Stonebranch Solutions

Indesca
Certificates and Command References
Implementation

indesca-certandcmdref-imp

Document Name	Indesca - Certificates and Command References Implementation
Document ID	indesca-certandcmdref-imp
Products	Universal Command

Stonebranch, Inc.
950 North Point Parkway, Suite 200
Alpharetta, GA 30005 USA
Tel: (678) 366-7887
Fax: (678) 366-7887

Stonebranch, Inc.® makes no warranty, express or implied, of any kind whatsoever, including any warranty of merchantability or fitness for a particular purpose or use

The information in this documentation is subject to change without notice.

Stonebranch shall not be liable for any errors contained herein or for incidental or consequential damages in connection with the furnishing, performance or use of this document.

All products mentioned herein are or may be trademarks of their respective owners.

SAP Certified Integration

Contents

Implementation Scope

Note: This implementation utilizes Indesca’s Universal Command component.

Schedule Netbackup and CA Access functions on UNIX that require root access to run. Scheduling of these functions will be managed with CA 7 and Universal Command.

In order to secure access to the root userid and ensure that only the required functions can be initiated with root authority via Universal Command, Stonebranch recommends implementation of the X.509 certificate and Command Reference features of Indesca.

Access to the root id on UNIX systems will be authenticated using an X.509 certificate. The commands available to the root id with be controlled using the Command Reference feature of Indesca.

X.509 Certificates Introduction

A certificate is an electronic object that identifies an entity. It is analogous to a passport. Just like a passport, certificates must be issued by a party that is trustworthy by all who accepts the certificate. Certificates are issued by trusted parties called Certificate Authorities (CAs). For example, VeriSign Inc. is a CA that most parties trust. We all have faith that a trusted CA takes the necessary steps to confirm a user's identity before issuing them a certificate.

Certificate technology is based on public/private key technology. There are a few different types of public / private keys: RSA, DH, and DSS. As their name denotes, the private key must be kept private like a password. The public key can be given to anyone or even published in a newspaper.

A property of public / private keys is that data encrypted with one can only be decrypted with the other. Therefore, if someone wants to send you a secret message, they encrypt the data with your public key, which everyone has. However, since you are the only one with your private key, you are the only one who can decrypt it. If you want to send a message to someone, such as a request for $100,000 purchase, you can "sign" it with your private key. Note that signing does not encrypt the data. Once the person receives your request, they can verify it is from you by verifying your electronic signature with your public key.

A certificate ties a statement of identity to a public key. Without the public key, the certificate is meaningless. Possession of a certificate alone does not prove your identity. You must have the corresponding private key. The two together prove your identity to any third party that trusts the CA that issued your certificate. That's a key point: if you don’t trust the CA that signed a certificate, you cannot trust the certificate.

Command References Introduction

Command references are predefined commands or scripts saved in files on the Universal Command Server system. Universal Command Managers can request command references to be executed by specifying a COMMAND_TYPE value of cmdref. The Manager specifies the command reference by name. The Server finds the command reference file and executes the command or script contained within the command reference.

A command reference provides the ability to precisely define and control what is executed by the Server. The Manager does not provide any commands or scripts. Everything is defined within the command reference. The command reference optionally can be defined to accept command or script options from the Manager.

By implementing Universal Access Control List (UACL) entries, command references can be used to control the specific commands that can be executed by any user under the control of Universal Command.

Implementation Description

Overview

The following steps are required to implement certificates with Universal Command for the purpose described in the previous section of this document:

1. Create Certificate Authority and User Certificate – One time action, completed.
2. Configure Server – One time action for each server.
3. Create Command Reference.
4. Modify JCL

Create Certificate Authority and User Certificate

For this implementation, a single certificate authority (CA) and a single certificate is required. The CA and certificate have already been generated on the mainframe using the example JCL provided in the `#HLQ.UNV.SUNVSAMP(UCRSAM1)` and `#HLQ.UNV.SUNVSAMP(UCRSAM2)`members.

The CA private key was generated to the following dataset:

```
MIS.UCERT.CA.PKEY
```

This dataset must be kept secured. It is recommended that only the CA 7 runtime userid has read access to this dataset.

The CA public certificate was generated to the following dataset:

```
MIS.UCERT.CA.CERT
```

This dataset must be made available (physically copied) to each server that requires to validate the user certificate. This is detailed in the Configure the Server section.

The User private key was generated to the following dataset:

```
MIS.UCERT.TEST.PKEY
```

This dataset must be kept secured. It is recommended that only the CA 7 runtime userid has read access to this dataset.

