Hewlett Packard Enterprise

Reference Architecture

HPE REFERENCE CONFIGURATION FOR CYBERSECURITY THREAT DETECTION USING TROVARES XGT GRAPH ENGINE ON HPE SUPERDOME FLEX

Combining graph analytics with HPE Superdome Flex for faster cybersecurity threat detection

CONTENTS

Executive summary 3
Introduction 3
- Cyber vulnerability assessment and data exfiltration 4
- Common cyber network incidents 4
- Cybersecurity analytics 5
- Graph analytics 6

Solution overview 6
- Cybersecurity graph analytics solution blueprint 7

Solution components 8
- Trovares xGT cybersecurity graph analytics toolkit 8
- HPE Superdome Flex Server 8
- HPE OneView 9
- Hardware 10
- Software 10
- Application software 11

Proof-of-concept solution implementation 11
- Use Case: Detecting network anomalies by identifying zombie reboot and RDP hacking events 11
- Scaling lateral movement cyber threat detection 13

Summary 14
- Implementing a proof-of-concept 14

Appendix A: Bill of materials 14
Resources and additional links 16

EXECUTIVE SUMMARY

As cybersecurity attacks continue to increase in numbers and severity, businesses across all industries are increasing their spending and resources to help mitigate risk and eliminate threats more quickly. As cyber criminals become more sophisticated, it becomes even more critical for cybersecurity teams to look for solutions that can help them prevent attacks and reduce the time it takes for threat detection to mitigate risk and costs associated with active threats. In addition, data growth is expanding the time and resources it takes to scan critical data and network logs searching for these threats. Solutions to address these problems need the right balance of compute and memory along with speed and accuracy to quickly identify and mitigate cybersecurity threats.

One solution that has shown great results in detecting cybersecurity threats more quickly is combining the large in-memory compute capabilities of the scale-up HPE Superdome Flex with Trovares xGT, a powerful property graph engine. HPE Superdome Flex with its Symmetric Multiprocessing (SMP) scale-up design allows cyber teams to address data-intensive problems holistically and unparalleled scale with single-system simplicity. With the ability to scale from 4-sockets/768GB memory to 32-sockets/48TB memory, the HPE Superdome Flex can scale to meet your largest in-memory compute needs in the data center. Trovares xGT delivers search queries hundreds of times faster than conventional graph tools with near linear scalability and high degrees of parallelism. Trovares xGT taps into the large pool of memory and high core count and numbers of threads available on HPE Superdome Flex to bring new levels of performance in the search for cybersecurity threats.

One common cybersecurity attack is called the lateral movement attack. In a lateral movement attack, a bad actor gains access to a network and moves through the network searching for vulnerabilities using common cyber-attack techniques such as phishing and other attacks described in the MITRE ATT&CK®[1] catalog. A big challenge for cybersecurity teams in detecting lateral movement attacks is the fact that they often look like normal network traffic and can be difficult to detect. Scanning for these threats by traversing through large network activity logs is not only challenging but can be very time consuming. In this document, we will explore how running Trovares xGT graph engine on the large in-memory footprint of HPE Superdome Flex helps businesses scan cyber logs more quickly and reduce the Mean Time To Detection (MTTD) for finding these threats.

Target audience: The intended audience of this document includes, but is not limited to cybersecurity teams, Chief Information Security Officer (CISO), Chief Data Officer (CDO), data scientists, IT managers, presales engineers, services consultants, partner engineers, and customers.

Document purpose: The purpose of this document is to describe a Reference Configuration, highlighting recognizable benefits to technical audiences. This reference configuration provides general guidelines for implementing the HPE Cybersecurity Threat Detection Solution combining Trovares xGT and HPE Superdome Flex. In addition to outlining the key solution components, this document also provides guidelines for configuring and deploying this combined solution.

This Reference Configuration describes solution testing performed in January 2020 in Hewlett Packard Enterprise engineering labs.

INTRODUCTION

The HPE Cybersecurity Threat Detection Solution combining HPE Superdome Flex with Trovares xGT is designed to complement existing cybersecurity mitigation tools focusing on helping businesses detect cybersecurity threats more quickly than conventional tools. This solution provides the following benefits:

- **Performance:** Enables faster threat detection scans reducing MTTD, thus mitigating risk exposure and costs associated with cyber-attacks.
- **Scale:** Achieves near linear scalability to mitigate data growth challenges and enable the ability to scan larger data logs more quickly.
- **Enhanced Capabilities:** Delivers enhanced complex query capabilities enabling new insights into cyber threats.
- **Simplification:** Enables ease-of-use through accessing from a Jupyter notebook to probe big data at terabyte scale.

The HPE Cybersecurity Threat Detection Solution is ideal for any business who is looking for a comprehensive cybersecurity solution that reduces the MTTD to detect and mitigate cybersecurity attacks like lateral movement threats, command-and-control threats, and data exfiltration. Lateral threat movements include attacks such as Zombie Distributed Denial of Service (DDoS) attack, Remote Desktop Hacking

[1] MITRE ATT&CK catalog: https://attack.mitre.org/

(RDP), and Privilege Escalation attacks. Command-and-control threats include attacks such as Proxy Hacking, Remote Service Hacking, and Windows Remote Management Hacking.

As cyber-attacks continue to increase in number and severity, it's critical that cybersecurity teams continue to look for solutions to help mitigate risk and reduce costs associated with these attacks. The following sections discuss some of the common cybersecurity techniques.

Cyber vulnerability assessment and data exfiltration

A vulnerability assessment is a process that organizations follow to help identify cyber vulnerabilities along with properly classifying and prioritizing these threats and their potential impact to business operations. These assessments can encompass many systems like information technology and other infrastructure and are another important part of the overall plan for addressing cybersecurity threats to the organization.

Data exfiltration is the unauthorized copying, transfer or retrieval of data from a computer or server. Some common data exfiltration techniques include attacks on outbound email servers, downloads and uploads of data to non-secure devices, and accessing cloud-based services in a non-secure manner creating a vulnerability to the user's system.

Common cyber network incidents

A cybersecurity incident or information security incident is defined by the US Department of Homeland Security[2] as "an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems". Depending on the severity of the cybersecurity incident, experiences may range from not noticing any impacts at all to systems to complete shutdown of impacted systems. In the most extreme cases, threat actors might severely damage or completely destroy systems requiring a complete shutdown of business operations.

