Admin Guides

Published: 2018-11-09

Discover Appliance

- ExtraHop Admin UI Guide
- ExtraHop Command-line Reference
- Discover and Command Post-deployment Checklist
- Configure ERSPAN with the Nexus 1000V
- Configure ERSPAN with VMware
- Configure RSPAN with VMware
- Configure Packet Capture on the ExtraHop Discover Appliance with VMware
- Configure the iDRAC Remote Access Console
- Repair a Degraded RAID 10 Configuration on the EH8000
- Analyze Lync Traffic
- Add a CPU Core to an EDA 1000v on Hyper-V
- Add a CPU Core to the EDA 1000v with VMware
- Apply an MS SQL Key to the ExtraHop System
- Install the SSL Decryption Board
- Install an SSD for Packet Capture on the ExtraHop Discover Appliance
- Port Channeling
- Packet Forwarding with RPCAP
- Configure RPCAP for a Trace Appliance
- Replace the Datastore Hard Drive
- Replace the firmware disk in an ExtraHop Discover appliance
- ExtraHop Rescue Media Guide
- Troubleshoot your connection to ExtraHop Cloud Services
- Upgrade from RAID 0 to RAID 10
- ExtraHop Open Data Stream for ELK

Command Appliance

- ExtraHop Admin UI Guide
- Discover and Command Post-deployment Checklist

Explore Appliance

- ExtraHop Explore Admin UI Guide
- Explore Post-deployment Checklist

Trace Appliance

- Introduction to the ExtraHop Trace Admin UI
- Trace Post-deployment Checklist

API Guides

Published: 2018-11-09

REST API

- ExtraHop REST API Guide
- ExtraHop Explore REST API Guide
- ExtraHop Trace REST API Guide

Trigger API

- ExtraHop Trigger API Reference
- Triggers Best Practices Guide

Concepts

Published: 2018-11-09

System Overview

- Introduction to the ExtraHop system
- Introduction to the ExtraHop Web UI

Metrics, records, and packets

- Metrics
- Records
- Packets
- Triggers

Data monitoring

- Dashboards
- Chart types
- Activity dashboard
- Network dashboard
- Security dashboard - Reveal(x) only
- Security Overview - Reveal(x) only
- Alerts

Data analysis and investigation

- Time intervals
- Analysis priorities
- Detections
- Activity maps
- Geomaps
- Threat intelligence - Reveal(x) only

ExtraHop administration and configuration

- System health
- Users and user groups
- Backup and restore
- Local and extended datastores
- Open Data Streams
- Bundles

Deployment

Published: 2018-11-09

Discover Appliance

- Deploy the ExtraHop Discover 10200 Appliance
- Deploy the ExtraHop Discover 9200 Appliance
- Deploy the ExtraHop Discover 8200 Appliance
- Deploy the ExtraHop Discover 6200 Appliance
- Deploy the ExtraHop Discover EDA 3100, EDA 6100, EDA 8100, or EDA 9100 Appliances
- Deploy the ExtraHop Discover EH3000, EH6000, or EH8000 Appliances
- Deploy the ExtraHop Discover Appliance 1100
- Deploy the ExtraHop Discover Appliance in AWS
- Deploy the ExtraHop Discover Appliance in Azure
- Deploy the ExtraHop Discover Appliance with Hyper-V
- Deploy the ExtraHop Discover Appliance on a Linux KVM
- Deploy the ExtraHop Discover Appliance with VMware
- Discover and Command Post-deployment Checklist
- Deploy ERSPAN with the ExtraHop Discover Appliance and Brocade 5600 vRouter in AWS
- Session key forwarding from an F5 LTM
- Install the ExtraHop session key forwarder on a Windows server
- Install the ExtraHop session key forwarder on a Linux server
- Install an SSD for Packet Capture on the ExtraHop Discover Appliance
- Replace 120 GB Packet Capture SSD with 480 GB SSD in the Discover Appliance
- Replace the firmware disk in an ExtraHop Discover appliance
- Integrate ExtraHop with AWS CloudFormation
- Integrate ExtraHop with Splunk
- Discover and Command Post-deployment Checklist

