

강자가 나타났다! 씬파서블 AD 복구!

Solution Consultant / Hongso Chae

hongso.chae@quest.com

Quest

Where Next Meets Now.

AD 서비스 연속성(재해복구)의 필요성

국내 동향



카카오 사태



서비스의 이해 부족
(재해복구에 사각지대 존재)

2024 디지털금융 및 사이버보안 이슈 전망

금융보안원

Key Issue
핵심이슈

디지털 경쟁력, 금융보안 프랜차이즈 전략이 필수



- IT복합성 등으로 금융보안 사고를 **원천 차단**하기에 **한계**가 있으므로, 사고 발생 시 **신속한 대응**을 강조하는 **사이버 복원력(Cyber resilience)의 설계·운영**이 필요할 전망

Da 디지털데일리

구독중

PICK ①

행정전산망 장애는 결국 관리의 문제...지방행정전산서비스 개편TF, 총체적 난맥 밝힐 수 있을까?

입력 2023.11.22 오전 11:17 | 기사원문

실제 업계에서도 단순 네트워크 문제로 사흘간이나 국가 행정망이 마비되는 사태가 일어나지는 않았을 것이라는데 의견이 모이고 있다.

이번에 문제가 된 네트워크 장애, 특히 L4와 같은 로드밸런서는 여러 시스템과 연계되어 있는 공급망 역할을 한다. 때문에 L4에서 다른 장비로 데이터 전송이 되지 않으면 애플리케이션간의 문제로 확산된다.

이는 정부 시스템은 물론 기업에 이르기까지 업무 애플리케이션이 상호 중속성이 있기 때문이다.

이번에 새 운영정보시스템에 접속하는 인증시스템(GPKI)에 장애가 발생한 것으로 확인됐는데 일개의 한 관계자는 "GPKI 인증시스템이 문제가 발생하면 인증시스템과 한 성인 LDAP(Lightweight Directory Access Protocol), 즉 사용자 정보들을 가지고 있는 부분과 서로 참조하게 되는데 서비스 호출이 되지 않으면 애플리케이션 문제로 불거진다"며 "통신이 안 되면 전체 애플리케이션에 장애가 발생한다. 문제는 장애 발생으로 재부팅 등을 할 때 애플리케이션 중속성을 따져 순서에 맞게 해야 하는데 그 과정에서 문제가 생긴 것 같다"고 밝혔다.

이는 시스템을 관장하는 행정안전부, 국가정보자원관리원, 한국지역정보개발원 등 여러 관리주체가 나눠져 있기 때문에 풀이된다. 국가정보자원관리원은 사실상 인프라 관리 등에 초점이 맞춰져 있고 애플리케이션 관리 및 유지보수는 지방행정전산서비스 주무기관인 한국지역정보개발원처럼 업무 주체가 운영을 맡고 있기 때문이다.

때문에 단순히 네트워크 장애에만 판단하고 서둘러 재부팅, 혹은 장비교체를 했더라도 이 과정에서 전체 애플리케이션에 영향을 어떻게 미쳤는지 파악이 안돼 장기간의 장애로 이어졌을 것이라 관측이다.

일개의 한 관계자는 "L4를 셋다운 시키고 장애 복구에 나서더라도 애플리케이션 단에서의 시스템 및 구조를 이해를 못하고 애플리케이션 단 장애가 어디까지 확산돼 있는지를 이해를 못하면 문제가 생길 수 밖에 없다"고 지적했다.

어플리케이션의 이해는 필수(LDAP인증)

IT는 문제가 발생할 수밖에 없는데, 핵심은 문제를 얼마나 빠르게 복구(복원력)하여 서비스를 지속할지 여부

Quest

Where Next Meets Now.