The HPE Cybersecurity Threat Detection Solution uses anomaly-based detection methods to mitigate vulnerabilities such DDoS attacks and zero-day outbreaks. DDoS attacks are often used maliciously to consume the resources of hosts and network that would otherwise be used to serve legitimate users. The overall goal with DDoS attacks is to overwhelm the target network resources making it more difficult for users to be able to access legitimate services. Figure 1 outlines some of the most common cybersecurity threats.

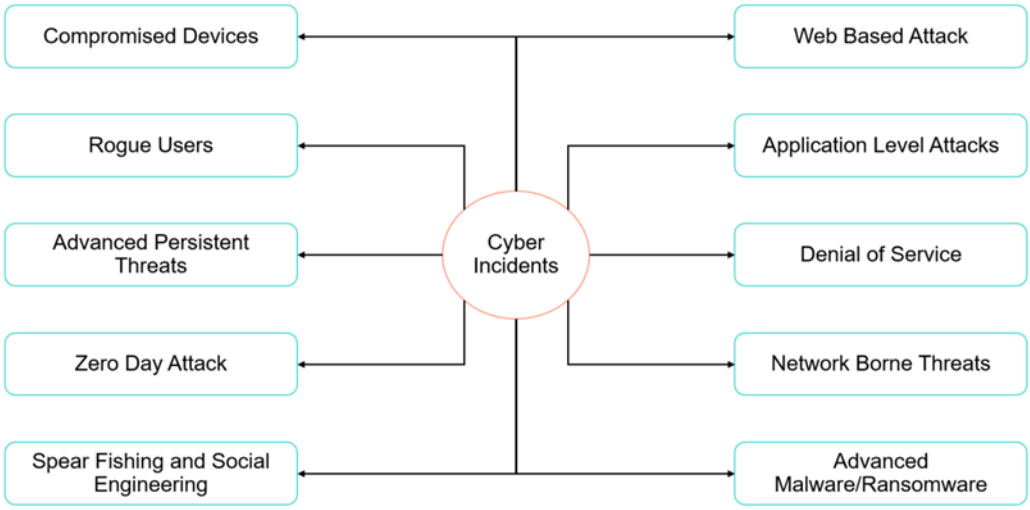


FIGURE 1. Common cybersecurity threats

[2] Source: US Department of Homeland Security "Cyber Incident Reporting – A Unified Message for Reporting to the Federal Government" - https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf

- **Cybercrime:** Any crime that involves the use of a computer and network where the computer is either the target of the crime or used as an accessory to commit a crime.
- **Malware:** Any malicious software designed to cause damage to IT systems, including computer viruses, ransomware, Trojan horses, and spyware.
- **Ransomware:** Malware built to extort money from victims by blocking access to their computers and files until they pay the requested ransom to free up the resource.
- **Spyware:** Malware designed specifically to collect personal information about users without their consent.
- **Social engineering**: A technique used by cyber criminals to manipulate people into revealing confidential and sensitive information. Phishing is one of the most common examples of a social engineering technique to gain access to unauthorized information.
- **Phishing:** A fraudulent attempt to obtain sensitive and confidential information using email or other electronic communication means. The bad actor typically poses as a legitimate user such as an IT employee in order to gain trust and solicit the requested information.
- **DDoS attack:** Attackers target a system or network with an overwhelming number of requests making it more difficult for users to be able to access legitimate services.
- **Botnet:** A network of devices that have been infected with malware to carry out malicious cyber activities such as ransomware and DDoS attacks.

Cybersecurity analytics

Cybersecurity analytics involve analysis of server logs and network logs to find cybersecurity threats and anomalies that could suggest emerging cyber threats. A typical IT network can be mapped showing the relationships and interactions between all of the network hosts, routers and servers in a graphical format. Each device within the network is mapped as a node with the communication traffic between nodes represented as edges in the graph. The analysis of the communication traffic between nodes forms the basis for cybersecurity analytics of the IT network.

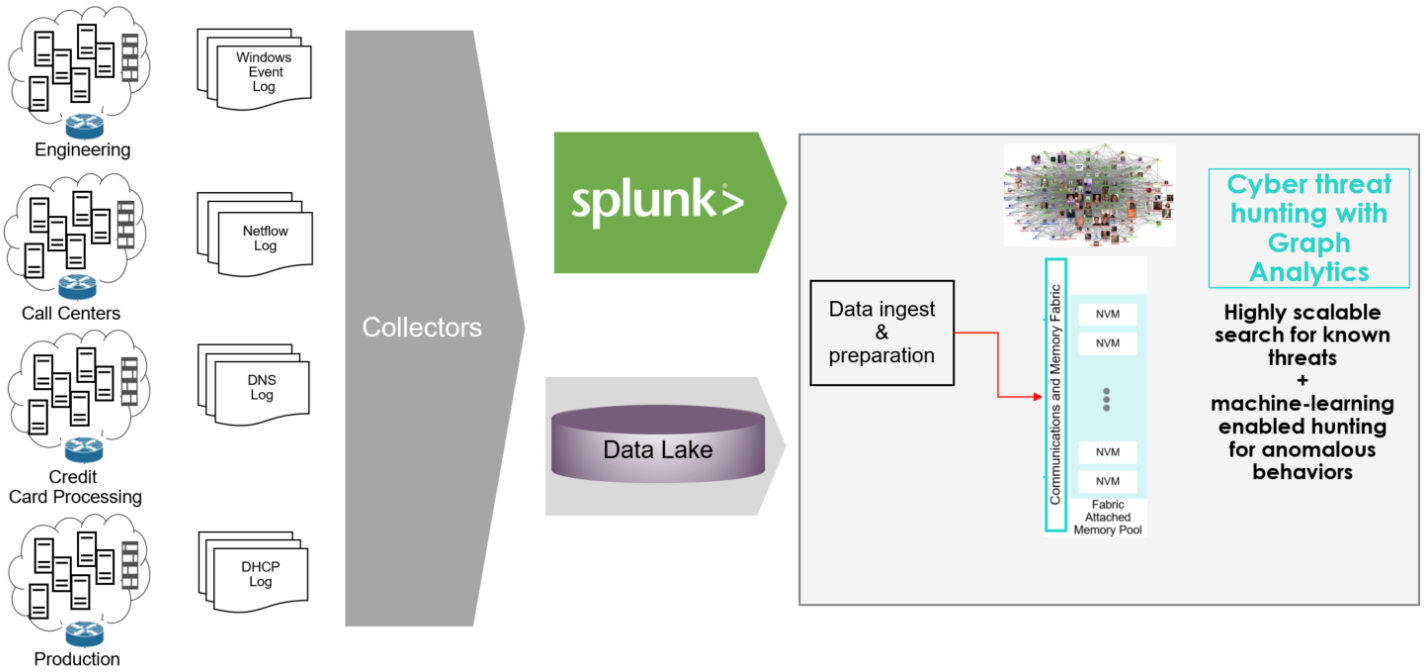


FIGURE 2. Cybersecurity analytics deployment landscape

Typical landscape of cybersecurity analytics includes the following key components:

