

Hinar ýmsu gerðir umsjónarverkfæra

Tryggvi R. Jónsson

2. mars 2022

Til hvers?

Rekstraraðilum upplýsingakerfa standa til boða mörg og mismunandi verkfæri til að einfalda og auka gæði rekstrar.

Hvað á að kaupa RMM, PSA?

Á að skrá tíma eða ekki tíma?

Þarf að mæla þjónustustig (SLA)?

Þarf að kaupa nýtt (enn eitt!) kerfið eða á ég þetta kannski bara nú þegar?

Á þetta ekki bara að gera allt sjálfkrafa fyrir mig og ég get farið til Tene?

Hverjar eru þarfirnar og kröfurnar?

- Umsjónar- og rekstrartólakeðjan er verkfærataskan sem við tökum með okkur og verkfærin sem við eigum heima á “verkstæðinu”.
- Það krefst öðruvísi verkfæra að fara á milli marga mismunandi staða eða geta komið ser fyrir á einum stað.
- Kröfurnar geta verið mismunandi eftir þroskastigi umhverfa.

Ólík verkfæri – nokkur dæmi

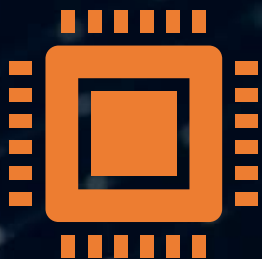
- RMM: Remote Management and Monitoring
 - Fyrir einn aðila per uppsetningu sbr. Intune, MDM, Manage Engine Desktop Central
 - Fyrir marga aðila (t.d. alla viðskiptavini) sbr. NinjaOne, ConnectWise Automate, Datto RMM
 - Yfirtaka, skráning búnaðar, eftirlit með loggum, sjálfvirk viðbrögð
- PSA: Professional Service Automation Tickets / Communications
 - AutoTask, ConnectWise Manage
 - Email, Slack, Teams
- SIEM: Security Incident and Event Management
 - DataDog, Solarwinds SIEM (úbs!), Splunk, PagerDuty, OnPage
- Documentation and Knowledge Management:
 - Confluence, ITGlue, ITBoost, DIY

Mismunandi umhverfi

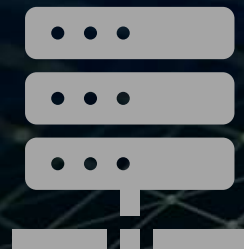
- Einn “viðskiptavinur” eða margir?
 - Setur okkur mjög skýr mörk um hvaða verkfæri við getum nota
 - Passa upp á leka á milli aðila á móti hagræði við „Single Pane of Glass“
- Eitt umhverfi per viðskiptavin?
 - On-Prem vs. Cloud
 - Linux vs. Windows
 - Netbúnaður – vélbúnaður (Infra/Virtual) – Stýrikerfi – Applications
 - Margir þjónustu- og rekstraraðilar



Hvað hentar okkar “tempói” ?



**Þarf að styðja við cloud native –
Infrastructure as Code – DevOps ferla?**



**Er innviðarekstur byggður á on-prem
sýndarumhverfi eða hýstu?**

þurfum við bara að vakta álag/notkun/aðgerði

Hversu hátt upp í tæknistakkinn þurfum við að fara?

Eitt fullkomið kerfi?

- Eitt kerfi sem hentar öllum eða uppfyllir allar kröfur er ekki til!
- Hvaða virkni er mikilvæg fyrir okkur, tímaskráning, þjónustumælingar, reikningagerð, sjálfvirk skráning búnaðar?
- Á hvaða þroskastigi erum við, t.d. út frá CMM:
 - Initial
 - Repeatable
 - Defined
 - Managed
 - Optimizing



Upplýst ákvörðun að bæta öðru kerfi við

- Er núverandi verkfærakista með svipaða eða sambærilega virkni?
- Er nú nógu góð?
- Er réttlætanlegt að leita eftir öðru verkfæri til að bæta virknina eða er ávinningurinn óverulegur?
- Er líklegt eða víst að við (og aðrir) munum nota alla virkni verkfærisins?

Gátlistinn gæti verið

- Hvert er umhverfið sem ég er að sjá um?
- Hvaða formkröfur þarf ég að uppfylla (hlíting, tímaskráning, mælingar)?
- Þurfa aðrir að nota verkfærin? Er líklegt að þeir geri það?
- Búa kerfin til aukinn rekstur/kostnað og er það réttlætanlegt?
- Höfum við tíma til að sinna þeim? Fá ávinninginn sem við ætluðum?
- Samþættast kerfin t.d. sjálfvirk stofnun og lokun ticketa út frá stöðu í vöktun ?
- Skapa kerfin nýjar öryggishættur?

Heildarmyndin

- Hvert ert hlutverk kerfisins?
 - Viðbót við bilanagreiningu/rekstur tiltekins umhverfis
 - Ná sýnileika yfir mörg kerfi fyrir fáa aðilar?
 - Samræma vinnulag/samskipta margra?
- Höfum við strategíu um þessi mál?
 - Hugsa fyrst – Kaupa svo
 - Ekki bæta við kerfi nema þörfin sé skýr og ávinningur meiri en kostnaður
 - Margir birgjar styðja orðið samþættingar og sjálfvirkni milli kerfa, stundum þarf að veðja á vistkerfi af lausnum frekar en eina tiltekna lausn.

Dæmi: Microsoft umhverfi

- Intune, MDM, Autopilot – Uppsetningar, eftirlit o.fl.
- Compliance center og Logs – SIEM
 - mögulega skoða verkfæri til að taka logga og senda á SOC ?
- Teams – Samskipti og beiðnir (Lists ekki tölvupóstur!)
 - Innleiða samþykktarferla í Teams ef formfesta er meiri
 - Beiðnir og samskipti við önnur beiðnakerfi í gegnum bots/api
- Lists – Skjölun og yfirlit,

Dæmi: AWS cloud native DevOps

- IaC: CloudFormation
- Logs: CloudWatch og OpenSearch og Kibana
 - DataDog ef þörf er á virkni sem er meiri en platformið hefur
- Slack – Samskipti og beiðnir
- Notion – Skjölun og yfirlit