AD서비스 영향

서비스 로그인 장애



vmware®

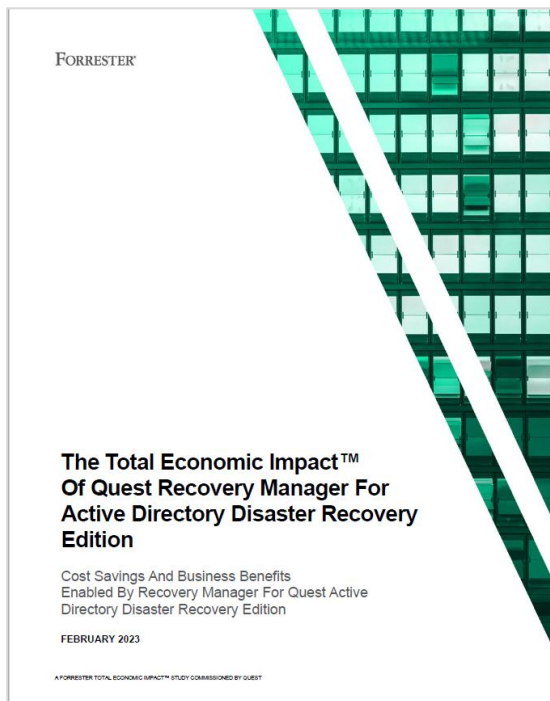


- A
- DRM
- NAC
- SSO
- 등에 당



비즈니스 금액 손실

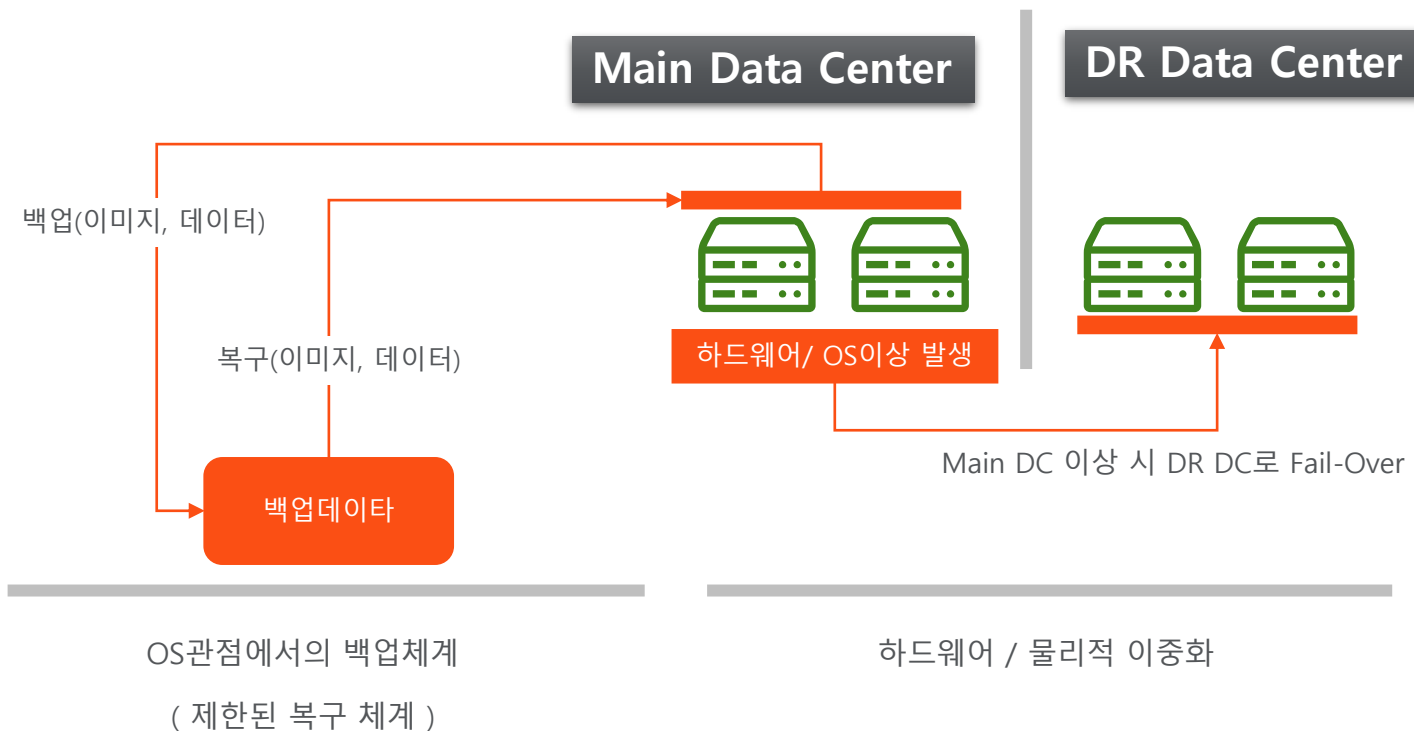
3년간 \$820K(약 10억원)의 손실



Faster And More Accurate Recovery From A Disaster Scenario (Weighted By Likelihood Of Attack)					
Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Cost of one hour of downtime during ransomware attack	Interviews	\$730,000	\$730,000	\$730,000
A2	Hours to recover Active Directory without Quest RMAD DRE	Interviews	30	30	30
A3	Business losses during Active Directory recovery	A1*A2	\$21,900,000	\$21,900,000	\$21,900,000
A4	Reduction in time to recover Active Directory due to Quest RMAD DRE	Interviews	85%	88%	90%
A5	Hours to recover Active Directory with Quest RMAD DRE	A2*(1-A4)	4.5	3.6	3.0
A6	Business value protected due to Quest RMAD DRE during the event of a ransomware attack	A3*A4	\$18,615,000	\$19,272,000	\$19,710,000
A7	Average likelihood of a successful ransomware attack impacting Active Directory each year	Ponemon	1.5%	1.5%	1.5%
At	Faster and more accurate recovery from a disaster scenario (weighted by likelihood of attack)	A6*A7	\$279,225	\$289,080	\$295,650
	Risk adjustment	15%			
Atr	Faster and more accurate recovery from a disaster scenario (weighted by likelihood of attack) (risk-adjusted)		\$265,264	\$274,626	\$280,868
Three-year total: \$820,757			Three-year present value: \$679,132		

AD 재해복구의 현재

AD 재해복구 환경 구성의 현재



AD DR의 현재

AD의 기본 기능(Replication)

- 다수의 DC를 구성해서 하드웨어 적인 이슈에 대해서만 제한적으로 대응 가능
- 이상 데이터 변경과 같은 상황에서는 Replication이 오히려 문제를 확대시킴

Microsoft

- 상태백업을 통한 복구를 권고하지만 DR 구성은 안됨

Enterprise Backup

- 주로 이미지 백업을 통한 복구를 지원하고 DR 구성에 제약
- 대부분은 AD에 특화된 기능 제공이 되지 않고 가이드도 되지 않음

운영 - DR을 위한 복구 시나리오

- 별도의 복구 필요 항목이나 복구 시나리오가 준비되어 있지 않음
- DR구성에 대해서 준비되지 않음

우리는 재해복구가 되어 있는가?

AD 복구 또는 DR 체계가 없을 때



Maersk

- NotPetya로 150개 DC중 149개 유실
- AD복구에 9일이 걸림
- \$\$ Millions 손실
- 뉴스 헤드라인 장식



국내 기업

- 랜섬웨어 공격
- 이전 OS 백업으로 복구
- Domain의 Trust가 깨져서 모든 단말에서 Domain 재 Join 수행
- Domain Re-Join에 몇 주 소요

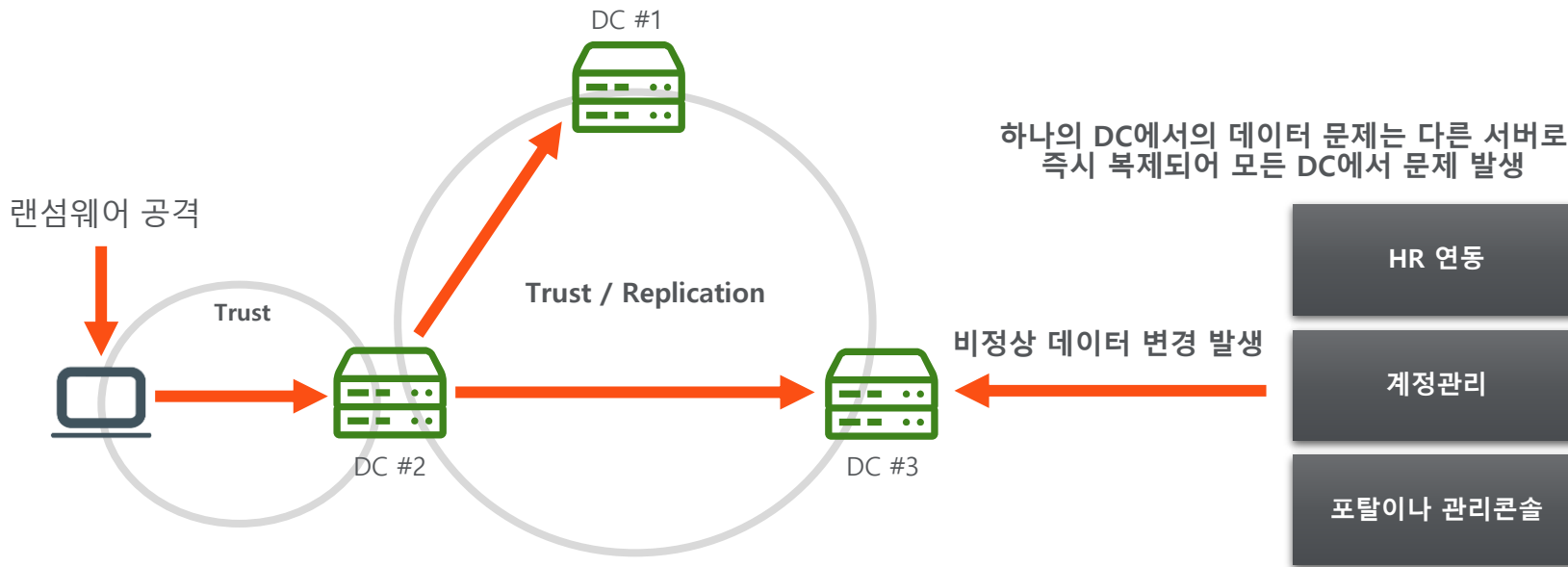


국내 기업

- 운영과정에서 문제 발생
- SYSVOL 삭제
- Enterprise 백업으로 복구
- 서비스 비정상으로 추가 조치 (2일 소요)

Active Directory 특징

AD의 주요 특징 : Trust와 Replication



단말과 DC, DC와 DC간에는 Trust가 되어 있어서

“랜섬웨어 공격이 발생하면 하나의 DC에서 연결된 다른 DC로는 연결된 포트를 통해서 손쉽게 공격가능”

