Role-Based Access Control Challenges & Solutions

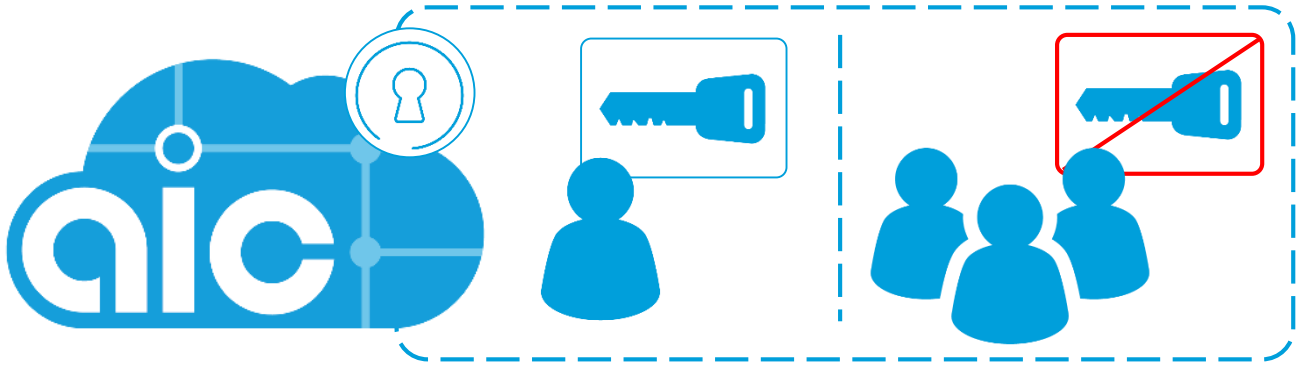
AT&T

RBAC Significance & Challenges

AIC continues to expand in scope and number of business critical functions it supports

AIC's security posture has become a heavy focus

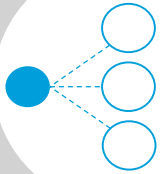
One facet of that security posture is the effective implementation of RBAC across AIC



AIC has experienced **challenges** in successfully implementing RBAC policies across underlying components & infrastructure

Primary RBAC Issues

No granularity - granular admin roles do not exist, only a global admin that has full access to all resources across all tenants.



Policy action mapping – Some cases where a policy action dictates access to multiple APIs. Policy actions mapping to single APIs would provide greater security.

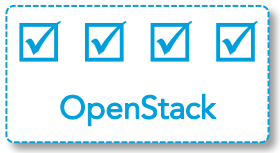
Lack of documentation – No record stating which policy actions map to each API or which policy actions map to specific actions.

Error identification – Not possible to read Neutron code and determine where errors occur during RBAC testing, due to highly customized and dynamic enforcement.

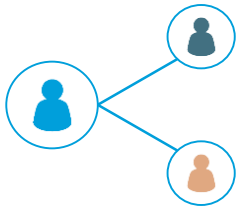
Upstream work summary

Upstream work has been started to address these RBAC implementation challenges in the February 2018 - OpenStack Queens Release

OpenStack Queens



Administrative Rights - Treat consistently across all OpenStack Services



System Scope – Separate project and systems admin

Kubernetes Integration – Looking to utilize Keystone for Kubernetes authentication & identity