1. Host and network data from deployed network elements are captured in various logs such as netflow logs, conn logs, DHCP logs, HTTP logs, and so on.
2. Critical data about deployed infrastructure and applications are available in enterprise end-points such as DIR Svcs, Usage Data, CMS, and so on.
3. Data from these multiple sources would be collected for data aggregation and discovery as pre-processing for cybersecurity analytics.
4. Log data is processed to identify cyber network elements and then used to build a cyber network graph representing network elements.
5. Data scientists leverage these graphs to further analyze cybersecurity analytics activities.
6. Cyber threat patterns can then be identified and analyzed to detect cyber intrusion activities.
7. This data is then used to develop pre-trained models in the form of graph queries to subsequently leverage for day-zero threat detection.

Graph analytics

Graphs are mathematical structures used to model many types of entities and relationships in physical, biological, social, and information systems. A graph consists of nodes or vertices (representing the entities in the system) which are connected by edges (representing relationships between those entities). Graphs, however, are more than just nodes and edges; they are powerful data structures you can use to represent complex dependencies in your data. These vertices and edges carry properties describing the characteristics of entities and relationships.

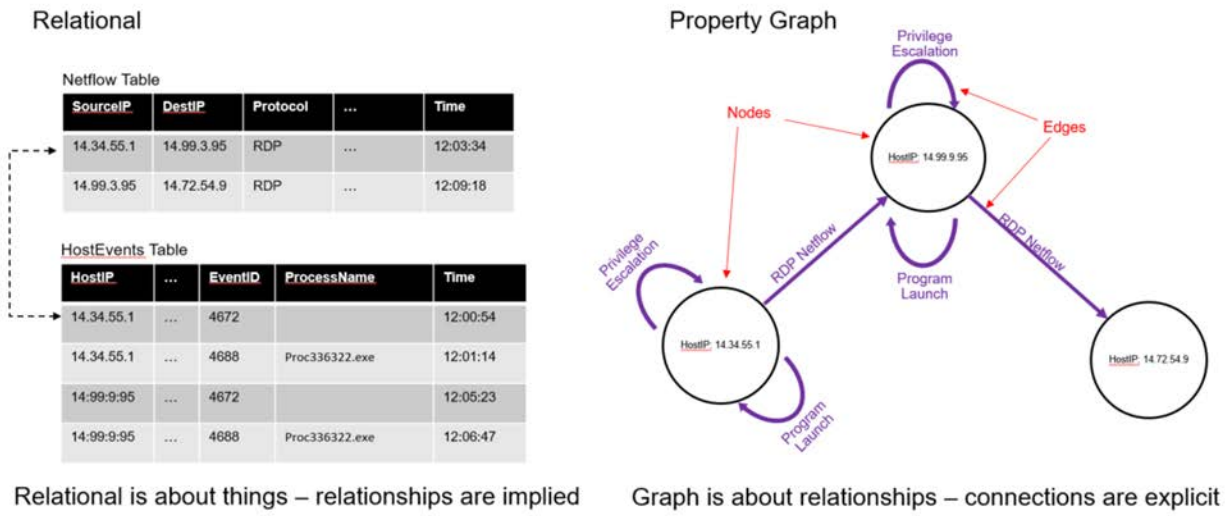


FIGURE 3. Graph representation with entities and relationships

Graph algorithms or graph analytics are analytic tools used to determine strength and direction of relationships between objects in a graph. The focus of graph analytics is on pairwise relationship between two objects at a time and structural characteristics of the graph as a whole.

SOLUTION OVERVIEW

The HPE Cybersecurity Threat Detection Solution combining HPE Superdome Flex with Trovares xGT is designed to complement existing cybersecurity mitigation tools focusing on helping businesses detect cybersecurity threats more quickly than conventional tools. It provides a comprehensive cybersecurity solution that reduces the MTTD to detect and mitigate cybersecurity attacks such as lateral movement threats, command-and-control threats, and data exfiltration.

Cybersecurity graph analytics involves identifying cyber intrusion behaviors in a deployed infrastructure comprised of a complex network of IT infrastructure. Developing a cybersecurity graph analytics model involves analyzing a comprehensive set of IT infrastructure network traffic information from sources such as network logs and establishing a network of infrastructure entities and relationships. This task involves building

a network graph to help with detection of network anomaly patterns which ultimately leads to identifying cybersecurity threats. Schemas which are typical of SQL are used to define how data is ingested into a graph.

The typical size for a large enterprise network graph can reach billions of graph nodes and properties and relationships between graph nodes. Discovering anomaly patterns across these billions of nodes in near real-time requires loading the entire graph in-memory which requires a server with TBs of memory capacity. The HPE Superdome Flex is the ideal server to handle this large in-memory analytics use case.

Cybersecurity graph analytics solution blueprint

Conventional graph tools often limit companies to sampling slices of their log data given the size of the logs which increases the time it takes to analyze and detect cybersecurity threats. Since some enterprise accounts can have a substantial amount of network activity in just a few seconds of their network data logs, not scanning all available data adds risk and increases the chances of not detecting all cybersecurity threats. The costs associated with not detecting and closing active cybersecurity threats can have huge impacts on business operations over time. Therefore, it's imperative that cybersecurity teams deploy solutions that can scan all data within relevant logs to help close the MTTD for these threats to help reduce risk and costs associated with the cybersecurity attacks.

Trovares xGT is a property graph engine that delivers search queries hundreds of times faster than the conventional graph tools with near linear scalability and high degrees of parallelism for true high performance computing. Trovares has optimized the xGT engine around HPE Superdome Flex's SMP capabilities which makes it the ideal graph engine to handle your larger in-memory compute needs. With rapid ingest rates and the ability to execute complex queries driven by Python scripts, Trovares xGT provides unprecedented performance and scalability, especially when processing very large data.