Trust와 Replication 이슈



Computer

Trust가 깨지면

Domain Re-Join 필요

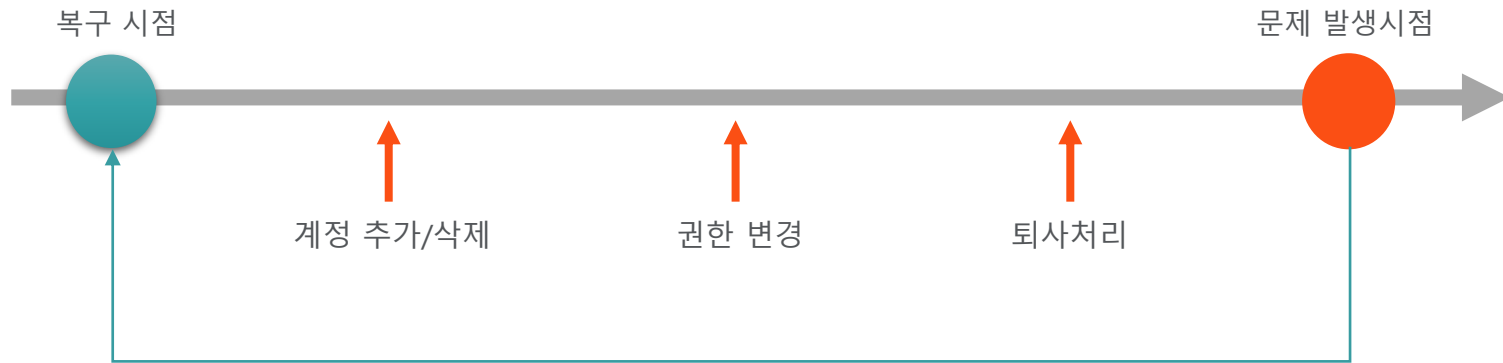


User

객체가 새로 생성되면

단말 Profile Migration 필요

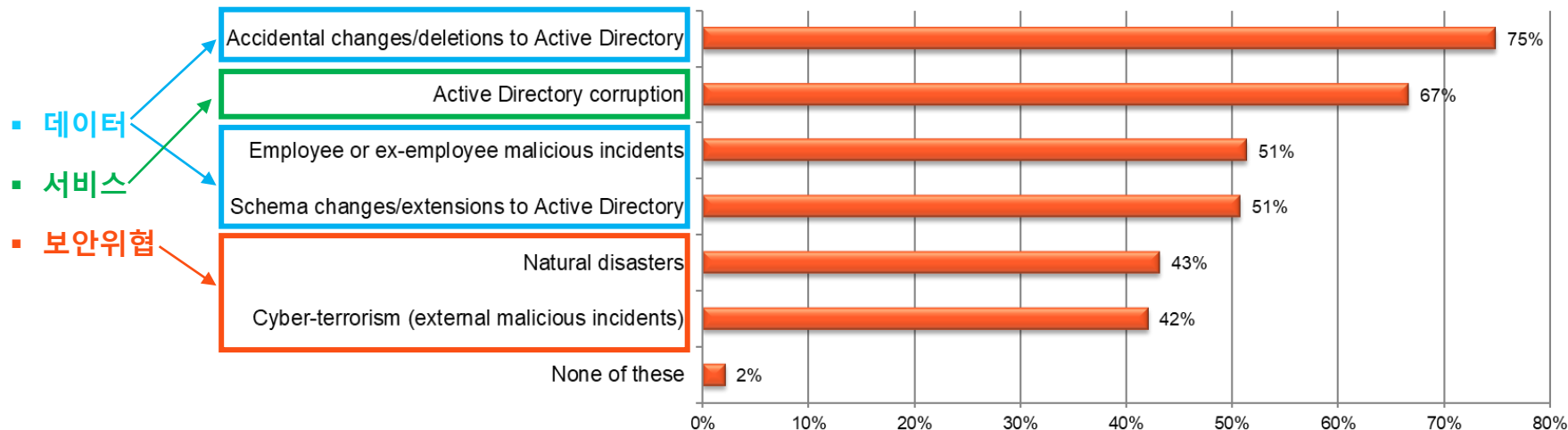
데이터 Validation = 보안



적용되지 않은 변경 사항은 서비스 및 보안이슈

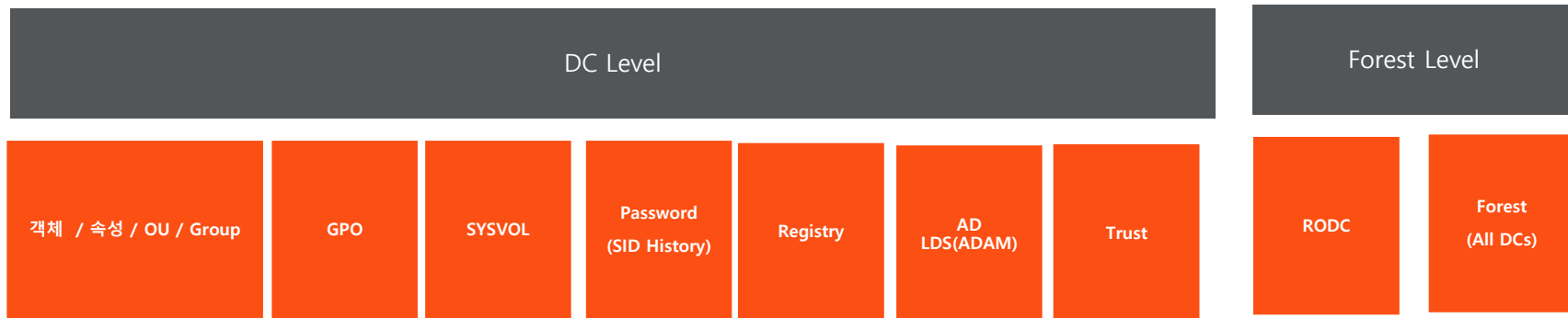
주요 복구 대상은?

On-Prem AD



데이터/서비스 복구의 필요성이 높으나 보안위협은 가능성은 낮으나 큰 피해 발생

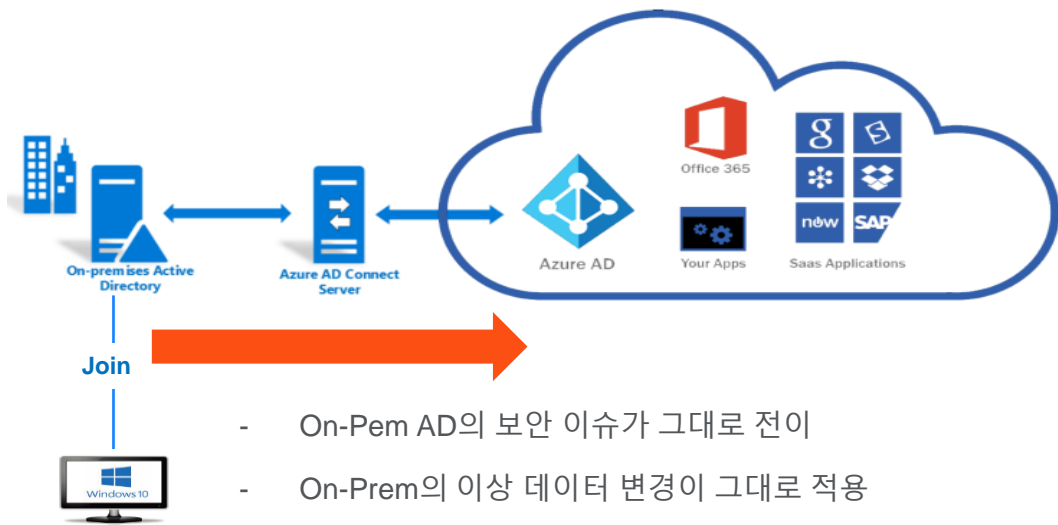
On-Prem AD에서 주요한 복구 대상



특정 대상만 선택적으로 복구 필요



M365



- On-Pem AD의 보안 이슈가 그대로 전이
- On-Prem의 이상 데이터 변경이 그대로 적용

운영 과정에서의 데이터 유실 / 서비스 이슈



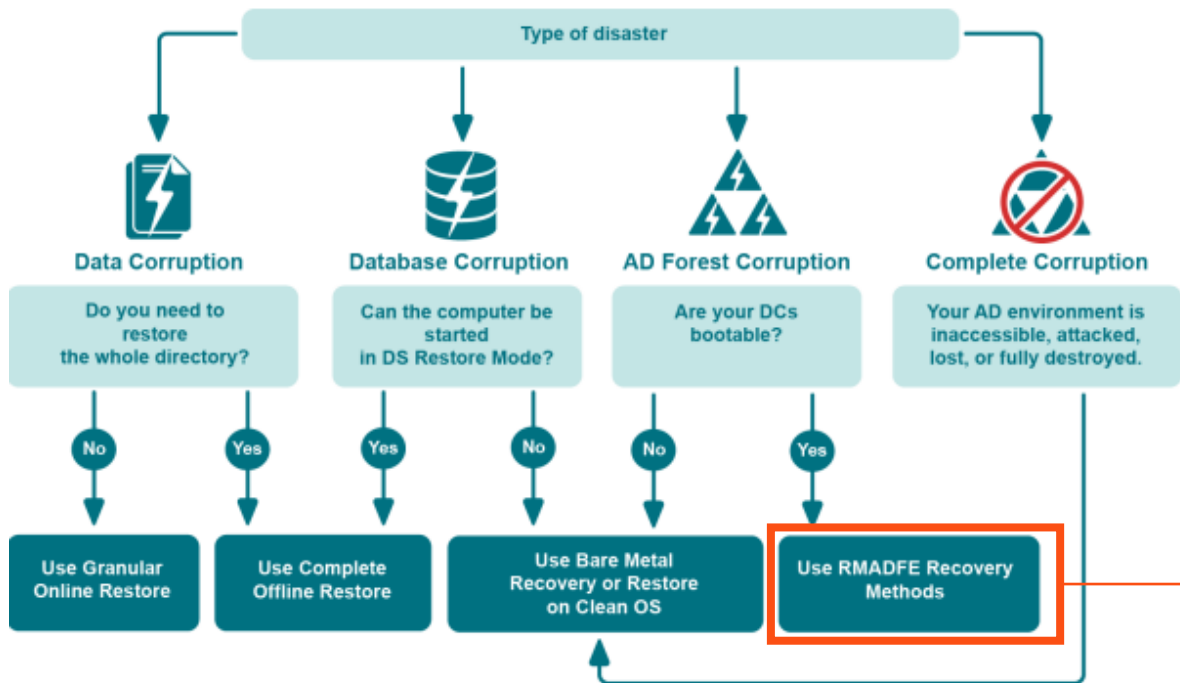
계정과 데이터는 고객 관리 영역

- Single sign-on
- Office 365 라이선스
- Application 역할 지정
- Office 365 그룹
- Teams membership
- SharePoint 권한
- .. 그리고 다른 클라우드 특화된 데이터

Quest 솔루션으로는 어떻게 복구?

