Experis
ManpowerGroup

dON’T PANIC!!!11

Disaster Recovery for AD

Agenda

About me

1 Part I – High Level

- The bigger picture
- What are the most common shortcomings?
- Challenges during the disaster
- Q&A

2 Part II – Low Level

- What is an AD disaster?
- How to back up AD?
- AD Forest recovery plan
- Suggested design for test environment for AD restore
- Lessons learned
- Q&A

About me

Rostyslav Yevdiukhin, aka Ross

- Have worked in HP (and by proxy in P&G), EDB/EVRY, IBM, Visma and now started consultant life in Experis. Have been working in IT for 20 years, last 12 with Identity. Core areas – AD/IAM, Infrastructure, ZTNA, PAM and especially the defense aspect of the above. Think attack, do defense.
- Originally from Ukraine, moved to Norway in 2011 with my family – have wife and 2 kids, who are now 15 and 19.
- Work is my major hobby, but I don't mind travelling and doing various activities, from windsurfing to mushroom picking. Since the full scale invasion of Ukraine, joined a group organizing and leading the protests requesting more support to Ukraine. You can often meet me near Stortinget at 17:00 on workdays, 12:00 on weekends.
- https://www.linkedin.com/in/ross-ua/

1. High Level

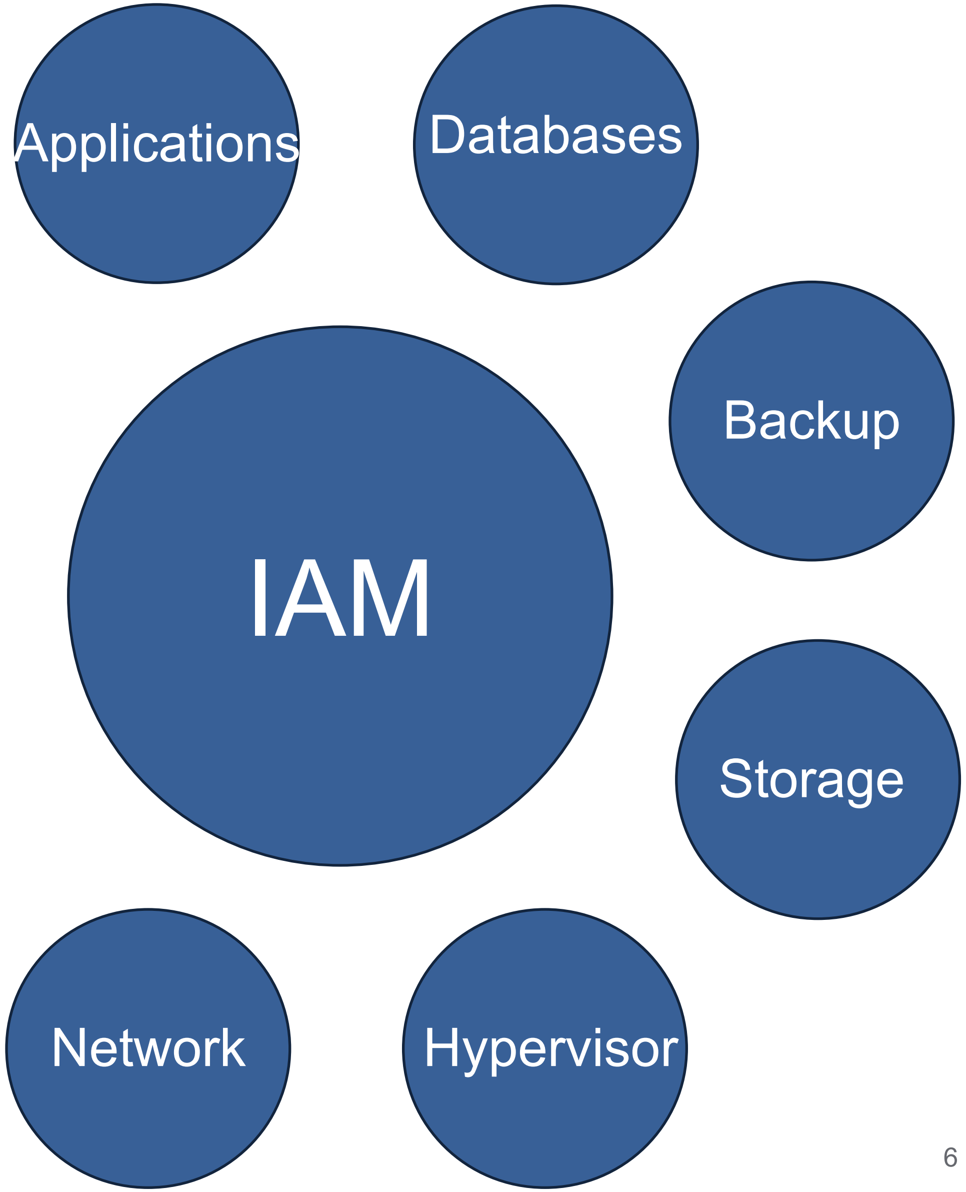
Part I – High Level. The bigger picture.

- When you work in Identity, you will clearly see that Identity is in the middle of everything.

IAM

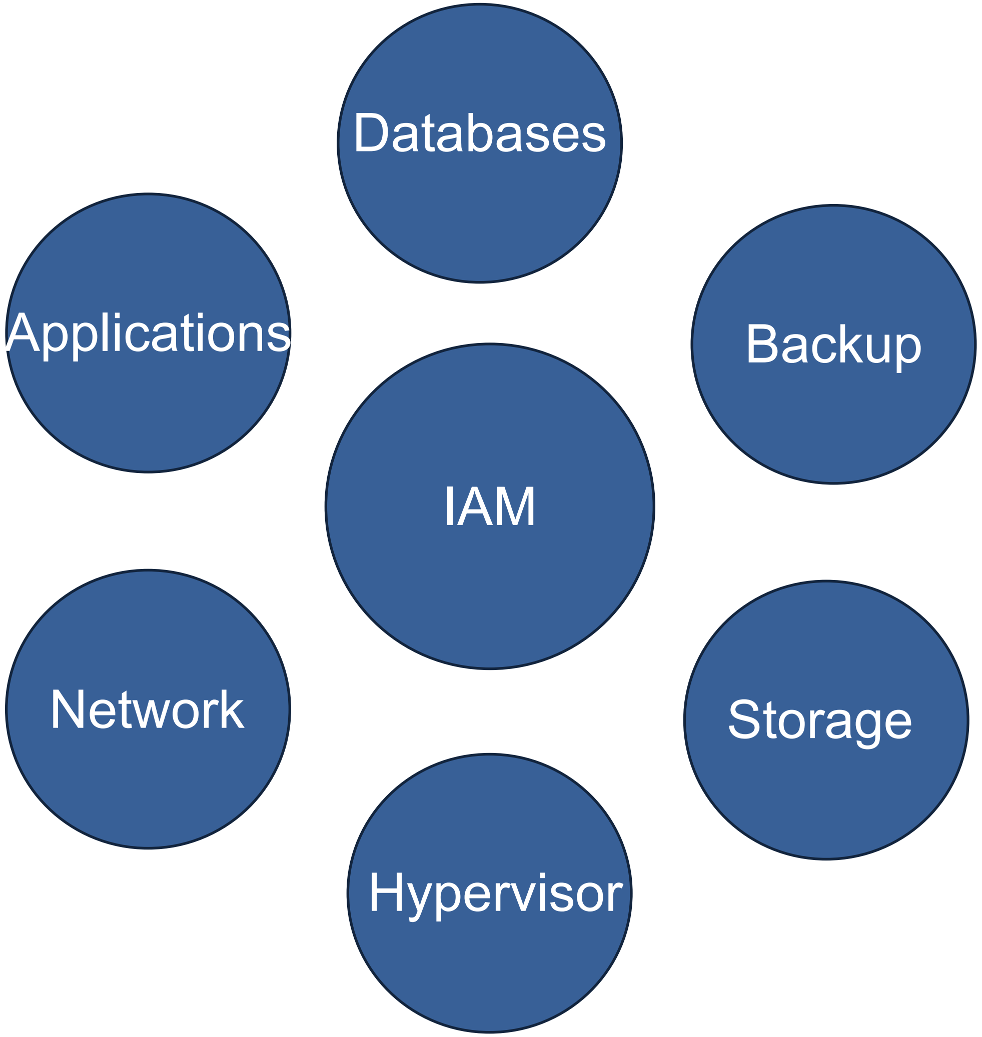
Part I – High Level. The bigger picture.

- When you work in Identity, you will clearly see that Identity is in the middle of everything.
- All other areas are dependent on proper functioning of IAM



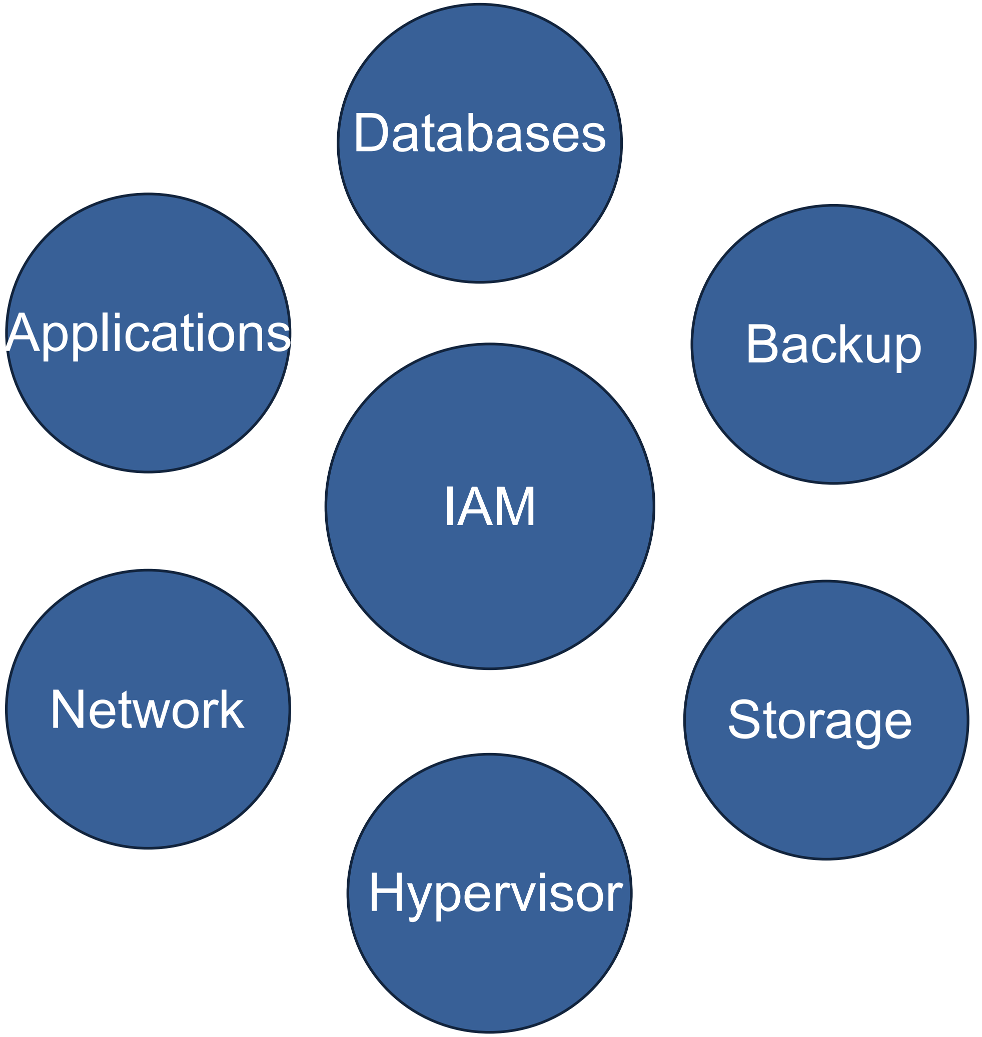
Part I – High Level. The bigger picture.

