The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decision. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

NDMP Security Extension

Radhika Vullikanti

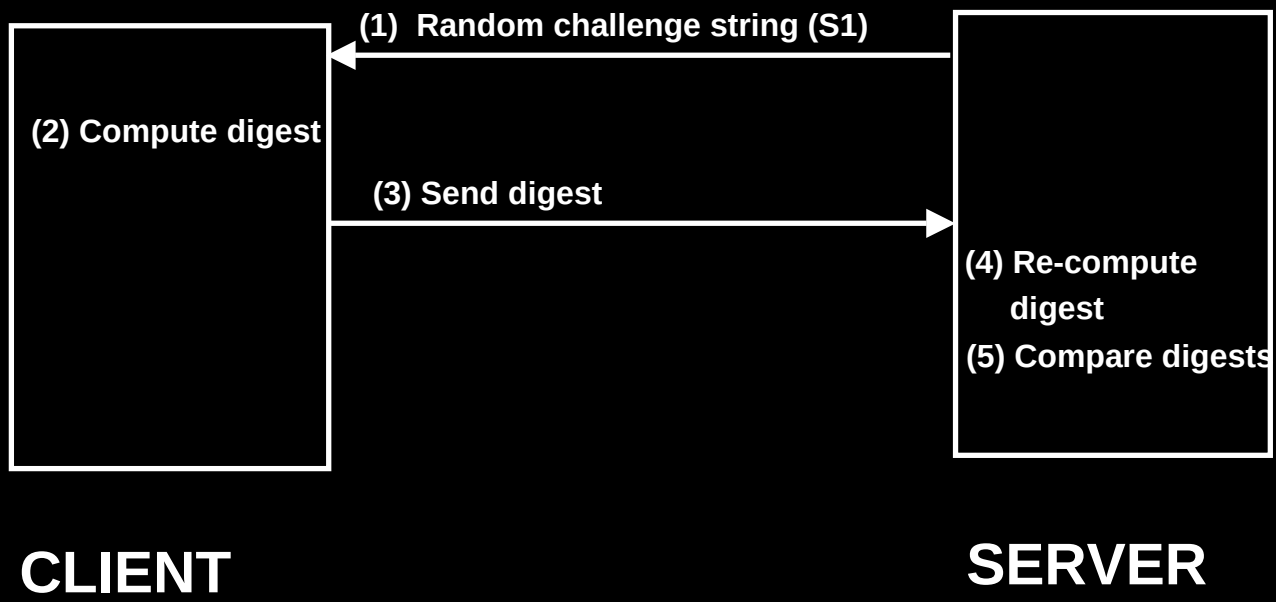
Senior Engineer

Oracle Secure Backup

Introduction

Current NDMP authentication models

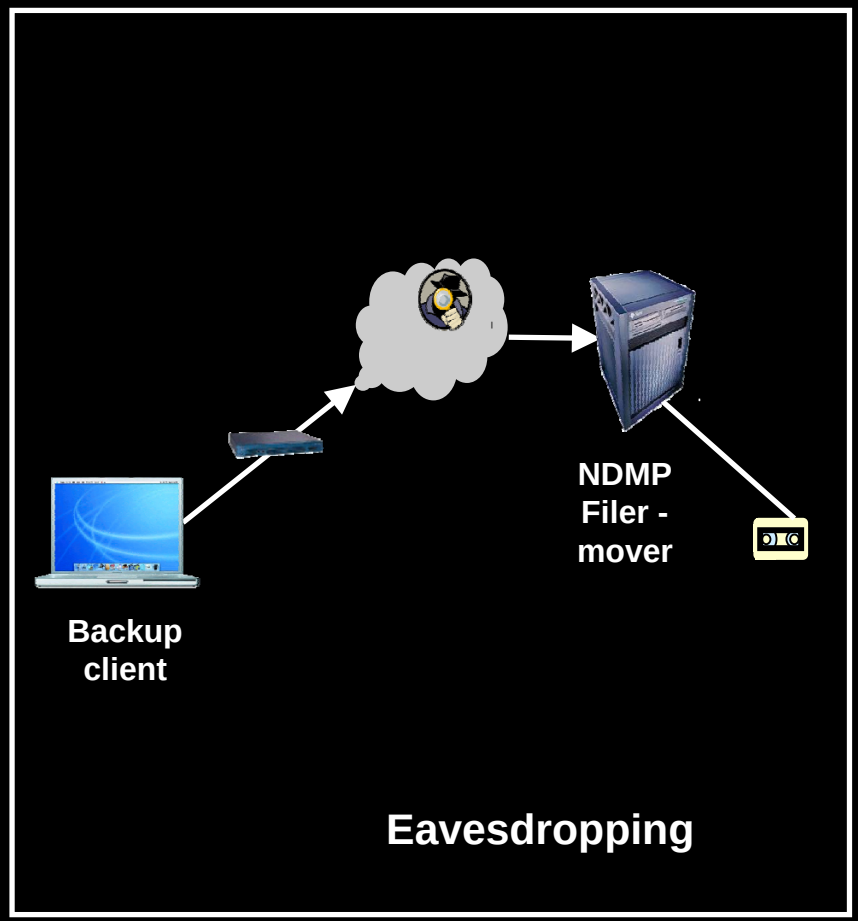
- Plaintext password-based authentication
  - User name & password sent in clear text