(RMAD DRE - Recovery Manager for AD DRE)

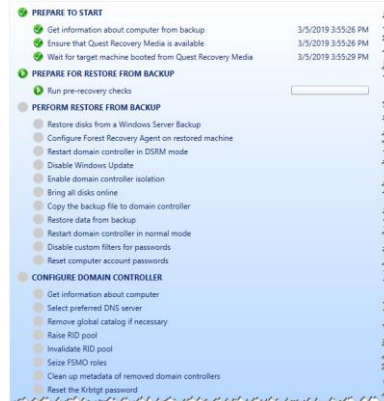
RMAD를 통한 복구



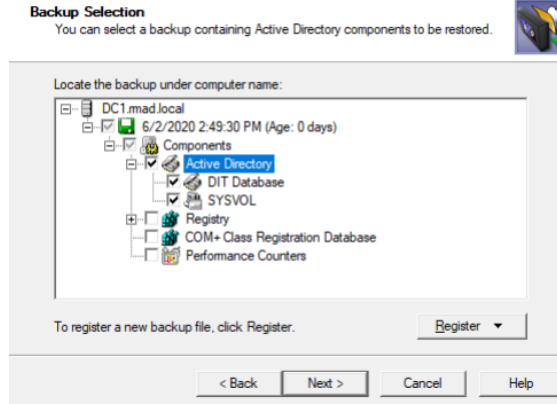
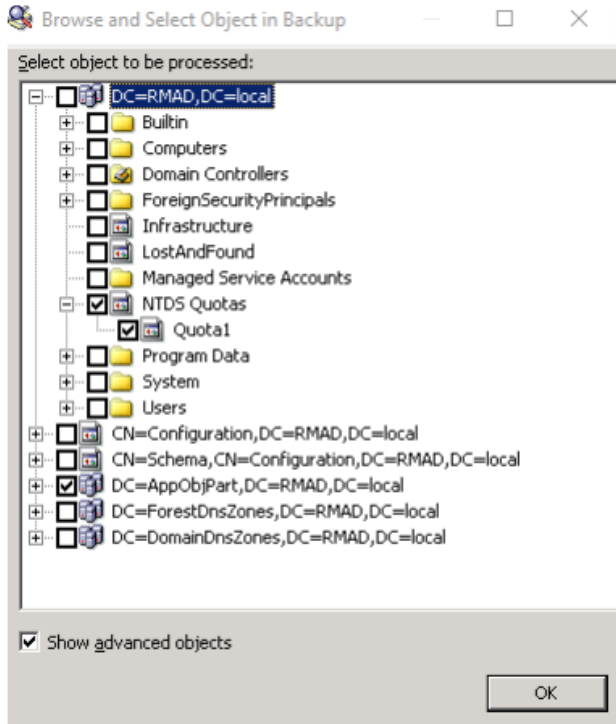
AD복구에 필요한 다양한 복구 옵션 지원

- Restore Active Directory from backup method
- Install Active Directory method
- Reinstall Active Directory method
- Uninstall Active Directory method
- Restore SYSVOL
- Restore Active Directory on Clean OS method
- Bare Metal Active Directory Recovery method
- Do not recover method
- Do nothing method
- Adjust to Active Directory changes method

모든 복구는 자동화되어 처리

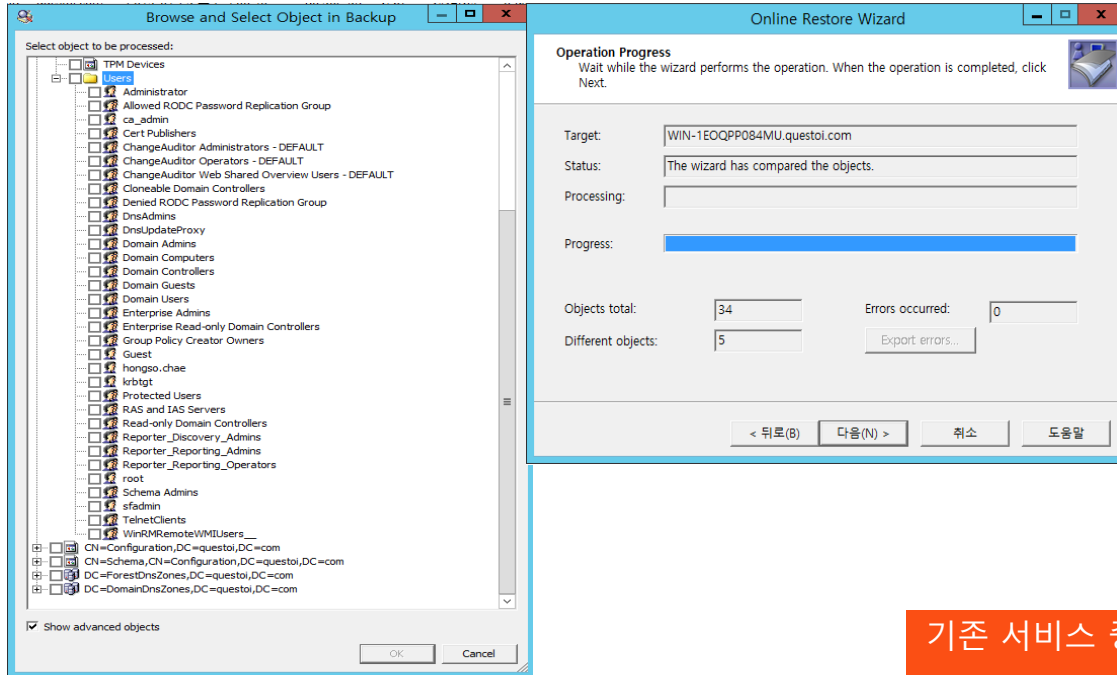


데이터 복구 - 상세 복구



Active Directory서비스에 필요한 데이터를 손쉽게 복구

데이터 복구- 객체,속성 비교 및 개별 복구



Operation: Compare backup against live computer
Finished on: 2/11/2019 3:13:19 PM
Source backup: C:\ProgramData\Quest\Recovery Manager for Active Directory\Backups\WIN-1EQQPP084MU.questoi.com\2019-01-25 11-42-45.bkf (1/25/2019 11:45:50 AM)
Target live computer: WIN-1EQQPP084MU.questoi.com
Number of processed objects: 34
Operation status: Completed successfully
This report provides information about: Added, deleted, and modified objects.
 Added, deleted, and modified attributes.

