Organizační opatření ZKB technickým pohledem

ALEF

§ 26

Nástroj pro zajišťování úrovně dostupnosti

§ 9

Bezpečnost lidských zdrojů

ZÁKON

ze dne 23. července 2014

o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

316

VYHLÁŠKA

ze dne 15. prosince 2014

o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

§ 32

Forma a náležitosti hlášení kybernetických bezpečnostních incidentů

§ 10

Řízení provozu a komunikací

§ 8

Řízení aktiv

§ 12

Akvizice, vývoj a údržba

Bezpečnost průmyslových a řídicích systémů

§ 13

Zvládání kybernetických bezpečnostních událostí a incidentů

§ 11

Řízení přístupu a bezpečné chování uživatelů

§ 14

Řízení kontinuity činností

§ 18

Nástroj pro ověřování identity uživatelů

§ 16

Fyzická bezpečnost

§ 31

Kategorie kybernetických bezpečnostních incidentů

§ 20

Nástroj pro ochranu před škodlivým kódem

§ 19

Nástroj pro řízení přístupových oprávnění

§ 23

Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

§ 22

Nástroj pro detekci kybernetických bezpečnostních událostí

ZÁKON

ze dne 8. března 2017,

kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony

§ 3

Systém řízení bezpečnosti informací

§ 30

Typy kybernetických bezpečnostních incidentů

§ 5

Bezpečnostní politika

§ 7

Stanovení bezpečnostních požadavků pro dodavatele

§ 15

Kontrola a audit kritické informační infrastruktury a významných informačních systémů

§ 17

Nástroj pro ochranu integrity komunikačních sítí

§ 21

Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů

§ 25

Kryptografické prostředky

§ 4

Řízení rizik

§ 28

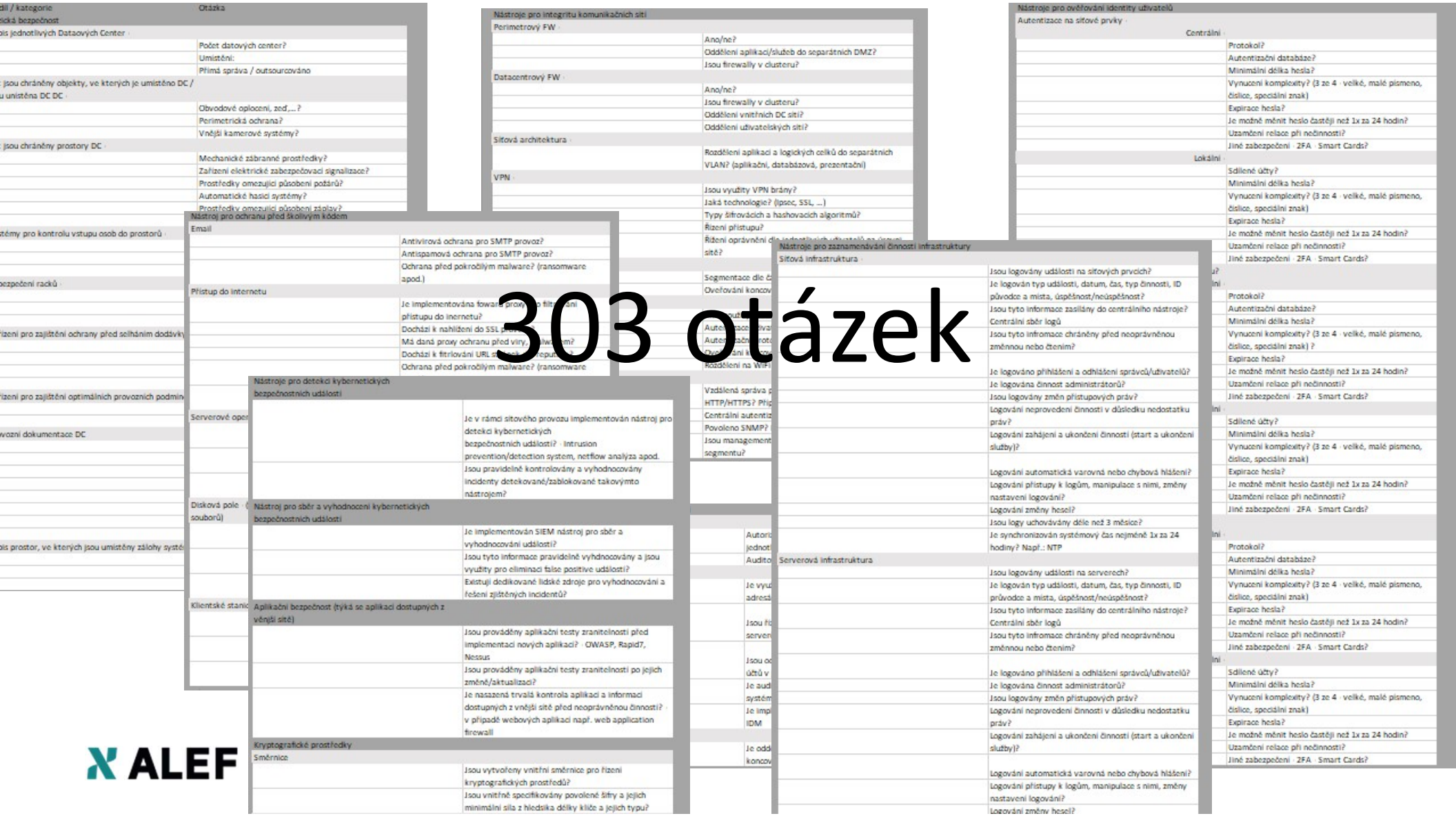
Bezpečnostní dokumentace

§ 24

Aplikační bezpečnost

§ 29

Prokázání certifikace



ALEF

- Jak zhodnotit současný stav?
- Kde aplikovat technická opatření?

ALEF

- Významný informační systém
- Kritická informační infrastruktura
- ISZS – Informační systém základních služeb
- Informační systém
- Komunikační systém
- Primární aktiva
- Podpůrná aktiva

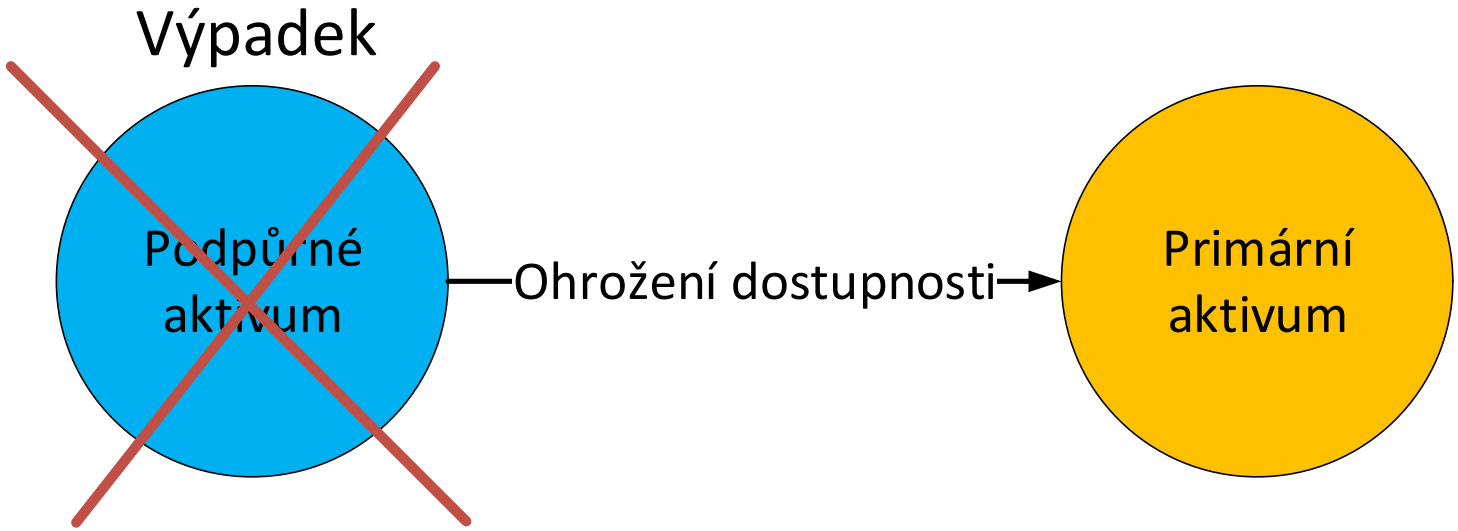
ALEF

Co je podpůrné aktivum?

