aws migration evaluator

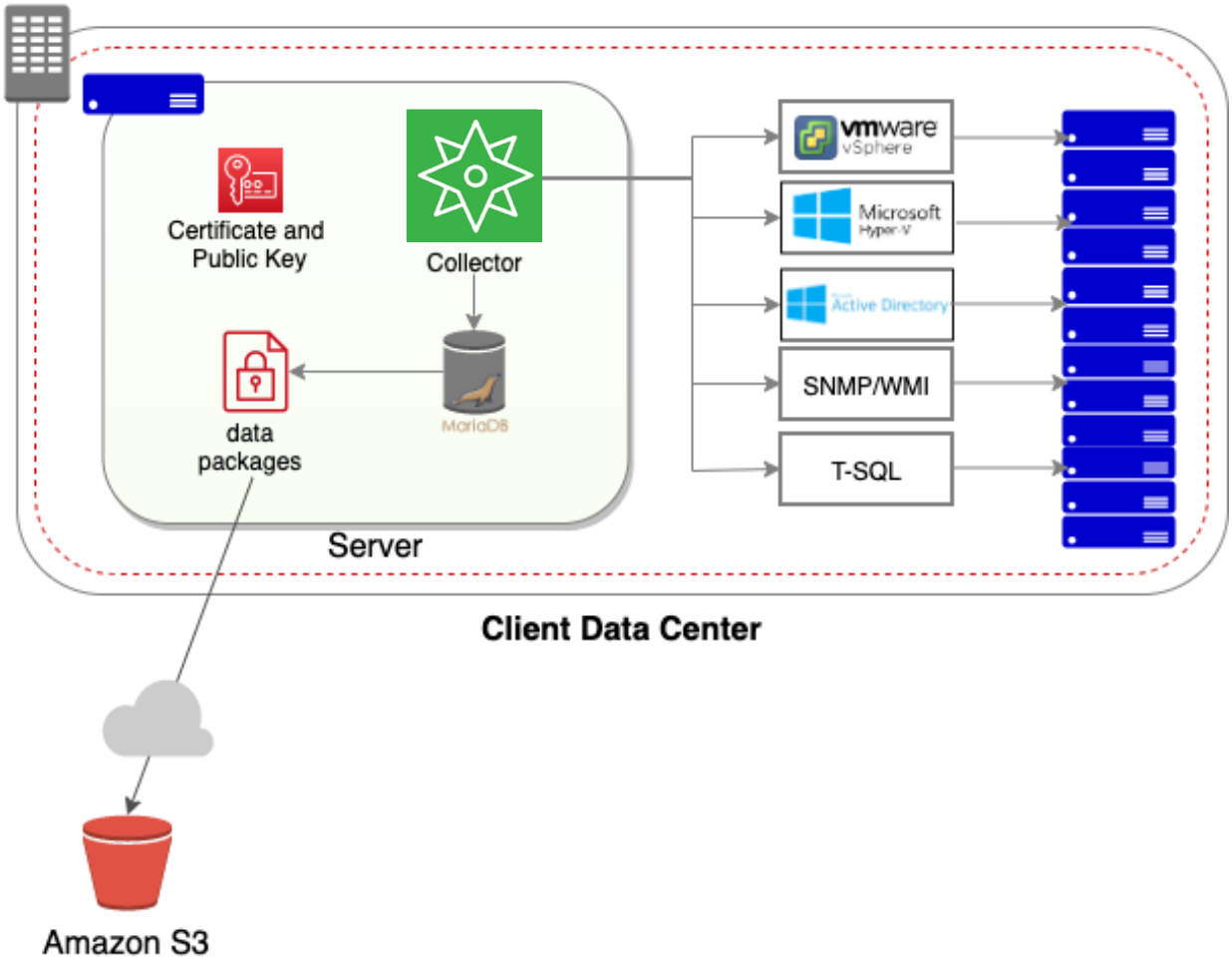
Overview for Agentless Collector

Version 20.08.05

Formerly TSO Logic

Overview

The following document outlines the flow of data during an engagement with Migration Evaluator (Formerly TSO Logic) in which the customer chooses to acquire provisioning and utilization patterns via the on-premises agentless collector. The network traffic is broken into two logical phases: data collection and data synchronization. All data collected is encrypted at rest (via a customer specific certificate) and transport (via HTTPS).



Data Collection

Monitoring VMware Infrastructure

For monitoring VMware, the collector communicates with each vSphere virtual appliance (not the actual virtual machine). Monitoring adds no additional load on the host system or virtual machines. Communication is done via the vSphere SOAP API over HTTPS (TCP 443). Usernames and passwords are encrypted at rest leveraging DPAPI and are not included in the data synchronised to the Migration Evaluator (Formerly TSO Logic) analytics engine.

