

Copy the file from `copy-data-company-A` on the MSP node to `data-company-A` on the Customer node.
7. Recommendations / troubleshooting

High network interface usage
In case of such situations make sure that data replication tasks are balanced in your schedule. If there are many tasks at the same time, try to reorganize your schedule so replication tasks do not interfere with each other. If there is a constant high usage, try to add more network interfaces and create bonding.

High load
If the system reports high load most of the time, consider upgrading your hardware. Monitor CPU usage and disks I/O. If the CPU usage falls within acceptable limits, try to upgrade your RAID configuration (better RAID controller, better or more drives in array).

Monitoring with graphs
Each service monitored should have graphs with different scopes, for example: last 4 hours, last 24 hours, last week, last month, last year. Monitoring configured with instructions from Chapter 5.3 does that by default. When using different monitoring solutions we highly recommend to implement graphs as they are a priceless source of information in case of troubles.

Slow replication rate
Make sure that the Internet connection between nodes works with good performance. Try to measure the connection speed between nodes to estimate the maximum performance that could be achieved. To do that, you can use iperf from some live system to exclude software problems or even connect a different machine to same link to exclude hardware issues. You can do a separate checks with and without a VPN tunnel to exclude the VPN software or VPN hardware from the factors slowing down the system. You can also check system performance (load, CPU usage, disks I/O). If any of these parameters is high most of the time, please try to eliminate it.

Open-E software version
All configurations were conducted using Open-E DSS V7 up54 build 18432.
8. Open-E Technical Support – Contact information

You have issues with the setup or need help with configuring the cluster or a customer server? Depending on the support level you are using, please open a ticket for your registered Open-E DSS V7 licenses:

https://www.open-e.com/partner-portal/technical-support/new/

Your product isn't registered yet? Please follow the link to the registration form:

https://www.open-e.com/partner-portal/partner-area/products/commercial/

For more information on Open-E's support services, please read our Support Policy:

http://www.open-e.com/support/general-information/

If you have any additional questions please call +1 (678) 666 2880 for US / +49 (89) 800777 0 for Europe or send an e-mail to info@open-e.com