- When you work in Identity, you will clearly see that Identity is in the middle of everything.
- All other areas are dependent on proper functioning of IAM
- Just like IAM is dependent on every other core infrastructure area



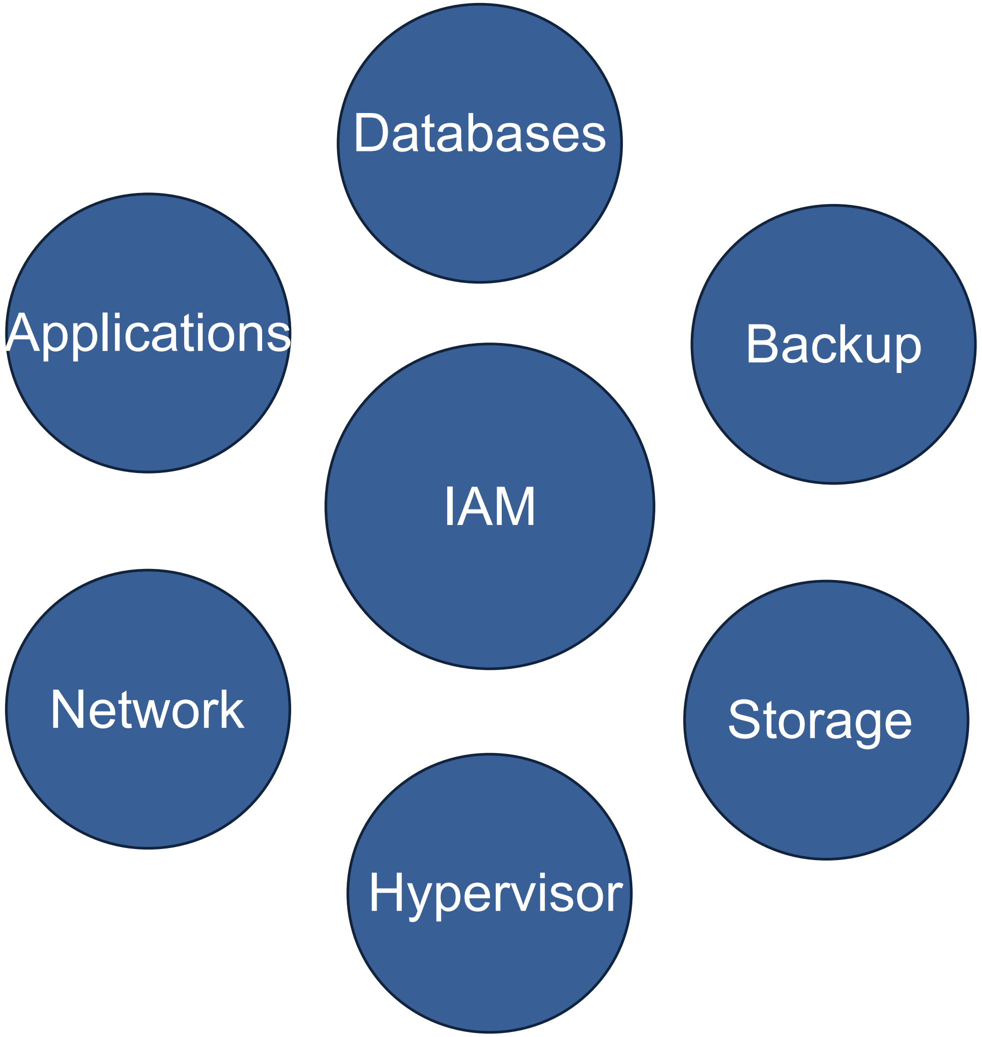
Part I – High Level. The bigger picture.

- When you work in Identity, you will clearly see that Identity is in the middle of everything.
- All other areas are dependent on proper functioning of IAM
- Just like IAM is dependent on every other core infrastructure area
- Which becomes evident like never before when disaster happens on one of the services



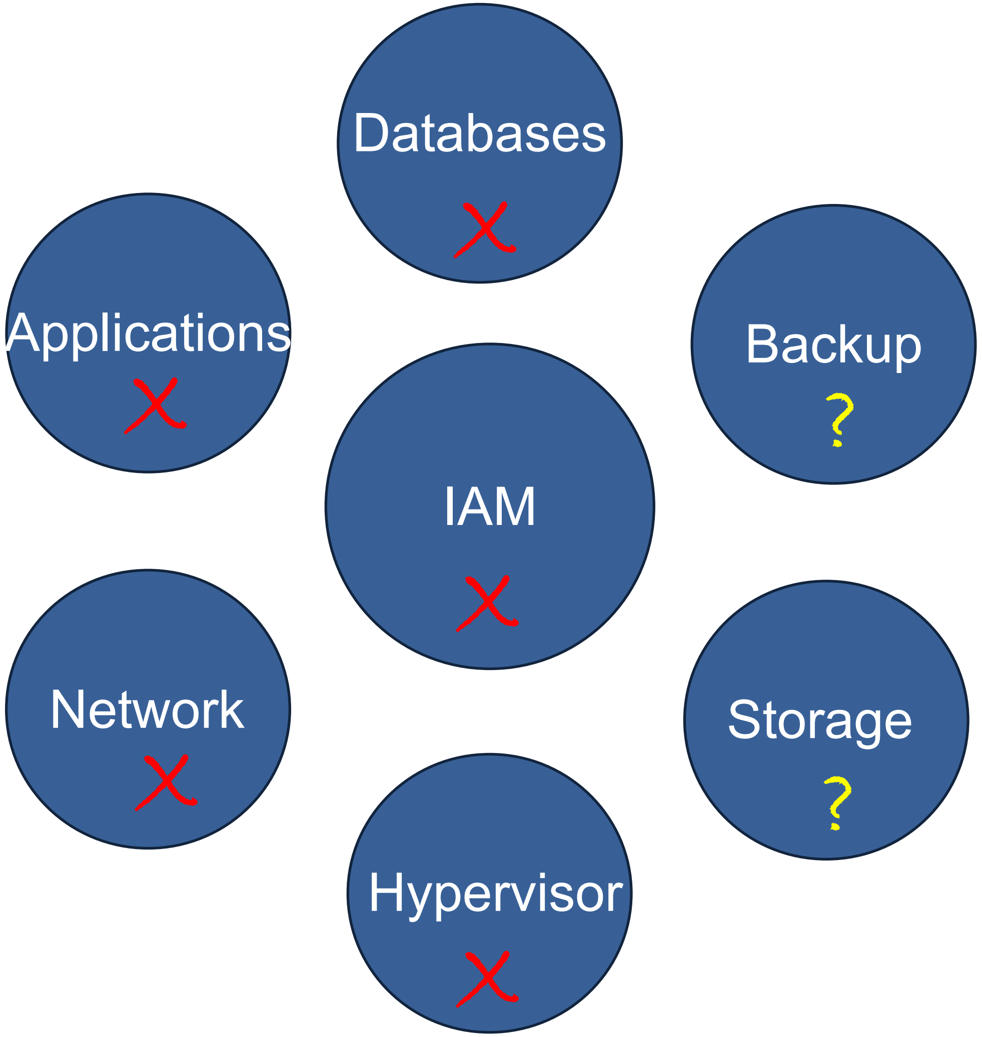
Part I – High Level. The bigger picture.

- When you work in Identity, you will clearly see that Identity is in the middle of everything.
- All other areas are dependent on proper functioning of IAM
- Just like IAM is dependent on every other core infrastructure area
- Which becomes evident like never before when disaster happens on one of the services
- Every area normally has a DR plan to recover, so what's missing?



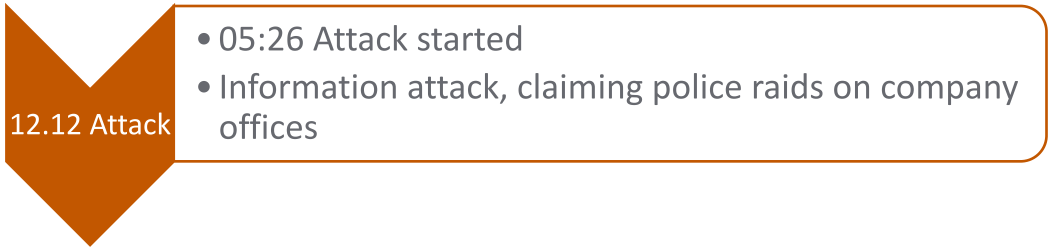
Part I – High Level. Most common shortcomings.

- When problem start happening on more than 1 service, DR plans stop working
- DR plans are almost always assuming that all other parts are working
- When multiple areas are in disaster situation, the order of restore is not clear
- To restore any area, credentials are vital element. When IdP is not available, most DR plans will stop working



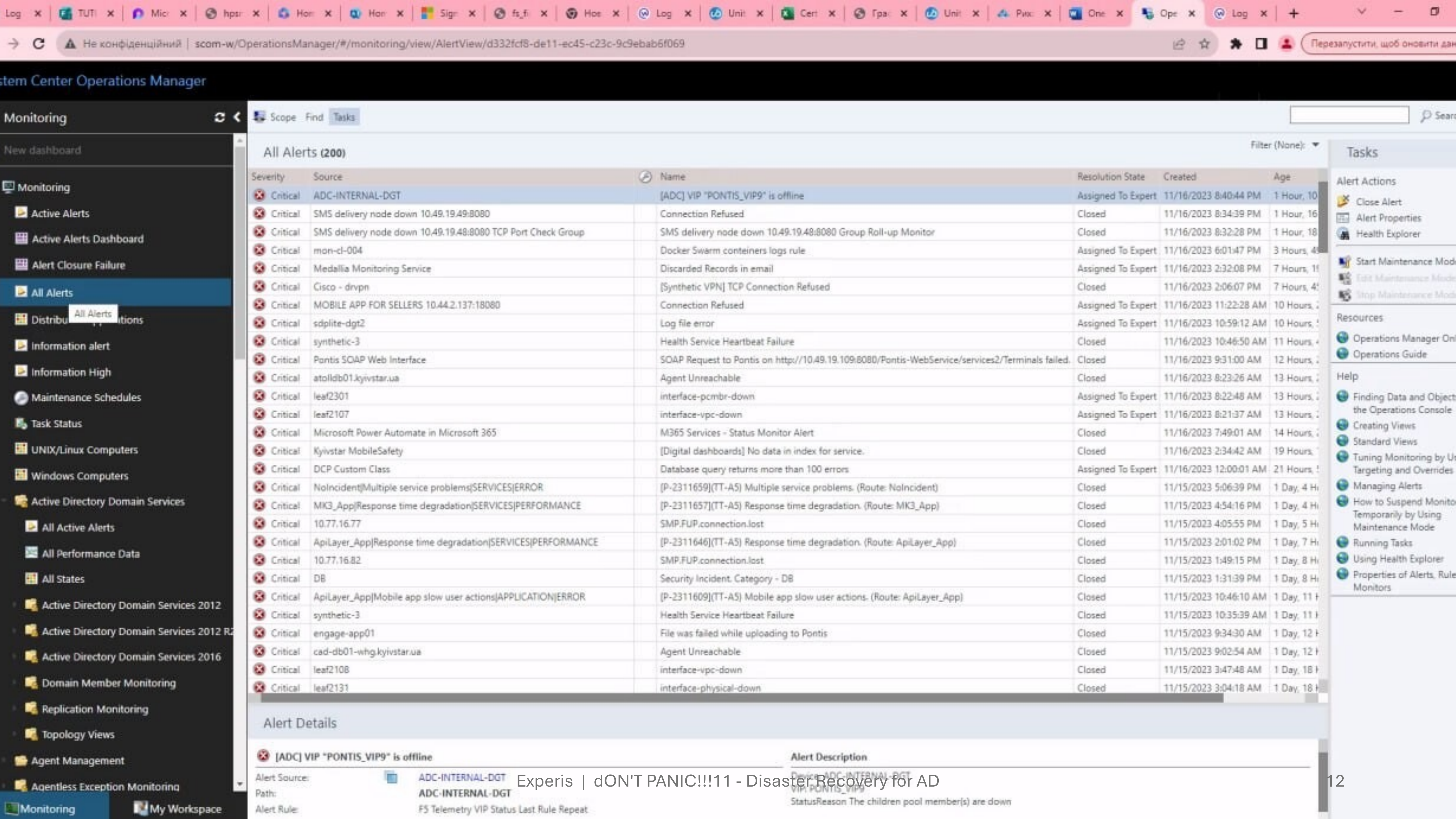
Bonus: Large attack on Telecom company - Kyivstar

- 24M subscribers
- Core infrastructure damaged, including backups.
- Mobile network down, base stations damaged. Subscriber equipment damaged.
- Air raid alarms not working
- POS terminals and ATMs not working
- In some cities, street lighting had to be turned off manually



12.12 Attack

- 05:26 Attack started
- Information attack, claiming police raids on company offices



All Alerts (200)

Severity	Source	Name	Resolution State	Created	Age
Critical	ADC-INTERNAL-DGT	[ADC] VIP "PONTIS_VIP9" is offline	Assigned To Expert	11/16/2023 8:40:44 PM	1 Hour, 10
Critical	SMS delivery node down 10.49.19.49:8080	Connection Refused	Closed	11/16/2023 8:34:39 PM	1 Hour, 16
Critical	SMS delivery node down 10.49.19.48:8080 TCP Port Check Group	SMS delivery node down 10.49.19.48:8080 Group Roll-up Monitor	Closed	11/16/2023 8:32:28 PM	1 Hour, 18
Critical	mon-cl-004	Docker Swarm conteiners logs rule	Assigned To Expert	11/16/2023 6:01:47 PM	3 Hours, 4
Critical	Medallia Monitoring Service	Discarded Records in email	Assigned To Expert	11/16/2023 2:32:08 PM	7 Hours, 1
Critical	Cisco - drvpn	[Synthetic VPN] TCP Connection Refused	Closed	11/16/2023 2:06:07 PM	7 Hours, 4
Critical	MOBILE APP FOR SELLERS 10.44.2.137:18080	Connection Refused	Assigned To Expert	11/16/2023 11:22:28 AM	10 Hours,
Critical	sdplite-dgt2	Log file error	Assigned To Expert	11/16/2023 10:59:12 AM	10 Hours,
Critical	synthetic-3	Health Service Heartbeat Failure	Closed	11/16/2023 10:46:50 AM	11 Hours,
Critical	Pontis SOAP Web Interface	SOAP Request to Pontis on http://10.49.19.109:8080/Pontis-WebService/services2/Terminals failed.	Closed	11/16/2023 9:31:00 AM	12 Hours,
Critical	atolldb01.kyivstar.ua	Agent Unreachable	Closed	11/16/2023 8:23:26 AM	13 Hours,
Critical	leaf2301	interface-pcmbr-down	Assigned To Expert	11/16/2023 8:22:48 AM	13 Hours,
Critical	leaf2107	interface-vpc-down	Assigned To Expert	11/16/2023 8:21:37 AM	13 Hours,
Critical	Microsoft Power Automate in Microsoft 365	M365 Services - Status Monitor Alert	Closed	11/16/2023 7:49:01 AM	14 Hours,
Critical	Kyivstar MobileSafety	[Digital dashboards] No data in index for service.	Closed	11/16/2023 2:34:42 AM	19 Hours,
Critical	DCP Custom Class	Database query returns more than 100 errors	Assigned To Expert	11/16/2023 12:00:01 AM	21 Hours,
Critical	NoIncident|Multiple service problems|SERVICES|ERROR	[P-2311659](TT-A5) Multiple service problems. (Route: NoIncident)	Closed	11/15/2023 5:06:39 PM	1 Day, 4 H
Critical	MK3_App|Response time degradation|SERVICES|PERFORMANCE	[P-2311657](TT-A5) Response time degradation. (Route: MK3_App)	Closed	11/15/2023 4:54:16 PM	1 Day, 4 H
Critical	10.77.16.77	SMP.FUP.connection.lost	Closed	11/15/2023 4:05:55 PM	1 Day, 5 H
Critical	ApiLayer_App|Response time degradation|SERVICES|PERFORMANCE	[P-2311646](TT-A5) Response time degradation. (Route: ApiLayer_App)	Closed	11/15/2023 2:01:02 PM	1 Day, 7 H
Critical	10.77.16.82	SMP.FUP.connection.lost	Closed	11/15/2023 1:49:15 PM	1 Day, 8 H
Critical	DB	Security Incident. Category - DB	Closed	11/15/2023 1:31:39 PM	1 Day, 8 H
Critical	ApiLayer_App|Mobile app slow user actions|APPLICATION|ERROR	[P-2311609](TT-A5) Mobile app slow user actions. (Route: ApiLayer_App)	Closed	11/15/2023 10:46:10 AM	1 Day, 11 H
Critical	synthetic-3	Health Service Heartbeat Failure	Closed	11/15/2023 10:35:39 AM	1 Day, 11 H
Critical	engage-app01	File was failed while uploading to Pontis	Closed	11/15/2023 9:34:30 AM	1 Day, 12 H
Critical	cad-db01-whg.kyivstar.ua	Agent Unreachable	Closed	11/15/2023 9:02:54 AM	1 Day, 12 H
Critical	leaf2108	interface-vpc-down	Closed	11/15/2023 3:47:48 AM	1 Day, 18 H
Critical	leaf2131	interface-physical-down	Closed	11/15/2023 3:04:18 AM	1 Day, 18 H