The following vSphere SOAP API calls are made by the collector:

- RetrieveEntityPermissions
- CreatePropertyCollector
- CreateContainerView
- RetrieveServiceContent
- CurrentTime
- CreateFilter
- DestroyPropertyFilter
- QueryPerf
- RetrievePropertiesEx
- ContinueRetrievePropertiesEx
- WaitForUpdatesEx

The following are the default polling intervals:

- compute and storage provisioning every one hour
- compute utilization every 15 minutes
- power state every 15 minutes
- storage utilization every six hours

VMware infrastructure provisioning is persisted by the agentless collector along with their relationships and time-series usage. (i.e., a VirtualMachine runs on a HostSystem or a HostSystem runs within this ClusterComputeResource)

ClusterComputeResource

Attribute	Example Value
Key	domain-c518
Name	PROD-SHARED-SVC

ComputeResource

Attribute	Example Value

Key	domain-s173
Name	192.168.0.226

Datacenter

Attribute	Example Value
Key	datacenter-2
Name	PROD

Datastore

Attribute	Example Value
Accessible	TRUE
Key	datastore-126041
MultipleHostAccess	TRUE
Name	PRD-APX-G-V-CDP-002-PRODLNX30660
Type	VMFS
Url	ds:///vmfs/volumes/59c283f4-8e0be3ba-31ee-0025b50aa00f/

Folder

Attribute	Example Value
Key	group-v73828
Name	Colleague Portal

HostSystem

Attribute	Example Value
AssetTag	
CpuMhz	2799
CpuModel	Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
Key	host-356
MemorySizeInBytes	17037066240
Model	UCSB-B200-M3
Name	3005.bc.abcd.net
NormalizedUuId	b52500000b000000000000000000005
NumCpuCores	20
NumCpuPkgs	2
NumCpuThreads	40
ServiceTag	FCH2020JFBP

Uuid	b5250000-0b00-0000-0000-000000000005
Vendor	Cisco Systems Inc

VirtualApp

Attribute	Example Value
Key	resgroup-v819
Name	VIPR SRM

VirtualDisk

Attribute	Example Value
BackingContentId	
BackingFilename	
BackingLunUuid	
BackingThinProvisioned	FALSE
BackingType	
BackingUuid	
CapacityInKb	0
DeviceId	4003
Label	
VirtualMachineKey	vm-231571

VirtualMachine

Attribute	Example Value
CpuAllocationLimit	-1
CpuAllocationReservation	0
FullName	Red Hat Enterprise Linux 6 (64-bit)
GuestId	rhel6_64Guest
GuestState	notRunning
HostName	prodlnx3028.bc.abcd.net
InstanceUuId	502efe96-0150-b395-682f-adb11f482945
IpAddress	
IpAddresses	
Key	vm-886
MemoryMb	16384
Name	prodlnx3028
NumCpu	8
Template	FALSE
ToolsRunningStatus	guestToolsNotRunning

UuId	422e44c8-5caa-4648-387c-ecc6e6ddb546

Monitoring Hyper-V Infrastructure

For monitoring Hyper-V, the collector communicates with each Hyper-V host (not the actual virtual machine). Monitoring adds no additional load on the virtual machines. Communication is done via WMI over TCP port 135 + ephemeral TCP port range (49152 - 65535). *Note: WMI can be problematic through firewalls due to maintaining contracts in the ephemeral port range.* Usernames and passwords are encrypted at rest leveraging DPAPI and are not included in the data synchronised to the Migration Evaluator (Formerly TSO Logic) analytics engine.

The following are the default polling intervals:

- compute and storage provisioning every one hour
- compute and storage utilization every nine minutes
- power state every nine minutes

Hyper-V infrastructure provisioning is persisted by the agentless collector along with their relationships and time-series usage. (ie, a VirtualMachine runs on a HostSystem)

HostSystem

Attribute	Example Value
AllocatedDisk	254008094720
AverageProcessorClockSpeed	3600
CredentialProfile	hyperV
FQDN	HYPERV4.WORKGROUP
HostName	192.168.0.50
IdentifyingNumber	3F4C9M2
Model	OptiPlex 7050
NumberOfCores	4
NumberOfCpus	1
NumberOfLogicalProcessors	8
OperatingSystemVersion	6.3.9600
ProcessorId	BFEBFBFF000906E9
ProcessorName	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz
TotalPhysicalMemory	17037066240
Uuid	4C4C4544-0046-3410-8043-B3C04F394D32
Vendor	Dell Inc.
WmiCredentialsUsed	1e40b1ba-0a63-4f12-9669-31c6ca166d32

