ztC Edge Benutzerhandbuch

Hinweis

Die Informationen in diesem Dokument können ohne Ankündigung geändert werden.

SOFERN NICHT AUSDRÜCKLICH IN EINER SCHRIFTLICHEN, VON EINEM AUTORISIERTEN REPRÄSENTANTEN VON STRATUS TECHNOLOGIES SIGNIERTEN VEREINBARUNG FESTGELEGT, GIBT STRATUS KEINE GARANTIEN ODER ERKLÄRUNGEN JEGLICHER ART HINSICHTLICH DER HIERIN ENTHALTENEN INFORMATIONEN, EINSCHLIESSLICH DER GARANTIE DER MARKTFÄHIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK.

Stratus Technologies übernimmt keine Verantwortung oder Verpflichtung jeglicher Art für hierin enthaltene Fehler oder in Verbindung mit der Bereitstellung, Leistung oder Verwendung dieses Dokuments. Die in Stratus-Dokumenten beschriebene Software (a) ist das Eigentum von Stratus Technologies Ireland, Ltd. oder der Drittpartei, (b) wird unter Lizenz bereitgestellt und (c) darf nur kopiert oder verwendet werden wie in den Lizenzbedingungen ausdrücklich erlaubt.

Die Stratus-Dokumentation beschreibt alle unterstützten Funktionen der Benutzeroberflächen und der Anwendungsprogrammierschnittstellen (APIs), die von Stratus entwickelt wurden. Etwaige nicht dokumentierte Funktionen dieser Benutzeroberflächen und Schnittstellen sind ausschließlich für Stratus-Mitarbeiter gedacht und können ohne Ankündigung geändert werden.

Copyright

Name des Handbuchs: *ztC Edge Benutzerhandbuch*

Produktversionsnummer: Stratus Redundant Linux Version 2.2.0.0

Veröffentlicht am: Mittwoch, 25. November 2020

Stratus Technologies, Inc.

5 Mill and Main Place, Suite 500

Maynard, Massachusetts 01754-2660

Inhaltsverzeichnis

Teil 1: ztC Edge Benutzerhandbuch

Das *ztC Edge Benutzerhandbuch* beschreibt ztC Edge-Systeme, ihre Bereitstellung und ihre Verwendung.

Systembeschreibungen einschließlich der Betriebsmodi und der Speicher- und Netzwerkarchitektur finden Sie unter:

- Einführung in ztC Edge-Systeme

Informationen zur Planung und Bereitstellung finden Sie unter:

- Erste Schritte

In den folgenden Themen wird die Verwaltung von ztC Edge-Systemen beschrieben:

- Verwenden der ztC Console
- Aktualisieren der Stratus Redundant Linux-Software
- Verwalten von physischen Maschinen
- Verwalten von virtuellen Maschinen
- Warten von physischen Maschinen
- Überwachen des Systems, Windows-basierter VMs und Anwendungen (auf Systemen, die für diese Überwachung lizenziert sind)

1

Kapitel 1: Einführung in ztC Edge-Systeme

Eine Einführung in ztC Edge-Systeme finden Sie in den folgenden Themen:

- ztC Edge-Systemüberblick
- Betriebsmodi
- Netzwerkarchitektur
- Systemnutzungseinschränkungen

ztC Edge-Systemüberblick

Ein ztC Edge-System bietet die automatisierte Wiederherstellung ohne Datenverlust, falls es zu einem Hardwareausfall kommt. Weitere Informationen zu den Systemfunktionen und -merkmalen finden Sie in den folgenden Themen.

- Beschreibung des ztC Edge-Systems
- Physische Maschinen und virtuelle Maschinen
- Administrative Operationen
- Alarme
- Remotesupport
- Lights Out Management
- Verwaltungstools von Drittanbietern

Beschreibung des ztC Edge-Systems

Mit der Stratus Redundant Linux-Software können zwei einzelne ztC Edge-Computer (mit den entsprechenden Lizenzen) als einzelnes, hochverfügbares oder fehlertolerantes System zusammenarbeiten. Jeder dieser Computer wird als physische Maschine (PM) oder Knoten bezeichnet.

Beide PMs

- führen dasselbe Host-Betriebssystem aus (CentOS)
- enthalten replizierte virtuelle Maschinen und Speicher (über direkte Ethernet-Verbindungen zwischen den beiden PMs synchronisiert)
- unterstützen virtuelle Maschinen, die unterstützte Gastbetriebssysteme ausführen

Weitere Informationen zur Konfiguration von PMs in einem ztC Edge-System finden Sie unter Übersicht über die Systemanforderungen.

Stratus Redundant Linux-Software kann auch auf einer einzelnen PM ausgeführt werden, wenn das System für einen Knoten lizenziert ist. In dieser Konfiguration ist das System ein Simplexsystem, es ist nicht fehlertolerant oder hochverfügbar, und im normalen Betrieb zeigt das System Netzwerkfehler an.

Verwandte Themen

Übersicht über die Systemanforderungen

Getestete Gastbetriebssysteme

Netzwerkarchitektur

Physische Maschinen und virtuelle Maschinen

Ein ztC Edge-System mit zwei physischen Maschinen (PMs), auch als Knoten bezeichnet, schützt Anwendungen transparent durch das Erstellen von redundanten virtuellen Maschinen (VMs), die auf beiden Knoten ausgeführt werden.

ztC Edge-Software kann auch in einem System mit einer einzelnen PM ausgeführt werden, wenn das System für einen Knoten lizenziert ist. Informationen zu Systemen, die für einen Knoten lizenziert sind, finden Sie unter Beschreibung des ztC Edge-Systems. Die weiteren Informationen in diesem Thema gelten für Systeme, die für zwei Knoten lizenziert sind.

Die Stratus Redundant Linux-Verwaltungssoftware kann eine Gast-VM ganz neu erstellen, es ist aber auch möglich, vorhandene VMs aus anderen Umgebungen zu importieren und in Gast-VMs umzuwandeln. Durch das Erstellen einer identischen Instanz der ausgewählten VM auf einer zweiten Host-PM bietet die

Verwaltungssoftware automatisch Hochverfügbarkeit Schutz der FT-Klasse für die VM. Der Systemadministrator verwaltet diese Entität von einer separaten, browsergestützten Verwaltungskonsole aus. Dies ist die ztC Console.

Weder die Anwendung noch der Benutzer ist den redundanten Computerressourcen auf den beiden Host-PMs ausgesetzt. Die Anwendung „sieht“ nur einen Hostnamen, nur eine MAC-Adresse für jede Netzwerkschnittstelle, die der VM bereitgestellt wird, und eine IP-Adresse für jede VM-Netzwerkschnittstelle, die der VM bereitgestellt wird. Ein Systemadministrator lädt die Anwendungen auf die Gast-VM und konfiguriert sie dort genau wie auf einem physischen Server. Wenn bei einem Datenträger oder Netzwerkgerät ein Fehler oder Ausfall passiert, leitet die Software Input/Output automatisch an die gekoppelte Host-PM um, damit der Betrieb nicht unterbrochen wird. Zwar ist bis zur Behebung des Ausfalls keine Redundanz gegeben, die VM kann jedoch weiterhin normal betrieben werden. Die Anwendung wird weiterhin ausgeführt, als ob nichts geschehen wäre. Die Redundanz, Fehlererkennung, Isolierung und Verwaltung sind für die Windows- oder Linux-Umgebung und die darin ausgeführte Anwendung vollkommen transparent. Die Reparatur der PM ist ebenfalls transparent und automatisch. Wenn eine fehlerhafte Komponente der PM repariert wurde, bezieht die Software die reparierten Komponenten automatisch in die geschützte Umgebung der Gast-VM mit ein und stellt die Redundanz transparent wieder her.

Verwandte Themen

Verwenden der ztC Console

Die Seite „Physische Maschinen“

Die Seite „Virtuelle Maschinen“

Administrative Operationen

Viele administrative Aufgaben im ztC Edge-System können Sie von der ztC Console aus ausführen. Dies ist eine browserbasierte Benutzeroberfläche, die den Zugriff auf das System als Ganzes sowie auf physische Maschinen, virtuelle Maschinen und andere Ressourcen ermöglicht. Weitere Informationen finden Sie unter Die ztC Console.

Alarme

Mit Alarmmeldungen benachrichtigt das ztC Edge-System den Systemadministrator, wenn etwas seine Aufmerksamkeit erfordert. Zum Beispiel:

- Konfigurationsaufgaben, die ausgeführt werden müssen
- Benachrichtigung über Betriebszustände des Systems
- Systemprobleme, die ein Eingreifen erfordern

Klicken Sie im linken Navigationsbereich auf **Dashboard**, um Alarmmeldungen mit Beschreibungen anzuzeigen. Klicken Sie im linken Navigationsbereich auf **Alarme**, um das Alarmprotokoll anzuzeigen.

Die folgenden Symbole geben den Zustand einer Alarmmeldung an.

 Zur Information

 Normal oder OK

 Geringfügig, Warnung oder ungleichmäßiger Zustand

 Moderater Zustand

 Beschädigt, ausgefallen oder schwerwiegender Zustand

Remotesupport

Um die Remotesupportfunktionen des ztC Edge-Systems aufzurufen, klicken Sie im linken Navigationsbereich auf **Voreinstellungen**. In den Voreinstellungen können Sie Support- und Proxyspezifikationen festlegen, indem Sie Folgendes wählen:

- **Supportkonfiguration** – Konfigurieren Sie Einstellungen, um zuzulassen, dass der Remotesupport über Ihren autorisierten Stratus-Servicemitarbeiter Zugriff auf Ihr System hat, und um es dem System zu ermöglichen, Integritäts- und Statusbenachrichtigungen an Ihren autorisierten Stratus-Servicemitarbeiter zu senden. Ausführliche Informationen finden Sie unter Konfigurieren der Remotesupport-Einstellungen.
- **Proxykonfiguration** – Ermöglicht Ihnen die Konfiguration eines Proxyservers für den Internetzugriff. Ausführliche Informationen finden Sie unter Konfigurieren der Internetproxyeinstellungen.

Lights Out Management

ztC Edge-Systeme bieten Intel® Active Management Technology (AMT) LOM-Unterstützung, die standardmäßig deaktiviert ist. Sie können diese Unterstützung aktivieren und konfigurieren, indem Sie **Strg-P** drücken, während der BIOS-Begrüßungsbildschirm beim Systemstart angezeigt wird. Wichtige Informationen zur AMT-Konfiguration und zu Einschränkungen finden Sie in der Knowledge Base im Artikel *AMT and Remote Access in ztC Edge* (KB-8219). Siehe Zugriff auf Artikel in der Knowledge Base.

AMT-Features sind am Netzwerk-Port **P1** des Systems zugänglich.

Verwaltungstools von Drittanbietern

Sie können Verwaltungstools von Drittanbietern in ztC Edge-Systemen installieren. Beispiele für solche Tools sind unter anderem anbieterspezifische Hilfsprogramme für die Verwaltung/Überwachung, Unternehmenshilfsprogramme für die Verwaltung/Überwachung und verschiedene andere Software für die Verwaltung/Überwachung. Beachten Sie Folgendes:

- Im Allgemeinen sollten Verwaltungstools, die unter dem Host-Betriebssystem (CentOS) laufen, auch in ztC Edge-Systemen verwendet werden können. Mögliche Ausnahmen sind Tools, die die CentOS KVM-basierte Virtualisierung verwalten/überwachen. Verwenden Sie zur Verwaltung/Überwachung der ztC Edge-Virtualisierung die integrierten ztC Edge-Verwaltungstools.
- Stratus empfiehlt, vor der Bereitstellung des ztC Edge-Systems zu überprüfen, dass es korrekt mit den installierten Verwaltungstools betrieben werden kann.
- Stratus empfiehlt, für Verwaltungstools von Drittanbietern ein anderes Konto als das root-Konto einzurichten.
- Sie können über das Verwaltungsnetzwerk auf Ihr ztC Edge-System zugreifen, indem Sie die IP-Adresse(n) verwenden, die während des Installationsvorgangs angegeben wurden (oder vom DHCP-Server zugewiesen wurden, falls die Schnittstelle für DHCP konfiguriert wurde).
- Wenn Sie Verwaltungstools von Drittanbietern im Host-Betriebssystem einer physischen Maschine (PM) installieren und diese PM später ersetzen müssen, vergessen Sie nicht, die Tools auf der Ersatz-PM zu installieren.

> **Hinweis**: Verwaltungstools von Drittanbietern können die Umgebung des Hostbetriebssystems und die Systemsoftware destabilisieren. Möglicherweise müssen Sie Verwaltungstools entfernen, die sehr viel RAM oder Festplattenspeicher benötigen oder das Produkt auf andere Weise destabilisieren können. Halten Sie sich an die Empfehlungen von Ihrem autorisierten Stratus-Servicemitarbeiter.

Informationen zum Zugriff auf das Host-Betriebssystem finden Sie unter Zugriff auf das Host-Betriebssystem.

Verwandte Themen

Erste Schritte

Systemreferenzinformationen

Betriebsmodi

Ein ztC Edge-System bietet zwei Betriebsmodi, um benutzerdefinierte Verfügbarkeitsstufen für VMs festzulegen:

- Hochverfügbarkeitsbetrieb
- Fehlertoleranter Betrieb

Sowohl der HV- als auch der FT-Betrieb erreichen ihre jeweilige Redundanzstufe durch den Einsatz von zwei physischen Maschinen (PMs). Der FT-Betrieb benötigt mehr Systemressourcen, was zu einer langsameren Performance von Anwendungen führen kann.

Stratus empfiehlt die Konfiguration eines Quorumdienstes sowohl für den HV- als auch den FT-Betrieb. Der Quorumdienst verhindert eine *Split Brain* genannte Situation, in der beide PMs eines Paars im HV-Betrieb und im FT-Betrieb unabhängig voneinander laufen. Weitere Informationen finden Sie unter Quorumserver.

Hochverfügbarkeitsbetrieb

Die ztC Edge-Software bietet zwei benutzerdefinierte Verfügbarkeitsstufen für VMs: Hochverfügbar (HV) und Fehlertolerant (FT).

Im HV-Betrieb erkennt, isoliert und behebt Stratus Redundant Linux die meisten Hardwareausfälle und sorgt so für den fortgesetzten Betrieb Ihrer Anwendungen. Mit der HV-Remotesupporttechnologie benachrichtigt die Software das Stratus-Supportcenter über verschiedene Probleme und gibt dabei den Fehlertyp und den genauen Ort an. Diese Kombination aus automatischer Fehlererkennung, Isolierung und Remotesupporttechnologie stellt den raschen Zugriff der Technikexperten des Supportteams und damit die schnelle Problemlösung sicher.

Die Verfügbarkeitsstufe einer VM wird festgelegt, wenn Sie die VM mit der ztC Console erstellen oder importieren.

Der HV-Betrieb bietet, sofern diese Option aktiviert ist, grundlegendes Failover und Wiederherstellung, wobei einige Fehler einen (automatischen) Neustart der VM für die Wiederherstellung der VM und die Rückkehr zum HV-Betrieb erfordern:

- verhindert Ausfallzeiten für viele, aber nicht alle CPU-, Arbeitsspeicher-, E/A- oder andere Fehler bei der physischen Maschine (PM)
- behandelt Fehler ohne IT-Eingreifen
- bietet die kontinuierliche, aktive Überprüfung aller Komponenten
- stellt jederzeit vollständige Redundanz und Wiederherstellung sicher

Der HV-Betrieb eignet sich für Anwendungen, die gelegentliche Ausfälle für einige Minuten tolerieren können.

Verwandte Themen

Die Seite „Virtuelle Maschinen“

Verwenden der ztC Console

Fehlertoleranter Betrieb

Die ztC Edge-Software bietet zwei benutzerdefinierte Verfügbarkeitsstufen für VMs: Hochverfügbar (HV) und Fehlertolerant (FT). Im FT-Betrieb wird eine Anwendung bei einem Fehler weiter ausgeführt, ohne dass es zu Ausfallzeiten kommt. Verwenden Sie den FT-Betrieb für Anwendungen, die auf höchste Verfügbarkeit angewiesen sind.

Die Verfügbarkeitsstufe einer VM wird festgelegt, wenn Sie die VM mit der ztC Console erstellen oder importieren.

Im FT-Betrieb schützt die ztC Edge-Software eine Anwendung transparent durch das Erstellen einer redundanten Umgebung für eine VM auf zwei physischen Maschinen (PMs). Mit einer identischen Instanz der ausgewählten VM auf einem zweiten Host bietet die ztC Edge-Software Schutz der FT-Klasse für die VM.

Wenn diese Option aktiviert ist, schützt der FT-Betrieb eine VM transparent ohne Ausfallzeit gegen alle Fehler, außerdem kann der FT-Betrieb:

- Ausfallzeiten wegen CPU-, Arbeitsspeicher-, E/A- oder anderen Fehlern der physischen Maschine (PM) verhindern
- Fehler ohne IT-Eingreifen behandeln
- Datenverluste verhindern
- kontinuierliche, aktive Überprüfung aller Komponenten bieten
- jederzeit vollständige Redundanz und Wiederherstellung sicherstellen

Verwandte Themen

Die Seite „Virtuelle Maschinen“

Verwenden der ztC Console

ALSR-Konfigurationen

Eine *Automated Local Site Recovery* (ALSR) *-Konfiguration* verbindet zwei physische Maschinen in zwei separaten Anlagen (Sites). Es handelt sich um eine notfalltolerante Implementierung, die Hardwareredundanz sowie die Redundanz physischer Rechenzentren und der Gebäude, die sie enthalten, bereitstellt. Aufgrund der räumlichen Trennung muss in einer ALSR-Konfiguration sorgfältig geplant werden, wo Komponenten platziert werden, und die Netzwerktopologie ist komplexer. **Für ALSR-Konfigurationen empfiehlt Stratus dringend, den Quorumdienst zu verwenden, da die A-Link-Netzwerke in einer ALSR-Konfiguration dem Risiko weiterer potenzieller Ausfallszenarien ausgesetzt sind.** (ALSR-Konfigurationen sind bei Systemen, die für einen Knoten lizenziert sind, nicht verfügbar.)