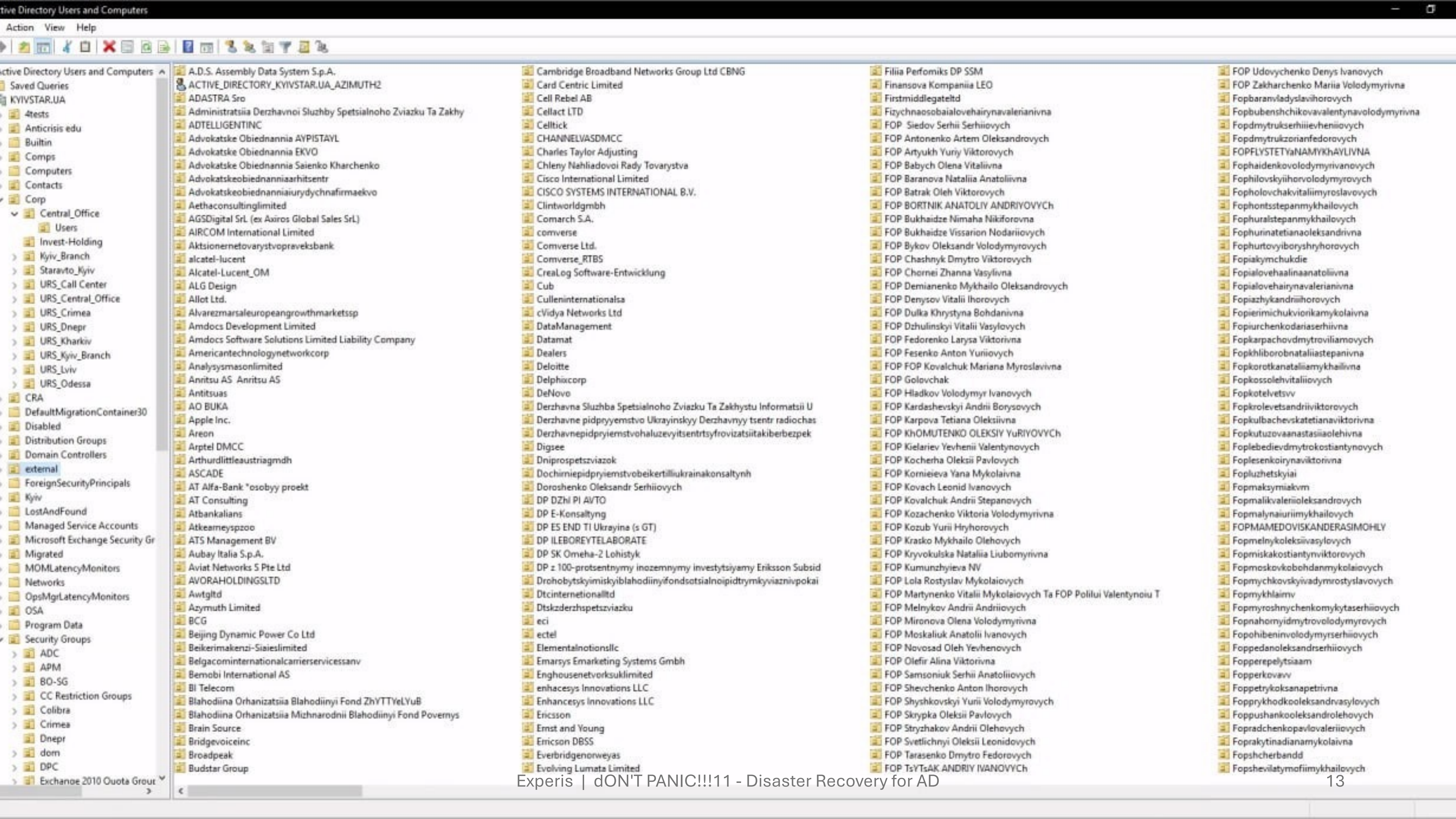
Alert Details

[ADC] VIP "PONTIS_VIP9" is offline

Alert Source: ADC-INTERNAL-DGT
Path: ADC-INTERNAL-DGT
Alert Rule: F5 Telemetry VIP Status Last Rule Repeat

Alert Description

Device ADC-INTERNAL-DGT
VIP PONTIS_VIP9
StatusReason The children pool member(s) are down



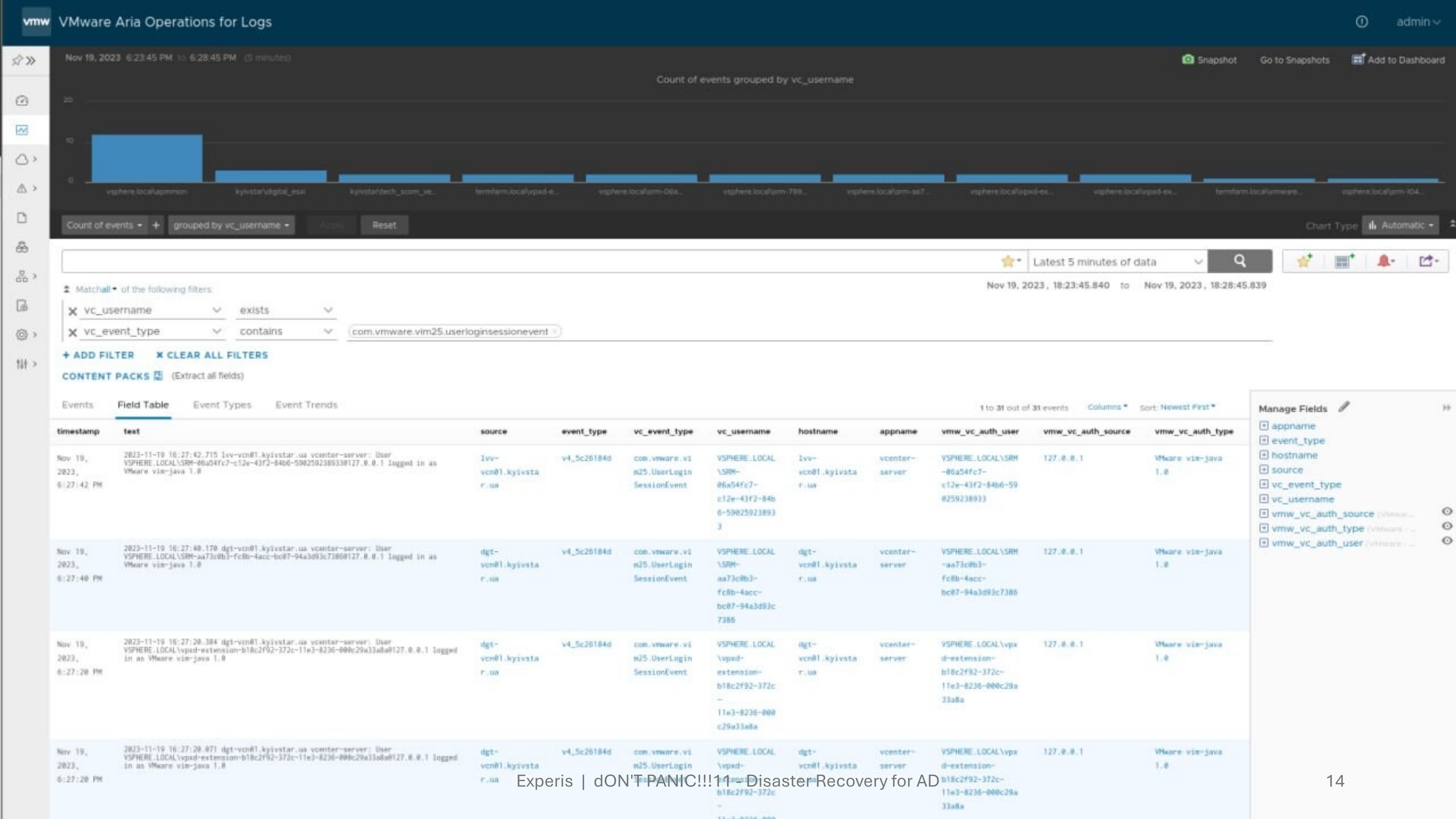
ctive Directory Users and Computers
Saved Queries
KYIVSTAR.UA
4tests
Anticrisis edu
Builtin
Comps
Computers
Contacts
Corp
Central_Office
Users
Invest-Holding
Kyiv_Branch
Staravto_Kyiv
URS_Call Center
URS_Central_Office
URS_Crimea
URS_Dnepr
URS_Kharkiv
URS_Kyiv_Branch
URS_Lviv
URS_Odessa
CRA
DefaultMigrationContainer30
Disabled
Distribution Groups
Domain Controllers
external
ForeignSecurityPrincipals
Kyiv
LostAndFound
Managed Service Accounts
Microsoft Exchange Security Gr
Migrated
MOMLatencyMonitors
Networks
OpsMgrLatencyMonitors
OSA
Program Data
Security Groups
ADC
APM
BO-SG
CC Restriction Groups
Colibra
Crimea
Dnepr
dom
DPC
Exchange 2010 Quota Grour

A.D.S. Assembly Data System S.p.A.
ACTIVE_DIRECTORY_KYIVSTAR.UA_AZIMUTH2
ADASTRA Sro
Administratsiia Derzhavnoi Sluzhby Spetsialnoho Zviazku Ta Zakhy
ADTELLIGENTINC
Advokatske Obiednannia AYPISTAYL
Advokatske Obiednannia EKVO
Advokatske Obiednannia Saienko Kharchenko
Advokatskeobiednanniaarhitsentr
Advokatskeobiednanniaiurydychnafirmaekvo
Aethaconsultinglimited
AGSDigital SrL (ex Axiros Global Sales SrL)
AIRCOM International Limited
Aktsionernetovarystvopraveksbank
alcatel-lucent
Alcatel-Lucent_OM
ALG Design
Allot Ltd.
Alvarezmarsaleuropeangrowthmarketssp
Amdocs Development Limited
Amdocs Software Solutions Limited Liability Company
Americantechnologynetworkcorp
Analysysmasonlimited
Anritsu AS Anritsu AS
Antitsuas
AO BUKA
Apple Inc.
Areon
Arptel DMCC
Arthurdlittleaustriagmdh
ASCADE
AT Alfa-Bank "osobyy proekt
AT Consulting
Atbankalians
Atkearneyspzoo
ATS Management BV
Aubay Italia S.p.A.
Aviat Networks S Pte Ltd
AVORAHOLDINGSLTD
Awtgltd
Azymuth Limited
BCG
Beijing Dynamic Power Co Ltd
Beikerimakenzi-Siaieslimited
Belgacominternationalcarrierservicessanv
Bemobi International AS
BI Telecom
Blahodiina Orhanizatsiia Blahodiinyi Fond ZhYTTYeLYuB
Blahodiina Orhanizatsiia Mizhnarodnii Blahodiinyi Fond Povernys
Brain Source
Bridgevoiceinc
Broadpeak
Budstar Group