VirtualMachine

Attribute	Example Value
AllocatedDisk	53687091200
AllocatedMemory	512
FQDN	W2012-2
IpAddresses	192.168.0.66
Key	548922cb-35b1-4db0-863b-47f57625b8ac
LastReplicationTime	16010101000000.000000-000
LastReplicationType	0
Name	W2012-2
OperationalStatus	
OSName	Windows Server 2012 Standard
ProcessorCores	1
ProcessorLimit	100000
ProcessorReservation	0
ProcessorWeight	100
ReplicationHealth	0
ReplicationMode	0
ReplicationState	0

Monitoring Bare Metal Infrastructure

For monitoring bare metal servers, the collector communicates with each server directly. For Windows servers, collection can be configured to leverage WMI, SNMP v2c or SNMP v3. For Linux servers, SNMP v2c or v3 is available. Communication via SNMP is done over UDP port 161. Communication via WMI is over TCP port 135 + ephemeral TCP port range (49152 - 65535). *Note: WMI can be problematic through firewalls due to maintaining contracts in the ephemeral port range.* Usernames and passwords are encrypted at rest leveraging DPAPI and are not included in the data synchronised to the Migration Evaluator (Formerly TSO Logic) analytics engine.

The following WMI namespaces are queried:

- \default\StdRegProv (HKEY_USERS)
- \cimv2\Win32_PerfFormattedData_PerfOS_Processor
- \cimv2\Win32_PerfFormattedData_PerfOS_Memory
- \cimv2\Win32_ComputerSystem
- \cmiv2\Win32_LogicalDisk
- \cimv2\Win32_PerfFormattedData_Tcpip_TCPv4
- \cimv2\Win32_OperatingSystem

- \cimv2\Win32_Processor

The following SNMP OIDs are queried:

Description	Linux	Windows
CPU Utilization	1.3.6.1.2.1.25.3.3.1.2	1.3.6.1.2.1.25.3.3.1.2
Memory Utilization	1.3.6.1.4.1.2021.4	1.3.6.1.2.1.25
Active Users	1.3.6.1.2.1.25.1.5.0	1.3.6.1.2.1.25.1.5.0
Active or open TCP Connections	1.3.6.1.2.1.6.9.0	1.3.6.1.2.1.6.9.0
Network packet Rate	1.3.6.1.2.1.2.2.1.11	1.3.6.1.2.1.2.2.1.11
Load Average	1.3.6.1.4.1.2021.10	

The following are the default polling intervals:

- compute and storage utilization every nine minutes
- compute provisioning (WMI only) every nine minutes
- power state every nine minutes.

Bare metal infrastructure provisioning is persisted by the agentless collector along with time-series usage.

Device

Attribute	Example Value
FQDN	
IpAddress	192.168.0.63
Local Storage Size	
Location	
MacAddress	
MachineType	
Name	Server-1
OperatingSystem	Windows Server 2012 Standard
Physical Memory	
Processor String	Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz
Uuid	

Discovering SQL Server Instances

For discovering which servers are running Microsoft SQL Server, the collector communicates with each server directly. Communication via T-SQL is over TCP port 1433. Usernames and

passwords are encrypted at rest leveraging DPAPI and are not included in the data synchronised to the Migration Evaluator (Formerly TSO Logic) analytics engine.

The following queries are run:

- SELECT @@SERVICENAME, @@VERSION
- SELECT * FROM sys.databases
- SELECT * FROM sys.master_files

The default polling interval for scanning all servers is 24 hours. Scanning can be manually initiated from the collector UI.

The following metadata is persisted about the Microsoft SQL Server database instance bound to TCP port 1433.

Database Instance

Attribute	Example Value
Instance Name	versionDisplayString
SQL Server version	Microsoft SQL Server 2016
SQL Server edition	Standard Edition (64-bit)

The following metadata is persisted for each database running on the database instance

Database Information

Attribute	Example Value
Database Name	master
Description	LOG
Size	The current size in MB
Max Size	The maximum size in MB

Data Synchronization

The data collected each day is exported from the local encrypted database and re-encrypted using a customer specific certificate into individual data packages on the local filesystem. If configured, the data packages are automatically synchronized to the Migration Evaluator (Formerly TSO Logic) managed, AWS S3 bucket in US East-1.

When manually providing files for an assessment, the customer authenticates with the Management Console using their personal username, password and optional multi-factor authentication token. Files are stored in a Migration Evaluator (Formerly TSO Logic) managed, AWS S3 bucket in US East-1.

To support automatic data synchronization, egress traffic to https://s3.amazonaws.com is required.