Planen Sie einen Dashboard-Bericht über Active Directory

Veröffentlicht: 2024-01-31

Active Directory ist eine wichtige Anwendung, deren Überwachung und Problembehandlung zeitaufwändig sein kann. Im ExtraHop Bundle for Active Directory haben wir Dashboards zusammengestellt, die eine umfassende Ansicht der Active Directory Directory-Daten auf oberster Ebene bieten, sodass Sie leicht auf potenzielle Probleme achten können.

Damit Sie Änderungen einfach überwachen können, können Sie einen Bericht für Ihr Active Directory Directory-Dashboard planen. Ein Dashboard-Bericht liefert eine PDF-Datei mit Dashboard-Daten an jeden E-Mail-Empfänger, den Sie angeben.

In dieser exemplarischen Vorgehensweise zeigen wir Ihnen, wie Sie das Paket herunterladen und auf Ihr ExtraHop-System anwenden und wie Sie einen zweiwöchentlichen Dashboard-Bericht für Ihre Stakeholder über den Zustand Ihrer Active Directory Directory-Umgebung planen.

Hinweis Sie können Berichte nur von einer Konsole aus planen.

Voraussetzungen

- Sie müssen Zugang zu einem haben Konsole.
- Sie benötigen ein Benutzerkonto bei eingeschränkte oder vollständige Schreibrechte um ein Dashboard zu erstellen

Rufen Sie das ExtraHop Active Directory Directory-Paket ab

Bevor Sie das Active Directory Directory-Paket auf Ihr ExtraHop-System hochladen können, müssen Sie das Paket aus dem ExtraHop Solution Bundle Index abrufen.

1. Gehe zum Seite „Active Directory Directory-Bundle“.
2. Wenn Sie sich noch nicht auf der ExtraHop-Website angemeldet haben, klicken Sie auf **Einloggen** im rechten Bereich und geben Sie dann einen gültigen Benutzernamen und ein Passwort ein.
3. Klicken Sie im Abschnitt So erhalten Sie dieses Paket auf den Link, um eine Serviceanfrage zum Abrufen des Pakets zu erstellen.

Laden Sie das Active Directory Directory-Paket hoch und wenden Sie es auf Ihr ExtraHop-System an

In den folgenden Schritten laden Sie das Paket, das Sie von der ExtraHop-Website heruntergeladen haben, hoch und installieren es auf Ihrem Konsole.

1. Loggen Sie sich ein in Konsole durch `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie in der oberen rechten Ecke auf das Symbol Systemeinstellungen.
3. klicken **Bündel**.
4. Auf dem Bündel Seite, klick **Paket hochladen**.
5. klicken **Wählen Sie Datei**, und wählen Sie dann die Active Directory Directory-.json-Datei aus, die Sie im vorherigen Abschnitt heruntergeladen haben.
6. Wählen Sie im Abschnitt Installationsoptionen die folgenden Kontrollkästchen aus:
   a) Wählen Sie die Standort aus, auf der Sie das Paket installieren möchten.

b) Wählen Sie den **Wenden Sie 9 enthaltene Aufgaben an** Checkbox.

Diese Option weist das Paket den im Bundle enthaltenen Metrikquellen zu. In den meisten Fällen ist es am besten, die Standardzuweisungen anzuwenden.

c) Wählen Sie den **Bestehenden Inhalt überschreiben** Checkbox.

Diese Option überschreibt alle Objekte, die denselben Namen wie Objekte im Paket haben. Wenn Sie bereits Systemobjekte mit demselben Namen haben , die Sie beibehalten möchten, müssen Sie diese Objekte umbenennen, um zu verhindern, dass sie mit den Objekten im Paket überschrieben werden.

7. klicken **Installieren**, und klicken Sie dann auf **Erledigt**. Ihr Paket ist installiert und in der Tabelle aufgeführt!

Konfigurieren Sie die Active Directory Directory-Trigger

In den folgenden Schritten aktivieren und konfigurieren Sie einen Auslöser, der die Einstellungen für Sperrungen und privilegierte Konten in Ihrer Active Directory Directory-Umgebung widerspiegelt.