Unter Erfüllen der Netzwerkanforderungen sind die Anforderungen für Netzwerke in einer ALSR-Konfiguration aufgeführt.

ALSR und Quorumdienst

Konfigurieren Sie in einer ALSR-Konfiguration zwei Quorumdienstcomputer in Übereinstimmung mit den Best Practices, die für die Quorumbereitstellung empfohlen werden (siehe Quorumserver und Platzieren und Erstellen des Quorumservers). In einer ALSR-Konfiguration befindet sich ein bevorzugter Quorumdienstcomputer in einer dritten Anlage und ein alternativer in einer vierten Anlage (oder, bei sorgfältiger Platzierung, ebenfalls in der dritten). Die Netzwerke sind miteinander verbunden.

Quorumdienstcomputer sollten so isoliert wie möglich sein. Falls sich beide in ein und derselben Anlage (der dritten Anlage) befinden müssen, achten Sie unbedingt darauf, dass sie nicht von derselben Stromversorgung abhängig sind.

Physische Konnektivität zwischen einer ztC Edge-PM und den Quorumdienstcomputern darf nicht über die Anlage der anderen PM geführt werden.

Durch die Platzierung eines Quorumdienstcomputers in derselben Anlage wie eine der ztC Edge-PMs wird die Datenintegrität sichergestellt. Bestimmte Sitefehler machen es in diesem Fall jedoch erforderlich, dass die VMs heruntergefahren werden müssen, bis die manuelle Wiederherstellung erfolgt ist.

Das Verwaltungsnetzwerk verbindet die beiden ztC Edge-PMs und die Quorumdienstcomputer physisch. Damit dies korrekt funktioniert, müssen Sie beide ztC Edge-PMs so konfigurieren, dass sie unterschiedliche Gateways verwenden, um mit den Quorumdienstcomputern zu kommunizieren. Wenn die beiden PMs dasselbe Gateway verwenden, um die Quorumdienstcomputer zu erreichen, ist bei Ausfällen die Datenintegrität sichergestellt. Bestimmte Sitefehler machen es in diesem Fall jedoch erforderlich, dass die VMs heruntergefahren werden müssen, bis die manuelle Wiederherstellung erfolgt ist.

Verwandte Themen

Erstellen einer ALSR-Konfiguration

Netzwerkarchitektur

Quorumserver

Ein *Quorumdienst* ist ein auf dem Windows-Betriebssystem basierender Dienst, der auf einem anderen Server als den beiden Servern (physischen Maschinen, PMs) bereitgestellt wird. Quorumserver bieten bei bestimmten Fehlern in einer ztC Edge-Umgebung Zusicherung der Datenintegrität und automatische Neustartfunktionen. Stratus empfiehlt dringend die Verwendung von Quorumservern, besonders im ALSR-Betrieb. Sie können ein ztC Edge-PM-Paar mit 0, 1 oder 2 Quorumservern konfigurieren.

Quorumserver stellen die Integrität von VMs für verschiedene Netzwerkausfallszenarien sicher, darunter Split-Brain, und ermöglichen nach bestimmten Fehlern den Start von VMs ohne Benutzereingreifen. Die Kommunikation mit Quorumservern erfolgt über das Verwaltungsnetzwerk.

Quorumserver sind in ALSR-Konfigurationen besonders wichtig. Ein bewährtes Verfahren für ALSR ist es, einen bevorzugten Quorumcomputer in einer dritten und einen alternativen Quorumcomputer in einer vierten Anlage zu platzieren. Sie können den alternativen Quorumdienstcomputer jedoch auch mit dem bevorzugten Quorumcomputer zusammen platzieren und trotzdem einen zufriedenstellenden Dienst erreichen. Weitere Informationen finden Sie unter ALSR-Konfigurationen.

Wenn nur zwei Anlagen verfügbar sind (die oben empfohlene Konfiguration also nicht möglich ist) und dann eine PM ausfällt und die andere PM nicht mit dem Quorumserver kommunizieren kann (zum Beispiel, weil er sich in derselben Anlage wie die ausgefallene PM befindet), werden die VMs in der verbliebenen funktionierenden Anlage automatisch heruntergefahren, um den Split-Brain-Betrieb zu vermeiden.

Verwandte Themen

Erstellen einer ALSR-Konfiguration (hier werden auch Quorumserver behandelt)

Konfigurieren der Quorumserver

Netzwerkarchitektur

Ethernet-Netzwerke stellen Kommunikationswege in einem System bereit. Die wichtigsten Ethernet-Netzwerktypen sind:

- *Availability-Link-Netzwerke*, kurz *A-Link-Netzwerke* (an den blauen (**A2** oder •) und gelben (**A1** oder • •) Netzwerkports) in ztC Edge-Systemen, die für zwei Knoten lizenziert sind, werden virtuellen Maschinen (VMs) zugewiesen und zum Synchronisieren von Daten oder zum Migrieren von VMs zwischen zwei PMs verwendet. Ein A-Link-Netzwerk (am blauen (**A2** oder •) Netzwerkport) ist ein *privates Netzwerk* (priv0), das die beiden ztC Edge-PMs verbindet. Weitere Informationen finden Sie unter A-Link- und private Netzwerke. (Systeme, die für einen Knoten lizenziert sind, bieten keine A-Link-Funktionalität.)
- *Unternehmensnetzwerke* (am Netzwerk-Port **P1** und an **P2**, falls aktiviert) in allen ztC Edge-Systemen ermöglichen die Verbindung Ihrer Anwendungen mit dem vorhandenen Netzwerk. Ein Unternehmensnetzwerk (am Netzwerk-Port **P1**) kann auch ein *Verwaltungsnetzwerk* (ibiz0, manchmal als Netzwerk0 bezeichnet) sein, das mit der ztC Console verbunden ist und von den Quorumservern verwendet wird. Weitere Informationen finden Sie unter Unternehmens- und Verwaltungsnetzwerke.

Ein ztC Edge-System bietet auch einen Mechanismus zur Erkennung der Netzwerksegmentierung. Informationen hierzu finden Sie unter Erkennung und Behebung von Fehlern bei der Netzwerksegmentierung.

A-Link- und private Netzwerke

Jedes ztC Edge-System, das für zwei physische Maschinen (PMs, auch als Knoten bezeichnet) lizenziert ist, benötigt ein Netzwerk für den privaten Verwaltungsdatenverkehr zwischen den beiden PMs. Dieses private Netzwerk wird als *priv0* bezeichnet. Dies ist eine physische, direkte Ethernet- oder VLAN-Verbindung zwischen den Knoten. priv0 wird für die Erkennung verwendet und kann keine anderen Entitäten enthalten, die auf IPv4-Broadcasts reagieren.

Zusätzlich zum priv0 verfügt jedes System, das für zwei Knoten lizenziert ist, über A-Link-Netzwerke, um die Leistung bei der Datenreplikation zwischen den PMs zu verbessern. Über A-Link-Netzwerke können Sie Datenträger synchronisieren, Netzwerke verbinden, VMs migrieren, Heartbeat-Überprüfungen ausführen und fehlertoleranten Arbeitsspeicher synchronisieren.

Die A-Link-Netzwerke und priv0 sind auf die gleiche Weise mit den PMs verbunden. Die A-Links sind mit den blauen und gelben Netzwerk-Ports der beiden PMs verbunden, wobei priv0 mit dem A-Link am blauen Netzwerk-Port geteilt wird.

Das einfachste priv0 besteht aus einem einzelnen Ethernet-Kabel (Crossover oder nicht gekreuzt), das direkt mit einem Embedded-Ethernet-Port auf jedem Server verbunden ist. Wenn ein anderes Netzwerkgerät als ein einzelnes Ethernet-Kabel für priv0 verwendet wird, lesen Sie ALSR-Konfigurationen.

Verwandte Themen

Unternehmens- und Verwaltungsnetzwerke

Anforderungen für A-Link- und private Netzwerke

Netzwerkarchitektur

Unternehmens- und Verwaltungsnetzwerke

Alle Ethernet-Ports, die nicht von A-Link-Netzwerken und dem privaten Netzwerk verwendet werden, gelten als Unternehmensnetzwerk-Ports, über die sich Ihre Gastbetriebssysteme mit Ihrem Netzwerk verbinden.

Ein Unternehmensnetzwerk ist das *Verwaltungs*netzwerk, das auf die ztC Console zugreift und verschiedene Verwaltungsaufgaben übernimmt sowie den Quorumserver verwaltet. Jede PM hat ein einzelnes Verwaltungsnetzwerk, das als *ibiz0*bezeichnet wird und das Netzwerk mit der Bezeichnung **P1** verwendet.

Sie richten das Verwaltungsnetzwerk ein, wenn Sie installieren das System bereitstellen. Sie können auch Unternehmensnetzwerke für alle Unternehmensnetzwerk-Ports einrichten, die während der Bereitstellung physisch verbunden sind. Informationen zum Verbinden eines zweiten Unternehmensnetzwerks nach Abschluss der Bereitstellung finden Sie unter Verbinden eines zweiten Unternehmensnetzwerks.

Verwandte Themen

A-Link- und private Netzwerke

Anforderungen für Unternehmens- und Verwaltungsnetzwerke

Netzwerkarchitektur

Erkennung und Behebung von Fehlern bei der Netzwerksegmentierung

Wenn ein Netzwerkfehler auftritt, bei dem die beiden Enden eines gemeinsamen Netzwerks nicht miteinander kommunizieren können, aber jeweils noch über die externe Netzwerkverbindung verfügen, spricht man von einem *Netzwerksegmentierungsfehler*.

Ein ztC Edge-System bietet einen *Mechanismus zur Erkennung von Netzwerksegmentierungsfehlern*, der die aktive VM auf den Knoten platziert, der über die beste externe Netzwerkkonnektivität verfügt, wenn das System diesen Fehler erkennt. Im Rahmen dieser Funktion sendet das ztC Edge-System ständig UDP-Pakete über die Unternehmensnetzwerkschnittstelle zwischen den aktiven und den Standbyknoten. Die

Netzwerksegmentierungslogik des Systems erkennt einen Fehler, wenn dieser Paketfluss unterbrochen wird, während beide Seiten noch eine aktive Netzwerkverbindung haben. In diesem Fehlerszenario haben beide Knoten noch aktive Netzwerkverbindungen, deshalb liegt der Fehler bei einem Switch außerhalb des ztC Edge-Systems.

Wenn dieser Fall erkannt wird, behandelt das ztC Edge-System den Fehler basierend auf der Logik, die ermittelt, welche Seite die bessere externe Konnektivität hat. Das ztC Edge-System trifft diese Fehlerbehandlungsentscheidung, indem der eingehende Broadcast-/Multicast-Datenverkehr ständig überwacht wird, um zu bestimmen, welcher Knoten den meisten eingehenden Datenverkehr hat. In diesem Fehlerfall führt das ztC Edge-System ein Failover des VM-Netzwerks auf den Knoten mit dem meisten eingehenden Datenverkehr aus, falls die VM nicht bereits auf diesem Knoten aktiv ist. Diese Fehlererkennungsfunktion muss nicht durch den Benutzer konfiguriert werden, da die Entscheidung auf dem Datenverkehr basiert, der normalerweise in jedem System auftritt.

Verwandte Themen

Netzwerkarchitektur

Systemnutzungseinschränkungen

Beachten Sie die Einschränkungen für die Systemnutzung, die in den folgenden Themen beschrieben werden:

- QEMU
- Zugriff auf das Host-Betriebssystem

QEMU

Stratus ztC Edge-Systeme unterstützen den Open-Source-Hypervisor QEMU („Quick EMUlator“), der eine Hardwarevirtualisierung ausführt. Bei der Verwendung als Virtualisierungstool führt QEMU den Gastcode direkt auf der Host-CPU aus und erzielt so eine bessere Leistung.

ztC Edge-Benutzer sollten keine Änderungen am QEMU-Virtualisierungsmodul oder an der Konfiguration vornehmen.

Zugriff auf das Host-Betriebssystem

Nachdem Sie die ztC Edge-Bereitstellung abgeschlossen haben, können Sie lokal über die physische Konsole der PM oder remote mit einem SSH-Client (Secure Shell) auf das Hostbetriebssystem (CentOS) zugreifen.

Wenn Sie mit einem SSH-Client beim Host-Betriebssystem anmelden, verwenden Sie die Verwaltungs-IP-Adresse, die während der Bereitstellung angegeben wurde (oder vom DHCP-Server bereitgestellt wurde, falls die Schnittstelle bei der Bereitstellung für DHCP konfiguriert wurde). Bei Bedarf können Sie die Verwaltungs-IP-Adresse für jede PM wie in diesem Thema beschrieben herausfinden.

Achtung: Aktualisieren Sie das CentOS-Hostbetriebssystem auf dem ztC Edge-System nicht aus irgendeiner anderen Quelle als Stratus. Verwenden Sie nur die CentOS-Version, die mit der Stratus Redundant Linux-Software installiert wurde.

Hinweis: Um sicherzustellen, dass administrative Befehle ordnungsgemäß ausgeführt werden können, melden Sie sich bei der physischen Konsole oder der IP-Adresse der primären PM an (falls Sie nicht unbedingt Komponenten auf der sekundären PM ausführen müssen). Stellen Sie keine Verbindung zur IP-Adresse des Systems her, da sie von PM zu PM wandern kann.

Hinweis: Das Standardkennwort für das Root-Konto ist **KeepRunning**. Aus Sicherheitsgründen sollten Sie das `root`-Kennwort auf jeder PM so bald wie möglich ändern. Wenn Sie sich zum ersten Mal als root bei einer PM anmelden, werden Sie vom System aufgefordert, das Kennwort zu ändern. Wenn Sie das Kennwort später erneut ändern möchten, führen Sie auf jeder PM den Befehl `passwd` aus.

Informationen zur Verwendung von Drittanbietertools unter CentOS finden Sie unter Verwaltungstools von Drittanbietern.

So finden Sie die IP-Adresse jeder PM in der ztC Console heraus

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **System** auf **IP-Konfiguration**.
3. Notieren Sie die **IP-Adresse** jeder PM – **Knoten0** und **Knoten1**.

4. Klicken Sie im linken Navigationsbereich auf **Physische Maschinen**, um die Seite **Physische Maschinen** zu öffnen.
5. Notieren Sie sich, welche PM der primäre Knoten des Systems ist; dies wird als **Knoten*n* (primär)** angezeigt. Melden Sie sich bei der IP-Adresse des primären Knotens an, um sicherzustellen, dass administrative Befehle ordnungsgemäß ausgeführt werden können.

So greifen Sie von einem Windows-basierten System auf das Host-Betriebssystem zu

Sie können PuTTY herunterladen und verwenden, eine Suite von Open-Source-SSH-Clients:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Der `putty.exe`-Client ermöglicht es Ihnen, auf eine Shell zuzugreifen, um Programme von der Befehlszeile des Host-Betriebssystems auszuführen. PuTTY enthält auch das Befehlszeilen-Utility `pscp.exe`, mit dem Sie Dateien sicher von einem Remotesystem an das Host-Betriebssystem übertragen können.

Wenn Sie einen SCP-Client (Secure Copy) mit einer grafischen Benutzeroberfläche bevorzugen, können Sie auch das Open-Source-Utility WinSCP verwenden:

http://winscp.net/eng/index.php

So greifen Sie von einem Linux-basierten System auf das Host-Betriebssystem zu

Bei vielen Linux- und UNIX-basierten Systemen sind SSH-Utilitys bereits standardmäßig installiert und aktiviert. Informationen zur Verwendung dieser Utilitys finden Sie unter „ssh(1)“ und „scp(1)“.

2

Kapitel 2: Erste Schritte

In den folgenden Themen werden die ztC Edge-Planung, Bereitstellung und Aufgaben nach der Bereitstellung beschrieben:

- Planung
- Bereitstellung
- Aufgaben nach der Bereitstellung

Planung

In den folgenden Themen finden Sie Informationen zur Planung Ihrer Systemkonfiguration.

- Sicherheitsmaßnahmen
- Übersicht über die Systemanforderungen
- Platzanforderungen
- Systemspezifikationen: ztC Edge 110i-Systeme
- Systemspezifikationen: ztC Edge 100i-Systeme
- DIN-Schienen- und Wandhalterungsmontage: ztC Edge 110i-Systeme
- DIN-Schienen- und Wandhalterungsmontage: ztC Edge 100i-Systeme
- Produktkonformität
- Allgemeine Netzwerkanforderungen und -konfigurationen
- Anforderungen für Unternehmens- und Verwaltungsnetzwerke
- Anforderungen für A-Link- und private Netzwerke

- Anforderungen für die ztC Console
- Kompatible Internetbrowser
- Anforderungen und Überlegungen für die Stromversorgung
- Erstellen einer ALSR-Konfiguration (falls für Ihre Konfiguration zutreffend)

Nachdem Sie die Systemkonfiguration geplant haben, fahren Sie mit der Bereitstellung fort.

Sicherheitsmaßnahmen

Machen Sie sich mit den folgenden wichtigen Sicherheitshinweisen vertraut, bevor Sie anfangen.

Warnung: Vergewissern Sie sich, dass die Stromquelle über die richtige Spannung verfügt, bevor Sie das Produkt anschließen.

Warnung: Wartungsarbeiten sind von qualifizierten Servicemitarbeitern durchzuführen; es gibt keine Komponenten, die vom Benutzer gewartet werden können.

Warnung: Es besteht Explosionsgefahr, wenn der Akku durch ein ungeeignetes Modell ersetzt wird. Entsorgen Sie verbrauchte Akkus anweisungsgemäß.
IL Y A RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACEE PER UNE BATTERIE DE TYPE INCORRECT. METTRE AU REBUT LES BATTERIES USAGEES CONFORMEMENT AUX INSTRUCTIONS

Warnung: Heiße Oberfläche - nicht berühren.

