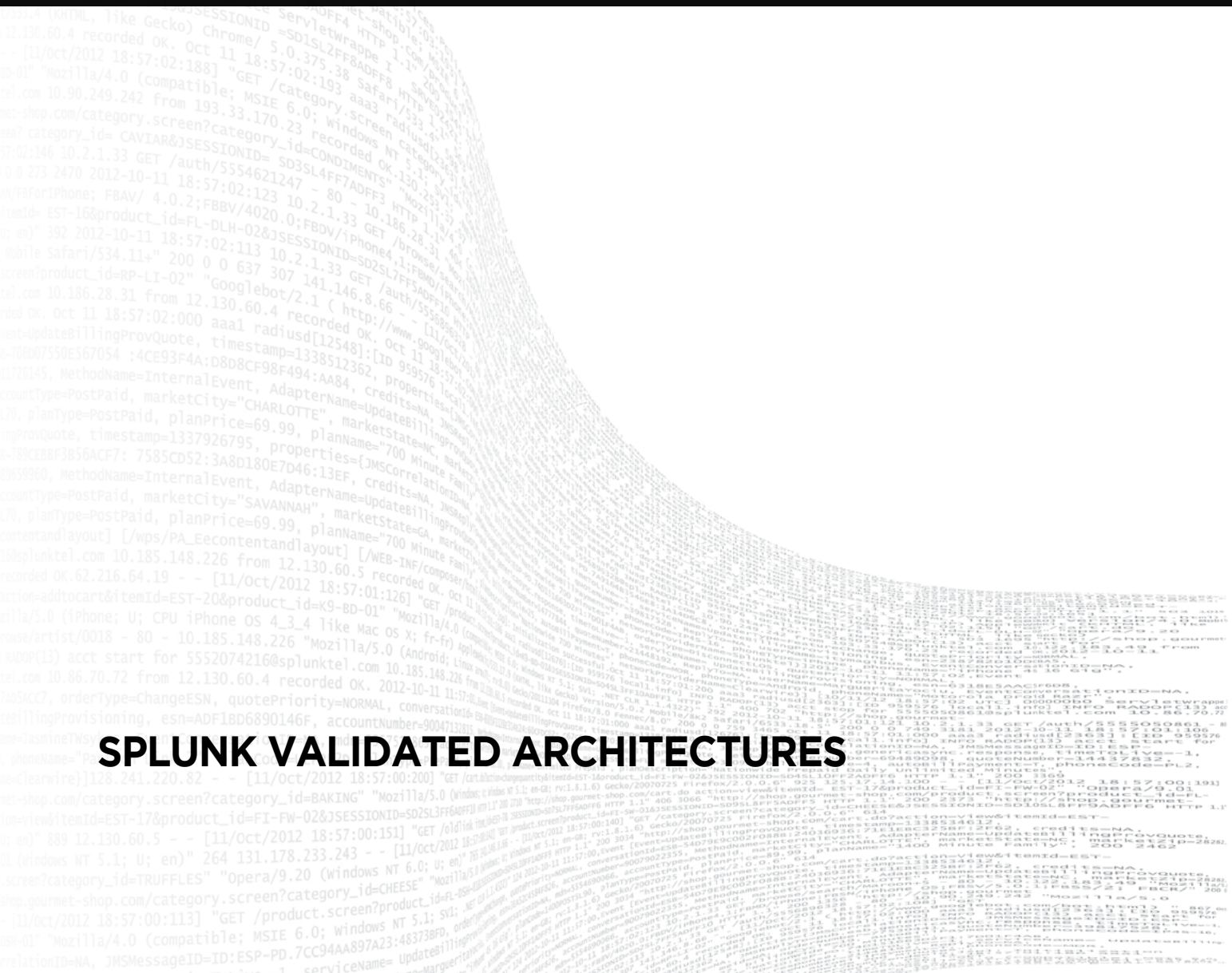
splunk>

WHITEPAPER

SPLUNK VALIDATED ARCHITECTURES



Inhalt

Einleitung

Splunk Validated Architectures (SVAs) sind bewährte Referenzarchitekturen für stabile, effiziente und reproduzierbare Splunk-Bereitstellungen. Viele Bestandskunden von Splunk haben schnelle Aneignung von Technologien und Wachstum durchlaufen und sehen sich dadurch Herausforderungen bei der Skalierung gegenüber. Zugleich suchen neue Splunk-Kunden in stärkerem Maß nach Richtlinien und zertifizierten Architekturen, um sicherzustellen, dass ihre anfängliche Bereitstellung auf einem sicheren Fundament aufbaut. SVAs wurden entwickelt, um den wachsenden Bedarf unserer Kunden zu bedienen zu können.

Gleich, ob Sie Neukunde oder Bestandskunde von Splunk sind, können SVAs Ihnen beim Aufbau einer Umgebung helfen, die einfacher zu warten ist und in der sich Probleme leichter beheben lassen. SVAs sind dafür ausgelegt, Ihnen optimale Ergebnisse zu liefern und zugleich Ihre Gesamtbetriebskosten zu minimieren. Darüber hinaus baut dann Ihr gesamtes Splunk-Fundament auf einer reproduzierbaren Architektur auf, die es Ihnen ermöglicht, Ihre Bereitstellung bei im Lauf der Zeit steigenden Anforderungen zu skalieren.

SVAs bieten Topologieoptionen, die eine große Bandbreite von Anforderungen in Organisationen abdecken. Sie können daher leicht eine Topologie erkennen und finden, die sich für Ihre Ansprüche eignet. Der Auswahlprozess für Splunk Validated Architectures hilft Ihnen bei der Zuordnung Ihrer spezifischen Anforderungen zu der Topologie, die den Bedürfnissen Ihrer Organisation optimal entspricht. Wenn Sie in Splunk einsteigen, empfehlen wir Ihnen, für Ihre anfängliche Bereitstellung eine Validated Architecture zu implementieren. Wenn Sie Bestandskunde sind, empfehlen wir Ihnen, die Option der Ausrichtung an der Topologie einer Validated Architecture zu untersuchen. Sofern Sie keine einzigartigen Anforderungen haben, die den Aufbau einer benutzerdefinierten Architektur erforderlich machen, ist es sehr wahrscheinlich, dass eine Validated Architecture Ihre Anforderungen erfüllen kann und dabei kostengünstig bleibt.

Dieses Whitepaper gibt Ihnen einen Überblick zu SVAs. In diesem Whitepaper finden Sie die erforderlichen Ressourcen, um den SVA-Auswahlprozess zu durchlaufen, einschließlich eines Anforderungsfragebogens, Diagrammen zur Bereitstellungstopologie, Entwurfsprinzipien und allgemeinen Richtlinien.

Wenn Sie Hilfe beim Implementieren einer Splunk Validated Architecture benötigen, wenden Sie sich an Splunk Professional Services (https://www.splunk.com/en_us/support-and-services/splunk-services.html).

Dokumentstruktur

SVAs gliedern sich in drei inhaltliche Hauptbereiche:

1. Indizierung und Suchtopologien
2. Architekturkomponenten der Datenerfassung
3. Entwurfsprinzipien und Best Practices

Indizierung und Suche deckt die Architekturschichten ab, die die Kernfunktionen einer Splunk-Bereitstellung zu Suche und Indizierung zur Verfügung stellen. Der Abschnitt zur Datenerfassungskomponente führt Sie durch die Wahl der richtigen Mechanismen zur Datenerfassung für Ihre Anforderungen.

Entwurfsprinzipien und Best Practices betreffen Ihre Architektur um Ganzen und helfen Ihnen, beim Ausarbeiten der Details Ihrer Bereitstellung die richtigen Entscheidungen zu treffen.

Gründe für die Verwendung von Splunk Validated Architectures

Das Implementieren einer Validated Architecture versetzt Sie in die Lage, Splunk mit größerer Sicherheit zu entwerfen und bereitzustellen. SVAs helfen Ihnen, einige der häufigsten Herausforderungen zu bewältigen, mit denen Organisationen konfrontiert sind, darunter:

Performance

- Organisationen möchten Verbesserungen bei Leistung und Stabilität sehen.

Komplexität

- Organisationen geraten manchmal in die Falle benutzerdefinierter Bereitstellungen, insbesondere, wenn sie zu schnellem oder organischem Wachstum ausgesetzt waren. In solchen Fällen kann die Umgebung leicht mit zu großer Komplexität überfrachtet werden. Diese Komplexität erweist sich oftmals als hartnäckiges Hindernis bei der Skalierung.

Effizienz

- Um den maximalen Nutzen aus ihrer Splunk-Bereitstellung zu ziehen, müssen Organisationen die Betriebseffizienz steigern und die Amortisierungszeit verkürzen.

Kosten

- Organisationen suchen nach Wegen, die Gesamtbetriebskosten (Total Cost of Ownership, TCO) zu senken und zugleich allen ihren Anforderungen gerecht zu werden.

Agilität

- Organisationen müssen sich bei Skalierung und Wachstum an veränderte Bedingungen anpassen.

Wartung

- Die Optimierung der Umgebung ist oftmals erforderlich, um den Wartungsaufwand zu verringern.

Skalierbarkeit

- Organisationen sind auf die Fähigkeit zur effizienten und nahtlosen Skalierung angewiesen.

Überprüfung

- Stakeholder in der Organisation möchten sichergestellt wissen, dass ihre Splunk-Bereitstellung auf bewährten Methoden aufgebaut ist.

Grundpfeiler von Splunk Validated Architectures

Splunk Validated Architectures wurden auf diesen Grundpfeilern errichtet. Weitere Informationen zu diesen Grundpfeilern finden Sie in Anhang "A" unten.

VERFÜGBARKEIT	PERFORMANCE	SKALIERBARKEIT	SICHERHEIT	VERWALTBARKEIT
Das System ist **ständig betriebsbereit** und in der Lage, sich nach geplanten oder ungeplanten Ausfällen oder Unterbrechungen wiederherzustellen.	Das System kann einen **optimalen Servicelevel** unter wechselnden Nutzungsmustern aufrecht erhalten.	Das System ist in allen Schichten skalierbar ausgelegt und ermöglicht Ihnen so die **effektive Verarbeitung gesteigerter Workloads**.	Das System ist **für den Schutz von Daten, Konfigurationen und Vermögenswerten konzipiert** und liefert gleichzeitig fortgesetzt Mehrwert.	Das System kann **von einem zentralen Ort aus betrieben und in allen Schichten verwaltet** werden.

Diese Grundpfeiler unterstützen direkt den **Plattformverwaltungs- und Support-**Service im Splunk Center Of Excellence-Modell.

Was Sie von Splunk Validated Architectures erwarten können

Bitte beachten Sie, dass SVAs keine Technologien zur Bereitstellung oder Dimensionierung beinhalten. Dies hat die folgenden Gründe:

- Bereitstellungstechnologien, wie etwa Betriebssysteme und Serverhardware, werden im Kontext von SVAs als Implementierungsoptionen angesehen. Verschiedene Kunden wählen verschiedene Optionen, so dass eine Verallgemeinerung nur schwer möglich ist.
- Für die Dimensionierung von Bereitstellungen ist eine Bewertung des Volumens der Datenerfassung, der verwendeten Datentypen, der Suchvolumina und der Anwendungsfälle der Suche erforderlich, alles stark kundenspezifische Parameter, die im Allgemeinen keinen Einfluss auf die eigentliche, grundlegende Bereitstellungsarchitektur haben. Verfügbare Dimensionierungstools können diesen Prozess unterstützen, sobald Sie Ihre Bereitstellungsarchitektur festgelegt haben. Splunk Storage Sizing (https://splunk-sizing.appspot.com/) zählt zu den verfügbaren Tools.

Dies bieten SVAs:	**Dies bieten SVAs nicht:**
✅ Optionen für die Bereitstellung mit und ohne Clusterarchitektur. ✅ Diagramme der Referenzarchitektur. ✅ Richtlinien zur Wahl der für Sie richtigen Architektur ✅ Schichtspezifische Empfehlungen. ✅ Best Practices für den Ausbau Ihrer Splunk-Bereitstellung	❌ Implementierungsoptionen (Betriebssystem, Bare Metal i. Vgl. mit virtuell i. Vgl. mit Cloud usw.). ❌ Bereitstellungsdimensionierung. ❌ Eine förmliche Genehmigung Ihrer Architektur. Hinweis: SVAs bieten Empfehlungen und Richtlinien, so dass Sie im Endeffekt die richtige Entscheidung für Ihre Organisation treffen können. ❌ Einen Topologievorschlag für jedes denkbare Bereitstellungsszenario. In manchen Fällen können einzigartige Faktoren die Entwicklung einer benutzerdefinierten Architektur erforderlich machen. Splunk-Experten stehen Ihnen bei der Entwicklung eventuell benötigter benutzerdefinierter Lösungen zur Seite. Wenn Sie Bestandskunde sind, setzen Sie sich mit Ihrem Splunk Account Team in Verbindung. Wenn Sie neu in Splunk einsteigen, erreichen Sie uns hier (https://www.splunk.com/en_us/talk-to-sales.html).

Rollen und Zuständigkeiten

Splunk Validated Architectures sind für die Belange von Entscheidungsträgern und Administratoren von großer Bedeutung. Enterprise Architects, Berater, Splunk-Administratoren und Managed Service-Provider sollten alle in den SVA-Auswahlprozess einbezogen werden. Unten finden Sie eine Beschreibung dieser einzelnen Rollen:

Rolle	**Beschreibung**
Enterprise Architects	Für die Architektur von Splunk-Bereitstellungen nach Maßgabe der Unternehmensanforderungen zuständig.
Berater	Für die Bereitstellung von Dienstleistungen im Zusammenhang mit der Splunk-Architektur, dem Entwurf und der Implementierung zuständig.
Splunk-Techniker	Für die Verwaltung des Splunk-Lebenszyklus zuständig.
Managed Service-Provider	Entitäten, die Splunk als Dienst für Kunden bereitstellen und betreiben.

Der Auswahlprozess für Splunk Validated Architectures im Überblick

Der Auswahlprozess für Splunk Validated Architectures hilft Ihnen, die einfachste und am stärksten optimierte Architektur zu ermitteln, die allen Bedürfnissen Ihrer Organisation entspricht.

Schritte im Auswahlprozess	Ziele	Überlegungen
Schritt 1: Definieren der Anforderungen für: a) Indizierung und Suche b) Datenerfassungs-mechanismen	*Definieren der Anforderungen.*	• Entscheidungsträger, Stakeholder und Administratoren sollten die Anforderungen Ihrer Organisation gemeinsam ermitteln und definieren. • Wenn bereits eine Bereitstellung vorhanden ist, können Sie Ihre aktuelle Architektur bewerten, um festzustellen, welche Dinge für den Wechsel zu einem validierten Modell erforderlich sind. *Einen Fragebogen, der Sie beim Definieren Ihrer Anforderungen unterstützt, finden Sie in Schritt 1 unten.*
Schritt 2: Auswählen einer Topologie für: a) Indizierung und Suche b) jeden einzelnen Mechanismus zur Datenerfassung	*Auswählen einer Topologie, die den ermittelten Anforderungen entspricht.*	• Sie wählen eine Topologie, die Ihren Anforderungen optimal entspricht. • Verkomplizieren Sie Ihr System nicht, und bleiben Sie im Rahmen der SVA, damit Sie den einfacheren Weg zu Skalierbarkeit nutzen können. *Diagramme und Beschreibungen zu Topologieoptionen finden Sie in Schritt 2 unten.*
Schritt 3: Anwenden von Entwurfs-prinzipien und Best Practices	*Priorisieren Sie Ihre Entwurfsprinzipien, und arbeiten Sie die Best Practices zur Implementierung schichtspezifisch durch.*	• Jedes Entwurfsprinzip stärkt einen oder mehrere Grundpfeiler der Splunk Validated Architectures. • Sie priorisieren Entwurfsprinzipien nach Maßgabe der Anforderungen Ihrer Organisation. • Die Implementierung Ihrer Topologie wird durch schichtspezifische Empfehlungen geleitet. *Eine Aufschlüsselung der Entwurfsprinzipien finden Sie in Schritt 3 unten.*

Schritt 1a: Definition Ihrer Anforderungen an Indizierung und Suche

Um die geeignete Bereitstellungstopologie auszuwählen, müssen Sie eine tiefschürfende Analyse Ihrer Anforderungen durchführen. Nachdem Sie Ihre Anforderungen definiert haben, sind Sie in der Lage, das einfachste und kostengünstigste Verfahren zum Implementieren von Splunk auszuwählen. Unten finden Sie einen Fragebogen, der Sie bei der Definition der wichtigsten Anforderungsbereiche für die Indizierungs- und Suchschichten Ihrer Bereitstellung unterstützt.

Der Anforderungsfragebogen legt den Schwerpunkt auf Bereiche, die einen direkten Einfluss auf Ihre Bereitstellungstopologie haben. Daher empfehlen wir Ihnen, Ihre Antworten auf die Fragen unten unbedingt festzuhalten, bevor Sie im nächsten Schritt eine Topologie auswählen.

Punkte, die berücksichtigt werden sollten

Überprüfen Sie Ihre Anwendungsfälle

Beim Definieren Ihrer Anforderungen sollten Sie die beabsichtigten Anwendungsfälle Ihrer Splunk-Infrastruktur im Blick haben. Beispielsweise ist die Topologie für einen DevOps-Anwendungsfall in einer Abteilung oftmals einfacher als die für einen unternehmenswichtigen Anwendungsfall (allerdings trifft das nicht immer zu). Sie sollten Anwendungsfälle, die Folgendes beinhalten, in vollem Umfang berücksichtigen:

- Suche
- Verfügbarkeit
- Complianceanforderungen (dies ist insbesondere dann wichtig, wenn Sie jederzeit 100 % Datentreue und Verfügbarkeit benötigen)
- Andere, für Ihre Organisation spezifische Anwendungsfallszenarien

Abhängig von Ihren Anwendungsfallszenarien muss Ihre Bereitstellung möglicherweise weitere Architekturmerkmale zur Verfügung stellen.

Berücksichtigen Sie zukünftiges Wachstum

Um Ihre Anforderungen zu definieren, müssen Sie Ihre unmittelbaren Bedürfnisse in den Mittelpunkt stellen. Jedoch sollten Sie darüber zukünftiges Wachstum und Skalierbarkeit nicht aus dem Blick verlieren. Das Skalieren Ihrer Bereitstellung kann Ausgaben, weiteres Personal oder andere Ressourcen erforderlich machen, deren Berücksichtigung schon in der aktuellen Planung sinnvoll sein kann.

Kategorien von Topologien

Die folgende Tabelle stellt einen Schlüssel der SVA-Topologiekategorien dar. Diese Kategorien werden im Fragebogen unten verwendet. Ferner finden Sie in den nächsten Schritten des SVA-Auswahlprozesses Verweise auf diese Kategorien.

Kategorien der Indizierungsschicht

Kategoriecode	Erläuterung
S	Die Kategorie "S" bezeichnet den Indexer einer Splunk-Single Server-Bereitstellung
D	Kategorie "D" bezeichnet das Erfordernis einer verteilten Indexerschicht mit mindestens 2 Indexern
C	Kategorie "C" bezeichnet das Erfordernis einer Indexer-Clusterschicht (Datenreplikation ist erforderlich)

Kategoriecode	Erläuterung
M	Kategorie "M" bezeichnet das Erfordernis einer Indexer-Clusterschicht mit mehreren Standorten

Kategorien der Suchschicht

Kategoriecode	Erläuterung
1	Kategorie "1" gibt an, dass ein einzelner Search Head möglicherweise zur Erfüllung der Anforderungen ausreicht
2	Kategorie "2" gibt an, dass zum Erfüllen der Anforderungen mehrere Search Heads erforderlich sind
3	Kategorie "3" gibt an, dass zum Erfüllen der Anforderungen ein Search Head-Cluster erforderlich ist
4	Kategorie "4" gibt an, dass ein Search Head-Cluster, der mehrere Standorte überspannt (ein "ausgedehnter" SHC) erforderlich ist, um die Anforderungen zu erfüllen
+10	Kategorie "+10" gibt an, dass ein dedizierter Search Head (Cluster) zur Unterstützung der Enterprise Security-App erforderlich ist. Fügen Sie der Topologiekategorie der Suchschicht 10 hinzu, und lesen Sie die Beschreibung der Topologie hinsichtlich der besonderen Anforderungen für diese App sorgfältig.