- MD5 digest based authentication (below)

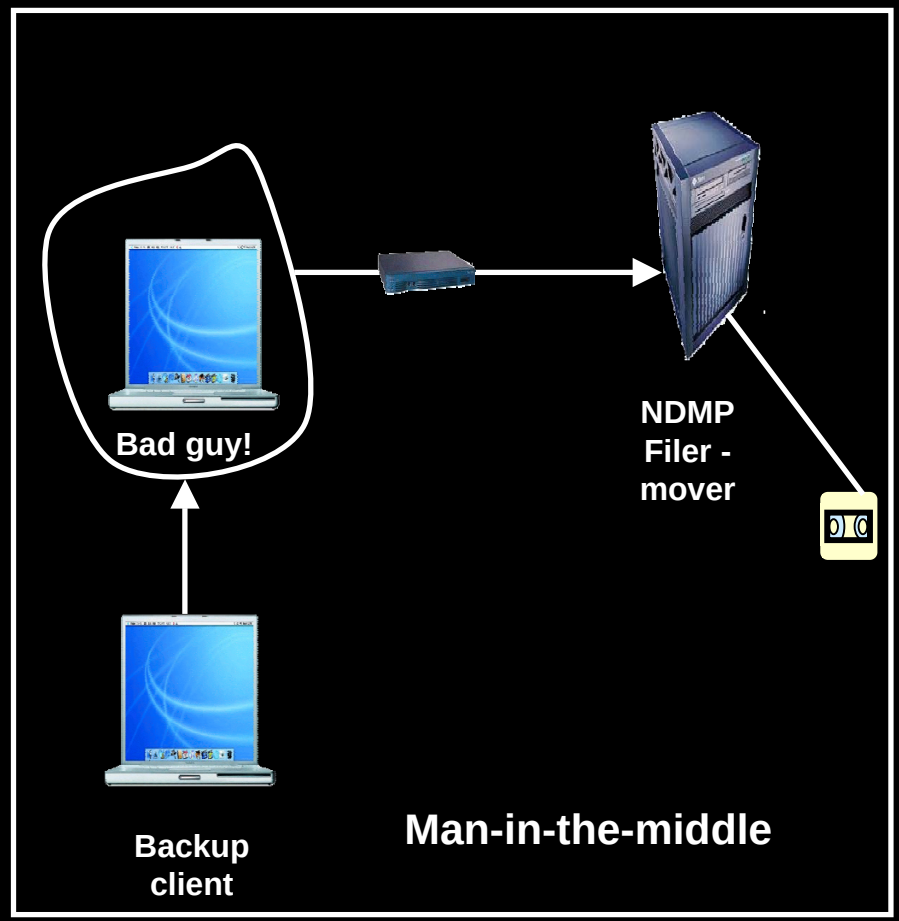


Problems

- Plain text authentication
  - No security
- MD5 digest authentication
  - Protection from replay attacks rests on the strength of random challenge string handling on the server
  - Server authentication not enforced
  - Most importantly, provides no support for encryption over the wire