Die folgenden Informationen gelten nur für ztC Edge 110i-Systeme:

- Diese Geräte sind „offene" Geräte, die in einem Gehäuse installiert werden müssen, das für die Umgebung geeignet ist und dessen innerer Bereich nur mithilfe eines Werkzeugs zu öffnen ist.
- GEEIGNET FÜR DIE VERWENDUNG AN GEFÄHRLICHEN STANDORTEN DER KLASSE I, ABSCHNITT 2, GRUPPEN A, B, C UND D ODER AN UNGEFÄHRLICHEN STANDORTEN.

Warnung: EXPLOSIONSGEFAHR - GERÄTE NICHT TRENNEN, WÄHREND DER SCHALTKREIS UNTER SPANNUNG STEHT, BZW. NUR, WENN DER BEREICH NACHWEISLICH FREI VON ENTFLAMMBAREN KONZENTRATIONEN IST.

Übersicht über die Systemanforderungen

ztC Edge-Systemhardware -Spezifikationen und -Anforderungen sind nachstehend zusammengefasst, für jeden PM-Typ. Empfehlungen zur Platzierung von PMs finden Sie unter Platzanforderungen.

Informationen zu Gastbetriebssystemen finden Sie unter Getestete Gastbetriebssysteme.

Systemhardware

Funktion	ztC Edge 100i PM	ztC Edge 110i PM
RAM (physischer Arbeitsspeicher)	32 GB	32 GB oder 64 GB
Speicherplatz	512-GB-SSD, auf der ungefähr 475 GB für VMs verfügbar sind.	2-TB-SSD, auf der ungefähr 1,9 TB für VMs verfügbar sind.
Netzwerkports	Jede PM hat vier 1-Gbit/s-Ethernet-Ports. Bei einem System, das für zwei Knoten lizenziert ist, verwenden Sie: • Blau (•) für ein kombiniertes A-Link- und priv0-Netzwerk (privates Netzwerk) • Gelb (• •) für ein zweites, dediziertes A-Link-Netzwerk Bei einem System, das für zwei Knoten oder für einen Knoten lizenziert ist, verwenden Sie: • **P1** für ein kombiniertes Unternehmens- und Verwaltungsnetzwerk • **P2** für ein optionales Unternehmensnetzwerk	Jede PM hat acht Netzwerkports: sechs 1-Gbit/s-Ports (**P1** bis **P6**) auf der Vorderseite und zwei 10-Gbit/s-Ports (**A1** und **A2**) auf der Rückseite. Bei einem System, das für zwei Knoten lizenziert ist, verwenden Sie: • **A1** (gelbe Kennzeichnung), für A-Link 1 • **A2** (blaue Kennzeichnung) für priv0 Bei einem System, das für zwei Knoten oder für einen Knoten lizenziert ist, verwenden Sie: • **P1** für ein kombiniertes Unternehmens- und Verwaltungsnetzwerk. • **P2** bis **P6** für optionale

Funktion	ztC Edge 100i PM	ztC Edge 110i PM
		Unternehmensnetzwerke.
	Hinweis: **P1** wird manchmal als Netzwerk0 oder ibiz0 bezeichnet; **P2** wird manchmal als Netzwerk1 oder ibiz1 bezeichnet; **P3** wird manchmal als Netzwerk3 oder ibiz3 bezeichnet usw.	

Das System bietet auch Lights-out-Unterstützung für Intel® Active Management Technology (AMT); über den Port **P1** jeder PM haben Sie Zugriff darauf.

Für ALSR-Konfigurationen gelten andere Netzwerkanforderungen. Weitere Informationen finden Sie unter Erfüllen der Netzwerkanforderungen.

Weitere Informationen finden Sie unter Netzwerkarchitektur, A-Link- und private Netzwerke und Unternehmens- und Verwaltungsnetzwerke.

IP-Adressen

Jedes ztC Edge-System braucht eine statische IPv4-IP-Adresse, die der Verwendung durch die Verwaltungssoftware zugewiesen ist. Fragen Sie Ihren IT-Netzwerkadministrator nach IP-Adressen für primäre und sekundäre DNS-Server sowie Informationen zu Gateway und Subnetzmaske. Weitere Informationen finden Sie unter Beziehen der System-IP-Informationen.

Ports

ztC Edge-Systeme verwenden Port 443 in der lokalen Firewall für die HTTPS-Kommunikation, Port 22 für ssh und 5900-59*nn* für jeden aktiven VNC, der den einzelnen VMs zugeordnet ist. Firewalls müssen den Datenverkehr durch die entsprechenden Ports zulassen. Firewalls müssen zulassen, dass VMs über UDP-Port 4557 mit Quorumdienstcomputern kommunizieren. Weitere Informationen zu TCP- und UDP-Ports finden Sie in der Knowledge Base im Artikel *TCP and UDP ports used by ztC Edge* (KB-9357). Siehe Zugriff auf Artikel in der Knowledge Base.

Verwandte Themen

Wichtige Überlegungen für physische Maschinen und virtuelle Maschinen

Empfehlungen und Einschränkungen für virtuelle Maschinen

Planen von VM-Ressourcen

Konfigurieren der IP-Einstellungen

Platzanforderungen

Damit der Installationsstandort alle Anforderungen eines ztC Edge 100i- oder 110i-System hinsichtlich Ausstattung, Belüftung und Platz erfüllt, beachten Sie die folgenden Empfehlungen.

Platzanforderungen für Knoten, die auf einem Tisch aufgestellt werden:

- Mindestens 5,08 cm Platz auf der linken und rechten Seite eines Knotens
- Mindestens 7,62 cm Platz über einem Knoten
- Mindestens 12,7 cm Platz vor und hinter einem Knoten
- Mindestens 5,08 cm Platz zwischen zwei Knoten

Platzanforderungen für Knoten, die an einer DIN-Schiene angebracht werden:

- Mindestens 5,08 cm Platz auf der linken und rechten Seite eines Knotens
- Mindestens 12,7 cm Platz über und unter einem Knoten
- Mindestens 5,08 cm Platz zwischen zwei Knoten

Weitere Empfehlungen zum Installationsort:

- Knoten können entweder horizontal (auf einer ebenen Fläche liegend) oder vertikal (an einer Wand) installiert werden. Bei der vertikalen Installation muss die Seite mit dem Stratus-Logo nach oben weisen.
- Damit die Kabel des Systems nicht beschädigt werden, dürfen sie nicht mit einem Kurvenradius von weniger als 5,08 cm verlegt werden.
- Platzieren Sie keine Geräte, die Wärme erzeugen, unter dem Knoten.
- Achten Sie darauf, die zulässige Betriebstemperatur des Knotens nicht zu unter- oder überschreiten.
- Jeder Knoten braucht für die optimale Wärmeableitung einen Luftstrom von mindestens 100 LFM (0,51 m/s) über dem Kühlkörper.

Beachten Sie zusätzlich zu den genannten Empfehlungen die spezifischen Anforderungen Ihres Installationsorts. Wenn Sie weitere Beratung brauchen, wenden Sie sich an Ihren autorisierten Stratus-Servicemitarbeiter.

Systemspezifikationen: ztC Edge 110i-Systeme

In der folgenden Tabelle sind Systemspezifikationen aufgeführt.

Komponente	**Beschreibung**
CPU	
CPU	Intel Core I7-8700T Prozessor, 35 W
Systemarbeitsspeicher	2 x 260 Pin unbuffered DDR4-2400 MHz SO-DIMM-Sockel, 32 GB oder 64 GB insgesamt
I/O	
Display	1 x HDMI 1 x DVI-Port
Ethernet	6 x 10/100/1000 Ethernet-Ports 2 x 10 Gb Ethernet-Ports
USB-Ports	2 x USB 3.2, Gen 2 (10 Gbit/s) (früher als USB 3.1, Gen 2 bezeichnet) 2 x USB 3.2, Gen 1 (5 Gbit/s) (früher als USB 3.1, Gen 1 bezeichnet)
Speicher	1 SATA SSD, 2 TB
Anzeigen	1 grüne LED als Anzeige für den PWR-Status (Betrieb) 1 grüne LED als Anzeige für den SYS-Status (System) 1 grüne LED als Anzeige für SSD-Aktivität
Schalter	1 Ein/Aus-Schalter 1 Reset-Schalter

System	
Netzteil	24 VDC Eingang Optionales AC-Netzteil, 100 bis 240 VAC, 50/60 Hz, 5 A
Typische Leistung und BTU	62 W, 213 BTU/hr
Umgebung	
Betriebstemperatur	-20 °C bis 55 °C
Lagertemperatur	-40 °C bis 80 °C
Luftfeuchtigkeit	10 % bis 95 % (nicht kondensierend)
Stoß	IEC 60068-2-27 (mit SSD: 25 G bei Wandmontage, Halbsinus, 11 ms Dauer)
Vibrationsfestigkeit	IEC 60068-2-64 (mit SSD: 3 Grms STD, zufällig, 5-500 Hz,1 h/Achse)
Abmessungen	
Gewicht	5,2 kg ohne Karton 6,2 kg mit Karton
Höhe	86,9 mm
Breite	280 mm
Tiefe	210 mm

Systemspezifikationen: ztC Edge 100i-Systeme

In der folgenden Tabelle sind Systemspezifikationen aufgeführt.

Komponente	**Beschreibung**
CPU	

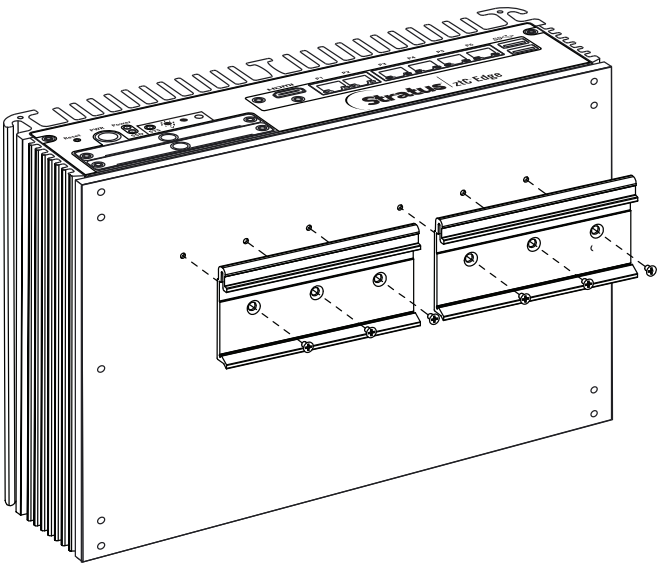
CPU	Intel Core I7-6700TE Prozessor, 35 W
Systemarbeitsspeicher	2 x 260 Pin unbuffered DDR4-2400 MHz SO-DIMM-Sockel, 32 GB
I/O	
Display	1 x HDMI 1 x DVI-Port
Ethernet	4 x 10/100/1000 Ethernet-Ports
USB-Ports	2 x USB 2.0 6 x USB 3.2, Gen 1 (5 Gbit/s) (früher als USB 3.1, Gen 1 bezeichnet)
Speicher	1 SATA SSD, 512 GB
Anzeigen	1 grüne LED als Anzeige für den PWR-Status (Betrieb) 1 grüne LED als Anzeige für den SYS-Status (System) 1 grüne LED als Anzeige für SSD-Aktivität
Schalter	1 Ein/Aus-Schalter 1 Reset-Schalter
System	
Netzteil	9-36 VDC Eingang Optionales AC-Netzteil, 100 bis 240 VAC, 50/60 Hz, 5 A
Typische Leistung und BTU	41 W, 140 BTU/hr
Umgebung	
Betriebstemperatur	-40 °C bis 60 °C
Lagertemperatur	-40 °C bis 80 °C

Luftfeuchtigkeit	10 % bis 95 % (nicht kondensierend)
Stoß	IEC 60068-2-27 (mit SSD: 50 G bei Wandmontage, Halbsinus, 11 ms Dauer)
Vibrationsfestigkeit	IEC 60068-2-64 (mit SSD: 3 Grms STD, zufällig, 5-500 Hz,1 h/Achse)
Abmessungen	
Gewicht	4,8 kg ohne Karton 5,6 kg mit Karton
Höhe	75 mm
Breite	280 mm
Tiefe	190 mm

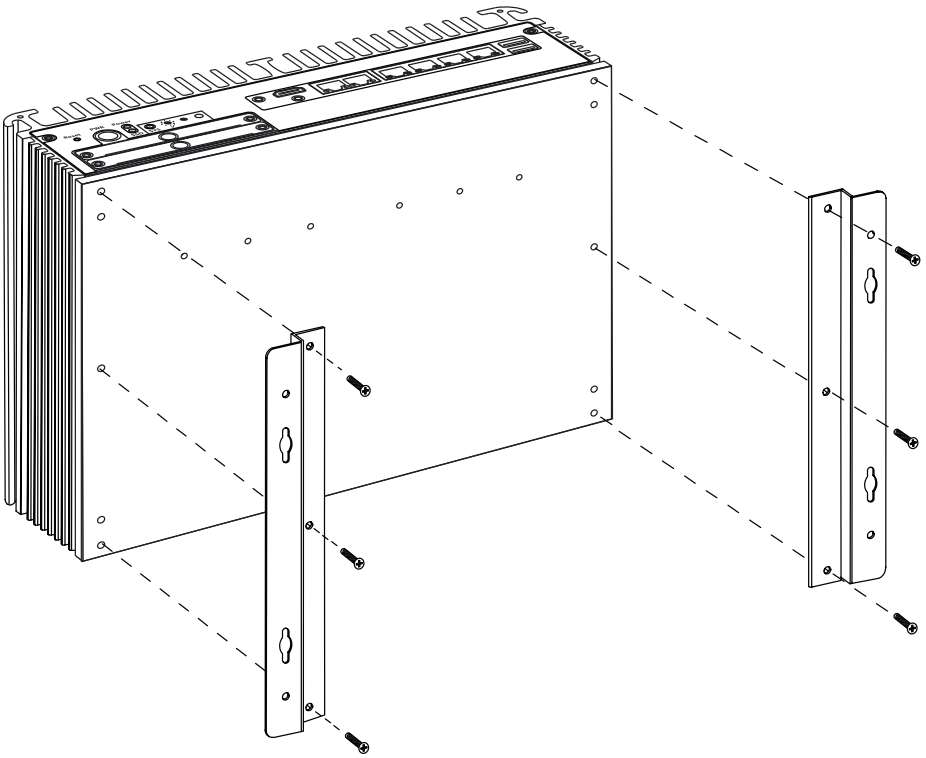
DIN-Schienen- und Wandhalterungsmontage: ztC Edge 110i-Systeme

Hinweis: Achten Sie bei der Anbringung der DIN-Schiene oder des Wandmontage-Sets an einem ztC Edge-Knoten darauf, dass die Seite mit dem Stratus-Logo nach oben zeigt.

Verwenden Sie zur Anbringung des DIN-Schienenmontage-Sets die sechs M3-Flachkopfschrauben aus dem Zubehörkarton.



Um das Wandmontage-Set anzubringen, entfernen Sie die sechs M3-Flachkopfschrauben (12 mm) auf der Unterseite des Knotens (drei Schrauben auf jeder Seite). Verwenden Sie diese sechs Schrauben, um das Wandmontage-Set anzubringen.



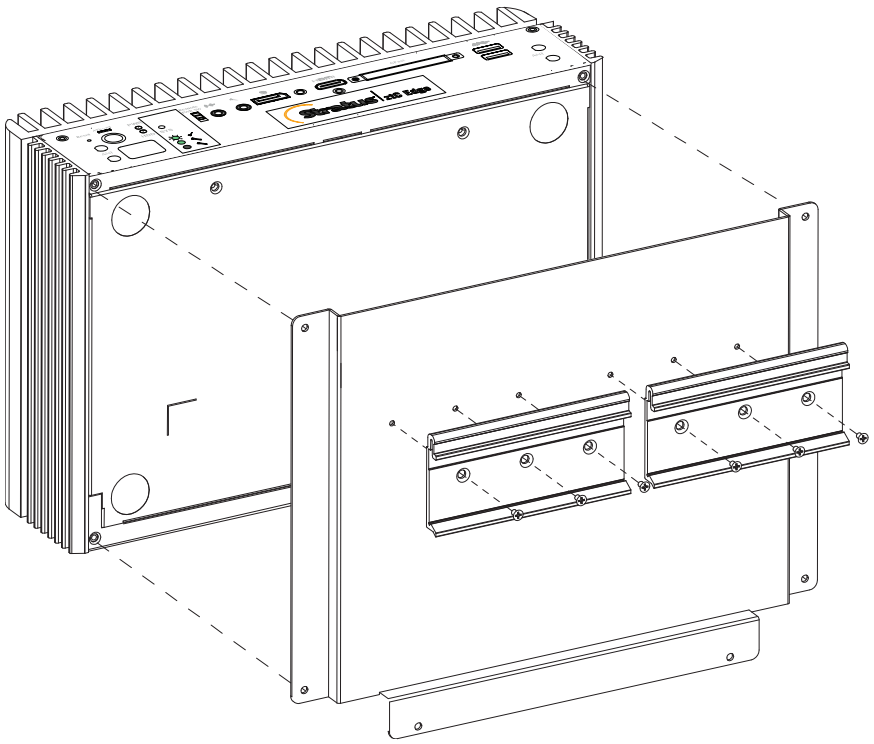
Hinweis: Wenn Sie die Schrauben in einer Gipskartonwand anbringen, verwenden Sie geeignete Hohlraumdübel, damit die Einheit nicht durch den Zug des Kabels und Netzsteckers von der Wand abgezogen wird. Verwenden Sie einen maximalen Schraubendurchmesser von 4,2 mm mit einem Mindestdurchmesser des Schraubenkopfes von 5,5 mm.

