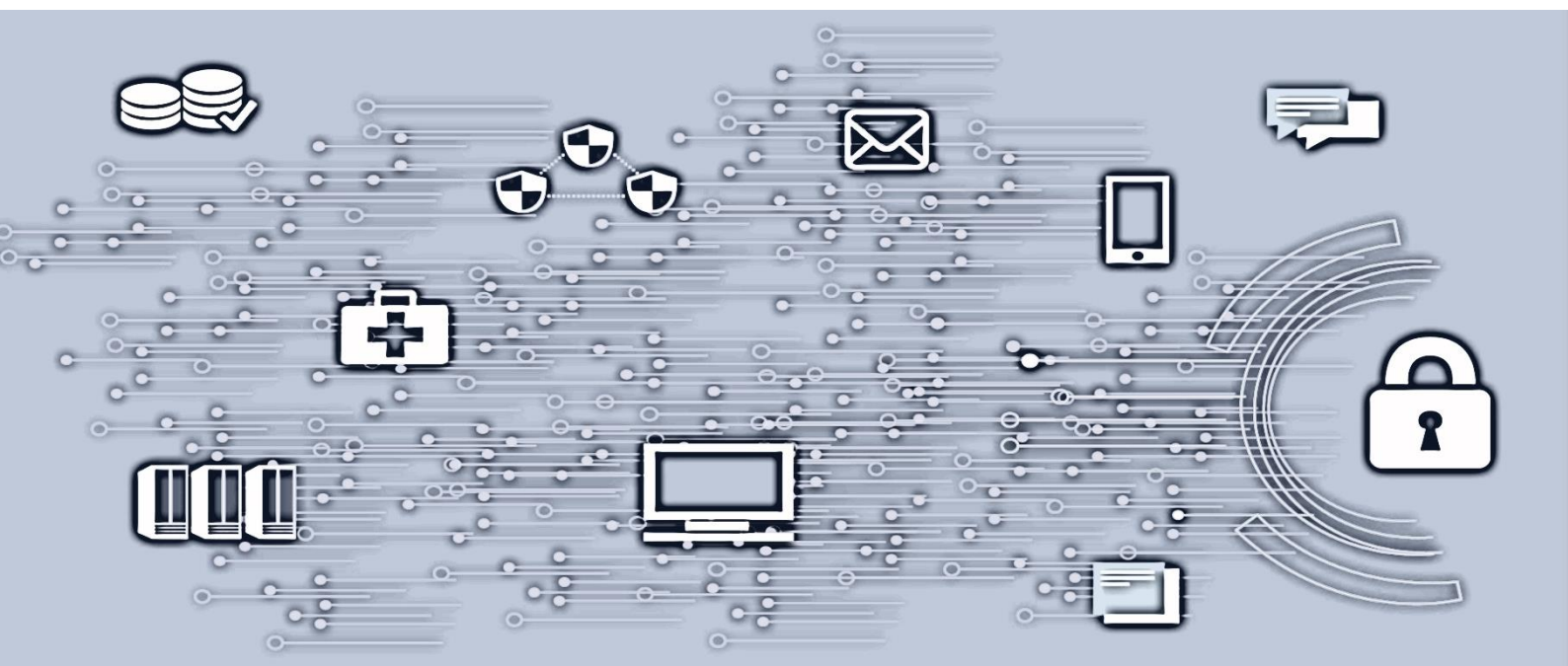


SNMP i Sykehuspartners management-nettverk

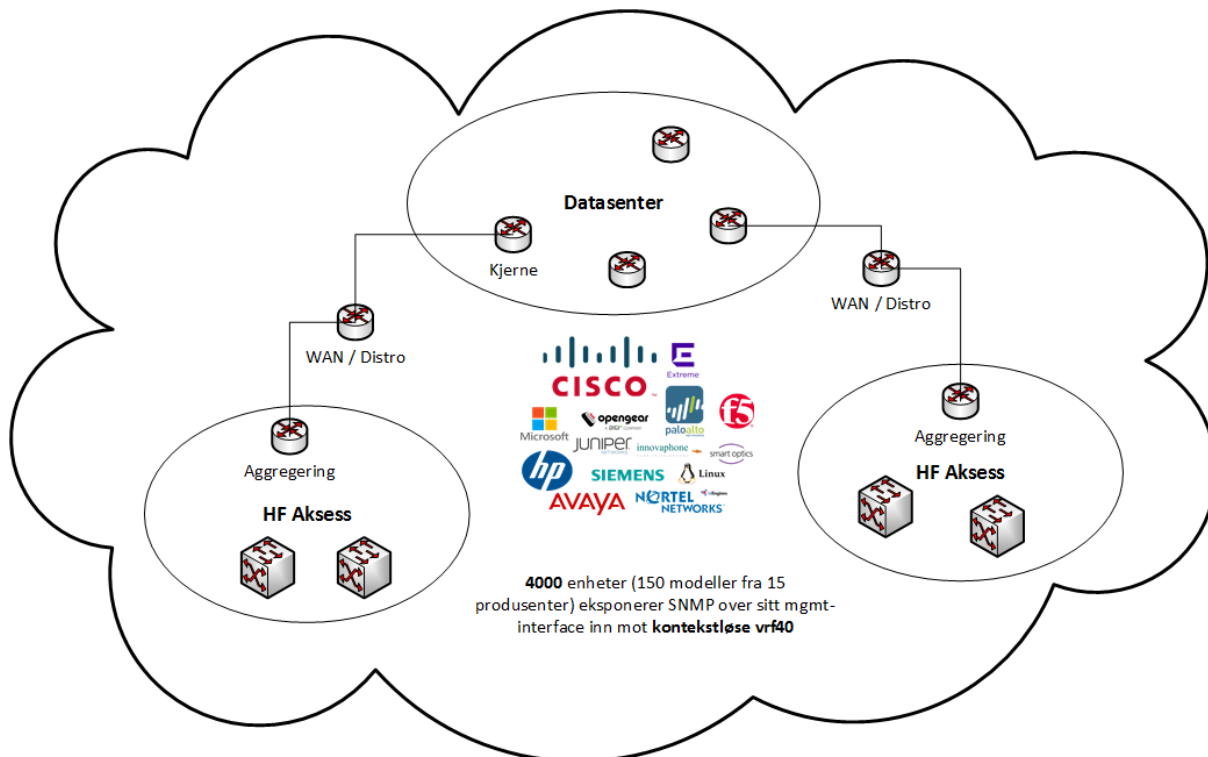


Innhold

1.	Bakgrunn	3
2.	Omfang	4
3.	Standard SNMP minimums-konfigurasjon	4
4.	Avvik	4

Versjon	Dato	Godkjent av
1.0	23.09.2022	Christian Jacobsen

1. Bakgrunn



Simple Network Management Protocol (SNMP) er en protokoll som benyttes til å administrere og overvåke nettverkskomponenter. Avdeling Datakommunikasjon bruker SNMP-protokollen til mange ulike verktøy som understøtter ulike funksjoner i nettverksdriften. De ulike verktøy bruker SNMP på ulikt vis og med ulike versjoner i et multi-leverandør-miljø. 4000 enheter, 150 ulike modeller fra 15 produsenter gjør at vi har multiple måter å konfigurere SNMP på.

Datakommunikasjon sin SNMP-bruk skjer i et separat management-nett, VRF40, som er delt opp i IP-regioner tildelt hvert offentlig HF. Av historiske årsaker har vi både v2c- og v3-implementasjoner gående med varierende v2c communities og v3 userid, passord + kryptering.

Denne kompleksitet medfører uforholdsmessig mye arbeid knyttet til SNMP-konfigurasjoner både på de enkelte nettverksenheter og på verktøy de SNMP-kommuniserer med.

Som følge av dette brukes det unødvendig tid til feilsøking rundt SNMP-problemer.

Vi trenger en omforent SNMP-standard som balanserer konfigurasjons-/feilsøkings-innsats med tilstrekkelig sikkerhet.

2. Omfang

Poenget med denne policy er å definere en minimumsstandard på hvordan SNMP skal konfigureres og brukes i avdeling Datakommunikasjon sitt management-nett.

