

Konfigurieren der ThreatGrid-Appliance für Cluster-Vorgänge

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[Initialer Cluster-Knoten](#)

[EULA](#)

[Lizenzinstallation](#)

[NFS konfigurieren](#)

[Clustereinstellungen](#)

[Überprüfung und Installation](#)

[Knoten zu bestehendem Cluster hinzufügen](#)

[EULA](#)

[Lizenzinstallation](#)

[NFS konfigurieren](#)

[Clustereinstellungen](#)

[Überprüfung und Installation](#)

Einleitung

In diesem Dokument wird beschrieben, wie die ThreatGrid-Appliance für Cluster-Vorgänge konfiguriert wird.

Mitwirkend von TJ Busch, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco ThreatGrid-Appliance

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

ThreatGrid Appliance enthält die Funktionen zum Clustern mehrerer TG-Appliances, um die Anzahl gleichzeitiger Stichproben zu erhöhen, die gleichzeitig verarbeitet werden können. Beachten Sie, dass TGA derzeit bei der aktuellen Implementierung der Clustering-Funktion keine Hochverfügbarkeit unterstützt.

Warnung: Knoten müssen frei von übermittelten Beispielen sein. Es wird empfohlen, den Befehl "**Zerstören-Daten**" von der TGSH-Konsole aus zu verwenden.

Konfiguration

Initialer Cluster-Knoten

Schritt 1: Einrichten der Threat Grid-Knoten-Netzwerkschnittstellen wie im [Threat Grid Appliance Getting Started Guide](#) definiert, um alle erforderlichen Einstellungen zu aktivieren/konfigurieren.

Warnung: Alle Cluster-Schnittstellen müssen mit demselben physischen Layer-2-Switch im gleichen VLAN verbunden sein. Layer-3-Routing oder Layer-2-Erweiterungstechnologien werden nicht unterstützt.

EULA

Schritt 1: Zeigen Sie auf die DNS/IP-Adresse der Admin-Schnittstelle, die in Schritt 1 mithilfe von HTTPS konfiguriert wurde.

Schritt 2: Geben Sie das ursprüngliche Administratorkennwort ein, das Sie aus dem TGSH-Dialogfeld kopiert haben, und klicken Sie auf **Anmelden**. Die Seite Kennwort ändern wird geöffnet.

Schritt 3: Geben Sie das Kennwort aus dem TGSH-Dialog in das Feld Altes Kennwort ein.

Schritt 4: Neues Kennwort eingeben und bestätigen

Schritt 5: Klicken Sie auf **Kennwort ändern**.

Schritt 6: Lesen Sie die Endbenutzer-Lizenzvereinbarung.

Schritt 7: Blättern Sie nach unten, und klicken Sie auf "**Ich habe LESEN UND STIMME ZU**".

Lizenzinstallation

Schritt 1: Klicken Sie in der linken Spalte auf die Registerkarte **Lizenz**.

Schritt 2: Klicken Sie unter Neue Lizenz hochladen auf **Datei auswählen**, und wählen Sie die angegebene Lizenzdatei aus Ihrem Dateimanager aus.

Schritt 3: Geben Sie das Lizenzkennwort ein, das Sie in das Feld Passphrase eingegeben haben.

Schritt 4: Klicken Sie auf **Hochladen**. Die aktualisierten Lizenzinformationen werden in den vorherigen leeren Feldern angezeigt.

Schritt 5: Klicken Sie auf **Weiter**, um fortzufahren.

NFS konfigurieren

Schritt 1: Konfigurieren Sie die Optionen wie empfohlen:

- Host - Der NFSv4-Hostserver. Die Verwendung der IP-Adresse wird gegenüber dem Hostnamen empfohlen.
- Path: Der absolute Pfad zum Speicherort auf dem NFS-Host-Server, unter dem Dateien gespeichert werden.
- Opts (Optionen) - Verwendung von NFS-Mount-Optionen, falls dieser Server Abweichungen von den Standard-Linux-Standard-Einstellungen für NFSv4 erfordert
- Status - Wählen Sie aus dem Dropdown-Menü Enabled (Aktiviert) aus (Schlüssel ausstehend).

Schritt 2: **Weiter** auswählen

Schritt 3: Klicken Sie unter "FS Encryption Password File" auf **Generate (Generieren)**.

Schritt 4: Klicken Sie nach der Generierung auf **Herunterladen**.

Vorsicht: Verschlüsselungsschlüssel können nicht abgerufen werden, nachdem sie vom System generiert wurden. Sichern Sie den Schlüssel an einem sicheren Ort, um Datenverluste zu vermeiden.