- podpůrná aktiva jsou technická aktiva, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému
- technickým aktivem je technické vybavení, komunikační prostředky a programové vybavení informačního systému

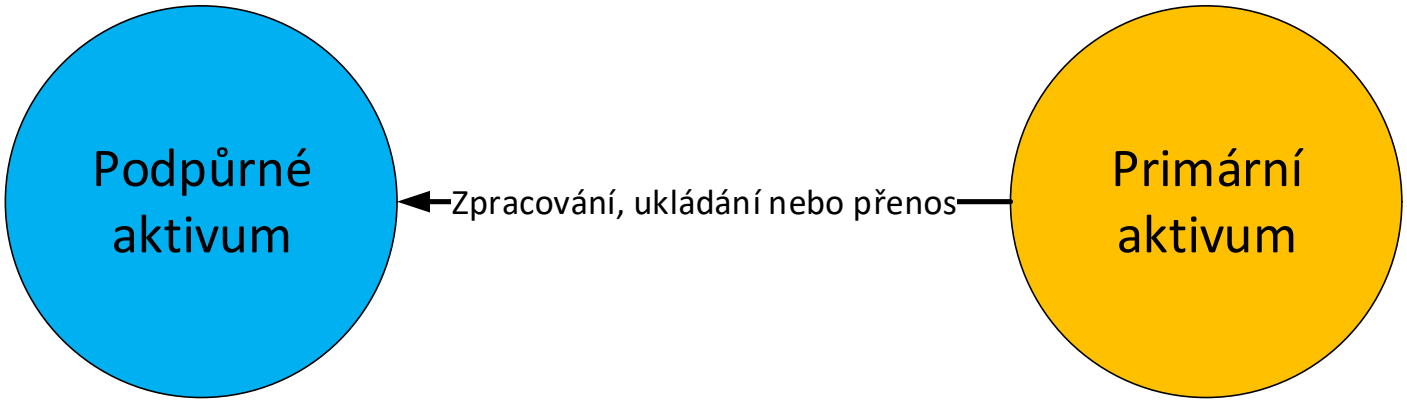
ALEF

Jak poznat podpůrné aktivum



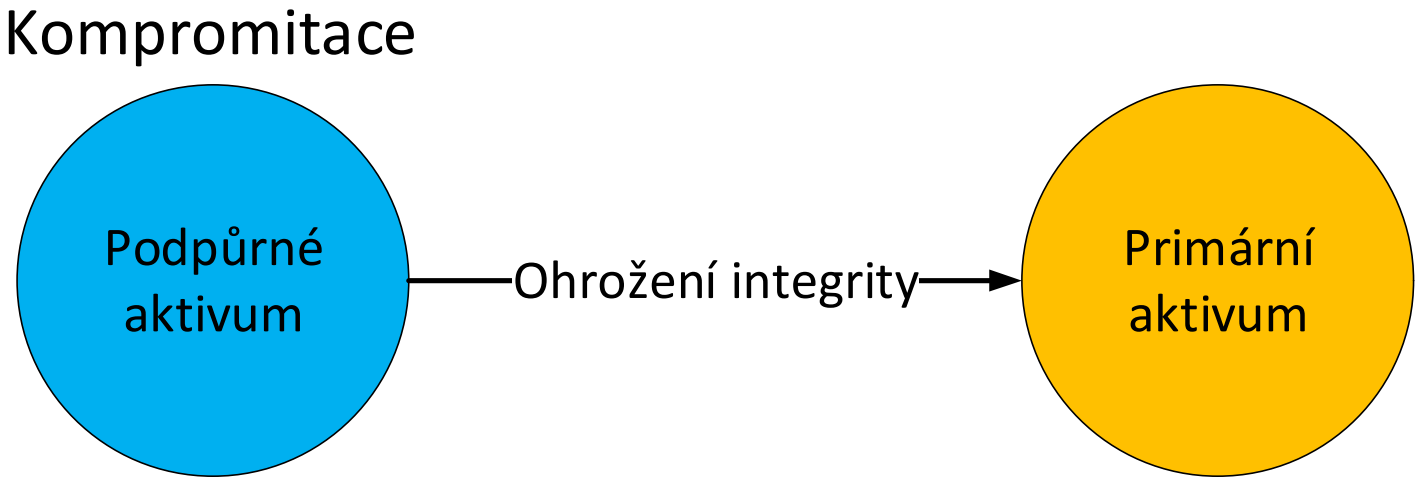
ALEF

Jak poznat podpůrné aktivum



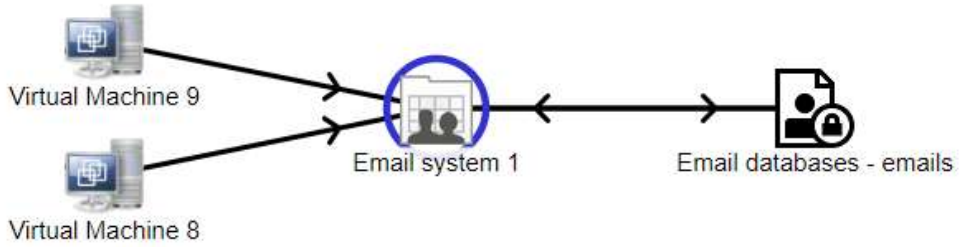
ALEF

Jak poznat podpůrné aktivum

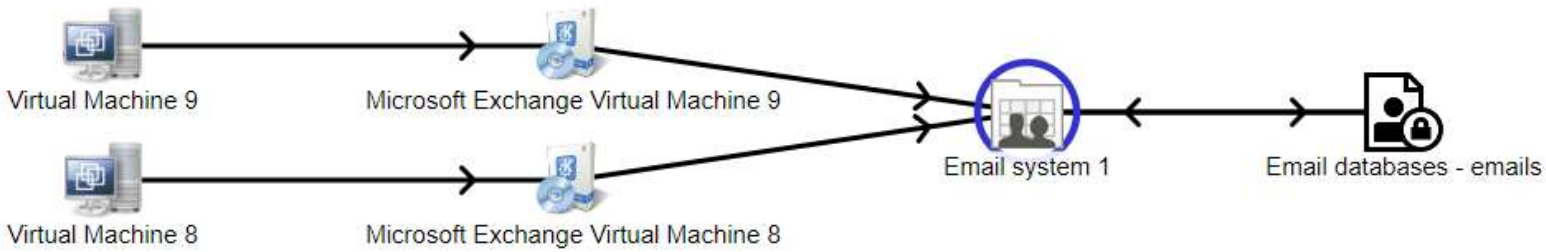


ALEF

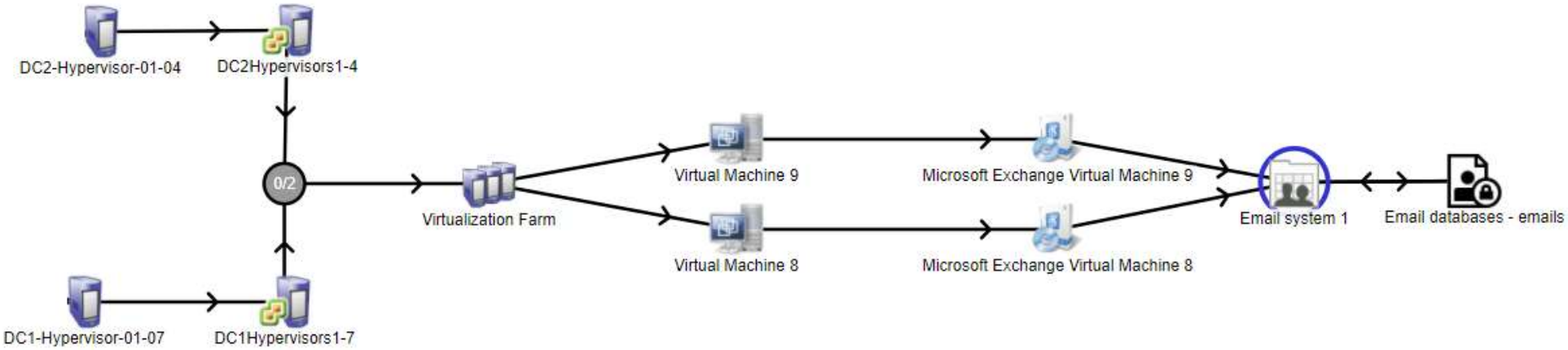