Possible Attacks





NDMP v4 Security Extension

Goals:

- **Allow authentication of all connection end-points**
- **Ensure message integrity**
- **Support over-the-wire encryption**
- **Leverage the extensibility of NDMP v4 protocol**
  - **Dynamically detect the support for secure NDMP**
  - **Remain compatible with servers/DMAs that do not support secure NDMP yet**

ORACLE

Key Ingredient - SSL

SSL fulfills all our goals as described previously:

- End-point authentication
  - Achieved by means of certificate exchange during SSL handshake
- Over the network encryption of data and control messages
  - The encryption algorithms to use are negotiable for performance reasons
  - Negotiated during SSL handshake
- Message integrity
  - Ensured by the use of message authentication code (MAC)

Scope

Prerequisite for SSL support:

- **Servers and DMAs should possess a valid X.509 certificate from a trusted authority**

Out of scope:

- **Procedure of obtaining X.509 certificates**
- **Encryption of data at rest**

Protocol Implementation Details

Overview of changes

- New NDMP auth type
  - NDMP_AUTH_SSL
- New control messages
  - NDMP_SEC_SSL_LISTEN
  - NDMP_SEC_DATA_SSL_CONNECT
  - NDMP_SEC_DATA_SSL_LISTEN
  - NDMP_SEC_MOVER_SSL_CONNECT
  - NDMP_SEC_MOVER_SSL_LISTEN
- New Data service/Mover states
  - NDMP_DATA_STATE_SSL_LISTEN
  - NDMP_MOVER_STATE_SSL_LISTEN