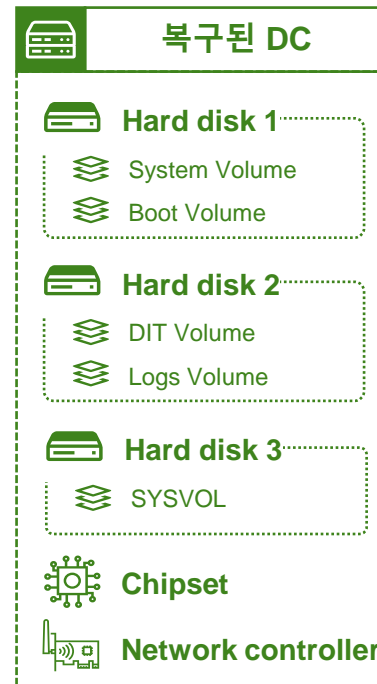
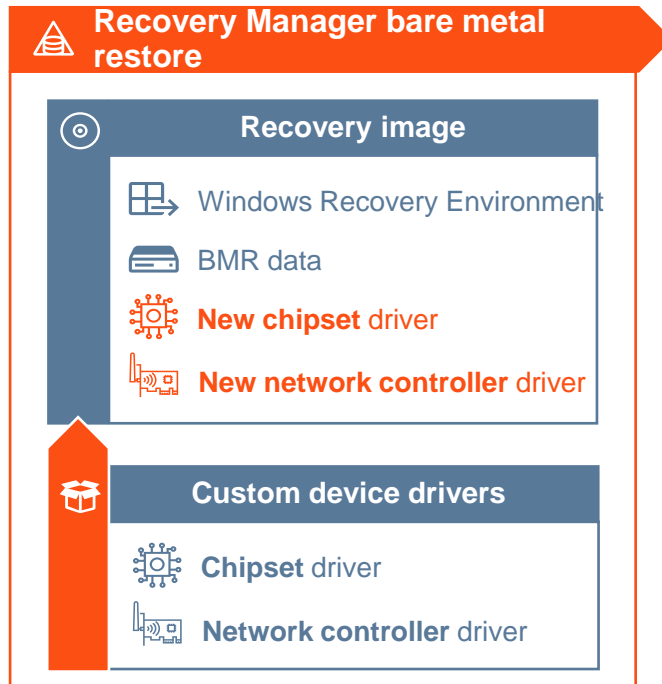
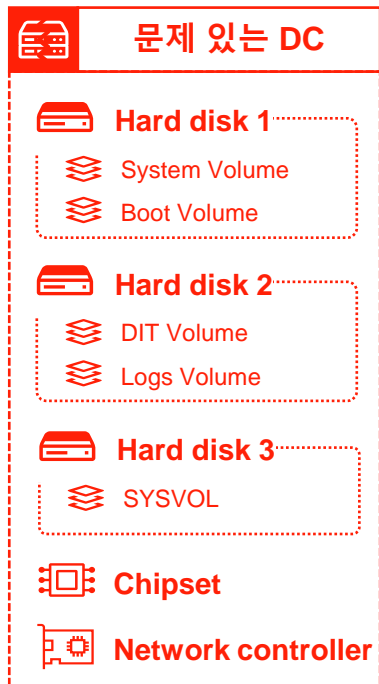
Number of objects by type of change

Expand all | Collapse all

Object DN	Object class	Type of change	Modified by
CN=Administrator,CN=Users,DC=questoi,DC=com	User	Modified	
CN=ca_admin,CN=Users,DC=questoi,DC=com	User	Deleted	
CN=Domain Admins,CN=Users,DC=questoi,DC=com	Group	Modified	
CN=sfadmin,CN=Users,DC=questoi,DC=com	User	Modified	
CN=Users,DC=questoi,DC=com	Container	Modified	

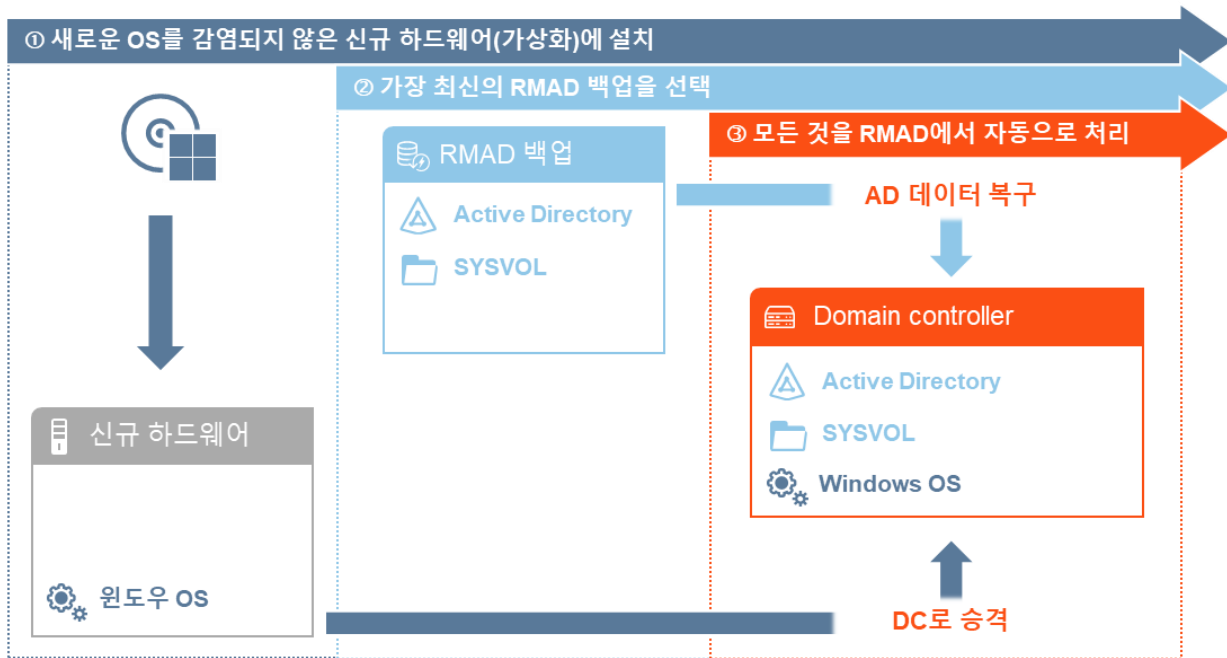
기존 서비스 중단없이, 필요한 데이터만 선택적으로
 비교 및 복구 가능 (복구후에 서비스 추가 설정 필요없음)