Command Appliance

- Deploy the ExtraHop Command Appliance in AWS
- Deploy the ExtraHop Command Appliance in Azure
- Deploy the ExtraHop Command Appliance with Hyper-V
- Deploy the ExtraHop Command Appliance on a Linux KVM
- Deploy the ExtraHop Command Appliance with VMware
- Discover and Command Post-deployment Checklist

Explore Appliance

- Deploy the ExtraHop Explore 5200 Appliance
- Deploy the ExtraHop Explore 5100 Appliance
- Deploy the ExtraHop Explore Appliance in AWS
- Deploy the ExtraHop Explore Appliance in Azure
- Deploy the ExtraHop Explore Appliance on a Linux KVM
- Deploy the ExtraHop Explore Appliance with VMware
- Increase the capacity of your ExtraHop Explore cluster in VMware
- Explore Post-deployment Checklist

Trace Appliance

- Deploy the ExtraHop Trace 8250 Appliance

- Deploy the ExtraHop Trace 6150 Appliance
- Deploy the ExtraHop Trace Appliance in AWS
- Deploy the ExtraHop Trace Appliance in Azure
- Deploy the ExtraHop Trace Appliance with VMware
- ExtraHop Trace Post-deployment Checklist
- Add storage capacity to the ExtraHop Trace appliance

FAQs

Published: 2018-11-09

How To's

Published: 2018-11-09

Activity Maps

- Create an activity map
- Save and share an activity map
- Load and manage a saved activity map

Admin

- Configure a static IP address through the CLI
- Add a local user account
- Configure remote authentication through LDAP
- Configure remote authentication through RADIUS
- Configure remote authentication through TACACS+
- Manage imported LDAP user groups
- Register your ExtraHop appliance
- Configure the system time
- Upgrade the firmware on your ExtraHop appliance
- Connect to Atlas services
- Create a certificate signing request from your ExtraHop appliance
- Add a trusted certificate to your ExtraHop appliance
- Send audit log data to a remote syslog server
- Configure email settings for notifications
- Configure settings to send notifications to an SNMP manager
- Send system notifications to a remote syslog server
- Configure license expiration notifications for Discover and Command appliances
- Configure the Discover appliance to collect traffic from NetFlow and sFlow devices
- Set up shared SNMP credentials for your NetFlow or sFlow networks
- Save system settings to the running config file
- Download the running config as a text file
- Reset the local datastore and remove all device metrics from the Discover appliance
- Calculate the size needed for your extended datastore
- Configure an extended CIFS or NFS datastore
- Archive an extended datastore for read-only access
- Troubleshoot issues with the extended datastore
- Create an Explore cluster
- Connect the Discover and Command appliances to Explore appliances
- Connect the Discover and Command appliances to the Trace appliance
- Install the ExtraHop session key forwarder on a Windows server
- Install the ExtraHop session key forwarder on a Linux server
- Configure the iDRAC IP address with a monitor, keyboard, and mouse
- Import external data to your Discover appliance
- Configure an HTTP target for an open data stream
- Configure a Kafka target for an open data stream
- Configure a MongoDB target for an open data stream
- Configure a raw data target for an open data stream
- Configure a syslog target for an open data stream
- Back up a Discover or Command appliance

- Restore a Discover or Command appliance from a system backup
- Restore a Discover or Command appliance from a backup file
- Migrate settings to a new Command or Discover appliance
- Run a support script
- Upload a threat intelligence collection to ExtraHop Reveal(x)
- Enable network overlay decapsulation
- Discover new devices by IP address
- Integrate ExtraHop with Splunk
- Increase the capacity of your ExtraHop Explore cluster in VMware
- Disable record ingest on an Explore cluster

Alerts

- Configure detection alert settings
- Configure threshold alert settings
- Configure trend alert settings
- Assign an alert configuration to a source
- Add a notification to an alert configuration
- Add Markdown to an alert description
- Create an exclusion interval for alerts

Applications

- Create an application through the Web UI
- Create an application through the Trigger API

