Groupe de travfail Réseau
Request for Comments : 5021
RFC mise à jour : 4120
Catégorie : En cours de normalisation

S. Josefsson
SJD
août 2007
Traduction Claude Brière de L'Isle

Extension d'échanges du centre de distribution de clé de Kerberos version 5 sur TCP

Résumé
Le présent document décrit un mécanisme d'extension pour la version 5 du protocole Kerberos utilisé sur un transport TCP. Le mécanisme utilise le bit réservé de poids fort dans le champ de longueur. Il peut être utilisé pour négocier des extensions Kerberos spécifiques de TCP.

1 Introduction

La spécification Kerberos V5 [3] réserve, à son paragraphe 7.2.2, le bit de plus fort poids du champ de longueur initiale pour l'expansion future du transport TCP. La présente mise à jour du document [3] décrit le comportement lorsque ce bit est établi. Ce mécanisme est destiné aux extensions spécifiques du transport TCP.

2 Conventions utilisées dans ce document

Dans le présent document, les mots clé "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14 [RFC2119].

3 Mécanisme d'extension pour le transport TCP

Le bit réservé de fort poids du champ longueur de la demande est utilisé pour signaler l'utilisation de ce mécanisme d'extension. Lorsque le bit réservé est établi dans le champ de longueur, les 31 bits restants des quatre octets initiaux sont interprétés comme une table de concordance binaire. Chaque bit du gabarit binaire peut être utilisé pour demander une extension particulière. Les 31 bits forment le "gabarit binaire d'extension". Il est prévu que d'autres documents décrivent le détail des significations des bits particuliers.

Une valeur de 4 octets avec le seul bit de plus fort poids établi, et donc tout le gabarit binaire d'extension à zéro, est appelé SONDE *(PROBE)*. Un client peut envoyer une sonde pour découvrir quelles extensions prend en charge un KDC *(centre de distribution de clés)*. Un client peut aussi établir des bits particuliers directement dans le gabarit binaire de l'extension, si il n'a pas besoin d'interroger le KDC sur les extensions disponibles avant de décider quelles extensions demander.

Noter que les clients ne sont pas forcés d'utiliser ce mécanisme d'extension, et de plus, il est prévu que les clients ne l'utilisent que lorsqu'ils souhaitent négocier une extension particulière.

Le protocole est le suivant. Le client DOIT commencer par envoyer une valeur de 4 octets avec le bit de plus fort poids établi *(mis à 1)*. Le paquet est donc soit une SONDE soit une demande spécifique d'une ou plusieurs extensions. Le client NE DOIT PAS envoyer de données supplémentaires avant que le serveur ait répondu.

Si un KDC reçoit une demande pour un ensemble d'extensions qu'il prend en charge, il DOIT répondre par l'envoi d'une valeur de 4 octets à zéro, c'est à dire, 0x00000000. Le KDC PEUT envoyer directement des données supplémentaires après la valeur à zéro, sans attendre la réponse du client, comme spécifié par l'extension négociée particulière. (Note : Une valeur de 4 octets à zéro ne peut jamais être envoyée par une mise en œuvre conforme à la RFC4120 et qui ne prend pas en charge de mécanisme d'extension, parce qu'une KRB-ERROR est toujours d'une taille différente de zéro.)

Si un KDC reçoit une SONDE, ou si un KDC ne prend pas en charge toutes les extensions correspondant aux bits établis dans le gabarit binaire d'extension, il DOIT retourner 4 octets avec le bit de plus fort poids mis à un, et avec le reste du gabarit binaire qui indique quelles extensions il prend en charge. Le KDC DOIT alors attendre, et le client DOIT envoyer une seconde valeur de 4 octets avec le bit de plus fort poids mis à un. Si la seconde valeur de 4 octets est une SONDE ou une extension non prise en charge, le KDC DOIT clore la connexion. Ceci peut être utilisé par le client pour terminer une session lorsque le KDC ne prend pas en charge une extension qui est exigée par le client. Si la seconde valeur de 4 octets est une extension prise en charge, le KDC DOIT répondre par l'envoi d'une valeur de 4 octets à zéro, c'est à dire, 0x00000000. Le KDC PEUT envoyer directement des données supplémentaires après la valeur à zéro, comme spécifié par l'extension négociée particulière.

Le client et le KDC DEVRAIENT attendre que l'autre côté réponde conformément au présent protocole, et le client et le KDC NE DEVRAIENT PAS clore prématurément la connexion. Des considérations de disponibilité de ressources peuvent influencer si, et pour combien de temps, le client et le KDC vont attendre que l'autre côté réponde à une demande.