1. Klicken Sie auf das Symbol Systemeinstellungen .
2. klicken **Auslöser**.
3. Aktivieren Sie jeden Auslöser im Active Directory v4-Paket, indem Sie die folgenden Schritte ausführen.
   a) Klicken Sie in der Tabelle auf einen Triggernamen, der mit beginnt **ANZEIGE**.
   b) Lösche das **Trigger deaktivieren** Checkbox, um den Auslöser zu aktivieren.
   c) klicken **Speichern und schließen**.
4. Ändern Sie bestimmte Felder im Kerberos-Trigger so, dass sie Ihren Active Directory Directory-Konten entsprechen, indem Sie die folgenden Schritte ausführen.
   a) Klicken Sie in der Tabelle auf **AD: Kerberos** und klicken Sie dann auf **Herausgeber** Registerkarte.
   b) Stellen Sie die `failedLoginDisableInterval` konstant zur Übereinstimmung mit dem Wert von `Reset account lockout counter after` Richtlinieneinstellung in Ihrer Active Directory Directory-Umgebung.
   c) Stellen Sie die `accountLockoutDuration` konstant auf den Wert von `Account lockout duration` Richtlinieneinstellung in Ihrer Active Directory Directory-Umgebung.
   d) Fügen Sie die vollständigen Namen aller privilegierten Konten in Ihrer Umgebung zur `priv_names` Liste und alle teilweisen Übereinstimmungen mit der `priv_regex` Liste. Beispiele für privilegierte Konten sind:

```
var priv_names = {'admin', 'administrator', 'root', 'ss', 'sys',
        'sysadmin, 'informix'}
```

   e) klicken **Speichern und schließen**.

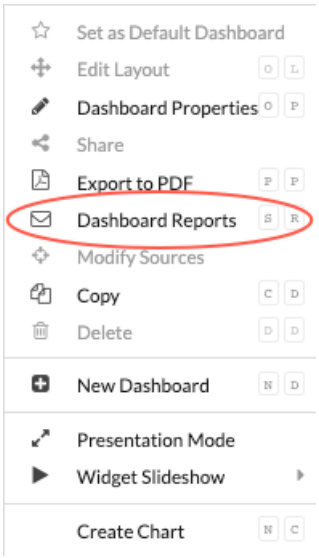
Erstellen, planen und speichern Sie einen Dashboard-Bericht

In den folgenden Schritten zeigen wir Ihnen, wie Sie einen wöchentlichen Dashboard-Bericht planen, der montags und donnerstags um 7:00 Uhr ausgeführt wird. Wir zeigen Ihnen auch, wie Sie den Dashboard-Bericht an einen Kollegen senden, z. B. an jemanden, der die Authentifizierungsdienste in Ihrem Unternehmen verwaltet.

1. klicken **Armaturenbretter** oben auf der Seite, und klicken Sie dann auf **Überblick über Active Directory** Dashboard im linken Bereich.

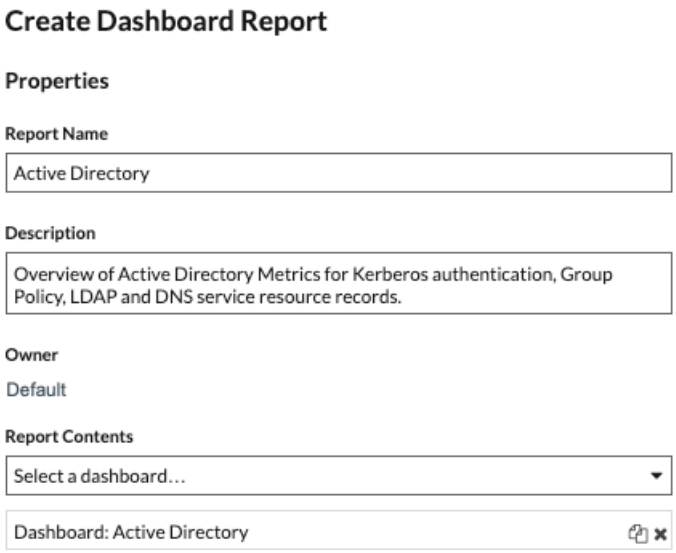
Hinweis: Jeder Bericht kann nur mit einem Dashboard verknüpft werden. Sie können jedes Dashboard auswählen , das Ihnen gehört oder das mit Ihnen geteilt wurde, um einen Bericht zu erstellen.