Analýza podpůrných aktiv



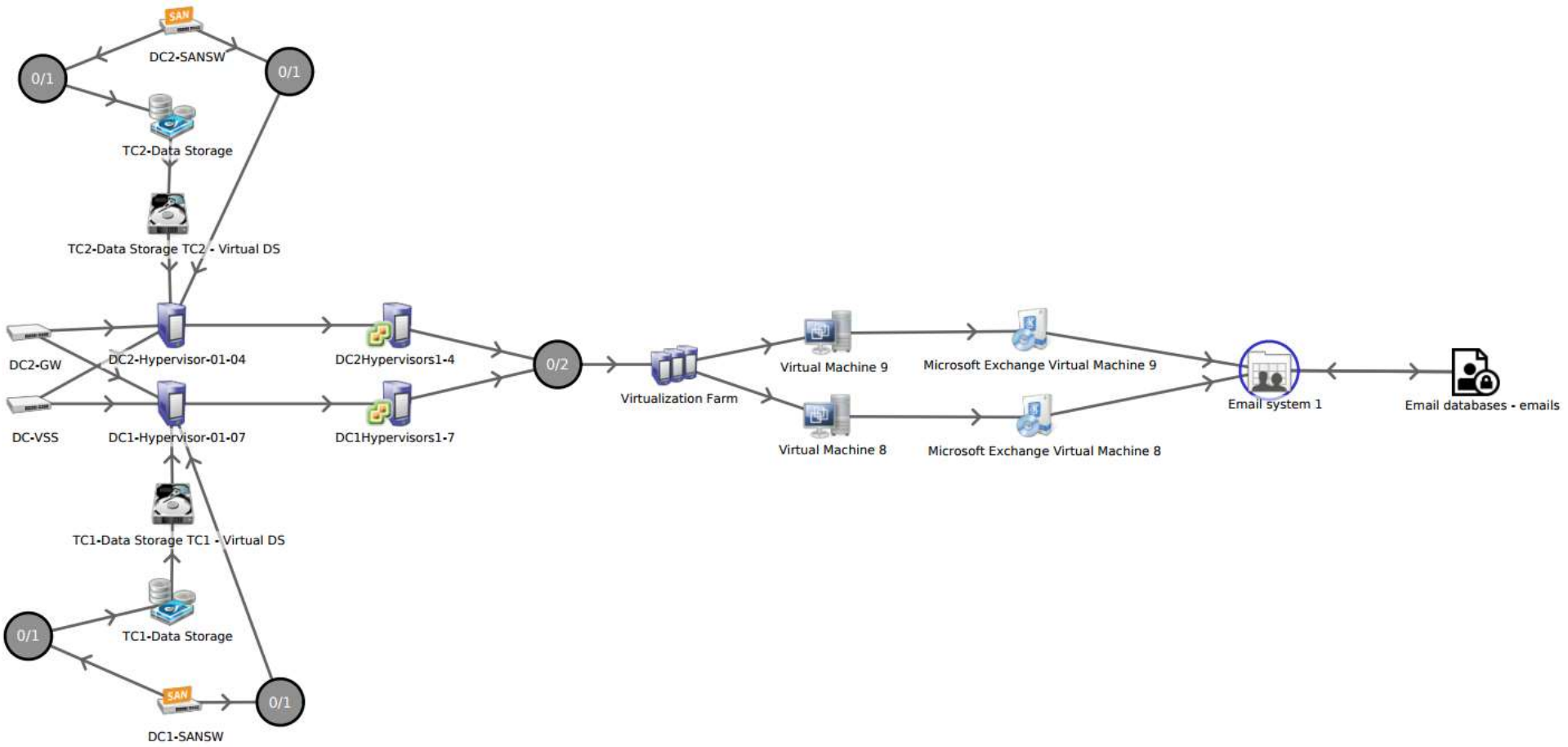
ALEF


Virtual Machine 9
Microsoft Exchange Virtual Machine 9
Virtual Machine 8
Microsoft Exchange Virtual Machine 8
Email system 1
Email databases - emails

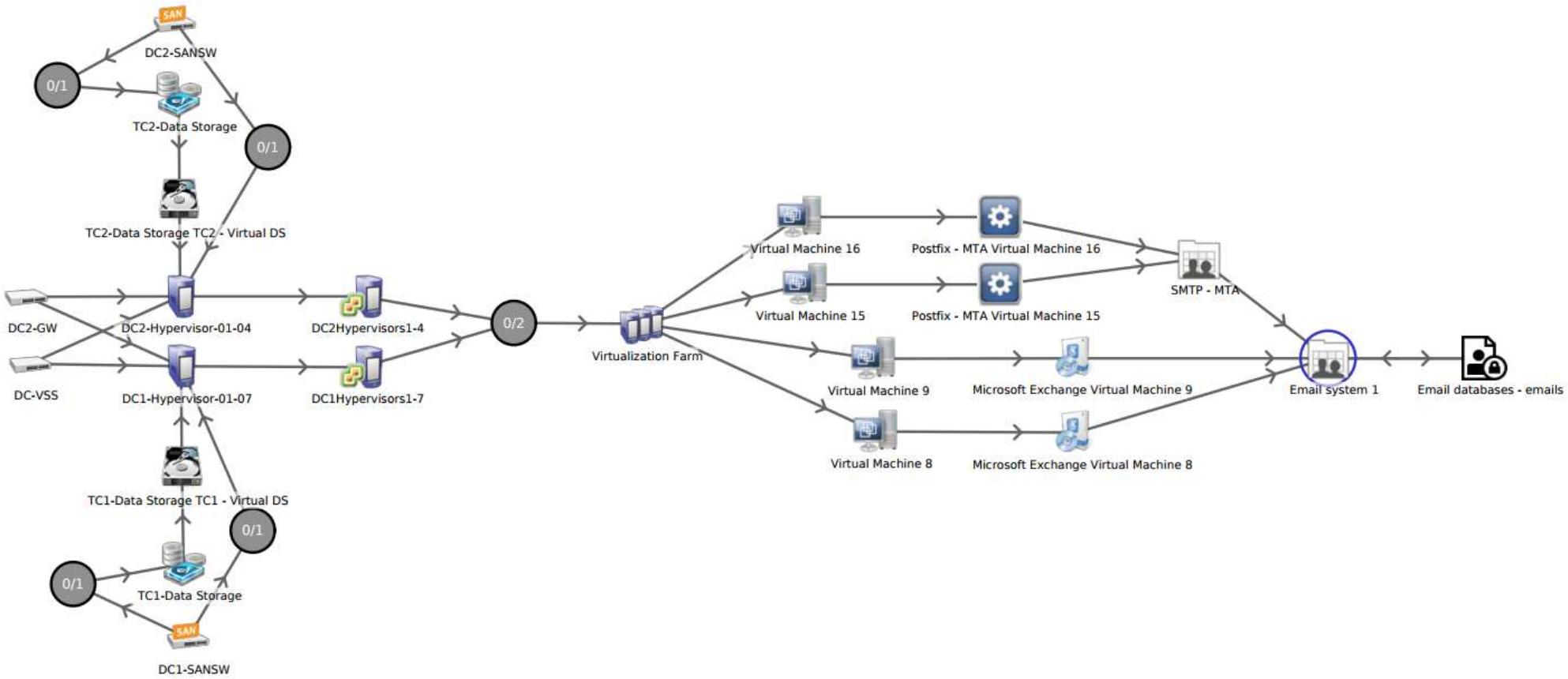
ALEF


DC2-Hypervisor-01-04
DC2Hypervisors1-4
0/2
Virtualization Farm
Virtual Machine 9
Virtual Machine 8
Microsoft Exchange Virtual Machine 9
Microsoft Exchange Virtual Machine 8
Email system 1
Email databases - emails
DC1-Hypervisor-01-07
DC1Hypervisors1-7