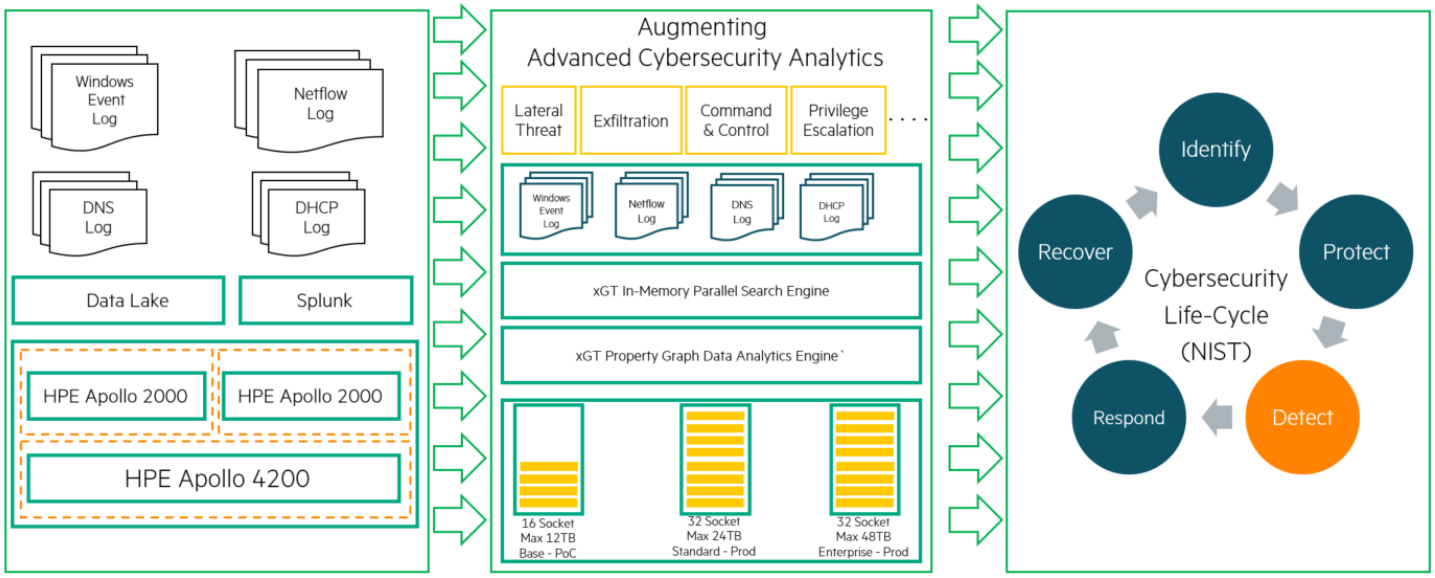
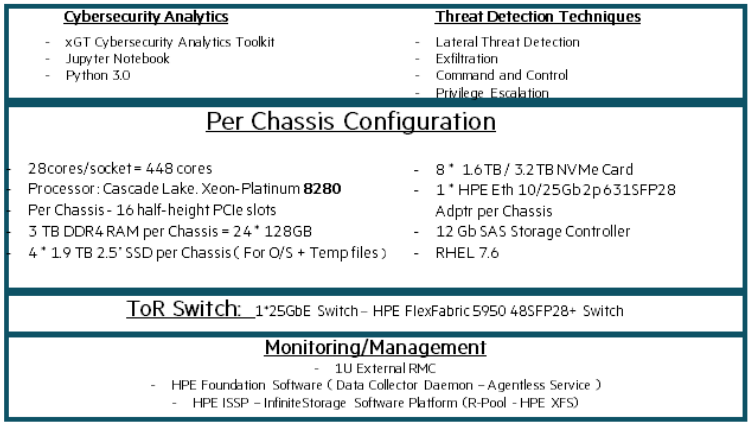


FIGURE 4. Cybersecurity graph analytics with Trovares xGT on HPE Superdome Flex solution architecture

Figure 5 provides the graph analytics software framework and infrastructure foundation needed for anomaly detection to detect wide range of cybersecurity threat patterns.

The configuration outlined in Figure 5 are driven by size of cyber network graph and threat pattern anomaly detection requirements.



	Base Configuration	Standard Configuration	Enterprise Configuration
Scaling Cyber Graphs (Typical)	3B Vertices / 30B Edges / 300B Properties	6B Vertices / 60B Edges / 600B Properties	6B Vertices / 60B Edges / 600B Properties
Total Sockets	16	32	32
Total Cores	448	896	896
Total Memory (TB)	12	24	48
Total Storage NVME (TB)	50	100	200

FIGURE 5. Reference Configuration – Cybersecurity analytics with Trovares xGT graph analytics on HPE Superdome Flex

SOLUTION COMPONENTS

Trovares xGT cybersecurity graph analytics toolkit

Trovares offers a new type of graph analytics tool which returns search queries hundreds of times faster than the conventional graph tools. It supports extremely large in-memory graphs for faster queries. Designed around SMP architecture like the HPE Superdome Flex, the Trovares xGT engine delivers maximum performance for cyber, fraud detection, government, and other graph analytics use cases.

The Trovares xGT engine has high degrees of parallelism and is optimized around supercomputing techniques such as extreme multi-threading and fine-grain locks to deliver near-linear speed and scale for graphs with up to billions of edges. This enables the HPE Cybersecurity Threat Detection Solution with HPE Superdome Flex and Trovares xGT to keep pace with your data growth needs.

HPE Superdome Flex Server

The HPE Superdome Flex Server is a compute breakthrough that can power critical applications, accelerate data analytics, and tackle AI and HPC workloads holistically. It delivers an unmatched combination of flexibility, performance, and reliability for critical environments of any size. With a unique modular scale-up architecture utilizing a 4-socket building block, it lets you start small and grow at your own pace.

