Keycloak default roles and their descriptions

Role	Description
Administrators	Administrator is for superuser access and should not be assigned to any clients. This privilege should **only** be assigned to [**ui] staff** and managed through Azure Active Directory
Core.BackOfHouse	Read only access to back of house dashboard
Monitoring.AlertColours.Read	Read only access to view Monitoring & Alerting colours
Monitoring.AlertColours.Write	Ability to edit / define Monitoring Alert colours
Monitoring.AlertThresholds.Read	Read only access to view Monitoring & Alerting thresholds
Monitoring.AlertThresholds.Write	Ability to edit / define Monitoring Alert Thresholds
Monitoring.All.Read	Read only access to all Monitoring
Monitoring.All.Write	Ability to edit all Monitoring configurations
Monitoring.EmailGroups.Read	Read only access to view Monitoring Email Groups
Monitoring.EmailGroups.Write	Ability to edit Monitoring Email Groups
Monitoring.EmailTemplates.Read	Read only access to view Monitoring Email Templates
Monitoring.EmailTemplates.Write	Ability to edit Monitoring Email Templates
Monitoring.MonitoringColours.Read	Read only access to view Monitoring Colours
Monitoring.MonitoringColours.Write	Ability to edit / define Monitoring Colours
Monitoring.MonitoringThresholds.Read	Read only access to view Monitoring & Alerting colours
Monitoring.MonitoringThresholds.Write	Ability to edit / define Monitoring Thresholds
Monitoring.SiteMonitor	Site Monitor dashboard access
Overview.Read	Read only access to the overview dashboard
Reader	Regular users will be given the reader role and have no special permissions. A reader has access to dashboards including downloading csvs, etc.

Tenant admin	Tenant admins have permission to access all dashboards. They also have special privileges to access the *User Management Console* which allows them to add/edit/delete users and their permissions.
VehicleLocations.Drilldown.Read	Read only access to the VehicleLocationsDrilldown
Uma_authorisation	UMA = User Managed Access https://wso2.com/library/article/2018/12/a-quick-guide-to-user-managed-access-2-0/ The uma_authorization role is a default realm role. Default Role uma_authorization. An AAT enables a client application to query the server for user permissions. Client applications can obtain an AAT from Keycloak like any other OAuth2 access token. https://www.keycloak.org/docs/latest/authorization_services/#_service_user_managed_access

Monitoring vs alerting

Monitoring is a constantly updating view of the state of the system. It doesn't generate any events such as sending e-mails. It allows users to see which telemetry values are above or below a specified threshold, or which data packets have arrived later than a specified delay. Current monitoring information is always available, but users have to go and check for it.

Alerting on the other hand is for events that the system has detected that require some attention. Alerts can be triggered by telemetry values crossing a threshold or data packets arriving later than expected, but the intention is that they are triggered on more extreme thresholds, and a response is initiated, such as sending an e-mail, that draws attention to that event – perhaps prompting a mitigating action can be performed.