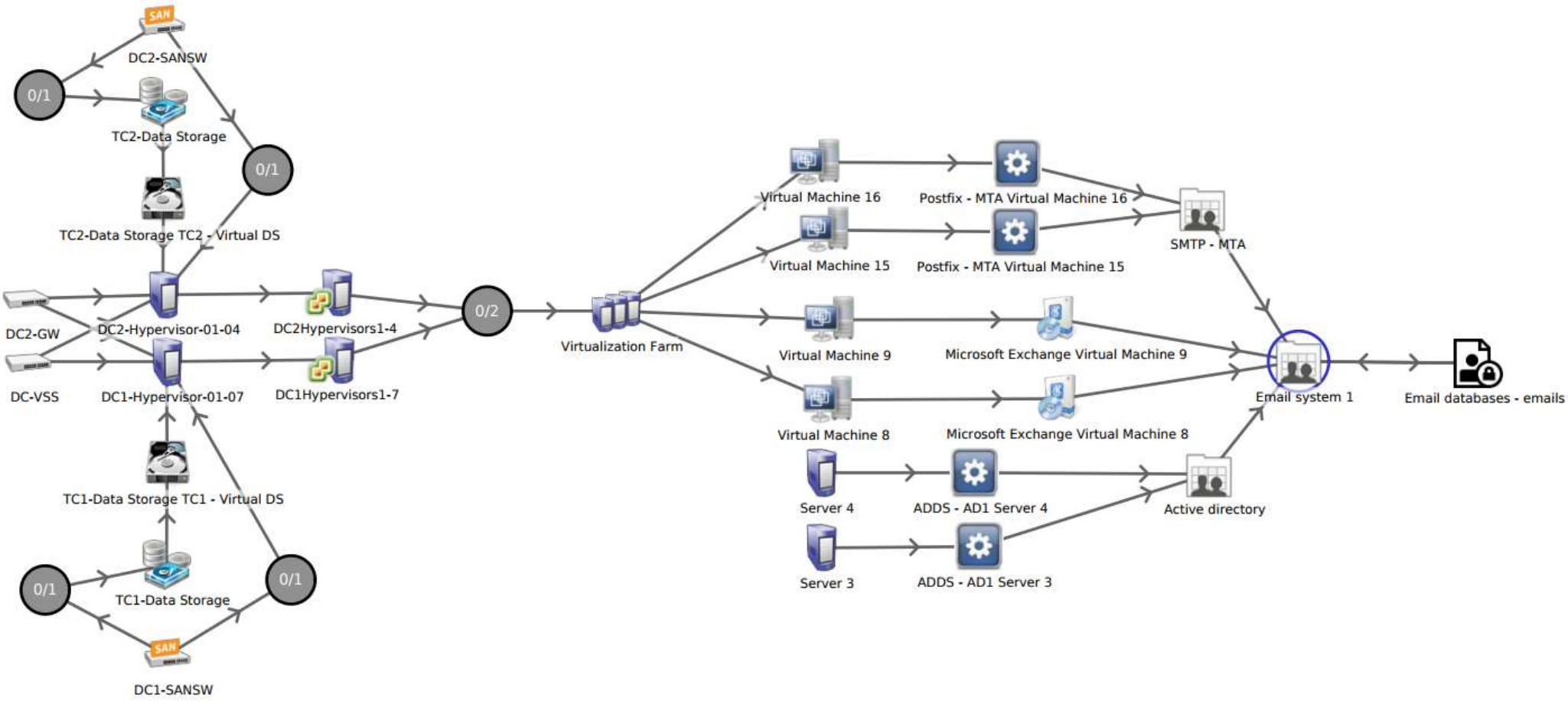
ALEF


DC2-SANSW
0/1
0/1
TC2-Data Storage
TC2-Data Storage TC2 - Virtual DS
DC2-GW
DC2-Hypervisor-01-04
DC2Hypervisors1-4
0/2
Virtualization Farm
Virtual Machine 9
Microsoft Exchange Virtual Machine 9
Email system 1
Email databases - emails
DC-VSS
DC1-Hypervisor-01-07
DC1Hypervisors1-7
Virtual Machine 8
Microsoft Exchange Virtual Machine 8
TC1-Data Storage TC1 - Virtual DS
0/1
TC1-Data Storage
0/1
DC1-SANSW

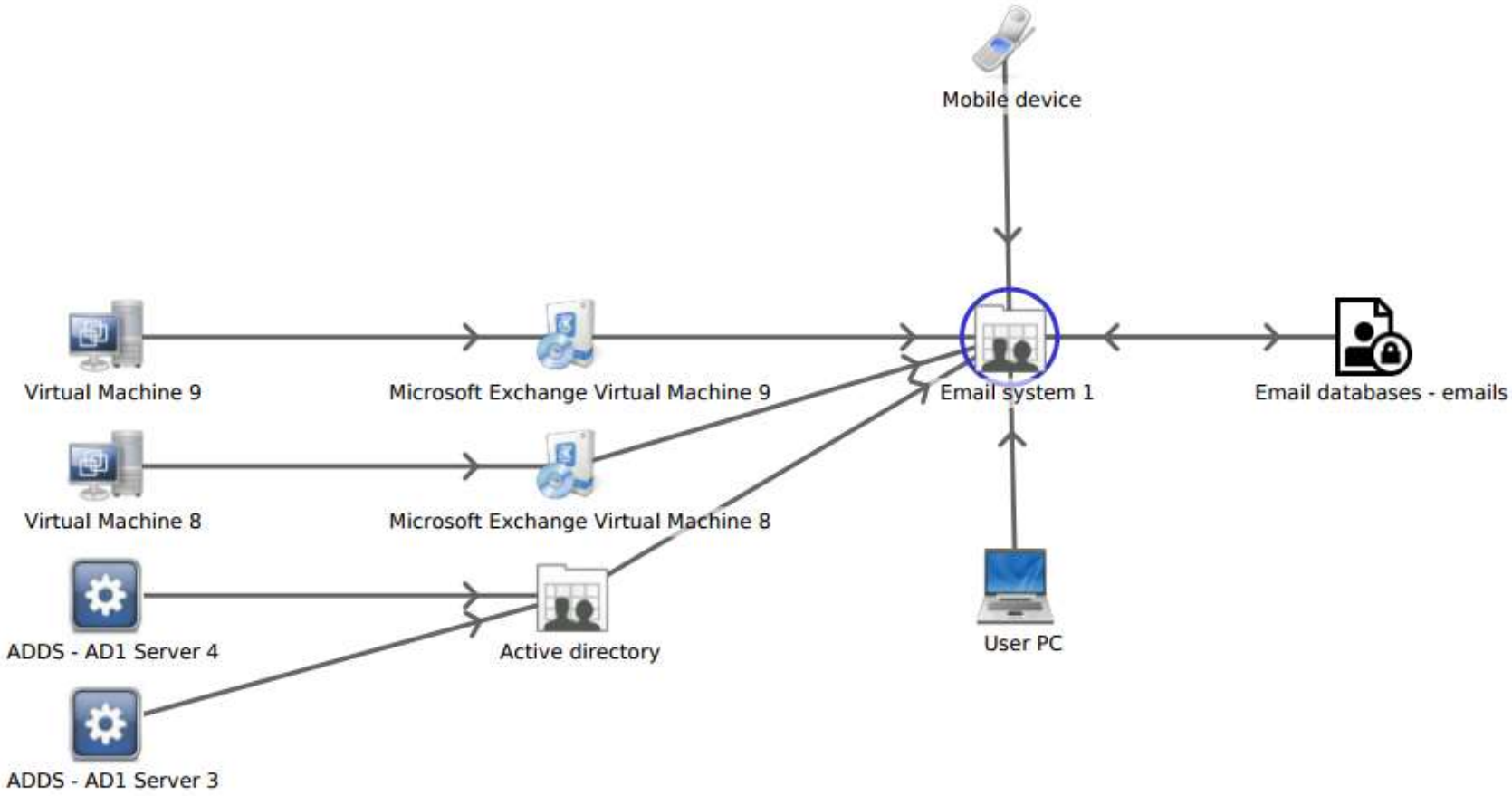
ALEF


DC2-SANSW
0/1
TC2-Data Storage
0/1
TC2-Data Storage TC2 - Virtual DS
DC2-GW
DC2-Hypervisor-01-04
DC2Hypervisors1-4
0/2
DC-VSS
DC1-Hypervisor-01-07
DC1Hypervisors1-7
TC1-Data Storage TC1 - Virtual DS
0/1
0/1
TC1-Data Storage
DC1-SANSW
Virtualization Farm
Virtual Machine 16
Postfix - MTA Virtual Machine 16
Virtual Machine 15
Postfix - MTA Virtual Machine 15
SMTP - MTA
Virtual Machine 9
Microsoft Exchange Virtual Machine 9
Email system 1
Email databases - emails
Virtual Machine 8
Microsoft Exchange Virtual Machine 8