Cambridge Broadband Networks Group Ltd CBNG
Card Centric Limited
Cell Rebel AB
Cellact LTD
Celltick
CHANNELVASDMCC
Charles Taylor Adjusting
Chleny Nahliadovoi Rady Tovarystva
Cisco International Limited
CISCO SYSTEMS INTERNATIONAL B.V.
Clintworldgmbh
Comarch S.A.
comverse
Comverse Ltd.
Comverse_RTBS
CreaLog Software-Entwicklung
Cub
Culleninternationalsa
cVidya Networks Ltd
DataManagement
Datamat
Dealers
Deloitte
Delphixcorp
DeNovo
Derzhavna Sluzhba Spetsialnoho Zviazku Ta Zakhystu Informatsii U
Derzhavne pidpryyemstvo Ukrayinskyy Derzhavnyy tsentr radiochas
Derzhavnepidpryiemstvohaluzevyitsentrtsyfrovizatsiitakiberbezpek
Digsee
Dniprospetszviazok
Dochirniepidpryiemstvobeikertilliukrainakonsaltynh
Doroshenko Oleksandr Serhiiovych
DP DZhI PI AVTO
DP E-Konsaltyng
DP ES END TI Ukrayina (s GT)
DP ILEBOREYTELABORATE
DP SK Omeha-2 Lohistyk
DP z 100-protsentnymy inozemnymy investytsiyamy Eriksson Subsid
Drohobytskyimiskyiblahodiinyifondsotsialnoipidtrymkyviaznivpokai
Dtcinternationalltd
Dtskzderzhspetszviazku
eci
ectel
Elementalnotionsllc
Emarsys Emarketing Systems Gmbh
Enghousenetvorksuklimited
enhacesys Innovations LLC
Enhancesys Innovations LLC
Ericsson
Ernst and Young
Ericson DBSS
Everbridgenorweyas
Evolving Lumata Limited

Filiia Perfomiks DP SSM
Finansova Kompaniia LEO
Firstmiddlegateltd
Fizychnaosobaialovehairynavalerianivna
FOP Siedov Serhii Serhiiovych
FOP Antonenko Artem Oleksandrovych
FOP Artyukh Yuriy Viktorovych
FOP Babych Olena Vitaliivna
FOP Baranova Nataliia Anatoliivna
FOP Batrak Oleh Viktorovych
FOP BORTNIK ANATOLIY ANDRIYOVYCh
FOP Bukhaidze Nimaha Nikiforovna
FOP Bukhaidze Vissarion Nodariiovych
FOP Bykov Oleksandr Volodymyrovych
FOP Chashnyk Dmytro Viktorovych
FOP Chornei Zhanna Vasylivna
FOP Demianenko Mykhailo Oleksandrovych
FOP Denysov Vitalii Ihorovych
FOP Dulka Khrystyna Bohdanivna
FOP Dzhulinskyi Vitalii Vasylovych
FOP Fedorenko Larysa Viktorivna
FOP Fesenko Anton Yuriiovych
FOP FOP Kovalchuk Mariana Myroslavivna
FOP Golovchak
FOP Hladkov Volodymyr Ivanovych
FOP Kardashevskyi Andrii Borysovych
FOP Karpova Tetiana Oleksiivna
FOP KhOMUTENKO OLEKSIY YuRIYOVYCh
FOP Kielariev Yevhenii Valentynovych
FOP Kocherha Oleksii Pavlovych
FOP Kornieieva Yana Mykolaivna
FOP Kovach Leonid Ivanovych
FOP Kovalchuk Andrii Stepanovych
FOP Kozachenko Viktoria Volodymyrivna
FOP Kozub Yurii Hryhorovych
FOP Krasko Mykhailo Olehovych
FOP Kryvokulska Nataliia Liubomyrivna
FOP Kumunzhyieva NV
FOP Lola Rostyslav Mykolaiovych
FOP Martynenko Vitalii Mykolaiovych Ta FOP Polilui Valentynoiu T
FOP Melnykov Andrii Andriiovych
FOP Mironova Olena Volodymyrivna
FOP Moskaliuk Anatolii Ivanovych
FOP Novosad Oleh Yevhenovych
FOP Olefir Alina Viktorivna
FOP Samsoniuk Serhii Anatoliiovych
FOP Shevchenko Anton Ihorovych
FOP Shyshkovskyi Yurii Volodymyrovych
FOP Skrypka Oleksii Pavlovych
FOP Stryzhakov Andrii Olehovych
FOP Svetlichnyi Oleksii Leonidovych
FOP Tarasenko Dmytro Fedorovych
FOP TsYTsAK ANDRIY IVANOVYCh

FOP Udovychenko Denys Ivanovych
FOP Zakharchenko Mariia Volodymyrivna
Fopbaranvladyslavihorovych
Fopbubenshchikovavalentynavolodymyrivna
Fopdmytrukserhiiievheniiovych
Fopdmytrukzorianfedorovych
FOPFLYSTETYaNAMYKhAYLIVNA
Fophaidenkovolodymyrivanovych
Fophilovskyiihorvolodymyrovych
Fopholovchakvitaliimyroslavovych
Fophontsstepanmykhailovych
Fophuralstepanmykhailovych
Fophurinatetianaoleksandrivna
Fophurtovyiboryshryhorovych
Fopiakymchukdie
Fopialovehaalinaanatoliivna
Fopialovehairynavalerianivna
Fopiazhykandriihorovych
Fopierimichukviorikamykolaivna
Fopiurchenkodariaserhiivna
Fopkarpachovdmytroviliamovych
Fopkhliborobnataliiastepanivna
Fopkorotkanataliiamykhailivna
Fopkossolehvitaliiovych
Fopkotelvetsvv
Fopkrolevetsandriiviktorovych
Fopkulbachevskatetianaviktorivna
Fopkutuzovaanastasiiaolehivna
Foplebedievdmytrokostiantynovych
Foplesenkoirynaviktorivna
Fopluzhetskyiai
Fopmaksymiakvm
Fopmalikvaleriioleksandrovych
Fopmalynaiuriimykhailovych
FOPMAMEDOVISKANDERASIMOHLY
Fopmelnykoleksiivasylovych
Fopmiskakostiantynviktorovych
Fopmoskovkobohdanmykolaiovych
Fopmychkovskyivadymrostyslavovych
Fopmykhlaimv
Fopmyroshnychenkomykytaserhiiovych
Fopnahornyidmytrovolodymyrovych
Fopohibeninvolodymyrserhiiovych
Foppedanoleksandrserhiiovych
Fopperepelytsiaam
Fopperkovavv
Foppetrykoksanapetrivna
Fopprykhodkooleksandrvasylovych
Foppushankooleksandrolehovych
Fopradchenkopavlovaleriiovych
Foprakytinadianamykolaivna
Fopshcherbandd
Fopshevilatymofiimykhailovych



Nov 19, 2023 6:23:45 PM to 6:28:45 PM (5 minutes)

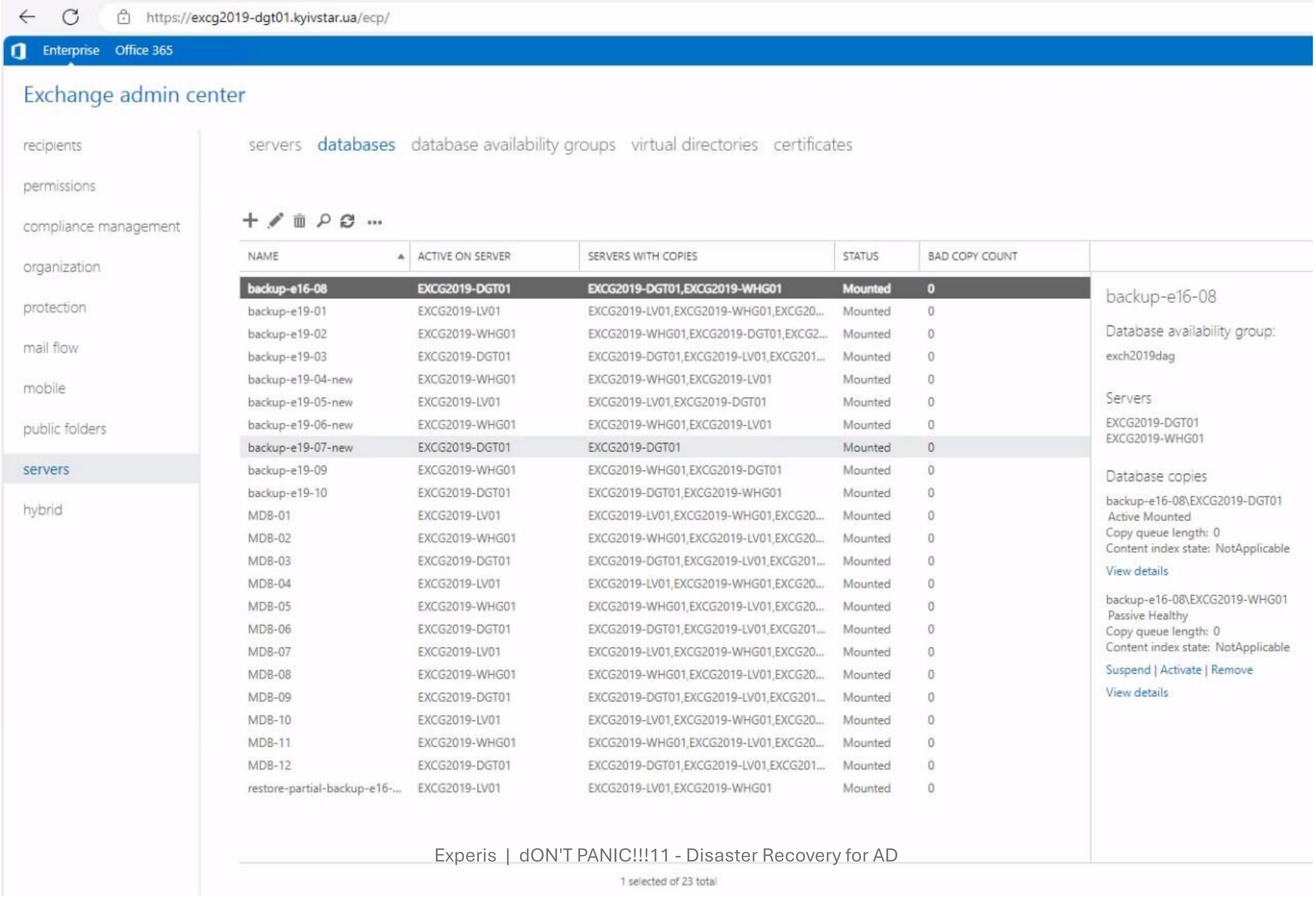
Nov 19, 2023, 18:23:45.840 to Nov 19, 2023, 18:28:45.839

Match all of the following filters:

- ✕ vc_username | exists
- ✕ vc_event_type | contains | com.vmware.vim25.userloginsessionevent

1 to 31 out of 31 events · Sort: Newest First

timestamp	text	source	event_type	vc_event_type	vc_username	hostname	appname	vmw_vc_auth_user	vmw_vc_auth_source	vmw_vc_auth_type
Nov 19, 2023, 6:27:42 PM	2023-11-19 16:27:42.715 lvv-vcn01.kyivstar.ua vcenter-server: User VSPHERE.LOCAL\SRM-06a54fc7-c12e-43f2-84b6-5902592389330127.0.0.1 logged in as VMware vim-java 1.0	lvv-vcn01.kyivstar.ua	v4_5c26184d	com.vmware.vim25.UserLoginSessionEvent	VSPHERE.LOCAL\SRM-06a54fc7-c12e-43f2-84b6-590259238933	lvv-vcn01.kyivstar.ua	vcenter-server	VSPHERE.LOCAL\SRM-06a54fc7-c12e-43f2-84b6-590259238933	127.0.0.1	VMware vim-java 1.0
Nov 19, 2023, 6:27:40 PM	2023-11-19 16:27:40.170 dgt-vcn01.kyivstar.ua vcenter-server: User VSPHERE.LOCAL\SRM-aa73c0b3-fc8b-4acc-bc07-94a3d93c73860127.0.0.1 logged in as VMware vim-java 1.0	dgt-vcn01.kyivstar.ua	v4_5c26184d	com.vmware.vim25.UserLoginSessionEvent	VSPHERE.LOCAL\SRM-aa73c0b3-fc8b-4acc-bc07-94a3d93c7386	dgt-vcn01.kyivstar.ua	vcenter-server	VSPHERE.LOCAL\SRM-aa73c0b3-fc8b-4acc-bc07-94a3d93c7386	127.0.0.1	VMware vim-java 1.0
Nov 19, 2023, 6:27:20 PM	2023-11-19 16:27:20.384 dgt-vcn01.kyivstar.ua vcenter-server: User VSPHERE.LOCAL\vpxd-extension-b18c2f92-372c-11e3-8236-000c29a33a8a0127.0.0.1 logged in as VMware vim-java 1.0	dgt-vcn01.kyivstar.ua	v4_5c26184d	com.vmware.vim25.UserLoginSessionEvent	VSPHERE.LOCAL\vpxd-extension-b18c2f92-372c-11e3-8236-000c29a33a8a	dgt-vcn01.kyivstar.ua	vcenter-server	VSPHERE.LOCAL\vpxd-extension-b18c2f92-372c-11e3-8236-000c29a33a8a	127.0.0.1	VMware vim-java 1.0
Nov 19, 2023, 6:27:20 PM	2023-11-19 16:27:20.071 dgt-vcn01.kyivstar.ua vcenter-server: User VSPHERE.LOCAL\vpxd-extension-b18c2f92-372c-11e3-8236-000c29a33a8a0127.0.0.1 logged in as VMware vim-java 1.0	dgt-vcn01.kyivstar.ua	v4_5c26184d	com.vmware.vim25.UserLoginSessionEvent	VSPHERE.LOCAL\vpxd-extension-b18c2f92-372c-	dgt-vcn01.kyivstar.ua	vcenter-server	VSPHERE.LOCAL\vpxd-extension-b18c2f92-372c-11e3-8236-000c29a33a8a	127.0.0.1	VMware vim-java 1.0