The HPE Superdome Flex delivers extreme and proven Superdome RAS features for highest service levels. HPE Serviceguard for Linux delivers high availability and disaster recovery capabilities and HPE Pointnext Services and expertise lowers your risk for the best mission-critical experience. The HPE Superdome Flex is designed for the future based on Memory-Driven Computing design principles to boost analytics performance:

- Modular architecture that scales seamlessly from 4- to 32-sockets in 4-socket increments in a single system
- Up to 896 cores and 1,792 threads for faster graph analytics operations

- Shared memory capacity from 768GB up to 48TB
- Features Intel® Xeon® Scalable processors 1st or 2nd generation
- Proven RAS capabilities not available on other standard platforms
- Best-in-class predictive fault-handling analysis engine, predicts hardware faults and initiates self-repair without operator assistance
- Firmware First approach to log analysis ensures error containment at the firmware level, including memory errors, before any interruption can occur at the OS layer
- Mission-critical resiliency from end-to-end implementation of processor RAS features, to redundancy of key system components to advanced system software

With the SMP capabilities of HPE Superdome Flex, all processes within the Trovares xGT graph engine access the shared memory within a single OS image and can read and write memory at internal system speeds with no network latency. These features along with Trovares xGT graph engine's high degree of parallelism and multi-threading capability make the HPE Superdome Flex the ideal server for this cybersecurity solution.

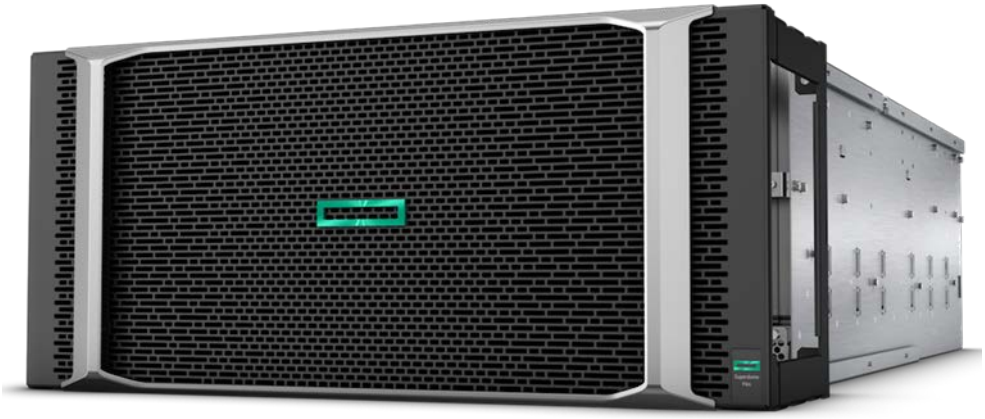


FIGURE 6. HPE Superdome Flex chassis

HPE OneView

HPE OneView is a converged infrastructure management platform that provides a unified interface for the administration of systems in a data center. Through a single GUI—sometimes referred to as a single pane of glass—administrators can automate management and maintenance tasks that have traditionally been performed manually and required several different tools. Within the data center, HPE OneView can manage physical systems, storage arrays, and network connectivity. HPE OneView is licensed to enable functionality in two modes, Monitor mode and Managed mode. HPE OneView will automatically enable the license for Managed mode if HPE OneView is version 5.0 or newer and HPE Superdome Flex firmware is version 3.0.x or newer. Please refer to HPE Superdome Flex Server Manageability for more details.

NOTE

HPE OneView standard and advanced licenses are included with the purchase of a HPE Superdome Flex Server.

Hardware

Table 1 shows the hardware components deployed for this solution.

TABLE 1. Solution hardware components

Component	Description
1U External RMC	HPE Superdome Flex Server complex contains one or more HPE Superdome Flex Server chassis in a rack that each contain individual compute, memory, networking, and storage resources. An nPartition is created and managed using the Rack Management Controller (RMC).
HPE Superdome Flex 4-socket Base Chassis	A chassis that includes BaseIO in the hardware that provides drive bays, network ports, and USB ports
HPE Superdome Flex 4-socket Expansion Chassis	An add-on chassis to scale-up the capacity of a non-partitionable system
HPE FlexFabric 5950 Switch	Top-of-the-rack Data Center Network Switch
HPE NVMe x8 Lanes Mixed Use	High performance NVMe drives for data storage for cybersecurity graph analytics

TABLE 2. Solution server components – base and expansion chassis

Component	Description
Processor	Four 28-core Intel Xeon 8280 processors at 2.70GHz
Memory	3TB memory (24 x 128GB HPE DDR4 SmartMemory LRDIMMs)
Built-in Network Adapters	1 x 10 Gb dual port Ethernet adapter, 1 x 1GbE dual port Ethernet adapter
Additional Network Adapters	1 x 10/25 Gb dual port 631SFP28 Ethernet adapter
OS disk	4 x 1.9 TB SSD
Data disk	8 x HPE 1.6 TB NVMe x8 MU HH DS Card

Software

Table 3 shows the software components deployed for this solution.

TABLE 3. Solution software components

Component	Description
Red Hat 7.6	Linux Distro
Open JDK 1.8	Java Development Kit
Python 3.0	Compatible Python runtime for Interactive Notebook and graph analytics
HPE ISSP	Infinite storage software platform
Jupyter iPython Notebook	Interactive Notebook for cybersecurity graph analytics
SAR Analyzer	Performance analyzer for CPU, memory, network, I/O utilization

Application software

Table 4 shows the application software deployed for this solution.

TABLE 4. Application components

Quantity	Description
Trovares xGT 1.3	Graph analytics toolkit

PROOF-OF-CONCEPT SOLUTION IMPLEMENTATION

The following section describes a cybersecurity graph analytics use case implemented with Trovares xGT deployment on HPE Superdome Flex.

Use Case: Detecting network anomalies by identifying zombie reboot and RDP hacking events

The HPE Cybersecurity Threat Detection Solution can be deployed to identify cyber threats in large enterprise organizations. The use case considered here is to detect network anomalies by identifying zombie reboot and RDP hacking events in a deployed enterprise network. The attack pattern for these types of network hacks are called lateral movement attacks.

A lateral movement is a cyberattack pattern that describes how a bad actor leverages a single successful infiltration within a network to compromise other systems within that network. Identifying and stopping lateral movement attacks in a timely manner is an important step in controlling the potential damage in terms of cost and reputation from a data breach. It also plays an important role in forensic analysis of a cyberattack to help identify its source and structure to help prevent similar future attacks.