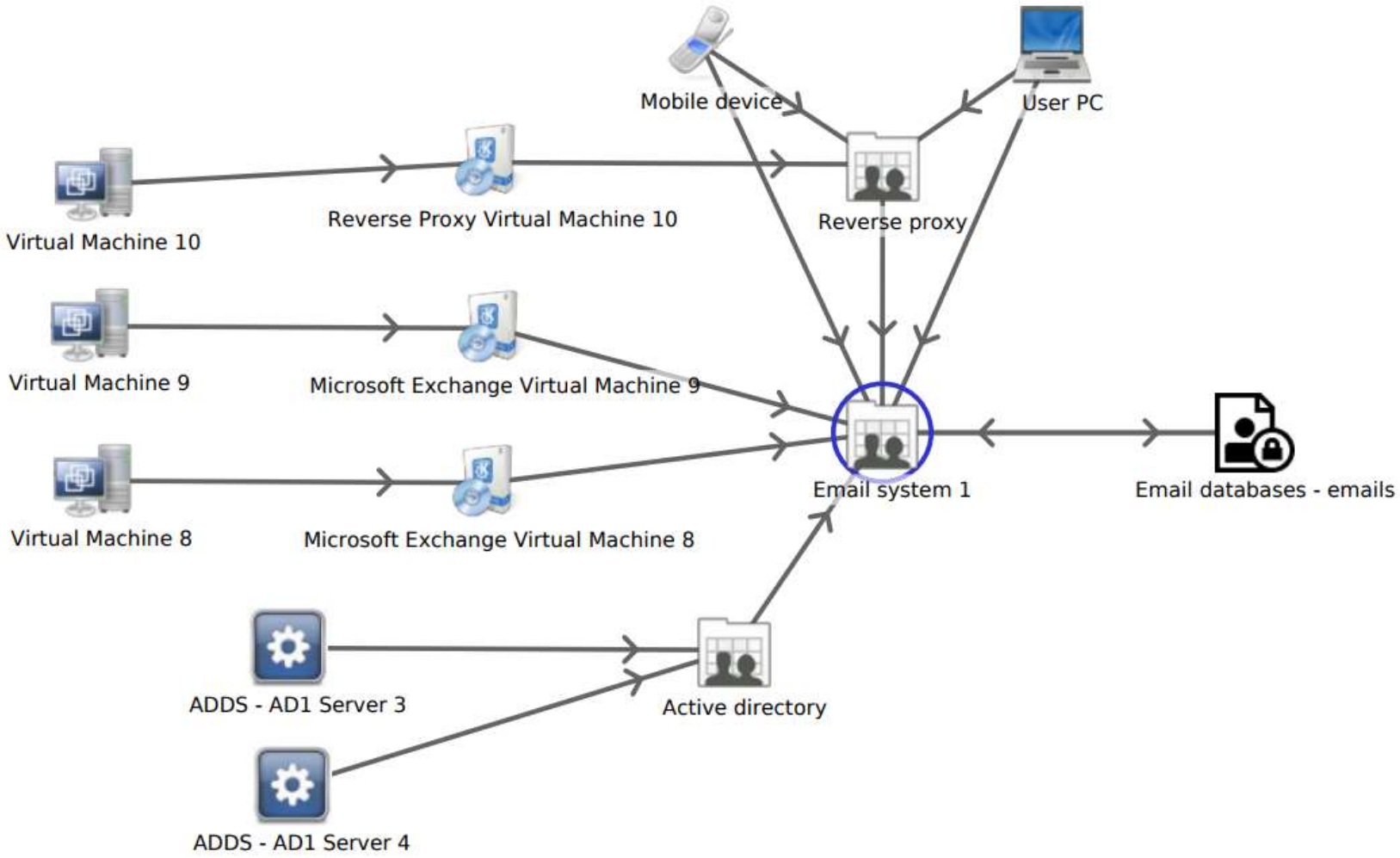
ALEF


DC2-SANSW
0/1
TC2-Data Storage
0/1
TC2-Data Storage TC2 - Virtual DS
DC2-GW
DC2-Hypervisor-01-04
DC2Hypervisors1-4
0/2
DC-VSS
DC1-Hypervisor-01-07
DC1Hypervisors1-7
TC1-Data Storage TC1 - Virtual DS
0/1
TC1-Data Storage
0/1
DC1-SANSW
Virtualization Farm
Virtual Machine 16
Postfix - MTA Virtual Machine 16
Virtual Machine 15
Postfix - MTA Virtual Machine 15
SMTP - MTA
Virtual Machine 9
Microsoft Exchange Virtual Machine 9
Virtual Machine 8
Microsoft Exchange Virtual Machine 8
Email system 1
Email databases - emails
Server 4
ADDS - AD1 Server 4
Active directory
Server 3
ADDS - AD1 Server 3

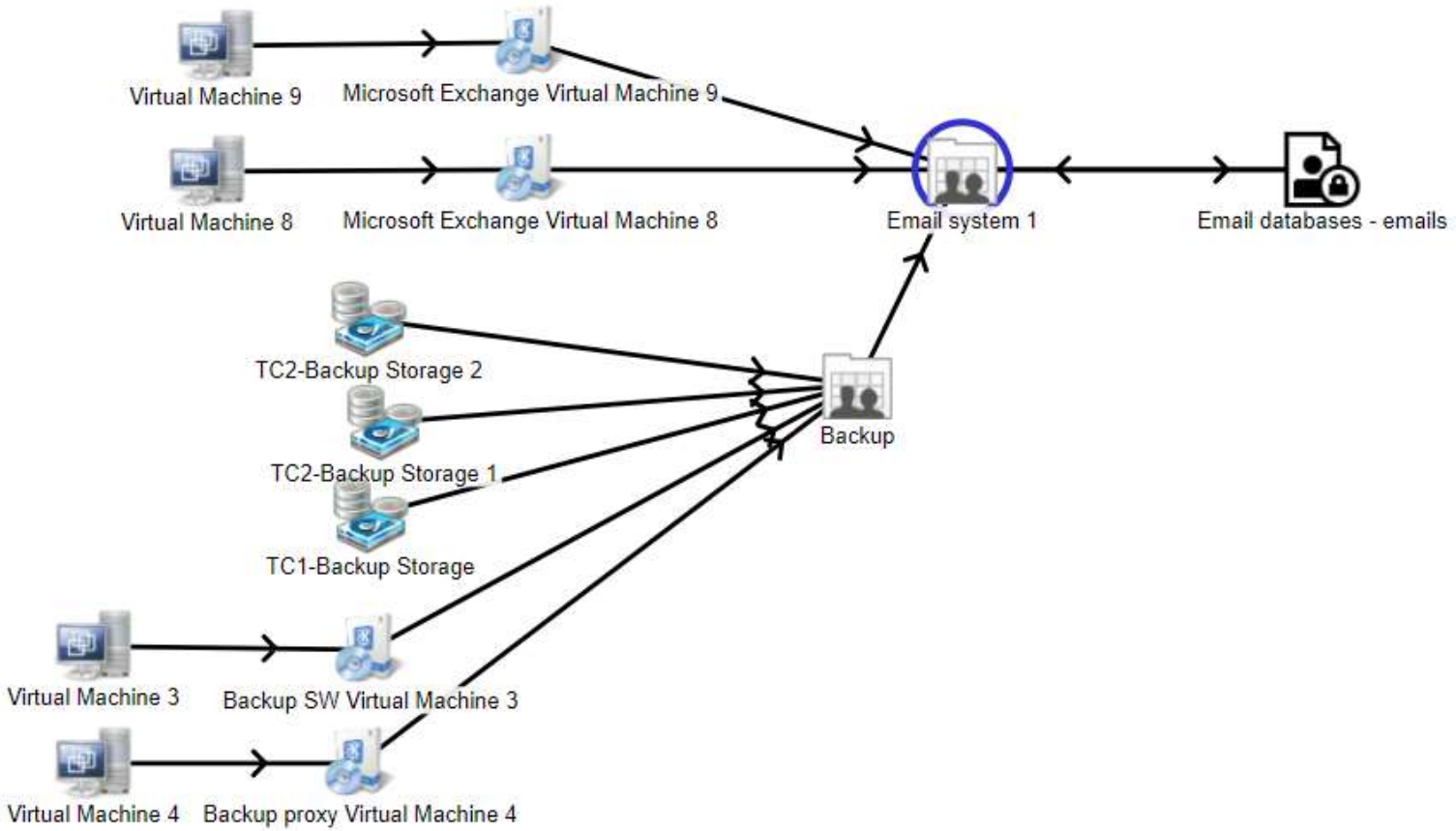
ALEF


Mobile device
Virtual Machine 9
Microsoft Exchange Virtual Machine 9
Email system 1
Email databases - emails
Virtual Machine 8
Microsoft Exchange Virtual Machine 8
ADDS - AD1 Server 4
Active directory
User PC
ADDS - AD1 Server 3

