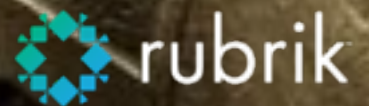


Backup - Den siste forsvarslinjen

Helge J. Kveseth

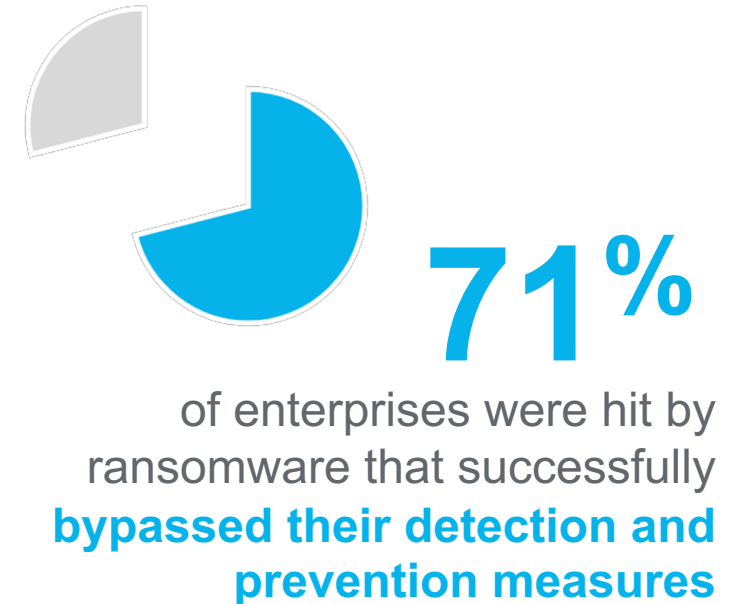
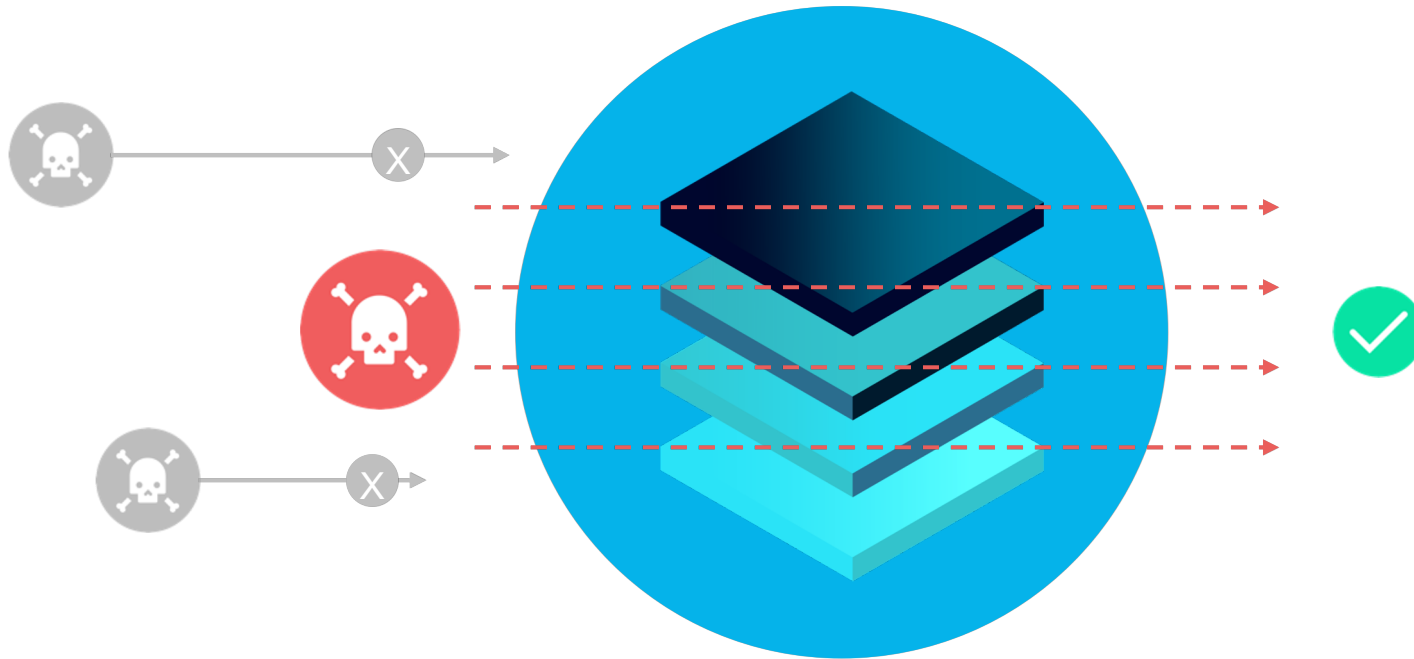
Sales Engineer