Denne policy regulerer ikke bruken av SNMP i andre deler av HSØ-nettverket.

Datakommunikasjon sitt management-nett, VRF40, kopler alle management-interface på alt nettverksutstyr inn i samme IP-nett. Det er ingen kopling mellom VRF40 og soner/kontekster som bærer nytte data.

Tilgang til VRF40 styres av AD og PAM. Trafikk til/fra VRF40 må via brannmur i datasenter.

Risiko- og sårbarhetsanalyse av verktøy, som bruker SNMP i management-nettet, må avklare om denne SNMP-policy er sikker nok for verktøyet. Eller om ytterligere spissing (egen legitimasjon, instansiering, sterkere kryptering, lengre passord osv.) kreves.

3. Standard SNMP minimums-konfigurasjon

Nettverksutstyr som Datakommunikasjon drifter for HSØ eksponerer sin SNMP-agent i vlan VRF40, og skal settes opp med SNMP versjon 3.

SNMPv3 skal minimum konfigureres slik:

- Autentiseringsprotokoll: SHA-2/384 (Secure Hash Algorithm)
- SNMPv3 Aut. bruker: minimum 8 tegn
- SNMPv3 Aut. passord: minimum 16 tegn (ulikt krypteringspassordet)
- Krypteringsprotokoll: AES256 (Advanced Encryption Standard)
- Krypteringspassord: minimum 16 tegn (ulikt autentiseringspassordet)
- Aksesslister: Alle hosts plassert i vlan VRF40
- Tilgangsnivå: Read Only
- Instansiering: Ingen
- Endringstakt: 2-3 års syklus (i synk med LCM)

Alle SNMP-verktøy og administrerte enheter plassert i samme management-nett (VRF40) kan i utgangspunktet konfigureres til å bruke samme SNMPv3-legitimasjon.

4. Avvik

SNMP-verktøy og SNMP-agenter på enheter som ikke støtter minimumskravene, registreres som avvik i Helse-CIM.