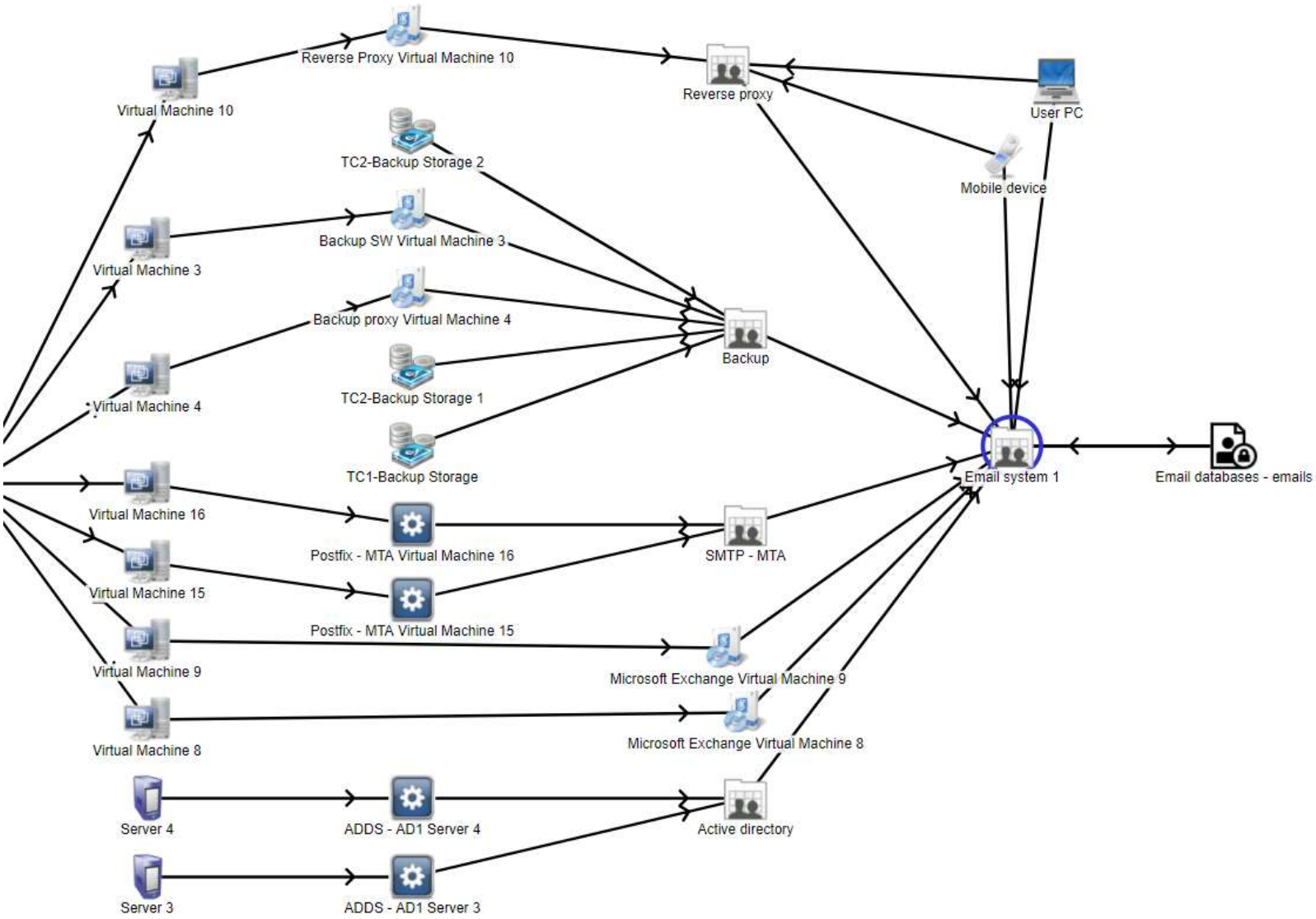
ALEF


Mobile device
User PC
Virtual Machine 10
Reverse Proxy Virtual Machine 10
Reverse proxy
Virtual Machine 9
Microsoft Exchange Virtual Machine 9
Email system 1
Email databases - emails
Virtual Machine 8
Microsoft Exchange Virtual Machine 8
ADDS - AD1 Server 3
Active directory
ADDS - AD1 Server 4

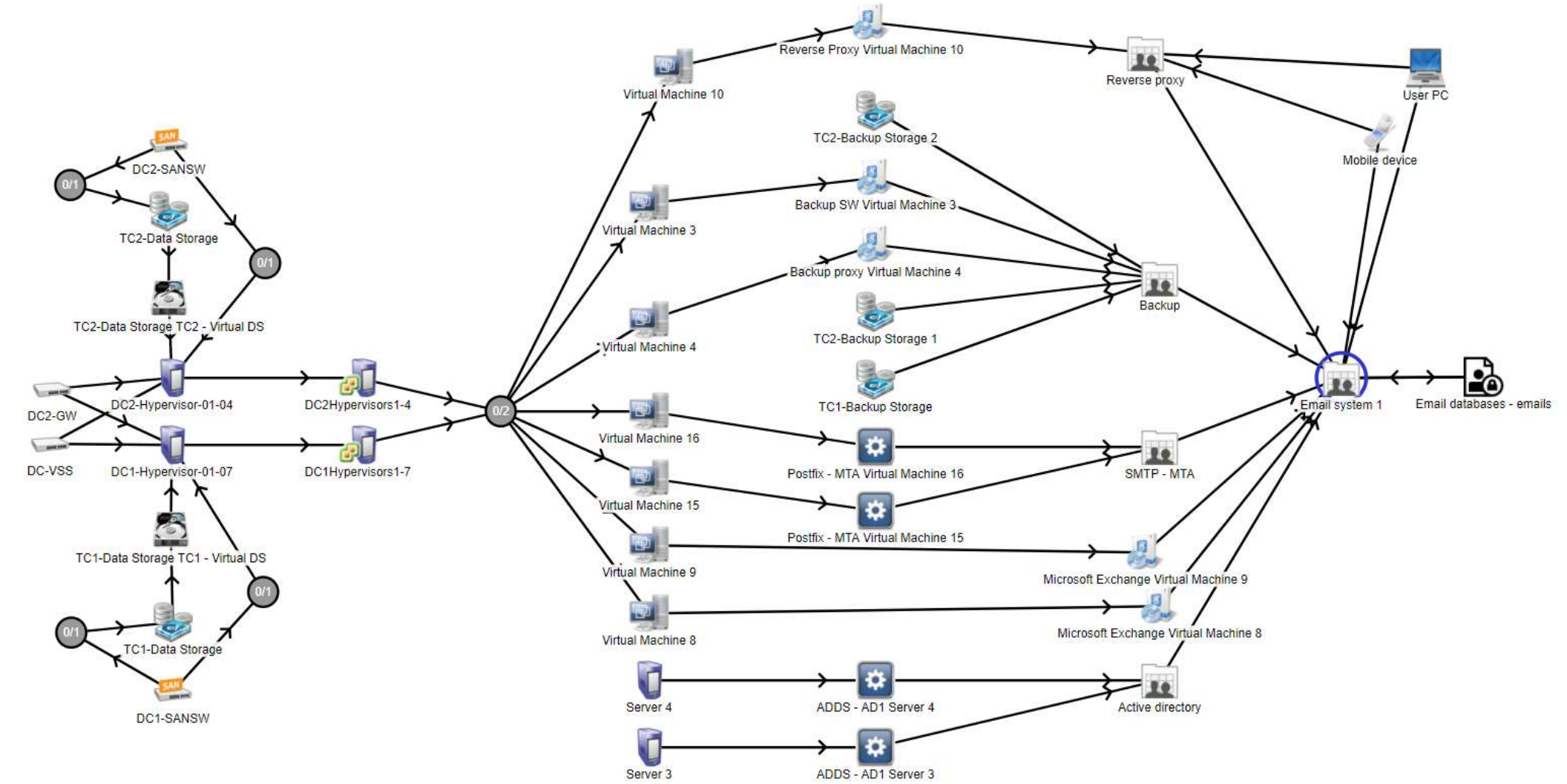
ALEF


Virtual Machine 9
Microsoft Exchange Virtual Machine 9
Virtual Machine 8
Microsoft Exchange Virtual Machine 8
Email system 1
Email databases - emails
TC2-Backup Storage 2
TC2-Backup Storage 1
TC1-Backup Storage
Backup
Virtual Machine 3
Backup SW Virtual Machine 3
Virtual Machine 4
Backup proxy Virtual Machine 4