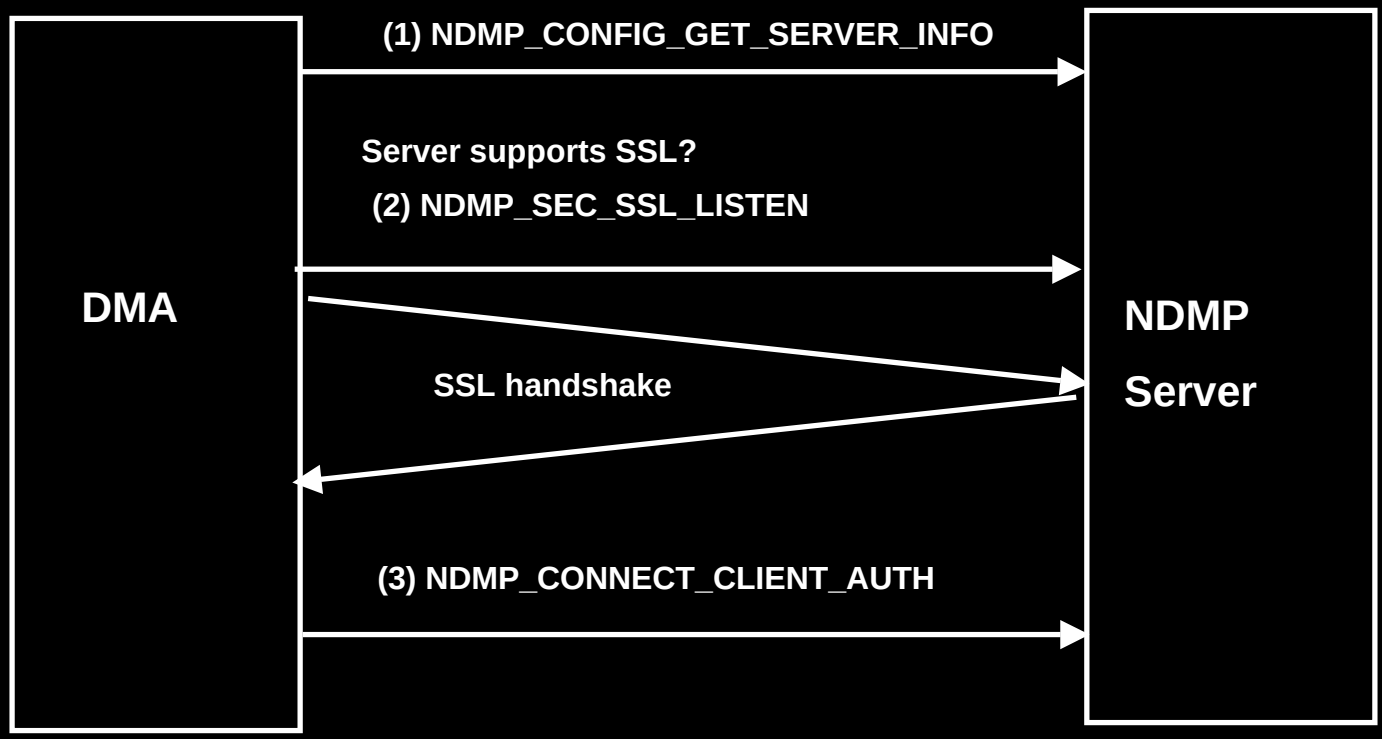
Advertising SSL support

- NDMP_CONFIG_GET_SERVER_INFO response

```
enum ndmp_auth_type
{
    NDMP_AUTH_NONE   = 0,
    NDMP_AUTH_TEXT   = 1,
    NDMP_AUTH_MD5    = 2,
    NDMP_AUTH_SSL    = 3
}
```

- NDMP_CONFIG_GET_EXT_LIST response
  - Only sent after the NDMP_CONNECT_CLIENT_AUTH request
  - Extension class: 0x20C0

NDMP_SEC_SSL_LISTEN



NDMP_SEC_SSL_LISTEN

- Can be sent prior to client authentication
  - Client authentication can happen over SSL
- Used to set up SSL over the control connection
- Initiated by DMA
- Error codes
  - NDMP_NO_ERR
  - NDMP_ILLEGAL_STATE_ERR
    SSL already setup
  - NDMP_SEC_SSL_INIT_ERR
    SSL initialization error
  - NDMP_NOT_SUPPORTED_ERR
    SSL extension not supported

