What is the Authorized Keys File in SSH?

By Admin

Published: 2019-08-27 · Archived: 2026-04-06 00:59:49 UTC

The `authorized_keys` file in SSH specifies the SSH keys that can be used for logging into the user account for which the file is configured. It is a highly important configuration file, as it **configures permanent access** using SSH keys and needs proper management.

The default configuration in most SSH implementations allows users to deploy new authorized keys for themselves and anyone they like. Such access is permanent, and may bypass privileged access management systems.

Self-provisioning is anathema to identity and access management and having a controlled access provisioning and termination process, as required by most cybersecurity laws and regulations.

When organizations deploy a formal process for managing access using SSH keys, one of the first steps is usually lock-down, basically moving the `authorized_keys` files to root-owned locations, which prevents self-provisioning for normal users.

Configuring Authorized_keys

How to configure authorized keys depends on the SSH implementation.

- How to configure authorized keys for Tectia SSH (Windows, Unix, Linux, z/OS)
- How to configure authorized keys for OpenSSH (Unix, Linux)

Tectia SSH comes with support service that frequently helps customers in SSH key management. OpenSSH offers no support services.

Automating Management of Authorized Keys

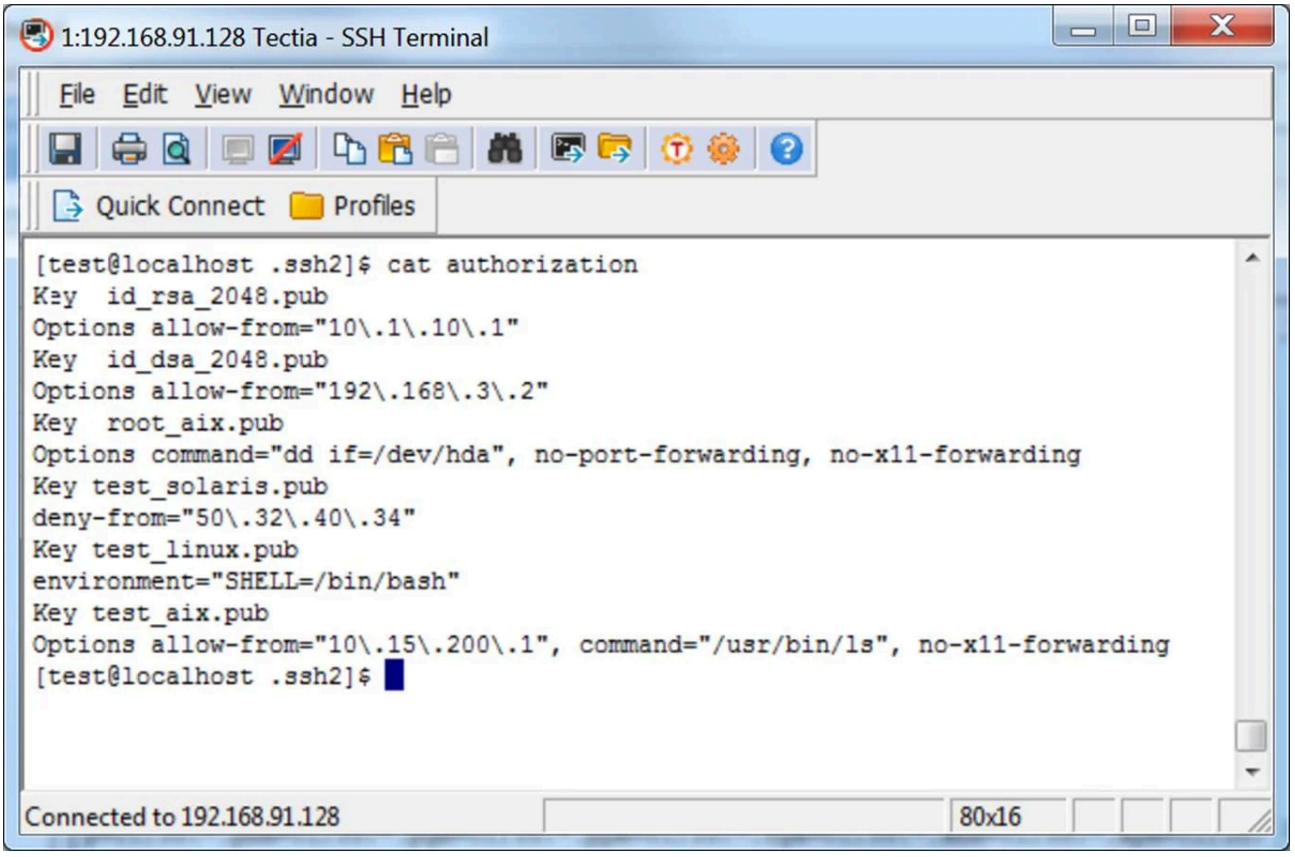
Managing `authorized_keys` files manually is costly and error-prone. We had a customer with a 15-person dedicated team for manually installing SSH keys. Another customer estimated having 200 system administrators who spend 10% of their time setting up SSH keys. Automating the process can **save a lot of money** and **eliminate outages due to human errors**.