ALEF

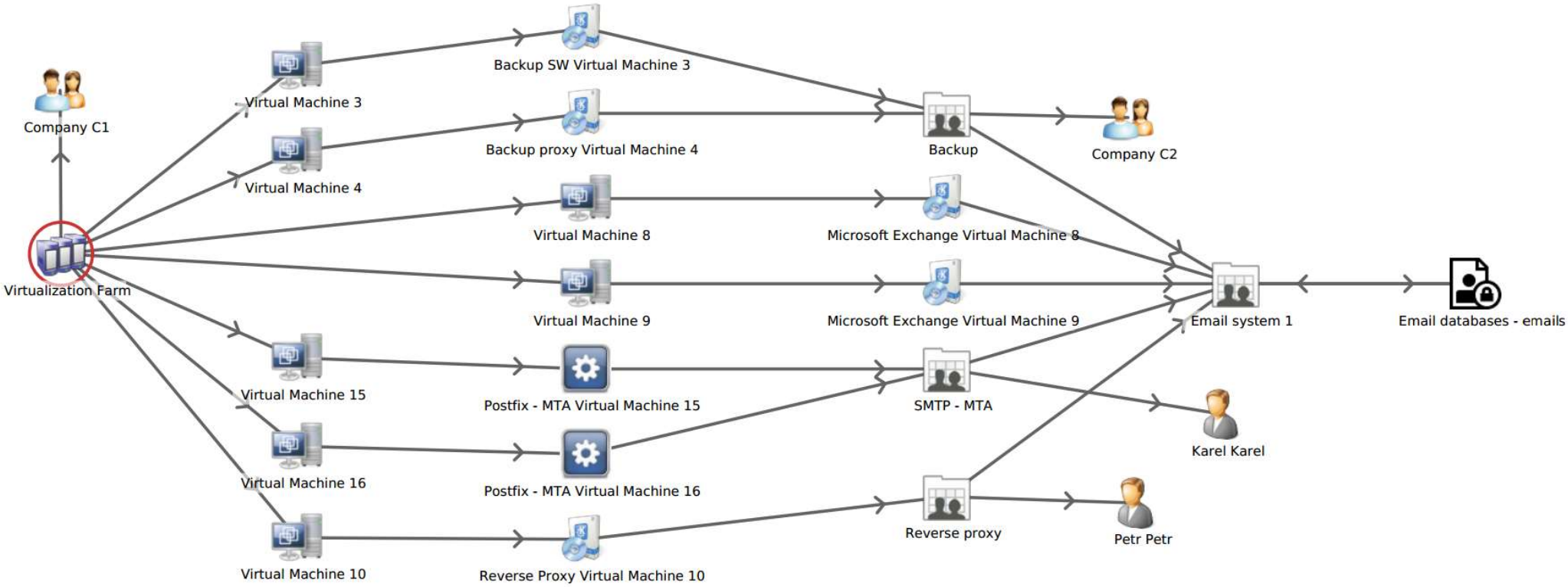

Reverse Proxy Virtual Machine 10
Virtual Machine 10
Reverse proxy
User PC
TC2-Backup Storage 2
Mobile device
Backup SW Virtual Machine 3
Virtual Machine 3
Backup proxy Virtual Machine 4
Backup
Virtual Machine 4
TC2-Backup Storage 1
TC1-Backup Storage
Email system 1
Email databases - emails
Virtual Machine 16
Postfix - MTA Virtual Machine 16
SMTP - MTA
Virtual Machine 15
Postfix - MTA Virtual Machine 15
Virtual Machine 9
Microsoft Exchange Virtual Machine 9
Virtual Machine 8
Microsoft Exchange Virtual Machine 8
Server 4
ADDS - AD1 Server 4
Active directory
Server 3
ADDS - AD1 Server 3

ALEF

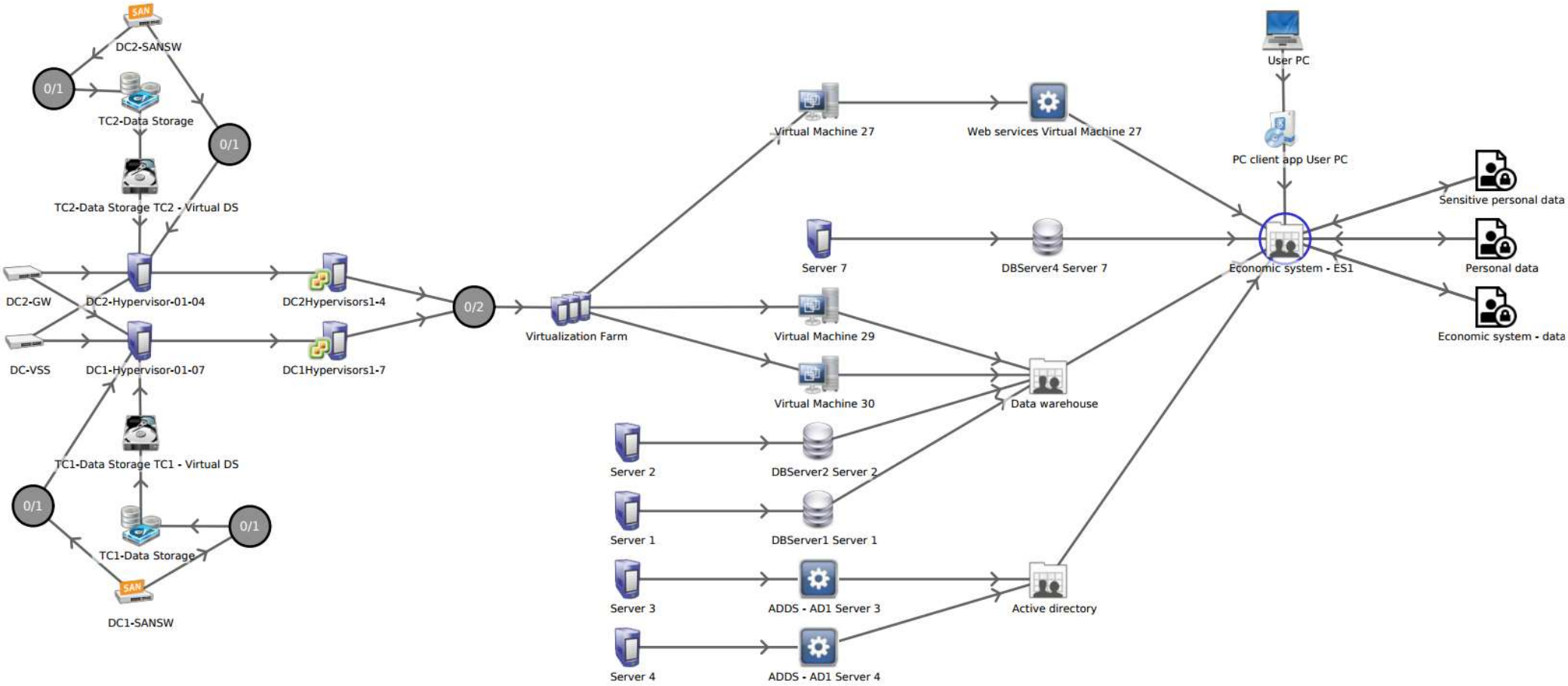

DC2-SANSW
0/1
TC2-Data Storage
0/1
TC2-Data Storage TC2 - Virtual DS
DC2-GW
DC2-Hypervisor-01-04
DC2Hypervisors1-4
DC-VSS
DC1-Hypervisor-01-07
DC1Hypervisors1-7
TC1-Data Storage TC1 - Virtual DS
0/1
0/1
TC1-Data Storage
DC1-SANSW
0/2
Virtual Machine 10
Reverse Proxy Virtual Machine 10
Virtual Machine 3
Virtual Machine 4
Virtual Machine 16
Virtual Machine 15
Virtual Machine 9
Virtual Machine 8
Server 4
Server 3
TC2-Backup Storage 2
Backup SW Virtual Machine 3
Backup proxy Virtual Machine 4
TC2-Backup Storage 1
TC1-Backup Storage
Postfix - MTA Virtual Machine 16
Postfix - MTA Virtual Machine 15
ADDS - AD1 Server 4
ADDS - AD1 Server 3
Reverse proxy
Backup
SMTP - MTA
Microsoft Exchange Virtual Machine 9
Microsoft Exchange Virtual Machine 8
Active directory
User PC
Mobile device
Email system 1
Email databases - emails