The User certificate was generated to the following dataset:

```
MIS.UCERT.TEST.CERT
```

This dataset will be presented to the server as part of the session negotiation performed by Universal Command.

Configure the Server

The following steps are required for the one-time configuration of each server, root access will be required to complete some of these steps:

1. Create the directory `/opt/universal/CA`.
2. Copy the CA certificate file (`MIS.UCERT.CA.CERT`) in text mode to:
   `/opt/universal/CA`.
3. Update the `/etc/universal/ubroker.conf` to include the following parameter:
   `ca_certificates       /opt/universal/CA/MIS.UCERT.CA.CERT`
4. Replace `/etc/universal/uacl.conf` with the following:

```
cert_map
'id=SCHED,subject="/C=US/ST=Georgia/L=Alpharetta/O=XXX/CN=CA7.PROD.MAIN
/"'

ucmd_access ALL,*,root,deny,auth


ucmd_cert_access       SCHED,root,allow,noauth
ucmd_cert_access       *,*,deny,auth

ucmd_request         *,*,cmdref,*,deny,auth


ucmd_cert_request      SCHED,root,cmdref,*,allow,noauth
ucmd_cert_request      SCHED,root,*,*,deny,auth
```

5. Recycle the ubroker daemon.

Create Command Reference

For each command that is required to be run with root access, create a command reference in the `/var/opt/universal/cmdref` directory. Ensure that only authorized personnel are able to create or update command reference files in this directory.

The following example is for the Netbackup process and corresponds with the JCL example in the next section.

```
# Example Command Reference
# Execute Netbackup Command
#
-format script
-type   shell
-allow_options yes
<eof>
bpbackup $1
```

JCL Set-up

CA 7 batch jobs needing to use the User Certificate to authenticate for root access require some additional SYSIN DD parameters and DD statements.

SYSIN DD Parameters

The following additional SYSIN DD parameters are required:

- CERT specifies the DDNAME that allocates the User Certificate dataset.
- PRIVATE_KEY specifies the DDNAME that allocates the User Private Key dataset.

Script Parameter

The -SCRIPT parameter is replaced by:

- CMD_TYPE is used to specify that a command reference will be used.
- CMD parameter specifies the command reference and associated parameters.

```
-cert          CERT
-private_key   PKEY
-cmd_type         cmdref
-cmd                 "cmd_reference_name cmd_reference_parameters"
```

DD Statements

The User Certificate and the User Private key must be allocated in the Universal Command JCL.

```
//CERT     DD  DISP=SHR,DSN=MIS.UCERT.TEST.CERT
//PKEY     DD  DISP=SHR,DSN=MIS.UCERT.TEST.PKEY
```

JCL Example

```
//ZOPRRSEC JOB P015095Y01685000,'OPR-TEST U/C W',
//   CLASS=8,MSGCLASS=Z,REGION=0M
//*
//**********************************************************
//**********************************************************
//**                                                      **
//** Test running on adcsecacsq2 certificates             **
//**                                                      **
//**********************************************************
//*
//JS000100 EXEC UCMDPRC       ,CMD=ADCSECQ2
//UNVOUT   DD  SYSOUT=*
//PWDDD    DD  DISP=SHR,DSN=MIS.PRDT.DATA(DUMMY)
//CERT     DD  DISP=SHR,DSN=MIS.UCERT.TEST.CERT
//PKEY     DD  DISP=SHR,DSN=MIS.UCERT.TEST.PKEY
// EXEC UCADCSEC
```

JCL Notes

1. The SCRIPT DD that can be found in Universal Command is not required.
2. A 'dummy' encrypted password member is required.

The included member UCADCSEC expands to:

```
//UCADCSEC DPROC
```

```
 -HOST            adcsecacsq2
 -u               root
 -f               PWDDD
 -CERT            CERT
 -PRIVATE_KEY     PKEY
 -cmd_type        cmdref
 -cmd             "bpbackup -p AC_AIX_QA -i -h adccaq1 -t 0 -s Inc -
w”
 -MANAGERFT       YES
 -G               no
//   DNEST UCCMDID
```

Notes for Implementing on Windows Servers

Windows environments differ from UNIX systems in the following ways:

1. The Windows operating system environment does not support the 'noauth' option for the Universal Access Control Lists. This means that a valid password is still required for all Universal Command sessions.
2. The Universal Products configuration options are stored in the windows registry and are edited via the Universal Configuration Manager control panel applet.
3. The default location for command references is `C:\Program Files\Universal\cmdref`.

stonebranch

950 North Point Parkway, Suite 200
Alpharetta, Georgia 30005
U.S.A.