Bundles

- Install a bundle
- Create a bundle
- Post a bundle to the ExtraHop website

Charts

- Create a chart
- Copy a chart
- Edit a chart with the Metric Explorer
- Drill down
- Export data
- Display a rate or count in a chart
- Display percentiles or a mean in a chart
- Edit metric labels in a chart legend
- Add a dynamic baseline to a chart
- Add a static threshold line to a chart
- Display device group members in a chart
- Create regular expression filters in a chart
- Find all devices talking to external IP addresses
- Monitor a device for external IP address connections

Custom Metrics

- Create a custom metric
- Delete a custom metric

Dashboards

- Create a dashboard
- Copy a dashboard
- Display a dashboard in a NOC or SOC
- Create a dashboard with dynamic sources
- Edit a dashboard layout
- Edit a chart with the Metric Explorer
- Edit a text box widget
- Edit a dashboard region
- Change the time interval for a dashboard region
- Edit dashboard properties
- Present a dashboard
- Share a dashboard
- Share a dashboard with a restricted user
- Export data
- Create a PDF file
- Organize custom and shared dashboards

Detections

- Connect to ExtraHop Cloud Services
- Investigate detections
- Share a detection
- Troubleshoot your connection to ExtraHop Cloud Services
- Configure ticket tracking for detections

Devices

- Find a device
- Create a device group
- Create a device group based on discovery time
- Remove devices from a static device group
- Change a device name
- Change a device role
- Create a tag
- Add a tag to a device
- Create a custom device
- Delete or disable custom devices
- Migrate pseudo devices to custom devices
- Prioritize groups for Advanced Analysis
- Prioritize groups for Standard Analysis
- Add a device to the watchlist
- Remove a device from the watchlist
- Transfer management of analysis priorities for a Discover appliance
- Specify the locality for IP addresses

General

- Create a scheduled report
- Change a scheduled report
- Disable or delete a scheduled report
- Export data

- Create a PDF file
- Compare time intervals to find the metric delta
- Zoom in on a custom time range
- Freeze the time interval to create a custom time range
- Set a global display theme
- Enable or disable detection markers

Geomaps

- Generate a geomap

Packet Capture

- Configure global packet capture
- Analyze a packet capture file on the Discover appliance
- Filter packets with Berkeley Packet Filter syntax
- Store SSL session keys on connected Trace appliances
- Download session keys with packet captures

Records

- Collect flow records
- Collect L7 records
- Collect custom records
- Query for stored records on an Explore appliance from a Discover or Command appliance
- Enable record queries for custom metrics

REST API

- Change a dashboard owner through the REST API
- Create custom devices through the REST API
- Extract metrics through the REST API
- Extract the device list through the REST API
- Tag a device through the REST API
- Upload STIX files through the REST API to Reveal(x)
- Create a trusted SSL certificate through the REST API
- Update system health REST API scripts

Triggers

- Build a trigger
- Monitor trigger performance

User Guides

Published: 2018-11-09

- ExtraHop Web UI Guide
- Protocol Metrics Reference
- Default Port Specifications Reference
- ExtraHop Glossary
- Bundles Best Practices Guide
- How Mirroring Works
- ExtraHop Security, Privacy, and Trust Overview

Walkthroughs

Published: 2018-11-09

Activity Maps

- Plan and monitor your migration with activity maps

Bundles

- Install a bundle to identify potential ransomware attacks
- Identify Kerberos brute force attacks with the Active Directory bundle

Dashboards

- Monitor website performance in a dashboard
- Monitor database health in a dashboard
- Monitor DNS errors in a dashboard
- Monitor load balancer performance in a dashboard

Metrics

- Explore metrics in the ExtraHop system to investigate DNS failures
- Create a custom device to monitor remote office traffic

Open Data Streams

- Configure an open data stream to send metric data to AWS Cloudwatch

Records

- Commit a custom record to monitor suspicious port activity
- Query records to find missing web resources

Scheduled Reports

- Schedule a report about Active Directory

System Health

- Analyze System Health charts to assess trigger performance

Triggers

- Build a trigger to collect custom metrics for HTTP 404 errors
- Build a trigger to monitor responses to NTP monlist requests
- Initiate precision packet captures to analyze zero window conditions