DIN-Schienen- und Wandhalterungsmontage: ztC Edge 100i-Systeme

Hinweis: Achten Sie bei der Anbringung der DIN-Schiene oder des Wandmontage-Sets an einem ztC Edge-Knoten darauf, dass die Seite mit dem Stratus-Logo nach oben zeigt.

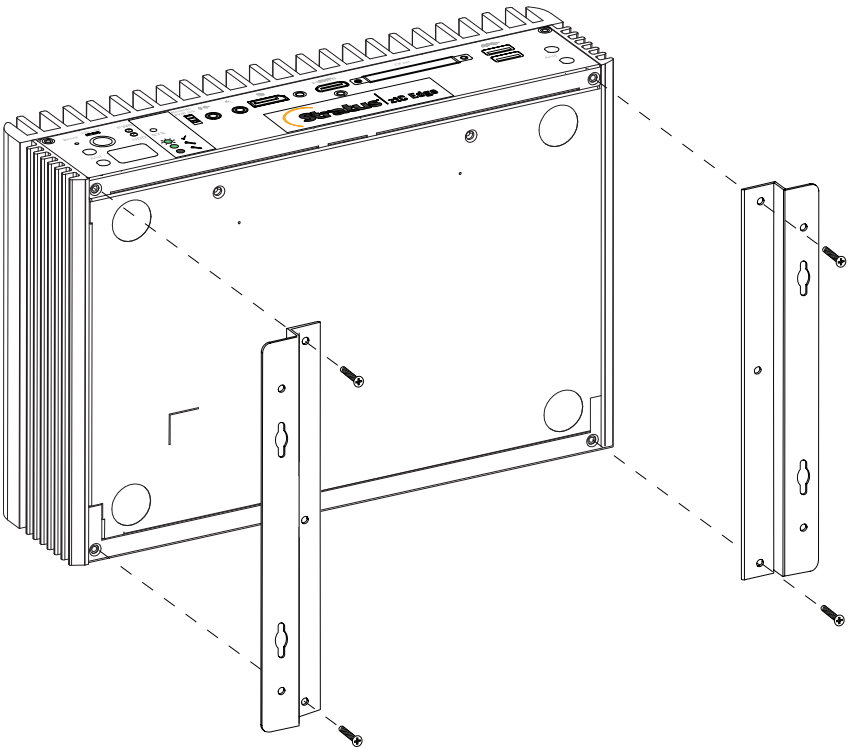
So befestigen Sie das DIN-Schienenmontage-Set:

- Entfernen Sie die vier M3-Flachkopfschrauben (6 mm) auf der Unterseite des Knotens (zwei Schrauben auf jeder Seite).
- Verwenden Sie die vier M3-Rundkopfschrauben (6 mm) aus dem Zubehörkarton, um die DIN-Schienen-Montageplatte am Knoten zu befestigen.
- Verwenden Sie die sechs M3-Flachkopfschrauben (6 mm) aus dem Zubehörkarton, um die beiden DIN-Schienen-Montagehalterungen an der DIN-Schienen-Montageplatte zu befestigen.



So befestigen Sie das Wandmontage-Set:

- Entfernen Sie die vier M3-Flachkopfschrauben (6 mm) auf der Unterseite des Knotens (zwei Schrauben auf jeder Seite).
- Verwenden Sie die vier M3-Rundkopfschrauben (6 mm) aus dem Zubehörkarton, um die Wandmontagehalterungen am Knoten zu befestigen.



Hinweis: Wenn Sie die Einheit an einer Gipskartonwand oder ähnlichem anbringen, verwenden Sie geeignete Hohlraumdübel, damit die Einheit nicht durch den dauernden Zug des Kabels von der Wand abgezogen wird. Verwenden Sie Schrauben mit einem Mindestdurchmesser von 3,5 mm, einer Mindestlänge von 38,1 mm und einem Mindestdurchmesser des Schraubenkopfes von 5,5 mm. Achten Sie darauf, dass die Schrauben zu den ausgewählten Hohlraumdübeln passen.

Produktkonformität

Informationen zu Konformität von ztC Edge 100i- und ztC Edge 110i-Systemen finden Sie auf dieser Website:

https://stratadoc.stratus.com/compliance_info/Compliance_Information_for_Stratus_Products.htm

Allgemeine Netzwerkanforderungen und -konfigurationen

Hinweis: Für ALSR-Netzwerke gelten einige zusätzliche und andere Netzwerkanforderungen und Empfehlungen. Lesen Sie zusätzlich zu den folgenden Informationen auch Erstellen einer ALSR-Konfiguration.

Bevor Sie ein ztC Edge-System bereitstellen, sorgen Sie dafür, dass Ihr Netzwerk die folgenden Anforderungen erfüllt:

- ztC Edge-Systeme verwenden vollständigen IPv4- und IPv6-Protokollzugriff einschließlich IPv6-Multicast. Jegliche Einschränkungen dieses Datenverkehrs können eine erfolgreiche Bereitstellung verhindern oder die Verfügbarkeit eines laufenden ztC Edge-Systems beeinträchtigen.

In den folgenden Themen finden Sie spezifische Anforderungen für die einzelnen Netzwerktypen:

- Anforderungen für A-Link- und private Netzwerke
- Anforderungen für Unternehmens- und Verwaltungsnetzwerke

Anforderungen für Unternehmens- und Verwaltungsnetzwerke

Für Unternehmens- und Verwaltungsnetzwerke gelten die folgenden Anforderungen:

- Die Netzwerke verwenden die verbindungslokale IPv6-Adressierung.
- Die Netzwerke unterstützen einen MTU-Wert von bis zu 9000.
- Die Netzwerke unterstützen weder Bonding noch VLAN-Trunking.
- Virtuelle Maschinen (VMs) können IPv4, IPv6 und andere Ethernet-Protokolle verwenden.
- Alle Unternehmensnetzwerke können für den IPv6-Hostzugriff verwendet werden, wenn an Ihrem Standort SLAAC oder DHCPv6 aktiviert ist.
- Verwenden Sie für den Zugriff auf die ztC Console ibiz0, welches die IPv4-Adresse ist, die zur primären Verwaltungs-PM migriert (PM= physische Maschine). Jede PM hat auch ihre eigene ibiz0-IPv4-Adresse im Verwaltungsnetzwerk.
- Jede PM benötigt mindestens ein Unternehmensnetzwerk (speziell das Verwaltungsnetzwerk).

Um sicherzustellen, dass der Ethernet-Datenverkehr ungehindert zu und von den VMs jeder PM fließen kann:

- Die Switchports, die mit Unternehmensnetzwerken verbunden sind, dürfen keine ARP-Pakete filtern, dies gilt auch für überflüssige ARP-Pakete. Ein ztC Edge-System sendet überflüssige ARP-Pakete für Gast-VMs, um Ethernet-Switches dazu zu bringen, ihre Portweiterleitungstabellen zu aktualisieren, um VM-Datenverkehr an den richtigen physischen Ethernet-Port der richtigen PM zu leiten.
- Die mit Unternehmensnetzwerken verbundenen Switchports müssen Layer2-Multicasts (Adresse: 01:E0:09:05:00:02) mit Ethernettyp 0x8807 zulassen.

- Wenn Sie RHEL- oder CentOS-Gäste so konfigurieren, dass sie mehrere NICs in demselben Subnetz haben, kann es wegen des asymmetrischen Routings zu Problemen mit der Konnektivität des Gastnetzwerks kommen. Um dies zu vermeiden, bearbeiten Sie die Datei **/etc/sysctl.conf** auf der Gast-VM, sodass sie die folgenden Zeilen enthält, speichern die Datei und starten die VM neu.
  - `net.ipv4.conf.default.rp_filter = 2`
  - `net.ipv4.conf.all.rp_filter = 2`
- Geben Sie nicht den Befehl `ifdown` vom Hostbetriebssystem einer PM ein, um die Unternehmensnetzwerkverbindung einer VM (ibiz*x*) vorübergehend auszuschalten. Damit wird die physische Schnittstelle von der Bridge getrennt, sodass die VM nicht mehr über das Netzwerk zu erreichen ist. Verwenden Sie stattdessen den Befehl `ifconfig down`.
- Die mit Unternehmensnetzwerken verbundenen Switches dürfen keine Sicherheitsfunktionen für MAC-Adressen aktivieren, die das Verschieben einer MAC-Adresse von einer Unternehmensverbindung zur entsprechenden Unternehmensverbindung auf der anderen PM verhindern würden.
- Zur optimalen Failoverantwort konfigurieren Sie alle Switches, die mit Ihrem System verbunden sind, so, dass ihre MAC-Ablaufzeiten weniger als eine Sekunde betragen.

Falls diese Anforderungen nicht erfüllt werden oder der Switch seine Weiterleitungstabelle nicht korrekt aktualisiert, wenn eine VM von einer ztC Edge-PM zu einer anderen migriert wird, kann es bei der VM zu einem Blackout kommen, bei dem der Netzwerkdatenverkehr nicht korrekt an die und von der VM geleitet wird.

Verwandte Themen

Netzwerkarchitektur

Unternehmens- und Verwaltungsnetzwerke

Anforderungen für A-Link- und private Netzwerke

Für A-Link- und private Netzwerke gelten die folgenden Anforderungen:

- Die Netzwerke verwenden die verbindungslokale IPv6-Adressierung.
- Alle A-Link- und privaten Netzwerke auf einer PM in einem ztC Edge-System müssen sich in derselben L2-Broadcastdomäne befinden wie die entsprechenden Links auf der anderen physischen Maschine (PM), ohne Protokollfilterung.
- Ethernet-Pakete, die zwischen zwei PMs eines Systems gesendet werden, dürfen nicht behindert oder eingeschränkt werden. Stellen Sie sicher, dass sie nicht von einer L3-Netzwerkinfrastruktur geroutet oder geswitcht werden.
- Die Geschwindigkeit von A-Link-Netzwerken sollte mindestens so hoch wie die Geschwindigkeit von Unternehmens- oder Verwaltungsnetzwerken sein.
- Der Netzwerkdatenverkehr für die Speicherreplikation zwischen PMs wird über A-Link-Netzwerke gesendet.
- Mit privaten Netzwerken sind keine anderen Hosts als die ztC Edge-Endpunkte verbunden.

Verwandte Themen

A-Link- und private Netzwerke

Anforderungen für die ztC Console

Die ztC Console ermöglicht die browsergestützte Remoteverwaltung des ztC Edge-Systems, seiner physischen Maschinen (PMs) und seiner virtuellen Maschinen (VMs).

- Der Computer benötigt Zugriff auf das Subnetz, in dem sich das ztC Edge-Verwaltungsnetzwerk befindet (das am Netzwerk-Port **P1** aktiviert ist.
- Verwenden Sie einen unterstützten Browser. Siehe Kompatible Internetbrowser.

Weitere Informationen finden Sie unter Verwenden der ztC Console.

Kompatible Internetbrowser

Die Verbindung mit der ztC Console erfolgt über einen Browser. Verwenden Sie nur Browser, die mit ztC Edge-Systemen kompatibel sind. Wenn Sie keinen kompatiblen Browser verwenden, kann es zu Darstellungsproblemen kommen, möglicherweise werden auch einige Assistenten ausgelassen.

Die folgenden Browser sind mit ztC Edge-Systemen kompatibel.

Kompatible Browser	Version
Microsoft Internet Explorer™	11.0.648 oder höher
Microsoft Edge	42.17134 oder höher
Mozilla® Firefox®	65.0 oder höher
Google® Chrome™	73.0 oder höher

Anforderungen und Überlegungen für die Stromversorgung

Um die bestmögliche Verfügbarkeit zu gewährleisten, empfiehlt Stratus dringend, dass die fehlertolerante (FT) ztC Edge-Software auf physischen Maschinen (PMs), auch als Knoten bezeichnet, ausgeführt wird, die von redundanten Netzteilen mit Strom versorgt werden. Außerdem sollte jedes PM-Netzteil an eine separate Stromquelle angeschlossen sein.

Siehe Anschließen der Stromversorgung mit Beispielabbildungen von Stromversorgungskonfigurationen.

Bereitstellung

Bei der erstmaligen Bereitstellung des System:

> **Hinweis**: Wenn Sie bereits ein System bereitgestellt und konfiguriert haben und es für die Bereitstellung an einer neuen Site vorbereiten wollen, lesen Sie Erneutes Bereitstellen eines ztC Edge-Systems.

1. Lesen Sie noch einmal die Informationen zur Netzwerkverkabelung. Nehmen Sie gegebenenfalls erforderliche Änderungen am Netzwerk vor. Siehe Verbinden von Ethernet-Kabeln.
2. Stellen Sie das System bereit. Siehe Bereitstellen des Systems.

Nach Abschluss der Bereitstellung lesen Sie Aufgaben nach der Bereitstellung.

Verwandte Themen

Aktualisieren der Stratus Redundant Linux-Software

Anschließen der Stromversorgung

Um die Stromversorgung anzuschließen, konfigurieren Sie ein ztC Edge-System, das für zwei Knoten lizenziert ist, mit redundanten Netzteilen, die an separate Stromquellen angeschlossen sind. Sie können optional zwei unterbrechungsfrei Stromversorgungen (USV) anschließen wie unten abgebildet.

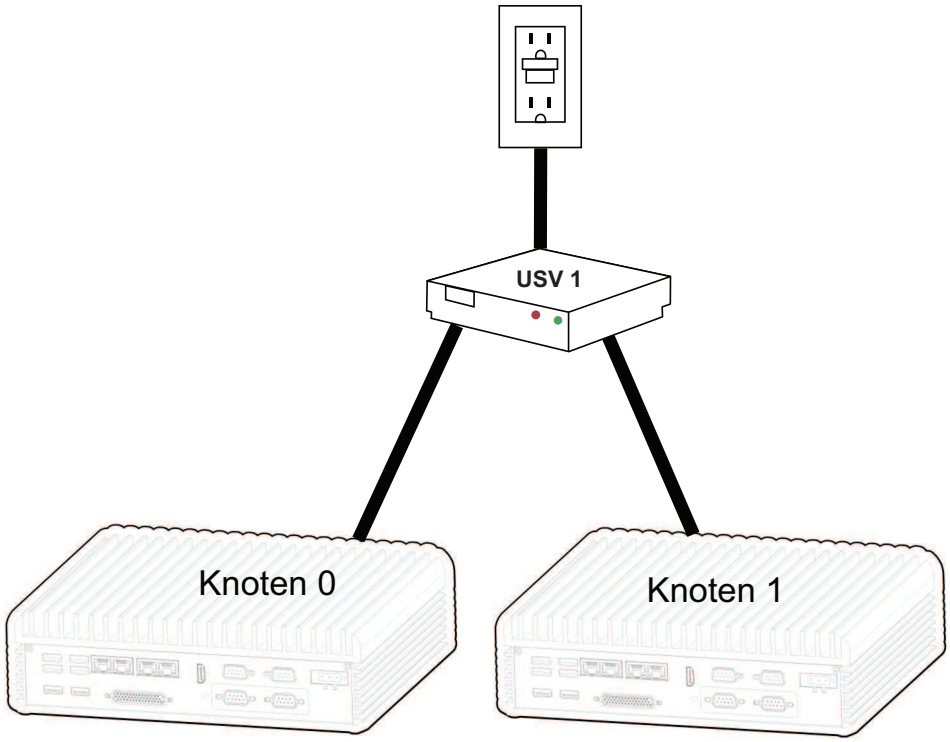
Kehren Sie nach dem Anschließen der Stromversorgung zu Bereitstellen des Systems zurück.

USV (optional)

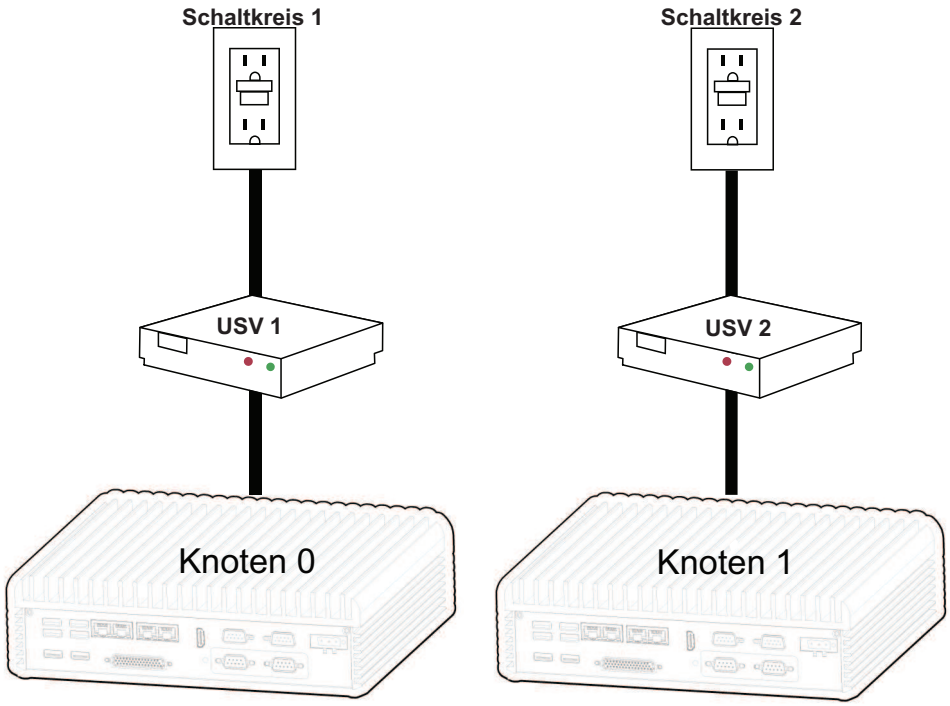
Die Abbildungen zeigen, wie Sie eine oder zwei optionale USV-Einheiten an ein ztC Edge-System anschließen, das für zwei Knoten lizenziert ist.

