

FOR509 – Enterprise Cloud Forensics and Incident Response - Azure

Topics

A	
Accessing Microsoft Azure	2-17
1. Portal	2-18
2. CLI	2-19
3. PowerShell	2-25
Audit Logs	2-55, 2-59
Azure Compute	2-28
Azure General Structure	2-5
Azure Resource Manager	2-7
Azure Virtual Network (VNet)	2-34
B	
Blob storage	2-37-38
D	
DFIR Evidence	
Cloud Shell	2-21-24
Crypto mining VM (VmSize)	2-32
Generated keys	2-111
Log Sources Summary	2-135
NSG Flow Logs	2-102
NSG Logs	2-101
Tenant logs	2-47
Usefulness of each level of logs	2-43-44
Diagnostic setting	2-58
E	
Event Hubs Stream	2-73
Export logs via Graph API	2-75
I	
Interrupted sign-in status	2-50
IR in Cloud	2-138
K	
Key Resources	2-9
KQL	2-61
L	
Log Analytics Workspace	2-45
Logs description	2-59

Setup	2-58
Subscription Logs	2-86
Tenant Logs	2-61

M

MFA	2-53
MITRE ATTCK and Azure	2-16

N

Network Security Group	2-35, 2-98
1min interval collection	2-35
Flow Log Configuration	2-102
Flow Logs	2-102
Import into SOF-ELK	2-107
Logs	2-101
Network Watcher	2-104
Traffic Analytics	2-106
Network Virtual Appliance	2-36
Network Watcher	2-104

P

Provisioning Logs	2-59
-------------------------	------

R

Resource Groups	2-8
Resource ID	2-10
Role-Based Access Control (RBAC)	2-13
1. Security Principal	2-13
2. Role Definition	2-13
3. Scope	2-13
List user Role Assignments	2-15

S

Sign-in Logs	2-50, 2-59
Snapshot	2-140
Sources of Logs	2-43
Storage Account	2-37, 2-65
Access	2-109
Access Keys	2-109
Shared access signature (SAS)	2-109
Blob storage	2-37
Exfiltration (generated keys)	2-110, 111
Logs	2-108
Logs Enable by Policies	2-114
Subscription Logs	2-80
1. resourceId	2-81
2. operationName	2-81
3. resultType resultSignature	2-81
4. callerIpAddress	2-81
5. correlationId	2-81, 82
6. Identity claims	2-81
Subscriptions	2-6



FOR509 – Enterprise Cloud Forensics and Incident Response - Azure

T

Tenant Logs

Import into SOF-ELF2-71

Tools

az2-15, 2-20

azcopy (download snapshot) 2-148

Azure Storage Explorer 2-68

U

Universal Resource Identifier2-11

V

VM Insights2-133

VM Storage 2-31

VM Types 2-29

W

Windows Agents 2-120