Network Working Group	Wilkinson
Internet-Draft	YFS
Intended status: Informational	December 7, 2010
Expires: June 10, 2011	

TOC

Adding Extended Authentication Names to the Bos Super User list
draft-wilkinson-afs3-bos-identities-00

Abstract

This document describes an additional set of RX remote procedure calls which may be used to managed extended authenticated names within the AFS-3 basic overseer service's SuperUser list

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as “work in progress.”

This Internet-Draft will expire on June 10, 2011.

Table of Contents

1. Introduction

TOC

AFS-3 provides a management service (the "basic overseer service", or "bos" for short) which manages service wide configuration information, and launches the daemons which provide each of the individual AFS services. This management service also maintains a list of identities which are granted super user privileges to bos itself, and to the services it manages. This list is maintained via a number of RX remote procedure calls which can be used to list, add, and remove identities. Traditionally, AFS-3's security model was Kerberos v4 based, and the existing RPCs for managing the super user list are based around Kerberos v4 names.

Extended authentication names (Brashear, D., “Authentication Name Mapping extension for AFS-3 Protection Service,” November 2010.) [I-D.brashear-afs3-pts-extended-names] provide a mechanism for encapsulating a wider variety of name types within the AFS-3 system. These new identity types bring with them a requirement to be able to manipulate bos super user lists containing extended identities.

2. Error codes

TOC

The existing BZNOENT, BZEXISTS and BZPERM error codes are used by the RPCs defined within this document.

3. RPC Interface

TOC

Three new RPCs are defined for the bos service. These are direct equivalents of existing RPCs, with the exception that they add support for extended authentication names.

TOC

3.1. AddSuperIdentity

This is a direct equivalent of the existing AddSUser call. It adds an identity to the service's super user list.

```
AddSuperIdentity(IN struct PrAuthName *name) = XXX;
```

On success, the call returns 0. If the user doesn't have sufficient permission, then BZACCESS is returned. If the given identity already exists within the super user list BZEXISTS is returned.

When called with a name with the PRAUTHTYPE_KRB4 data type (a Kerberos v4 name), the behaviour of this function MUST be identical to that of the existing AddSUser function.

3.2. DeleteSuperIdentity

TOC

This is a direct equivalent of the existing DeleteSUser call. It deletes an identity from the service's super user list.

```
DeleteSuperIdentity(IN struct PRAuthName *name) = XXX;
```

On success, the call returns 0. If the user doesn't have sufficient permission, then BZACCESS is returned. If the identity doesn't exist within the super user list, then BZNOENT is returned.

When called with a name with the PRAUTHTYPE_KRB4 data type the behaviour of this function MUST be identical to that of the existing DeleteSUser function

---

3.3. ListSuperIdentities

TOC

This is an equivalent to the existing ListSUsers call. It provides a mechanism for building an iterator over the server's super user list.

```
ListSuperIdentities(IN afs_int32 cookie,
                    OUT struct PRAuthName *name,
                    OUT afs_int32 *newcookie) = XXX;
```

The first time this function is called, cookie MUST be set to 0. The server will then return the first entry in the super user list (or BZNOENT, if the super user list is empty). In newcookie, it will return a value that can be used to obtain the next entry from the

server, or 0 if the current entry is the last one. The client may then repeat its call using newcookie as the cookie value, until it has obtained the desired number of entries, or until newcookie is 0, and the iteration is complete.

This call MUST return all super users registered with the bos server, regardless of whether they were created using the RPCs defined in this document, or by the existing AFS-3 bos RPCs. Names created through the AddSUser interface should be returned as PRAuthNames with the PRAUTHTYPE_KRB4 type, as detailed in the extended authentication name specification.

On success, the RPC will return 0. If the user doesn't have sufficient permissions to read the super user list, then BZACCESS is returned. If an entry pointed to by a specific cookie has ceased to exist, or if the super user list is empty, then BZNOENT is returned.

---

4. Behaviour of existing RPCs

TOC

The existing RPCs, and the ones described within this document, MUST both provide access to the same super user list. Where equivalent functionality is available to both new, and old, RPCs, there should be no observable difference between using the old or new forms.

Calling AddSUser must have an identical result to calling AddSuperIdentity on the corresponding Kerberos v4 name

Calling DeleteSUser must have an identical result to calling DeleteSuperIdentity on the corresponding Kerberos v4 name

The ListSUsers RPC only iterates over Kerberos v4 form names. Due to the behaviour of existing clients spaces MUST NOT be left in the iteration sequence for extended identities in the user list. This means that ListSUsers will present an incomplete view of the super identities present on a particular server. Consideration SHOULD, therefore, be given to removing the ListSUsers call when support for the RPCs listed in this document is added.

---

5. Security Considerations

TOC

Current AFS-3 implementations provide a high degree of access to identities on the super user list. Whilst this document doesn't proscribe particular levels of access control for the RPCs it specifies, implementers should consider whether restricting these RPCs to particular security classes, and protection levels, is appropriate

PrAuthNames contain both display and exported name forms, with the display name being provided purely for user interface purposes. When returning names to the client, servers MUST regenerate the display

name from the given exported name. Where regeneration is impossible (for instance, because the name's underlying mechanism is unavailable), servers must indicate that the display name is unverified.

6. IANA Considerations

TOC

This document doesn't require any IANA registrations.

7. AFS-3 Registry Considerations

TOC

This documentation requires the registration of code points for the 3 new RPCS detailed above.

8. Normative References

TOC

[I-D.brashear-afs3-pts-extended-names]	Brashear, D., "Authentication Name Mapping extension for AFS-3 Protection Service," draft-brashear-afs3-pts-extended-names-07 (work in progress), November 2010 (TXT).

Author's Address

TOC

	Simon Wilkinson
	Your File System Inc
Email:	simon@sxw.org.uk