Fragebogen 1: Definition Ihrer Anforderungen an die Indizierungs- und Suchschichten

♦ *Eine Erläuterung der Topologiekategoriecodes finden Sie in der Schlüsseltabelle oben. Wenn Sie mehrere Fragen mit "Ja" beantworten, verwenden Sie den Topologiekategoriecode für die Frage mit der höchsten Nummer.*

Nr.	Frage	Überlegungen	Einfluss auf Topologie	Topologie-kategorie der Indexer-schicht ♦	Topologie-kategorie der Suchschicht ♦
1	Beträgt Ihre erwartete tägliche Datenerfassung weniger als ~300 GB/Tag?	Berücksichtigen Sie kurzfristiges Wachstum der täglichen Datenerfassung (~ 6–12 Monate)	Kandidat für eine Single Server-Bereitstellung, abhängig von den Antworten auf die verfügbarkeitsbezogenen Fragen	S	1
2	Benötigen Sie hohe Verfügbarkeit für die Datenerfassung/Indizierung?	Wenn Sie nicht die Verwendung von Splunk für Überwachungsanwendungsfälle planen, die fortlaufende Datenerfassung erfordern, ist eine vorübergehende Unterbrechung des eingehenden Datenflusses	Erfordert verteilte Bereitstellung, um fortlaufende Erfassung zu unterstützen	D	1

Nr.	Frage	Überlegungen	Einfluss auf Topologie	Topologie-kategorie der Indexer-schicht ♦	Topologie-kategorie der Suchschicht ♦
		möglicherweise akzeptabel; immer unter der Annahme, dass keine Logdaten verloren gehen.			
3	Unter der Annahme, dass ein Search Head zum Ausführen einer Suche verfügbar ist: Müssen Ihre Daten jederzeit vollständig durchsuchbar sein, d. h., ein Einfluss auf die Vollständigkeit der Suchergebnisse muss ausgeschlossen sein?	Wenn Ihr Anwendungsfall beispielsweise in der Berechnung von Leistungsmetriken und allgemeinem Nutzungs-Monitoring mithilfe von Aggregatfunktionen besteht, wirkt sich der Ausfall eines einzelnen Indexers möglicherweise nicht wesentlich auf die Berechnung von Statistiken über eine große Anzahl Ereignisse aus. Wenn Ihr Anwendungsfall in der Sicherheitsüber-wachung und Bedrohungs-erkennung besteht, sind blinde Flecken in den Suchergebnissen höchstwahrscheinlich unerwünscht.	Erfordert Indexcluster mit einem Replikations-faktor von mindestens (2). Hinweis: Zwar bietet ein Replikations-faktor von 2 die minimale Schutzstufe – Ausfall eines einzelnen Indexerknotens – der empfohlene (und standardmäßige) Replikations-faktor ist jedoch 3.	Z	1
4	Betreiben Sie mehrere Rechenzentren und benötigen eine automatische Wiederherstellung Ihrer Splunk-Umgebung für den Fall eines Rechenzentrums-ausfalls?	Anforderungen an Disaster Recovery können den fortlaufenden Betrieb aus zwei Einrichtungen vorschreiben (aktiv/aktiv) oder RTO/RPO-Ziele für manuelle Disaster Recovery definieren	Für fortlaufenden Betrieb sind das Clustern von Indexern an mehreren Standorten und mindestens zwei aktive Search Heads erforderlich, um Failover sowohl in der Daten-erfassungs-/Indexerschicht als auch in der Suchschicht sicherzustellen.	M	2
5	Unter der Annahme von	Wenn Splunk für fortlaufendes	Erfordert redundante	D/C/M	3

Nr.	Frage	Überlegungen	Einfluss auf Topologie	Topologie-kategorie der Indexer-schicht ♦	Topologie-kategorie der Suchschicht ♦
	fortlaufender, verlustfreier Datenerfassung, benötigen Sie HA für die benutzerseitige Suchschicht?	Kurzzeitmonitoring verwendet wird, sind Unterbrechungen in der Suchschicht wahrscheinlich nicht hinnehmbar. Das kann auch auf andere Anwendungsfälle zutreffen.	Search Heads, möglicherweise Clustering von Search Heads		
6	Müssen Sie eine große Anzahl gleichzeitiger Benutzer und/oder eine erhebliche geplante Workload für die Suche unterstützen?	Die Anforderungen bei mehr als ~50 gleichzeitigen Benutzern/Suchen erfordern normalerweise horizontale Skalierung der Suchschicht	Erfordert möglicherweise eine Topologie mit einem Search Head-Cluster in der Suchschicht	D/C/M	3
7	Müssen in einer Umgebung mit mehreren Rechenzentren Artefakte von Benutzern (Suchen, Dashboards und sonstige Wissensobjekte) zwischen den Standorten synchronisiert werden?	Dies entscheidet darüber, ob Benutzer im Fall des Ausfalls eines Standorts eine aktuelle und konsistente Erfahrung erleben.	Erfordert einen standortüber-greifenden, "ausgedehnten" Search-Head-Cluster mit geeigneter Konfiguration. **Wichtig:** Zwar kann ein ausgedehnter SHC die Verfügbarkeit der Suche während des Komplettausfalls eines Standorts verbessern, es besteht aber keine Garantie, dass alle Artefakte jederzeit über beide Standorte repliziert werden. Dies kann Einfluss auf bestimmte Anwendungen haben, die auf konsistente und aktuelle Artefakte angewiesen sind, wie etwa die Splunk App for	M	4

Nr.	Frage	Überlegungen	Einfluss auf Topologie	Topologie-kategorie der Indexer-schicht ♦	Topologie-kategorie der Suchschicht ♦
			Enterprise Security. Das Clustern von Search Heads allein ergibt keine vollständige DR-Lösung. Andere Vorzüge von SHC gelten dessen ungeachtet.		
8	Möchten Sie die Splunk App for Enterprise Security (ES) bereitstellen?	Achten Sie in diesem Fall darauf, dass Sie die spezifischen Einschränkungen, denen die Splunk App for Enterprise Security unterliegt und die für jede Topologie dokumentiert sind, lesen und verstehen.	ES erfordert eine dedizierte Search Head-Umgebung (entweder eigenständig oder als Cluster).	D/C/M	+10
9	Verfügen Sie über eine geografisch verteilte Umgebung, die gesetzlichen Bestimmungen zum Umgang mit Daten unterliegt?	Die Bestimmungen einiger Länder erlauben es nicht, dass im Land generierte Daten die inländischen Systeme verlassen	Derartige Bestimmungen verhindern die Bereitstellung einer zentralen Splunk-Indizierungs-schicht und erfordern die Entwicklung einer benutzer-definierten Architektur durch eine Zusammen-arbeit zwischen Splunk/Partner und dem Kunden, die den Details einer solchen Bereitstellung tiefgreifend Rechnung trägt. Anders ausgedrückt, es gibt keine SVA, die dieser Anforderung genügt.	Benutzer-definiert	Benutzer-definiert
10	Gelten bei Ihnen stark restriktive Sicherheits-	Möglicherweise ist aufgrund von Unternehmens-	Mehrere, unabhängige Indizierungs-	Benutzer-definiert	Benutzer-definiert

Nr.	Frage	Überlegungen	Einfluss auf Topologie	Topologie-kategorie der Indexer-schicht ♦	Topologie-kategorie der Suchschicht ♦
	richtlinien, die die gemeinsame Unterbringung bestimmter Logdatenquellen auf gemeinsam genutzten Servern/Indexern verhindern?	richtlinien die gemeinsame Unterbringung vertraulicher Logdaten zusammen mit weniger sensiblen Datasets auf dem gleichen physischen System oder innerhalb der gleichen Netzwerkzone nicht zulässig.	umgebungen sind erforderlich, eventuell mit einer gemeinsamen, hybriden Suchschicht. Dies liegt jenseits des von SVAs abgedeckten Bereichs und erfordert benutzer-definierte Architektur-entwicklung.		

Bestimmen Ihres Topologiekategoriecodes

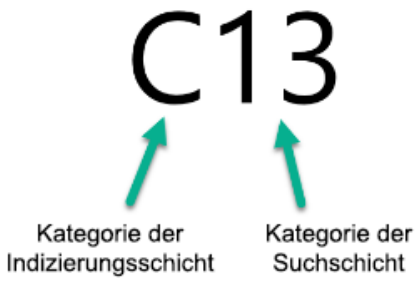
Auf der Grundlage Ihrer Antworten auf den Anforderungsfragebogen oben erhalten Sie einen kombinierten Kategorieindikator für die Topologie, der es Ihnen ermöglicht, die beste Topologie für Ihre Anforderungen zu bestimmen. Anweisungen und Beispiele finden Sie unten.

Anweisungen

1. Schreiben Sie die Fragen auf, die Sie mit "Ja" beantwortet haben.
2. Wenn Sie mehrere Fragen mit "Ja" beantwortet haben, befolgen Sie die Topologieempfehlung für die Frage mit der höchsten Nummer. Wenn mehrere Topologieoptionen angegeben sind (beispielsweise "D/C/M"), sehen Sie sich die vorhergehenden Fragen an, um zu bestimmen, welche Option sich für Sie am besten eignet.
3. Ihr Topologiekategoriecode beginnt mit dem Buchstaben, der die Indexerschicht darstellt (z. B. "C" oder "M"). Auf diesen Buchstaben folgt die Zahl, die die Suchschicht darstellt (z. B. "1" oder "13").

Beispiel 1

Angenommen, Sie haben die Fragen 3, 5 und 8 mit "Ja" beantwortet. Sie erhalten schließlich die Topologiekategorie "C13", was die Notwendigkeit einer Cluster-Indizierungsschicht mit zwei Search Head-Clustern angibt.



Beispiel 2

Nehmen wir nun an, Sie haben nur Frage 1 mit "Ja" beantwortet. Sie erhalten als Ergebnis die Topologiekategorie "S1", was eine Single Server-Bereitstellung von Splunk als Ihre ideale Topologie bedeutet.

Schritt 2a: Wahl einer Topologie für Indizierung und Suche

Topologien teilen sich allgemein in Bereitstellungen mit und ohne Cluster auf. Bereitstellungen ohne Cluster erfordern die kleinste Menge von Einzelkomponenten und bieten hervorragende Skalierungseigenschaften. Bedenken Sie, dass Bereitstellungen ohne Cluster zwar eingeschränkte Funktionen zu Verfügbarkeit und Disaster Recovery bieten, diese Bereitstellungsoption aber trotzdem eine gute Wahl für Ihre Organisation sein kann.

Denken Sie daran: Das Hauptziel des SVA-Auswahlprozesses besteht darin, Ihnen den Aufbau der benötigten Lösung zu ermöglichen, ohne unnötige Komponenten einzufügen.

Hinweis

Zwar können Sie sich für die Implementierung einer Topologie entscheiden, die über Ihre unmittelbaren Bedürfnisse hinaus zusätzliche Vorzüge bietet, Sie sollten aber bedenken, dass dies wahrscheinlich unnötige Kosten nach sich zieht. Darüber hinaus ist die Einbringung weiterer Komplexität im Hinblick auf Prozesseffizienz oftmals kontraproduktiv.

Wichtiger Hinweis zu Topologiediagrammen

Die Symbole in den Topologiediagrammen stellen **funktionale Splunk-Rollen** dar und implizieren keine dedizierte Infrastruktur für die Ausführung. Hinweise dazu, welche Splunk-Rollen in der gleichen Infrastruktur/auf dem gleichen Server ausgeführt werden können, finden Sie im Anhang.

Verwenden Ihres Topologiekategoriecodes

Es empfiehlt sich, vor der Wahl einer Topologieoption den Anforderungsfragebogen auszufüllen, um Ihren Topologiekategoriecode zu bestimmen. Wenn Sie dies noch nicht getan haben, gehen Sie bitte zurück, und schließen Sie oben den vorhergehenden Schritt ab. Sobald Sie Ihren Topologiekategoriecode ermittelt haben, können Sie die Bereitstellungsoption bestimmen, die für die von Ihnen angegebenen Anforderungen optimal passt.

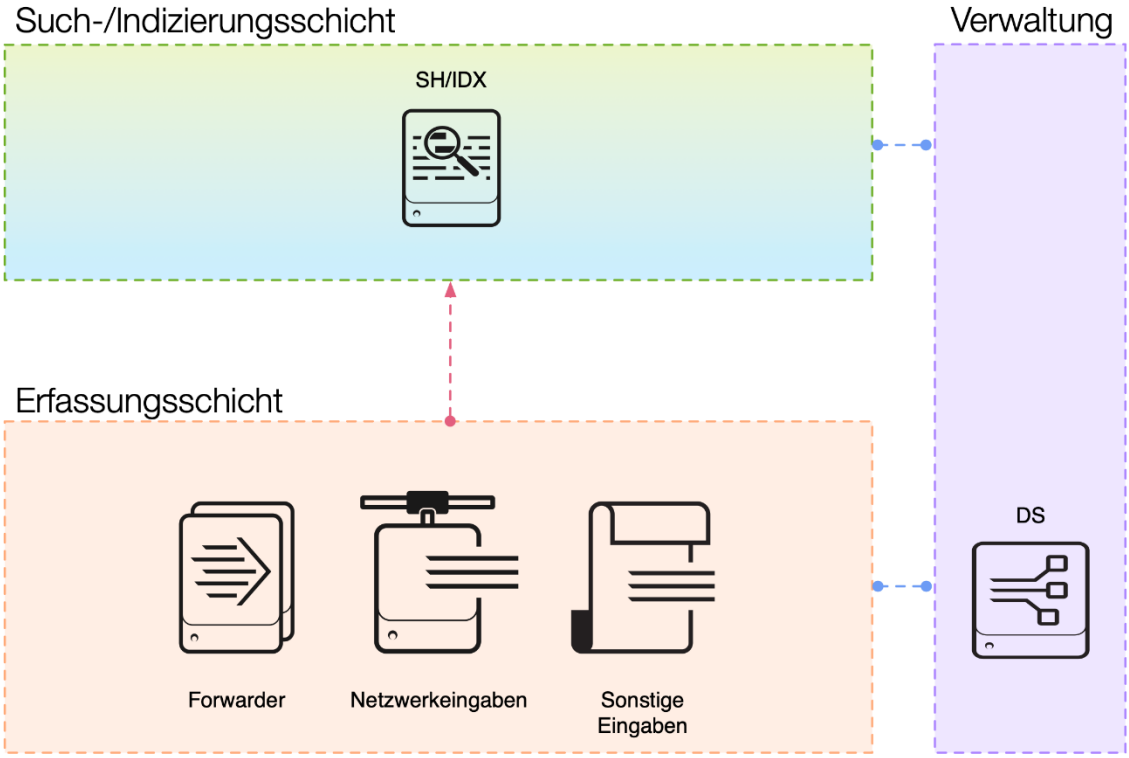
Bereitstellungsoptionen ohne Cluster

Unten finden Sie die folgenden Topologieoptionen:

Art der Bereitstellung	Topologiekategoriecode(s)
Single Server-Bereitstellung	S1
Verteilte Bereitstellung ohne Cluster	D1/D11

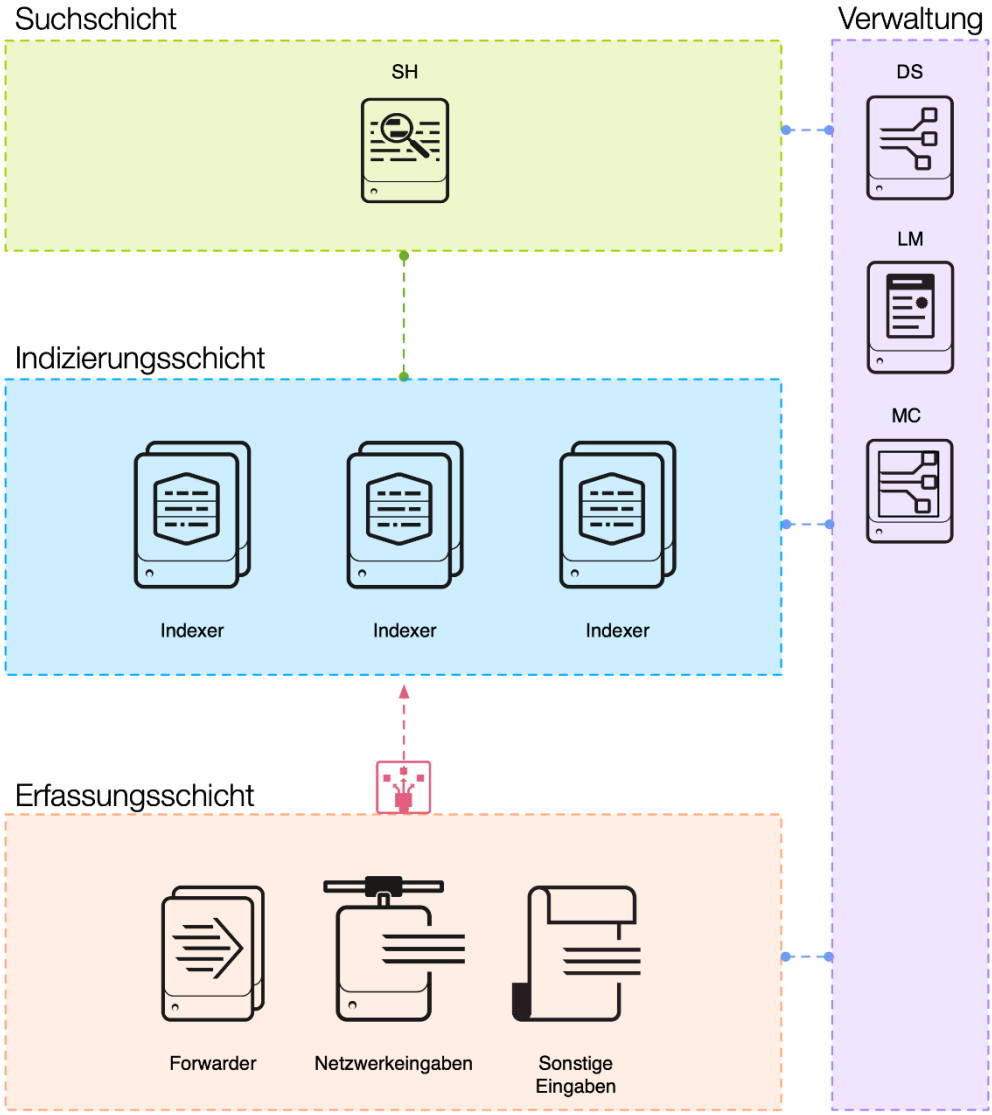
Eine Erläuterung der Topologiekomponenten finden Sie in Anhang "B" unten.

Single Server-Bereitstellung (S1)



Beschreibung der Single Server-Bereitstellung (S1)	Einschränkungen
Diese Bereitstellungstopologie bietet Ihnen eine sehr kostengünstige Lösung, wenn Ihre Umgebung allen der folgenden Kriterien entspricht: a) Es besteht kein Erfordernis zur Bereitstellung von Hochverfügbarkeit oder automatischer Disaster Recovery für Ihre Splunk-Bereitstellung, b) Das Volumen Ihrer täglichen Datenerfassung liegt unterhalb von 300 GB/Tag und c) Sie haben eine kleine Benutzeranzahl ohne kritische Suchanwendungsfälle. Diese Topologie wird normalerweise für kleinere, nicht unternehmenswichtige Anwendungsfälle (häufig in Abteilungen) eingesetzt. Zu den geeigneten Anwendungsfällen zählen Testumgebungen für Datenintegration, kleine DevOps-Anwendungsfälle und Integrationsumgebungen und ähnliche Szenarien. Zu den wichtigsten Vorzügen dieser Topologie gehören die einfache Verwaltung, gute Suchleistung für kleinere Datenvolumen und feste Gesamtbetriebskosten.	• Keine Hochverfügbarkeit für Suche/Indizierung • Skalierbarkeit durch die Hardwarekapazität eingeschränkt (geradliniger Migrationspfad zu einer verteilten Bereitstellung)

Verteilte Bereitstellung ohne Cluster (D1/D11)



Beschreibung der verteilten Bereitstellung ohne Cluster (D1/D11)	Einschränkungen
Sie müssen in den folgenden Situationen auf eine verteilte Topologie umstellen: a) Ihr tägliches Datenvolumen, das an Splunk gesendet werden soll, übersteigt die Kapazität einer Single Server-Bereitstellung oder b) Sie möchten/müssen hoch verfügbare Datenerfassung bereitstellen. Das Bereitstellen mehrerer, unabhängiger Indexer ermöglicht Ihnen die lineare Skalierung Ihrer Indexkapazität und erhöht implizit die Verfügbarkeit zur Datenerfassung. Die Gesamtbetriebskosten steigen in einer vorhersagbaren und linearen Weise in dem Maß, da Sie Indexerknoten hinzufügen. Die empfohlene Einführung der Monitoring-Konsolenkomponente (Monitoring Console, MC) erlaubt es Ihnen, Integrität und Kapazität Ihrer verteilten Umgebung zu überwachen. Darüber hinaus stellt die MC ein zentrales Warnsystem bereit, so	• Keine Hochverfügbarkeit für die Suchschicht • Eingeschränkte Hochverfügbarkeit für die Indizierungsschicht, Ausfall von Knoten kann zu unvollständigen Suchergebnissen für Verlaufssuchen führen

Beschreibung der verteilten Bereitstellung ohne Cluster (D1/D11)	Einschränkungen
dass Sie von fehlerhaften Zuständen in Ihrer Bereitstellung in Kenntnis gesetzt werden. Die Search Heads müssen bei jedem Hinzufügen neuer Indexer manuell mit der Liste der verfügbaren Such-Peers konfiguriert werden. **Hinweis für ES-Kunden:** Wenn Ihr Kategoriecode D1 ist (d.h., Sie beabsichtigen, die Splunk App for Enterprise Security bereitzustellen), ist **ein einzelner dedizierter** Search Head für die Bereitstellung der App erforderlich (dies ist im Topologiediagramm nicht dargestellt). Die Erfassungsschicht muss bei jedem Hinzufügen neuer Indexer mit der Liste der Zielindexer konfiguriert werden (mithilfe eines Verteilungs-Servers). Diese Bereitstellungstopologie lässt sich linear bis auf über 1.000 Indexerknoten skalieren und kann auf diese Weise extrem hohe Erfassungs- und Suchvolumina unterstützen. Die Suchleistung kann über große Datasets durch übergreifende parallele Ausführung der Suche auf mehreren Indexern (Map/Reduce) aufrecht erhalten bleiben. Auch wenn er nicht spezifisch als separate Topologie aufgegliedert ist, kann ein Search Head-Cluster zum Erhöhen der Suchkapazität in der Suchschicht verwendet werden (mehr dazu finden Sie in der Suchschicht in Topologie C3/C13).	