Schritt 5: Klicken Sie auf **Aktivieren**

Schritt 6: Klicken Sie auf **Weiter**

Clustereinstellungen

Schritt 1: Wählen Sie unter Clustering-Status die Option **Cluster starten aus**.

Schritt 2: Der Status wechselt von **Standalone (nicht gespeichert)** zu **Clustered**

Schritt 3: Klicken Sie auf **Weiter**

Überprüfung und Installation

Warnung: Wenn der anfängliche Cluster-Knoten die Installation nicht abschließen kann, bevor der Vorgang abgeschlossen ist, treten Fehler auf, die einen Neustart des Prozesses erfordern. Nach der Konfiguration des ersten Knotens können Sie mehrere Knoten

gleichzeitig zum primären Knoten verbinden.

Schritt 1: Klicken Sie auf **Installation starten**

Schritt 2: Nach 20-30 Minuten wird der Knoten zum Neustart aufgefordert. Klicken Sie auf **Neustart**.

Schritt 3: Nach 20-30 Minuten wird der Knoten aktiv. Sie können mit dem Hinzufügen von Knoten fortfahren.

Knoten zu bestehendem Cluster hinzufügen

EULA

Schritt 1: Zeigen Sie auf die DNS/IP-Adresse der Admin-Schnittstelle, die in Schritt 1 mithilfe von HTTPS konfiguriert wurde.

Schritt 2: Geben Sie das ursprüngliche Administratorkennwort ein, das Sie aus dem TGSH-Dialogfeld kopiert haben, und klicken Sie auf **Anmelden**. Die Seite Kennwort ändern wird geöffnet.

Schritt 3: Geben Sie das Kennwort aus dem TGSH-Dialog in das Feld Altes Kennwort ein.

Schritt 4: Neues Kennwort eingeben und bestätigen

Schritt 5: Klicken Sie auf **Kennwort ändern**.

Schritt 6: Lesen Sie die Endbenutzer-Lizenzvereinbarung.

Schritt 7: Blättern Sie nach unten, und klicken Sie auf "**Ich habe LESEN UND STIMME ZU**".

Lizenzinstallation

Schritt 1: Klicken Sie in der linken Spalte auf die Registerkarte **Lizenz**.

Schritt 2: Klicken Sie unter Neue Lizenz hochladen auf **Datei auswählen**, und wählen Sie die angegebene Lizenzdatei aus Ihrem Dateimanager aus.

Schritt 3: Geben Sie das Lizenzkennwort ein, das Sie in das Feld Passphrase eingegeben haben.

Schritt 4: Klicken Sie auf **Hochladen**. Die aktualisierten Lizenzinformationen werden in den vorherigen leeren Feldern angezeigt.

Schritt 5: Klicken Sie auf **Weiter**, um fortzufahren.

NFS konfigurieren

Schritt 1: Konfigurieren Sie die Optionen wie empfohlen:

- Host - Der NFSv4-Hostserver. Die Verwendung der IP-Adresse wird gegenüber dem Hostnamen empfohlen.

- Path: Der absolute Pfad zum Speicherort auf dem NFS-Host-Server, unter dem Dateien gespeichert werden.
- Opts (Optionen) - Verwendung von NFS-Mount-Optionen, falls dieser Server Abweichungen von den Standard-Linux-Standard-Einstellungen für NFSv4 erfordert
- Status - Wählen Sie aus dem Dropdown-Menü Enabled (Aktiviert) aus (Schlüssel ausstehend).

Schritt 2: **Weiter** auswählen

Schritt 3: Klicken Sie unter FS Encryption Password File (FS-Verschlüsselungskennwortdatei) auf **Choose file (Datei auswählen)**, und navigieren Sie zum gespeicherten Primärknotenschlüssel.

Schritt 4: Klicken Sie auf **Hochladen**

Schritt 5: Klicken Sie auf **Aktivieren**

Schritt 6: Klicken Sie auf **Weiter**

Clustereinstellungen

Anmerkung: Der TGA-Startknoten muss über die Cluster-Schnittstelle erreichbar und reaktionsfähig sein, damit weitere Knoten dem Cluster beitreten können.

Schritt 1: Wählen Sie unter Clustering-Status die Option **Cluster beitreten aus**.

Schritt 2: Der Status wechselt von **Standalone (nicht gespeichert)** zu **Clustered**

Schritt 3: Klicken Sie auf **Weiter**

Überprüfung und Installation

Schritt 1: Klicken Sie auf **Installation starten**

Schritt 2: Nach 20-30 Minuten wird der Knoten zum Neustart aufgefordert. Klicken Sie auf **Neustart**.

Schritt 3: Nach 20-30 Minuten wird der Knoten aktiv und zeigt die Verbindung zum Cluster an.