2. Klicken Sie in der oberen rechten Ecke der Dashboard-Seite auf das Befehlsmenü und wählen Sie dann **Dashboard-Berichte**.



EIN Dashboard-Berichte Eine Seite wird angezeigt, auf der alle auf der Konsole gespeicherten Berichte angezeigt werden. Wenn dies Ihr erster Bericht ist, ist diese Seite leer.

3. Klicken Sie in der oberen rechten Ecke **Erstellen**.
4. Im Feld Berichtsname wird der Name des Dashboard angezeigt. Lassen Sie uns die Hostinformationen der verbundenen Standort aus dem Titel entfernen, wie in der folgenden Abbildung dargestellt.

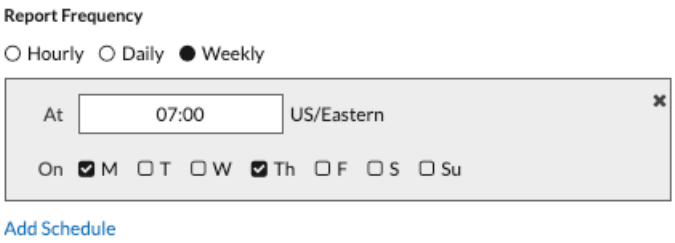


5. Lassen Sie uns die Seite nach unten springen, um den Zeitplan für den Dashboard-Bericht festzulegen. Wählen Sie im Abschnitt Zeitintervall den Zeitrahmen der Dashboard-Daten aus, die Sie in der Berichts-PDF-Datei anzeigen möchten. Lassen Sie uns für diese exemplarische Vorgehensweise über die Daten der letzten 4 Tage berichten. Klicken Sie auf **Zuletzt** Feld und geben Sie dann 4 ein.

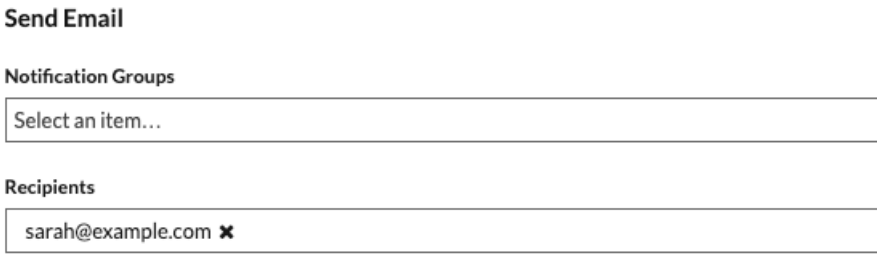
Hinweis: Weitere Informationen zur Konfiguration der einzelnen Feld finden Sie unter Erstellen Sie einen geplanten Dashboard-Bericht.

6. Legen Sie im Abschnitt Berichtshäufigkeit den Zeitplan für die E-Mail-Zustellung fest. Für diese Komplettlösung senden wir einen wöchentlichen Bericht an zwei verschiedenen Tagen um 7:00 Uhr. Führen Sie die folgenden Schritte aus:
   a) Klicken Sie auf **Bei** Drop-down-Liste und wählen **07:00**. Mit dieser Einstellung wird die Übermittlung des Berichts für 7:00 Uhr geplant.

      Die für Ihre Konsole festgelegte Systemzeit bestimmt die Zeitzone, die bei der Konfiguration Ihres Berichts angezeigt wird. Weitere Informationen zur Konfiguration der Zeitzone für Ihr ExtraHop-System über die ExtraHop-Administrationseinstellungen finden Sie unter Systemzeit konfigurieren.
   b) Aktivieren Sie die Kontrollkästchen neben M und Do, um die Zustellung des Berichts für Montag und Donnerstag zu planen.