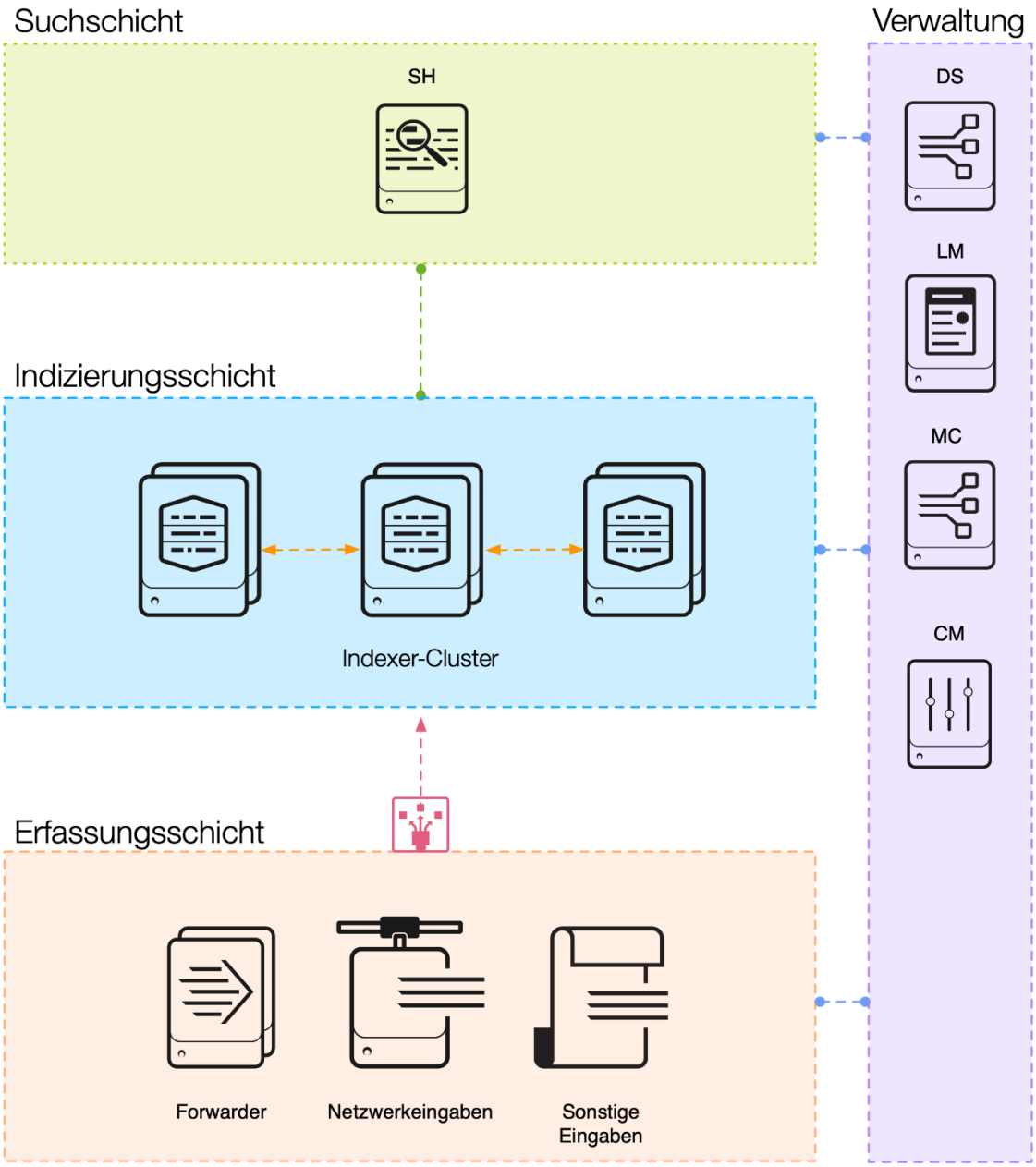
Bereitstellungsoptionen mit Cluster

Unten finden Sie die folgenden Topologieoptionen:

Art der Bereitstellung	Topologiekategoriecode(s)
Verteilte Bereitstellung mit Cluster – Einzelner Standort	C1/C11
Verteilte Bereitstellung mit Cluster + SHC – Einzelner Standort	C3/C13
Verteilte Bereitstellung mit Cluster – Mehrere Standorte	M2/M12
Verteilte Bereitstellung mit Cluster + SHC – Mehrere Standorte	M3/M13
Verteilte Bereitstellung mit Cluster + SHC – Mehrere Standorte	M4/M14

Eine Erläuterung der Topologiekomponenten finden Sie in Anhang "B" unten.

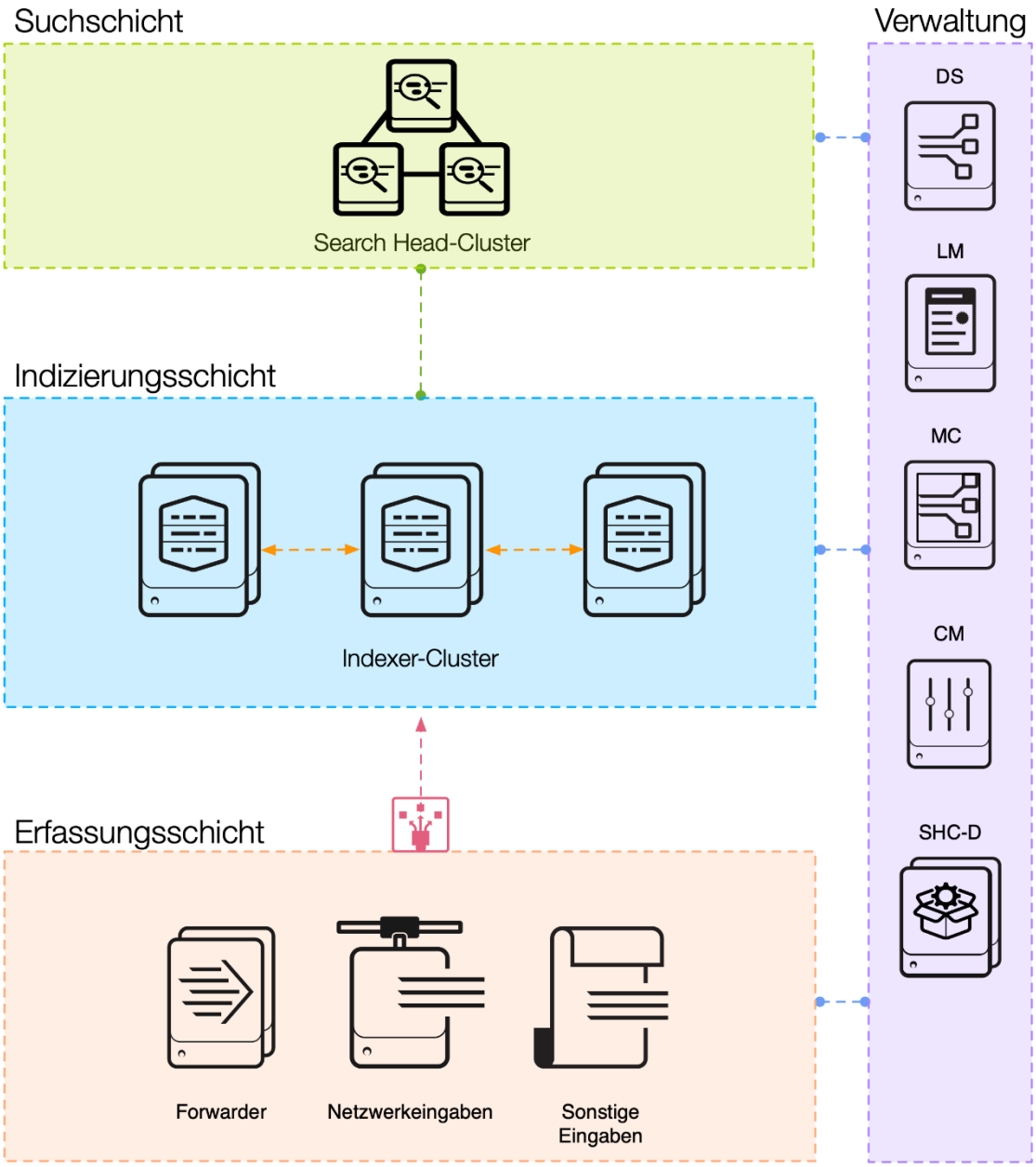
Verteilte Bereitstellung mit Cluster – Einzelner Standort (C1/C11)



Beschreibung der verteilten Bereitstellung mit Cluster – Einzelner Standort (C1/C11)	Einschränkungen
Diese Topologie führt Indexer-Clustering in Verbindung mit einer passend konfigurierten Richtlinie zur Datenreplikation ein. Dadurch steht Hochverfügbarkeit der Daten für den Fall des Ausfalls eines Indexer-Peer-Knotens zur Verfügung. Es sollten Ihnen jedoch bewusst sein, dass dies nur für die Indizierungsschicht gilt und kein Schutz vor Search Head-Ausfällen besteht. **Hinweis für ES-Kunden:** Wenn Ihr Kategoriecode C11 ist (d.h., Sie beabsichtigen, die Splunk App for Enterprise Security bereitzustellen), ist **ein einzelner dedizierter** Search Head für die Bereitstellung der App	• Keine Hochverfügbarkeit für die Suchschicht • Die Gesamtzahl der eindeutigen Buckets im Indexer-Cluster ist auf 5 MM (V6.6+) bei 15 MM Buckets insgesamt beschränkt • Keine Fähigkeit zu automatischem DR im Fall eines Rechenzentrumsausfalls

Beschreibung der verteilten Bereitstellung mit Cluster – Einzelner Standort (C1/C11)	Einschränkungen
erforderlich (dies ist im Topologiediagramm nicht dargestellt). Für diese Topologie ist eine zusätzliche Splunk-Komponente erforderlich, die als Cluster-Master (CM) bezeichnet wird. Der CM ist für die Koordination und Durchsetzung der konfigurierten Richtlinie zur Datenreplikation zuständig. Der CM dient außerdem als verbindliche Quelle für verfügbare Cluster-Peers (Indexer). Die Search Head-Konfiguration vereinfacht sich, indem der CM anstelle einzelner Such-Peers konfiguriert wird. Es besteht die Option, die Weiterleitungsschicht zu konfigurieren, um verfügbare Indexer über den CM zu ermitteln. Dies vereinfacht die Verwaltung der Weiterleitungsschicht. Bedenken Sie, dass Daten innerhalb des Clusters auf nicht deterministische Weise repliziert werden. Sie haben keine Kontrolle darüber, wo angeforderte Kopien einzelner Ereignisse gespeichert werden. Ferner bestehen trotz linearer Skalierbarkeit Einschränkungen hinsichtlich der Clustergesamtgröße (~50 PB durchsuchbarer Daten unter Idealbedingungen). Wir empfehlen die Bereitstellung der Monitoring-Konsole (Monitoring Console, MC) zur Überwachung der Integrität Ihrer Splunk-Umgebung.	

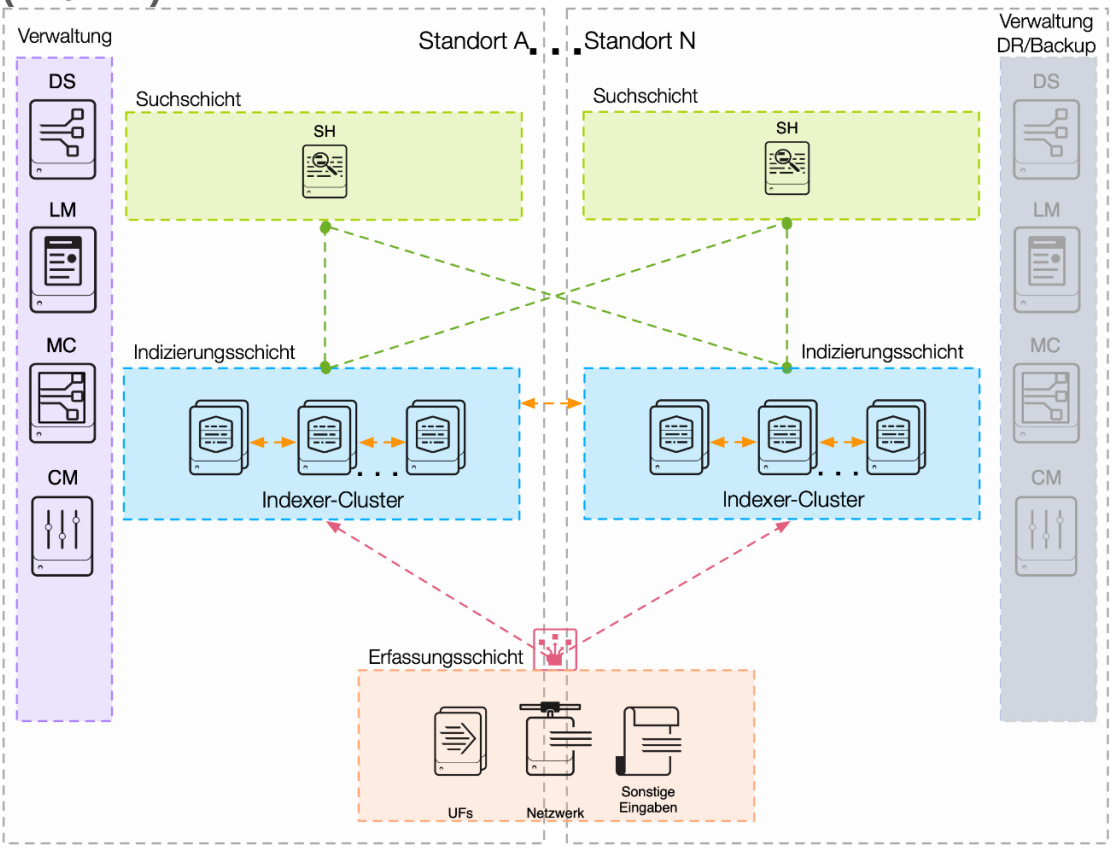
Verteilte Bereitstellung mit Cluster + SHC – Einzelner Standort (C3/C13)



Beschreibung der verteilten Bereitstellung mit Cluster + SHC – Einzelner Standort (C3/C13)	Einschränkungen
Diese Topologie fügt horizontale Skalierbarkeit hinzu und beseitigt die isolierte Schwachstelle (Single Point of Failure) aus der Suchschicht. Zum Implementieren eines SHCs sind mindestens drei Search Heads erforderlich. Zum Verwalten der SHC-Konfiguration ist für jeden SHC eine zusätzliche Splunk-Komponente erforderlich, die als Search Head Cluster-Verteiler (Search Head Cluster Deployer)bezeichnet wird. Diese Komponente ist erforderlich, um Änderungen an den Konfigurationsdateien im Cluster zu verteilen. Für den	• Keine Fähigkeit zum DR im Fall eines Rechenzentrumsausfalls • ES erfordert einen dedizierten SH/SHC • Das Verwalten einer ES-Bereitstellung auf einem SHC ist unterstützt, aber schwierig durchzuführen (beinhaltet PS) • Ein SHC kann nicht mehr als 100 Knoten aufweisen

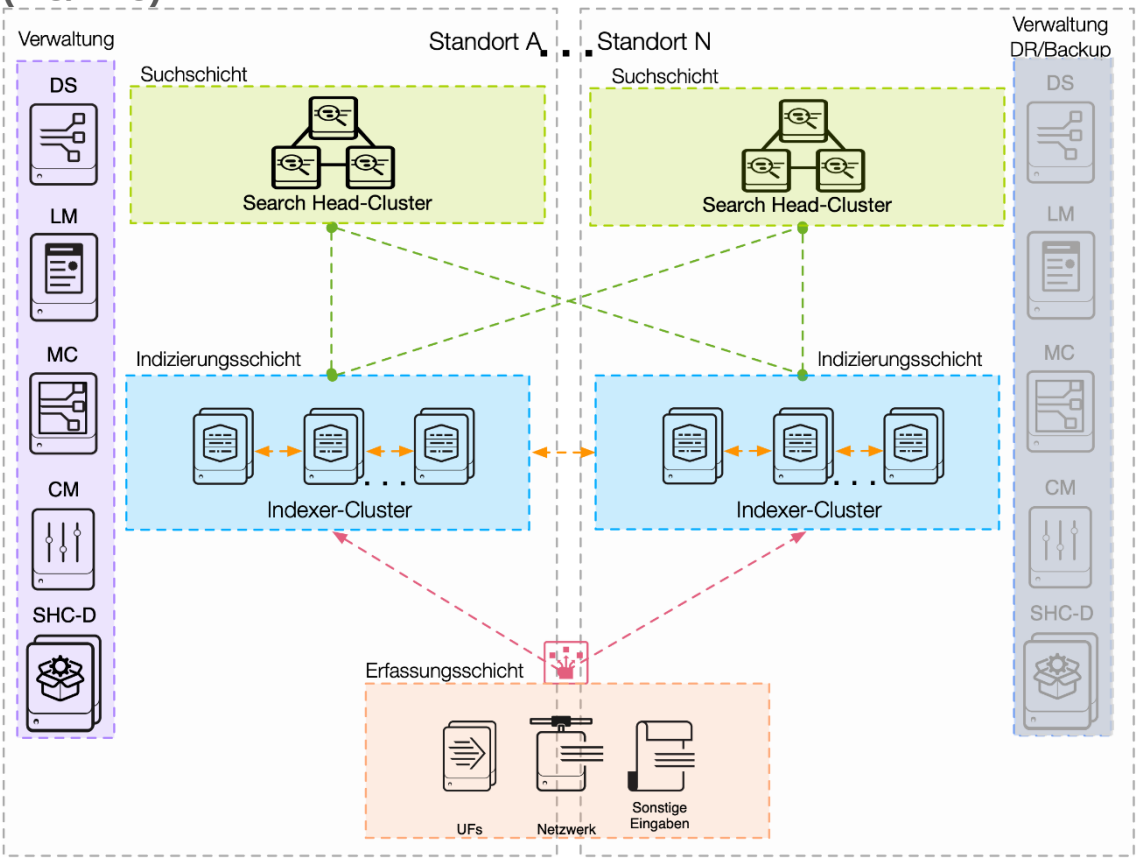
Beschreibung der verteilten Bereitstellung mit Cluster + SHC – Einzelner Standort (C3/C13)	Einschränkungen
Search Head Cluster-Verteiler gelten keine HA-Anforderungen (keine Laufzeitrolle). Der SHC stellt den Mechanismus zur Erhöhen der verfügbaren Suchkapazität jenseits dessen zur Verfügung, was ein einzelner Search Head leisten kann. Darüber hinaus ermöglicht der SHC die Verteilung geplanter Suchworkloads über den Cluster. Der SHC bietet außerdem optimales Benutzerfailover im Fall eines Search Head-Ausfalls. Ein Netzwerk-Load Balancer mit Unterstützung von Sticky Sessions vor den SHC-Mitgliedern ist erforderlich, um ordnungsgemäßen Lastenausgleich über den gesamten Cluster sicherzustellen. **Hinweis für ES-Kunden:** Wenn Ihr Kategoriecode C13 ist (d. h., Sie beabsichtigen, die Splunk App for Enterprise Security bereitzustellen), ist **ein dedizierter** Search Head-Cluster für die Bereitstellung der App erforderlich (dies ist im Topologiediagramm nicht dargestellt). Die Suchschicht kann gruppierte und nicht gruppierte Search Heads enthalten (also in Clustern oder einzeln), abhängig von den Anforderungen Ihrer Organisation und der erforderlichen Kapazität (auch dies ist im Topologiediagramm nicht dargestellt).	