RDP hijacking is actually a family of attacks, each with different characteristics on how to obtain the privileges required to perform the RDP hijacking. The attack broadly looks like this:

1. Lateral movement attack starts from a foothold where a bad actor already has gained access. This is represented as host A in Figure 7.
2. The attacker uses some privilege escalation technique to obtain an important system privilege.
3. The attacker then leverages their system privilege to perform a hijack operation enabling them to move through a network to another vulnerable system. The result is logged in another system where the RDP attack occurred. This is represented as host B in Figure 7.
4. This hijacking operation can be repeated to form longer chains of lateral movement attacks to various other systems (see host C in Figure 7). These chains of attacks can be detected and represented as graph patterns.

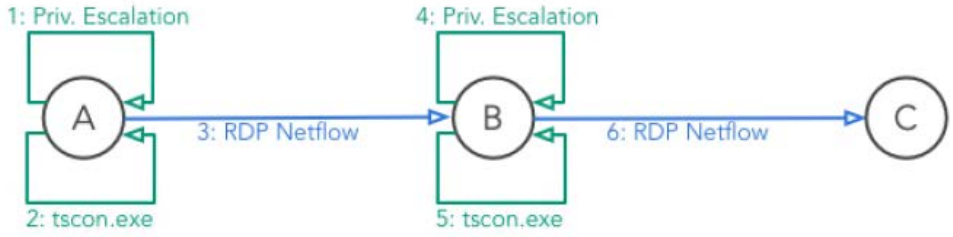


FIGURE 7. RDP hacking lateral movement attack pattern

The following steps are required for detecting network anomalies using the HPE Cybersecurity Threat Detection Solution:

1. The Trovares xGT engine reads data into memory from desired network and data logs for performing fast pattern search operation. The data load can be achieved leveraging the load function in the Trovares xGT module.
2. The data is then represented in the form of an in-memory graph model (local structure) with each vertex uniquely identifying cyber network elements and devices represented by vertex_frames. The connection between these devices represents network traffic and the relationships are represented as edges which carry properties representing the nature of network traffic represented by edge_frames.
3. Trovares Query Language (TQL) uses a subset of cypher language to express queries. Trovares xGT offers strongly typed graph elements (fixed schema) with cypher language-based TQL. Typical query subset is represented as follows:

```
MATCH <structure>
WHERE <optional constraints or properties>
SET <optional property modifications>
MERGE <optional addition of vertices>
CREATE <optional addition of vertices and edges>
DETACH DELETE <optional deletion of vertices>
DELETE <optional deletion of edges>
RETURN <description of answer set>
INTO <results table name>
```

The steps involved in detection of zombie reboot and RDP hacking events for the identifying cyber network attack are as follows:

1. A 2-chassis single partition environment was created in the HPE Superdome Flex system and RHEL 7.6 was installed and repositories were configured to implement Trovares xGT graph analytics toolkit.
2. Ingest host and network log data and persist into fast storage media implemented with NVMe drives in HPE Superdome Flex.
3. Data loading is performed using load function available in Trovares xGT. Aggregated data is transformed into a graph data model and a network graph is built to represent these network entities with vertex_frames and edge_frames.
4. 90 Days of netflow event and host event data are loaded and transformed in graph data model in Trovares xGT creating a network graph of 20 billion graph edges (17.9 billion netflow edges and 1.5 billion log edges) and 212 billion graph edge properties against 3TB of input data from network.
5. Interactive query operation is performed to detect bot-net behavior over network.
   a. Extract the forward RDP edges.
   b. Extract the reverse RDP edges.
   c. Extract the RDPFlow edge frames.
   d. Build temporal constraints in RDPFlow edge frames.

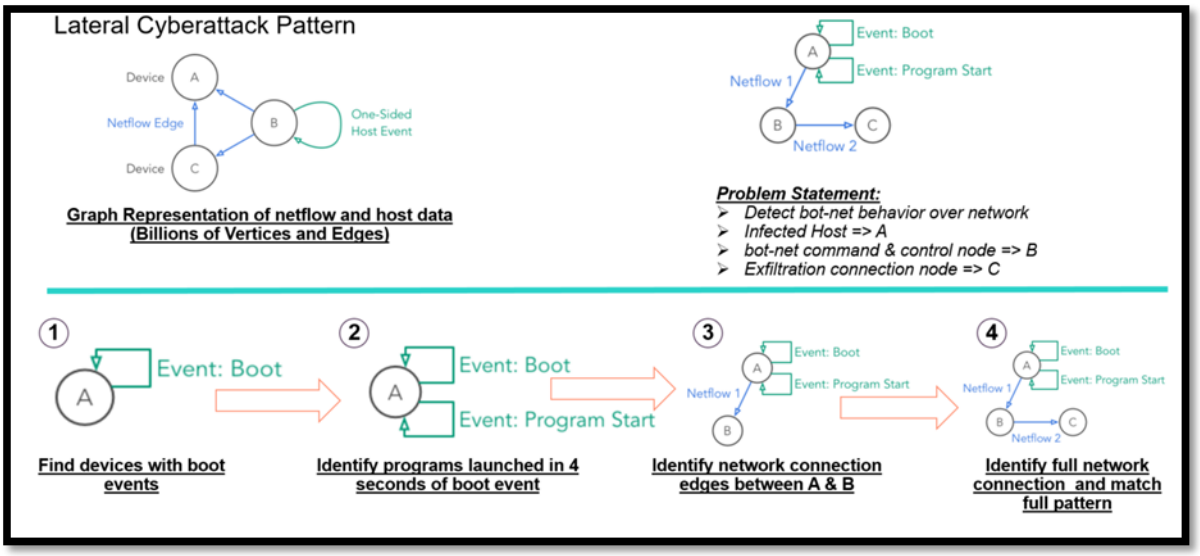


FIGURE 8. Detect RDP cyber-attack pattern with Trovares xGT graph analytics toolkit

Scaling lateral movement cyber threat detection

The LANL Unified Host and Network Dataset, a set of netflow and host event data collected on an internal Los Alamos National Lab network, will be used for this example.

Our goal is to turn about 1.5TB of CSV files into a single connected graph. A cybersecurity analyst should provide the criteria for detecting specific cyber threat patterns. Subgraph Isomorphism or pattern matching is performed on large memory graphs and sub-graphs are queried to detect infected host systems.

The LANL Unified Host and Network Dataset is a subset of network and computer (host) events collected from the Los Alamos National Laboratory enterprise network over the course of approximately 90 days. The host event logs originated from most enterprise computers running the Microsoft Windows operating system on Los Alamos National Laboratory's (LANL) enterprise network. The network event data originated from many of the internal enterprise routers within the LANL enterprise network.

