NP-93: NameFLOW-Paradise piloting X.500(93) - Phase Two -

Date: 5 February, 1997
Reference: VB(97)005
version: 1

Description:
        Inter working and Scaling test
Time schedule:
        Preparations: January 1997 and onwards
        Testing: 19 -23 May, 1997
        Evaluation: To be determined
Participants:
        Open to both NP customers and other organisations
Mailing list:
        NP-93@dante.org.uk

Introduction

The goal of the NameFLOW-Paradise X.500(93) pilot (abbr. NP-93) is to determine which Directory technology is suitable for a global Directory. The pilot will assess if current X.500(93) implementations can fulfil this requirement. An overview of the NP-93 pilot is given in the Framework document (see [1]). This document describes phase two of NP-93 with a focus on interworking and large scale directories. The previous tests, Initial Experience Test and the Root Context Test have been successfully completed. This Phase Two document starts with the results of the Phase One. It contains a description of the preparations required for the tests, an introduction to the tests and the proposed test structure including schema definitions. In addition there is a short explanation on how test results should be submitted and a time schedule when the test will take place. After the test period, the results will be made available in a separate report.

Phase One: The Root Context Test

The primary objective of Phase One was to test top level replication referred to as the Root Context. The replication uses the Directory Information Shadowing Protocol (DISP) which was newly introduced in the X.500(93) standard. The second objective was to test basic DAP and DSP including the X.500(93) extensions. The third objective (if possible) was to test the significantly changed Access Control model of X.500(93). The complete test plan is available via the web [2].

Phase One: The Results

The Root Context Test was successful, however some shortcomings were detected in both the

software and the standard itself. This paragraph gives a short summary of the test results; the full report is available via [3]. Phase one indicated that there are no major problems with DAP and DSP. DISP is a relatively new protocol and is only partially implemented and suffered clearly from teething problems. The Root Context proposal was tested and further shortcomings were discovered. These defects have been submitted to the ISO, have been accepted and technical corrigenda have been prepared. Access Control is very different from the Quipu model and automatic conversion could be optimised. Although LDAP was not oficially part of the test, some LDAP test were performed but failed as an outdated or non-standard version of the protocol was supported. A major improvement were the new management and conversion tools. The overall value judgement of the testers was that the products were "almost ready" for usage in a production environment. Phase two starts one year after Phase One so the vendors have had ample time to correct software faults and fix the defects.

Objective Phase Two: Interworking and Scaling

Phase two is a continuation of phase one and extends the objectives of Phase One. Phase two will test interworking - from a user perspective - on a real life network between different X.500(93) and other directory implementations such as Quipu and LDAP servers/clients. This is significantly different from conformance testing where an implementation is "compared" with the standard to prove conformance. This interworking test will focus on coexistence of X.500(93) with the existing Quipu implementations and with LDAP servers. The other objective is to test large data sets, e.g. a university with thousands of entries would be an excellent candidate for this test. Participants can be organisations with an interest in X.500(93) including the traditional NP customers.

Preparation

The tests will take up one week. To make the test week efficient and successful a number of preparations must to be made prior to start date. Currently the following five steps are anticipated:

1. Hardware and network

The first preparation is getting the hardware and network connection in place. Most of the participants will have easy access to an operational machine ready for testing with an adequate (wide area) network connection via TCP/IP. For the lower layer connectivity participants must use TCP/IP (with RFC 1006), although other transport stacks can be tested.

2 Software installation

The second preparation is the software, starting with installation of an operating system on the test machine. The directory software package must be obtained, unpacked, compiled if necessary, and configured locally.

3 Data acquisition

The third preparation is the data acquisition or data conversion. The Directory information needs to be collected and translated into the correct format. In a best case scenario the data can be converted or synchronised from an existing Directory format (e.g. EDB format) to the required format.

4 Getting connected

The fourth preparation before testing is getting the DSA connected to the rest of the infrastructure (external configuration). For the Root Context or FLDSAs this will be in coordination with ULCC and for others with their local (national) FLDSA maintainers.

5. Remote target system

The final step is finding a remote target DSA or other system to test against. The goal of the test is to demonstrate interworking over a live network, so part of the tests have to be done remotely.

