

Statut du document	<i>Internet-Draft</i>
Titre	<i>WebDAV Access Control Protocol</i> , version 7.1 http://www.webdav.org/acl/protocol/draft-ietf-webdav-acl-07.1.htm
Mot clé	Attestation et sécurité
Source	IETF
Date de publication	Avril 2002
Nombre de pages	44
Langue	Anglais Note : Une version en français de la norme WebDAV générale de l'IETF (RFC 2518) est accessible à l'adresse http://www.ics.uci.edu/~ejw/authoring/protocol/rfc2518.fr.html .
Lien avec autres normes	Associée à WebDAV à titre d'extension, elle permet un contrôle d'accès avec le protocole HTTP 1.1 en utilisant XML.
Situation actuelle	
Description	<p>Ce document présente les méthodes, les en-têtes et les corps de message qui définissent les extensions pour le contrôle d'accès avec le protocole WebDAV. Le but est d'obtenir un mécanisme de contrôle interopérable entre serveurs WebDAV, allant du simple fichier Unix à des modèles sophistiqués. Le contrôle d'accès fait dépendre les autorisations d'une identité authentifiée par un titre, tel un certificat de clé publique, auquel est attachée une liste des autorisations par ressource, ou tout regroupement de ressources ou toutes les ressources d'un domaine donné. Un titre peut obtenir une autorisation en tant que membre d'une collection de titres (membre d'un groupe, tenant d'un rôle).</p> <p>Les privilèges (<i>privileges</i>) portent sur les méthodes applicables à une ressource : <i>lire</i> et <i>écrire</i>, applicables au contenu et aux propriétés non dynamiques d'une ressource, mais en permettant de distinguer entre la liste d'autorisation au complet et un sous-ensemble de celle-ci. Les opérations autorisées peuvent être agrégées. Le terme <i>privilege</i> circonscrit en fait deux des trois positions logiques d'un énoncé d'autorisation : le sujet (titre) est vide, seuls sont exprimés le verbe (méthode ou opération) et son complément d'objet direct (la ressource à laquelle la méthode s'applique).</p> <p>Les sujets pouvant être autorisés à effectuer une opération détiennent un titre qui doit contenir une propriété de nom affichable et une autre qui en indique le type. Dans certaines implantations, il sera avantageux de fournir un URL supplémentaire associé à un titre afin d'y placer une description plus riche du détenteur et de ses autorisations.</p> <p>Toute ressource HTTP que l'on veut protéger avec le contrôle d'accès WebDAV doit être affectée des propriétés de contrôle d'accès suivantes :</p> <ul style="list-style-type: none"> - Titre du détenteur. - Ensemble des privilèges associés à la ressource (<i>supported privilege set</i>) comme une structure XML visualisable en arborescence (cette forme d'affichage est considérée comme ergonomique et est proposée pour aider la création de la liste des autorisations). - Ensemble des privilèges associés à l'utilisateur courant dûment authentifié (<i>current user privilege set</i>). - La liste complète des entrées d'autorisation pour l'ensemble des sujets possibles ; pour chaque entrée est indiquée : <ul style="list-style-type: none"> • sa catégorie de sujet (authentifié, non authentifié, tous, soi, propriété), <ul style="list-style-type: none"> - s'il s'agit d'accorder ou de refuser le privilège, • si entrée est protégée, • si l'entrée a été héritée d'une autre ressource, • selon quelle source il faut interpréter la sémantique de cette liste de contrôle d'accès, • la référence à une collection de sujets.

	<p>La sémantique de la liste de contrôle d'accès définit :</p> <ul style="list-style-type: none"> - Comment sont combinées de multiples entrées d'autorisation qui s'appliquent à l'utilisateur courant : <ul style="list-style-type: none"> • le premier trouvé dans la liste pour un titre doit apparier complètement la demande d'accès (<i>first match</i>), • l'ensemble des entrées applicables à un titre doivent être présents et aucun refus partiel correspondant (<i>all grant before –any deny</i>), • les autorisations accordées à un titre individuel ne doivent pas être refusées dans une quelconque appartenance de groupe de ce titre (<i>specific –deny –overrides grant</i>). - Les contraintes sur leur mise en ordre : d'abord tous les autres refus. - Les contraintes sur l'entrée : une seule entrée par titre pour une ressource, ou liste sans refus. - Les catégories de sujets admissibles dans une entrée de cette liste. <p>Différentes sections techniques complètent ce document.</p>
--	---

Remarque

Lexique anglais-français

Access Control Entries (ACE)	Entrées de contrôle d'accès	Chacun des énoncés accordant ou refusant à un sujet (titre) la permission d'effectuer une opération sur une ressource.
Access Control List (ACL)	Liste de contrôle d'accès	Syn. : liste des autorisations, liste des entrées d'autorisation
Deny	Refuser	Par opposition à permettre.
Display name	Nom affichable	Chaîne de caractères plus faciles à lire et reconnaître pour un humain que ne le seraient les identifiants, comme un URL.
Grant	Accorder	Par opposition à refuser. Syn. : Permettre (privilège)
Owner	Détenteur	
Principal	Titre	Désignation par son URL d'une ressource HTTP identifiant un humain ou une entité logicielle dont l'identité doit être authentifiée lors de l'accès à des ressources en réseau.

Note : Dans ce document de l'IETF, le terme sert souvent à indiquer le sujet, qu'il ait un titre ou pas.

Rédacteur : Richard Parent
Organisation source : Secrétariat du Conseil du trésor
Date de publication : 10 juillet 2002
Raison d'être : Connaissance technologique
Programme gouvernemental : Inforoutes et ressources informationnelles

Nom du modificateur :

Date de dernière modification :

Note numéro :

127