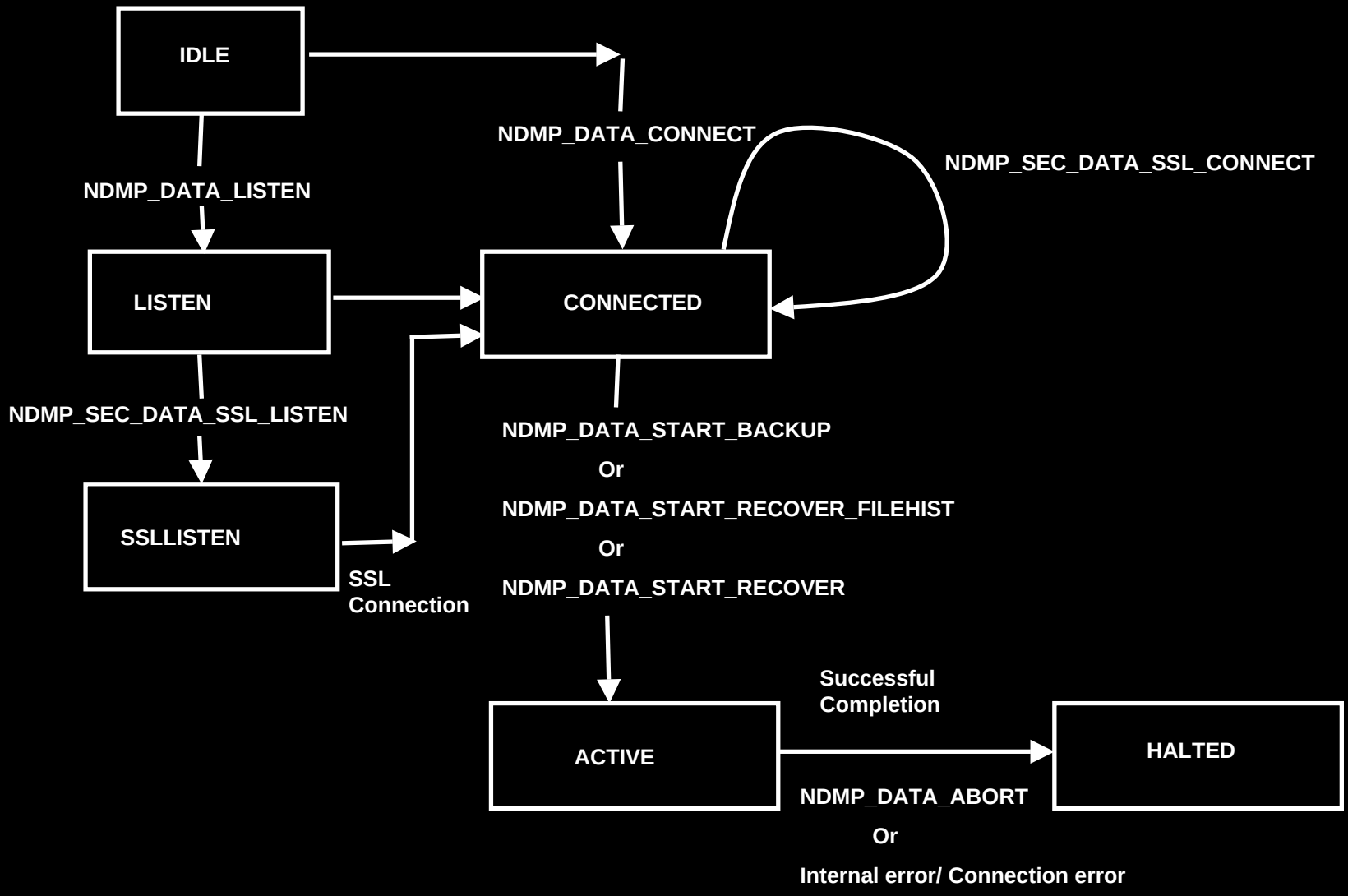
NDMP_SEC_DATA_SSL_LISTEN

- DMA instructs data server to create SSL connection end point
- Error codes
  - NDMP_NO_ERR
  - NDMP_ILLEGAL_STATE_ERR
    SSL already setup for this connection
  - NDMP_PRECONDITION_ERR
    Received before NDMP_DATA_LISTEN
  - NDMP_SEC_SSL_INIT_ERR

NDMP_SEC_DATA_SSL_CONNECT

- DMA instructs the data server to complete SSL handshake
- Error codes
  - NDMP_NO_ERR
  - NDMP_ILLEGAL_STATE_ERR
    SSL already setup
  - NDMP_PRECONDITION_ERR
    Received before NDMP_DATA_CONNECT request
  - NDMP_SEC_CERT_NOT_OK
    Verification of peer certificate failed
  - NDMP_SEC_SSL_INIT_ERR