ALEF

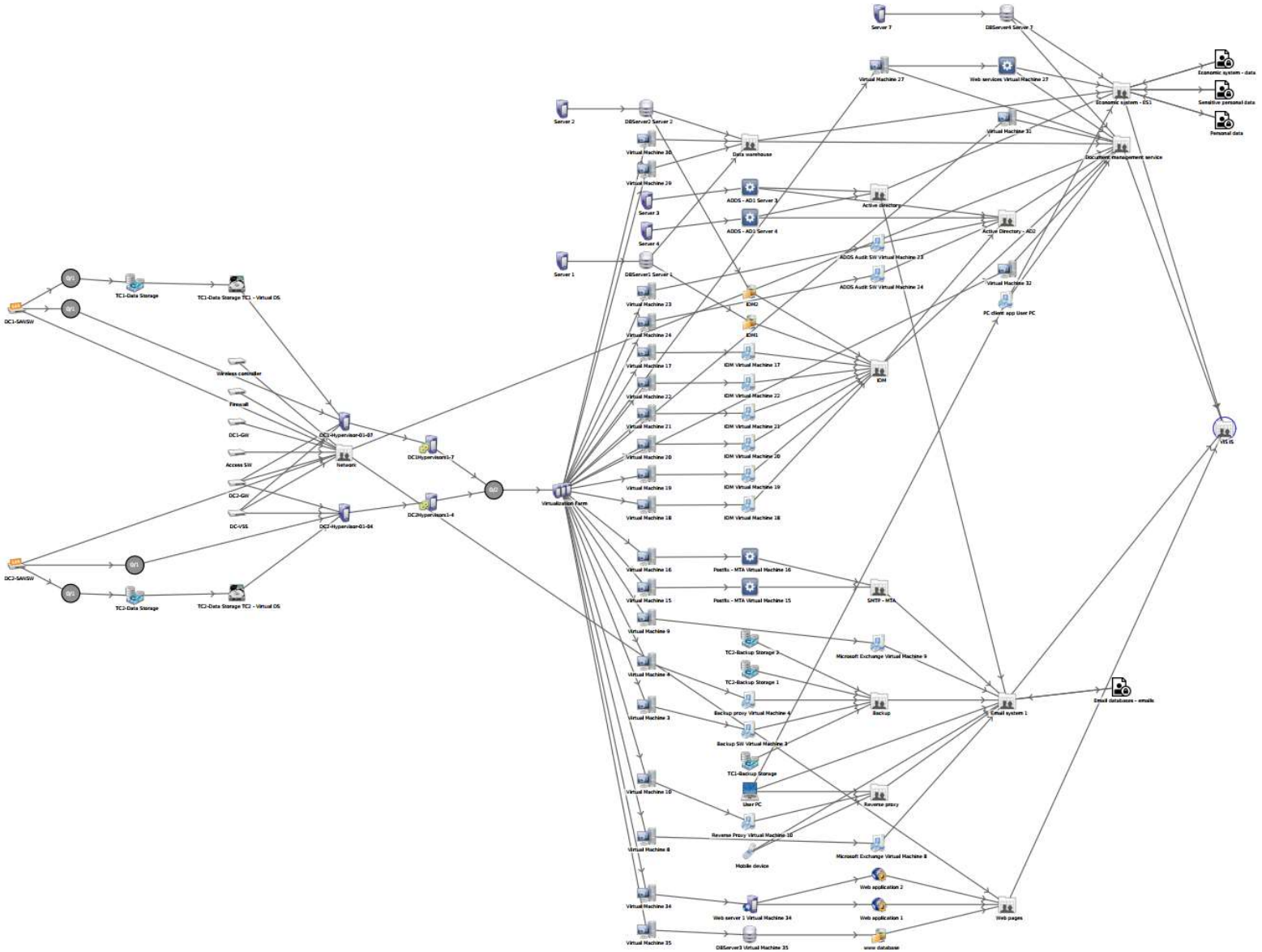
Další příklady



ALEF


DC2-SANSW
0/1
TC2-Data Storage
0/1
TC2-Data Storage TC2 - Virtual DS
DC2-GW
DC2-Hypervisor-01-04
DC2Hypervisors1-4
DC-VSS
DC1-Hypervisor-01-07
DC1Hypervisors1-7
0/2
TC1-Data Storage TC1 - Virtual DS
0/1
0/1
TC1-Data Storage
DC1-SANSW
Virtualization Farm
Virtual Machine 27
Web services Virtual Machine 27
Server 7
DBServer4 Server 7
Virtual Machine 29
Virtual Machine 30
Data warehouse
Server 2
DBServer2 Server 2
Server 1
DBServer1 Server 1
Server 3
ADDS - AD1 Server 3
Active directory
Server 4
ADDS - AD1 Server 4
User PC
PC client app User PC
Economic system - ES1
Sensitive personal data
Personal data
Economic system - data

ALEF


Server 7
DBServer4 Server 7
Economic system - data
Sensitive personal data
Personal data
Virtual Machine 27
Web services Virtual Machine 27
Economic system - ES1
Server 2
DBServer2 Server 2
Virtual Machine 31
Virtual Machine 30
Data warehouse
Document management service
Virtual Machine 29
ADDS - AD1 Server 3
Active directory
Server 3
ADDS - AD1 Server 4
Active Directory - AD2
Server 4
ADDS Audit SW Virtual Machine 23
Server 1
DBServer1 Server 1
ADDS Audit SW Virtual Machine 24
Virtual Machine 32
Virtual Machine 23
IDM2
PC client app User PC
Virtual Machine 24
IDM1
Virtual Machine 17
IDM Virtual Machine 17
IDM
Virtual Machine 22
IDM Virtual Machine 22
Virtual Machine 21
IDM Virtual Machine 21
VSS 01
Virtual Machine 20
IDM Virtual Machine 20
Virtual Machine 19
IDM Virtual Machine 19
Virtual Machine 18
IDM Virtual Machine 18
TC1-Data Storage
TC1-Data Storage TC1 - Virtual DS
DC1-SANSW
Wireless controller
Firewall
DC1-GW
Access SW
DC2-GW
DC-VSS
DC1-Hypervisor-01-07
Network
DC1Hypervisors1-7
DC2Hypervisors1-4
DC2-Hypervisor-01-04
Virtualization Farm
Virtual Machine 16
Postfix - MTA Virtual Machine 16
Virtual Machine 15
Postfix - MTA Virtual Machine 15
SMTP - MTA
Virtual Machine 9
TC2-Backup Storage 3
Microsoft Exchange Virtual Machine 9
Virtual Machine 4
TC2-Backup Storage 1
Email system 1
Email databases - emails
Virtual Machine 3
Backup proxy Virtual Machine 4
Backup
Backup SW Virtual Machine 3
TC1-Backup Storage
Virtual Machine 10
User PC
Reverse proxy
Reverse Proxy Virtual Machine 10
Virtual Machine 8
Microsoft Exchange Virtual Machine 8
Mobile device
Web application 2
Virtual Machine 34
Web server 1 Virtual Machine 34
Web application 1
Web pages
Virtual Machine 35
DBServer3 Virtual Machine 35
www database
TC2-Data Storage
TC2-Data Storage TC2 - Virtual DS
DC2-SANSW

ALEF

- Pro implementaci vhodných organizačních a technických opatření je nutné znát skutečný rozsah a vazby odvozených podpůrných aktiv v ISMS, tak aby opatření byla efektivní

ALEF

Využití

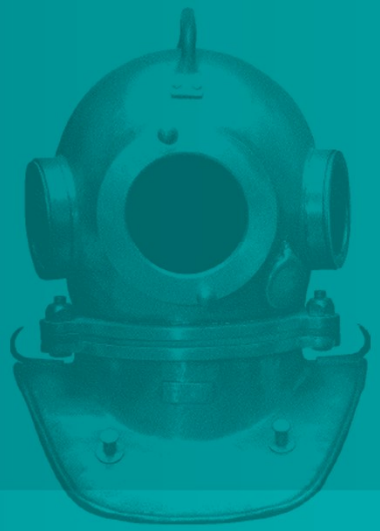
Modely jsou vhodné pro:

- Návrh ISMS
- Implementace ISMS
- Provoz ISMS
- Audit ISMS

ALEF

Kontakt

ALEF



Děkuji za pozornost

ALEF