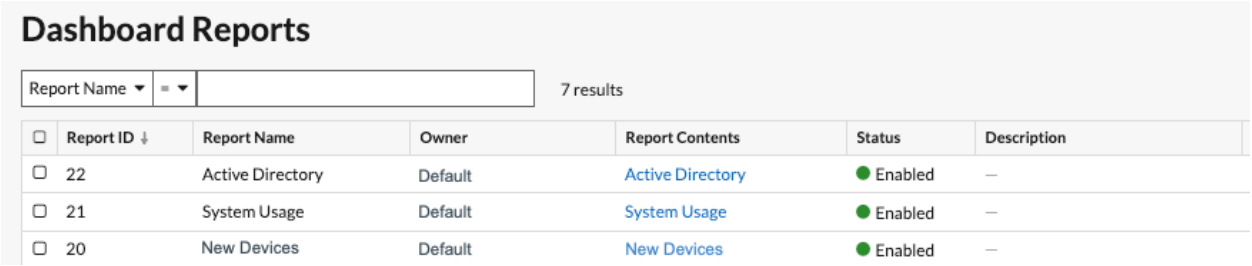


7. Um die E-Mail-Adresse Ihres Kollegen hinzuzufügen, scrollen Sie nach unten zum Abschnitt Senden an. Klicken Sie auf das Feld E-Mail-Adressen und geben Sie die E-Mail-Adresse ein.



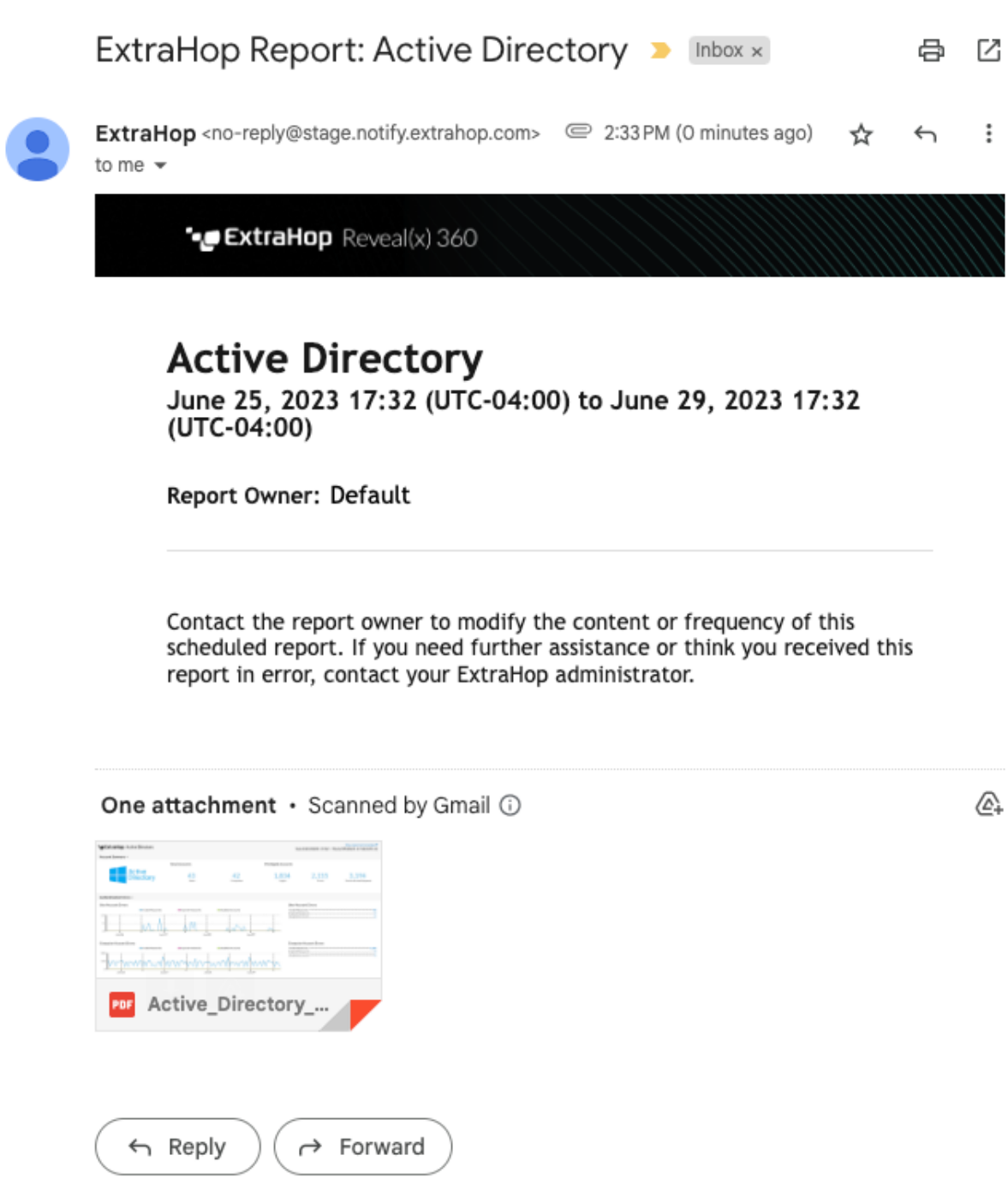
Hinweis: Das ExtraHop-System speichert keine E-Mail-Adressen für ExtraHop-Benutzerkonten. Wenn Ihr ExtraHop Reveal (x) Enterprise-System jedoch mit einer E-Mail-Gruppe konfiguriert, Sie können eine Benachrichtigungsgruppe auswählen, die per E-Mail gesendet werden soll. Reveal (x) 360 unterstützt keine E-Mail-Benachrichtigungsgruppen.