NAME	ACTIVE ON SERVER	SERVERS WITH COPIES	STATUS	BAD COPY COUNT
backup-e16-08	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-WHG01	Mounted	0
backup-e19-01	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
backup-e19-02	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-DGT01,EXCG2...	Mounted	0
backup-e19-03	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
backup-e19-04-new	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01	Mounted	0
backup-e19-05-new	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-DGT01	Mounted	0
backup-e19-06-new	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01	Mounted	0
backup-e19-07-new	EXCG2019-DGT01	EXCG2019-DGT01	Mounted	0
backup-e19-09	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-DGT01	Mounted	0
backup-e19-10	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-WHG01	Mounted	0
MDB-01	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
MDB-02	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01,EXCG20...	Mounted	0
MDB-03	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
MDB-04	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
MDB-05	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01,EXCG20...	Mounted	0
MDB-06	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
MDB-07	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
MDB-08	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01,EXCG20...	Mounted	0
MDB-09	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
MDB-10	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
MDB-11	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01,EXCG20...	Mounted	0
MDB-12	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
restore-partial-backup-e16-...	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01	Mounted	0

backup-e16-08

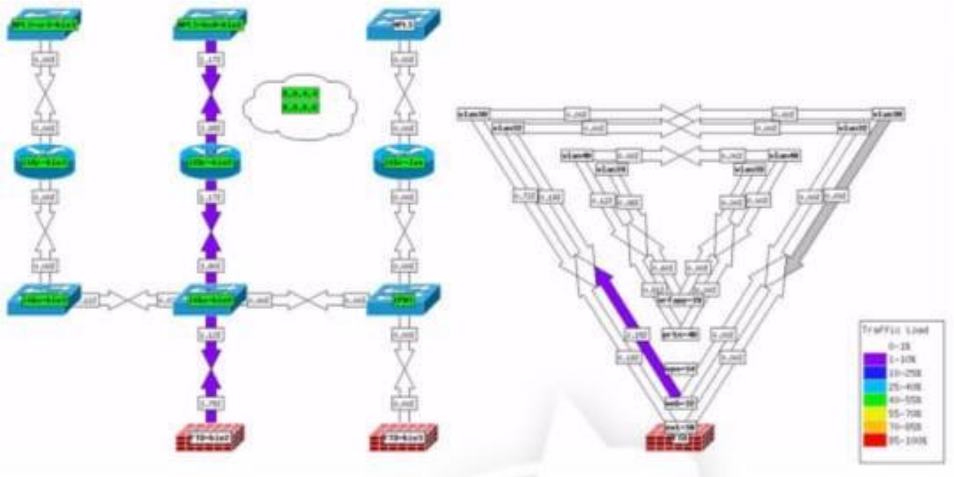
Database availability group:
exch2019dag

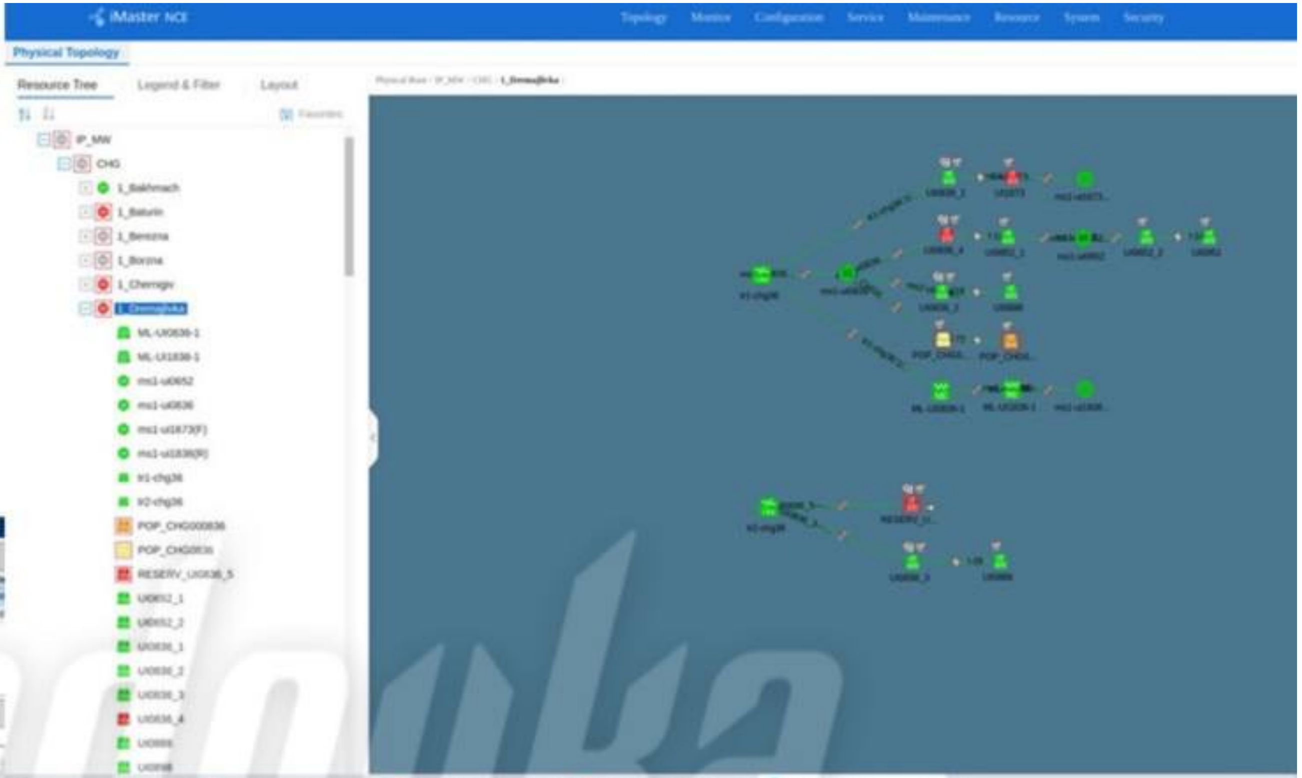
Servers
EXCG2019-DGT01
EXCG2019-WHG01

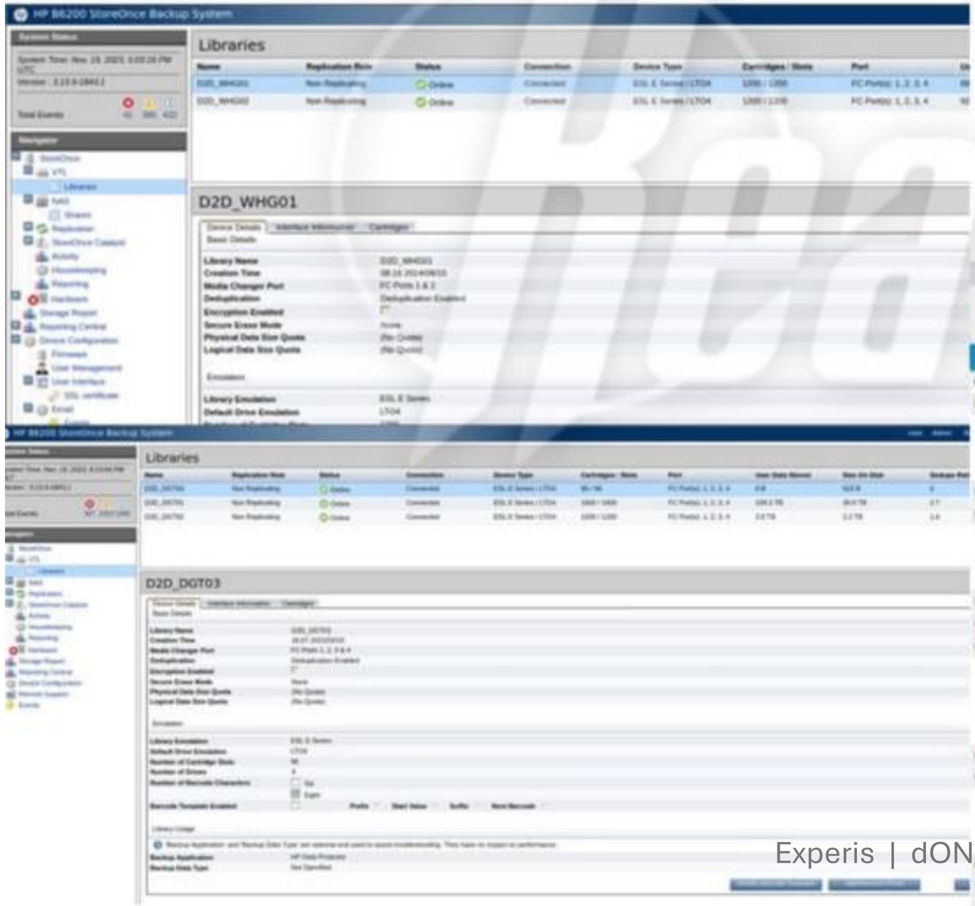
Database copies
backup-e16-08\EXCG2019-DGT01
Active Mounted
Copy queue length: 0
Content index state: NotApplicable
View details

backup-e16-08\EXCG2019-WHG01
Passive Healthy
Copy queue length: 0
Content index state: NotApplicable
Suspend | Activate | Remove
View details

1 selected of 23 total







HP B6200 StoreOnce Backup System

Libraries

Name	Replication Role	Status	Connection	Device Type	Cartridges / Slots	Port
D2D_WHG01	Non Replicating	Online	Connected	ESL E Series / LTO4	1200 / 1200	FC Port(s): 1, 2, 3, 4
D2D_WHG02	Non Replicating	Online	Connected	ESL E Series / LTO4	1200 / 1200	FC Port(s): 1, 2, 3, 4

D2D_WHG01

Device Details | Interface Information | Cartridges

Basic Details

Library Name	D2D_WHG01
Media Changer Port	FC Ports 1 & 2
Deduplication	Deduplication Enabled
Encryption Enabled	
Secure Erase Mode	None
Physical Data Size Quota	(No Quota)
Logical Data Size Quota	(No Quota)