Verteilte Bereitstellung mit Cluster – Mehrere Standorte (M2/M12)



Beschreibung der verteilten Bereitstellung mit Cluster –- Mehrere Standorte (M2/M12)	Einschränkungen
Um im Fall eines katastrophalen Ereignisses (wie eines Rechenzentrumsausfalls) nahezu automatische Disaster Recovery zu bieten, ist eine Clusterumgebung mit mehreren Standorten die Architektur der Wahl. Ein intakter Cluster mit mehreren Standorten erfordert akzeptable Netzwerklatenz zwischen den Standorten, wie in der Splunk-Dokumentation dargelegt. Mithilfe dieser Topologie können Daten **deterministisch** auf zwei oder mehr Gruppen von Indexer-Cluster-Peers repliziert werden. Sie können die Standortreplikation und den Suchfaktor konfigurieren. Dieser Standortreplikationsfaktor ermöglicht Ihnen, festzulegen, wohin Replikatkopien gesendet werden, und stellt sicher, dass die Daten über mehrere Standorte verteilt sind. Die Verwaltung erfolgt trotzdem über einen einzelnen Cluster-Master-Knoten, für den im Notfall ein Failover auf den DR-Standort ausgeführt werden muss. Multi-Site-Clustering stellt Datenredundanz über physisch voneinander getrennte verteilte Standorte bereit, mit der Möglichkeit einer geografisch getrennten Verteilung. Das Failover von Benutzern auf den DR-Standort kann automatisch erfolgen, um die Verfügbarkeit sicherzustellen. Diese Topologie stellt jedoch keinen Mechanismus zum automatischen standortübergreifenden Synchronisieren der Konfiguration der Suchschicht und der Laufzeitartefakte bereit. Die standortübergreifende verfügbare Such-Peer-Kapazität (Indexerkapazität) kann für die Suchausführung in einem aktiv/aktiven Modell genutzt werden. Nach Möglichkeit kann Standortaffinität konfiguriert werden, um sicherzustellen, dass die beim Search Head eines bestimmten Standorts angemeldeten Benutzer nur die lokalen Indexer durchsuchen. **Hinweis für ES-Kunden:** Wenn Ihr Kategoriecode M11 ist (d. h., Sie beabsichtigen, die Splunk App for Enterprise Security bereitzustellen), ist **ein einzelner dedizierter** Search Head für die Bereitstellung der App erforderlich (dies ist im Topologiediagramm nicht dargestellt). Für den ES-Search Head beinhaltet ein Failover das Einrichten eines "Schatten"-Search Heads am Failoverstandort, der nur in DR-Situationen aktiviert und verwendet wird. Verpflichten Sie die Splunk Professional Services mit der Entwicklung und Implementierung eines Standort-Failovermechanismus für Ihre Enterprise Security-Bereitstellung.	• Keine gemeinsame Verwendung der verfügbaren Search Head-Kapazität und keine **standortübergreifende** Replikation von Suchartefakten • Ein Ausfall der Managementfunktionen muss bei einem Standortausfall außerhalb von Splunk behandelt werden • Die standortübergreifende Latenz für Indexreplikation muss innerhalb der empfohlenen Grenzwerte liegen

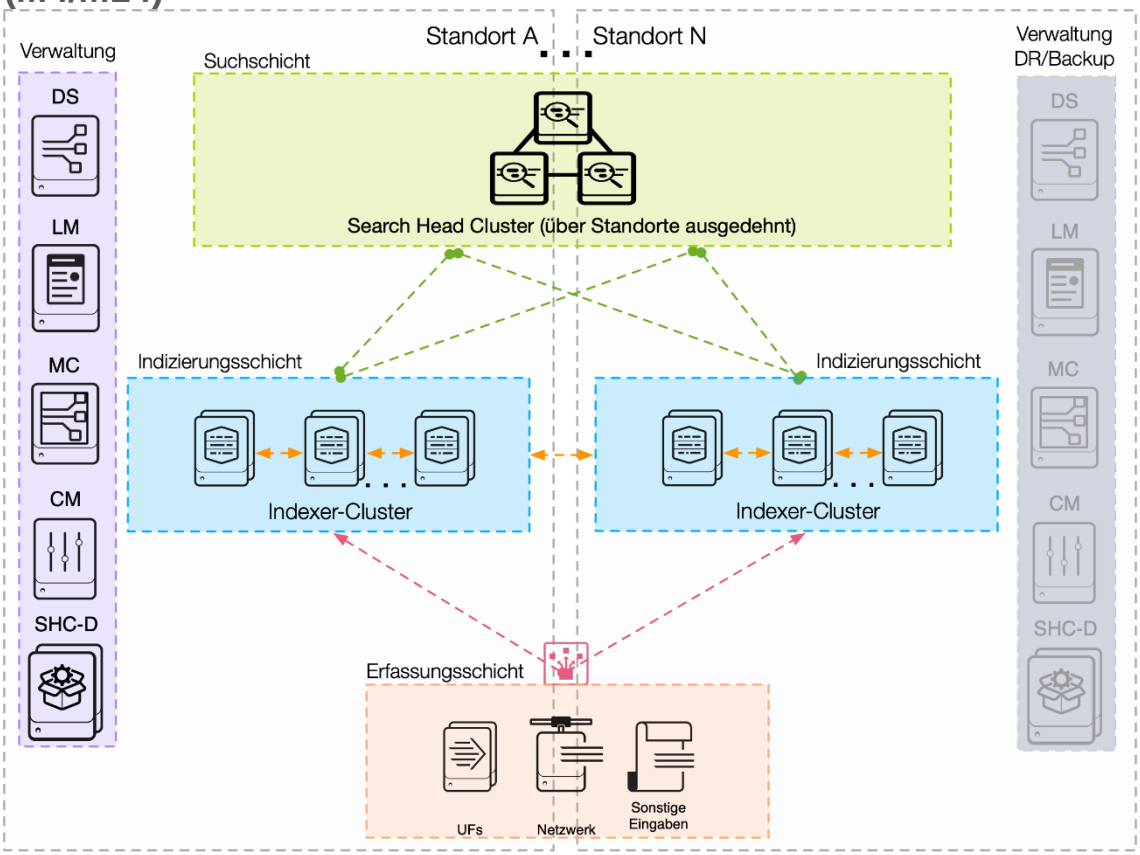
Verteilte Bereitstellung mit Cluster + SHC – Mehrere Standorte (M3/M13)



Beschreibung der verteilten Bereitstellung mit Cluster + SHC – Mehrere Standorte (M3/M13)	Einschränkungen
Diese Topologie fügt horizontale Skalierbarkeit hinzu und beseitigt die isolierte Schwachstelle (Single Point of Failure) aus der Suchschicht an jedem Standort. Zum Implementieren eines SHCs sind mindestens drei Search Heads (pro Standort) erforderlich. Zum Verwalten der SHC-Konfiguration ist **für jeden** SHC eine zusätzliche Splunk-Komponente erforderlich, die als Search Head Cluster Deployer bezeichnet wird. Diese Komponente ist erforderlich, um Änderungen an den Konfigurationsdateien im Cluster zu verteilen. Für den Search Head Cluster Deployer gelten keine HA-Anforderungen (keine Laufzeitrolle). Der SHC bietet die folgenden Vorzüge: a) erhöhte verfügbare Suchkapazität jenseits dessen, was von einem einzelnen Search Head zur Verfügung gestellt werden kann, b) Workloadverteilung von geplanten Suchen über den Cluster und c) optimales Benutzerfailover bei Ausfall eines Search Heads. Ein Netzwerk-Lastenausgleich mit Unterstützung von Sticky Sessions vor den SHC-Mitgliedern ist an jedem Standort erforderlich, um ordnungsgemäßen Lastenausgleich über den gesamten Cluster sicherzustellen.	• Keine standortübergreifende Replikation von Suchartefakten, die SHCs sind eigenständig • Die standortübergreifende Latenz für Indexreplikation muss innerhalb der dokumentierten Grenzwerte liegen. • Ein SHC kann nicht mehr als 100 Knoten aufweisen

Beschreibung der verteilten Bereitstellung mit Cluster + SHC – Mehrere Standorte (M3/M13)	Einschränkungen
Hinweis für ES-Kunden: Wenn Ihr Kategoriecode M13 ist (d. h., Sie beabsichtigen, die Splunk App for Enterprise Security bereitzustellen), ist ein einzelner dedizierter Search Head-Cluster *innerhalb jedes Standorts* für die Bereitstellung der App erforderlich (dies ist im Topologiediagramm nicht dargestellt). Um eine ES SH-Umgebung nach einem Standortausfall wiederherstellen zu können, kann Technologie von Drittanbietern verwendet werden, um einen Failover der Search Head-Instanzen auszuführen. Alternativ kann ein ES SH in "warmem Standby" bereitgestellt und mit der primären ES-Umgebung synchron gehalten werden. Es wird dringend empfohlen, für die Bereitstellung von ES in einer HA/DR-Umgebung mit den Splunk Professional Services Kontakt aufzunehmen.	

Verteilte Bereitstellung mit Cluster + SHC – Mehrere Standorte (M4/M14)



Beschreibung der verteilten Bereitstellung mit Cluster + SHC – Mehrere Standorte (M4/M14)	Einschränkungen
Dies ist die komplexeste validierte Architektur, ausgelegt für Bereitstellungen, für die strenge Anforderungen an Hochverfügbarkeit und Disaster Recovery gelten. Für eine ordnungsgemäße Bereitstellung empfehlen wir dringend die Einschaltung der Splunk Professional Services. Bei ordnungsgemäßer Bereitstellung bietet	• Die Netzwerklatenz zwischen den Standorten muss innerhalb der dokumentierten Grenzwerte liegen • Für das Failover des SHCs sind möglicherweise manuell

Beschreibung der verteilten Bereitstellung mit Cluster + SHC – Mehrere Standorte (M4/M14)	Einschränkungen
diese Topologie fortlaufenden Betrieb Ihrer Splunk-Infrastruktur zur Datenerfassung, Indizierung und Suche. Diese Topologie bringt die Implementierung eines "ausgedehnten" Search Head-Clusters mit sich, der einen oder mehrere Standorte überspannt. Dies bietet optimales Failover für Benutzer beim Ausfall eines Suchknotens oder Rechenzentrums. Suchartefakte und andere Wissensobjekte zur Laufzeit werden im SHC repliziert. Sorgfältige Konfiguration ist erforderlich, um sicherzustellen, dass die Replikation standortübergreifend erfolgt, da der SHC seinerseits keine Standorterkennung besitzt (d. h., die Replikation von Artefakten ist nicht deterministisch). Es kann Standortaffinität konfiguriert werden, um sicherzustellen, dass die WAN-Verbindung zwischen den Standorten nur in Fällen verwendet wird, in denen eine Suche nicht lokal bedient werden kann. Ein Netzwerk-Load Balancer mit Unterstützung von Sticky Sessions vor den SHC-Mitgliedern ist erforderlich, um ordnungsgemäßen Lastenausgleich über den gesamten Cluster sicherzustellen. **Hinweis für ES-Kunden:** Wenn Ihr Kategoriecode M14 ist (d. h., Sie beabsichtigen, die Splunk App for Enterprise Security bereitzustellen), ist ein einzelner dedizierter Search Head-Cluster *innerhalb jedes Standorts* für die Bereitstellung der App erforderlich (dies ist im Topologiediagramm nicht dargestellt). Für ES muss ein konsistenter Satz Laufzeitartefakte verfügbar sein, und dies kann bei einem ausgedehnten SHC beim Ausfall eines Standorts nicht gewährleistet werden. Um eine ES SH-Umgebung nach einem Standortausfall wiederherstellen zu können, kann Technologie von Drittanbietern verwendet werden, um einen Failover der Search Head-Instanzen auszuführen. Alternativ kann ein ES SH in "warmem Standby" bereitgestellt und mit der primären ES-Umgebung synchron gehalten werden. Es wird dringend empfohlen, für die Bereitstellung von ES in einer HA/DR-Umgebung mit den Splunk Professional Services Kontakt aufzunehmen.	auszuführende Schritte erforderlich, wenn nur eine Minderheit der Clustermitglieder weiter ausgeführt wird

Schritt 1b: Definition Ihrer Anforderungen an die Datenerfassung

Die Datenerfassungsschicht bildet eine Kernkomponente einer Splunk-Bereitstellung. Sie ermöglicht jedem Gerät in Ihrer Umgebung die Weiterleitung von Daten an die Indizierungsschicht zur Verarbeitung, damit sie für die Suche in Splunk zur Verfügung gestellt werden können. Der wichtigste Faktor ist hier, sicherzustellen, dass Weiterleitung und Indizierung so effizient und zuverlässig wie möglich erfolgen, da die für den Erfolg und die Leistung Ihrer Splunk-Bereitstellung kritisch ist.

Berücksichtigen Sie die folgenden Architekturaspekte Ihrer Datenerfassungsschicht:

- Den Ursprung Ihrer Daten. Stammen sie aus Logdateien, Syslog-Quellen, Netzwerkeingaben, Event-Protokollierungsfunktionen von Betriebssystem, Anwendungen, Message Bus oder von anderswo?
- Anforderungen an Latenz und Durchsatz der Datenerfassung
- Ideale Ereignisverteilung über die Indexer in Ihrer Indizierungsschicht
- Fehlertoleranz und automatische Wiederherstellung (HA)
- Sicherheit und Anforderungen an die Datenherrschaft

Dieser Abschnitt von SVAs legt den Schwerpunkt auf die allgemeinen Methoden der Datenerfassung. Er erörtert darüber hinaus Architektur und Best Practices für jede Datenerfassungsmethode und weist auf potenzielle Probleme hin, die Sie bei der Auswahl Ihrer Implementierung berücksichtigen müssen.

Wichtige Architekturüberlegungen und die Gründe ihrer Wichtigkeit

Angesichts der wesentlichen Rolle der Datenerfassungsschicht ist ein Verständnis der in den Entwurf der Architektur einfließenden Grundüberlegungen unverzichtbar.

Während einige dieser Überlegungen für Sie auf der Grundlage Ihrer Anforderungen relevant oder irrelevant sein können, beschreiben die fett formatierten Überlegungen in der Tabelle unten grundlegende Punkte, die für jede Umgebung relevant sind.

Überlegung	**Warum ist dieser Punkt wichtig?**
Die Daten werden ordnungsgemäß erfasst (Zeitstempel, Zeilenumbrüche, Beschneidung)	Die Wichtigkeit der idealen Ereignisverteilung unter den Indexern kann gar nicht genug betont werden. Die Indizierungsschicht arbeitet dann besonders effizient, wenn alle verfügbaren Indexer gleichmäßig ausgelastet werden. Dies gilt sowohl für die Datenerfassung als auch für die Suchleistung. Ein einzelner Indexer, der erheblich mehr erfasste Daten als seine Peers verarbeitet, kann die Antwortzeiten der Suche negativ beeinflussen. Bei Indexern mit beschränktem lokalem Datenträger-Speicherplatz kann die ungleiche Ereignisverteilung sogar zu einem vorzeitigen Ablauf von Daten führen, bevor der konfigurierten Richtlinie für die Datenaufbewahrung Genüge getan ist.
Die Daten sind optimal auf die verfügbaren Indexer verteilt	Wenn die Daten nicht ordnungsgemäß erfasst werden, weil Ereigniszeitstempel und Zeilenumbrüche nicht ordnungsgemäß konfiguriert sind, wird das Durchsuchen dieser Daten sehr schwierig. Dies hat den Grund, dass Ereignisgrenzen zum Suchzeitpunkt erzwungen werden müssen. Fehlerhafte oder fehlende Konfigurationen zur Zeitstempelextraktion können zu unerwünschter impliziter Zuweisung von Zeitstempeln führen. Dies ist für Ihre Benutzer verwirrend und macht das Erzielen von Mehrwert aus Ihren Daten sehr viel schwieriger als nötig.
Alle Daten erreichen die Indizierungsschicht zuverlässig und ohne Verlust	Alle Protokolldaten, die zum Zweck zuverlässiger Analyse erfasst werden, müssen vollständig und gültig sein, damit auf den Daten ausgeführte Suchen zu gültigen und akkuraten Ergebnissen führen.

Alle Daten erreichen die Indizierungsschicht mit minimaler Latenz	Verzögerungen bei der Datenerfassung verlängern die Zeit zwischen dem Eintreten eines möglicherweise kritischen Ereignisses und der Möglichkeit, nach ihm zu suchen und auf es zu reagieren. Minimale Latenz bei der Datenerfassung ist oftmals kritisch in Monitoring-Anwendungsfällen, bei denen Warnungen an Mitarbeiter ausgelöst oder automatisierte Aktionen eingeleitet werden.
Die Daten sind während der Übermittlung gesichert	Wenn die Daten entweder vertraulich sind oder während des Transports über nicht vertrauenswürdige Netzwerke geschützt werden müssen, ist ggf. Verschlüsselung der Daten erforderlich, um unberechtigtes Abfangen durch Dritte zu verhindern. Im Allgemeinen empfehlen wir, dass für alle Verbindungen zwischen Splunk-Komponenten SSL aktiviert wird.
Die Nutzung von Netzwerkressourcen wird minimiert	Der Einfluss der Logdatenerfassung auf Netzwerkressourcen muss minimiert werden, um anderen kritischen geschäftlichen Netzwerkverkehr nicht zu beeinträchtigen. Bei Netzwerken auf gemieteten Leitungen trägt die Minimierung der Netzwerknutzung außerdem zu geringeren Gesamtbetriebskosten Ihrer Bereitstellung bei.
Authentifizierung/Autorisierung von Datenquellen	Um die Beeinträchtigung Ihrer Indizierungsumgebung durch unzulässige Datenquellen zu verhindern, erwägen Sie die Implementierung von Verbindungsauthentifizierung/-autorisierung. Dies kann durch die Verwendung von Netzwerkkontrollen oder durch den Einsatz von Mechanismen auf Anwendungsebene (z. B. SSL/TLS) erfolgen.

Aufgrund der wichtigen Rolle, die sie in Ihrer Bereitstellung spielt, konzentriert sich die in diesem Dokument gegebene Orientierung auf Architekturen, die eine ideale Ereignisverteilung unterstützen. Wenn eine Splunk-Umgebung nicht die erwartete Suchleistung bereitstellt, wird dies in nahezu allen Fällen durch nicht erfüllte Minimalanforderungen an die Speicherleistung und/oder ungleichmäßige Verteilung von Ereignissen verursacht, die die Nutzung der Suchparallelisierung einschränkt.

Da Ihnen die kritischsten Überlegungen zur Architektur jetzt bekannt sind, finden wir heraus, welche spezifischen Anforderungen an die Datenerfassung Sie erfüllen müssen.

Fragebogen 2: Definition Ihrer Anforderungen an die Datenerfassung

Durch Beantworten der folgenden Fragen erhalten Sie eine Liste der Datenerfassungskomponenten, die Sie in Ihrer Bereitstellung benötigen. Sie können die Schlüssel in der äußerst rechten Spalte verwenden, um weitere Details zu den einzelnen Komponenten weiter unten im Dokument herauszufinden.

Nr.	Frage	Überlegungen	Einfluss auf Topologie	Relevante Daten-erfassungs-komponenten
1	Müssen Sie lokale Dateien überwachen oder Skripts zur Datenerfassung auf	Dies stellt eine Kernanforderung für nahezu alle Splunk-Bereitstellungs-szenarien dar.	Sie müssen auf den Endpunkten den universellen Forwarder installieren und seine	UF

	Endpunkten ausführen?		Konfiguration zentral verwalten.	
2	Müssen Sie Logdaten erfassen, die mithilfe von Syslog von Geräten gesendet werden, auf denen Sie keine Software installieren können (Appliances, Netzwerkschalter usw.)?	Syslog ist ein geradezu allgegenwärtiges Transportprotokoll, das oftmals von zweckspezifischen Geräten verwendet wird, die keine Installation von benutzerdefinierter Software zulassen.	Sie benötigen eine Syslog-Serverinfrastruktur, die als Erfassungspunkt dient.	SYSLOG HES
3	Müssen Sie die Erfassung von Logdaten aus Anwendungen unterstützen, die auf eine API protokollieren, statt auf lokale Datenträger zu schreiben?	Das Schreiben von Logdateien auf Endpunkten erfordert das Bereitstellen von Datenträger-Speicherplatz und eine entsprechende Verwaltung der Logdateien (Rotation, Löschung usw.). Manche Kunden möchten diesem Modell den Rücken kehren und mithilfe verfügbarer Logbibliotheken direkt in Splunk protokollieren.	Sie müssen die Splunk HTTP-Ereignissammlung (HES) oder eine andere Technologie verwenden, die als Logsenke dient.	HES
4	Müssen Sie Daten von einem Streaming-Ereignisdatenanbieter erfassen?	Viele Unternehmen haben ein Event Hub-Modell übernommen, bei dem eine zentrale Datenstreaming-Plattform (wie AWS Kinesis oder Kafka) als Nachrichtentransport zwischen den Produzenten und Verbrauchern von Logdaten dient.	Sie benötigen eine Integration zwischen dem Datenstreaming-anbieter und Splunk.	KAFKA KINESIS HES
5	Sind bei Ihnen nicht verhandelbare Sicherheitsrichtlinien aktiv, die die Einrichtung direkter TCP-Verbindungen mit der Indizierungs-schicht verhindern?	Manchmal bestehen Netzwerktopologien aus mehreren Netzwerkzonen mit restriktiven Firewallregeln zwischen ihnen, und es ist möglicherweise nicht möglich, allgemein den Fluss von Datenverkehr auf Splunk-Ports zwischen Zonen zuzulassen. Das Konfigurieren und	Sie benötigen eine direkte Weiterleitungsschicht, die den Fluss von Datenverkehr zwischen Netzwerkzonen ermöglicht.	IF

		Verwalten von Firewallregeln für einzelne Quell-/Ziel-IP-Adressen wäre zu mühselig.		
6	Müssen Sie Logdaten programmgesteuert erfassen, beispielsweise durch den Aufruf von REST-APIs oder das Abfragen von Datenbanken?	Splunk stellt verschiedene modulare Eingaben zur Verfügung, die eine Ausführung von Skripts für APIs für eine große Bandbreite von Anwendungsfällen zur Datenerfassung ermöglichen, einschließlich DBX zum Erfassen von Daten aus relationalen Datenbanken.	Für Ihre Datenerfassungs-schicht ist mindestens ein Datenerfassungs-knoten (Data Collection Node, DCN) erforderlich, der mit einem komplexen Splunk-Forwarder implementiert sein muss.	DCN
7	Müssen Sie (eine Teilmenge der) Daten an andere Systeme neben – und zusätzlich zu – Splunk routen?	Einige Anwendungsfälle erfordern die zusätzliche Weiterleitung von in Splunk indizierten Daten an ein weiteres System. Oftmals bestehen die weitergeleiteten Daten nur aus einer Teilmenge der Quelldaten, oder die Daten müssen vor der Weiterleitung geändert werden.	Abhängig von den Besonderheiten des Anwendungsfalls benötigen Sie möglicherweise eine direkte Weiterleitungsschicht, die mit einem komplexen Forwarder aufgebaut ist, um Routing und Filtering ereignisbasiert zu unterstützen. Alternativ können Sie Daten nach der Indizierung mithilfe des cefout-Befehls weiterleiten, der in der Splunk App für CEF enthalten ist.	HF
8	Verfügen Sie über Remotestandorte mit eingeschränkter Netzwerkbandbreite, für die vor dem Senden über das Netzwerk in erheblichem Umfang Filtern von Daten erforderlich ist?	Das Filtern von Daten vor der Übertragung erfordert einen analysierenden (komplexen) Forwarder. Die von einem HWF verwendete Netzwerkbandbeite beträgt etwa das Fünffache der Netzwerkbandbreite für einen UF, so dass die Filterung nur dann sinnvoll ist, wenn eine erhebliche Anzahl Ereignisse ausgefiltert wird (Faustregel: > 50 % der Quelldaten). Idealerweise sollten	Wenn Sie das Logvolumen nicht an der Quelle reduzieren können, benötigen Sie einen zwischen-geschalteten HF am Remotestandort, der die Quelldaten analysiert und Ereignisse auf der Grundlage seiner Konfiguration herausfiltert.	IF HF

		Sie den Detailgrad Ihrer Protokollierung so anpassen, dass Sie die benötigte Verringerung des Logvolumens erreichen.		
9	Müssen Sie vertrauliche Daten maskieren/vernebeln, bevor sie zur Indizierung über ein öffentliches Netzwerk gesendet werden?	Manchmal ist das Schützen von Forwarder-Datenverkehr mithilfe von SSL nicht ausreichend, um vertrauliche Daten bei der Übertragung über öffentliche Netzwerke zu schützen, und einzelne Teile von Ereignissen müssen vor der Übertragung maskiert werden (SSNs, CC-Daten usw.). Im Idealfall erfolgt diese Datenmaskierung in der Anwendung, die die Logdaten produziert.	Wenn Sie keine Daten in der generierenden Anwendung maskieren können, benötigen Sie einen zwischen-geschalteten HF an Ihrem Standort, der Quelldaten analysiert und auf der Grundlage seiner Konfiguration die erforderlichen Maskierungsregeln anwendet, bevor die Daten an die Indexer gesendet werden.	IF HF
10	Müssen Sie Metriken mithilfe von statsd oder collectd erfassen?	Statsd und collectd sind weit verbreitete Technologien zur Erfassung von Metriken von Hostsystemen und Anwendungen.	Splunk unterstützt spezifische Indextypen und Erfassungs-methoden, um diese Indizes mithilfe von UF, HF oder HES zu speisen.	METRICS
11	Müssen Teile Ihrer Datenerfassungs-komponenten hochverfügbar sein?	Normalerweise zwar nicht für Endpunkte, doch für andere Datenerfassungs-komponenten kann Verfügbarkeit ein Anliegen sein, etwa für zwischengeschaltete Forwarder oder Knoten zur Datenerfassung.	Es müssen entsprechend Überlegungen dazu angestellt werden, wie sich Ausfälle auf die Verfügbarkeit der einzelnen Komponenten auswirken und wie dem entgegengewirkt werden kann.	HA

Schritt 2b: Wahl Ihrer Komponenten für die Datenerfassung

Nachdem Sie den Fragebogen ausgefüllt haben, verfügen Sie über eine Liste der erforderlichen Datenerfassungskomponenten, um den Anforderungen für Ihre Bereitstellung zu genügen. In diesem Abschnitt werden die einzelnen Komponenten der Datenerfassungsarchitektur ausführlicher erörtert. Vorher möchten wir aber noch etwas allgemeine Orientierung vermitteln.