데이터베이스, 서비스 복구 – BMR



데이터베이스, 서비스 복구 – Clean OS 복구

장애 DC



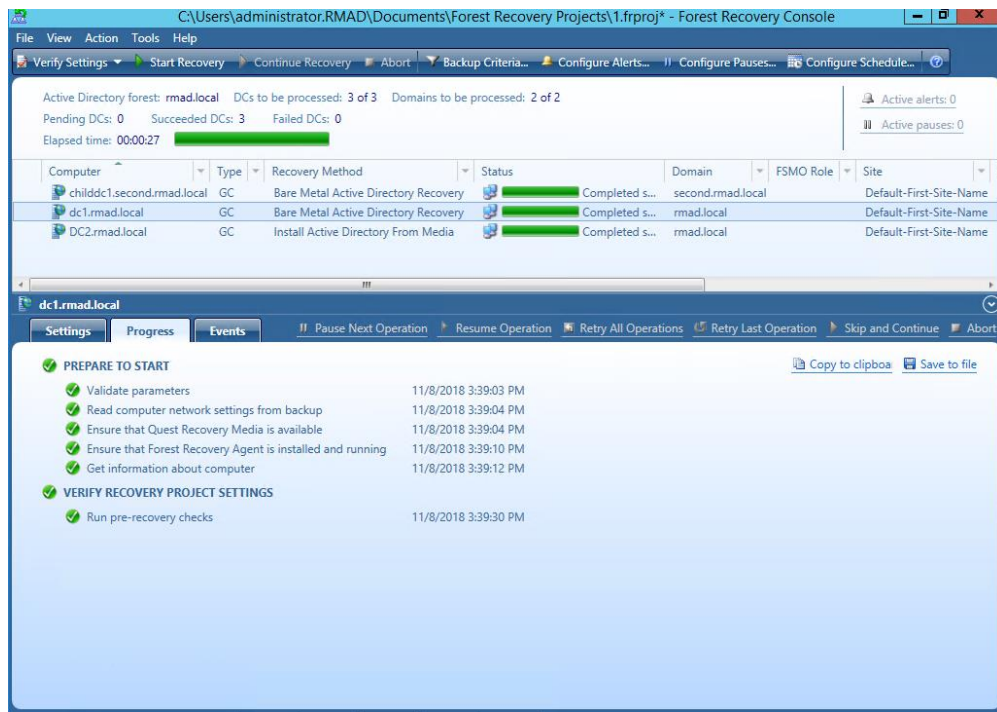
정상 DC



특허

18개의 설정과 40단계의 복구 과정을 자동화

Forest 단위 복구

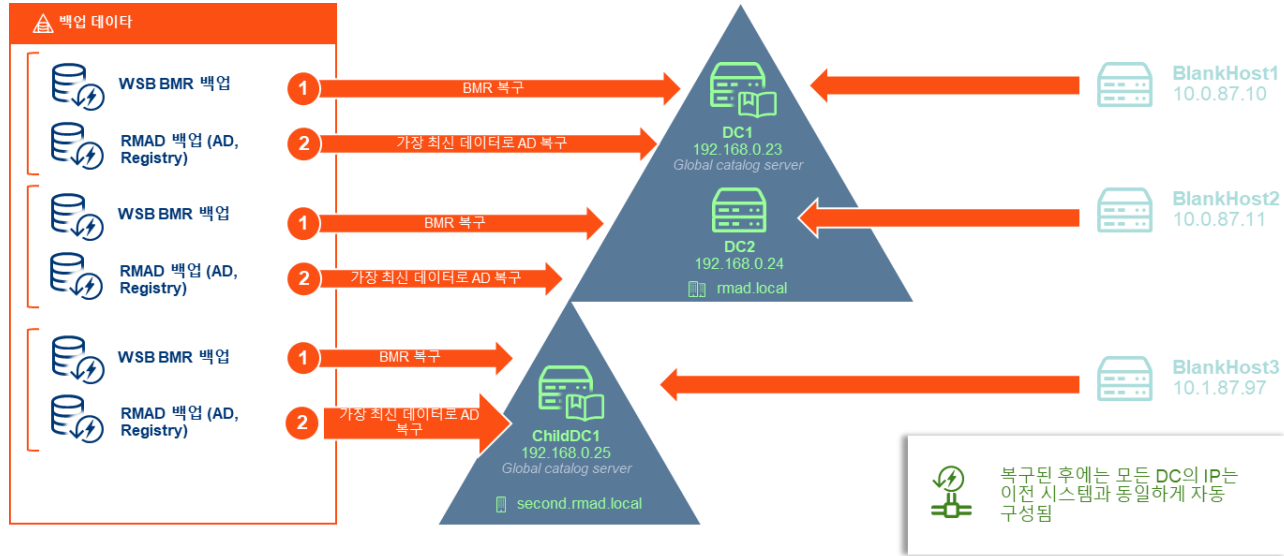


Forest에 대한 복구 Project 생성 및 주기적인 Validation 수행

- Restore Active Directory from backup method
- Install Active Directory method
- Reinstall Active Directory method
- Uninstall Active Directory method
- Restore SYSVOL
- Restore Active Directory on Clean OS method
- Bare Metal Active Directory Recovery method
- Do not recover method
- Do nothing method
- Adjust to Active Directory changes method

- 자체 검증 기능 지원
- 진행상황을 시각적으로 제공
- 복구후에 Health Check 수행

데이터와 OS 분리 백업 및 복구



- Remove global catalog (if you did not specify to keep the existing global catalog)
- Raise RID pool
- Invalidate RID pool
- Seize FSMO roles
- Clean up metadata of removed domain controllers
- Reset the Krbtgt password
- Reset password for users in privileged groups
- **Reset computer account passwords**
- Enable custom password filters
- Restart domain controller in normal mode
- **Reset trust passwords**

Trust 복구

복구 속도

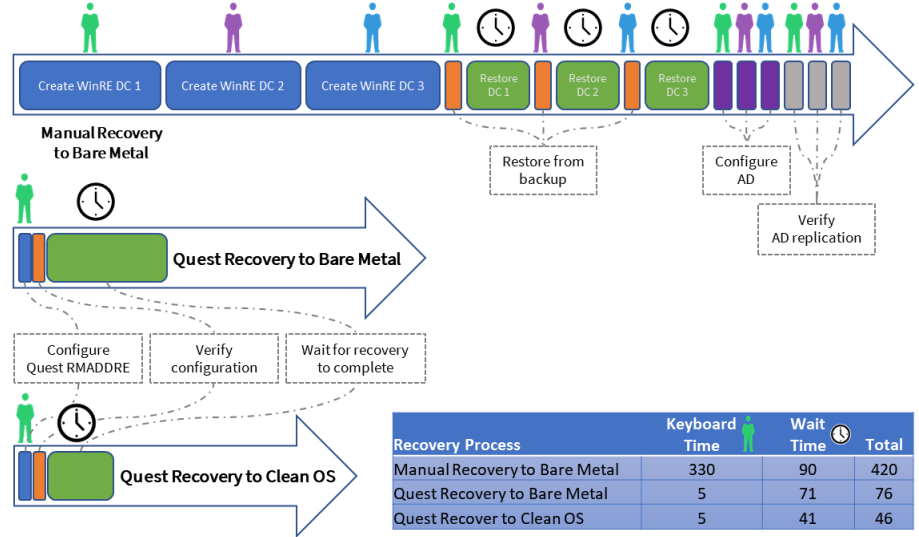
객체

Agent-based restore

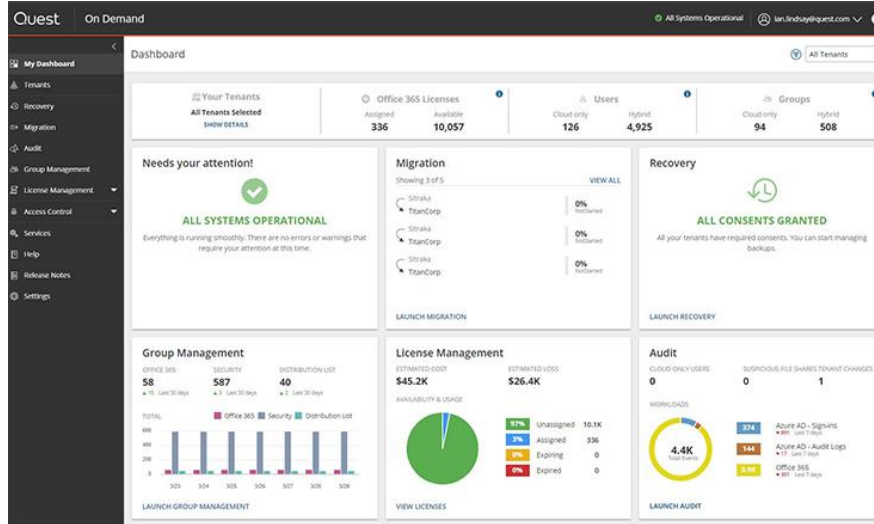
Number of objects - Required time

- 1000 - 20 - 40 sec
- 10000 - 04 - 06 min
- 50000 - 23 - 34 min

재해복구



Azure AD 복구



Tenant	Migration Status	Recovery Status
Straka	0% Not Started	0% Not Started
TranCorp	0% Not Started	0% Not Started
Straka	0% Not Started	0% Not Started
TranCorp	0% Not Started	0% Not Started
Straka	0% Not Started	0% Not Started
TranCorp	0% Not Started	0% Not Started

Activity	User	Time	Status
Azure AD - Signins	438	Last 7 days	374
Azure AD - Audit Logs	111	Last 7 days	144
Office 365	100	Last 7 days	8,888

- ✔ Office 365 licenses
- ✔ Mailbox
- ✔ Application role assignments
- ✔ Office 365 groups & Teams membership
- ✔ Multi-factor authentication & password reset configuration
- ✔ Azure AD Roles membership
- ✔ Conditional Access Policies rules
- ✔ Custom properties for cloud applications
- ✔ SharePoint permissions

“완벽한 데이터 복구 지원”



부가 기능 : 운영환경을 가상화에 자동 구성

Source Active Directory forest: acme.test Total computers: 3 Connected to: vcenter.acme.test (VMware vCenter)

Computer Name	Target Type	Target FSMO Roles	Target Network	Forest Recovery Agent	VMware Agent	Operation Status	Operation	Domain
acme.test (3)								
dc1.acme.test	GC	P R S D	192.168.0.1 on Internal Virtual Network	8.6.0.5302	5.5	Completed	Get source computer co...	acme.t
dc2.acme.test	DC	I	192.168.0.2 on Internal Virtual Network	8.6.0.5302	5.5	Completed	Get source computer co...	acme.t
dc3.acme.test	GC		192.168.0.3 on Internal Virtual Network	8.6.0.5302	5.5	Completed	Get source computer co...	acme.t

General Hardware Active Directory Events

Target Virtual Machine Name: dc1.acme.test (Virtual Lab) VM folder: Virtual Machines Host Name: 10.30.66.70 Storage: datastore1 Space available: 465 GB free of 931 GB

Source Computer Access User name: acme\administrator Password: Password Source Computer Details Operating system: Windows 2003 Number of processors: 1 Memory (RAM): 512 MB Network adapters: 1

- 손쉽게 테스트환경 구성

Enable Network Adapters

The virtual lab has been successfully created.

