Role Based Access Control in SSH

552 admin September 28, 2023 Features & Functionalities 1793

Definition of SSH Gateway and Purpose in a Network

SSH gateway uses a secure shell protocol to securely connect to other servers within a network; acting as a mediator between a user's computer and a target server to access remote services.

A proclivity to use ssh gateway would be its security measures; by limiting direct access to any other network servers with authentication. It helps to prevent unauthorized access to other servers which will also help to palliate the risk of attacks and data breaches.

Importance of Implementing proper security measures in SSH Gateway

Key reasons for taking security measures in ssh gateway would be to prevent data breaches, mitigate the risk of attacks, preventing unauthorized access which reduces overall risks of threats.

Role-Based Access Control (RBAC)

RBAC is a security model which is used to manage data and user access in organizations; providing control over the access permissions and simplifying the management to comply with the requirements.

RBAC or **Role Based Access Control in SSH** is a method to *restrict the access of measures in SSH users* or server administrators to the remote servers based on their role. Most enterprises have thousands of servers. Granting SSH access to employees is a big headache or security concern for companies. Using Role based access control, we can ensure that ssh users or system administrators are using only the relevant information they need to perform their tasks. We can restrict their access to only a particular group of servers and also can control their actions on those servers too.

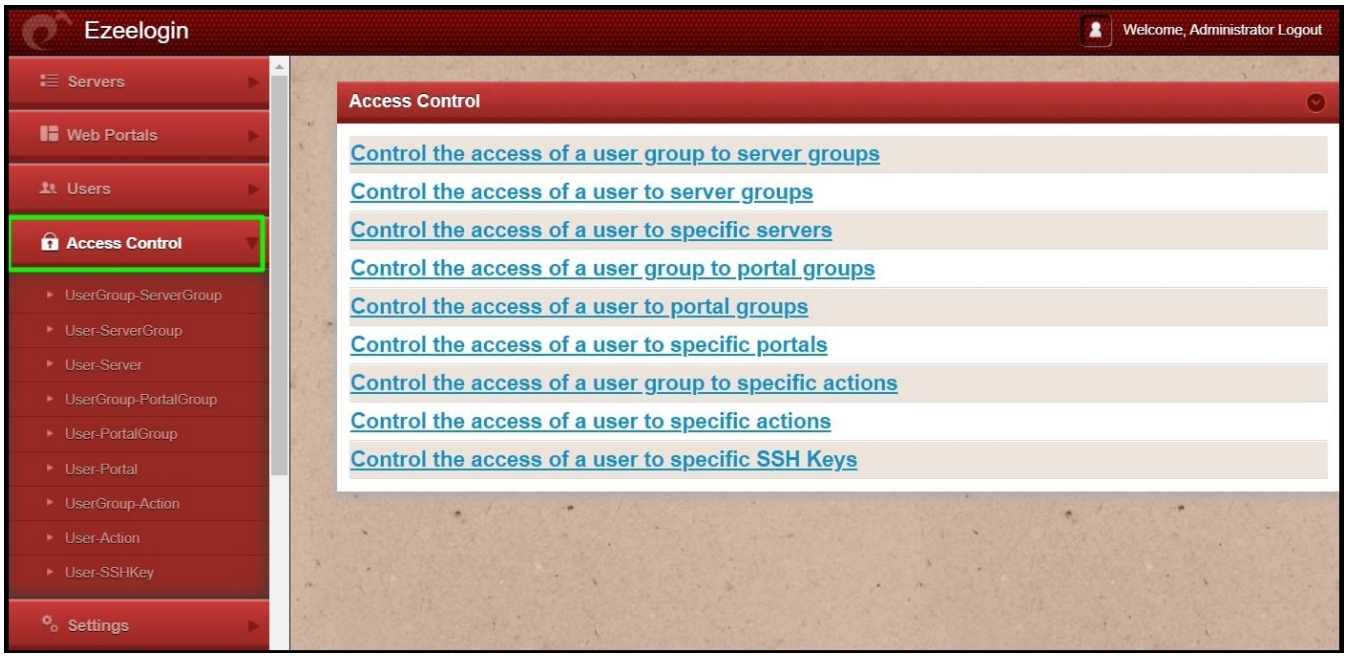
- **Key Principles** include role based, permission based, separation of duties, the centralized, auditable trial of users, and dynamic changes.
- **Key Components** include Users, Permissions, and Roles. It allows flexible management of user access by allowing and modifying roles and permissions as per need.

When we talk about the benefits of RBAC, being a powerful security model it helps in improved security, Flexibility, Scalability, Cost-effective, and Simplified Access management.

How to configure role based access control**?**

To achieve this, we can group the servers and SSH users into different categories based on our requirements and we can decide which user or user group can get access to which server group. Ezeelogin has the feature RBAC. Using this, you can configure role based access control in ssh.

Configuring rbac **in SSH using ezeelogin jump server**



Different ways to achieve RBAC in ssh :

- Restrict user actions on the server
- Map ssh user to a particular server
- Map ssh user to a group of servers
- Map ssh user group to a single server
- Map ssh user group to group of servers

Adding and removing groups in RBAC.

Use the drop-down menu to choose the Group whose accessibility needs to be altered. Then remove or Add accordingly.

Limiting the number of users with administrative privileges.

Admin user can provide permissions to limit the number of user access on certain servers and groups as per need.

You can also implement multi-factor authentication (MFA) in users for added security

Refer detailed article for user authentication - MFA authentication for user

---

Final thoughts and recommendations.

Regularly reviewing and updating roles and permissions.

Limits unnecessary user access to any servers.

Regulate access of user to SSH keys.

Related Articles

Detailed Tutorial on Role Based Access Control

Refer User manual