To allow easy communication a restricted mailing list will be operational, <np-93@dante.org.uk> (where subscription will be moderated/restricted to participants only). During the start of the test an overview of all list subscribers will be distributed.

Schema definition

The minimum schema that must be supported by the test systems should include at least the following object classes: "country", "organisation", "organizationalUnit", "applicationProcess", "applicationEntity", "person", "organizationalPerson" and "newPilotPerson". (OID of newPilotPerson0.9.23.42.19200300.100.4.4)

Test structure

The test set up is based on the client-server model. For the first (L)DAP tests a client or Directory User Agent will directly test interworking to the local server or Directory Systems agent.

```
      ---------              ---------
     |  DUA    |<--------->|  DSA    |
      ---------      DAP     ---------
       client                 server
```
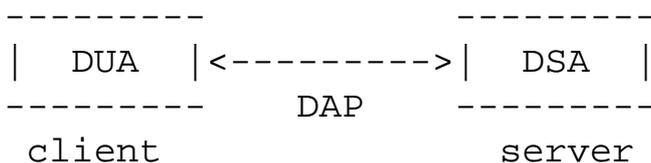
The second test set is similar to the first set, but this time the target server is a remote DSA. (I.e. still using (L)DAP, but over the wide area network)

To test the Directory Systems Protocol the DUA will make a connection to a local server and, from there, test the remote system using DSP. This mode of operation is called chaining.

```
      ---------              ---------              ---------
     |  DUA    |<--------->|  DSA    |<--------->|  DSA    |
```

```
    ---------     DAP     ---------     DSP     ---------
     client               local server         remote server
```

The replication of Directory Information (shadowing) will be done
between two DSAs that will act in a consumer and supplier role.

```
    ---------               ---------
   |  DSA  |<---------->|  DSA  |
    ---------    DISP       ---------
     consumer               supplier
```

This type of replication requires a shadow agreement between the two parties. For these tests a specific type of replication will be used which will allow replication between First Level DSAs.

Test Data

The test structure of the directory information tree (DIT) will be similar to the current infrastructure with supplementary NP-93 entries for the organisations participating in the test. For the basic test set-up a participant must add an organisational unit entry:

```
OU= NP-93
```

to their organisation entry:

```
O= my_org
```

with several test entries; five persons, an applicationProcess and an applicationEntity.

An example for a test person under c=GB, o=DANTE, OU= NP-93:

```
Common Name = Person One
Surname = Digger
Description = Salvage Clerk
Telephone Number = +44 1902 111111
Etcetera
```

The content of the entries will be defined in the NP-93 test document that will be provided. The suite will include tests for DAP and DSP, DISP test for the Root Context, ACI tests and some specific LDAP tests.

The Tests

The tests suites are largely based on the EuroSInet interworking test suites but are modified for the NP-93 specific requirements. A (draft) version of the test suite document will be distributed to the

participants of the test only.

All tests have a short description: purpose, procedure and expected results. For example, the first test would be:

```
#1 Bind Test
Purpose: Bind anonymous to a DSA
Procedure: The DUA issues a BIND operation to the responding
DSA with no credential information (anonymous bind)
Expected Results: The test is successful if the DAP connection
can be established without errors
```

DAP and DSP

For the DAP and DSP there are three sets tests:

> 1) DAP tests between DUA and DSA,
> 2) DSP tests between two DSAs and
> 3) extended scenario for more than two DSAs.

The following test operations will be performed: Bind, Read, Search, List, Remove and Unbind. The extended DAP test includes test for 93 specific attributes and Sub entries. For DSP there is an extended scenario to test Chaining and Referrals. This test is relevant to test X.500 in a distributed and live network.

Scaling

One of the objectives of this particular phase is to test Directory Servers with medium to large data sets. These are typically DSAs run by universities with tens of thousands of entries or a DSA collecting/ hosting information for several other organisations. The DSAs tested will hold an exact (or similar in size) copy of the real data set. This phase could include an LDAP server for a large organisation.

Coexistence with LDAP

The current popularity of LDAP needs to be taken into account for this test. The majority of queries within NP are received via LDAP (usage from the WWW) and more applications are starting to support native LDAP as the directory protocol. In addition Directory Servers based on LDAP are being shipped by the large software vendors for acceptable prices. In this context the X.500(93) infrastructure can provide a backbone for LDAP Directory Servers. The LDAP coexistence test has two objectives:

1. test Directory access using the LDAP protocol, and

2. test the interworking between stand-alone LDAP Directory servers and the X.500 infrastructure.

