Workgroup:	Network Working Group
Internet-Draft:	draft-ssh-virtualhost
Updates:	4252 (if approved)
Published:	27 October 2019
Intended Status:	Experimental
Expires:	29 April 2020
Author:	R. H. B. van Kleef, Ed.

Username field reused as authority field

Abstract

This document describes an extension for SSH that allows an SSH server to identify which virtual host a client is attempting to connect to. It ensures that unextended clients can interoperate with extended servers and vice-versa, albeit without the features provided as a result of this document.

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 https://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 29 April 2020.

Copyright Notice

Table of Contents

1. Introduction

Many application-layer protocols already have means of specifying which "virtual host" a client intends to connects to. Examples are the HTTP 'Host' header as specified by the IANA Message Headers [IANA_MH] list, and the FTP HOST command [RFC7151]. Most of these implementations note that it is used to identify different virtual hosts where multiple DNS names resolve to one IP address. The goal of this document is to make it possible to implement similar features to SSH by enhancing the 'username' field in the user authentication packet so that it can be used to specify to which virtual host the client means to connect.

2. Conventions Used in This Document

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in [RFC2119].

Throughout this document, when the fields are referenced, they will appear within single quotes. When values to fill those fields are referenced, they will appear within double quotes. Using the above example, possible values for 'data' are "foo" and "bar".

The required syntax is defined using the Augmented BNF defined in [RFC5243]. Some general ABNF definitions are required throughout the document; they will be defined in subsequent sections.

With the increased use of virtualization technologies, there may be several possible definitions for the term "virtual host". This document follows the definition from Section 4.1.14 of [RFC3875], where several virtual hosts share the same IP address, and hostnames are used by the server-SSH process to route sessions to the appropriate virtual host.

3. Updates for the Protocol Version Exchange

SSH has a method of exchanging details about the protocol version and supported featureset. This is described in section 4.2 of [RFC4253]. Both the server and the client **MUST** add a 'comments' entry containing the string "x-virtualhost" in the version string as specified in the aforementioned section of the aforementioned RFC. The client or server respectively, can then use the presence or absence of the value "x-virtualhost" in the list of 'comments' to determine whether the server or client, respectively, supports the protocol extension described in this document.

4. Updates for SSH_MSG_USERAUTH_REQUEST

This document proposes the name of the virtual host be placed in the 'username' field of the `SSH_MSG_USERAUTH_REQUEST` message next to the actual username.

4.1. Syntax of the 'username' Field

The method of embedding the name of the virtual host in the 'username' field of the aforementioned packet is separating the username and the name of the virtual host by an "@"-sign. The name of the virtual host **MUST** be a valid hostname as specified by section 3.2.2 of [RFC3986].

It should still be possible to simply specify a username without a specification of a virtual host. If this is wanted, an "@"-sign **MUST** be appended to the username, unless the username does not contain an "@"-sign, in which case, an "@"-sign **SHOULD NOT** be appended to the username.

Formalizing the preceding text, the value of the 'username' field of the `SSH_MSG_USERAUTH_REQUEST` will conform to this grammar:

```
username_value    =  username "@" virtual_host_name
username_value    =/ username "@"
username_value    =/ username_noat

username          =  1*(%x01-%x10FFFF)
username_noat     =  1*(%x01-%x39 / %x41-%x10FFFF)
virtual_host_name =  <See section 3.2.2 of RFC3986>
```

Figure 1: 'username' field grammar

4.2. Examples

Transmitted string	Actual username	Actual host
`user@host.example`	`user`	`host.example`
`user@@host.example`	`user@`	`host.example`
`user`	`user`	
`user@name@host.example`	`user@name`	`host.example`
`user@x@@`	`user@x@`	
`user@[ff::ff]`	`user`	`[ff::ff]`

Table 1: Examples of values in the 'username' field

5. Interoperability

It is essential that older implementations of SSH servers and clients will keep working, even when the other party does support the protocol alterations as described in this document. It is acceptable to fall back to the behaviour and featureset of the SSH protocol without the features and behaviours resulting from the extension described in this document.

When a new client is used to connect to a server that does not support the extension described in this document, the client **MUST NOT** submit a name of the virtual host and **MUST NOT** append the username with an "@"-sign. Any services that depend on the specification of a virtual host can be expected to be absent or dysfunctional, and should not be requested.

When the server detects a client that does not support the extension described in this document, the server **MUST** interpret the username field as if it is a username in its entirity, without attempting to split out a hostname. The server should then proceed as if no virtual host was specified by the client.

6. Security considerations

All the credentials are submitted over a secure line. That means that the name of the virtual host is submitted over a secure transport as well. The extension information is not submitted over a secure line. It is, in fact, submitted over plaintext. That means that a potential attacker could override advertised support, or lack thereof, of the extension described in this document. This does not introduce a critical security issue, as overriding this will very likely cause a failed authentication, either because the requested user does not exist on the server, or because the credentials used are not valid for the requested user.

7. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3875] Robinson, D. and K. Coar, "The Common Gateway Interface (CGI) Version 1.1", RFC 3875, DOI 10.17487/RFC3875, October 2004, <https://www.rfc-editor.org/info/rfc3875>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[RFC4253] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, DOI 10.17487/RFC4253, January 2006, <https://www.rfc-editor.org/info/rfc4253>.

[RFC5243] Ogier, R., "OSPF Database Exchange Summary List Optimization", RFC 5243, DOI 10.17487/RFC5243, May 2008, <https://www.rfc-editor.org/info/rfc5243>.

[RFC7151] Hethmon, P. and R. McMurray, "File Transfer Protocol HOST Command for Virtual Hosts", RFC 7151, DOI 10.17487/RFC7151, March 2014, <https://www.rfc-editor.org/info/rfc7151>.

8. Informative References

[IANA_MH] Internet Assigned Numbers Authority, "IANA Message Header registry", <https://www.iana.org/assignments/message-headers/message-headers.xhtml>.

Author's Address

Rolf van Kleef (EDITOR)
Email: rfc@rolfvankleef.nl
URI: https://rolfvankleef.nl/