Allgemeine Orientierung zur Weiterleitungsarchitektur

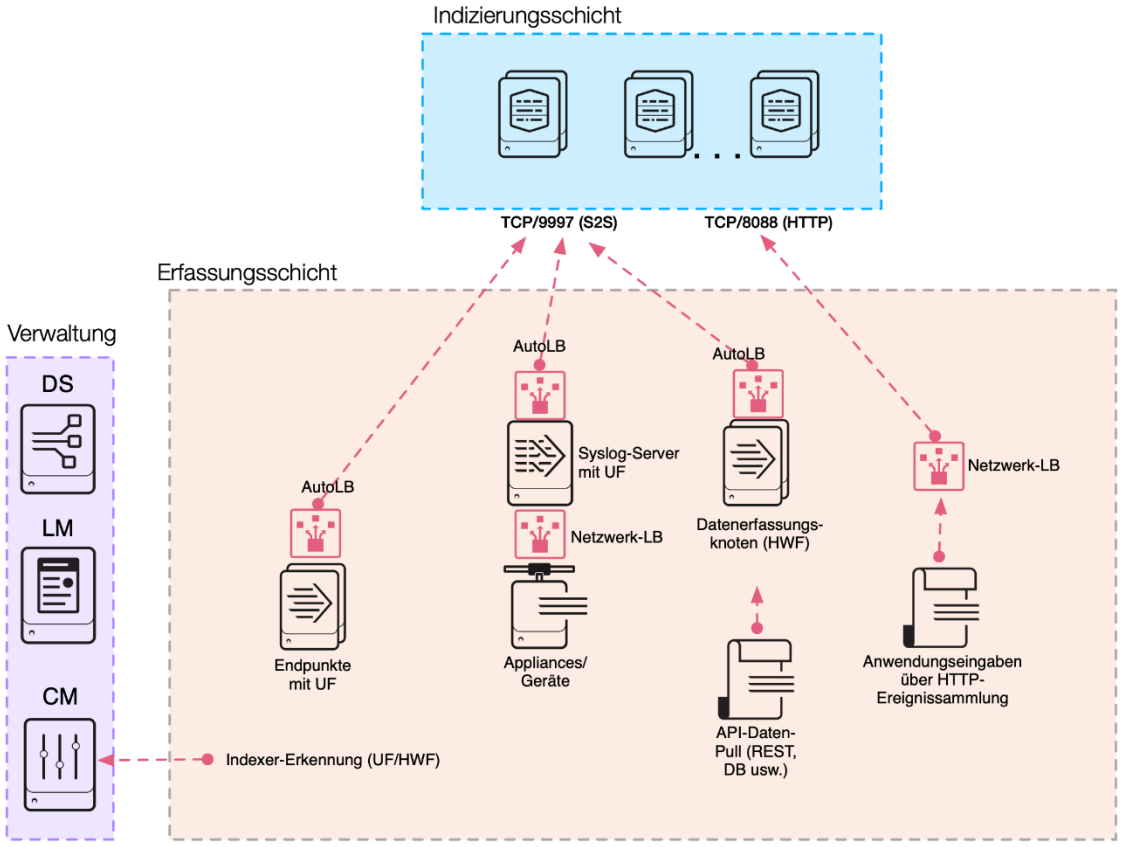
Idealerweise ist die Datenerfassungsschicht so "flach" wie möglich. Dies bedeutet, dass Datenquellen lokal von einem universellen Forwarder erfasst und direkt an die Indizierungsschicht weitergeleitet werden. Dies ist eine Best Practice, weil sie minimale Latenz bei der Datenerfassung (Zeit bis zur Suche) sicherstellt und eine ordnungsgemäße Ereignisverteilung über die verfügbaren Indexer ermöglicht. Das Befolgen dieser Best Practice führt zu leichter Verwaltung und Einfachheit im Betrieb. Wir sehen häufig, dass Kunden eine zwischengeschaltete Weiterleitungsschicht bereitstellen. Im Allgemeinen sollten Sie dies vermeiden, es sei denn, den Anforderungen kann nicht auf andere Weise entsprochen werden. Aufgrund des potenziellen Einflusses von zwischengeschalteten Forwardern enthält dieses Dokument einen separaten Abschnitt zu diesem Thema mit mehr Details.

Es gibt Endpunkte, die keine Installation des universellen Forwarders zulassen (wie etwa Netzwerkgeräte, Appliances) und mithilfe von Syslog protokollieren. Eine separate Best Practice-Architektur zum Erfassen solcher Datenquellen ist im Abschnitt mit dem Titel "Erfassung von Syslog-Daten" umrissen.

Für Datenquellen, die mit programmgesteuerten Mitteln erfasst werden müssen (APIs, Datenbankzugriff), wird das Bereitstellen eines Datenerfassungsknotens (DCN) auf der Grundlage einer vollständigen Splunk Enterprise-Installation empfohlen. Dies wird auch als komplexer Forwarder bezeichnet. Sie sollten diese Art von Eingaben in der Search Head-Schicht ausschließlich in Entwicklungsumgebungen ausführen.

Das folgende Diagramm zeigt eine allgemeine Architektur zur Datenerfassung, die dieser Orientierung Rechnung trägt.

Übersicht der Datenerfassungstopologie



Das Diagramm oben zeigt den Verteilungs-Server (Deployment Server, DS) in der Verwaltungsschicht, der zum Verwalten der Konfigurationen auf Datenerfassungskomponenten verwendet wird. Außerdem ist hier der Lizenz-Master (LM) dargestellt, da Datenerfassungsknoten Zugriff auf den LM benötigen, um Funktionen von Splunk Enterprise zu aktivieren. Der Cluster-Master (CM) kann, sofern verfügbar, von Forwardern für die Ermittlung von Indexern verwendet werden, wodurch die Notwendigkeit entfällt, die verfügbaren Indexer in der Ausgabekonfiguration der Forwarder zu verwalten.

Im Diagramm oben stellt AutoLB den integrierten automatischen Lastenausgleichs-mechanismus von Splunk dar. Dieser Mechanismus wird dafür verwendet, die ordnungsgemäße Ereignisverteilung für Daten sicherzustellen, die mithilfe des proprietären Splunk-Protokolls S2S gesendet werden (Standardport 9997). Hinweis: Die Verwendung eines externen Netzwerk-Load Balancers für S2S-Verkehr wird aktuell nicht unterstützt und nicht empfohlen.

Für den Lastenausgleich von Verkehr von Datenquellen, die mit einem Branchenstandard-protokoll (wie HTTP oder Syslog) kommunizieren, wird ein Netzwerk-Load Balancer verwendet, um gleichmäßige Auslastung und Ereignisverteilung über die Indexer in der Indizierungsschicht zu gewährleisten.

(UF) Universelle Forwarder

Der universelle Forwarder (UF) ist die beste Wahl für eine große Menge von Anforderungen an die Datenerfassung von Systemen in Ihrer Umgebung. Er stellt einen zweckspezifischen Datenerfassungsmechanismus mit sehr minimalen Ressourcenanforderungen dar. Der UF sollte die Standardwahl zum Erfassen und Weiterleiten von Logdaten sein. Der UF bietet:

- Checkpoint-/Neustartfunktion für verlustfreie Datenerfassung.
- Effizientes Protokoll, das die Nutzung der Netzwerkbandbreite minimiert.

- Möglichkeit zur Drosselung.
- Integrierter Lastenausgleich zwischen den verfügbaren Indexern.
- Optionale Netzwerkverschlüsselung mithilfe von SSL/TLS.
- Datenkomprimierung (nur ohne SSL/TLS zu verwenden).
- Mehrere Eingabemethoden (Dateien, Windows-Ereignisprotokolle, Netzwerkeingaben, skriptbasierte Eingaben).
- Eingeschränkte Funktionen zur Ereignisfilterung (nur Windows-Ereignisprotokolle).
- Unterstützung für eine parallele Erfassungspipeline zum Erhöhen des Durchsatzes/Verringern der Latenz.

Mit wenigen Ausnahmen für strukturierte Daten (JSON, CSV, TSV) zerlegt der UF Logquellen nicht in Ereignisse, so dass er keine Aktion ausführen kann, die ein Verständnis für das Format der Protokolle voraussetzt. Er wird außerdem mit einer abgespeckten Version von Python geliefert, die ihn mit allen modularen Eingabe-Apps inkompatibel macht, für deren Funktion ein vollständiger Splunk-Stack erforderlich ist.

Es ist normal, dass eine große Anzahl UFs (mehrere 100 bis mehrere 10.000) an Endpunkten und auf Servern in einer Splunk-Umgebung bereitgestellt und zentral oder mithilfe eines Verwaltungstools von Drittanbietern verwaltet wird (wie etwa Puppet oder Chef).

(HF, Heavy Forwarder) Komplexer Forwarder

Der komplexe Forwarder (Heavyweight Forwarder, HWF) ist eine vollständige Splunk Enterprise-Bereitstellung, die so konfiguriert ist, dass sie als Forwarder mit deaktivierter Indizierung agiert. Ein HWF führt im Allgemeinen keine anderen Splunk-Rollen aus. Der Hauptunterschied zwischen einem UF und einem HWF besteht darin, dass der HWF die gesamte Analysepipeline enthält und die identischen Funktionen wie ein Indexer ausführt, ohne tatsächlich Ereignisse auf Datenträger zu schreiben und zu indizieren. Dadurch kann der HWF einzelne Ereignisse verstehen und auf ihrer Grundlage agieren, um beispielsweise Daten zu maskieren oder Filtern und Routen auf der Grundlage von Ereignisdaten auszuführen. Da es sich um eine vollständige Splunk Enterprise-Installation handelt, kann er modulare Eingaben hosten, für deren Funktion ein vollständiger Python-Stack erforderlich ist, um Datenerfassung auszuführen oder als Endpunkt für die Splunk HTTP-Ereignissammmlung (HES) zu dienen. Der HWF führt die folgenden Funktionen aus:

- Zerlegen von Daten in Ereignisse.
- Filtern und Routen auf der Grundlage einzelner Ereignisdaten.
- Größerer Ressourcenfußabdruck als der UF.
- Größerer Netzwerkbandbreiten-Fußabdruck als der UF (~5x).
- GUI zur Verwaltung.

In Allgemeinen werden HWFs nicht auf Endpunkten zur Zweck der Datenerfassung installiert. Stattdessen werden sie auf eigenständigen Systemen verwendet, um Datenerfassungsknoten oder zwischengeschaltete Weiterleitungsschichten zu implementieren. **Verwenden Sie nur dann einen HWF, wenn die Anforderungen zum Erfassen von Daten von anderen Systemen mit einem UF nicht erfüllt werden können.**

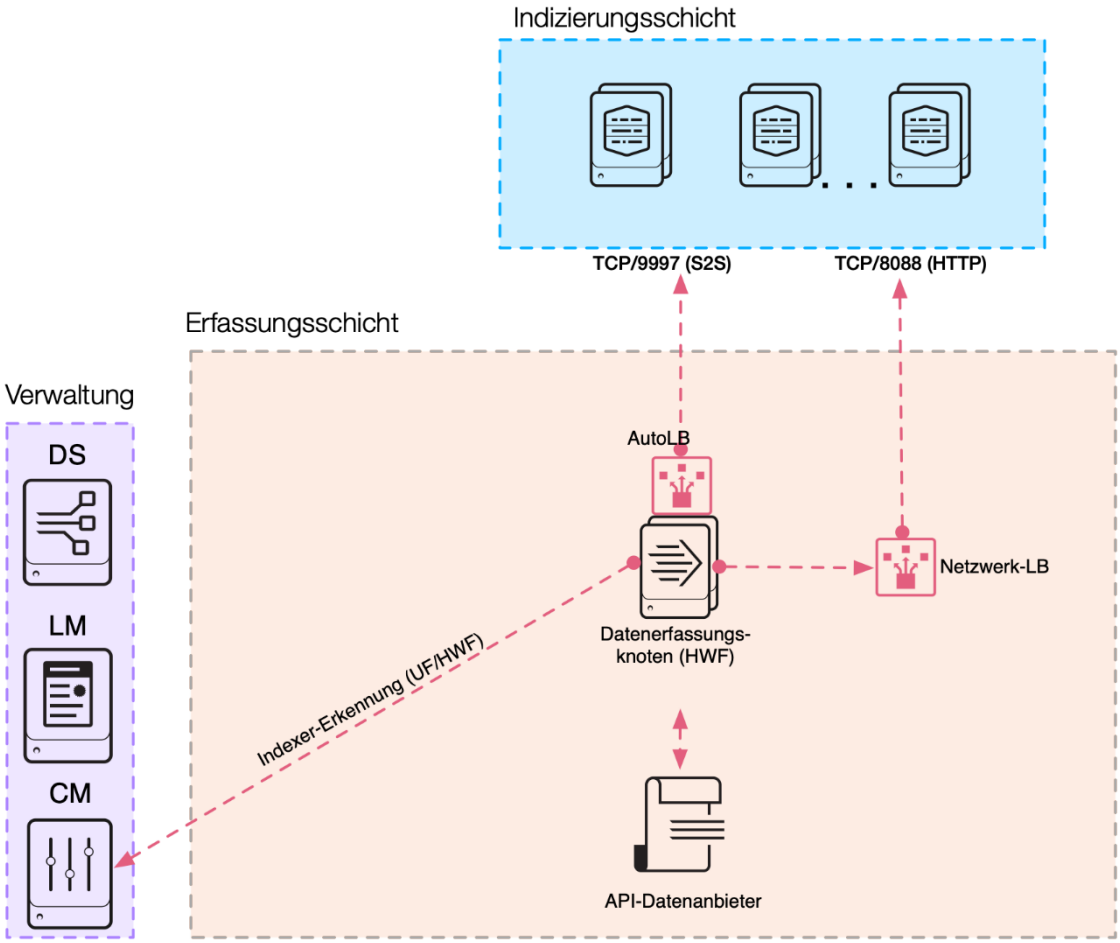
Hier ein paar Beispiele für solche Anforderungen:

- Lesen von Daten von RDBMS zum Zweck der Erfassung in Splunk (Datenbankeingaben).
- Erfassen von Daten von Systemen, die über eine API erreichbar sind (Cloud-Services, VMware-Monitoring, proprietäre Systeme usw.).
- Bereitstellen einer dedizierten Schicht zum Hosten des HTTP-Ereignissammlungsdiensts.
- Implementieren einer zwischengeschalteten Weiterleitungsschicht, die einen analysierenden Forwarder zum Routen/Filtern/Maskieren erfordert.

(DCN) Komplexer Forwarder als Datenerfassungsknoten

Einige Datenquellen erfordern die Erfassung mithilfe einer API. Zu diesen APIs können REST, Webdienste, JMS und/oder JDBC als Abfragemechanismus gehören. Splunk sowie die Entwickler von Drittanbietern bieten eine große Bandbreite von Anwendungen, die diese API-Interaktionen ermöglichen. Meistens werden diese Anwendungen mithilfe des Splunk-Frameworks zur modularen Eingabe implementiert, für deren ordnungsgemäße Funktion eine vollständige Installation der Splunk Enterprise-Software erforderlich ist. Die Best Practice zur Realisierung dieses Anwendungsfalls besteht in der Bereitstellung eines oder mehrerer Server(s), die als komplexe Forwarder fungieren und als Datenerfassungsknoten (Data Collection Node, DCN) konfiguriert sind.

Datenerfassungsknoten – Topologie

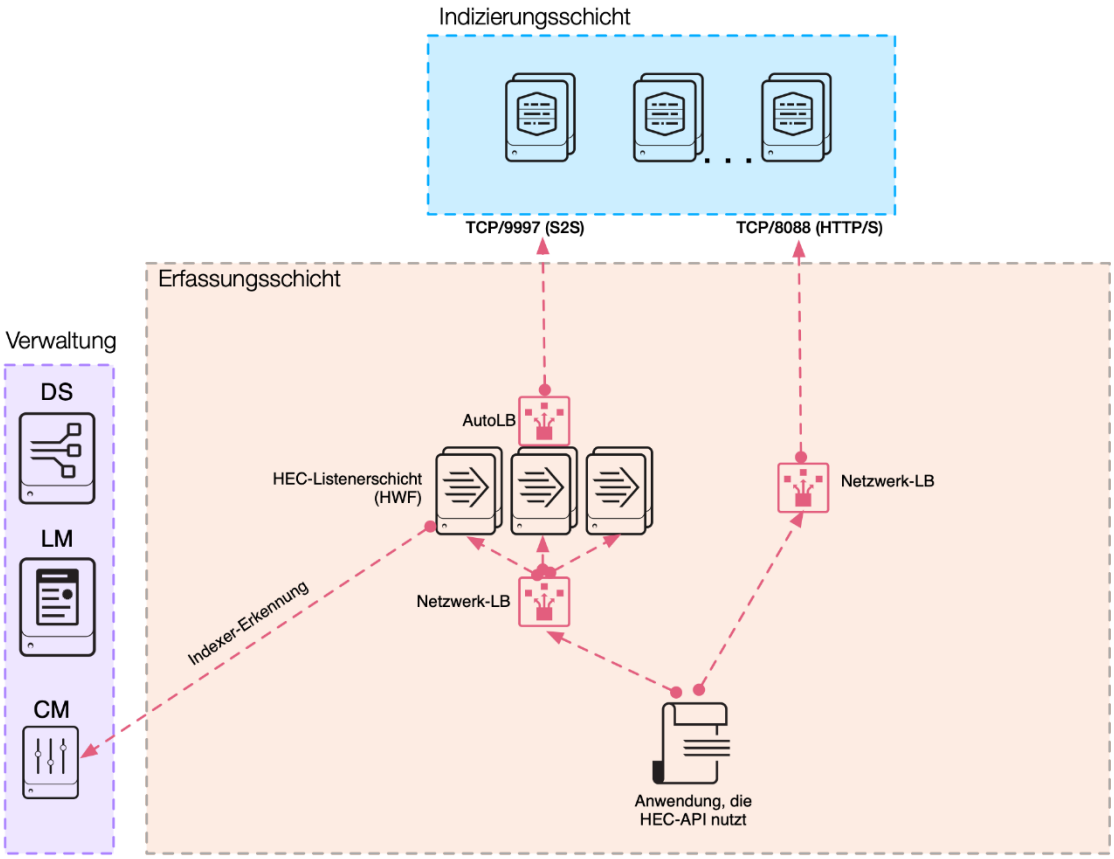


(HES) HTTP-Ereignissammlung

Die HES stellt serverseitig einen Listener-Service zur Verfügung, der HTTP/S-Verbindungen akzeptiert, und clientseitig eine API aufweist, was es Anwendungen ermöglicht, Nutzlasten aus Logdaten direkt in der Indexerschicht oder in einer dedizierten HES-Empfängerschicht zu posten, die aus einem oder mehreren komplexen Forwardern besteht. HES stellt zwei Endpunkte bereit, die das Senden von Daten wahlweise im Rohformat oder im JSON-Format unterstützen. Die Nutzung von JSON kann die Aufnahme von zusätzlichen Metadaten in die Ereignisnutzlast ermöglichen, mit denen sich beim späteren Durchsuchen der Daten größere Flexibilität erzielen lässt.

Das folgende Diagramm veranschaulicht die zwei Bereitstellungsoptionen für HES:

HES-Topologieoptionen



Die Verwaltungsschicht enthält den Lizenz-Master (für HF erforderlich) sowie den Verteilungs-Server zum Verwalten der HTTP-Eingaben an den lauschenden Komponenten. Hinweis: Wenn die Indizierungsschicht einen Cluster verwendet und direkt HES-Datenverkehr empfängt, wird die HES-Konfiguration mithilfe des Cluster-Masters anstelle des Verteilungs-Servers verwaltet.

Ihr Entscheidung für die verwendete Bereitstellungstopologie hängt stark von Ihren spezifischen Anforderungen ab. Durch eine dedizierte HES-Listenerschicht wird eine weitere Architekturkomponente in Ihre Bereitstellung eingeführt. Positiv ist zu vermerken, dass die Schicht unabhängig skaliert werden kann und aus Verwaltungssicht ein gewisses Maß an Isolation gegenüber der Indizierungsschicht bereitstellt. Da die dedizierte HES-Schicht einen HF erfordert, analysiert sie außerdem den gesamten eingehenden Datenverkehr und entlastet so die Indexer von dieser Workload.