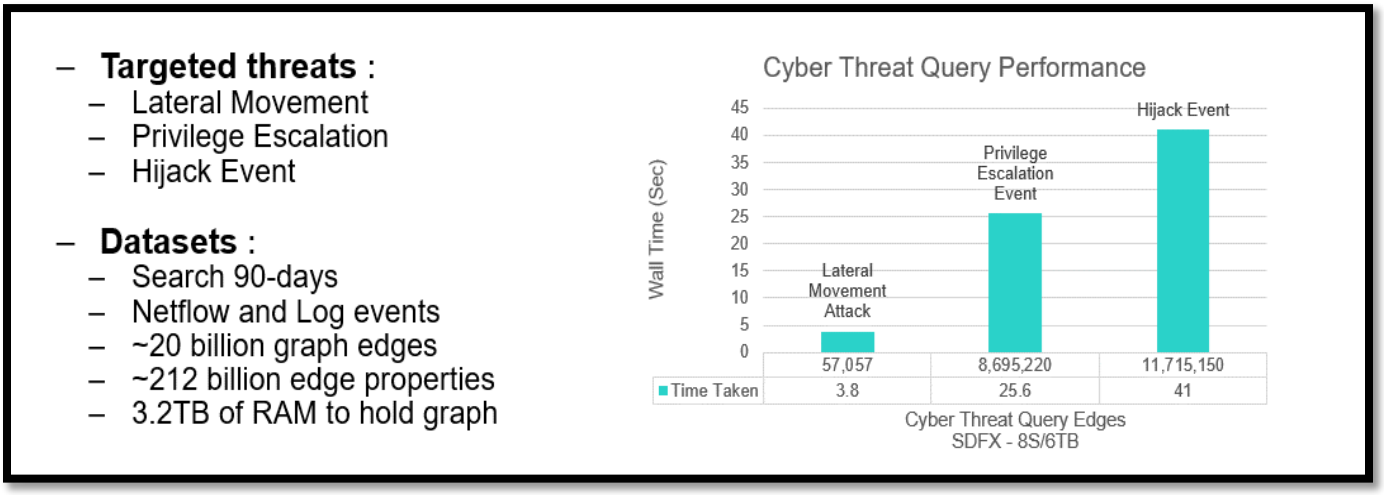


FIGURE 9. Cybersecurity threat detection with Trovares xGT on HPE Superdome Flex

Figure 9 highlights the performance scalability of lateral movement cyber-attack detection:

- 90 Days of host event logs and network logs were processed and transformed into cyber network graph representing 933,714 devices and ~20 billion graph edges.
- The in-memory graph required 3TB of memory to hold the entire graph with >90% CPU utilization.
- Lateral movement attack query was executed to detect affected network edges. 57,057 network edges were detected from among ~20 billion graph edges.
- Cyber threat detection time:
  - Data preparation: 136 seconds
  - Privilege escalation event: 25.6 seconds
  - Hijack event: 41 seconds
  - Lateral movement attack: 3.8 seconds
  - Total query execution time took 207 seconds to complete

SUMMARY

The HPE Cybersecurity Threat Detection Solution combining HPE Superdome Flex with Trovares xGT is designed to complement existing cybersecurity mitigation tools focusing on helping businesses detect cybersecurity threats more quickly than conventional tools. This document provides a Reference Configuration for deploying Trovares xGT on HPE Superdome Flex infrastructure and management software. These configurations leverage HPE servers, storage and networking, along with integrated management software and bundled support. In addition, this document has been created to assist in the rapid design and deployment of cyber graphs on HPE Superdome Flex.

Implementing a proof-of-concept

As a matter of best practice for all deployments, Hewlett Packard Enterprise recommends implementing a proof-of-concept (POC) using a test environment that matches as closely as possible the planned production environment. In this way, appropriate performance and scalability characterizations can be obtained. For help with a POC, contact a Hewlett Packard Enterprise Services representative (hpe.com/us/en/services/consulting.html) or your Hewlett Packard Enterprise partner.

APPENDIX A: BILL OF MATERIALS

NOTE

Part numbers are at time of publication/testing and subject to change. The bill of materials does not include complete support options or other rack and power requirements. If you have questions regarding ordering, please consult with your Hewlett Packard Enterprise Reseller or Hewlett Packard Enterprise Sales Representative for more details at hpe.com/us/en/services/consulting.html.

TABLE A1. Bill of materials – Base Configuration: Designed for POC for HPE Cybersecurity Threat Detection Solution

Quantity	Part number	Description
1	M0S66A	HPE Virtual Rack
1	Q2N05B	HPE Superdome Flex 4-socket Base Chassis
4	R0W99A	HPE Superdome Flex Intel Xeon-Platinum 8280 (2.7GHz/28-core/205W) Processor Kit
24	R0X07A	HPE Superdome Flex 128GB (1x128GB) Quad Rank x4 DDR4-2933 Load Reduced Memory Kit
4	R2A74A	HPE 1.92TB SATA 6G Mixed Use SFF (2.5in) RW 3yr Wty Digitally Signed Firmware SSD
1	Q2N09A	HPE Superdome Flex PCIe Low Profile 16-slot 4 Riser Configuration Kit
1	Q2N41A	HPE Superdome Flex DVD-RW Drive
1	817718-B21	HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter
8	P10264-H21	HPE 1.6TB NVMe x8 Lanes Mixed Use HHHL 3yr Wty Digitally Signed Firmware Card
3	Q6L89B	HPE Superdome Flex 4-socket Partition Expansion Chassis
12	R0W99A	HPE Superdome Flex Intel Xeon-Platinum 8280 (2.7GHz/28-core/205W) Processor Kit
72	R0X07A	HPE Superdome Flex 128GB (1x128GB) Quad Rank x4 DDR4-2933 Load Reduced Memory Kit
12	R2A74A	HPE 1.92TB SATA 6G Mixed Use SFF (2.5in) RW 3yr Wty Digitally Signed Firmware SSD
3	Q2N09A	HPE Superdome Flex PCIe Low Profile 16-slot 4 Riser Configuration Kit
3	Q2N41A	HPE Superdome Flex DVD-RW Drive
3	817718-B21	HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter
24	P10264-H21	HPE 1.6TB NVMe x8 Lanes Mixed Use HHHL 3yr Wty Digitally Signed Firmware Card
1	Q9Z05A	HPE Superdome Flex 16-socket Interconnect and Partition Activation Kit
1	Q2N07A	HPE Superdome Flex Rack Management Controller
4	Q7N11A	HPE Foundation Software 2 for Red Hat Enterprise Linux Media License RTU