Hinweis: Stratus empfiehlt die Verwendung von zwei USV-Einheiten, die an separate und unabhängige Stromquellen angeschlossen sind. Bei Verwendung von zwei Stromquellen wird das System auch dann mit Strom versorgt, wenn eine der Einheiten ausfällt.

Einzelne USV:



Zwei USVs:



Verwandte Themen

Anforderungen und Überlegungen für die Stromversorgung

Bereitstellen des Systems

In diesem Thema wird die Bereitstellung eines ztC Edge-Systems beschrieben. Dies ergänzt die Informationen in der Bereitstellungsanleitung für Ihr System. (Bei einem System, das für einen Knoten lizenziert ist: Wenn Ihr System bereits läuft und Sie einen zweiten Knoten hinzufügen möchten, lesen Sie Hinzufügen eines Knotens zu einem Einzelknotensystem.)

So stellen Sie ein System bereit

1. Schließen Sie Tastatur, Monitor und Stromversorgung an einen Knoten an (Schritt 1 in der Bereitstellungsanleitung für Ihr System). Sie können wahlweise eine oder zwei unterbrechungsfreie Stromversorgungen (USV) anschließen. Weitere Informationen finden Sie unter Anschließen der Stromversorgung.

2. Der Knoten wird automatisch eingeschaltet. Sollte dies nicht geschehen, drücken Sie die Ein/Aus-Taste (Schritt 2 in der Bereitstellungsanleitung für Ihr System).

   Wenn auf dem Monitor Anweisungen angezeigt werden, führen Sie einen der folgenden Schritte aus:

   - Bei einem System, das für zwei Knoten lizenziert ist, drücken Sie die Taste **[1]**, um den ersten Knoten bereitzustellen.
   - Bei einem System, das für einen Knoten lizenziert ist, drücken Sie die Taste **[1]**, um den einzelnen Knoten bereitzustellen.
   - Bei einem System, das für Sie vorkonfiguriert wurde, drücken Sie die Taste **[c]**, um mit der erneuten Bereitstellung des Systems fortzufahren.

     Die Option **[c]** wird nur angezeigt, wenn ein Systemintegrator das System bereits für Sie konfiguriert und anschließend die Netzwerkeinstellungen für die erneute Bereitstellung an Ihrem Standort gelöscht hat. Wenn Sie ein System erneut bereitstellen, bleiben die vorkonfigurierte Auswahl von ein oder zwei Knoten, VMs und andere Systemeinstellungen erhalten.

3. Es wird ein Fenster eingeblendet, in dem Sie aufgefordert werden, eine Tastaturbelegung auszuwählen. Verwenden Sie die **Tabulatortaste**, Pfeiltasten oder die **Esc**-Taste, um eine Auswahl zu treffen:

   - **Germany - map = DE**
   - **Japan - map = JP106**
   - **USA - map = US** (Standardeinstellung)

   Navigieren Sie mithilfe der **Tabulatortaste** zu **OK** und drücken Sie die **Eingabetaste**.

   > **Hinweis**: Sie können die Tastaturbelegung direkt nach der ersten Bereitstellung auswählen oder ändern. Weitere Informationen finden Sie unter Tastaturlayout.

4. Eine Meldung auf dem Bildschirm fordert Sie auf, die Methode zum Konfigurieren der Netzwerkadresse dieses Knotens auszuwählen. Verwenden Sie die **Tabulatortaste**, Pfeiltasten oder die **Esc**-Taste, um eine Auswahl zu treffen:

   - **Automatic configuration via DHCP** (Standardeinstellung) - Wählen Sie diese Methode aus, um P1 als dynamische IP-Konfiguration zu konfigurieren.

- **Manual configuration (Static Address)** - Wählen Sie diese Methode aus, um IP-Adressen für P1 anzugeben. Es wird ein Dialogfeld angezeigt, in dem Sie diese Werte eingeben können, die Sie von Ihrem Netzwerkadministrator erhalten (möglicherweise haben Sie diese Adressen auch im Abschnitt **Vom Benutzer bereitgestellte Komponenten** in der Bereitstellungsanleitung für Ihr System notiert):
  - IP-Adresse für diesen Knoten
  - Subnetzmaske für diesen Knoten
  - Standardgateway (optional)

  Wenn Sie ungültige Informationen eingeben, wird der Bildschirm solange angezeigt, bis Sie gültige Informationen eingeben.

Navigieren Sie mithilfe der **Tabulatortaste** zu **OK** (oder **Back** (Zurück)) und drücken Sie die **Eingabetaste**.

5. Es wird ein Bestätigungsdialogfeld angezeigt. Navigieren Sie mit den Pfeiltasten oder der Taste **Tab** zur Standardeinstellung **Save** (Speichern), um die angezeigten Werte zu speichern, oder zu **Back** (Zurück), um zum vorherigen Dialogfeld zurückzukehren. Drücken Sie dann die **Eingabetaste**.

   Wenn Sie die Werte gespeichert haben, wird einige Sekunden lang ein blauer Bildschirm angezeigt.

6. Bei einem System, das für zwei Knoten lizenziert ist, sehen Sie eine Meldung mit der Aufforderung, den zweiten Knoten auszupacken.

   Bei einem System, das für einen oder für zwei Knoten lizenziert ist, folgen Sie den Anleitungen auf dem Bildschirm, die auch erläutern, wie Sie die Netzwerkkabel anschließen sollen und - bei einem System, das für zwei Knoten lizenziert ist - den zweiten Knoten einschalten (Schritt 3 in der Bereitstellungsanleitung für Ihr System). Weitere Informationen zur Netzwerkkonfiguration finden Sie unter Verbinden von Ethernet-Kabeln.

   Der Bildschirm zeigt bei einem System, das für zwei Knoten lizenziert ist, bis zu 15 Minuten lang wechselnde Statusmeldungen an, und bei einem System, das für einen Knoten lizenziert ist, bis zu 5 Minuten lang.

7. Dann erscheint auf dem Bildschirm die Aufforderung, in einem Webbrowser eine Verbindung zu einer IP-Adresse herzustellen (Schritt 4 in der Bereitstellungsanleitung für Ihr System). Notieren Sie sich die IP-Adresse. Sie brauchen Sie später für die Anmeldung bei der ztC Console.

Der an den ersten Knoten angeschlossene Bildschirm zeigt keine weiteren Aufforderungen an. Falls Sie die IP-Adresse dynamisch konfiguriert haben (durch die Auswahl von **Automatische Konfiguration über DHCP**

für die Netzwerkadresse des Knotens), notieren Sie die IP-Adresse wie unter Aufzeichnen der Verwaltungs-IP-Adresse beschrieben.

> **Hinweis**: Wenn Sie versehentlich falsche Netzwerkeinstellungen eingegeben haben (zum Beispiel durch einen Tippfehler bei einer IP-Adresse), können Sie die Taste **[1]** drücken, um von vorne anzufangen.

Um die Bereitstellung abzuschließen, lesen Sie Erstmaliges Anmelden bei der ztC Console.

Bereitstellungsanleitungen

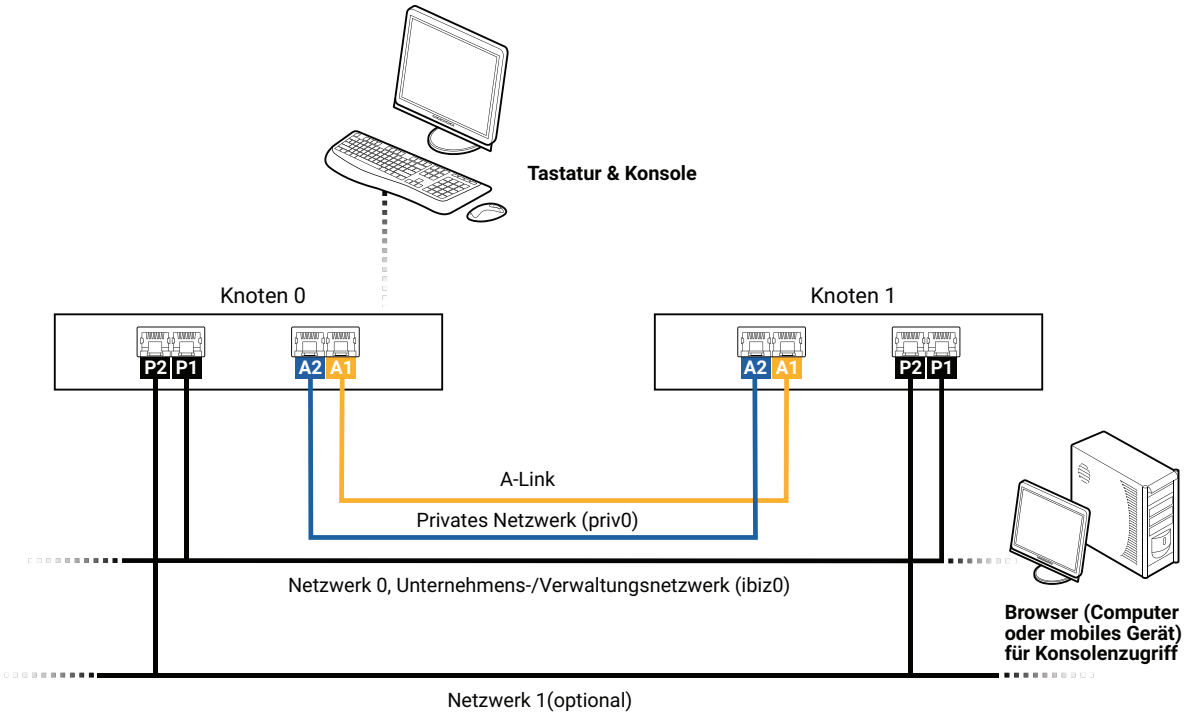
ztC Edge 100i/110i-Systeme: Ein System mit zwei Knoten bereitstellen (R012Z)

ztC Edge 100i/110i-Systeme: Ein System mit einem Knoten bereitstellen (R014Z)

Verbinden von Ethernet-Kabeln

Wenn Sie ein ztC Edge-System bereitstellen, müssen Sie Ethernet-Kabel anschließen. Die folgende Abbildung zeigt die Ethernet-Kabelverbindungen für die Netzwerkkonfiguration in einem System, das für zwei Knoten lizenziert ist. (Die Tastatur und die Konsole können an Knoten0 oder Knoten1 angeschlossen werden. In der Abbildung wird der Anschluss an Knoten0 gezeigt.) Bei einem System, das für einen Knoten lizenziert ist, folgen Sie den Anweisungen (unten), um Ethernet-Kabel mit **P1** für Netzwerk0 (ibiz0) und optional mit **P2** für Netzwerk1 (ibiz1) zu verbinden.

> **Hinweis**: Die Ethernet-Ports **P1** und **P2** sowie die Ports **A1** und **A2** befinden sich je nach Knotenmodell an der Vorderseite oder an der Rückseite des Knotens.



Wenn Sie das System bereitstellen (siehe Bereitstellen des Systems), verbinden Sie:

- Das blaue Kabel für **priv0** vom Embedded-Port **A2** auf Knoten0 mit dem entsprechenden Embedded-Port auf Knoten1.
- Das gelbe Kabel für A-Link1 vom Embedded-Port **A1** auf Knoten0 mit dem entsprechenden Embedded-Port auf Knoten1.

Für Netzwerk0 (ibiz0) verbinden Sie ein Ethernet-Kabel von **P1** auf jedem Knoten mit einem Netzwerk, auf das vom Computer für die Remoteverwaltung zugegriffen werden kann. Für das optionale Netzwerk1 (ibiz1) verbinden Sie ein Ethernet-Kabel von **P2** an jedem Knoten mit dem zusätzlichen Netzwerk.

Nehmen Sie ggf. erforderliche Änderungen an Ihrem Netzwerk vor, um diese Verbindungen vorzubereiten. Führen Sie dann den nächsten Schritt unter Bereitstellen des Systems aus.

Verwandte Themen

Bereitstellung

Anforderungen für A-Link- und private Netzwerke

Anforderungen für Unternehmens- und Verwaltungsnetzwerke

Anforderungen für die ztC Console

Tastaturlayout

Sie können nach der Bereitstellung eine andere Tastenbelegung für Ihre Tastatur konfigurieren.

Die folgenden Tastaturbelegungen werden unterstützt:

Layout	Sprache
de	Deutsch
de-latin1	Deutsch (Latin1)
de-latin1-nodeadkey	Deutsch (Latin1 ohne nicht belegte Tasten)
dvorak	Dvorak
jp106	Japanisch
sg	Deutsch (Schweiz)
sg-latin1	Deutsch (Schweiz) (Latin1)
uk	Englisch (Großbritannien)
us	Englisch (USA)
us-acentos	Englisch (International)

So konfigurieren Sie das Tastaturlayout nach der Bereitstellung

1. Melden Sie sich als `root` bei der ersten PM an.
2. Geben Sie in der Befehlszeile den Befehl `localectl` ein, um das richtige Tastaturlayout zu konfigurieren. Im folgenden Beispiel wird das deutsche Tastaturlayout konfiguriert:

   ```
   # localectl set-keymap de
   ```

3. Wiederholen Sie die oben beschriebenen Schritte auf der zweiten PM, sofern vorhanden.

Verwandte Themen

Aufgaben nach der Bereitstellung

Aufzeichnen der Verwaltungs-IP-Adresse

Ihr Netzwerkadministrator benötigt möglicherweise die Verwaltungs-IP-Adresse für jede physische Maschine (PM), um die IP-Adresse des Systems zu konfigurieren. Gehen Sie wie nachstehend beschrieben vor, wenn das Verwaltungsnetzwerk für die Verwendung einer dynamischen IP-Adresse konfiguriert wurde. (Ihr Netzwerkadministrator hat diese Informationen bereits, wenn das Verwaltungsnetzwerk eine statische IP-Adresse hat.)

1. Wenn die Installation auf der PM abgeschlossen ist und die PM neu gestartet wird, erscheint ein Bildschirm ähnlich wie der folgende:

   ```
   ztC Edge

        IPv4 address 10.84.52.117

        IPv6 address 3d00:feed:face:1083:225:64ff:fe8d:1b6e

        IPv6 address fe80: :225:64ff:fe8d:1b6e
   ```

2. Notieren Sie die IPv4-Adresse, die auf dem Bildschirm angezeigt wird.
3. Geben Sie diese IP-Adresse an Ihren Netzwerkadministrator weiter.

Kehren Sie zu Bereitstellen des Systems zurück, um die Bereitstellung fortzusetzen.

Verwandte Themen

Anforderungen für Unternehmens- und Verwaltungsnetzwerke

Aufgaben nach der Bereitstellung

Nachdem das System bereitgestellt wurde, müssen Sie noch verschiedene Aufgaben nach der Bereitstellung ausführen, darunter:

- Beziehen der System-IP-Informationen
- Erstmaliges Anmelden bei der ztC Console
- Registrieren des Systems und Beziehen einer dauerhaften Lizenz
- Konfigurieren der erforderlichen Systemvoreinstellungen:
  - Konfigurieren von Datum und Uhrzeit
  - Konfigurieren der Remotesupport-Einstellungen

    - Konfigurieren der Quorumserver
    - Eingeben der Besitzerinformationen
- Konfigurieren von Active Directory
- Verwalten lokaler Benutzerkonten

> **Hinweis**: Sie müssen für jedes Benutzerkonto, auch **admin**, eine E-Mail-Adresse angeben, damit die Funktion zum Zurücksetzen des Kennworts verwendet werden kann. Wenn ein Benutzerkonto keine E-Mail-Adresse enthält und der betreffende Benutzer in der Konsole auf den Link **Kennwort vergessen?** klickt, sendet das System eine E-Mail an **benutzer@beispiel.com**. Unter Verwalten lokaler Benutzerkonten wird beschrieben, wie Sie Benutzer hinzufügen und Benutzerkonten bearbeiten, darunter auch, wie Sie eine E-Mail-Adresse hinzufügen.

- Auflösen ausstehender Alarme im Dashboard
- Verbinden eines zweiten Unternehmensnetzwerks

In bestimmten Situationen kann es erforderlich sein, die folgenden zusätzlichen Aufgaben durchzuführen:

- Erneutes Bereitstellen eines ztC Edge-Systems
- Hinzufügen eines Knotens zu einem Einzelknotensystem

Beziehen der System-IP-Informationen

Nachdem Sie das System bereitgestellt haben, brauchen Sie die IP-Adresse von Knoten0, um sich erstmals bei der ztC Console anzumelden (siehe Erstmaliges Anmelden bei der ztC Console). Um die erste Anmeldung abzuschließen, brauchen Sie auch die System-IP-Informationen, die Sie vom Netzwerkadministrator bekommen. Geben Sie dem Netzwerkadministrator die IP-Adressen von Knoten0 und Knoten1 (falls vorhanden) (siehe Aufzeichnen der Verwaltungs-IP-Adresse), damit er die System-IP-Informationen leichter ermitteln kann. Die IP-Adresse des Systems muss eine statische IP-Adresse sein. Verwenden Sie keine dynamische IP-Adresse.

Verwandte Themen

Bereitstellung

Aufgaben nach der Bereitstellung

Erstmaliges Anmelden bei der ztC Console

Wenn Sie das System bereitstellen, melden Sie sich bei der ztC Console an, um die Endbenutzerlizenzvereinbarung (EULA) zu akzeptieren und Netzwerkinformationen einzugeben. Sie können zu diesem Zeitpunkt auch das System registrieren und eine dauerhafte Lizenz beziehen. Dies ist jedoch auch später noch möglich. Nach der ersten Installation eines Systems gilt für 30 Tage eine befristete Lizenz.

So melden Sie sich zum ersten Mal bei der ztC Console an

1. Geben Sie auf einem mit dem Netzwerk verbundenen PC oder Laptop die IP-Adresse von Knoten0 (primärer Knoten) in die Adressleiste des Browsers ein (Schritt 5 in der Bereitstellungsanleitung für Ihr System).