Furthermore, SSH keys grant access and having that access under control is required by laws and regulations such as HIPAA for the health care industry, Sarbanes-Oxley for all US public companies, PCI DSS for credit card processing, and FISMA/NIST SP 800-53 for US federal government agencies. It is also included in the US Cybersecurity Framework for critical infrastructure companies.

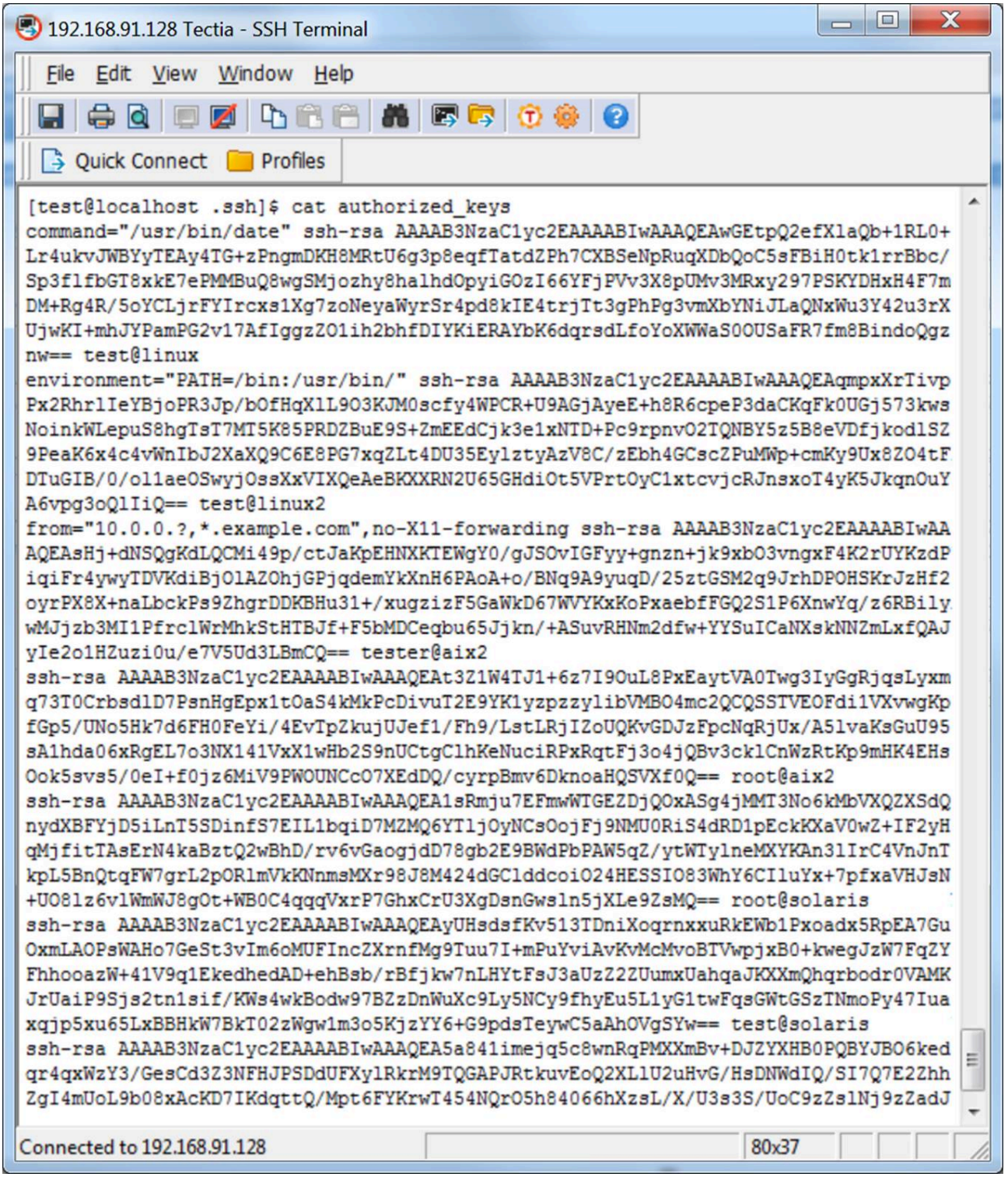
The leading solution is PrivX SSH Key Manager.

General information on managing SSH keys can be found on the SSH key management page.

Tectia SSH Authorizations File



Tectia SSH authorized_keys File



Source: https://www.ssh.com/ssh/authorized_keys/