Andererseits erhöht ein direktes Hosten des HES-Listeners auf den Indexern die Wahrscheinlichkeit einer guten Ereignisverteilung, da HTTP ein von allen Netzwerk-Load Balancern gut beherrschtes Protokoll ist und die entsprechende Lastenausgleichs-Richtlinie sicherstellen kann, dass die am wenigsten ausgelasteten Indexer zuerst bedient werden.

Dem Grundsatz folgend, dass Sie die einfachste der möglichen Architekturen bereitstellen sollten, die Ihren Anforderungen entspricht, empfehlen wir Ihnen, das direkte Hosten Ihres HES-Listeners auf den Indexern in Erwägung zu ziehen, vorausgesetzt, Sie verfügen über ausreichende Systemkapazität. Diese Entscheidung kann später ggf. leicht revidiert werden, einfach durch Bereitstellen einer passend dimensionierten und konfigurierten HF-Schicht und das Ändern der LB-Konfiguration in der Form, dass sie die IP-Adressen der HF-Schicht anstelle derer der Indexer verwendet. Diese Änderung sollte für Clientanwendungen transparent sein.

Hinweis: Wenn Sie für die über HES gesendeten Daten Indexer-Bestätigung benötigen, empfiehlt sich eine dedizierte HES-Listenerschicht, um das Auftreten von Nachrichtenduplikaten durch rollierende Neustarts von Indexern zu minimieren.

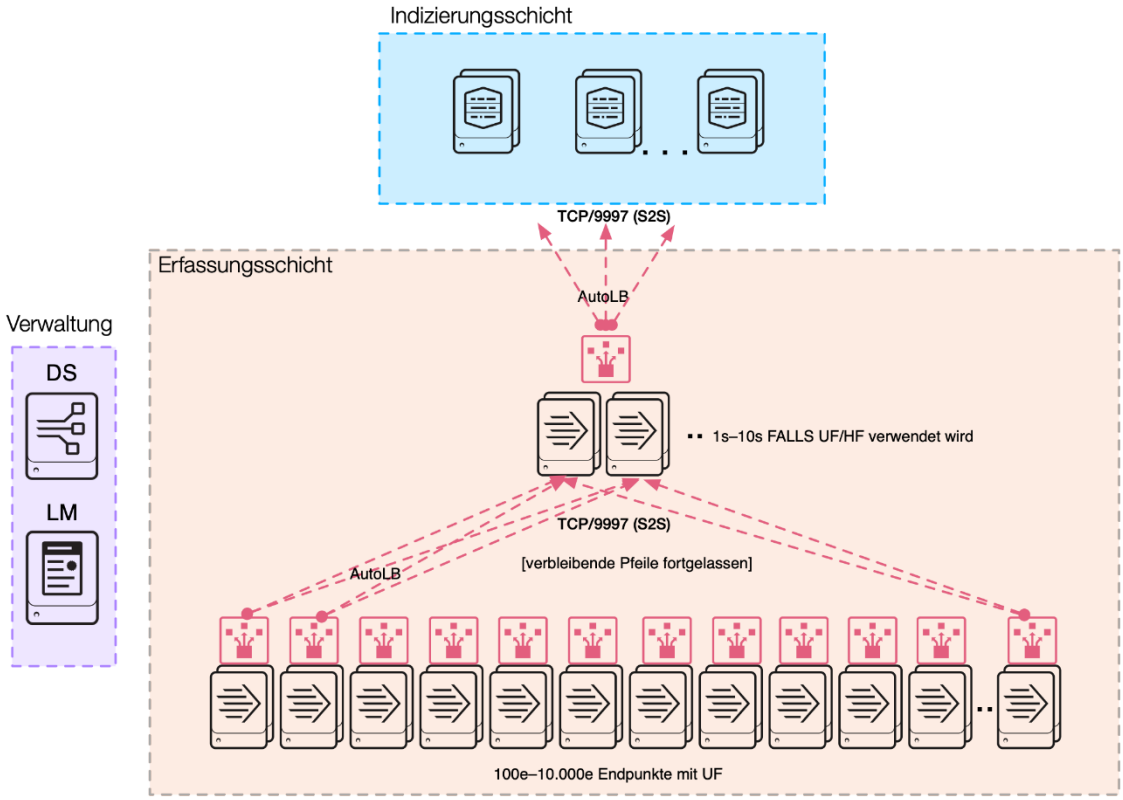
Hinweis: Diese HES-Bereitstellungsarchitektur stellt den Transport für einige der anderen später erörterten Datenerfassungskomponenten zur Verfügung, insbesondere die Syslog- und Metrikdatenerfassung.

(IF, Intermediary Forwarding Tier) Zwischengeschaltete Weiterleitungsschicht

In manchen Situationen sind zwischengeschaltete Forwarder für die Weiterleitung von Daten erforderlich. Zwischengeschaltete Forwarder empfangen Log-Streams von Endpunkten und leiten sie an eine Indexerschicht weiter. Mit zwischengeschalteten Forwardern stellen sich architektonische Herausforderungen, die einen sorgfältigen Entwurf erfordern, um negative Einflüsse auf die Splunk-Gesamtumgebung zu vermeiden. Die wichtigste Rolle spielen zwischengeschaltete Forwarder beim Konzentrieren von Verbindungen von mehreren 100 bis mehreren 10.000 Endpunktforwardern und der Weiterleitung an Indexer mithilfe einer sehr viel kleineren Anzahl Verbindungen. Dies kann sich erheblich auf die Datenverteilung in der Indizierungsschicht auswirken, da nur eine Teilmenge der Indexer zu jedem gegebenen Zeitpunkt Datenverkehr empfängt. Allerdings lassen sich diese negativen Nebenwirkungen durch ordnungsgemäße Dimensionierung und Konfiguration abmildern.

Das folgende Diagramm veranschaulicht diese Herausforderung gut:

Topologie mit zwischengeschalteten Forwardern



In einem Szenario mit einem einzelnen zwischengeschalteten Forwarder stellen alle Endpunkte Verbindungen (potenziell Tausende) mit diesem einzelnen Forwarder her, und der zwischengeschaltete Forwarder stellt zu jedem Zeitpunkt jeweils nur eine Verbindung mit einem Indexer her. Dies ist kein optimales Szenario, da die folgenden Konsequenzen mit hoher Wahrscheinlichkeit eintreten:

- Ein großer Datenstream von vielen Endpunkten wird durch eine einzelne Leitung gequetscht und erschöpft dadurch Ihre System- und Netzwerkressourcen.
- Eingeschränkte Failoverziele für die Endpunkte im Fall eines IF-Ausfalls (Ihr Ausfallrisiko ist umgekehrt proportional zur Anzahl der IFs).

- Zu jedem Zeitpunkt wird jeweils nur eine kleine Anzahl Indexer bedient. Suchen über kurze Zeiträume profitieren nicht so stark von Parallelisierung, wie es sonst möglich wäre.

Zwischengeschaltete Forwarder fügen Ihrer Bereitstellung darüber hinaus eine weitere Architekturschicht hinzu, was Verwaltung und Problembehandlung komplizierter gestalten und zu zusätzlicher Latenz in Ihrem Datenerfassungspfad führen kann. Versuchen Sie, den Einsatz zwischengeschalteter Weiterleitungsschichten möglichst zu vermeiden, es sei denn, sie stellen die einzige Option zum Erfüllen Ihrer Anforderungen dar. In diesen Fällen können Sie den Einsatz einer zwischengeschalteten Schicht in Erwägung ziehen:

- Sensible Daten müssen vor dem Senden über das Netzwerk an Indexer vernebelt/entfernt werden. Beispielsweise, wenn Sie ein öffentliches Netzwerk verwenden müssen.
- Strenge Sicherheitsrichtlinien lassen keine direkten Verbindungen zwischen Endpunkten und Indexern zu, etwa in Mehrzonen-Netzwerken oder bei Cloud-basierten Indexern.
- Eingeschränkte Bandbreite zwischen Endpunkten und Indexern macht die Filterung einer erheblichen Teilmenge der Ereignisse erforderlich.
- Das ereignisbasierte Routing an dynamische Ziele ist eine der Anforderungen.

Wägen Sie die Dimensionierungs- und Konfigurationsanforderungen für jede zwischengeschaltete Weiterleitungsschicht sorgfältig ab, um die Verfügbarkeit der Schicht zu gewährleisten, ausreichende Verarbeitungskapazität zum Verarbeiten des gesamten Datenverkehrs bereitzustellen und gute Verteilung von Ereignissen auf die Indexer zu unterstützen. Für die IF-Schicht gelten die folgenden Anforderungen:

- Ausreichende Gesamtzahl von Pipelines zur Datenverarbeitung.
- Redundante IF-Infrastruktur.
- Ordnungsgemäß optimierte Konfiguration des Splunk-Lastenausgleichs. Beispielsweise autoLBVolume, EVENT_BREAKER, EVENT_BREAKER_ENABLE, möglicherweise forceTimeBasedAutoLB bei Bedarf.

Die allgemeine Richtlinie schlägt doppelt so viele IF-Verarbeitungspipelines wie Indexer in der Indizierungsschicht vor.

Hinweis: Eine Verarbeitungspipeline kann nicht mit einem physischen IF-Server gleichgesetzt werden. Unter der Voraussetzung, dass ausreichende Systemressourcen, beispielsweise CPU-Kerne, Arbeitsspeicher und NIC-Bandbreite verfügbar sind, können auf einem einzelnen IF mehrere Verarbeitungspipelines konfiguriert werden.

Wenn Sie eine IF-Schicht benötigen (siehe dazu den Fragebogen), verwenden Sie standardmäßig UF für die Schicht, da diese bei kleinerem Ressourcen-Fußabdruck höheren Durchsatz für System und Netzwerk zur Verfügung stellen. Verwenden Sie HF, wenn die UF-Möglichkeiten Ihren Anforderungen nicht entsprechen.

(SYSLOG) Syslog-Datenerfassung

Das Syslog-Protokoll stellt eine nahezu allgegenwärtige Quelle für Logdaten im Unternehmen dar. Die meisten skalierbaren und verlässlichen Datenerfassungsschichten beinhalten eine Syslog-Erfassungskomponente. Es gibt viele Möglichkeiten für die Erfassung von Syslog-Daten in Splunk. Ziehen Sie die folgenden Methoden in Betracht:

- **Universeller Forwarder (UF)/Komplexer Forwarder (HF)**: Verwenden Sie einen Splunk UF oder HF, um die von einem Syslog-Server ausgegebenen Dateien (z. B. `rsyslog` oder `syslog-ng`) zu überwachen (erfassen).
- **Syslog-Agent zu HES**: Verwenden Sie einen Syslog-Agent mit der Fähigkeit zur Ausgabe an die Splunk-HES. (Es sind Module von Drittanbietern für rsyslog und syslog-ng erhältlich, die die Ausgabe an HES beherrschen). .
- **Direkte TCP/UDP-Eingabe**: Splunk besitzt die Fähigkeit, an einem TCP- oder UDP-Port zu lauschen (der Standardport ist UDP 514) und Quellen hier zu erfassen (**nicht** für den produktiven Einsatz empfohlen).

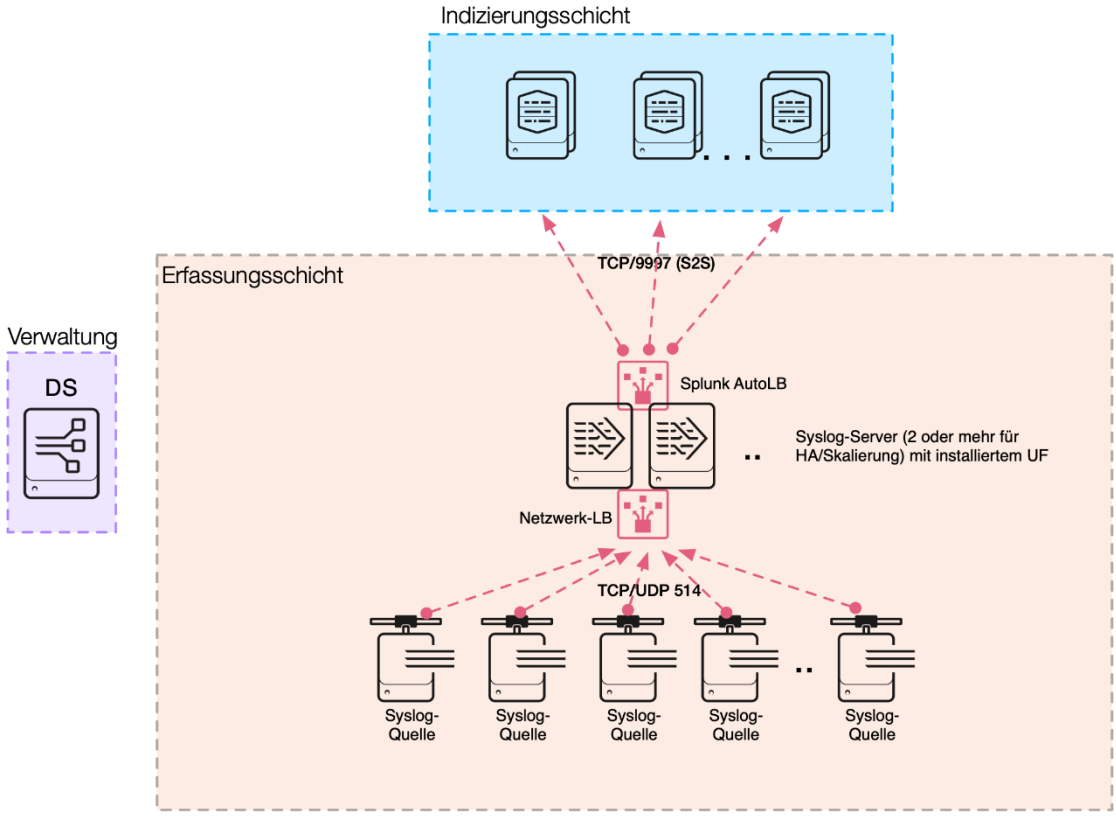
Syslog (Dateiüberwachung in Verbindung mit einem SCD)

Splunk kann mithilfe von `inputs.conf` Überwachung auf einem UF/HF verwenden, um mit einem Syslog-Erfassungs-Daemon (Syslog Collection Daemon, SCD) Syslog-Quellen zu verarbeiten und zu erfassen, die von einem Endpunkt auf einen Datenträger geschrieben werden. Am häufigsten anzutreffen sind `rsyslog`, `syslog-ng` und Fastvue, für die sowohl gewerbliche als auch kostenlose Lösungen verfügbar sind, die zugleich skalierbar sind und sich einfach in Umgebungen mit geringen Volumina sowie auch in verteilte Umgebungen im großen Maßstab integrieren und verwalten lassen.

Weitere Informationen über das Konfigurieren von Monitoren finden Sie unter Monitor files and directories (Überwachen von Dateien und Verzeichnissen) in *Getting Data In.*

Diese Architektur unterstützt die ordnungsgemäße Erfassung von Daten in der gleichen Weise wie ein universeller Forwarder auf beliebigen anderen Endpunkten. Sie können die SCD für die Erkennung mehrerer verschiedener Protokolltypen und zur Ausgabe von Protokollereignissen in geeigneten Dateien und Verzeichnissen konfigurieren, in denen sie von einem Splunk-Forwarder aufgenommen werden können. Dadurch wird erhält der Syslog-Protokollstream außerdem ein gewisses Maß an Robustheit, da Ereignisse auf einen Datenträger geschrieben werden, was die Anfälligkeit für Datenverlust bei Nachrichten, die über den unzuverlässigen UDP als Transport gesendet werden, einschränken kann.

Syslog-Datenerfassungstopologie mithilfe von UF



Das Diagramm zeigt Syslog-Quellen, die Daten mithilfe von TCP oder UDP an Port 514 an einen Pool von Syslog-Servern mit Lastenausgleich senden. Mehrere Server stellen Hochverfügbarkeit für die Erfassungsschicht sicher und können Datenverlust während Wartungsvorgängen verhindern. Jeder Syslog-Server ist dafür konfiguriert, Regeln auf den Syslog-Stream anzuwenden, die bewirken, dass Syslog-Ereignisse für jeden Sourcetyp (Firewallereignisse, Betriebssystem-Syslog, Netzwerkswitches, IPS, usw.) in dedizierte Dateien/Verzeichnisse geschrieben werden. Der UF, der für jeden Server bereitgestellt ist, überwacht diese Dateien und leitet die Daten zur Verarbeitung im entsprechenden Index an die Indizierungsschicht weiter. Splunk AutoLB wird verwendet, um die Daten gleichmäßig über die verfügbaren Indexer zu verteilen.

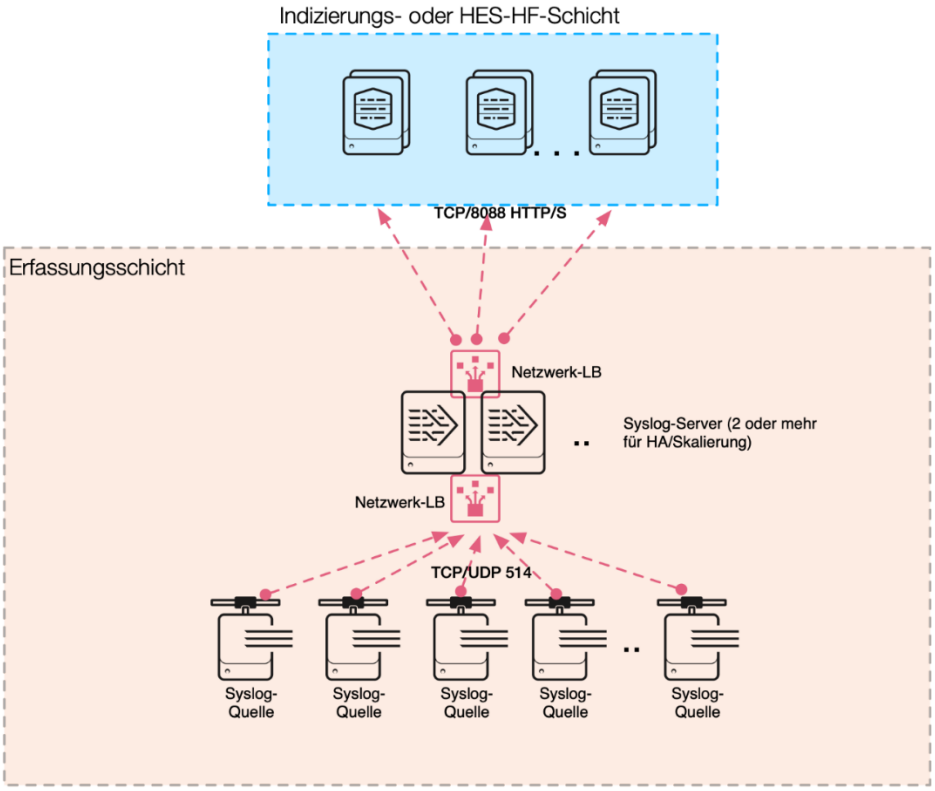
Der in der Verwaltungsschicht dargestellte Verteilungs-Server kann für die zentrale Verwaltung der UF-Konfiguration verwendet werden.

Syslog-Agent zu HES

Einhergehend mit dem verstärkten Einsatz der HES gibt es eine wachsende Zahl von Bereitstellungen, die ihre Bereitstellung der HES für die Erfassung von Syslog verwenden. Weitere Informationen finden Sie im Splunk Blogs-BeitragSyslog-ng and HEC: Scalable Aggregated Data Collection in Splunk (Syslog-ng und HES: skalierbare aggregierte Datenerfassung in Splunk).

Das Diagramm unten zeigt Syslog-Quellen, die Daten an Port 514 mithilfe eines Netzwerk-Load Balancers an eine Syslog-Serverfarm senden. Geeignete Syslog-Richtlinien mit einem benutzerdefinierten Syslog-Ziel und ein Python-Skript, das die HES-API nutzt, werden angewendet, und die Ereignisse werden an einen HES-Listener gesendet, ebenfalls mit einem Netzwerkverkehr-Load Balancer für die Indizierung:

Syslog-Datenerfassungstopologie mithilfe von HES



Ein Vorteil dieser Topologie besteht darin, dass sie das Erfordernis zum Bereitstellen und Konfigurieren von UF/HF beseitigt. Der HTTP-Load Balancer bedient die HES-Listener auf den Indexern (oder einer dedizierten HES-Listenerschicht), um sicherzustellen, dass die Daten gleichmäßig über die HES-Endpunkte verteilt werden. Konfigurieren Sie diesen Load Balancer mit der Richtlinie "Least Connections".

