



---

# TRUSTED, ACCURATE AND RELIABLE!

---

The most comprehensive IT certification  
preparation materials in the industry!

All rights reserved. No part of this document may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. Unauthorized copying, reselling, or distribution of this document is strictly prohibited and may result in legal action.

<https://www.virtulearner.com>  
[support@virtulearner.com](mailto:support@virtulearner.com)

**Juniper**

**JN0-214**

Cloud, Associate

**QUESTION: 1**

Which Linux protection ring is the least privileged?

- A. 0
- B. 1
- C. 2
- D. 3

**Answer(s):** D

**Explanation:**

In Linux systems, the concept of protection rings is used to define levels of privilege for executing processes and accessing system resources. These rings are part of the CPU's architecture and provide a mechanism for enforcing security boundaries between different parts of the operating system and user applications. There are typically four rings in the x86 architecture, numbered from 0 to 3:

**Ring 0 (Most Privileged):** This is the highest level of privilege, reserved for the kernel and critical system functions. The operating system kernel operates in this ring because it needs unrestricted access to hardware resources and control over the entire system.

**Ring 1 and Ring 2:** These intermediate rings are rarely used in modern operating systems. They can be utilized for device drivers or other specialized purposes, but most operating systems, including Linux, do not use these rings extensively.

**Ring 3 (Least Privileged):** This is the least privileged ring, where user-level applications run. Applications running in Ring 3 have limited access to system resources and must request services from the kernel (which runs in Ring 0) via system calls. This ensures that untrusted or malicious code cannot directly interfere with the core system operations.

**Why Ring 3 is the Least Privileged:**

**Isolation:** User applications are isolated from the core system functions to prevent accidental or intentional damage to the system.

**Security:** By restricting access to hardware and sensitive system resources, the risk of vulnerabilities or exploits is minimized.

**Stability:** Running applications in Ring 3 ensures that even if an application crashes or behaves unexpectedly, it does not destabilize the entire system.

**Reference:**

The Juniper Networks Certified Associate - Cloud (JNCIA-Cloud) curriculum emphasizes understanding virtualization, cloud architectures, and the underlying technologies that support them.

While the JNCIA-Cloud certification focuses more on Juniper-specific technologies like Contrail, it also covers foundational concepts such as virtualization, Linux, and cloud infrastructure.

In the context of virtualization and cloud environments, understanding the role of protection

rings is important because:

Hypervisors often run in Ring 0 to manage virtual machines (VMs).

VMs themselves run in a less privileged ring (e.g., Ring 3) to ensure isolation between the guest operating systems and the host system.

For example, in a virtualized environment like Juniper Contrail, the hypervisor (e.g., KVM) manages the execution of VMs. The hypervisor operates in Ring 0, while the guest OS and applications within the VM operate in Ring 3. This separation ensures that the VMs are securely isolated from each other and from the host system.

Thus, the least privileged Linux protection ring is Ring 3, where user applications execute with restricted access to system resources.

**Reference:**

Juniper JNCIA-Cloud Study Guide: Virtualization Basics x86 Architecture Protection Rings Documentation

**QUESTION: 2**

Which two statements are correct about cloud computing? (Choose two.)

- A. Cloud computing eliminates operating expenses.
- B. Cloud computing has the ability to scale elastically
- C. Cloud computing increases the physical control of the data resources.
- D. Cloud computing allows access to data any time from any location through the Internet.

**Answer(s):** B, D

**Explanation:**

Cloud computing is a model for delivering IT services where resources are provided over the internet on-demand. Let's analyze each statement:

A . Cloud computing eliminates operating expenses.

Incorrect: While cloud computing can reduce certain operating expenses (e.g., hardware procurement, maintenance), it does not eliminate them entirely. Organizations still incur costs such as subscription fees, data transfer charges, and operational management of cloud resources. Additionally, there may be costs associated with training staff or migrating workloads to the cloud.

B . Cloud computing has the ability to scale elastically.

Correct: Elasticity is one of the key characteristics of cloud computing. It allows resources (e.g., compute, storage, networking) to scale up or down automatically based on demand. For example, during peak usage, additional virtual machines or storage can be provisioned dynamically, and when demand decreases, these resources can be scaled back. This ensures efficient resource utilization and cost optimization.