Data server state diagram



NDMP_SEC_MOVER_SSL_LISTEN

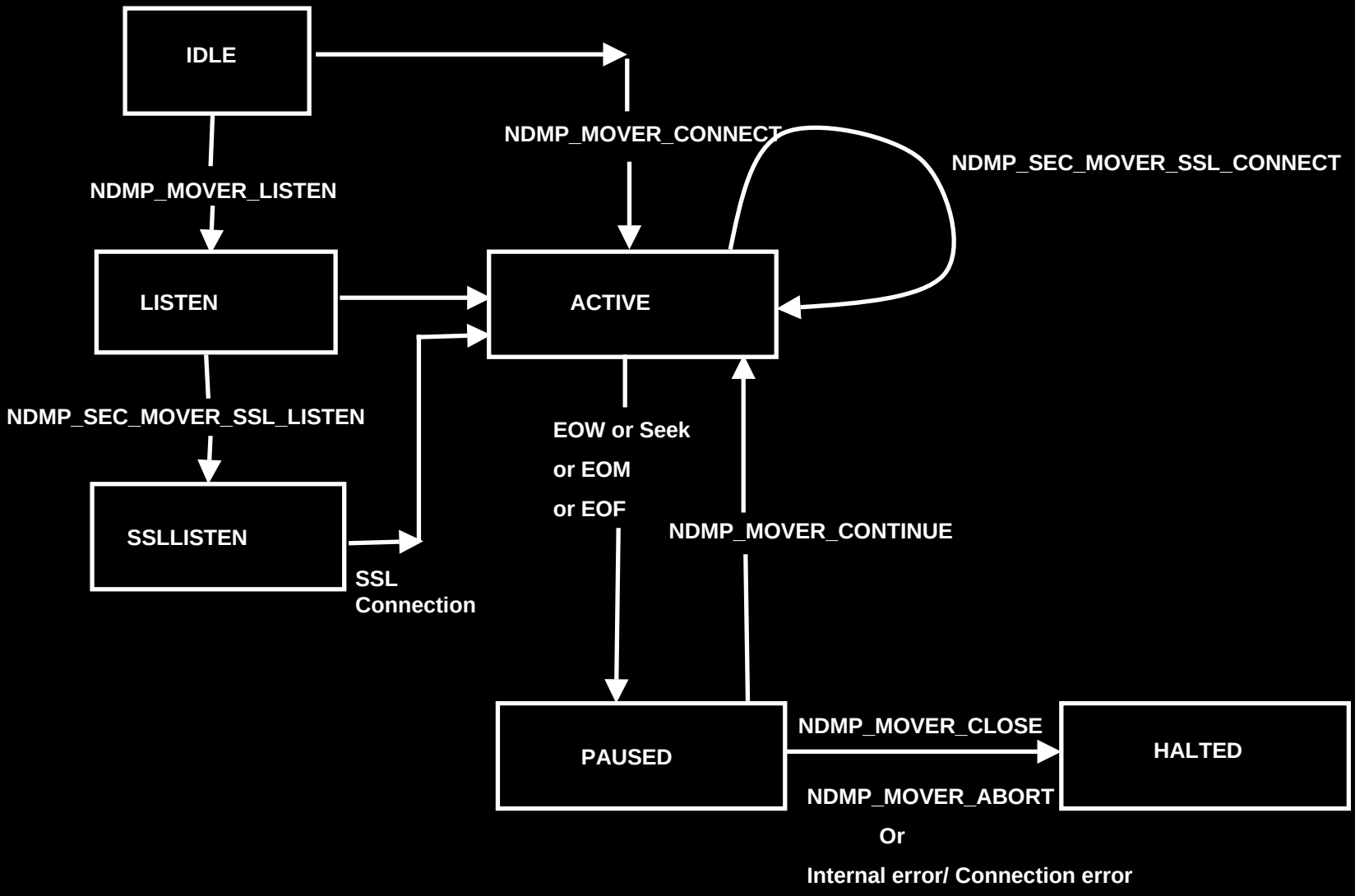
- DMA instructs mover to create SSL connection end point
- Error codes
  - NDMP_NO_ERR
  - NDMP_ILLEGAL_STATE_ERR
    SSL already setup
  - NDMP_PRECONDITION_ERR
    Received before NDMP_MOVER_LISTEN
  - NDMP_SEC_SSL_INIT_ERR

NDMP_SEC_MOVER_SSL_CONNECT

- DMA instructs the data server to complete SSL handshake

- Error codes
  - NDMP_NO_ERR
  - NDMP_ILLEGAL_STATE_ERR
    SSL already setup
  - NDMP_PRECONDITION_ERR
    Received before NDMP_MOVER_CONNECT
  - NDMP_SEC_CERT_NOT_OK
    Verification of peer certificate failed
  - NDMP_SEC_SSL_INIT_ERR

Mover state diagram



Real World Implementation

- This extension has been implemented in Oracle Secure Backup 10.1, our new centralized tape backup management software


QUESTIONS
ANSWERS