# 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 Monitoring node ...................................................................................... p.13
5. Configuration how-to’s ............................................................................................................................................... p.14
   5.1 Installing DSS V7 ................................................................................ p.16
   5.2 Detailed procedure of setting up MSP nodes ........................................ p.17
   5.3 Detailed procedure of setting up monitoring for MSP ......................... p.46
   5.4 Detailed procedure of setting up Customer node ................................. p.78
   5.5 Customer router configuration ............................................................. p.85
   5.6 Setting up replication between Customer node and MSP node ... p.86
   5.7 Optional procedure for setting up local backup for Customer node ........ p.92
6. Disaster recovery & data restore .......................................................................................................................... p.98
   6.1 Disaster recovery .................................................................................... p.99
      6.1.1 Without hardware replacement (remote) ..................................... p.99
      6.1.2 With hardware replacement (on-site) ......................................... p.102
   6.2 Restoring data from backup ................................................................. p.103
      6.2.1 Restoring data set from end-user’s local backup ....................... p.103
      6.2.2 Restoring a single file from MSP backup ................................ p.106
7. Recommendations / troubleshooting ...................................................................................................................... p.109
8. Open-E technical support contact info .............................................................................................................. p.110

---

**How-To Guide:** Cloud Data Protection Service by MSP

---

**open-e**
1. Introduction - overview of the solution, what are the benefits for both MSPs and for 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.

**Monitoring node**
MSP’s server running 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.

**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

Customer node 1
- Data server (company-a)
- Optional Local Backup
- Shares: data-company-A

Customer node 2
- Data server (company-b)
- Optional Local Backup
- Shares: data-company-B

Customer node 3
- Data server (company-c)
- Optional Local Backup
- Shares: data-company-C

MSP nodes
- High Availability Cluster

Monitoring node
- Real-time diagnostics of MSP and customer nodes

Customer node 4
- Data server (company-d)
- Optional Local Backup

Customer node N
- Data server (company-n)
- Optional Local Backup
- Shares: data-company-N

SSH tunnel
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

VIP: 10.10.10.1
VIP: 10.10.11.1
VIP: 20.20.20.1
VIP: 20.20.21.1

msp-node-b

- eth0 - 192.168.20.2
- eth1 - 192.168.10.2
- eth2 - 192.168.11.2
- eth3 - 192.168.12.2

VIP: 10.10.10.1
VIP: 10.10.11.1
VIP: 20.20.20.1
VIP: 20.20.21.1

Monitoring node

- eth0 - 192.168.20.100

A router with public IP address and port forwarding configured.

Customer router

VIP: 192.168.0.111

Customer node

VIP: 192.168.0.111

Customer node

VIP: 192.168.1.111

1Gbit eth0 (192.168.0.111) for secure data replication and storage access from internal network.

VIP: 192.168.1.111

1Gbit eth0 (192.168.1.111) for secure data replication and storage access from internal network.

VIP: 192.168.0.111

VIP: 192.168.0.111

VIP: 192.168.1.111

VIP: 192.168.1.111
4. Minimum hardware requirements
4. Minimum hardware requirements

4.1. MSP nodes

<table>
<thead>
<tr>
<th>Hardware specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel® Xeon® processors of the E5-2600 v2 family or better</td>
</tr>
<tr>
<td>RAM</td>
<td>16GB DDR3 base memory and 350MB additionally for each Customer node</td>
</tr>
<tr>
<td>Hard disk drive</td>
<td>2x RAID 5 (alternatively, RAID 6 or RAID 10) disk arrays, 8 hard drives each</td>
</tr>
<tr>
<td>Ethernet</td>
<td>2 x 10GbE, 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. 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></td>
<td><strong>Hardware specification</strong></td>
</tr>
<tr>
<td>Processor</td>
<td>4-core 2.5 GHz or better</td>
</tr>
<tr>
<td>RAM</td>
<td>4GB with ECC support or more</td>
</tr>
<tr>
<td>Hard disk drive</td>
<td>2-disk RAID 1 array</td>
</tr>
<tr>
<td>Ethernet</td>
<td>1 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.
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
- 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/)
5.2. Detailed procedure of setting up MSP nodes

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 up56 build 19059 installed on both servers
- A router with multiple-subnet support

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 encrypted data replication
- 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

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

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

**Configuration how to's**

---

**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.

---

**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

Configuration how to’s

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

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

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

5.2.2. 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 encrypted data replication
- 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

Configuration how to's

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. MSP router configuration

**Step 1.**

Configure port forwarding on the router in order to allow a connection request from Customer nodes.

Exemplary port forwarding configuration of MSP’s router is shown in the table on the left.

**Note:** You need a router with multiple-subnet support.

**Note:** The IP addresses and port numbers used in this example are for the purpose of this manual only. You should configure your Ethernet ports according to your network topology.