8. Optional: klicken **Jetzt senden** um eine Test-E-Mail an den Empfänger zu senden.
9. klicken **Erledigt**. Ihr Dashboard-Bericht wird jetzt auf der Seite Dashboard-Berichte angezeigt, wie in der folgenden Abbildung dargestellt.



10. Klicken Sie in der unteren rechten Ecke der Seite auf **Erledigt** erneut , um zu Ihrem Dashboard zurückzukehren.

Ihr Kollege erhält eine ähnliche E-Mail wie im folgenden Beispiel mit der angehängten PDF-Berichtsdatei.



Hinweis: Klicken Sie in der oberen rechten Ecke der PDF-Datei auf **Bericht auf ExtraHop ansehen** Link zum Zugriff auf das Dashboard, das den Bericht generiert hat. Für ExtraHop-Benutzer öffnet der Link die Konsole und stellt das Dashboard auf das im Bericht angegebene Zeitintervall ein. Sie können Metriken jetzt im Dashboard genauer untersuchen.

Eine weitere E-Mail-Adresse zu einem gespeicherten Bericht hinzufügen

Wenn Sie Änderungen an einem Dashboard-Bericht vornehmen möchten, können Sie jederzeit darauf zugreifen. Lassen Sie uns die E-Mail-Adresse eines neuen Stakeholders zu unserem Active Directory Directory-Bericht hinzufügen.

1. Klicken Sie auf der Dashboard-Seite auf das Befehlsmenü in der oberen rechten Ecke und wählen Sie dann **Dashboard-Berichte**.
2. In der **Name des Berichts** Feld, klicken Sie auf den Titel Ihres Berichts.
3. Scrollen Sie nach unten zum E-Mail senden Abschnitt.
4. Klicken Sie auf das Feld E-Mail-Adressen.
5. Geben Sie nach der ersten E-Mail-Adresse ein Komma und dann die neue E-Mail-Adresse ein.

6. klicken **Speichern**.
7. klicken **Erledigt** um zu Ihrem Dashboard zurückzukehren. Der geplante Bericht für diese exemplarische Vorgehensweise wurde jetzt aktualisiert.

Nächste Schritte
Im Laufe der Zeit möchten Sie möglicherweise die Übermittlung des Berichts unterbrechen, indem Sie Deaktivieren eines Dashboard-Berichts. Oder Sie möchten möglicherweise Änderungen an Ihrem Dashboard vornehmen, um verschiedene Diagramme oder Daten anzuzeigen. Weitere Informationen zum Ändern eines Dashboard finden Sie in diesen Ressourcen:

- Ein Dashboard-Layout bearbeiten
- Verwenden von Dashboards zum Organisieren und Präsentieren von Daten (Online-Schulung)
- Bearbeiten Sie ein Dashboard-Diagramm mit dem Metric Explorer
- Ein Textfeld-Widget bearbeiten

Im Folgenden finden Sie weitere Anleitungen zum Erstellen von Dashboards von Grund auf zur Überwachung von Protokollmetriken:

- Überwachen Sie die Leistung Ihrer Website in einem Dashboard (Komplettlösung)
- Überwachen Sie den Zustand der Datenbank in einem Dashboard (Exemplarische Vorgehensweise)
- Überwachen Sie DNS-Fehler in einem Dashboard (Exemplarische Vorgehensweise)