Le KDC NE DOIT PAS accepter le mécanisme d'extension s'il ne prend en charge aucune extension. Si aucune extension n'est prise en charge, le KDC DOIT retourner un message KRB-ERROR avec l'erreur KRB_ERR_FIELD_TOOLONG et DOIT clore le flux TCP, comme il le ferait pour une mise en œuvre qui ne comprend pas ce mécanisme d'extension.

Lorsque plus d'un bit de moindre poids est mis à un, le comportement dépend des mécanismes d'extension particuliers. Si une extension demandée (bit X) ne spécifie pas comment elle interagit avec une autre extension demandée (bit Y), le KDC DOIT traiter la demande comme une SONDE ou une extension non prise en charge, et procéder comme ci-dessus.

Chaque extension DOIT décrire la structure des données de protocole au delà du champ de longueur, et le comportement du client et du KDC. En particulier, la structure peut être un protocole avec son propre tramage de messages. Si un mécanisme d'extension réserve plusieurs bits, il DOIT décrire leur interaction.

4 Considérations d'interaction

Les mises en œuvre qui prennent en charge TCP et qui ne revendiquent pas la conformité à la RFC 4120 peuvent ne pas traiter correctement le bit de plus fort poids. Le comportement du KDC peut comporter la clôture de la connexion TCP sans aucune réponse, et l'enregistrement d'un message d'erreur dans le journal du KDC. Au moment de la rédaction de la présente spécification, ce problème existe dans des versions modernes de mises en œuvres ordinaires de KDC. Les mises en œuvre qui rencontrent des problèmes pour obtenir les réponses espérées d'un KDC peuvent supposer que le KDC ne prend pas en charge ce mécanisme d'extension. Un client devrait se souvenir de façon semi permanente de ceci, pour éviter de déclencher à chaque fois le même comportement problématique sur le KDC. Il faut veiller à éviter les comportements inattendus de la part de l'utilisateur lorsque le KDC est finalement mis à jour. Les mises en œuvre devraient aussi fournir un moyen pour activer et désactiver cette extension domaine par domaine. La façon de traiter ces bizarreries de rétro compatibilité n'est en général pas spécifiée.

5 Considérations pour la sécurité

Comme le champ de longueur initiale n'est pas protégé, il est possible à un attaquant actif (c'est-à-dire, quelqu'un qui est capable de modifier le trafic entre le client et le KDC) de faire croire au client que le serveur n'accepte pas ce mécanisme d'extension (attaque en dégradation). De plus, les attaquants actifs peuvent aussi interférer avec la négociation des extensions qui sont prises en charge, d'où peut aussi résulter une attaque en dégradation. Ce problème peut être résolu en ayant une politique, chez les clients et dans le KDC, de rejet des connexions qui n'ont pas les

propriétés souhaitées. Le problème peut aussi être atténué en ayant une somme de contrôle chiffrée des extensions offertes dans l'extension négociée.

6 Considérations relatives à l'IANA

L'IANA a créé un nouveau registre pour les "Extensions TCP de Kerberos". Le contenu initial de ce registre est :

n° de bit	Référence
0..29	DISPONIBLE pour l'enregistrement.
30	RÉSERVÉ. RFC 5021

L'IANA va enregistrer les valeurs 0 à 29 après l'approbation de l'IESG, comme défini dans le BCP 64 [2]. L'allocation de la valeur 30 exige une action de normalisation qui mette à jour ou rende obsolète le présent document.

Politique d'enregistrement : L'IESG agira comme intermédiaire pour l'espace de nom, en considérant si l'enregistrement est justifié étant donné la taille limitée de l'espace de nom. L'IESG confirmera aussi que les enregistrements proposés ne sont pas dommageables pour l'Internet.

7 Remerciements

Nicolas Williams, Jeffrey Hutzelman, Sam Hartman, et Chris Newman ont fourni des commentaires qui ont amélioré le protocole et le document.

Remerciements à Andrew Bartlettqui a mis en évidence que certaines mises en oeuvre (MIT Kerberos et Heimdal) ne suivent pas correctement la RFC 4120 par rapport au bit de plus fort poids, d'où résulte un problème d'interopérabilité.

8 Références normatives

[1] Bradner, S., "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

[2] Narten, T. et H. Alvestrand, "Lignes directrices pour la rédaction d'une section de Considérations relatives à l'IANA dans les RFC", BCP 26, RFC 2434, octobre 1998.

[3] Neuman, C., Yu, T., Hartman, S., et K. Raeburn, "Le service d'authentification de réseau Kerberos (V5)", RFC 4120, juillet 2005.

Appendice A Conditions de copie

Adresse de l'auteur

Simon Josefsson
SJD
mél : simon@josefsson.org

Déclaration de copyright

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Remerciement
Le financement de la fonction d'édition des RFC est fourni par la Administrative Support Activity (IASA) de l'IETF.