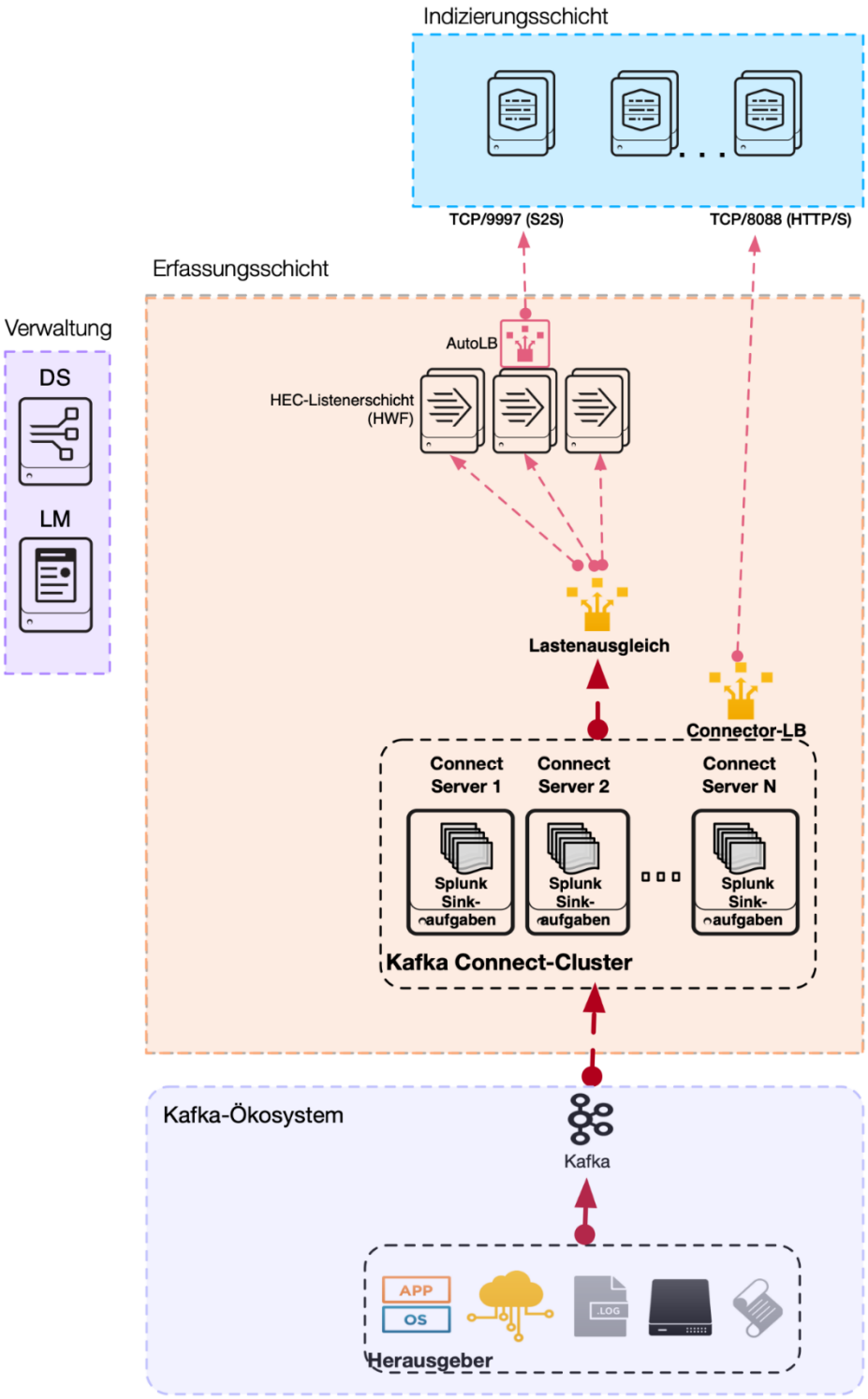
Splunk-UDP-Eingabe

Splunk kann eine direkte UDP-Eingabe auf einem UF oder HF nutzen, um Daten von Syslog zu empfangen. Informationen zum Konfigurieren von TCP- und UDP-Ports finden Sie unter Get data from TCP and UDP ports (Abrufen von Daten von TCP- und UDP-Ports) in *Getting Data In*. Die Möglichkeit, Ereignisse an UDP 514 zu empfangen, baut auf der Fähigkeit des UFs/HFs auf, als Stammdienst ausgeführt zu werden. Darüber hinaus muss der Agent 100 % der Zeit verfügbar sein, um möglichen Datenverlust zu verhindern. Bei Forwardern können häufige Neustarts zur Anwendung von Konfigurationsänderungen vorkommen, was nahezu eine Garantie für Datenverlust darstellt. Aus diesen Gründen **wird dies nicht als Best Practice für eine Produktionsbereitstellung angesehen**.

(KAFKA) Nutzung von Logdaten aus Kafka-Topics

Splunk bietet einen unterstützten Sink-Connector für das Nutzen von Daten aus Kafka-Themen mit dem Namen "Splunk Connect for Kafka". Eine detaillierte Produktdokumentation finden Sie unter Apache Kafka Connect im Splunk Connect for Kafka-Handbuch. Das Splunk Connect for Kafka-Paket wird in einem ordnungsgemäß dimensionierten Kafka Connect-Cluster (außerhalb von Splunk) installiert, wo es Topics gemäß seiner Konfiguration abonnieren und konsumierte Ereignisse mithilfe der HES zur Indizierung senden kann:

Datenerfassungstopologie mithilfe von Kafka und HES

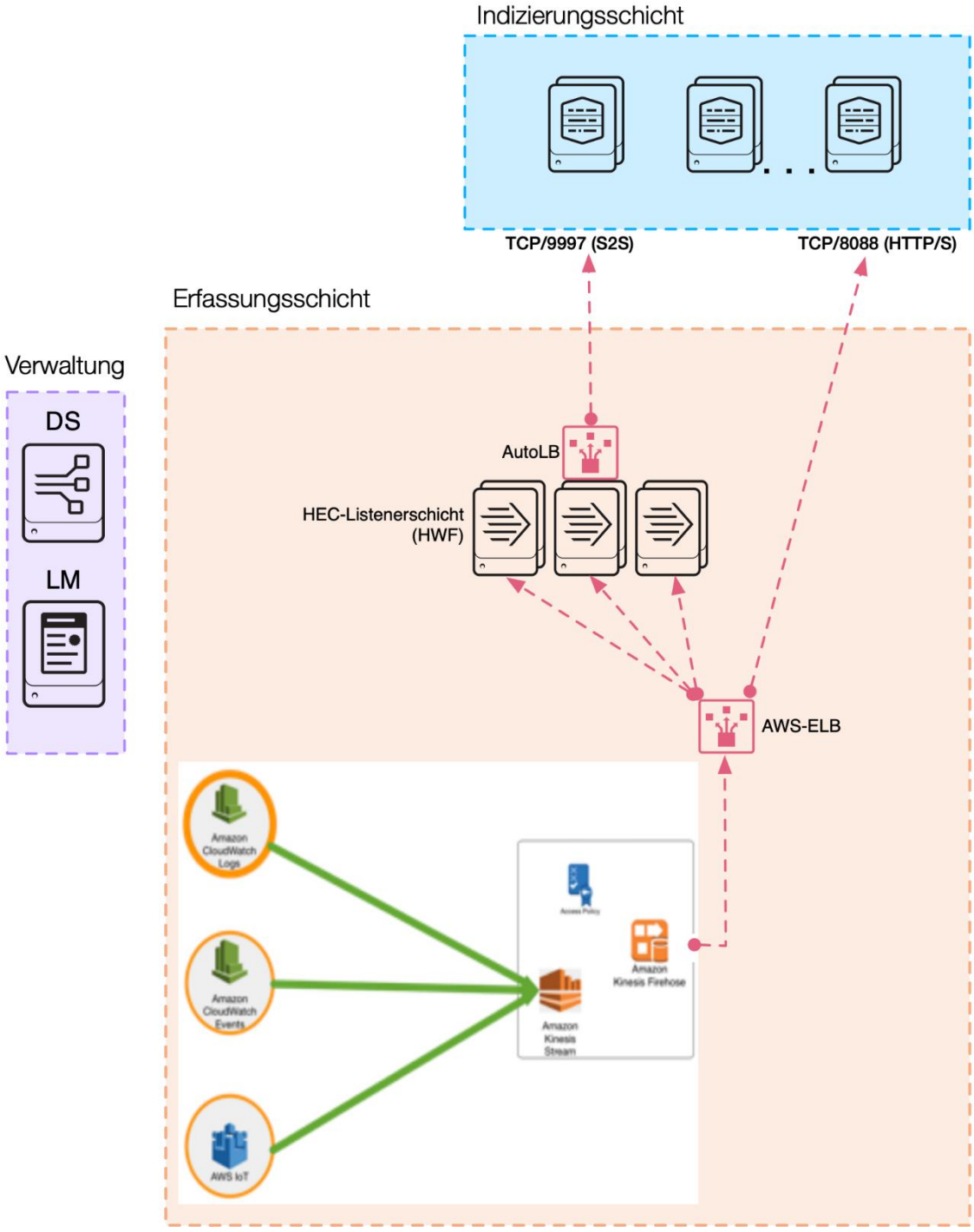


Das Diagramm zeigt Kafka-Herausgeber, die Nachrichten an den Kafka-Bus senden. Die im Kafka Connect-Cluster gehosteten Aufgaben verbrauchen diese Nachrichten über Splunk Connect for Kafka und senden die Daten mithilfe eines Netzwerk-Load Balancers an den HES-Listenerdienst. Wiederum kann der HES-Listenerdienst entweder direkt auf den Indexern oder in einer dedizierten HES-Listenerschicht gehostet sein. Bitte entnehmen Sie Details dem HES-Abschnitt. Komponenten der Verwaltungsschicht sind nur erforderlich, wenn eine dedizierte HF-Schicht bereitgestellt wird, um die HES-Listener zu hosten.

(KINESIS) Nutzung von Logdaten von Amazon Kinesis Firehose

Splunk und Amazon haben eine Integration zwischen Kinesis und der Splunk HES implementiert, die Ihnen das Streamen von Daten von AWS direkt zu einem HES-Endpunkt ermöglicht, über Ihre AWS-Konsole konfigurierbar. Diese wird durch das Splunk Add-On for Kinesis Firehose ergänzt, das CIM-konforme Kenntnis verschiedener aus AWS stammender Datenquellen zur Verfügung stellt.

Datenerfassungstopologie mithilfe von Amazon Kinesis



Das Diagramm zeigt AWS-Protokollquellen, die mithilfe eines Kinesis-Streams an die Firehose gesendet werden, die – bei ordnungsgemäßer Konfiguration – die Daten über einen AWS-ELB an den HES-Listenerdienst sendet. Wiederum kann der HES-Listenerdienst entweder direkt auf den Indexern oder in einer dedizierten HES-Listenerschicht gehostet sein. Bitte entnehmen Sie Details dem HES-Abschnitt.

Dia dargestellten Komponenten der Verwaltungsschicht sind nur erforderlich, wenn eine dedizierte HF-Schicht bereitgestellt wird, um die HES-Listener zu hosten.

(METRICS) Metrikerfassung

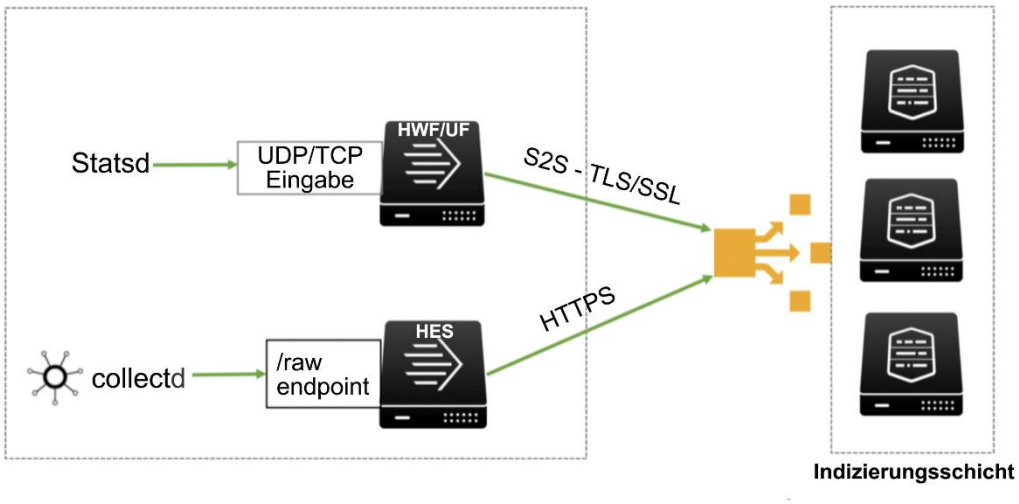
Splunk besitzt die Fähigkeit, Daten zur System- und Anwendungsleistung, oder Metrikdaten, aus einer großen Bandbreite an Drittanbieter-Software zu empfangen und zu erfassen. Für Metriken wird auf der Splunk-Plattform ein benutzerdefinierter Indextyp verwendet, der für die Speicherung und den Abruf von Metrikdaten optimiert ist.

Es gibt verschiedene Verfahren zum Konsumieren von Metrikdaten, und die Erfassungsmethode hängt von der verwendeten Technologie ab. Die gebräuchlichste Form der Metrikerfassung stellen Software-Daemons dar, wie etwa **collectd**, **statsd**, oder die Verwendung einer benutzerdefinierten Metrikdatendatei und einer gültigen Konfiguration für die Datenquelle.

Es gibt in der Hauptsache zwei Methoden, um Metriken in Splunk zu erfassen, wenn Agents wie **statsd** und **collectd** verwendet werden. Entweder mithilfe einer ***Direkten TCP/UDP***-Eingabe oder über die **HES**.

Die Verwendung von **HES** wird aufgrund der Robustheit und Skalierbarkeit des **HES**-Endpunkts und der Möglichkeit zur einfachen Skalierung der Erfassungsschicht als Best Practice angesehen.

Metrik-Datenerfassungstopologie



Statsd unterstützt aktuell **UDP**- und **TCP**-Transport, die als direkte Eingabe auf einem Splunk-Forwarder oder -Indexer verwendet werden können. Es ist jedoch keine Best Practice, TCP/UDP-Datenverkehr direkt an Forwarder in Produktionsumgebungen zu senden, da die Architektur keine Resilienz bietet und für den Verlust von Ereignissen anfällig ist (siehe Syslog-Erfassung), der durch die erforderlichen Neustarts der Splunk-Forwarder verursacht wird.

(HA) Überlegungen zu Hochverfügbarkeit für Komponenten der Weiterleitungsschicht

Es gibt ein verbreitetes Konzept von Hochverfügbarkeit (High Availability, HA) in der digitalen Welt. Jedoch kann sich die Bedeutung abhängig von der Organisation unterscheiden und eher einen Schwerpunkt bei Disaster Recovery (DR) als bei tatsächlich hoher Verfügbarkeit haben. Diese beiden Konzepte sind zwar ähnlich, haben aber eine verschiedene Bedeutung. HA ist ein Merkmal eines Systems, das darauf abzielt, ein vereinbartes Niveau von Betriebsleistung, normalerweise verfügbare Betriebszeit, über einen längeren als normalen Zeitraum zu gewährleisten. DR beinhaltet einen Satz von Richtlinien, Tools und Verfahrensweisen, um die Wiederherstellung lebenswichtiger technischer Infrastruktur und Systeme im Anschluss an einen Notfall zu ermöglichen.

Die folgenden Abschnitte umreißen verschiedene Formen von HA auf der zwischengeschalteten Schicht bzw. der Aggregationsschicht:

Zwischengeschaltete Schicht

- Für Kunden mit Bereitstellungen, die eine zwischengeschaltete Schicht bzw. Aggregationsschicht beinhalten, ist die HA der Forwarder unternehmenskritisch. In der Anwendungsschicht verfügt Splunk derzeit nicht über eine native Unterstützungsmethode für HA. Es gibt andere Strategien zum Bereitstellen von HA auf Betriebssystemebene, die nicht nativ für Splunk sind. Zu den gängigen Lösungen gehören VMware VMotion, AWS Autoscaling Groups und Linux-Cluster. Beraten Sie sich mit Ihrem Splunk-Architekten, um andere Entwurfsoptionen zu erörtern, die sich für Sie eignen.
- In Umgebungen mit einem HA-Erfordernis für eine dedizierte HES-Schicht besteht die Best Practice im Einsatz eines Netzwerkverkehr-Load Balancers (NTLB), wie etwa NGINX, vor mehreren komplexen Splunk-Forwardern. Dies bietet den Vorteil von maximalem Durchsatz, Skalierbarkeit und Verfügbarkeit. Sie verfügen über einen dedizierten Pool von HTTP-Ereignissammlungs-Instanzen, deren einziger Zweck im Empfangen und Weiterleiten von Daten besteht. Sie können weitere HES-Instanzen hinzufügen, ohne deshalb auch zwangsläufig weitere Indexer hinzufügen zu müssen. Wenn Ihre Indexer sich als Engpass erweisen, fügen Sie weitere Indexer hinzu.
- Für Umgebungen mit einem HA-Erfordernis für die Syslog-Erfassung besteht die Best Practice im Einsatz mehrerer Syslog-Server, die von einer (virtuellen) Cluster-IP-Adresse bedient werden, die von einer Lastenausgleichslösung gehostet wird, wie HAProxy oder F5, um das Maximum an Durchsatz, Skalierbarkeit und Verfügbarkeit zur Verfügung zu stellen. Sie verfügen über einen dedizierten Pool von Splunk-Instanzen, deren einziger Zweck im Empfangen und Weiterleiten von Daten besteht. Sie können weitere Instanzen hinzufügen, ohne deshalb auch zwangsläufig weitere Indexer hinzufügen zu müssen. Wenn Ihre Indexer sich als Engpass erweisen, fügen Sie weitere Indexer hinzu.

Weiterleitungsschicht

- In der Weiterleitungsschicht (Endpunkt) hängt die HA für den Agent selbst vom zugrundeliegenden Betriebssystem ab. Als absolutes Minimum sollten Sie sicherstellen, dass alle Dienste, die Weiterleitungsfunktionen implementieren, beim Neustart des Wirtsbetriebssystems automatisch neu gestartet werden. Darüber hinaus würden Best Practices für die Forwarder die Konfiguration und ordnungsgemäße Verwendung von AutoLB von den Forwardern zu mehreren Indexern beinhalten. Dies schließt auch den Einsatz von Indexer-Bestätigung ein, um die Ankunft der Daten bei der Indizierungsschicht sicherzustellen.

Schritt 3: Anwenden von Entwurfsprinzipien und Best Practices

Unten finden Sie Entwurfsprinzipien und Best Practices, getrennt nach Bereitstellungsschicht.

Bereitstellungsschichten

SVA-Entwurfsprinzipien gelten für alle der folgenden Bereitstellungsschichten:

Schicht	Definition
Suche	• Search Heads
Indizierung	• Indexer
Erfassung	• Forwarder • Modulare Eingabe • Netzwerk • HES (HTTP-Ereignissammlung) • usw.

Verwaltung/Hilfsprogramm	• CM • DS • LM • DMS • SHC-D

Ausrichten Ihrer Topologie an Best Practices

Sie müssen Ihre Anforderungen und Ihre Topologie im Blick behalten, um die geeigneten Entwurfsprinzipien und Best Practices für Ihre Bereitstellung auszuwählen. Daher sollten Sie Best Practices erst in Erwägung ziehen, nachdem Sie oben die Schritte 1 und 2 des Auswahlprozesses für Splunk Validated Architectures abgeschlossen haben.

Best Practices: Schichtspezifische Empfehlungen

Unten finden Sie Entwurfsprinzipien und Empfehlungen zu Best Practices für jede Bereitstellungsschicht. Jedes Entwurfsprinzip stärkt einen oder mehrere der SVA-Grundpfeiler: Verfügbarkeit, Performance, Skalierbarkeit, Sicherheit und Verwaltbarkeit.