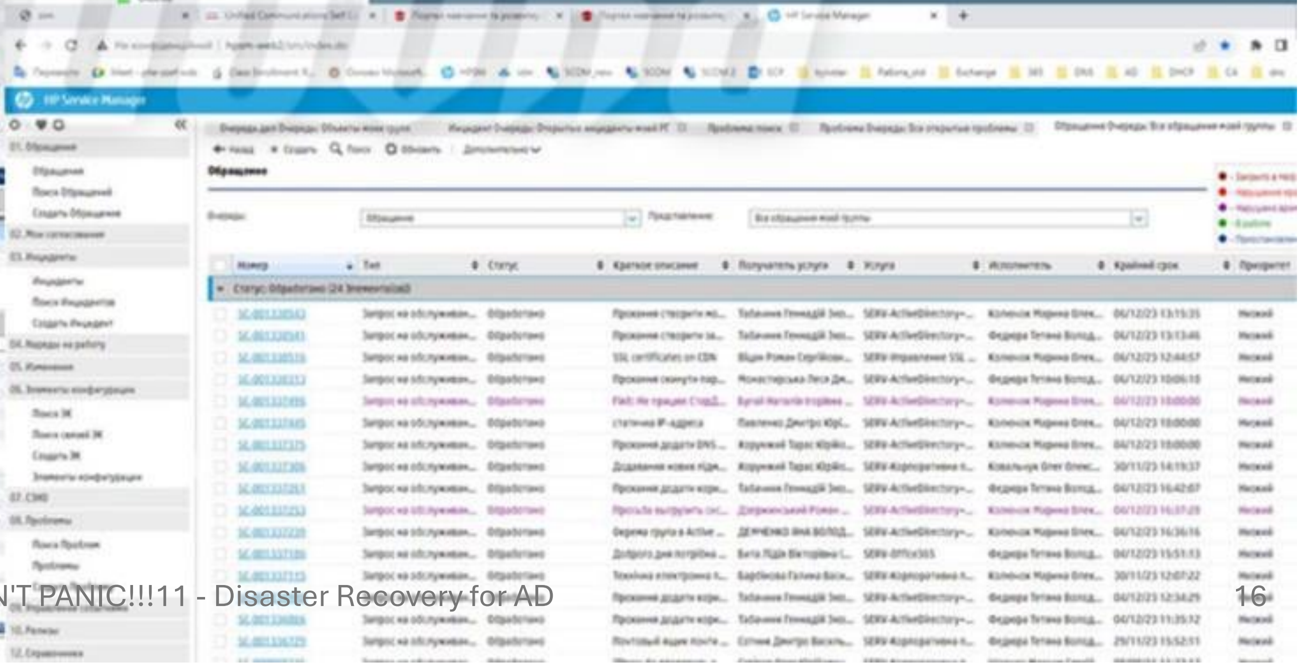
Emulation

Library Emulation	ESL E Series
Default Drive Emulation	LTO4

HP B6200 StoreOnce Backup System

Libraries

D2D_DGT03



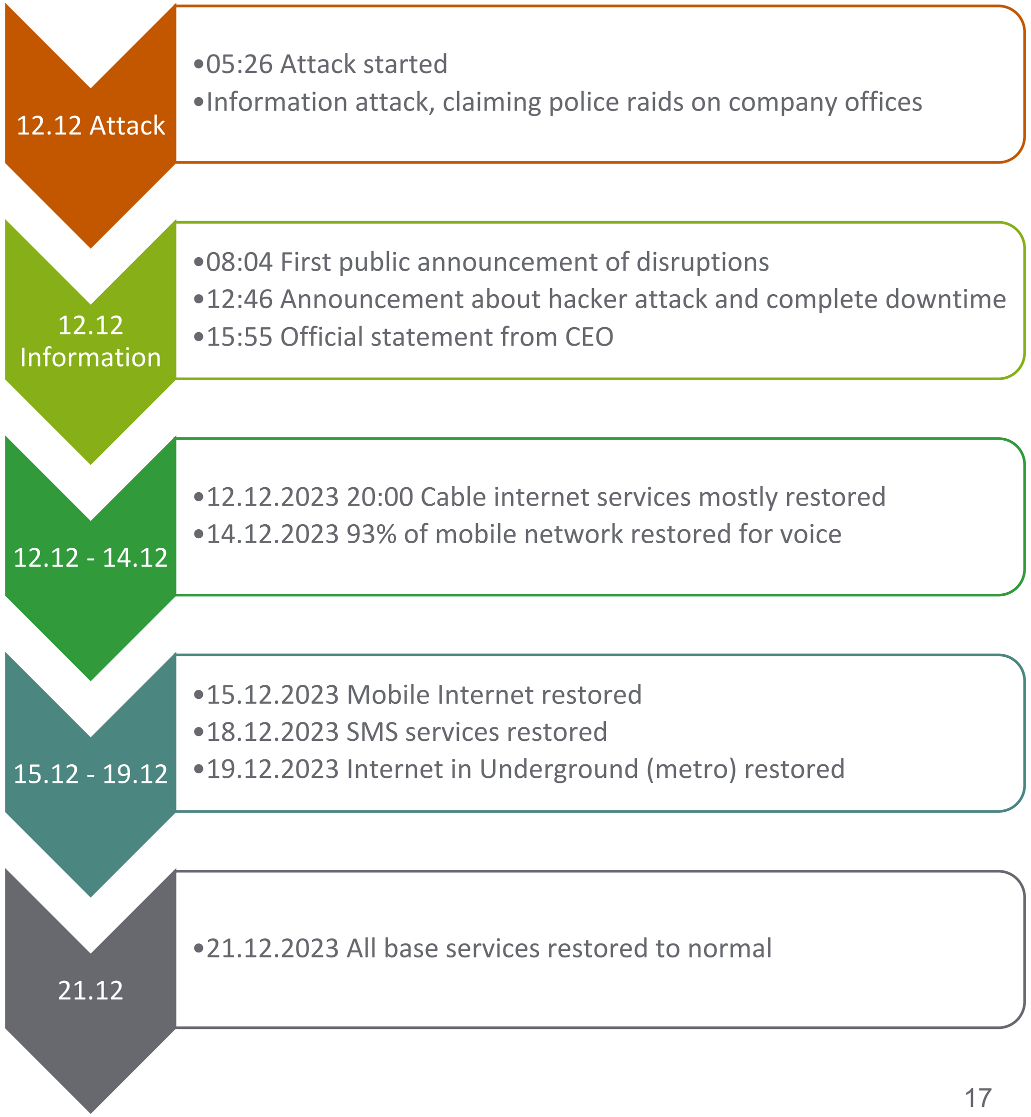
HP Service Manager

Обращение

Номер	Тип	Статус	Краткое описание	Получатель услуги	Услуга	Исполнитель	Крайний срок	Приоритет
Статус: Обработано (24 Элемент(а))								
[illegible]	Запрос на обслуживан...	Обработано	Прохання створити...	Табачник Геннадій Зін...	SERV-ActiveDirectory-...	[illegible]	06/12/23 13:15:35	Низкий
[illegible]	Запрос на обслуживан...	Обработано	SSL certificates on CDN	[illegible]	[illegible]	[illegible]	06/12/23 12:44:57	Низкий
[illegible]	Запрос на обслуживан...	Обработано	статична IP-адреса	[illegible]	SERV-ActiveDirectory-...	[illegible]	04/12/23 10:00:00	Низкий
[illegible]	Запрос на обслуживан...	Обработано	[illegible]	[illegible]	SERV-Office365	[illegible]	04/12/23 15:51:13	Низкий

Bonus: Large attack on Telecom company - Kyivstar

- 24M subscribers
- Core infrastructure damaged, including backups.
- Mobile network down, base stations damaged. Subscriber equipment damaged.
- Air raid alarms not working
- POS terminals and ATMs not working
- In some cities, street lighting had to be turned off manually



12.12 Attack

- 05:26 Attack started
- Information attack, claiming police raids on company offices

12.12 Information

- 08:04 First public announcement of disruptions
- 12:46 Announcement about hacker attack and complete downtime
- 15:55 Official statement from CEO

12.12 - 14.12

- 12.12.2023 20:00 Cable internet services mostly restored
- 14.12.2023 93% of mobile network restored for voice

15.12 - 19.12

- 15.12.2023 Mobile Internet restored
- 18.12.2023 SMS services restored
- 19.12.2023 Internet in Underground (metro) restored

21.12

- 21.12.2023 All base services restored to normal

Part I – High Level. Ransomware scenario

Imagine that everything is down and something is encrypted or damaged, CSIRT is assessing the damage and is determining safe restore points

- Are you able to login to your computer?
  - Need a plan if that is not available
- Are you able to communicate with your colleagues?
  - Need a backup communication channels
- Are you able to read the DR plans?
  - Need to store DR plans safe but accessible
- Are you able to get access to the Break-The-Glass accounts?
  - Password vault should be available during the disaster
- What is necessary to bring back remote access system?
  - Need a plan with the order of restoration in case of total disaster

Part I – High Level. Ransomware scenario - test

- Run tabletop exercise with the following audience:
  - ❑ Architects
  - ❑ Key operations personnel
  - ❑ Identity
  - ❑ Optionally include CSIRT for extended review
- Document gaps and issues
- Verify uncertain scenarios
- Provide input for architects to improve solutions
- Don’t panic

2. Low Level

Part II – Low Level. What is an AD disaster?

- AD has very robust, fool-proof design and recovery are rarely needed.

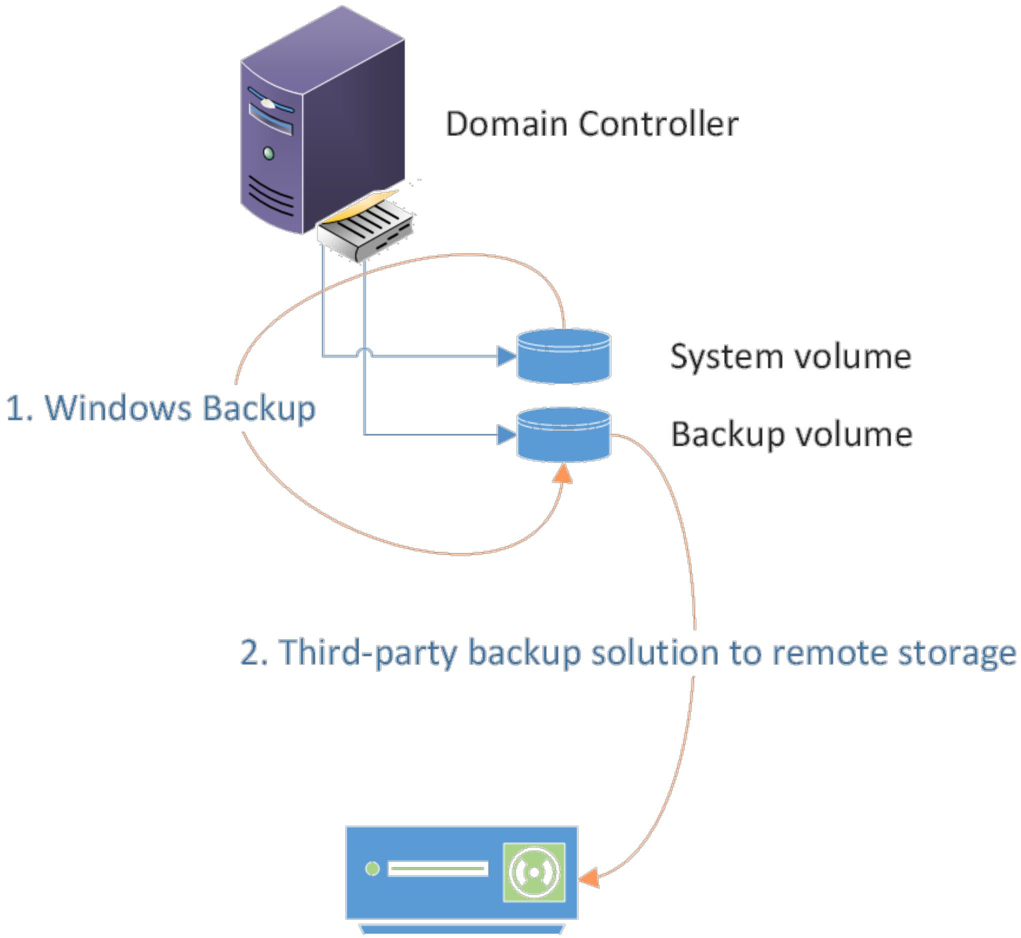
- There are many situations which can be called a disaster:
  - Mass removal of users or groups that needs to be reverted
  - Losing multiple domain controllers

- The real disaster would happen when:
  - All domain controllers are lost
  - *AD database is corrupted beyond repair*
  - *There's a need to roll-back the irreversible change*
  - *Domain eats through 2B (2,147,483,647) RID pool*

Part II – Low Level. How to back up AD?

Option 1

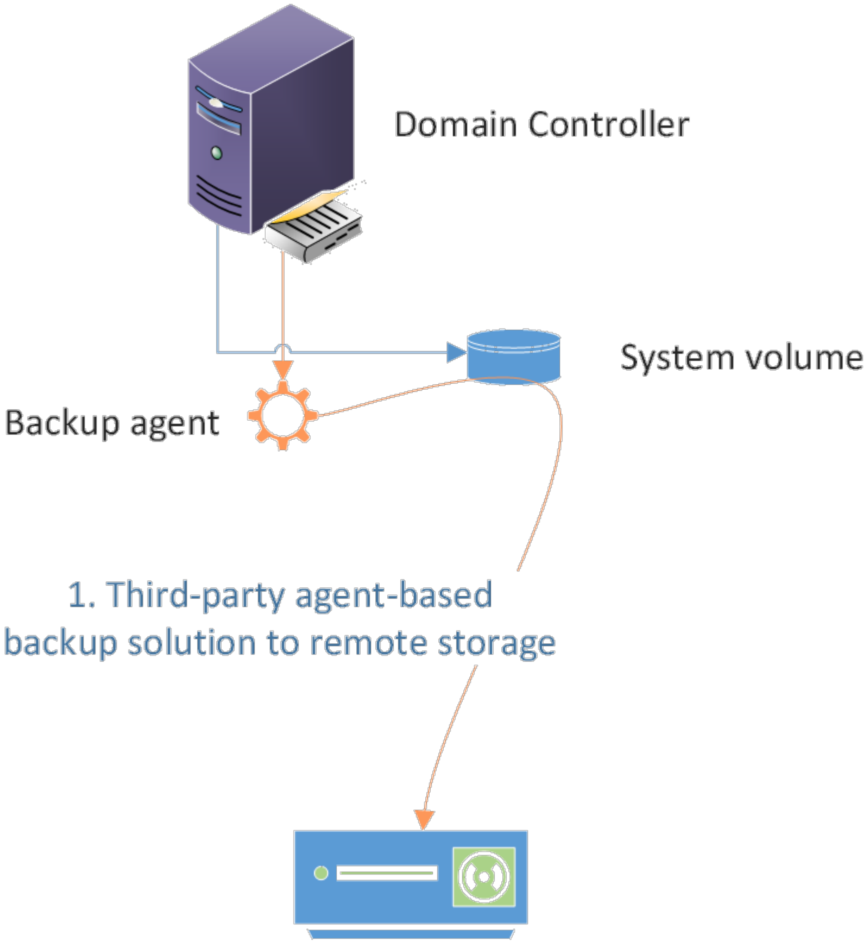
- Microsoft has a documented procedure for restoring AD from the Full Backup with Windows Backup
  - Officially it only requires System State, but restoring system state on another server was not supported earlier
  - One of the best practices 5-7 years ago were to backup several Domain Controllers in the domain to a safe location
  - Afterwards, for long term storage a standard third-party backup can be used to pick up Windows Backup contents



Part II – Low Level. How to back up AD?

Option 2

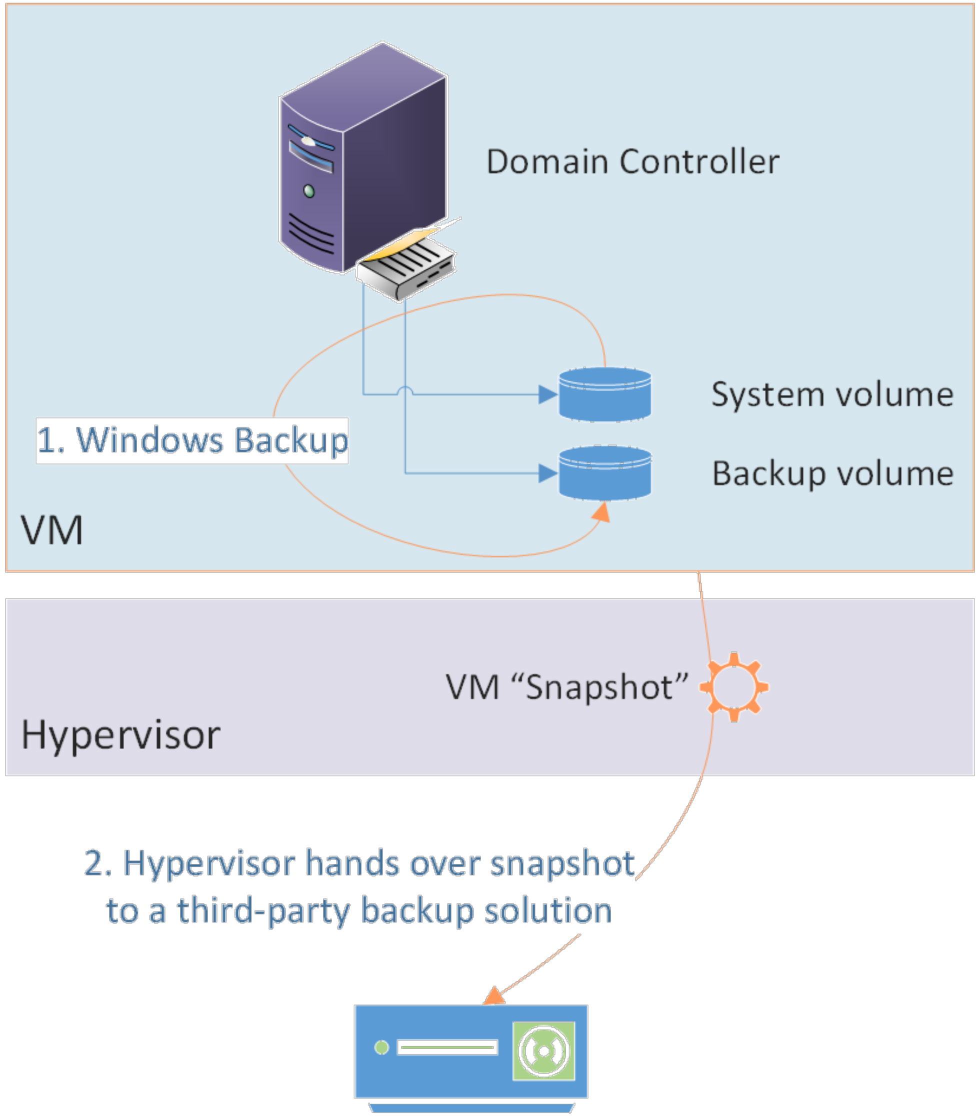
- Third-party agent-based backup, a classic (legacy) backup option
  - Must be tested, should not be expected to work until tested
  - How to restore from a complete loss? Install a fresh server, install agent, restore files and System State?
  - Authentication of agent to the backup server – very important, passwords should be treated as Domain Admins


Domain Controller
System volume
Backup agent
1. Third-party agent-based backup solution to remote storage

Part II – Low Level. How to back up AD?