   Hinweis: Wenn eine Sicherheitswarnung angezeigt wird, rufen Sie die Website trotzdem auf. Sie können später eine Sicherheitsausnahme hinzufügen, damit die Website ohne Sicherheitsmeldung geladen wird (siehe Konfigurieren von sicheren Verbindungen).

   Die Anmeldeseite der ztC Console wird angezeigt.

2. Geben Sie **admin** als **Benutzername** und **admin** als **Kennwort** ein (oder andere Anmeldedaten, die Ihnen ggf. mitgeteilt wurden) und klicken Sie auf **ANMELDEN**.

   Die Stratus ztC Edge-Endbenutzerlizenzvereinbarung (EULA) wird angezeigt.

3. Lesen Sie die EULA und klicken Sie auf **Akzeptieren**, wenn Sie mit den Bedingungen einverstanden sind. Wenn Sie die EULA nicht akzeptieren, wird die Bereitstellung beendet.

   Die Seite **ERSTKONFIGURATION** wird unter **Konfig** angezeigt.

4. Unter **BENACHRICHTIGUNGEN** ist das Kontrollkästchen **Supportbenachrichtigungen aktivieren** standardmäßig aktiviert. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie nicht möchten, dass das ztC Edge-System Integritäts- und Statusbenachrichtigungen an Ihren autorisierten Stratus-Servicemitarbeiter sendet. Sie können diese Einstellung auch später noch ändern (siehe Konfigurieren der Remotesupport-Einstellungen).

5. Geben Sie unter **IP-ADRESSE DES SYSTEMS** in das Feld **Statische System-IP-Adresse** die statische System-IP-Adresse ein, die Ihnen Ihr Netzwerkadministrator mitgeteilt hat (in der Bereitstellungsanleitung für Ihr System, siehe Abschnitt **Vom Benutzer bereitgestellte Komponenten**). (Die IP-Adresse des Systems wird manchmal auch als Cluster-IP-Adresse bezeichnet.)

6. Ebenfalls unter **IP-ADRESSE DES SYSTEMS** wählen Sie **DHCP** (Standardeinstellung) oder **Statisch**. Bei der Einstellung **DHCP** brauchen Sie keine weiteren Informationen einzugeben.

   Wenn Sie **Statisch** wählen, wird die statische IP-Adresse von Knoten0 angezeigt, die Sie bei der Bereitstellung eingegeben haben. Geben Sie die folgenden Werte an (in der Bereitstellungsanleitung für Ihr System, siehe Abschnitt **Vom Benutzer bereitgestellte Komponenten**):

   - Primärer und sekundärer DNS
   - Netzmaske
   - Gatewayadresse von Knoten0
   - IP-Adresse von Knoten1 (falls vorhanden)
   - Gatewayadresse von Knoten1 (falls vorhanden)

   Nachdem Sie die Netzwerkinformationen eingegeben haben, klicken Sie auf **Weiter**. Nach einem kurzen Moment wird das Fenster **LIZENZINFORMATIONEN** angezeigt.

7. Sie können das System jetzt registrieren und eine dauerhafte Lizenz installieren (Schritt 6 in der Bereitstellungsanleitung für Ihr System) oder dies später tun. Siehe Registrieren des Systems und Beziehen einer dauerhaften Lizenz.

8. Klicken Sie nach Abschluss der Registrierung auf **Fertigstellen**. Das Fenster **KONTOSICHERHEIT** wird angezeigt.

9. Geben Sie für **Neues Kennwort** im Fenster **KONTOSICHERHEIT** ein neues Kennwort für den Benutzer **admin** ein. Geben Sie das Kennwort unter **Kennwort bestätigen** erneut ein. Das Kennwort muss der Kennwortrichtlinie des Systems entsprechen (Informationen hierzu finden Sie unter Kennwortrichtlinie).

Hinweise:

- Aus Sicherheitsgründen müssen Sie das Kennwort für **admin** jetzt ändern. Sie können das Kennwort später erneut ändern. Außerdem sollten Sie den Standardanmeldenamen für das Konto **admin** ändern. Diese Änderungen nehmen Sie auf der Seite **Benutzer und Gruppen** vor (siehe Konfigurieren von Benutzern und Gruppen).
- Für noch mehr Sicherheit ändern Sie auch das Kennwort für **root** im Host-Betriebssystem jeder PM. Dies sollte so bald wie möglich nach der Bereitstellung erfolgen (siehe Zugriff auf das Host-Betriebssystem).

10. Klicken Sie auf **Fertigstellen**.

Die ztC Console wird angezeigt und die erstmalige Anmeldung ist abgeschlossen. Fügen Sie im Browser ein Lesezeichen hinzu oder notieren Sie sich die IP-Adresse des Systems, die Sie in Zukunft für die Anmeldung bei der Konsole verwenden.

Führen Sie ggf. zusätzliche Aufgaben wie unter Aufgaben nach der Bereitstellung beschrieben aus.

Verwandte Themen

Bereitstellung

Die ztC Console

Verwenden der ztC Console

Bereitstellungsanleitungen

ztC Edge 100i/110i-Systeme: Ein System mit zwei Knoten bereitstellen (R012Z)

ztC Edge 100i/110i-Systeme: Ein System mit einem Knoten bereitstellen (R014Z)

Registrieren des Systems und Beziehen einer dauerhaften Lizenz

Sie müssen ein System registrieren, wozu auch das Beziehen einer dauerhaften Lizenz gehört. Nach der ersten Bereitstellung eines Systems gilt für 30 Tage eine befristete Lizenz. (Eine befristete Lizenz wird in der Titelleiste mit **UNREGISTERED_TRIAL** als **Bestandskennung** angezeigt.) Sie können das System registrieren, wenn Sie sich zum ersten Mal bei der ztC Console anmelden, oder zu einem späteren Zeitpunkt. Die Registrierung kann auf Systemen mit oder ohne Internetverbindung erfolgen.

Bei einem System ohne Internetverbindung müssen Sie eine Datei zwischen dem Standort der Konsole (ohne Internetverbindung) und einem Standort mit Internetverbindung kopieren. Neben weiteren Methoden gibt es dafür die folgenden beiden Möglichkeiten:

- Ein USB-Stick – Sie verwenden einen USB-Stick auf einem Verwaltungscomputer (der eine Verbindung zum System herstellen kann) und auf einem Computer mit Internetverbindung.
- Ein mobiles Gerät, zum Beispiel Notebook oder Smartphone – Sie können ein mobiles Gerät zwischen einem Standort, an dem Sie sich bei der ztC Console anmelden können, und einem Standort mit Internetverbindung verwenden.

Voraussetzungen:

- Um das System zu registrieren, brauchen Sie das Blatt **Wichtige Informationen zur Anmeldung** von Stratus, das Sie zusammen mit dem System erhalten haben. Auf dem Blatt steht die BESTANDSKENNUNG für das ztC Edge-System. Falls Sie die BESTANDSKENNUNG nicht mehr finden, wenden Sie sich an Ihren autorisierten Stratus-Servicemitarbeiter, um sie zu erhalten.
- Lesen Sie So führen Sie die erforderlichen Schritte im Registrierungsportal aus, bevor Sie das System registrieren, um sicherzustellen, dass Sie alle erforderlichen Informationen zur Hand haben.

So führen Sie die erforderlichen Schritte im Registrierungsportal aus

Schritt 1: Allgemeine Informationen – Geben Sie die folgenden Informationen ein:

- **First Name** (Vorname) und **Last Name** (Nachname)
- **Company Email** (E-Mail-Adresse des Unternehmens) – Geben Sie die E-Mail-Adresse des Unternehmens ein, das dem Standort (der Site) der endgültigen Bereitstellung entspricht. Geben Sie keine persönliche E-Mail-Adresse ein.
- **Asset ID** (Bestandskennung) – Geben Sie die BESTANDSKENNUNG ein, die Sie auf dem Stratus-Registrierungsblatt finden.

Sie müssen auch die **Service Terms** (Nutzungsbedingungen) lesen und akzeptieren.

Schritt 2: Informationen zum Standort – Geben Sie die folgenden Informationen ein:

- **Company Email** (E-Mail-Adresse des Unternehmens) und **Retype Email** (E-Mail-Adresse erneut eingeben) – Geben Sie die E-Mail-Adresse des Unternehmens ein, das dem Standort (der

Site) der endgültigen Bereitstellung entspricht. Geben Sie keine persönliche E-Mail-Adresse ein.

- **Deployment Shipping Address** (Lieferadresse der Bereitstellung) – Geben Sie die vollständige Adresse für den Versand von Ersatzteilen an. Verwenden Sie die Adresse des Unternehmens, bei dem die endgültigen Bereitstellung erfolgt. Geben Sie kein Postfach an. Die einzelnen Felder:
  - **Address 1** (Adresse 1) und **Address 2** (Adresse 2)
  - **City** (Ort), **State** (Bundesstaat), **Postal Code** (PLZ) und **Country** (Land)
  - **Special Instructions** (Besondere Hinweise wie „Immer an Laderampe 2 liefern“)

Schritt 3: Kontaktinformationen – Geben Sie die folgenden Informationen ein:

- **Primary Technical Contact** (Erster technischer Ansprechpartner) und **Secondary Technical Contact** (Zweiter technischer Ansprechpartner) – Geben Sie die Namen der für die Technik zuständigen Kontakte an, die mit Ihrem autorisierten Stratus-Servicemitarbeiter kommunizieren werden.
- **Service Renewal Contact** (Ansprechpartner für Serviceverlängerung) – Geben Sie die Namen der Person an, die für die Verwaltung der jährlichen Verlängerungen des Servicevertrags zuständig ist.

Geben Sie für alle Kontakte jeweils **First Name** (Vorname), **Last Name** (Nachname), **Email Address** (E-Mail-Adresse), **Desk Phone** (Durchwahl) und **Mobile (optional)** (Handynummer, optional) an. Sie können später weitere Kontakte hinzufügen; verwenden Sie dazu das **Stratus Customer Service Portal** unter https://support.stratus.com.

Wenn Sie unten auf der Seite auf **Next** (Weiter) klicken, überprüft Stratus die Angaben.

Falls die Angaben fehlerhaft sind, wird das Fenster **Problem Encountered** (Fehler) angezeigt, in dem das Problem beschrieben wird. Klicken Sie auf **Back** (Zurück), um den Fehler zu korrigieren. Wenn es weiterhin ein Problem gibt, klicken Sie auf **Next** (Weiter), um eine Datei herunterzuladen, die Ihnen den Abschluss der Registrierung ermöglicht. Um Ihnen bei der Fehlerbehebung zu helfen und sicherzustellen, dass Ihr Konto richtig eingerichtet wurde, werden Sie von Ihrem autorisierten Stratus-Servicemitarbeiter kontaktiert.

Die Seite **Information Verification** (Überprüfung der Angaben) wird angezeigt. Falls Sie die Angaben ändern möchten, klicken Sie auf **Back** (Zurück). Klicken Sie auf **Next** (Weiter), um die Informationen zu senden und die Registrierung abzuschließen.

Schritt 4: Lizenzschlüssel – Klicken Sie auf **Finish** (Fertigstellen), um die Lizenzschlüsseldatei herunterzuladen, die Sie auf dem ztC Edge-System installieren werden. Notieren Sie sich den Speicherort, in den Sie die Datei herunterladen.

So registrieren Sie das System und beziehen eine dauerhafte Lizenz

Auf einem System mit Internetverbindung

1. Falls Sie das System registrieren möchten, wenn Sie sich zum ersten Mal bei der Konsole anmelden, beginnen Sie mit dem nächsten Schritt. Wenn Sie das System nach der Bereitstellung registrieren, führen Sie die folgenden Schritte aus:
    a. Klicken Sie in der ztC Console im Navigationsbereich auf der linken Seite auf **Voreinstellungen**.
    b. Klicken Sie auf der Seite **Voreinstellungen** auf **Produktlizenz**.
2. Bei **Online-Lizenzregistrierung und Aktivierung** klicken Sie auf **Online registrieren**, um einen neuen Browser-Tab mit dem Stratus-Registrierungsportal zu öffnen. Führen Sie die erforderlichen Schritte im Registrierungsportal aus.

    In **Schritt 4** laden Sie die dauerhafte Lizenzschlüsseldatei herunter und speichern Sie sie auf dem Computer.
3. Klicken Sie in der Konsole auf die Leiste **Lizenz installieren**.
4. Klicken Sie auf **Datei auswählen** und navigieren Sie zum Speicherort, an dem Sie die Datei gespeichert haben.
5. Wählen Sie die Datei aus, klicken Sie auf **Öffnen** und dann auf **Hochladen**, um die Datei an das System hochzuladen.

Auf einem System ohne Internetverbindung

Bei einem System ohne Internetverbindung müssen Sie eine Datei zwischen dem Standort der ztC Console (ohne Internetverbindung) und einem Standort mit Internetverbindung kopieren. Neben weiteren Methoden gibt es dafür die folgende Möglichkeit:

Auf einem Computer oder einem mobilen Gerät mit Zugriff auf die ztC Console

1. Wenn Sie einen Verwaltungscomputer verwenden, schließen Sie einen USB-Stick an einen USB-Anschluss an.

    Wenn Sie ein mobiles Gerät verwenden, stellen Sie sicher, dass es Zugriff auf die ztC Console hat.

2. Falls Sie das System registrieren möchten, wenn Sie sich zum ersten Mal bei der Konsole anmelden, fahren Sie mit dem nächsten Schritt fort. Wenn Sie das System nach der Bereitstellung registrieren, führen Sie die folgenden Schritte aus:
    a. Melden Sie sich bei der ztC Console an.
    b. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**.
    c. Klicken Sie auf der Seite **Voreinstellungen** auf **Produktlizenz**.
3. Bei Schritt 1, **Offline-Registrierung über URL-Datei**, (unter der Leiste **Offline-Lizenzregistrierung und manuelle Installation der Lizenz**) klicken Sie auf **URL-Datei herunterladen**. Speichern Sie die Datei ***register_site_file*.html** auf dem USB-Stick oder auf dem mobilen Gerät. Wenn Sie einen USB-Stick verwenden, trennen Sie ihn vom System.
4. Gehen Sie zu einem Computer mit Internetverbindung.

Auf einem Computer mit Internetverbindung

1. Wenn Sie einen USB-Stick verwenden, schließen Sie ihn an einen USB-Anschluss des Computers mit Internetverbindung an.
2. Navigieren Sie zu der Datei, die Sie gespeichert haben, und klicken Sie auf den Dateinamen. Ein Browser öffnet die Datei und wird zum Stratus-Registrierungsportal im Internet umgeleitet. Führen Sie die erforderlichen Schritte im Registrierungsportal aus.

    In **Schritt 4** laden Sie die dauerhafte Lizenzschlüsseldatei herunter und speichern Sie sie auf dem USB-Stick oder auf dem mobilen Gerät. Wenn Sie einen USB-Stick verwenden, trennen Sie ihn vom System.
3. Gehen Sie wieder zu dem Computer mit Zugriff auf die Konsole.

Auf einem Computer oder einem mobilen Gerät mit Zugriff auf die ztC Console

1. Wenn Sie einen USB-Stick verwenden, schließen Sie ihn an einen USB-Anschluss des Verwaltungscomputers an.

    Wenn Sie ein mobiles Gerät verwenden, stellen Sie sicher, dass es Zugriff auf die ztC Console hat.
2. Klicken Sie in der Konsole im Navigationsbereich auf der linken Seite auf **Voreinstellungen**.
3. Klicken Sie auf der Seite **Voreinstellungen** auf **Produktlizenz**.

4. Bei Schritt 2, **Aktivierte Lizenz auf dem System installieren**, (unter der Leiste **Offline-Lizenzregistrierung und manuelle Installation der Lizenz**) klicken Sie auf **Datei auswählen**. Navigieren Sie zum dem Speicherort, wo Sie die Lizenzschlüsseldatei gespeichert haben.
5. Wählen Sie die Datei aus, klicken Sie auf **Öffnen** und dann auf **Hochladen**, um die Datei an das System hochzuladen.

Wenn Sie sich zum ersten Mal bei der Konsole anmelden, kehren Sie zum letzten Schritt unter Erstmaliges Anmelden bei der ztC Console zurück, nachdem Sie die Lizenz hochgeladen haben.

Verwandte Themen

Erstmaliges Anmelden bei der ztC Console

Verwalten der Produktlizenz

Erneutes Bereitstellen eines ztC Edge-Systems

Sie können ein ztC Edge-System erneut bereitstellen, wenn Sie das System schon einmal bereitgestellt und konfiguriert haben. Dazu müssen Sie allerdings die Netzwerkeinstellungen zurücksetzen, um das System für die erneute Bereitstellung in einem anderen Netzwerk oder Subnetz, möglicherweise an einem neuen Standort, vorzubereiten.

Die erneute Bereitstellung eines neuen ztC Edge-Systems erfolgt typischerweise dann, wenn Sie das System mit Einstellungen und virtuellen Maschinen (VMs) für einen Endbenutzer vorbereiten, dann aber die Netzwerkeinstellungen zurücksetzen, damit der Endbenutzer das System erstmals an seinem Standort bereitstellen kann. (Dies ähnelt der Verwendung von Windows Sysprep zur Vorbereitung eines Windows-Systems auf die erste Endbenutzerbereitstellung oder Out-Of-Box Experience (OOBE).)

Nachdem Sie das System für den Endbenutzer konfiguriert haben, leiten Sie die erneute Bereitstellung in der ztC Console ein. Daraufhin löscht das System die Netzwerkeinstellungen des Systems und der Knoten, fährt alle laufenden VMs herunter und fährt das System herunter. Das System behält alle Einstellungen, die nicht mit dem Netzwerk zu tun haben, und die konfigurierten VMs, ist jetzt aber vorbereitet für die Bereitstellung wie in der Bereitstellungsanleitung für Ihr System beschrieben.