<table>
<thead>
<tr>
<th>Port forwarding for:</th>
<th>External IP address</th>
<th>External port number</th>
<th>Internal IP address</th>
<th>Internal port number</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>company-a</td>
<td>MSP public IP</td>
<td>41001</td>
<td>10.10.10.1</td>
<td>40000</td>
<td>TCP</td>
</tr>
<tr>
<td>company-b</td>
<td>MSP public IP</td>
<td>41002</td>
<td>10.10.11.1</td>
<td>40000</td>
<td>TCP</td>
</tr>
</tbody>
</table>
5.2. Detailed procedure of setting up MSP nodes

5.2.4. 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

5.2.5. Setting up and running Failover service

On msp-node-a go to Setup » Failover.

**Step 1.**

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.
Step 2.

Add two ping nodes.

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

Step 3.

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 4.

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

Configuration how to’s

**Step 5.**
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 6.**
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 192.168.11.1**).
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.
5.2. Detailed procedure of setting up MSP nodes

Step 7.

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 8.

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 Monitoring node (see Chapter 2 - Solution diagram / Network topology). The Monitoring node is a single node running Ubuntu Server 14.04 LTS with OMD (Open Monitoring Distribution) software installed.

Prerequisites

Please complete the following prerequisites.

- Server meets requirements for 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 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 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 Monitoring node

In order to install OMD package on MSP 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
```

In order to install OMD package, in the next steps we will follow instructions from [https://labs.consol.de/repo/stable/](https://labs.consol.de/repo/stable/).

**Step 2.**

Install the relevant GPG key in Ubuntu.

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

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

**Step 3.**

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 4.
Run `apt-get update` to refresh our distribution repositories.

```
apt-get update
```

Step 5.
Install the OMD.

```
apt-get install omd
```

Step 6.
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 v7.0up56 or above.

Click: [http://kb.open-e.com/How-can-I-obtain-and-apply-a-small-update-to-my-Open-E-software_63.html](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.

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

**Step 1.**

Go to **Maintenance » Software update** and navigate to System software update.

**Step 2.**

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 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).

```bash
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
```

**Note:** In case you want to add Customer node to Check_MK list of known hosts, the port number in the command should be set according to Customer's node port forwarding configuration and IP address should be Customer's router public IP address.

**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 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.

a. 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**).

b. 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`).

**Note:** In case you want to add Customer node to Check_MK list of known hosts, the port number in the command should be set according to Customer's node port forwarding configuration and IP address should be Customer's router public IP address.

c. 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.

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

Usually Check_MK uses a series of PING (ICMP echo request) in order to determine whether a host is up. In some cases this is not possible, however. The following steps show how to create a rule to make the Host Check Command use the status of the Check_MK Agent instead of ping for the monitored node.

**Step 17.**
Click the Hosts&Service Parameters in the WATO configuration section on the left side. Next, click Monitoring Configuration button.

**Step 18.**
Navigate to Host Checks section and click Host Check Command.
5.3. Detailed procedure of setting up monitoring for MSP

Step 19.

Click Create rule in folder button.

Step 20.

Navigate to Host Check Command section and select Use the status of the Check_MK Agent option from the droplist. Next click Save button.
5.3. Detailed procedure of setting up monitoring for MSP

Step 21.
Activate the changes made in configuration.

a. Click Changes button at the top.
b. Click Activate changes button.
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

<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
```

```
192.168.0.1 www.example.com
```

**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.

```bash
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.

```bash
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = localhost
inet_protocols = all
```

Step 10.
Restart Postfix.

```bash
service postfix restart
```

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

```bash
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

**Configuration how to’s**

**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

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.
5.4. Detailed procedure of setting up Customer node

**Step 2.**

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

It is recommended to configure one interface:

- 1Gbit (eth0) interface for:
  - access to Open-E DSS V7 web interface
  - encrypted data replication
  - storage access

**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.

**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.
5.4. Detailed procedure of setting up Customer node

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.

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.
5.4. Detailed procedure of setting up Customer node

Step 6.
Go to Configuration » NAS settings.

a. Check the Enable Data (file) replication agent.
b. Click apply button.

Step 7.
Next, navigate to FTP settings.

a. Check Use FTP.
b. Set FTP port, Max clients and Max. clients per host options.
c. Make sure SFTP is set as a encryption method.
d. Click apply button.
5.4. Detailed procedure of setting up Customer node

Step 8.

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/data-company-A 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.

Step 9.

Next, create share for restored data.

a. Enter a name for the share (in this example, the share name is restore_from_msp).
b. Select /lv0000/restore_from_msp as a default path for the share.
c. Click apply button.
5.4. Detailed procedure of setting up Customer node

Step 10.

Go to **Configuration » NAS resource » Users** and create a new user.

a. Set a name for the user.
b. Set a password for the user.
c. Click **create** button.

Step 11.