Option 3

- Hypervisor-level backup solution. Agent usually offered as an option
  - ○ Provide the fastest way to recover a complete VM
  - ○ Allows to skip System State restore and DSRM boot
  - ○ Agent is not needed and best be avoided, to reduce attack surface
  - ○ Must be tested

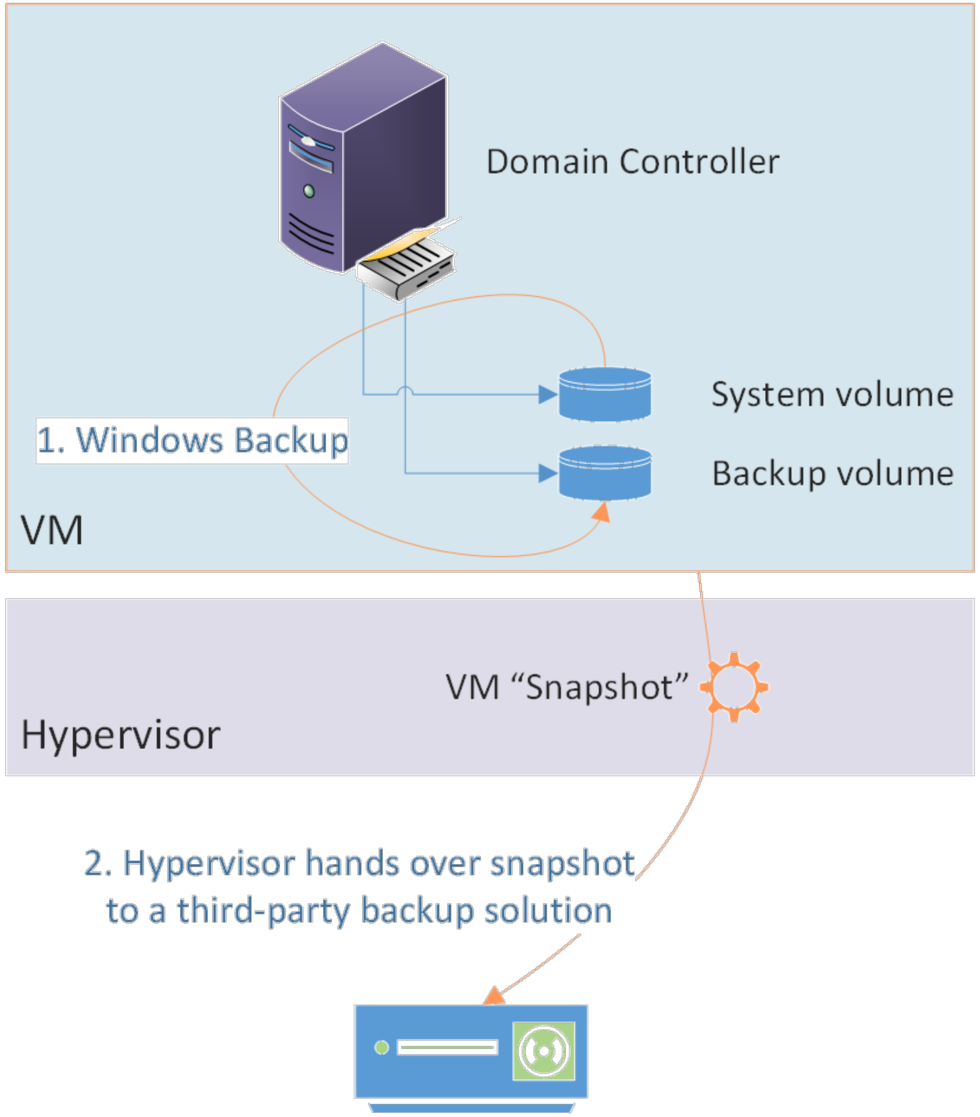


2. Hypervisor hands over snapshot to a third-party backup solution

Part II – Low Level. How to back up AD?

Keep security in mind

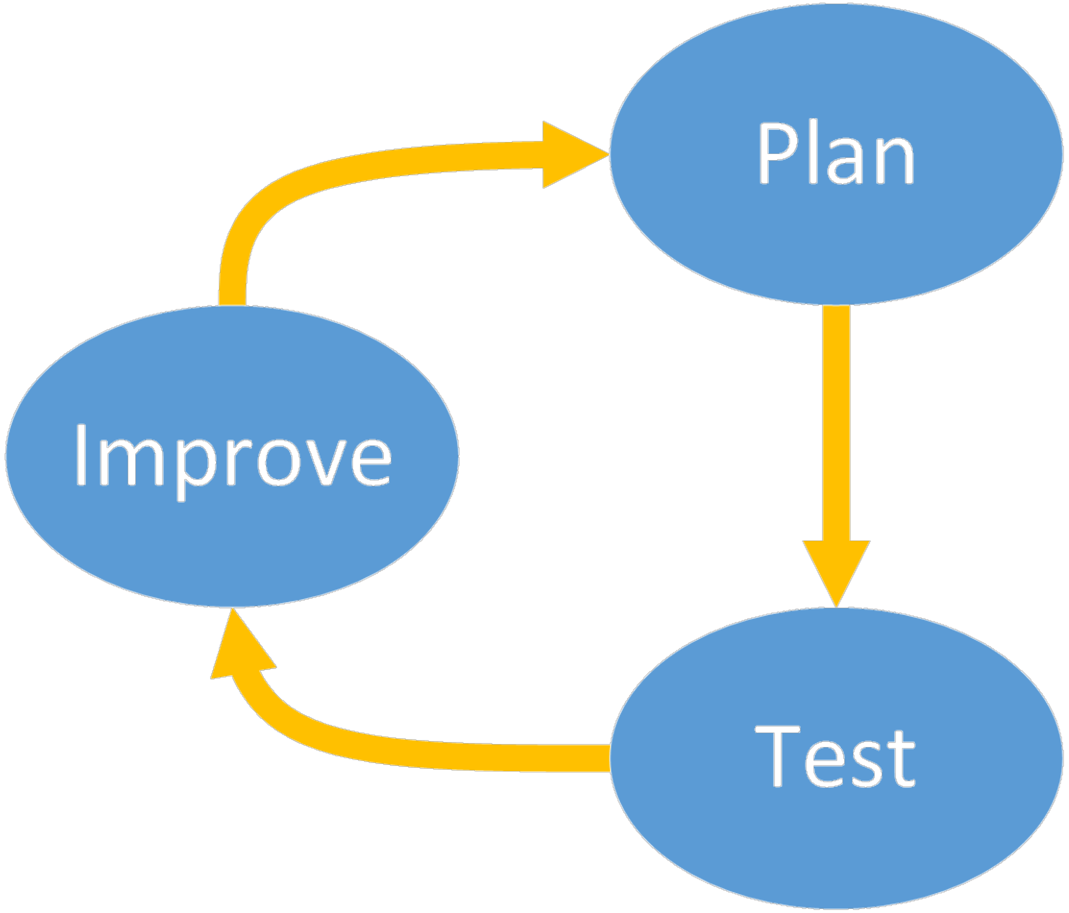
- Protect backup in each place of storage
  - Access to VM disk, credentials of backup agent from DCs, admins with access to backup console
  - People with access to DC backup should be considered Domain Admins (Tier 0)
  - Where possible, create a monitoring for events of access to backup files and attempts to restore
- Consider if you need to use agents and what benefits do they provide compared to built-in functionality (restoring group membership may be one of them)
- Test to see how restore works. Not tested = not existing



Part II – Low Level. How to back up AD?

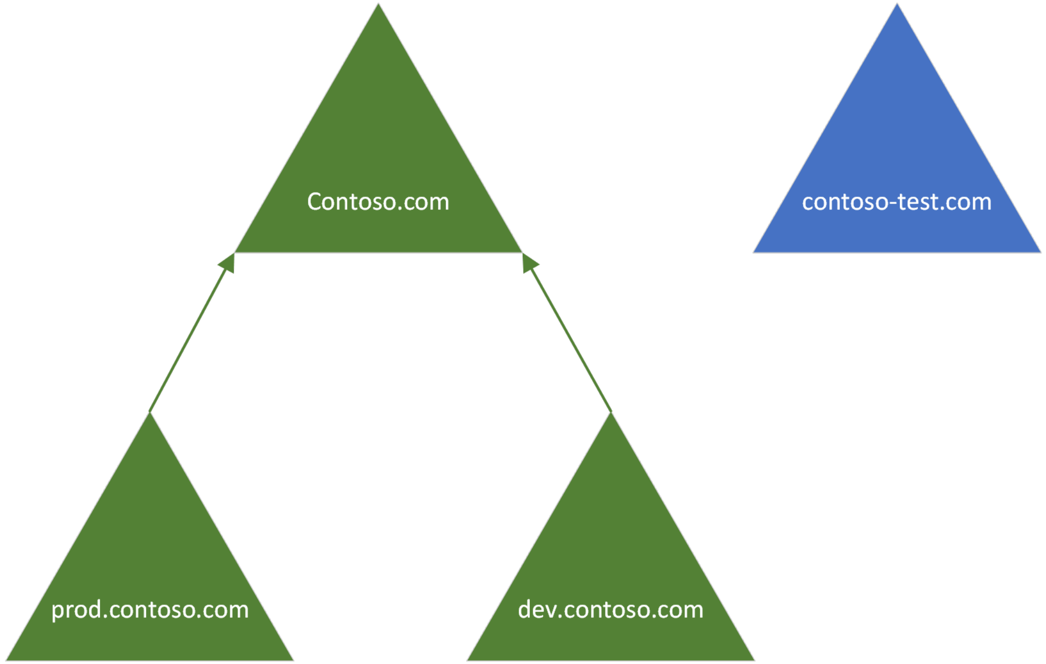
Feedback loop

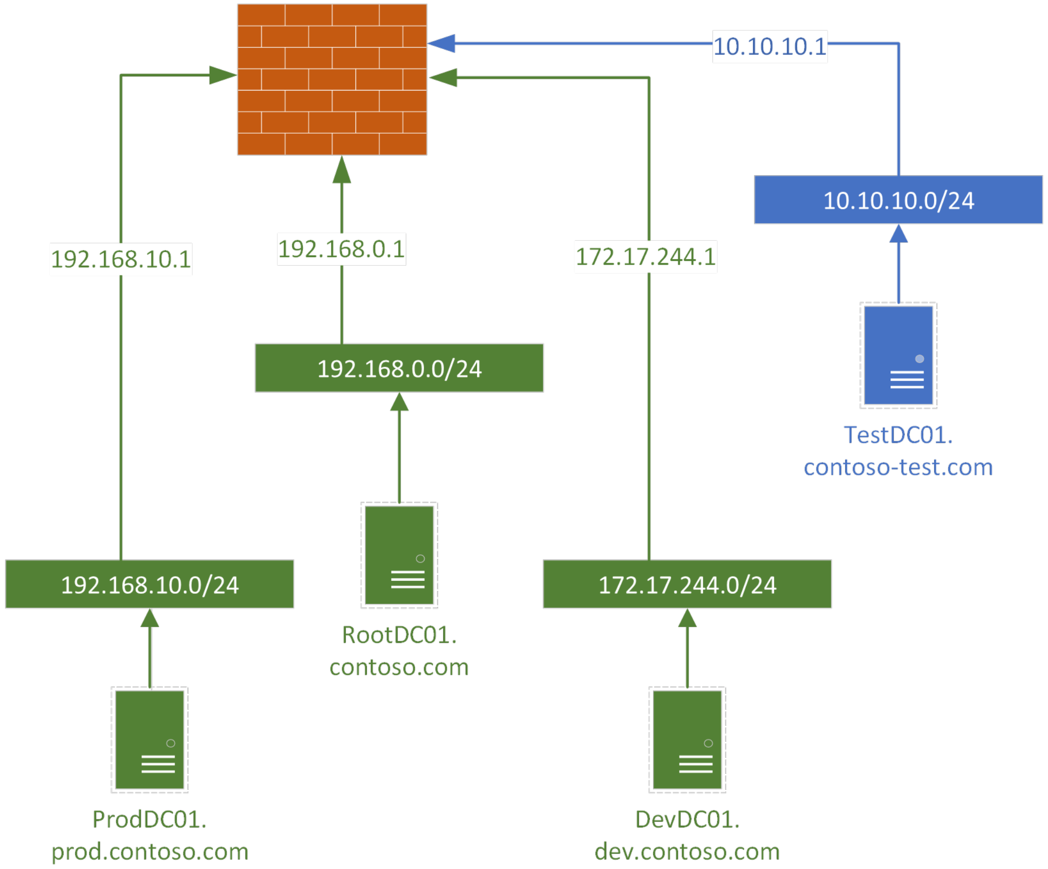
- If there is no plan yet – create a plan based on the available documentation. Estimate expected RTO for the following events:
  - Service partially restored – some authentication will work, e.g. logon to different servers and applications
  - Service fully restored (service fully functional from client side)
- Log every action, its timestamp and any errors
- Analyze deviations
- Implement fixes
- Do another round of testing