helge.kveseth@rubrik.com



Beskyttelse er essensielt, men angrep skjer allikevel

Prevention

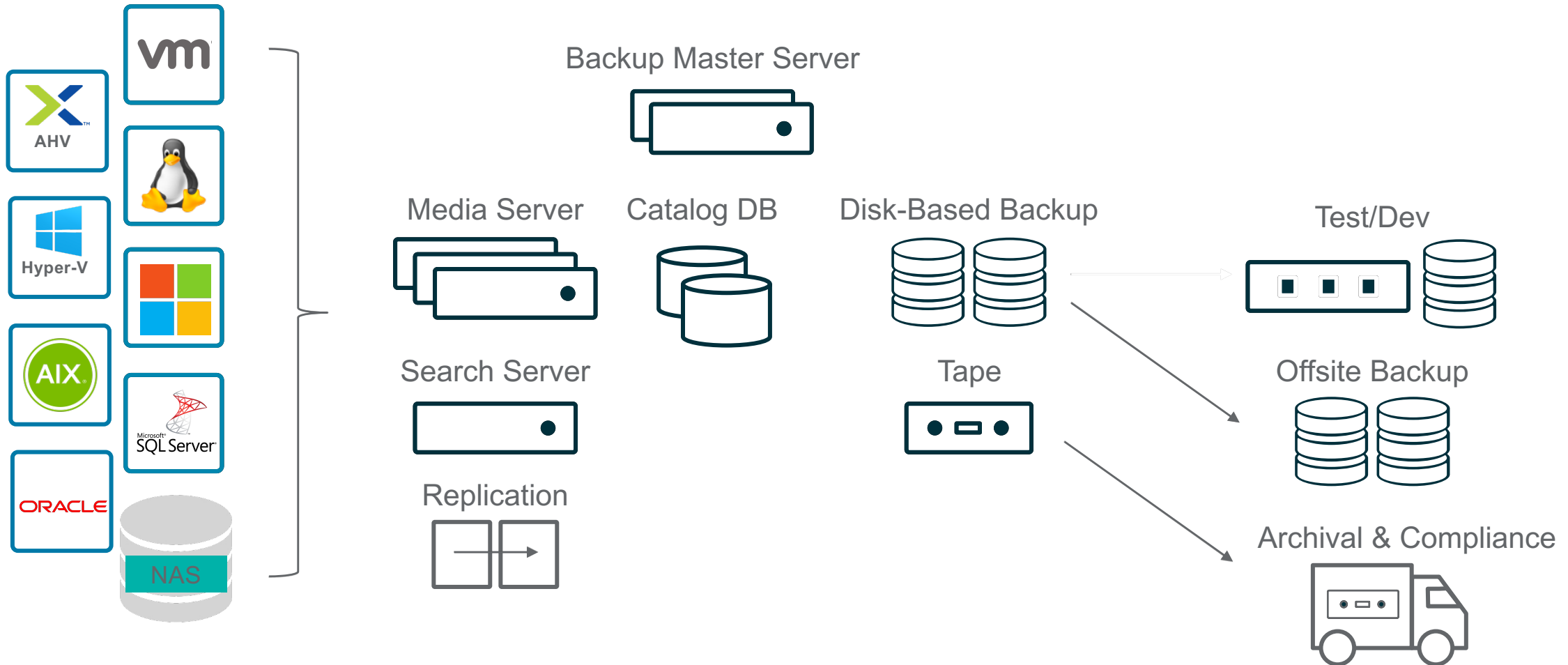


Source: Barkly Inc. survey

Trusselbildet



Utfordringer og kompleksitet i backupløsninger



Sikkerhetskontroll - infrastruktur

- Er operativsystemer og filsystemer/lagringsystemer på oppdatert nivå?
 - I hvilken rekkefølge må dette oppdateres/oppgraderes?
 - Hvordan påvirker en oppgradering andre deler av miljøet?
- Ligger backupdata tilgjengelig på nettverk? (NFS/SMB)
 - Kan jeg gjøre det utilgjengelig for innsyn?
- Er backupdataen min kryptert på både nettverk og disk?
 - Hvilken påvirkning har dette eventuelt på ytelse?
- Hvor og hvordan lagres backupdata? Hvem har skriverettigheter på filsystem/data?
- Hvilke porter er åpne internt i miljøet?

- Hva er prosessen for hardening?



Lag deg en sjekkliste, bruk best practises

- Local Account Security
- Domain Account Security
- Automation Security
- Roles and Permission Review
- System Reset Protection
- Enabling Auditing / Syslog
- Securing NTP Servers
- Login Banners
- SMB / NFS Security Review
- S3 / Archive Security Review
- SLA / Object Protection
