How to use a PSK when using SyncIQ since 7.0.0

Issue

Dell EMC Isilon OneFS has a SyncIQ vulnerability where the cluster may receive unauthorized replication of data, which may potentially be exploited by attackers to add, modify or remove files on the affected system. Furthermore, SyncIQ passwords are not supported in SmartLock compliance mode.

Details

There are two options to resolve this issue:

- Encryption
- Using a pre-shared key (PSK)

It is highly recommended for clusters with OneFS 8.2.0 or later to be configured to encryption-required in SyncIQ. For information about this procedure, see the Dell EMC Technical White Paper, Dell EMC Isilon SyncIQ: Architecture, Configuration, and Considerations.

If encryption cannot be done, a pre-shared key (PSK) lowers the risk. However:

- The key is target cluster specific, all sync policies targeting the cluster share a key.
- This still leaves the cluster vulnerable to brute force.
- This still leaves the cluster vulnerable to anyone in the path of a sync.

Resolution

To enable a pre-shared key (PSK) when using SyncIQ:

1. Open a secure shell (SSH) or a serial console connection to any node in the cluster and log in as root.

2. Check the SyncIQ jobs on both the source and target clusters:

   ```
   isi sync jobs list
   ```

3. If any jobs are running, complete the jobs, or use the following commands to cancel the jobs, where `<policy name>` is the name of the job:

   For specific jobs: `isi sync jobs cancel <policy name>`

For all jobs: `isi sync jobs cancel --all`

4. On the target cluster, open the `/ifs/.ifsvar/modules/tsm/` directory and create a file named `passwd`:

   NOTE on SyncIQ password requirements:

   - The `passwd` file should contain a single line with the cluster's SyncIQ password
   - The password must have no more than 255 characters and only contain letters and numbers; no spaces or special characters are permitted.
   - As a best practice, for better security isolation, do not use this password in other systems.

   ```
   touch /ifs/.ifsvar/modules/tsm/passwd
   chmod 700 /ifs/.ifsvar/modules/tsm/passwd
   ```

   NOTE: The `passwd` file will only exist if a PSK has already been configured.

5. To view the password, run the following command:

   ```
   cat /ifs/.ifsvar/modules/tsm/passwd
   ```

6. On the source cluster, modify all policies that replicate data to the target cluster:

   In OneFS 8.0 and later: `isi sync policies modify <policy-name> --set-password --password=<PSK-target-cluster>`

   In OneFS 7.1.x or 7.2.x: `isi sync policies modify <policy-name> --password <PSK-target-cluster>`

   In OneFS 7.0.x and earlier: `isi sync policy modify <policy-name> --passwd=<PSK-target-cluster>`

   NOTE:

   - Without the password, the job will fail with an `Authentication with target failed` message.
   - For jobs in the `isi sync jobs list`, the command will fail with a `The policy has an active job and cannot be modified` message.

7. Confirm the password is configured on the source cluster policy:

```
isi sync policies view <policy-name>
```

Output of the **Password Set** field should be set to **Yes**.

8. Resume the jobs:

```
isi sync jobs start <policy-name>
```

To disable pre-shared key (PSK) when using SyncIQ:

Remove the SyncIQ PSK password on the target cluster, and modify all policies replicating data to that target cluster:

In OneFS 8.0 and later: `isi sync policies modify <policy-name> --set-password --password="<null>"`

In OneFS 7.1.x or 7.2.x: `isi sync policies modify <policy-name> --password ""`

In OneFS 7.0.x and earlier: `isi sync policy modify <policy-name> --passwd=""`