Hinweise:

Wenn Sie ein ztC Edge-System erneut bereitstellen, beachten Sie die folgenden Einschränkungen und Workarounds:

- Deaktivieren Sie alle NFS/CIFS-Freigaben, bevor Sie ein System erneut bereitstellen.

  Aktive NFS/CIFS-Freigaben führen zu Störungen bei der Neubereitstellungsfunktion. Deaktivieren Sie die Freigaben, bis Sie die Konfiguration der Netzwerkeinstellungen im neuen Netzwerk abgeschlossen haben.

- Beim Festlegen einer neuen statischen System-IP-Adresse ist ein Systemneustart erforderlich.

  Ein System verliert den Zugriff auf den sekundären Knoten, wenn Sie das System erneut bereitstellen und herunterfahren, an einem neuen Ort starten und dann die neue statische System-IP-Adresse konfigurieren. Um wieder Zugriff auf den sekundären Knoten zu bekommen, starten Sie das System neu, indem Sie die Seite **System** öffnen und auf **Neu starten** klicken. Beim Neustarten des Systems werden die Gateway-Einstellungen auf dem sekundären Knoten aktualisiert, sodass die Verbindung zum System hergestellt werden kann.

- Wenn Sie ein System bereits in ein neues Netzwerk verschoben haben, aber vergessen haben, es zunächst erneut bereitzustellen, lesen Sie KB-8283 mit Anleitungen zur erneuten Bereitstellung des Systems.

- Wenn Sie einen individuellen, verwendeten Knoten als ersten Knoten in einem neuen System erneut bereitstellen müssen, oder als zweiten Knoten in einem anderem System, lesen Sie KB-9391.

So stellen Sie ein ztC Edge-System erneut bereit

1. Bereiten Sie das System für den Endbenutzer vor. Konfigurieren Sie die ztC Edge-Systemeinstellungen und erstellen Sie VMs nach Bedarf. (Wenn Sie das System erneut bereitstellen, werden nur die Netzwerkeinstellungen zurückgesetzt.)
2. Wenn Sie die Vorbereitung des Systems abgeschlossen haben, öffnen Sie die Seite **Voreinstellungen** in der ztC Console, klicken Sie auf **IP-Konfiguration** und dann auf **Erneut bereitstellen**.

3. Das System löscht die Netzwerkeinstellungen des Systems und der Knoten, fährt alle laufenden VMs herunter und fährt das System herunter.
4. Das System ist bereit für die Bereitstellung durch den Endbenutzer. Um das System bereitzustellen, lesen Sie die Bereitstellungsanleitung für Ihr System. (Bei Bedarf finden Sie weitere Informationen unter Bereitstellen des Systems.)

Verwandte Themen

Bereitstellung

Die ztC Console

Verwenden der ztC Console

Bereitstellungsanleitungen

ztC Edge 100i/110i-Systeme: Ein System mit zwei Knoten bereitstellen (R012Z)

ztC Edge 100i/110i-Systeme: Ein System mit einem Knoten bereitstellen (R014Z)

Hinzufügen eines Knotens zu einem Einzelknotensystem

In diesem Thema wird beschrieben, wie Sie einem System, das für einen Knoten lizenziert ist, einen zweiten Knoten hinzufügen, um ein redundantes System zu erstellen. Dies ergänzt die Informationen in Anleitung zum Hinzufügen eines Knotens für Ihr System. (Wenn Sie ein Systems erstmals bereitstellen, lesen Sie Bereitstellung.)

Voraussetzungen: Um dieses Verfahren abzuschließen, benötigen Sie Folgendes:

- Einen zweiten ztC Edge-Knoten, der dem Modell und der BESTANDSKENNUNG des laufenden Knotens entspricht, und eine Produktlizenz, die für die Unterstützung von zwei Knoten aktualisiert wurde. Wenden Sie sich bei Bedarf an Ihren autorisierten Stratus-Servicemitarbeiter.
- Eine statische IP-Adresse für den zweiten Knoten, falls Sie den ersten Knoten mit einer statischen IP-Adresse konfiguriert haben. (Die aktuelle Netzwerkkonfiguration können auf der Seite **Voreinstellungen** der ztC Console unter **IP-Konfiguration** überprüfen.)

So fügen Sie einen Knoten hinzu

1. Integrität des laufenden Knotens überprüfen - die SYS-LED blinkt und die Seite **Dashboard** der ztC Console zeigt grüne Häkchen ohne ausstehende Probleme an. Beheben Sie alle Probleme, bevor der

zweite Knoten hinzugefügt wird.

2. Öffnen Sie in der ztC Console die Seite **Voreinstellungen** und klicken Sie auf **Produktlizenz**. Klicken Sie auf **Lizenz jetzt überprüfen**, um die Lizenz für die Unterstützung von zwei Knoten zu aktualisieren. Nach der erfolgreichen Aktualisierung zeigt die Seite **Dashboard** an, dass das Zwei-Knoten-Upgrade aussteht.

   Hinweis: Die folgenden Schritte sollten eventuell bis zum nächsten Wartungszeitraum verschoben werden, da die VM-Leistung bis zum Neustart der VMs in Schritt 6 verlangsamt wird.

3. Verbinden Sie Port P1 des zweiten Knotens mit dem vorhandenen LAN und verbinden Sie die blauen und gelben Netzwerkkabel vom ersten Knoten mit dem zweiten Knoten (Ports A1 und A2). Schließen Sie den zweiten Knoten an die Stromversorgung an und überprüfen Sie, dass dieser eingeschaltet wird. Weitere Informationen zur Netzwerkkonfiguration finden Sie unter Verbinden von Ethernet-Kabeln.

   Hinweis: Die ztC-Konsole zeigt möglicherweise Warnungen für den zweiten Knoten an. Sie können diese Warnungen ignorieren, bis die Synchronisierung in Schritt 6 abgeschlossen wird.

4. Warten Sie nach dem Anschluss des zweiten Knotens bis zu 30 Minuten, bis die SYS-LED am zweiten Knoten blinkt und die Schaltfläche **PM hinzufügen** auf der Seite **Physische Maschinen** verfügbar ist. Klicken Sie auf **PM hinzufügen**. (Falls die Schaltfläche inaktiv bleibt, überprüfen Sie, ob die Produktlizenz aktualisiert wurde, die Netzwerk- und Stromkabel korrekt angeschlossen wurden und der zweite Knoten eingeschaltet ist.)

   Hinweis: Die Verwaltungskonsole ist bis zu 15 Minuten lang nicht verfügbar, während das System den neuen Knoten hinzufügt.

5. Öffnen Sie in der ztC-Konsole die Seite **Voreinstellungen** und klicken Sie auf **IP-Konfiguration**, um die Netzwerkeinstellungen zu überprüfen. Geben Sie, falls erforderlich, eine statische IP-Adresse für den zweiten Knoten (**Knoten1**) ein und klicken Sie auf **Speichern**.

6. Die Synchronisierung der VMs kann einige Stunden dauern. Danach müssen die VMs neu gestartet werden, um die Redundanz zu aktivieren und Meldungen aufzulösen. Bei Systemen, die den fehlertoleranten Betrieb (FT) unterstützen, sollten Sie eventuell die Einstellung für die Schutzstufe

(HV/FT) für die VMs ändern, während sie außer Betrieb sind. Siehe Ändern der Schutzstufe für eine virtuelle Maschine (HV oder FT). Nachdem das System synchronisiert wurde und die VMs ausgeführt werden, zeigt das **Dashboard** grüne Häkchen ohne ausstehende Problem an.

Anleitungen zum Hinzufügen eines Knotens

ztC Edge 100i/110i-Systeme: Einen Knoten hinzufügen (R015Z)

Verbinden eines zweiten Unternehmensnetzwerks

Wenn Sie ein ztC Edge-System erstmals bereitstellen, verbinden Sie ein Netzwerkkabel vom Port P1 jedes Knotens mit dem vorhandenen Netzwerk, um ein gemeinsames Unternehmens-/Verwaltungsnetzwerk zu erstellen, das als Netzwerk0 bezeichnet wird.

Wenn Sie nach der Bereitstellung ein zweites, dediziertes Unternehmensnetzwerk (Netzwerk1) hinzufügen möchten, verbinden Sie ein Netzwerkkabel vom Port P2 an jedem Knoten mit Ihrem vorhandenen Netzwerk.

Das Hinzufügen eines zweiten Unternehmensnetzwerks kann die Lastverteilung in einem System mit zwei oder mehr virtuellen Maschinen (VMs) verbessern, da Sie die VMs separaten Unternehmensnetzwerken zuweisen können. Die Entlastung von Netzwerk0 kann auch zur Leistungsverbesserung beitragen, da Netzwerk1 sowohl Verwaltungs- als auch Unternehmensdatenverkehr überträgt.

So verbinden Sie ein zweites Unternehmensnetzwerk

1. Verbinden Sie ein Netzwerkkabel vom Port **P2** an jedem Knoten mit Ihrem vorhandenen Netzwerk.
2. Rufen Sie in der ztC Console die Seite **Netzwerke** auf.
    a. Die neue Verbindung **Netzwerk1** sollte nach ungefähr einer Minute angezeigt werden.
    b. Vergewissern Sie sich, dass die neue Verbindung **Netzwerk1** ein grünes Prüfhäkchen anzeigt.
3. Verwenden Sie den Assistenten **Virtuelle Maschine neu zuweisen**, um **Netzwerk1** für jede VM zu aktivieren (und ggf. **Netzwerk0** zu deaktivieren). Weitere Informationen finden Sie unter Neuzuweisen von VM-Ressourcen.

Verwandte Themen

Verbinden von Ethernet-Kabeln

Anforderungen für A-Link- und private Netzwerke

Anforderungen für Unternehmens- und Verwaltungsnetzwerke

Allgemeine Netzwerkanforderungen und -konfigurationen

3

Kapitel 3: Verwenden der ztC Console

Die ztC Console ist eine browserbasierte Benutzeroberfläche, die die Verwaltung und Überwachung eines ztC Edge-Systems von einem Remoteverwaltungscomputer aus ermöglicht. Eine Übersicht über die Konsole finden Sie unter Die ztC Console.

Informationen zu den einzelnen Seiten der ztC Console finden Sie in den folgenden Themen:

- Die Seite „Dashboard“
- Die Seite „System“
- Die Seite „Voreinstellungen“
- Die Seite „Alarmverlauf“
- Die Seite „Auditprotokolle“
- Die Seite „Supportprotokolle“
- Die Seite „Physische Maschinen“
- Die Seite „Virtuelle Maschinen“
- Die Seite „Volumes“
- Die Seite „Netzwerke“
- Die Seite „Virtuelle CDs“
- Die Seite „Upgrade-Kits“

Die ztC Console

Die ztC Console ist eine browserbasierte Benutzeroberfläche, die die Verwaltung und Überwachung eines ztC Edge-Systems von einem Remoteverwaltungscomputer aus ermöglicht. Viele administrative Aufgaben können Sie von der Konsole aus ausführen, da diese den Zugriff auf das System als Ganzes sowie auf physische Maschinen, virtuelle Maschinen und andere Ressourcen ermöglicht.

Informationen zu den Anforderungen des Remoteverwaltungscomputers, auf dem die ztC Console ausgeführt wird, finden Sie unter Anforderungen für die ztC Console.

Mit der ztC Console können Sie verschiedene administrative Funktionen ausführen:

- Lesen Sie Systemalarme im Dashboard. Siehe Die Seite „Dashboard“.
- Zeigen Sie auf der Seite „System“ Statistiken zur VM, zur CPU, zum Arbeitsspeicher und zum Speicher an und starten Sie das System neu oder fahren Sie es herunter. Siehe Die Seite „System“.
- Legen Sie Voreinstellungen für das System, Benachrichtigungen (e-Alerts und SNMP-Konfiguration) sowie Remotesupport (Benachrichtigung und Zugriff) fest und greifen Sie auf administrative Tools zu, mit denen Sie eine sichere Verbindung herstellen können. Zu den Systemvoreinstellungen gehören Besitzerinformationen und Konfigurationswerte für IP-Adresse, Quorumdienste, Datum und Uhrzeit, usw. Siehe Die Seite „Voreinstellungen“.
- Zeigen Sie Alarme und Auditprotokolle an. Siehe Die Seite „Alarmverlauf“, Die Seite „Auditprotokolle“ und Die Seite „Supportprotokolle“.
- Überwachen, verwalten und warten Sie Ressourcen:
    - PM-Status, Speicher (einschließlich Datenträger), Netzwerk, VMs und USB-Geräte: siehe Die Seite „Physische Maschinen“.
    - VM-Status und Verwaltungsaufgaben wie Erstellen, Importieren/Wiederherstellen, Verwalten und Warten von VMs: siehe Die Seite „Virtuelle Maschinen“.
    - Volumes einschließlich deren Zustand, Name, Datensynchronisierungsstatus, Größe, Zustand und weitere Informationen: siehe Die Seite „Volumes“.
    - Netzwerke einschließlich Zustand, Verbindungszustand, Name, interner Name, Typ (z. B. A-Link), VMs, Geschwindigkeit, MAC-Adresse und Netzwerkbandbreite: siehe Die Seite „Netzwerke“.
    - Virtuelle CDs, einschließlich deren Zustand, Name, Größe und Angabe, ob die VCD entfernt werden kann oder nicht, siehe: Die Seite „Virtuelle CDs“.

- Überwachen und verwalten Sie Upgrade-Kits. Siehe Die Seite „Upgrade-Kits“.

Sie können auch Ihre Benutzerinformationen ändern (siehe Bearbeiten der Benutzerinformationen) sowie Benutzer und Gruppen konfigurieren (siehe Konfigurieren von Benutzern und Gruppen).

Verwandte Themen

Erstmaliges Anmelden bei der ztC Console

Anmelden bei der ztC Console

Verwenden der ztC Console

Anmelden bei der ztC Console

Melden Sie sich bei der ztC Console an, um das ztC Edge-System zu verwalten. Mit der Konsole verwalten Sie das System einschließlich der physischen Maschinen (PMs), virtuellen Maschinen (VMs), Speicher und Netzwerke. Sie können hier auch Alarme und Protokolle anzeigen und weitere administrative Aufgaben ausführen.

Hinweise:

1. Nach einer Stunde ohne Aktivität wird die Sitzung beendet.
2. Es können höchstens zehn Sitzungen beim System angemeldet sein.
3. Kennwörter müssen der Kennwortrichtlinie des Systems entsprechen.
4. Sie können ein Anmeldebanner konfigurieren, um auf der ztC Console-Anmeldeseite benutzerdefinierten Inhalt anzuzeigen. Siehe Konfigurieren des Anmeldebanners.

So melden Sie sich bei der ztC Console an

1. Geben Sie die IP-Adresse des ztC Edge-Systems oder den vollständig qualifizierten Domänennamen (FQDN) in die Adressleiste eines Browsers ein:

   http://*IP-Adresse*

   ODER

   http://*FQDN*

   IP-Adresse ist die statische IP-Adresse des ztC Edge-Systems, die während der Bereitstellung angegeben wird.

   FQDN ist der FQDN, der dieser IP-Adresse entspricht.

2. Wenn die Anmeldeseite angezeigt wird, geben Sie Ihren **Benutzernamen** und Ihr **Kennwort** ein.

   Wenn Sie Ihr Kennwort vergessen haben, klicken Sie auf **Kennwort vergessen?**, um die Seite **Kennwort zurücksetzen** aufzurufen. Geben Sie die erforderlichen Informationen ein, um Ihr Kennwort zurückzusetzen.

   > **Hinweis**: Damit Ihr Kennwort zurückgesetzt werden kann, benötigen Sie ein E-Mail-Konto im System. Dazu muss eine E-Mail-Adresse in Ihrem lokalen Benutzerkonto konfiguriert sein (siehe Verwalten lokaler Benutzerkonten). Wenn Sie keine E-Mails empfangen können, wenden Sie sich an Ihren Systemadministrator, der die Zurücksetzung Ihres Kennworts anfordert. (Der Systemadministrator muss den Administrator des Host-Betriebssystems darum bitten, das Kennwort zu ändern. Der Administrator des Host-Betriebssystems ändert das Kennwort dann mithilfe von Befehlen auf dem primären Knoten.)

   So setzen Sie Ihr Kennwort zurück

   > **Hinweis**: Damit Sie die E-Mail zum Zurücksetzen Ihres Kennworts empfangen können, muss der Mail-Server konfiguriert sein. Siehe Konfigurieren des Mail-Servers.

   a. Wenn die Seite **Kennwort zurücksetzen** angezeigt wird, geben Sie Ihren **Benutzernamen** ein und klicken Sie auf **Weiter**. Es wird eine E-Mail an die E-Mail-Adresse gesendet, die in Ihrem lokalen Benutzerkonto angegeben ist. Diese E-Mail enthält einen Link zu einer Seite, auf der Sie Ihr Kennwort ändern können.

b. Öffnen Sie die E-Mail mit dem Link zum Zurücksetzen des Kennworts und klicken Sie auf den Link. Die Seite **Kennwort zurücksetzen** wird wieder angezeigt.

c. Geben Sie für **Neues Kennwort** und **Kennwort bestätigen** ein neues Kennwort ein. Das neue Kennwort muss der Kennwortrichtlinie des Systems entsprechen.

   Klicken Sie auf **Weiter**.

d. Es wird eine Seite mit der Meldung angezeigt, dass Ihr Kennwort erfolgreich zurückgesetzt wurde und Sie sich jetzt mit dem neuen Kennwort beim System anmelden können. Klicken Sie auf **Fertigstellen**.

3. Klicken Sie auf **ANMELDEN**.

Kennwortrichtlinie

In der Kennwortrichtlinie des System ist festgelegt, dass ein Kennwort die folgenden Kriterien erfüllen muss:

- Es muss mindestens acht Zeichen enthalten.
- Es muss Groß- und Kleinbuchstaben enthalten.
- Es darf nicht mit dem Benutzernamen übereinstimmen.

