

Saturday, March 22, 2008

## Less known Solaris Features: iSCSI - Part 3: Bidirectional authenticated iSCSI

Okay, but we are in a public network. How can we protect the target against a user not allowed to use it? iSCSI supports a CHAP based authentication. It's the same scheme as with PPP. With this authentication, target and initiator can authenticate each other based on shared secrets. The configuration is a little bit more complex, as both initiator and target have to know the secrets and their names of each other.

### Prerequisites

At first we need some basic data. We need the IQN names of both. At first we look up the IQN of the initiator. Thus we login to gandalf and assume root privileges:

```
# iscsiadm list initiator-node
```

```
Initiator node name: iqn.1986-03.com.sun:01:00000000b89a.47e38163
```

```
Initiator node alias: gandalf
```

[...]Now we look up the IQN of the target. Okay, we login to theoden and assume root privileges: # iscsitadm list target

```
Target: testpool/zfsvolume
```

```
  iSCSI Name: iqn.1986-03.com.sun:02:b29a71fb-ff60-c2c6-c92f-ff13555977e6
```

```
iqn.1986-03.com.sun:02:b29a71fb-ff60-c2c6-c92f-ff13555977e6
```

```
  Connections: 1
```

Both IQN's are important in the following steps. We need them as a identifier for the systems.

Configuring the initiatorAt first we export the zpool and disable the discovery of targets. This steps has to be done on the initiator, in our example gandalf:# zpool export zfsviaiscsi

```
# iscsiadm remove discovery-address 10.211.55.200
```

```
# devfsadm -c iscsi -CYou don't have to do this steps. The zpool may only get unavailable while we configure the authentication and you will see a few more lines in your logfiles.
```

Okay, now we configure the CHAP authentication.

```
# iscsiadm modify initiator-node --CHAP-name gandalf
```

```
# iscsiadm modify initiator-node --CHAP-secret
```

```
Enter secret:
```

```
Re-enter secret:
```

```
# iscsiadm modify initiator-node --authentication CHAP
```

What have we done with this statements: We told the iSCSI initiator to identify itself as gandalf. Then we set the password and tell the initiator to use CHAP to authenticate.

Configuring the targetOkay, now we configure the target to use CHAP as well. This has to be done on the target, in our example theodenBut at first we have to set the CHAP name and the CHAP secret of the target itself:

```
# iscsitadm modify admin --chap-name theoden
```

```
# iscsitadm modify admin --chap-secret
```

```
Enter secret:
```

```
Re-enter secret:This isn't an admin login. This is a little misguiding.
```

Now we create an initiator object on the target.We connect the long IQN with a shorter name.# iscsitadm create initiator --iqn iqn.1986-03.com.sun:01:00000000b89a.47e38163 gandalf

Now we tell the target, that the initiator on the system gandalf will identify itself with the name gandalf:# iscsitadm modify initiator --chap-name gandalf gandalfOkay, now we set the password for this initiator. This is the same password we set on the initiator.# iscsitadm modify initiator --chap-secret gandalf

```
Enter secret:
```

```
Re-enter secret:
```

```
Finally we tell the target, that the system gandalf is allowed to access the testpool/zfsvolume:# iscsitadm modify target --acl gandalf test/zfsvolumeNow the initiator has to authenticate itself before the target daemon grants access to the target. You could skip the next steps and fast-forward to the section "Reactivation of the zpool" but the authentication is only unidirectional at the moment. The client(initiator) authenticate itself at the server(target).
```

Configuration of bidirectional configurationOkay, but it would be nice, that the target identifies himself to initiator as well.

Okay, at first we tell the initiator, that the target with the IQN

```
iqn.1986-03.com.sun:02:b29a71fb-ff60-c2c6-c92f-ff13555977e6 will authenticate itself with the name theoden. This
```

steps has to be done on the initiator, thus we login into gandalf again.

```
# iscsiadm modify target-param --CHAP-name theoden
```

```
iqn.1986-03.com.sun:02:b29a71fb-ff60-c2c6-c92f-ff13555977e6Now we set the secret to authenticate. This is the secret we configured as the CHAP-Secret on the target with iscsitadm modify admin --chap-secret:
```

```
# iscsiadm modify target-param --CHAP-secret iqn.1986-03.com.sun:02:b29a71fb-ff60-c2c6-c92f-ff13555977e6
```

```
Enter secret:
```

```
Re-enter secret:
```

```
Now we activate the bidirectional authentication for the IQN of theoden:
```

```
# iscsiadm modify target-param --bi-directional-authentication enable
```

```
iqn.1986-03.com.sun:02:b29a71fb-ff60-c2c6-c92f-ff13555977e6At last we tell the initiator to authenticate the target with CHAP.
```

```
# iscsiadm modify target-param -a chap iqn.1986-03.com.sun:02:b29a71fb-ff60-c2c6-c92f-ff13555977e6Okay, now we have completed the configuration for the bidirectional authentication.
```

Reactivation of the zpoolOkay ... now we can reactivate the zpool. We tell the initiator to discover targets on the target server again, scan for devices and import the zpool again:

```
# iscsiadm add discovery-address 10.211.55.200
```

```
# devfsadm -c iscsi -C
```

```
# zpool import zfsviaiscsi
```

```
# cd /zfsviaiscsi/
```

Posted by Joerg Moellenkamp in Solaris at 08:57