To enable network adapters in the virtual lab, review the settings below, and then click Enable.

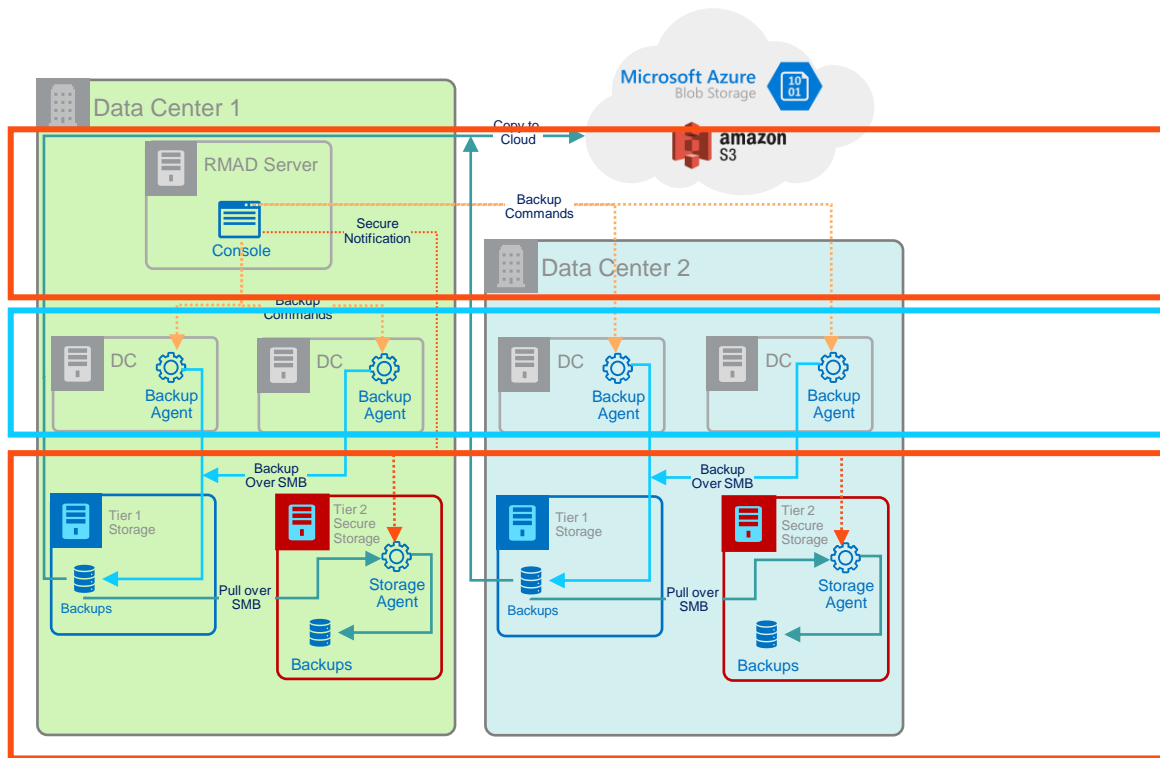
⚠ Ensure the virtual lab is isolated from the production environment.

Target Virtual Machi...	Domain	Network	IP Address	DNS Addresses
VM Network non-phys (on 10.30.66.24)				
<input checked="" type="checkbox"/>	shiraz.wine.msk.q...	wine.msk.qsft	VM Network non-phys (...)	192.168.0.2 192.168.0.27
<input checked="" type="checkbox"/>	fonseca.port.wine....	port.wine.msk.qsft	VM Network non-phys (...)	192.168.0.3 192.168.0.27
<input checked="" type="checkbox"/>	enomatic.wine.ms...	Non-domain contr...	VM Network non-phys (...)	192.168.0.27 192.168.0.27

Enable Close

제품의 구성은?

제품 자체적인 DR 구성 지원 (서버 – Agent)



관리콘솔은 단일 구성 및
2원화 구성 가능

DC에 Agent를 설치하여 동작

1차 기본 백업에
2차로 Immutable 백업

Enterprise 백업과 비교

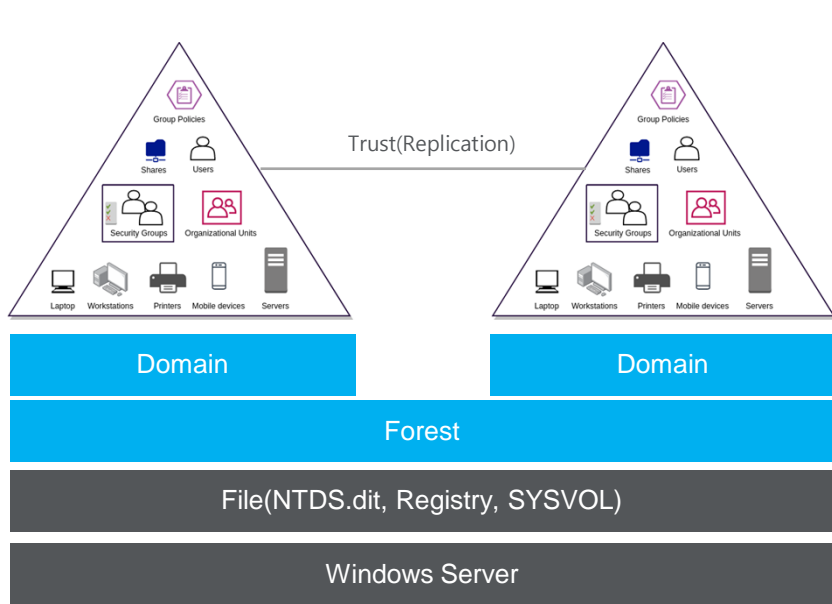
Restore vs. Rebuild — Strategies for Recovering Applications After a Ransomware Attack

Published 2 March 2022 - ID G00761039 - 11 min read

By Analyst(s): Nik Simpson, Ron Blair

“If possible, invest in dedicated tools for Active Directory recovery ... enterprise backup tools are often not fit for (this) purpose.”