- Physical Site Security
- Deliver copies of technical whitepapers on best practices

Local Account Security



DO's

Best Practices

1. Bruk unike og sterke passord
2. Passordrotasjon (30-90 dager)
3. Admin aksess skal være unntaket, ikke regelen
4. Syslog / Alert på admin loginforsøk / loginfeil
5. Etabler MFA på administratorkontoer
6. Lagre credentials kryptert eller i key stores
7. Separer primær og sekundær-credentials på ulike krypterte områder



DONT's

Best Practices

1. Ikke gjenbruk passord over ulike løsninger eller lokasjoner

Password Requirements

Minimum Characters
8

Minimum Lower Case Characters
1

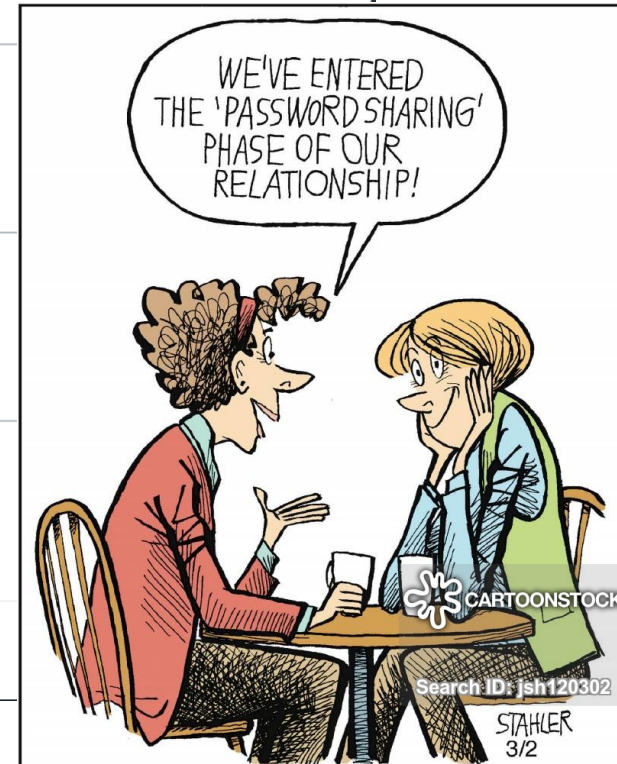
Minimum Upper Case Characters
1

Minimum Numeric Characters
1

Minimum Special Characters
1

Use ZXCVCBN
 Prevent Password Reuse

Cancel



Domain Account Security



DO's

Best Practices

1. Hvis mulig, unngå å bruke domenebrukere som administrative kontoer, eller ha egne påloggingsprosedyrer mot enkeltsystemer.
2. Bruk rollebasert aksesskontroll aktivt – sørg for å følge prinsippet om færrest mulig privilegier.
3. Bruk MFA for alle kontoer som har tilgang
4. SSO