The first set of tests can be done via WWW interfaces or other LDAP clients. A special condensed/ reduced LDAP test set will be made available to the LDAP test participants.

The second step to test the interworking will require an additional software module to bridge the gap between X.500 and LDAP. One product currently available is the X.500 Enabler and this will be put to the test with an stand-alone LDAP Directory Server.

Coexistence with Quipu

The majority of today's DSAs are using Quipu software (or X.500(88) plus enhancements) and it is assumed that not all DSAs are going to support X.500(93). To allow the connection of the current installed base with the planned X.500(93) infrastructure, coexistence has to be assured. During the transition it is expected that some organisations will run two DSAs in parallel, one using Quipu and one using X.500(93). The top-down transition model will make things easier as Quipu DSAs will only be operated as subordinate DSAs. The Quipu to X.500(93) interworking has partially been demonstrated in the previous test phase. However, the experimental tests performed at that time were not complete and need verification. It is the objective to incorporate at least one Quipu implementation in the tests, preferably a supported version and possibly an unsupported/free-ware version (i.e. versions until ISODE release 8.0).

Access Control

The Access test will focus on Basic Access Control as this is the minimal level that is implemented and can be tested. The basic operations performed are Read, Modify, List and Search. Entries with different Access Control will be created and operations should be allowed or rejected according to the Access Control Information. The Modify and ModifyDN operations may be tested. (Note that Modify and ModifyDN are not part of the DAP and DSP tests as they were considered vendor specific and are used by local administrators, not end users. The test will be limited to Access Control on a single DSA and replicated Access Control will remain outside the scope of this test phase.

DISP and Root Context

The Root Context is an important aspect; it provides a key function in the current infrastructure as it manages the connections between all First Level DSAs. The root functionality of the current Root DSA needs to be maintained for two reasons: it allows easy management of First Level knowledge references and provides central replication optimising the service. A full description on "Managing the Root Context" is written by David Chadwick [4]. The part that will be tested in this phase is the interim solution proposed in section four.

The DISP tests specify only two specific subsets of replication supported by all vendors. Both subsets replicate all attributes and Master and Shadow knowledge. The difference between the two subsets is that the replicated area component is "complete naming context" and "complete subtrees".

Unfortunately the two subsets do not provide sufficient functionality for the proposed interim solution. A Root Context test profile has been submitted as draft by David Chadwick to Integrated Directory Services Working Group at the IETF and this document is used to test replication for the root context. (See <URL:http://www.dante.net/np/ds/profile.html>).

To ensure continuity of the testing an out-of-band (i.e. ftp) replication mechanism will be available for the participants, if the Root Context replication via DISP fails.

Results

The results can be submitted in two ways. The first method is sending the results to the NP-93 mailing list. The second method will be to submit the results via a web page. This page will be made available via <URL:http://www.dante.net/np/93pilot>. At the end of the test the results will be collected, made anonymous and published in a report.

Time schedule

The week of 19 through 23 May 1997 is reserved to complete the tests. The preparations should be done prior to the test week, however the first day is reserved to install final bits of the software and make the proper arrangements for DSP and DISP connections.

Participants

There are over 10 (?) participants from 7 (?) different countries.

References

[1] "NameFLOW-Paradise piloting X.500(93) - Framework", Vincent Berkhout, DANTE Docs VB (97)004, <url:http://www.dante.net/np/93pilot/framework.html>

[2] "NP-93: Root Context Test Plan", Vincent Berkhout, DANTE Docs VB(96)006, <url:http://www.dante.net/np/93pilot/phase1-plan.html>

[3] "NP-93: Root Context Test Results", Vincent Berkhout, DANTE Docs VB(96)015, <url:http://www.dante.net/np/93pilot/phase1-results.html>

[4] "Managing the Root Context", David Chadwick, "DANTE in Print #18", <url:http://www.dante.net/pubs/dip/18/root.txt>

[5] "X.500 Shadowing Profiles", David Chadwick, draft-ietf-ids-x500-shadprof-00.txt (Expired January 1997, copy available via <url:http://www.dante.net/np/ds.html>)