백업/복구 관점에서 AD를 바라보는 차이



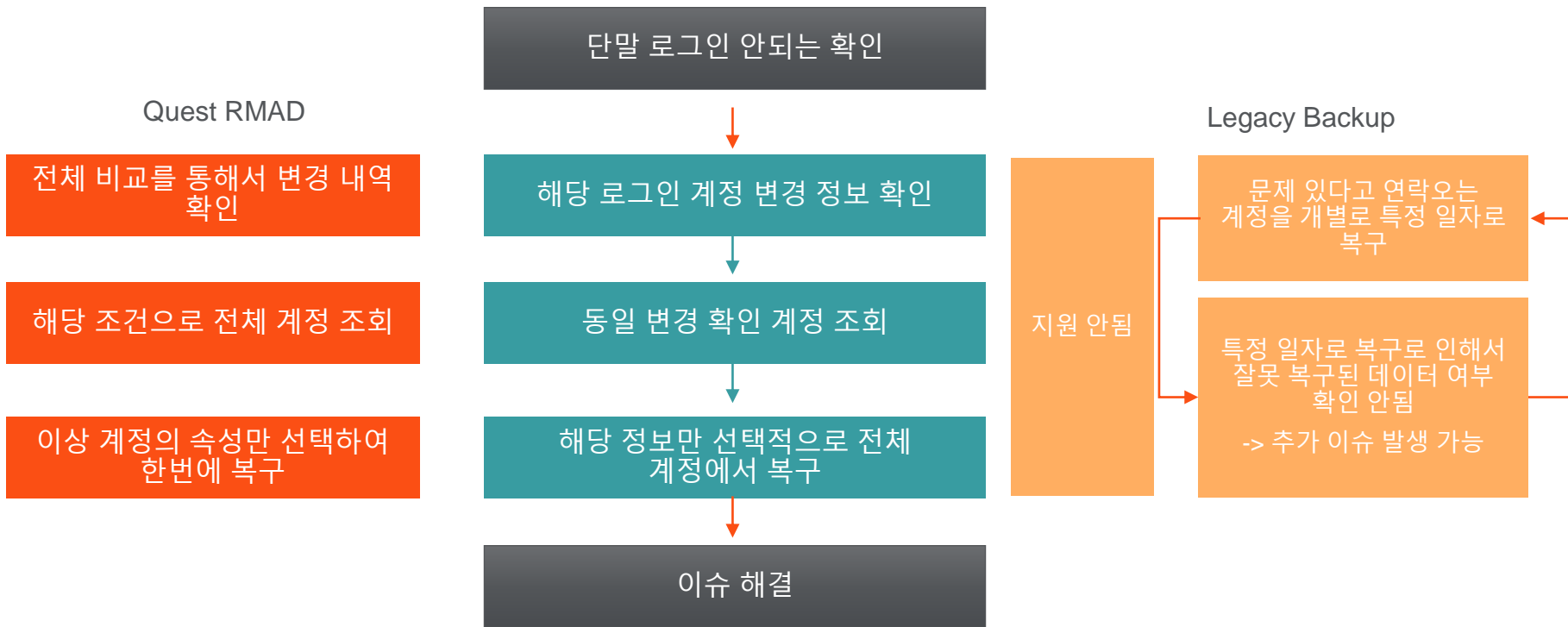
Quest RMAD DRE

서비스 관점에서의 백업 및 복구

Legacy Backup

OS(파일) 관점에서의 백업 및 복구

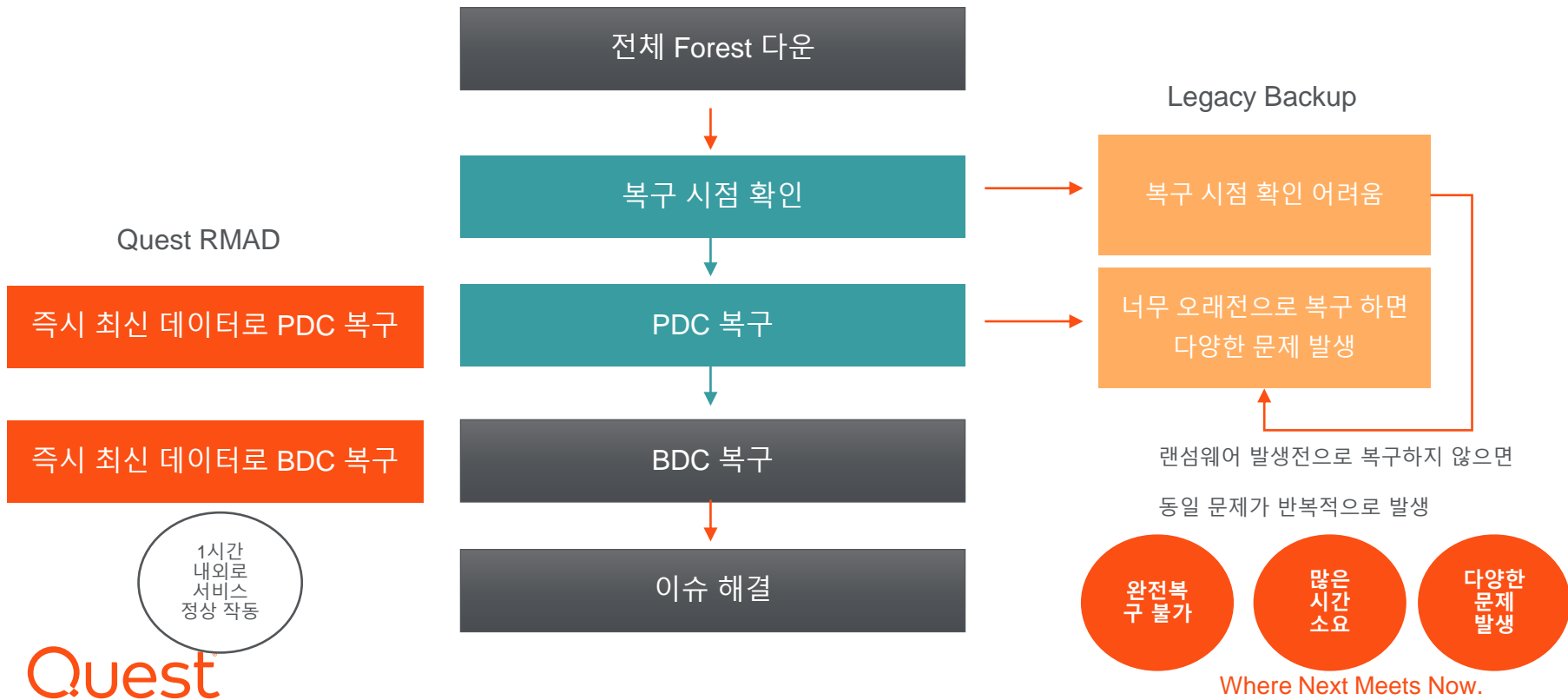
Use Case #1 : 속성변경



Use Case #2 : GPO 복구

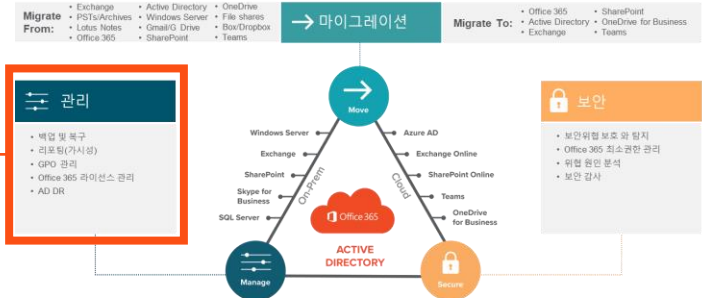


Use Case #3 : 랜섬웨어 발생



왜 퀘스트의 솔루션인가?

Quest는 AD영역의 글로벌 리더



On-Prem / Azure AD 환경을 통합 지원



- Active Directory migration
- AD monitoring, reporting and analytics
- Active Directory threat detection and response
- Active Directory backup
- Specialized AD management
- Access management
- Least privilege & separation of duty
- General-purpose PAM tools
- Active Directory bridging software to integrate non-Windows systems
- Identity governance and administration (IGA)
- Architectures for multitenant environments

“Quest는 Gartner가 제시한 AD 11개분야에 모든 솔루션을 제공하는 유일한 회사”



마이크로소프트의 VDI 솔루션 소개 및 퀘스트의 Active Directory DR의 구축전략

2023년 02월 16일(목) 14:00 - 15:00

마이크로소프트의 VDI 솔루션 소개 및 퀘스트의 Active Directory DR의 구축전략

이 세미나 개요

IT 운영자와 사용자가 손쉽게 접근할 수 있는 VDI 솔루션인 Azure Virtual Desktop에 대한 전반적인 소개와 클라우드를 활용할 때 준비해야 할 비즈니스 연속성에 대한 Azure의 전략을 소개합니다.

또한 비즈니스 연속성을 위한 핵심 서비스인 AD와 AAD에 대한 DR 전략에 대해 왜 현재 DR이 안되어 있는지 분석하고, AD 특징을 고려하여 어떻게 구성해야 하는지에 대한 내용을 사례 중심으로 소개합니다.

2023년 02월 16일(목)
14:00 - 15:00
온라인 무료세미나

[다시 보기](#)

[발표자료 >](#)



Where Next Meets Now.

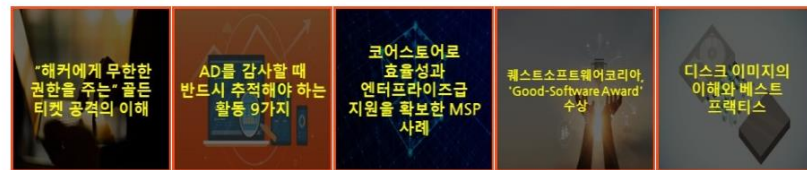
Quest 블로그

퀘스트 블로그에 방문하시면
퀘스트 솔루션들에 대한 다양하고 유익한
정보를 확인 하실 수 있습니다.

URL : https://blog.naver.com/quest_kor

프론트로그 | 블로그 | 퀘스트소프트웨어 소식 | 데이터베이스 관리 | 데이터 보호 | Microsoft 플랫폼 관리

인부



"해커에게 무한한 ... (1) AD를 감사할 때 반... (1) 코어스토어로 효율... 퀘스트소프트웨어... 디스크 이미지의 ...
2022. 10. 20 2022. 10. 18 2022. 10. 13 2022. 10. 12 2022. 10. 11



Where Next Meets Now.



Thank You