Empfehlungen für die Suchschicht

ENTWURFS-PRINZIPIEN/ BEST PRACTICES (Ihre Anforderungen legen fest, welche Verfahren für Sie gültig sind)		**SVA-GRUNDPFEILER**				
		VERFÜGBARKEIT	**PERFORMANCE**	**SKALIERBARKEIT**	**SICHERHEIT**	**VERWALTBARKEIT**
1	Halten Sie die Suchschicht nahe (in Netzwerkbegriffen) an der Indizierungsschicht *Alle Netzwerkverzög-erungen zwischen Such- und Indizierungsschicht wirken sich direkt auf die Suchleistung aus*		✓			
2	Vermeiden Sie den Einsatz mehrerer unabhängiger Search Heads *Unabhängige Search Heads erlauben keine gemeinsame Verwendung der von Benutzern erstellten Splunk-Artefakte. Sie skalieren außerdem nicht gut im Hinblick auf die Ressourcennutzung innerhalb der*	✓		✓	✓	✓

	Suchschicht. Sofern keine spezifische Anforderung für den Einsatz isolierter Search Head-Umgebungen besteht, gibt es eine bessere Option für die Skalierung.					
3	Nutzen Sie Search Head-Cluster beim Skalieren der Suchschicht *Ein Search Head-Cluster repliziert Benutzerartefakte über den gesamten Cluster und ermöglicht übergreifend über alle Mitglieder des Clusters eine intelligente Planung der Suchworkload. Er stellt darüber hinaus eine Hochverfügbarkeitslösung zur Verfügung.*	✅		✅		
4	Leiten Sie die internen Logs aller Search Heads an die Indizierungsschicht weiter *Alle indizierten Daten sollten nur in der Indizierungsschicht gespeichert werden. Dadurch entfällt die Notwendigkeit, hoch leistungsfähigen Speicher auf der Search Head-Schicht bereitzustellen, und die Verwaltung wird vereinfacht. Hinweis: Dies gilt auch für alle anderen Splunk-Rollen.*		✅			✅
5	Erwägen Sie die Verwendung von LDAP-Authentifizierung wann immer möglich *Die zentrale Verwaltung von Benutzeridentitäten zu Authentifizierungs-zwecken stellt allgemein eine Best Practice in Unternehmen dar, sie vereinfacht die Verwaltung Ihrer Splunk-Bereitstellung und steigert die Sicherheit.*				✅	✅
6	Stellen Sie sicher, dass genügend Kerne für die	✅	✅	✅		

	Anforderungen gleichzeitiger Suchen vorhanden sind *Jede Suche benötigt für die Ausführung einen CPU-Kern. Wenn für die Ausführung einer Suche keine Kerne verfügbar sind, wird die Suche in die Warteschlange eingestellt, was für den Benutzer Verzögerungen bei der Suche bedeutet. Hinweis: Dies trifft auch auf die Indizierungsschicht zu.*					
7	Nutzen Sie die Zeitfenster für die geplante Suche optimal/ausgeglichene Suchlast für die geplante Suche *Oftmals werden geplante Suchen zu bestimmten Zeitpunkten ausgeführt (zur vollen Stunde, 5/15/30 Minuten nach jeder vollen Stunde, um Mitternacht). Das Festlegen eines Zeitfensters, in dem Ihre Suche ausgeführt werden kann, hilft Staus aufgrund gleichzeitiger Ausführung von Suchen zu vermeiden.*		✅	✅		
9	Schränken Sie die Anzahl der einzelnen Search Head-Cluster ein, um die Indizierungsschicht nicht zu überfordern *Die Suchworkload kann nur innerhalb einer SH-Umgebung automatisch gesteuert werden. Unabhängige SHCs haben das Potenzial, mehr Workload durch gleichzeitige Suchen zu generieren, als die Indexerschicht (Such-Peer) verarbeiten kann. Das gleiche gilt für die sorgfältige Planung der Anzahl der eigenständigen Search Heads.*	✅		✅		

10	Verwenden Sie beim Aufbau von Search Head-Clustern eine ungleiche Knotenanzahl (3,5,7 usw.) *Die Auswahl des SHC-Captains erfolgt mithilfe eines mehrheitsbasierten Protokolls. Eine ungerade Anzahl Knoten stellt sicher, dass ein SHC bei Netzwerkausfällen nie in eine gerade Knotenanzahl geteilt werden kann.*	✓				✓

Empfehlungen für die Indizierungsschicht

ENTWURFS-PRINZIPIEN/ BEST PRACTICES (Ihre Anforderungen legen fest, welche Verfahren für Sie gültig sind)		**STÜTZPFEILER**				
		VERFÜGBARKEIT	**PERFORMANCE**	**SKALIERBARKEIT**	**SICHERHEIT**	**VERWALTBARKEIT**
1	Aktivieren Sie parallele Pipelines auf dafür geeigneten Servern *Parallelisierungsfunktionen ermöglichen die Nutzung von verfügbaren Systemressourcen, die ansonsten ungenutzt blieben. Beachten Sie, dass die E/A-Leistung adäquat sein muss, bevor Sie Parallelisierungsfunktionen der Erfassung aktivieren.*		✓	✓		
2	Erwägen Sie die Verwendung von SSDs für HOT/WARM-Volumes und Zusammenfassungen *SSDs haben ökonomisch vertretbare Preise erreicht und beseitigen alle möglichen EA-Einschränkungen, die oftmals den Grund für eine unbefriedigende Suchleistung darstellen.*		✓			
3	Halten Sie die Indizierungsschicht nahe (in		✓			

	Netzwerkbegriffen) an der Suchschicht *Die geringst mögliche Netzwerklatenz hat bei der Suche positive Auswirkungen auf die Benutzererfahrung.*					
4	Verwenden Sie Indexreplikation, wenn Hochverfügbarkeit für historische Daten/Berichte benötigt wird *Indexreplikation stellt sicher, dass mehrere Kopien jedes Ereignisses im Cluster vorhanden sind und schützt so vor Ausfällen von Such-Peers. Passen Sie die Anzahl der Kopien (Replikationsfaktor) gemäß Ihren SLAs an.*	✓				
5	Stellen Sie gute Hygiene bei der Datenerfassung sicher (z. B. Zeilenumbruch, Extraktion von Zeitstempeln, Zeitzone, und dass Quelle, Quelltyp, Host für jede Datenquelle ordnungsgemäß und explizit definiert sind), und richten Sie mithilfe der Monitoring-Konsole fortlaufendes Monitoring ein *Das explizite Konfigurieren von Datenquellen im Gegensatz zur Verwendung der Auto-Ermittlungsfunktionen von Splunk wirkt sich nachweislich günstig auf Datenerfassungskapazität und Indizierungslatenz aus, insbesondere bei Bereitstellungen, die hohe Volumina verarbeiten.*		✓	✓		✓
6	Ziehen Sie die Konfiguration von Suchparallelisierung im Batchmodus auf Indexern mit überschüssiger Verarbeitungsleistung in Erwägung *Das Ausnutzen der Funktionen zur Suchparallelisierung kann einen erheblichen Einfluss auf die Suchleistung für bestimmte Arten von Suchen haben und ermöglicht Ihnen die Nutzung von Systemressourcen, die*		✓	✓		

	andernfalls brachliegen könnten					
7	Überwachen Sie die ausgeglichene Datenverteilung über die Indexerknoten (=Such-Peers). *Eine gleichmäßige Ereignis-/Datenverteilung über die Such-Peers ist ein kritischer Faktor für die Suchleistung und die ordnungsgemäße Durchsetzung von Datenspeicherungsrichtlinien.*		✓	✓		✓
8	Deaktivieren Sie die Weboberfläche auf Indexern in verteilten/gruppierten Bereitstellungen. *Es gibt keinen vernünftigen Grund für den direkten Zugriff auf das WebUI auf Indexern.*		✓		✓	✓
9	Erwägen Sie vordefinierte Splunk Technologie-Add-Ons für bekannte Datenquellen *Anstatt eine eigene Konfiguration aufzubauen, um die Hygiene der Datenerfassung für gut bekannte Datenquellen sicherzustellen, können Sie mit von Splunk zur Verfügung gestellten TAs schneller Mehrwert erzielen und die optimale Implementierung sicherstellen.*		✓			✓
10	Überwachen Sie kritische Metriken von Indexern *Splunk gibt Ihnen eine Monitoring-Konsole an die Hand, die Ihnen wichtige Leistungsmetriken zur Leistung Ihrer Indizierungsschicht zur Verfügung stellt. Dies umfasst die CPU- und Arbeitsspeichernutzung sowie detaillierte Metriken interner Splunk-Komponenten (Prozesse, Pipelines, Warteschlangen, Suche).*	✓	✓			

Empfehlungen für die Erfassungsschicht

	ENTWURFSPRINZIPIEN/ BEST PRACTICES (Ihre Anforderungen legen fest, welche Verfahren für Sie gültig sind)	STÜTZPFEILER				
		VERFÜGBARKEIT	PERFORMANCE	SKALIERBARKEIT	SICHERHEIT	VERWALTBARKEIT
1	Verwenden Sie möglichst immer UF zur Weiterleitung von Daten. Die Verwendung komplexer Forwarder sollte auf die Anwendungsfälle beschränkt werden, in denen sie erforderlich ist. *Integriertes autoLB, Neustartfähigkeit, zentral konfigurierbar, geringe Ressourcenanforderungen*		✓			✓
2	Verwenden Sie mindestens 2x zwischengeschaltete Weiterleitungspipelines an Indexer, wenn Sie viele UFs zusammenfassen müssen *Das Bündeln einer großen Anzahl von Endpunkt-Forwardern über eine kleine Anzahl zwischengeschalteter Forwarder wirkt sich auf die gleichmäßige Ereignisverteilung über die Indexer und damit auf die Suchleistung aus.* ***Setzen Sie zwischengeschaltete Forwarder nur ein, wenn es absolut notwendig ist.***	✓	✓			
3	Erwägen Sie das Schützen von UF-IDX-Datenverkehr mithilfe von SSL				✓	
4	Verwenden Sie natives Splunk LB, um die Daten auf die Indizierungsschicht zu verteilen *Netzwerk-Load Balancer werden aktuell zwischen Forwardern und Indexern nicht unterstützt.*	✓		✓		
5	Verwenden Sie dedizierte Syslog-Server für die Syslog-Erfassung *Syslog-Server können TCP/UDP-Datenverkehr nach*	✓				✓

	Quellen dauerhaft auf Datenträgern erfassen und die ordnungsgemäße Quelltypkonfiguration für die Verarbeitung mit einem universellen Forwarder ermöglichen. Erforderliche Neustarts von Forwardern führen nicht zu Datenverlust.					
6	Verwenden Sie HES für die Erfassung ohne Agent (anstelle des nativen TCP/UDP) *Die HTTP-Ereignissammlung (HES) ist ein Listenerdienst, der das Posten von Ereignissen über das HTTP[/S]-Protokoll ermöglicht. Er kann direkt auf Indexern aktiviert oder in einer komplexen Forwarderschicht konfiguriert werden, in beiden Fällen von einen Load Balancer bedient.*	✓				✓

Empfehlungen für die Verwaltungs-/Hilfsprogrammschicht

	ENTWURFSPRINZIPIEN/ BEST PRACTICES (Ihre Anforderungen legen fest, welche Verfahren für Sie gültig sind)	STÜTZPFEILER				
		VERFÜGBARKEIT	PERFORMANCE	SKALIERBARKEIT	SICHERHEIT	VERWALTBARKEIT
1	Ziehen Sie für kleine Umgebungen die Konsolidierung von LM, CM, SHC-D und MC in einer einzelnen Instanz in Erwägung *Diese Serverrollen haben sehr geringe Ressourcen-anforderungen und sind gute Kandidaten für Colocation. In größeren Indexer-Clustern erfordert der CM möglicherweise einen dedizierten Server, um den Cluster effizient zu verwalten.*					✓
2	Ziehen Sie bei mittelgroßen bis großen Bereitstellungen eine separate Instanz für DS in Erwägung *Sobald eine signifikante Anzahl Forwarder über den Verteilungs-Server verwaltet wird, steigen die*					✓

	Ressourcenanforderungen bis zu einem Punkt an, an dem ein dedizierter Server erforderlich ist, um den Dienst aufrecht zu erhalten.					
3	Ziehen Sie bei sehr großen Bereitstellungen mehrere DSs hinter LB in Erwägung *Hinweis: Für die ordnungsgemäße Einrichtung und Konfiguration ist möglicherweise Hilfe durch die Splunk Professional Services erforderlich*	✓		✓		✓
4	Bestimmen Sie, ob phoneHomeIntervalInSecs auf dem Verteilungs-Server über den Standardwert von 60 Sekunden hinaus verlängert werden kann *Ein längeres Rückrufintervall wirkt sich positiv auf die Skalierbarkeit des Verteilungs-Servers aus*			✓		
5	Verwenden Sie dedizierte/geschützte Verteilungs-Server, um die Clientausnutzung durch App-Bereitstellung zu verhindern *Jeder mit Zugriff auf den Verteilungs-Server kann die von dem betreffenden Verteilungs-Server verwaltete Splunk-Konfiguration verändern, das schließt auch die Bereitstellung potenziell bösartiger Anwendungen auf Forwarder-Endpunkten ein. Es ist daher sinnvoll, diese Rolle angemessen zu schützen.*				✓	
6	Verwenden Sie die Monitoring-Konsole (Monitoring Console, MC), um die Integrität Ihrer Bereitstellung zu überprüfen und bei Problemen Warnungen auszugeben. *Die Monitoring-Konsole bietet eine Sammlung vorkonfigurierter, Splunk-spezifischer Überwachungslösungen und enthält erweiterbare Plattformwarnungen, die Sie über die nachlassende Integrität Ihrer Umgebung informieren können.*	✓	✓			✓

Zusammenfassung und nächste Schritte

Mit diesem Whitepaper haben Sie eine allgemeine Einführung in Splunk Validated Architectures erhalten. Eine Validated Architecture stellt sicher, dass die Anforderungen Ihrer Organisation auf die kostengünstigste, am besten verwaltbare und skalierbarste Weise erfüllt werden. SVAs verwirklichen Best Practices und Entwurfsprinzipien, die auf den folgenden Grundpfeilern aufbauen:

- Verfügbarkeit
- Performance
- Skalierbarkeit
- Sicherheit
- Verwaltbarkeit

In diesem Whitepaper wurde außerdem der aus drei Schritten bestehende Auswahlprozess für Splunk Validated Architectures behandelt: 1) Definition der Anforderungen, 2) Auswahl einer Topologie und 3) Anwenden von Entwurfsprinzipien und Best Practices. Da Sie jetzt mit den vielen Vorzügen von Splunk Validated Architectures vertraut sind, hoffen wir, dass Sie den Prozess des Auswählens einer passenden Bereitstellungstopologie für Ihre Organisation jetzt umsetzen können.

Nächste Schritte

Was geschieht nach der Auswahl einer Validated Architecture? Die nächsten Schritte auf Ihrem Weg zu einer funktionierenden Umgebung umfassen:

Anpassungen

- Betrachten Sie alle erforderlichen Anpassungen an der von Ihnen gewählten Topologie, die zum Erfüllen bestimmter Anforderungen erforderlich sein können.

Bereitstellungsmodell

- Entscheiden Sie sich für ein Bereitstellungsmodell (Bare Metal, virtuell, Cloud).

System

- Wählen Sie Ihre Technologie (Server, Speicher, Betriebssysteme) gemäß den Splunk-Systemanforderungen aus.

Dimensionierung

- Stellen Sie alle relevanten Daten zusammen, die Sie zur Dimensionierung Ihrer Bereitstellung benötigen (Datenerfassung, erwartetes Suchvolumen, Erfordernisse der Datenaufbewahrung, Replikation usw.) Splunk Storage Sizing (https://splunk-sizing.appspot.com/) zählt zu den verfügbaren Tools.

Personalausstattung

- Beurteilen Sie die erforderliche Personalausstattung, um Ihre Bereitstellung zu implementieren und verwalten. Dies ist ein wesentlicher Teil beim Aufbau eines Splunk Centers of Excellence.

Wir stehen bereit, Sie im Validated Architectures-Prozess und bei den nächsten Schritten zu unterstützen. Zögern Sie nicht, Ihr Splunk Account Team mit auftretenden Fragen zu befassen. Ihr Account Team hat Zugriff auf die gesamte Bandbreite der technischen und architektonischen Ressourcen bei Splunk und hilft Ihnen gerne mit weiteren Informationen.

Viel Spaß beim Splunken!

Anhang

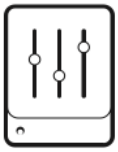
Dieser Abschnitt enthält ergänzende Referenzinformationen, die in den SVAs verwendet werden.

Anhang "A": Erläuterung: die Grundpfeiler von SVA

Grundpfeiler	Beschreibung	Hauptziele/Entwurfsprinzipien
Verfügbarkeit	Die Fähigkeit zur ständigen Betriebsbereitschaft und zur Wiederherstellung nach geplanten oder ungeplanten Ausfällen oder Unterbrechungen.	1. Beseitigen isolierter Schwachstellen (Single Points of Failure)/Hinzufügen von Redundanz 2. Erkennen geplanter und nicht geplanter Fehler/Ausfälle 3. Eindämmen geplanter/nicht geplanter Ausfälle, im Idealfall automatisch 4. Planen rollierender Upgrades
Performance	Die Fähigkeit zur effektiven Nutzung der verfügbaren Ressourcen, um ein optimales Serviceniveau unter wechselnden Nutzungsmustern aufrecht zu erhalten.	1. Hinzufügen von Hardware zum Steigern der Leistung; Rechenkapazität, Massenspeicher, Arbeitsspeicher. 2. Beseitigung von Engpässen "von unten nach oben" 3. Ausschöpfen aller Mittel zur parallelen Verarbeitung 4. Nutzen von Lokalität (d. h. Minimieren der Verteilung von Komponenten) 5. Optimierung für den gängigen Fall (80/20-Regel) 6. Vermeiden nicht benötigter Generalität 7. Zeitversetzte Berechnung (Vorausberechnung, Lazy Computing, gemeinsame Berechnung, Batchcomputing) 8. Abstriche an Sicherheit und Genauigkeit zugunsten der Geschwindigkeit (Randomisierung, Sampling)
Skalierbarkeit	Die Fähigkeit, sicherzustellen, dass das System für Skalierung in allen Schichten ausgelegt ist und gesteigerte Workloads effektiv verarbeiten kann.	1. Vertikale und horizontale Skalierung

Grundpfeiler	Beschreibung	Hauptziele/Entwurfsprinzipien
		2. Trennung von funktionalen Komponenten, die einzeln skaliert werden müssen 3. Minimieren von Abhängigkeiten zwischen Komponenten 4. Auslegung für absehbares zukünftiges Wachstum zum frühest möglichen Zeitpunkt 5. Einführung von Hierarchie in den Gesamtentwurf des Systems
Sicherheit	Die Fähigkeit, sicherzustellen, dass das System für den Schutz von Daten ebenso wie von Konfigurationen/Vermögenswerten ausgelegt ist, während es fortlaufend Mehrwert generiert.	1. Auslegung als sicheres System von Grund auf 2. Nutzung von Protokollen auf dem aktuellsten Stand der Technik für den gesamten Datenaustausch 3. Ermöglichen von allgemeinem und Detailzugriff auf Ereignisdaten 4. Einsatz von zentraler Authentifizierung 5. Implementierung von Überwachungsverfahren 6. Reduzierung von Angriffsflächen oder Ansatzpunkten zur böswilligen Verwendung
Verwaltbarkeit	Die Fähigkeit, sicherzustellen, dass das System für den Betrieb und die Verwaltung aller Schichten von einem zentralen Ort aus ausgelegt ist.	1. Bereitstellen einer zentralen Verwaltungsfunktion 2. Verwalten des Lebenszyklus von Konfigurationsobjekten (Versionsverwaltung) 3. Messen und Überwachen/Nutzung von Anwendungsprofilen (Splunk) 4. Messen und Überwachen der Systemintegrität

Anhang "B": Topologiekomponenten

Schicht	Komponente	Symbol	Beschreibung	Hinweise
Verwaltung	Verteilungs-Server (Deployment Server, DS)		Der Verteilungs-Server verwaltet die Konfiguration der Forwarder-Konfiguration.	Er sollte auf einer dedizierten Instanz bereitgestellt werden. Er kann zwecks einfacher Wiederherstellung bei Fehlern virtualisiert werden.
	Lizenz-Master (LM)		Der Lizenz-Master wird von anderen Splunk-Komponenten benötigt, um lizenzierte Funktionen zu aktivieren und das Volumen der täglichen Datenerfassung nachzuverfolgen.	Die Rolle des Lizenz-Master hat nur minimale Anforderungen an Kapazität und Verfügbarkeit und kann mit anderen Verwaltungsfunktionen auf dem gleichen System platziert werden. Er kann zwecks einfacher Wiederherstellung bei Fehlern virtualisiert werden.
	Monitoring-Konsole (Monitoring Console, MC)		Die Monitoring-Konsole stellt Dashboards für die Überwachung von Nutzung und Integrität Ihrer Umgebung zur Verfügung. Sie enthält darüber hinaus eine Reihe vorkonfigurierter Plattformwarnungen, die angepasst werden können, um Benachrichtigungen zu Betriebs-problemen bereitzustellen.	In Umgebungen mit Cluster kann der MC mit dem Master-Knoten auf einem System platziert werden, kommt kein Cluster zum Einsatz, können zusätzlich die Lizenz-Master- und die Verteilungs-Server-Funktion hinzugenommen werden. Er kann zwecks einfacher Wiederherstellung bei Fehlern virtualisiert werden.
	Cluster-Master (CM)		Der Cluster-Master ist der erforderliche Koordinator sämtlicher Aktivitäten in einer Bereitstellung mit Cluster(n).	In Clustern mit einer großen Anzahl von Indexbuckets (großes Datenvolumen/Aufbewahrung) ist für den Cluster-Master mit hoher Wahrscheinlichkeit ein dedizierter Server erforderlich. Er kann zwecks einfacher Wiederherstellung bei Fehlern virtualisiert werden.

Schicht	Komponente	Symbol	Beschreibung	Hinweise
	Search Head-Cluster-Verteiler (Search Head Cluster Deployer, SHC-D)		Der Search Head-Cluster-Verteiler ist für das Bootstrapping eines SHCs und für das Verwalten der auf dem Cluster bereitgestellten Splunk-Konfiguration erforderlich.	Der SHC-D ist keine Laufzeitkomponente und hat nur minimale Systemanforderungen. Er kann mit anderen Verwaltungsrollen zusammen auf dem gleichen System platziert werden. Hinweis: Jeder SHC benötigt eine eigene SHC-Verteiler-Funktion. Er kann zwecks einfacher Wiederherstellung bei Fehlern virtualisiert werden.
Suche	Search Head (SH)		Der Search Head stellt die Benutzeroberfläche für Splunk-Benutzer zur Verfügung und koordiniert die geplanten Suchaktivitäten.	Search Heads sind dedizierte Splunk-Instanzen in verteilten Bereitstellungen. Search Heads können zur leichten Wiederherstellung bei Fehlern virtualisiert werden, vorausgesetzt, sie wurden mit entsprechenden CPU- und Arbeitsspeicher-ressourcen bereitgestellt.
	Search Head Cluster (SHC)		Ein Search Head-Cluster ist ein Pool von mindestens drei Search Heads in einem Cluster. Er bietet horizontale Skalierbarkeit für die Search Head-Schicht und transparentes Benutzer-Failover bei Ausfällen.	Für Search Head-Cluster sind dedizierte Server mit idealerweise identischen Systemspezifikationen erforderlich. Mitglieder von Search Head-Clustern können zur leichten Wieder-herstellung bei Fehlern virtualisiert werden, vorausgesetzt, sie wurden mit entsprechenden CPU- und Arbeitsspeicher-ressourcen bereitgestellt.
Indizierung	Indexer		Indexer stellen die Kernkomponente von Splunk dar. Sie verarbeiten und indizieren alle eingehenden Daten und dienen darüber hinaus als Such-Peers, um die in der Suchschicht	Indexer müssen in verteilten Umgebungen oder Umgebungen mit Cluster(n) immer auf dedizierten Servern bereitgestellt werden. In einer Single Server-Bereitstellung stellt der Indexer außerdem die Benutzeroberfläche für

Schicht	Komponente	Symbol	Beschreibung	Hinweise
			eingeleiteten Suchanfragen zu bedienen.	die Suche zur Verfügung und übernimmt die Funktion als Lizenz-Master. Indexer erzielen die beste Leistung auf Bare Metal-Servern oder in dedizierten virtuellen Hochleistungs-maschinen, wenn entsprechende Ressourcen sichergestellt werden können.
Datenerfassung	Forwarder und andere Datenerfassung-komponenten		Allgemeines Symbol für jede Komponente, die an der Datenerfassung beteiligt ist.	Dies schließt universelle und komplexe Forwarder, Netzwerk-Dateneingaben und andere Formen der Datenerfassung (HES, Kafka usw.) ein.