TABLE A2. Bill of materials – Standard Configuration: Designed for scaling from Development to Production deployment of HPE Cybersecurity Threat Detection Solution

Quantity	Part number	Description
1	M0S66A	HPE Virtual Rack
1	Q2N05B	HPE Superdome Flex 4-socket Base Chassis
4	R0W99A	HPE Superdome Flex Intel Xeon-Platinum 8280 (2.7GHz/28-core/205W) Processor Kit
24	R0X07A	HPE Superdome Flex 128GB (1x128GB) Quad Rank x4 DDR4-2933 Load Reduced Memory Kit
4	R2A74A	HPE 1.92TB SATA 6G Mixed Use SFF (2.5in) RW 3yr Wty Digitally Signed Firmware SSD
1	Q2N09A	HPE Superdome Flex PCIe Low Profile 16-slot 4 Riser Configuration Kit
1	Q2N41A	HPE Superdome Flex DVD-RW Drive
1	817718-B21	HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter
8	P10264-H21	HPE 1.6TB NVMe x8 Lanes Mixed Use HHHL 3yr Wty Digitally Signed Firmware Card
7	Q2N06B	HPE Superdome Flex 4-socket Expansion Chassis
28	R0W99A	HPE Superdome Flex Intel Xeon-Platinum 8280 (2.7GHz/28-core/205W) Processor Kit
168	R0X07A	HPE Superdome Flex 128GB (1x128GB) Quad Rank x4 DDR4-2933 Load Reduced Memory Kit
7	Q2N09A	HPE Superdome Flex Rack Management Controller
7	817718-B21	HPE Superdome Flex PCIe Low Profile 16-slot 4 Riser Configuration Kit
56	P10264-H21	HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter
1	Q2N20A	HPE 1.6TB NVMe x8 Lanes Mixed Use HHHL 3yr Wty Digitally Signed Firmware Card
1	Q2N07A	HPE Superdome Flex 32-socket Interconnect and Scale Activation Kit

TABLE A3. Bill of materials – Enterprise Configuration: Designed for large scale production deployment of HPE Cybersecurity Threat Detection Solution

Quantity	Part number	Description
1	M0S66A	HPE Virtual Rack
1	Q2N05B	HPE Superdome Flex 4-socket Base Chassis
4	R0X00A	HPE Superdome Flex Intel Xeon-Platinum 8280M (2.7GHz/28-core/205W) Processor Kit
48	R0X07A	HPE Superdome Flex 128GB (1x128GB) Quad Rank x4 DDR4-2933 Load Reduced Memory Kit
4	R2A74A	HPE 1.92TB SATA 6G Mixed Use SFF (2.5in) RW 3yr Wty Digitally Signed Firmware SSD
1	Q2N09A	HPE Superdome Flex PCIe Low Profile 16-slot 4 Riser Configuration Kit
1	Q2N41A	HPE Superdome Flex DVD-RW Drive
1	817718-B21	HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter
8	P10266-H21	HPE 3.2TB NVMe x8 Lanes Mixed Use HHHL 3yr Wty Digitally Signed Firmware Card
7	Q2N06B	HPE Superdome Flex 4-socket Expansion Chassis
28	R0X00A	HPE Superdome Flex Intel Xeon-Platinum 8280M (2.7GHz/28-core/205W) Processor Kit
336	R0X07A	HPE Superdome Flex 128GB (1x128GB) Quad Rank x4 DDR4-2933 Load Reduced Memory Kit
7	Q2N09A	HPE Superdome Flex PCIe Low Profile 16-slot 4 Riser Configuration Kit
7	817718-B21	HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter
56	P10266-H21	HPE 3.2TB NVMe x8 Lanes Mixed Use HHHL 3yr Wty Digitally Signed Firmware Card
1	Q2N20A	HPE Superdome Flex 32-socket Interconnect and Scale Activation Kit
1	Q2N07A	HPE Superdome Flex Rack Management Controller

RESOURCES AND ADDITIONAL LINKS

HPE Reference Architectures, https://www.hpe.com/docs/reference-architecture

HPE Superdome Flex Servers: https://www.hpe.com/us/en/servers/superdome.html

HPE Superdome Flex manageability: https://h20195.www2.hpe.com/v2/GetDocument.aspx?docname=a50000335enw

Trovares: trovares.com

Trovares xGT trial software and training documentation: http://docs.trovares.com/1.3.1/

"Trovares Drives Memory-Driven, Property Graph Analytics Strategy with HPE", HPC wire: https://www.hpcwire.com/2019/10/10/trovares-memory-driven-property-graph-analytics-strategy-hpe/

"Accelerate cyber-threat detection with Trovares and HPE Superdome Flex" podcast: https://www.hpe.com/h22228/video-gallery/us/en/700000804/EN/US/e1447a78-ae42-451f-bc5c-cb58324dabff/accelerate-cyber_threat-detection-with-trovares-and-hpe-superdome-flex/video?lang=en-US

HPE OneView: www.hpe.com/info/oneview

HPE GreenLake Advisory and Professional Services, https://www.hpe.com/us/en/services/consulting.html

6-cybersecurity Mega Trends: https://www.hpe.com/us/en/insights/articles/6-security-megatrends-1905.html

Memory-Driven Computing in Superdome Flex: https://www.hpe.com/us/en/newsroom/blog-post/2017/05/memory-driven-computing-explained.html

Mission critical Infrastructure for Data Driven Enterprise: https://www.hpe.com/hpe-external-resources/a00037000-7999/enw/a00037029?resourceTitle=Mission-critical+infrastructure+for+the+data-driven+enterprise

HPE Performance Cluster Manager: http://www.hpe.com/software/hpcm

HPE Education Services: http://h10076.www1.hpe.com/ww/en/training/portfolio/bigdata.html

To help us improve our documents, please provide feedback at hpe.com/contact/feedback.

© Copyright 2020, 2021 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

MITRE ATT&CK is a registered trademark of The MITRE Corporation. Intel and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

a50001908enw, May 2021