Security issues in cluster systems

Vitalii Poliakov
Perccom
Done for IFMO seminar 2014

Completely based on the paper [1]

Security in clusters is a tremendous problem.

Issue #1

- People think that security solutions for general computers also suit for clusters

Why is it wrong?

- High bandwidth connections — DDOS exploitation

- Extensive computational power — Bruteforce

- Massive storage capacity — storing illegal data

"A 100-node cluster is different from 100 standalone systems." - In contrast, now the secure cluster considered as cluster where all the components are secured

Issue #2

Performance predominates over security. While login authentication and associated access rights are common, even minimal overhead from the use of encrypted communications is often considered unacceptable.

Security specifics for clusters p.1

- First, a cluster encompasses a collection of distributed resources to be protected. The challenge is to secure these internal distributed resources against unauthorized access while at the same time permitting easy access by legitimate users.

- Second, a cluster must provide mechanisms for resource management. The challenge here is to manage a cluster such that legitimate users can consume resources efficiently in an authorized way using an agreed-upon job prioritization system.

Security specifics for clusters p.2

- Third, a cluster may be composed of different hardware and software node configurations (heterogeneous clusters). Even in the case of clusters containing the same hardware and software node configurations, there is usually a separation of cluster nodes by specialized function. The challenge is to coordinate security across different node platforms and different specialized function nodes.

- Finally, cluster resources exhibit dependent risk. The security of the resources in a cluster environment relies on the integrity of all nodes.

Current methods to enchance security in clusters

- Hide the majority of cluster nodes (the "computing nodes") on a private network.

- Only those software packages which are necessary for the cluster operation should be installed.

- Intrusion Detection System (IDS) on head nodes.

Future work

- Tradeof between performance and security is required.

- Expectation is that security techniques in clusters will most likely be realized in the form of monitoring tools.

Conclusion

Security in clusters is <u>still</u> a tremendous problem.

References

- Cluster Security as a Unique Problem with Emergent Properties: Issues and Techniques, Yurcik et al., 2004

- http://melkon.com.ua/ru/novosti-i-statii/article-cluster-security.html