Procedure omtrent toegang tot databases Infectieradar

Hieronder wordt beschreven op welke wijze er omgegaan dient te worden m.b.t. toegang tot de diverse databases binnen de applicatie Infectieradar.

Situatie

De applicatie bevat 4 databases:

- global-infos (globaldb)
- default_messageDB (messagedb)
- default_studyDB (studydb)
- default_users (userdb)

De databases zijn te verdelen in 2 groepen:

- User-data (userdb)
- Overige-data (globaldb, messagedb en studydb)

Directe toegang tot de inhoud van deze databases is enkel toegestaan voor een beperkte groep medewerkers. Deze medewerkers mogen deze toegang enkel gebruiken voor het uitvoeren van hun functie/rol.
Iedere directe toenadering tot de databases dient enkel na aanmelding in de OpenShift-omgeving mogelijk te zijn.
Het dient dus onmogelijk te zijn om buiten de OpenShift-omgeving om toegang tot de inhoud van de databases te verkrijgen.
Ieder gebruik van rechten binnen OpenShift waarbij mogelijk toegang tot de inhoud van de databases gerealiseerd kan worden dient gelogd te worden. Rapportage hierop dient mogelijk te zijn.

Voor de vastlegging van de acties van de applicatiebeheerders zal Topdesk gebruikt worden.
Hierbij is het van belang dat dit zodanig afgeschermd wordt dat enkel de applicatiebeheerders en de verantwoordelijke applicatiebeheer hiertoe toegang hebben.

Rollen:

- Beheerder OpenShift
  - Heeft geen toegang nodig tot de inhoud van de databases. Dit zal dan ook zoveel mogelijk technisch onmogelijk gemaakt worden.
- Applicatiebeheerder
  - Heeft vanuit zijn functie mogelijk toegang tot de inhoud van de databases nodig.
  - Iedere applicatiebeheerder heeft toegang tot slechts 1 groep databases.
  - Indien meerdere databases uit verschillende database-groepen benaderd dient te worden (bijv. bij gebruik van scripts) zal een andere applicatiebeheerder (met toegang tot de andere database-groep) hierbij betrokken dienen te worden (zgn. 4-ogen principe).
  - Toegang tot database **userdb** is enkel bij noodzaak toegestaan.
  - Vastlegging vindt plaats in Topdesk. (welke actie, wie heeft het uitgevoerd, wie heeft meegekeken, tijdstip start, tijdstip einde)
  - Bij een query waarbij de database **userdb** gebruikt wordt zal naast de in het voorgaande punt genoemde zaken ook de gebruikte query gelogd worden in Topdesk.
  - Het verkrijgen van toegang tot de databases zal gelogd dienen te worden (en rapportage hierop is mogelijk/aansluiting met SIEM met alerting)

- Verantwoordelijke applicatiebeheer
    - Heeft geen toegang nodig tot de inhoud van de databases.
    - Geeft de toestemming aan de applicatiebeheerders om een gevoelige query op de databases uit te voeren.
    - Deze toestemming dient geregistreerd te worden in Topdesk.
    - Rapporteert (op aanvraag?) de gelogde toegang en queries.

Extra aanvullingen hierop:

- De inhoud van de database **userdb** wordt als 'gevoelig' gezien en daarom is het uitgangspunt dat de inhoud van deze database niet met andere databases gecombineerd wordt.
- Indien dit niet anders kan zal dit met expliciete toestemming van de perso(o)n(en) met de rol 'Verantwoordelijke applicatiebeheer' uitgevoerd worden. Deze toestemming zal worden vastgelegd in Topdesk.
- Er zal altijd minimaal 1 applicatiebeheerder met toegang tot database-groep User-data beschikbaar zijn tijdens supporttijden.
- Er zal altijd minimaal 1 applicatiebeheerder met toegang tot database-groep Overige-data beschikbaar zijn tijdens supporttijden.

De personen met (technische) toegang tot de database zijn:

5.1.2e (rol: beheerder OpenShift)
5.1.2e (rol: applicatiebeheerder, database-groep: xxx)
5.1.2e (rol: applicatiebeheerder, database-groep: xxx)
5.1.2e (rol: applicatiebeheerder, database-groep: xxx)
5.1.2e (rol: verantwoordelijke applicatiebeheer)