Part II – Low Level. Test environment

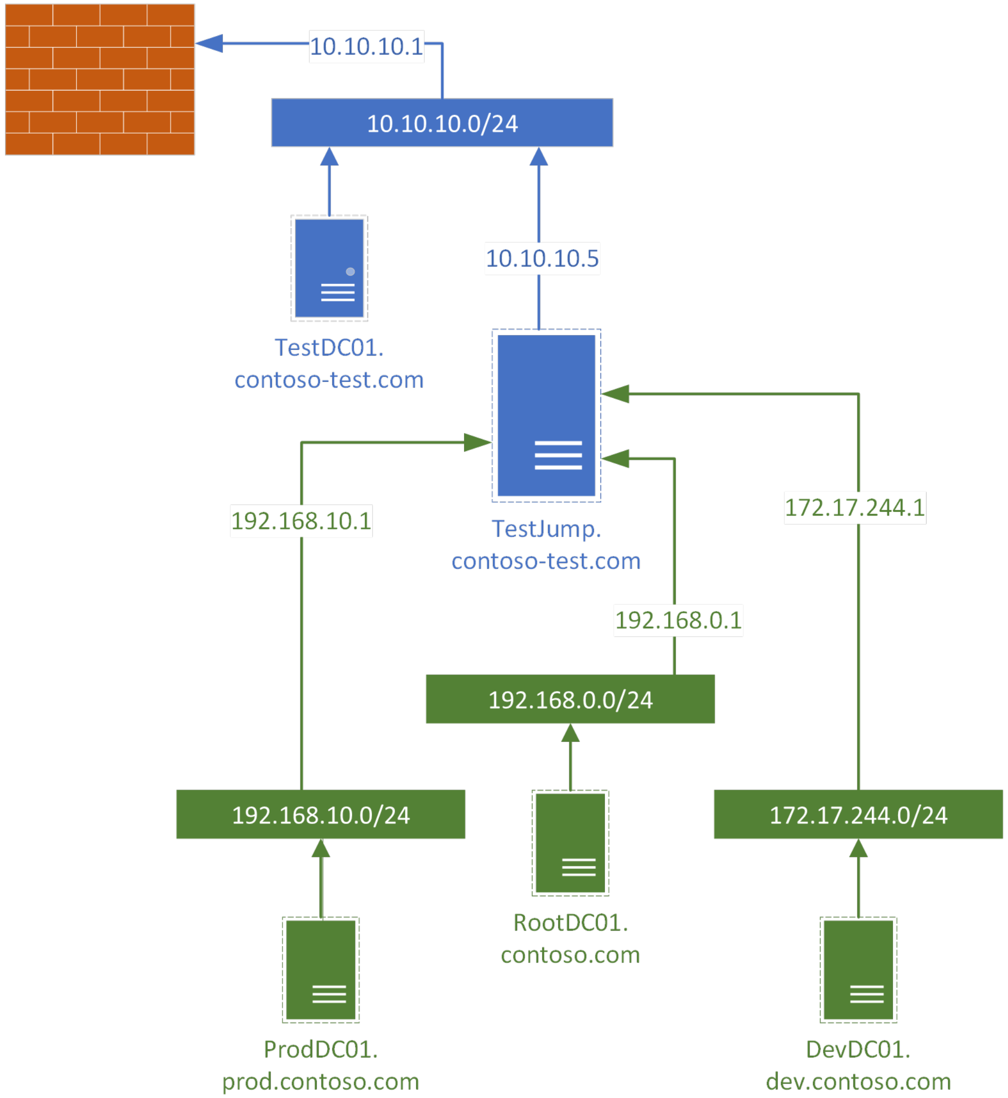
Consider the following setup





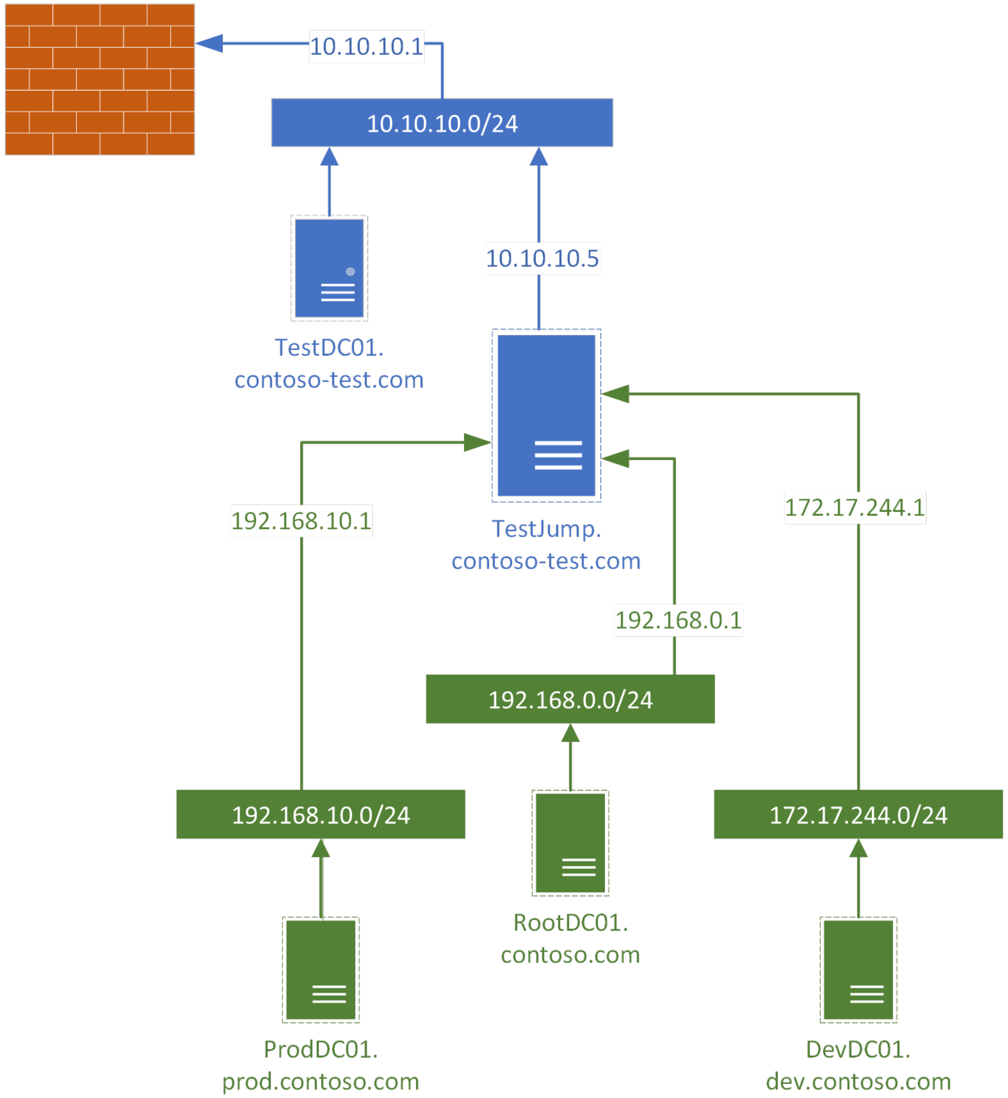
Part II – Low Level. Test environment

- You will need a separate test domain or another production domain
- Virtual machine, member of test domain with RDS role to allow more than 2 concurrent RDP sessions
- RRAS (Remote Access) to route between networks
- Configuration on TestJump.contoso-test.com
  - NIC1 – `10.10.10.5`, connected to company network, remove default gateway, add necessary routes manually using /32 netmask (monitoring, antivirus, patching, authentication, DNS)
  - NIC2 – `192.168.10.1, 192.168.0.1, 172.17.244.1`, connected to local VM cluster network
  - Routing and Remote Access configured in routing mode
  - Before restore, place a virtual machine in and test that traffic is not leaving test environment



Part II – Low Level. Test environment

- Once a Domain Controller is restored, it will be in a simulation of production network. You don't need to change IP address – because it impacts testing.
- Restore VM for a Domain Controller just like you would restore in production, only place it on a Host/Cluster with TestJump server and make sure to connect to a host local network
- Connect with RDP to TestJump and from there use RDP to connect to the restored Domain Controller, no need for console
- You will be able to copy/paste/auto-type which may not work through VM Console
- Multiple sessions are possible – several people working on several domains in parallel



Part II – Low Level. Test environment

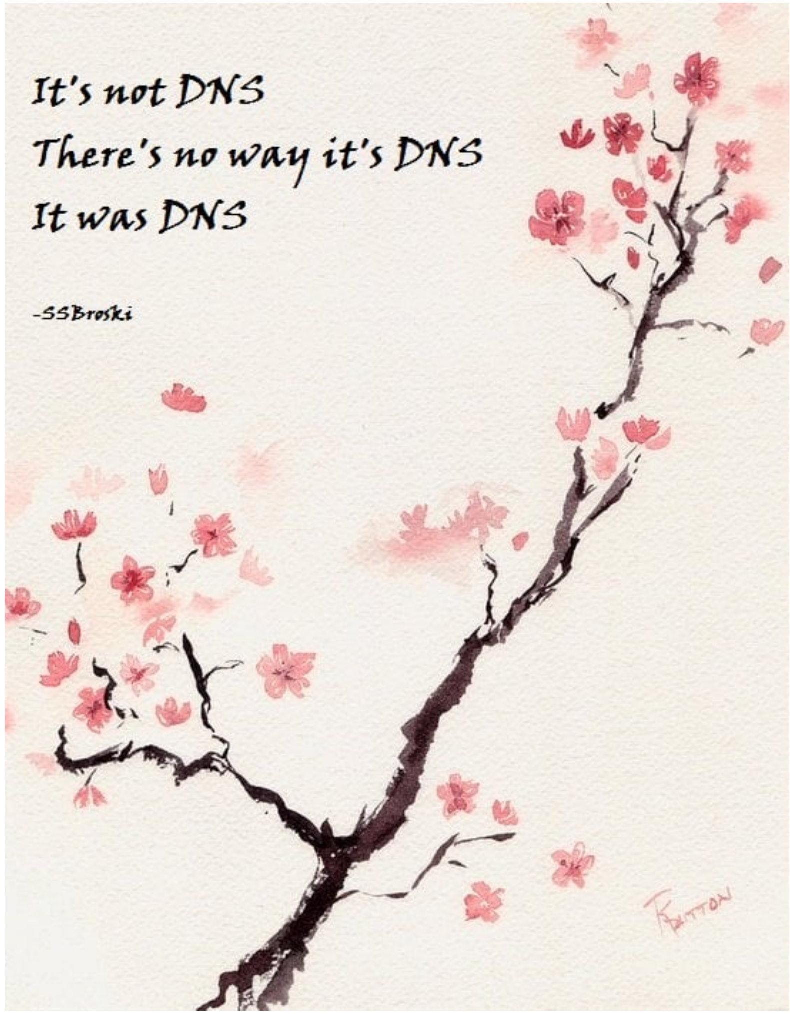
- Once you are logged on, don’t lock a screen or sign out
  - If you have a policy that is aggressively locking a screen, try changing it or overriding it with local policy
  - From Microsoft guide, regarding built-in Administrator account

    This guide used to recommend disabling the account. This was removed as the forest recovery white paper makes use of the default administrator account. The reason is, this is the only account that allows logon without a Global Catalog Server.
- Don’t use many special characters in DSRM passwords
  - Just make it 32 - 64 character long instead
- DNS – another promise not fulfilled.
  - Microsoft promises:

    Moreover, as part of metadata cleanup, DC Locator DNS resource records for all other DCs in the domain will be deleted from DNS.

    To help speed up DNS SRV record removal, run:

    ```
    nltest.exe /dsderegdns:server.domain.tld
    ```
  - Truth is – there is a lot of manual cleanup needed to remove DNS records from each AD Site, from various places under _msdcs zone on each restored DC
  - DNS is the biggest challenge in restoring replication between domains



Part II – Low Level. Test environment

Summary

- The complexity of AD Forest Restore is way bigger than of most other applications
- Even when you have performed the recovery several times and you think you know what will happen – new things pop up unexpectedly
- Every time I did exercise with my team, we were so happy that it was not a real case scenario
- Doesn’t matter how good is your Forest Recovery Plan – you will always find challenges. And it is only experience that will help you in those cases

Q&A

Contact info:

LinkedIn:

https://www.linkedin.com/in/ross-ua/

Signal:

RossUA.40

https://signal.me/#eu/mz8OdapNQpexl5wF5QhKst4fY0RK9qyCVkNlgUGMw6bJue_umd9LObXpFUR-DUnU