Select **restore_from_msp share** from the menu on the left side.

a. Navigate to **SMB settings**.
b. Uncheck **Use SMB**.
c. Click **apply** button.
5.4. Detailed procedure of setting up Customer node

**Step 12.**

Next, navigate to **FTP settings**.

a. Check **Use FTP**.

b. Make sure **Users with password** option is selected.

c. Click **apply** button.

**Step 13.**

Next, navigate to **Users share access (SMB/FTP/AFP)**.

a. Move the newly created user (in this example, the user is **msp**) from Available users to Granted access users.

b. Click **apply** button.
5.5. Customer router configuration

**Step 1.**
Configure port forwarding on the router in order to allow a connection request from MSP nodes. Exemplary port forwarding configuration of Customer's router is shown in the table on the left.

<table>
<thead>
<tr>
<th>Service</th>
<th>External IP address</th>
<th>External port number</th>
<th>Internal IP address</th>
<th>Internal port number</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSS V7 SSH RSYNC</td>
<td>Customer public IP</td>
<td>40000</td>
<td>192.168.0.111</td>
<td>40000</td>
<td>TCP</td>
</tr>
<tr>
<td>DSS V7 TUI</td>
<td>Customer public IP</td>
<td>40001</td>
<td>192.168.0.111</td>
<td>22222</td>
<td>TCP</td>
</tr>
<tr>
<td>DSS V7 CLI/API</td>
<td>Customer public IP</td>
<td>40002</td>
<td>192.168.0.111</td>
<td>22223</td>
<td>TCP</td>
</tr>
<tr>
<td>DSS V7 SFTP</td>
<td>Customer public IP</td>
<td>40003</td>
<td>192.168.0.111</td>
<td>21</td>
<td>TCP</td>
</tr>
</tbody>
</table>

**Note:** The IP addresses and port numbers used in this example are for the purpose of this manual only. You should configure your Ethernet ports according to your network topology.

- **DSS SSH RSYNC** is used for encrypted data replication from MSP node to Customer node
- **DSS TUI** is used for secure access to DSS V7's Terminal User Interface on Customer's node
- **DSS CLI/API** is used for the secure connection between Monitoring node and Customer node
- **DSS SFTP** is used for SFTP connection
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

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

Configuration how to’s

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. Click apply button.

Note: "Allow access IP" is not required as the function does not work in case of encrypted connection between MSP nodes and Customer node.

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. Click apply button.

Note: "Allow access IP" is not required as the function does not work in case of encrypted connection between MSP nodes and Customer node.
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. Click apply button.

*Note:* "Allow access IP" is not required as the function does not work in case of encrypted connection between MSP nodes and Customer node.
5.6. Setting up replication between Customer node and MSP node

How-To Guide: Cloud Data Protection Service by MSP

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. Click **apply** button.

**Note**: "Allow access IP" is not required as the function does not work in case of encrypted connection between MSP nodes and Customer node.
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 a public destination IP address and port number of the MSP node.
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. Select desired compression level (in this example the compression is disabled).
h. Select encryption algorithm (in this example the encryption algorithm is aes256-ctr).
i. Make sure "Log replication errors" is checked.
j. Select desired replication policy (in this example replication with backup is selected).
k. Select desired file synchronization policy (in this example block-based synchronization is selected).
l. Click apply button.
5.6. Setting up replication between Customer node and MSP node

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.
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. Click apply button.

Note: "Allow access IP" is not required as the function does not work in case of encrypted connection between MSP nodes and Customer node.

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. Assign the snapshot to the volume lv0000.

d. Set a size for the snapshot.

e. Click apply button.
6.1. Disaster recovery

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 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 public destination IP address and port number of the Customer node.

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. Select desired compression level (in this example the compression is disabled).

h. Select encryption algorithm (in this example the encryption algorithm is aes256-ctr).

i. Make sure “Log replication errors” is checked.

j. Select desired replication policy (in this example replication only is selected).

k. Select desired file synchronization policy (in this example block-based synchronization is selected).

l. 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.

Note: In order to connect remotely to Customer’s share you need a remote access and control tool (e.g. teamViewer).

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 `\192.168.0.111\backup_restore_A\backup\backup_job_A\2015-10-21 04.56.465\data-company-A` to `\192.168.0.111\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 with enabled FTP on the Customer node (in this example, share name is restore_from_smp).

**Note:** We use Filezilla as a FTP client application.

a. Enter Host IP address which is Customer node public IP address.
b. Enter a valid port number (in this example, the port number is 40003).
c. Select **SFTP-SSH File Transfer Protocol** from the list of available ftp protocols.
d. Select **Normal** as login type.
e. Enter user and password.
f. Click **Connect** button.

**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 `restore_from_msp` on the Customer node.

Step 5.

Copy the restored file from `restore_from_msp` 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 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 up56 build 19059.
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