NAME

ssh−audit − Map SSH key distribution and check for anomalies

SYNOPSIS

ssh-audit [*OPTIONS*] [−−] [*USER*@]*HOST* ...

DESCRIPTION

ssh-audit generates a Graphviz source file showing the relationship between keys and hosts, and prints warnings about anything it doens't like.

It must be able to access the host listed on the command line via SSH.

OPTIONS

−−no−local
Suppresses access to the local host's *.ssh* directory.

−−local *NAME*
Enables access to the local host's *.ssh* directory (which is the default) and sets its name. (By default the local node name is used.)

−−strip *SUFFIX*
Specifies a suffix to strip from key names.

−−strength *BITS*
The minimum security strength for a key not to be considered weak. The default is 112.

−−verbose
Print progress messages.

−−help
Display a usage message.

OUTPUT

The output is an input file for Graphviz.

Keys

Each key is shown as a box. The first row is the name of the key, the second the key type and the third an approximation to the key size in bits.

If the box is red then that means the key is weak (as defined by the **−−strength** options).

If the box filled in red then not only is the key weak but it can access some host. It is recommended that you correct any such situations.

If the box is grey then that means it can access no (known) host. (The test for weakness overrides this check.) Such keys may be candidates for deletion, though they may be used by some host not listed.

If the text is green then that means this key has more than one name. This isn't necessarily a problem but is very confusing.

If the text is blue then that means this key shares it's name with at least one other key. This isn't necessarily a problem but is very confusing.

Hosts

Each host is shown in an ellipse.

Inbound edges indicate keys that can access the host. If they are red, that means the key is weak.

Outbound edges to a key mean that the host has the private half of that key. If they are blue, that means more than one host has this private key. While there may be a good reason for this, it may also be a problem that should be corrected.

NOTES

Security Strengths

Security strengths are based on NIST recommendations.

If you think 1024−bit RSA/DSA is good enough then you should request a security strength of 80.

The default security strength of 112 corresponds to 2048−bit RSA/DSA keys and 224−bit ECC keys. This value may be raised in future versions.

SSH protocol version 1 is considered broken and assigned a security strength of 0, regardless of key size.

SEE ALSO

ssh(1), **dot**(1)