DONT's

Best Practices

1. Hvis man replikerer til andre løsninger, sørg for at disse ikke er i samme domene.



Automation Security



DO's

Best Practices

1. Bruk dedikerte brukerkontoer for ulike automatiseringsoppgaver
2. Prinsippet om færrest mulige privilegier gjelder også her
3. Sørg for at automatiseringsbruker **ikke** har rettigheter til å utløpe data eller endre retention
4. Benytt **TOKEN** istedenfor **Basic** autentisering
5. Lagre **TOKEN** og aksessnøkler sikkert



DONT's

Best Practices

1. Aldri lagre passord i åpen tekst i automatiseringskoden

Generate API Token

Duration (Days)

30

Tag

Cancel Generate

System Reset Protection



DO's

Best Practices

1. Sørg for at løsningen ikke tillater nullstilling eller formatering

```
C:\> Administrator: X:\windows\system32\cmd.exe - format c: /fs:
Microsoft Windows [Version 6.1.7601]

X:\Sources>format c: /fs:NTFS
The type of the file system is NTFS.

WARNING, ALL DATA ON NON-REMOVABLE DISK
DRIVE C: WILL BE LOST!
Proceed with Format (Y/N)? Y
```

```
Node reset is disallowed
This Rubik cluster has Retention Lock policies that prevent reset. Contact Support to enable reset.
```

Auditing / Syslog



DO's

Best Practices

1. Sørg for å etablere auditing via syslog ut av løsningen.
2. Benytt kryptert syslog trafikk med sertifikater
3. Etabler regelsett som gir deg riktig og kritisk informasjon

Add Syslog Export Rule

IP or Hostname
seim-local

Protocol
 TCP UDP

Port
514

Facility
Security

Severity
Warning

Enable TLS

Select a TLS Certificate. If you have not imported your TLS Certificate, import it from the [Certificate Management page](#).

*.rubrikdemo.com

Cancel Add

Securing NTP Time Sources



The Network Time Protocol (NTP) is an Internet protocol built to distribute precise time around a computer network. NTP makes use of UDP over TCP/IP to synchronize network time clients to a precise time reference. The NTP protocol can make use of encryption keys to authenticate a timeserver.



DO's

Best Practices

1. Benytt kryptert NTP Stratum-1 tidskilde hvis tilgjengelig
2. Etabler bade primær og sekundær NTP tidskilde for redundans

11:07:42.234

Login Banners



DO's

Best Practices

1. Benytt log-in bannere hvis mulig og ved behov
2. Sett sikkerhetsklassifisering hvis mulig og ved behov

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests?not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

I Agree

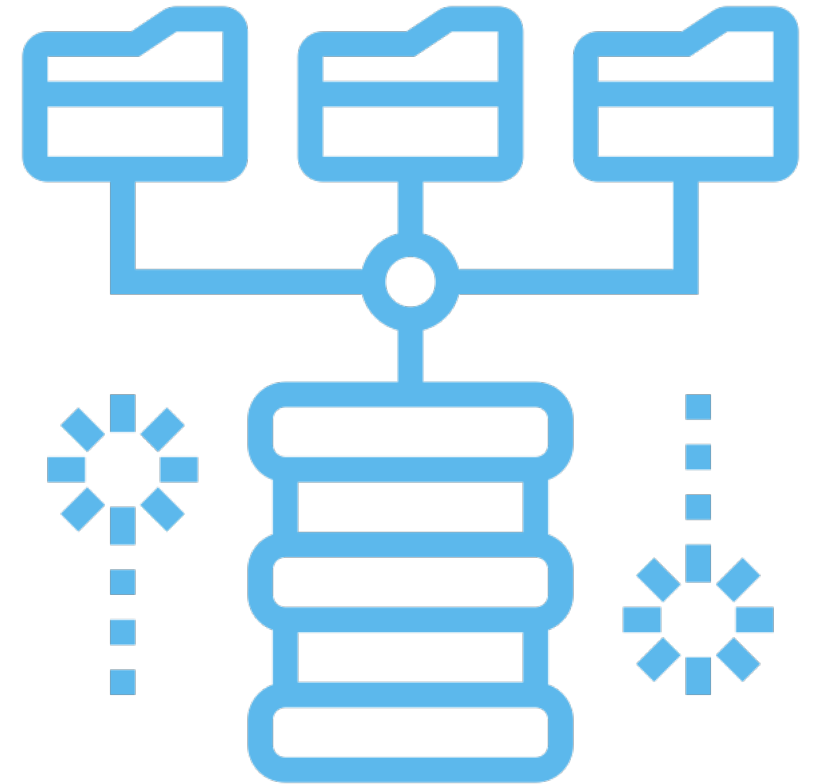
NFS / SMB Security



DO's

Best Practices

1. Bruk secure SMB for SMB shares
2. Bruk IP allow-lists for alle NFS shares og klienter
3. Sørg for å ha autentisering (brukernavn/passord) mot NFS shares



S3 / Archive Security



DO's

Best Practices

1. Bruk prinsippet om minst mulig privilegier
2. Lagre credentials sikkert
3. Lagre krypteringsnøkkel for arkivlokasjon sikkert / AWS CloudKMS
4. Benytt auditing verktøy for kontinuerlig monitorering
5. Bruk versjonering for ekstra beskyttelse på bucket / blob



Physical Site Security Protection



DO's

Best Practices

1. Sikre infrastruktur i låste rack og rom hvis mulig
2. Kun autorisert personell skal ha tilgang
3. Benytt prinsippet om 3-2-1 for backupdata (3 kopier av data, 2 ulike lokasjoner, 1 offsite) ved hjelp av replikering eller arkivering av data

Tilbake til sjekklista

- Local Account Security**
- Domain Account Security**
- Automation Security**
- Roles and Permission Review**
- System Reset Protection**
- Enabling Auditing / Syslog**
- Securing NTP Servers**
- Login Banners**
- SMB / NFS Security Review**
- S3 / Archive Security Review**
- SLA / Object Protection**
- Physical Site Security**
- Deliver copies of technical whitepapers on best practices**

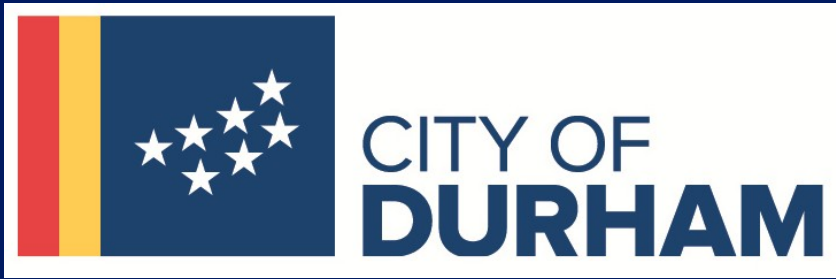
Reduksjon av nedetid – fokuser på restore!

- Når testet du sist DR/gjenoppretting?
- Hvor lang tid tar det å gjenopprette en server? Et miljø? Spesifikk data?
- Hvis (når) du får et ransomware-angrep, hvordan vet du hva du skal gjenopprette?
- Hva er prosessen/prosedyrene for å komme seg tilbake i full produksjon?
- Ha et forhold til at dette kommer (sannsynligvis) til å skje!

© Randy Glasbergen
glasbergen.com



**"I'm no expert, but I think it's
some kind of cyber attack!"**



**THE CITY CAN BE ASSURED THAT OUR BACKUPS
ARE VERY GOOD BECAUSE THEY'RE IMMUTABLE.**

**[THIS MEANS THAT] THEY COULD NOT BE CONSUMED BY
RANSOMWARE.**

Mayor Steve Schewell at City of Durham

Don't Backup. Go Forward.



www.rubrik.com