Hinweis: Das Intervall zwischen den Anmeldeversuchen beträgt 500 ms. Nach einem Anmeldeversuch müssen Sie also mindestens eine halbe Sekunde warten, bevor Sie es erneut versuchen können.

Verwandte Themen

Erstmaliges Anmelden bei der ztC Console

Die ztC Console

Verwenden der ztC Console

Bearbeiten der Benutzerinformationen

Bearbeiten Sie Ihre Benutzerinformationen (d. h. Ihr Benutzerprofil), indem Sie Ihren Benutzernamen, Ihre E-Mail-Adresse, Ihren tatsächlichen Namen oder Ihr Kennwort ändern.

So bearbeiten Sie Ihre Benutzerinformationen

1. Klicken Sie in der Konsole oben rechts auf Ihren Benutzernamen.

   Das Dialogfeld **Benutzer bearbeiten** wird angezeigt.

2. Bearbeiten Sie die folgenden Angaben:

   - **Benutzername**
   - **E-Mail-Adresse**
   - **Echtname**
   - **Kennwort**

     Hinweis: Kennwörter müssen der Kennwortrichtlinie des Systems entsprechen.

   - **Kennwort bestätigen**

3. Klicken Sie auf **Speichern**. (Oder klicken Sie auf **Abbrechen**, um die Änderungen zu verwerfen.)

Verwandte Themen

Die ztC Console

Verwenden der ztC Console

Die Seite „Dashboard“

Auf der Seite **Dashboard** wird eine Übersicht über die ausstehenden Alarme im ztC Edge-System angezeigt. Um diese Seite zu öffnen, klicken Sie im linken Navigationsbereich auf **Dashboard**.

Um zusätzliche Informationen zu ausstehenden Alarmen anzuzeigen, klicken Sie auf ein Alarmsymbol (zum Beispiel) im ztC Edge-Systemdiagramm oder klicken Sie auf einen Eintrag in der Liste der Alarme unter dem Systemdiagramm. Alarmlisten können auf Registerkarten wie **Alle**, **System** oder **Ignorierte** angezeigt werden, die je nach Alarm unter dem Systemdiagramm erscheinen können. Die Alarminformationen enthalten Folgendes:

- Die Komponente, die mit dem Problem verknüpft ist (zum Beispiel das ztC Edge-System, physische Maschine (PM) oder virtuelle Maschine (VM)).
- Eine Beschreibung der Aktivität oder der Aufgabe, die ein Eingreifen erfordert.
- Der Grund, weshalb das Problem behoben werden sollte, falls verfügbar.

Beheben Sie aktive Alarme so schnell wie möglich (siehe Auflösen ausstehender Alarme im Dashboard).

Das ztC Edge-Systemdiagramm

Das Systemdiagramm auf der Seite **Dashboard** ist eine grafische Darstellung des Systemstatus. Die primäre PM ist mit einem Sternchen gekennzeichnet. Alarmsymbole, falls vorhanden, stehen für informative oder kritische Alarme, die ein Eingreifen erfordern. Klicken Sie auf ein Alarmsymbol, um Informationen zu dem Alarm anzuzeigen.

Verwandte Themen

Die Seite „Physische Maschinen“

Die Seite „System“

Die Seite „Virtuelle Maschinen“

Auflösen ausstehender Alarme im Dashboard

Lösen Sie nach Abschluss der Systembereitstellung ggf. ausstehende Alarme auf, die auf der Dashboard-Seite aufgeführt sind.

So lösen Sie ausstehende Alarme auf

Sehen Sie auf der Dashboard-Seite der ztC Console nach Alarmen, die im unteren Teil der Seite aufgeführt sind. Sie haben die folgenden Optionen:

- Sie lösen den Alarm auf.

  Wenn zum Beispiel die Meldung **Zur bestmöglichen Unterstützung von Stratus sollten Sie den Supportbenachrichtigungsdienst aktivieren** angezeigt wird, aktivieren Sie den Supportbenachrichtigungsdienst.

- Klicken Sie auf **Ignorieren** (in der Spalte **Aktion**), um den Alarm zu ignorieren und aus der Liste zu entfernen. Geringfügige Alarme können einfach ignoriert statt aufgelöst werden. Wenn Sie auf **Ignorieren** klicken, wird der Alarm nicht mehr angezeigt.

  Wenn Sie einen ignorierten Alarm wieder in der Liste anzeigen möchten, klicken Sie über der Alarmliste auf **Ignoriert** und dann in der Spalte **Aktion** auf **Wiederherstellen.**

Verwandte Themen

Die Seite „Dashboard“

Die Seite „System“

Auf der Seite **System** werden Informationen zum ztC Edge-System angezeigt. Außerdem können Sie hier das System neu starten oder herunterfahren. Auf der Seite werden auch Statistiken und Ressourcenzuweisungen für das ztC Edge-System angezeigt. Um diese Seite zu öffnen, klicken Sie im linken Navigationsbereich auf **System**.

Auf der Seite **System** können Sie administrative Aufgaben ausführen, darunter:

- Neustarten des Systems
- Herunterfahren des Systems

Informationen zum Einschalten des Systems (an der physischen Konsole der PM)s finden Sie unter Einschalten des Systems.

Viele andere administrative Aufgaben im ztC Edge-System führen Sie mit der ztC Console aus. Weitere Informationen finden Sie unter Die ztC Console.

Anzeigen von Statistiken

Die Seite **System** enthält die folgenden Abschnitte mit Informationen und Statistiken zur Systemauslastung sowie zu den PMs und VMs:

- ***Systemname*** - Kreisdiagramme zeigen die CPU-Zuordnung, die Arbeitsspeicher-Zuordnung, Laufwerke (R/W) und die Netzwerkauslastung an.
- **Knoten0** und **Knoten1** (falls vorhanden) - Kreisdiagramme zeigen CPU-Nutzung, Arbeitsspeicher-Nutzung, Datenträgernutzung und Netzwerknutzung für jeden Knoten an. Für Datenträgernutzung und Netzwerknutzung können Sie das logische Laufwerk oder das Netzwerk auswählen, für das Sie Statistiken anzeigen möchten.

Verwandte Themen

Verwenden der ztC Console

Einschalten des Systems

Schalten Sie das System an der physischen Konsole jeder physischen Maschine (PM), auch als Knoten bezeichnet, ein. Dabei wird das System ordnungsgemäß gestartet, indem zuerst die Systemsoftware und dann die virtuellen Maschinen (VMs) im System gestartet werden. (Informationen zum Ausschalten eines Systems finden Sie unter Herunterfahren des Systems.)

Achtung: Wenn Sie das System zum ersten Mal einschalten, um es bereitzustellen, befolgen Sie die Anleitungen in der Bereitstellungsanleitung für Ihr System. (Bei Bedarf finden Sie weitere Informationen unter Bereitstellen des Systems.)

Hinweis: Falls eine PM von der Stromversorgung getrennt wird, weil Sie den Netzwerkstecker ziehen oder es einen Stromausfall gibt, ist jede PM in einem ztC Edge-System so eingestellt, dass sie beim Wiederherstellen der Stromversorgung automatisch eingeschaltet wird. Die Systemsoftware und die VMs werden automatisch gestartet.

So schalten Sie ein ztC Edge-System ein

1. Stellen Sie sicher, dass alle erforderlichen Netzwerkkabel an beide PMs angeschlossen sind.
2. Drücken Sie die Einschalttaste vorne an jeder PM im System.
3. Vergewissern Sie sich, dass die **PWR**-LED auf der Vorderseite jeder PM leuchtet.

Verwandte Themen

Die ztC Console

Die Seite „System“

Verwenden der ztC Console

Neustarten des Systems

Starten Sie das ztC Edge-System mit der ztC Console neu, um beide PMs sicher neu zu starten, ohne die VMs zu beeinträchtigen.

Achtung: Wenn Sie das ztC Edge-System mit einer anderen als der hier beschriebenen Methode neu starten (zum Beispiel Neustart der einzelnen PMs), kann es zu Datenverlusten kommen.

Hinweis: Sie können ein System, das für zwei PMs lizenziert ist, nur neu starten, wenn beide PMs ohne Probleme in Betrieb sind und sich nicht im Wartungsmodus befinden.

Voraussetzung: Vergewissern Sie sich bei einem System, das für zwei PMs lizenziert ist, vor dem Neustart, dass beide PMs in Betrieb sind.

So starten Sie das ztC Edge-System neu

1. Klicken Sie im linken Navigationsbereich auf **System**.
2. Klicken Sie auf die Schaltfläche **Neustart.** Mit einer Meldung werden Sie aufgefordert, den Neustart zu bestätigen. Klicken Sie zum Fortfahren auf **Ja**.

   Der Neustart kann bis zu 15 Minuten dauern. Sie können den Fortschritt im **Dashboard** und in der Titelleiste der ztC Console verfolgen. Die PMs des Systems werden nacheinander in den Wartungsmodus versetzt und dann aus dem Wartungsmodus genommen (Informationen zum Wartungsmodus finden Sie unter Wartungsmodus).
3. Überprüfen Sie, dass die PMs neu starten und alle VMs wie erwartet ausgeführt werden.

Nach dem Einleiten eines Neustarts zeigt eine Meldung in der Titelleiste den Status des Neustarts an. Falls erforderlich, können Sie den Neustart abbrechen, indem Sie in der Titelleiste auf **Neustart abbrechen** klicken.

Achtung: Wenn Sie einen Neustart abbrechen, bleibt das System im aktuellen Zustand und Sie müssen den betriebsfähigen Zustand manuell wiederherstellen.

Verwandte Themen

Die ztC Console

Die Seite „System“

Verwenden der ztC Console

Herunterfahren des Systems

Verwenden Sie die ztC Console, um das ztC Edge-System herunterzufahren. Dabei wird das System ordnungsgemäß heruntergefahren, indem zuerst die virtuellen Maschinen (VMs) und dann die physischen Maschinen (PMs) heruntergefahren werden. Verwenden Sie nur diese Methode, um das ztC Edge-System herunterzufahren. Vergewissern Sie sich bei einem System, das für zwei PMs lizenziert ist, vor dem Herunterfahren, dass beide PMs in Betrieb sind.

Achtung:

1. Beim Herunterfahren des ztC Edge-Systems werden die VMs außer Betrieb genommen, deshalb sollten Sie das System nur während eines geplanten Wartungszeitraums herunterfahren.
2. Wenn Sie das ztC Edge-System auf andere Weise herunterfahren (zum Beispiel durch Trennen der Stromversorgung von beiden PMs nacheinander), können Daten verloren gehen.

Hinweis: Wenn Sie das System herunterfahren, bleibt die Standby-Stromversorgung für das Lights Out Management (LOM) an, sofern Sie nicht das Stromkabel trennen oder die Stromversorgung ausschalten.

So fahren Sie das ztC Edge-System herunter

1. Vergewissern Sie sich bei einem System, das für zwei Knoten lizenziert ist, dass beide PMs in Betrieb sind, damit die Datenträger zwischen den Knoten synchronisiert werden können.
2. Klicken Sie im linken Navigationsbereich auf **System**.
3. Klicken Sie auf die Schaltfläche **Herunterfahren.** Es wird eine Warnung anzeigt: *Dabei wird das gesamte System heruntergefahren und mindestens eine VM wird beendet!* Klicken Sie zum Herunterfahren auf **Ja** oder klicken Sie auf **Nein**, um das Herunterfahren abzubrechen. Wenn Sie auf **Ja** klicken, wird eine zweite Warnung angezeigt, in der Sie aufgefordert werden, das Herunterfahren zu bestätigen. Klicken Sie zum Herunterfahren (erneut) auf **Ja** oder klicken Sie auf **Nein**, um das Herunterfahren abzubrechen.

Sie können den Prozess zum Teil im **Dashboard** und in der Titelleiste der ztC Console beobachten und sehen, wie die PMs des Systems nacheinander in den Wartungsmodus versetzt werden (Informationen zum Wartungsmodus finden Sie unter Wartungsmodus). Nachdem das System heruntergefahren wurde, ist die ztC Console jedoch nicht verfügbar und in der Titelleiste wird **Kommunikation unterbrochen** angezeigt.

Nach dem Herunterfahren des Systems geht die Verbindung zur Konsole verloren. Wenn das ztC Edge-System nicht vollständig heruntergefahren werden kann, kann möglicherweise eine VM nicht ordnungsgemäß heruntergefahren werden. Fahren Sie die VM wie folgt herunter:

- Verwenden Sie die VM-Konsole oder eine Remotedesktopanwendung, um sich bei der VM anzumelden. Verwenden Sie die Befehle des Betriebssystems, um die VM herunterzufahren.
- Melden Sie sich bei der ztC Console an. Klicken Sie im linken Navigationsbereich auf **Virtuelle Maschinen**, wählen Sie die VM aus und klicken Sie auf **Ausschalten**.

Verwandte Themen

Verwalten des Betriebs einer virtuellen Maschine

Die ztC Console

Die Seite „System“

Verwenden der ztC Console

Die Seite „Voreinstellungen“

Auf der Seite **Voreinstellungen** können Sie die ztC Edge-Systemeinstellungen konfigurieren. Um diese Seite zu öffnen, klicken Sie im linken Navigationsbereich auf **Voreinstellungen**.

In der folgenden Tabelle sind die Voreinstellungen aufgelistet und beschrieben.

Voreinstellung	Beschreibung
System	
Besitzerinformationen	Ermöglicht Ihnen, den Namen und die Kontaktinformationen für einen ztC Edge-Systemadministrator anzugeben und anzuzeigen. Diese Informationen werden auch in Antworten auf SNMP-Anfragen angegeben. Siehe Eingeben der Besitzerinformationen.
Produktlizenz	Ermöglicht Ihnen, die ztC Edge-Produktlizenz anzuzeigen und zu verwalten. Siehe Verwalten der Produktlizenz.
Softwareupdates	Damit können Sie die aktuelle Version der Systemsoftware anzeigen und prüfen, ob eine neuere Version verfügbar ist. Falls eine neue Version

Voreinstellung	Beschreibung
	verfügbar ist, können Sie sie herunterladen und die Versionshinweise lesen. Sie können auch festlegen, dass Benachrichtigungen gesendet werden, wenn eine Update verfügbar ist, und dass verfügbare Updates automatisch heruntergeladen werden. Siehe Verwalten von Softwareupdates.
IP-Konfiguration	Ermöglicht Ihnen, die IP-Adresse und die Netzwerkeinstellungen für das System anzugeben und anzuzeigen sowie ein System erneut bereitzustellen. Siehe Konfigurieren der IP-Einstellungen.
Quorumserver	Ermöglicht Ihnen die Anzeige vorhandener und neuer Quorumserver. Quorumserver bieten bei bestimmten Fehlern in der ztC Edge-Umgebung Zusicherung der Datenintegrität und automatische Neustartfunktionen. Siehe Quorumserver und Konfigurieren der Quorumserver.
Datum und Uhrzeit	Ermöglicht Ihnen die Anzeige der Systemzeit, das Festlegen der Werte durch das NTP (Network Time Protocol) (empfohlen) oder das manuelle Festlegen von Datum und Uhrzeit im System. Siehe Konfigurieren von Datum und Uhrzeit.
Mail-Server	Ermöglicht Ihnen, den Mail-Server zu konfigurieren, damit das ztC Edge-System eine E-Mail senden kann, zum Beispiel wenn ein Benutzer sein Kennwort zurücksetzen muss. Siehe Konfigurieren des Mail-Servers.
Administrative Tools	
Benutzer und Gruppen	Ermöglicht Ihnen, Benutzerkonten im ztC Edge-System hinzuzufügen, zu bearbeiten oder zu entfernen, Active Directory zu aktiveren (und Zugriff darauf zu gewähren) und einen Benutzer auszuwählen, um zu sehen, wann dessen Kennwort zuletzt geändert wurde. Administratoren können auf dieser Seite auch festlegen, dass ein ausgewählter Benutzer bei der nächsten Anmeldung sein Kennwort ändern muss. Siehe Konfigurieren von Benutzern und Gruppen

Voreinstellung	Beschreibung
Sichere Verbindung	Ermöglicht Ihnen, ausschließlich HTTPS-Verbindungen zum System zu aktivieren. Siehe Konfigurieren von sicheren Verbindungen.
VM-Gerätekonfiguration	Ermöglicht Ihnen, das Einlegen von virtuellen CDs (VCDs) oder das Anschließen von USB-Geräten bei allen VMs zu deaktivieren oder zu aktivieren. Siehe Konfigurieren von VM-Geräten.
IPtables-Sicherheit	Ermöglicht Ihnen, die IP-Paketfilterung mithilfe des administrativen Tools IPtables zu verwalten. Siehe Verwalten von IPtables.
Anmeldebanner-Hinweis	Ermöglicht Ihnen die Konfiguration eines Banners für die Anmeldeseite. Siehe Konfigurieren des Anmeldebanners.
ztC Advisor	Ermöglicht Ihnen die Aktivierung von ztC Advisor, damit Administratoren die Integrität des Systems remote im ztC Advisor-Dashboard beobachten können. Siehe Aktivieren von ztC Advisor.
Voreinstellungen speichern	Damit können Sie die Einstellungen von der Seite **Voreinstellungen** in einer Datei auf einem lokalen Computer oder in der Cloud speichern. Siehe Speichern und Wiederherstellen der Systemvoreinstellungen.
Voreinstellungen wiederherstellen	Damit können Sie die Einstellungen von der Seite **Voreinstellungen** aus einer Sicherungsdatei wiederherstellen. Siehe Speichern und Wiederherstellen der Systemvoreinstellungen.
Benachrichtigung	
e-Alerts	Ermöglicht Ihnen die Aktivierung von E-Mail-Meldungen (e-Alerts) für Systemadministratoren. Siehe Konfigurieren von e-Alerts.
SNMP-Konfiguration	Ermöglicht Ihnen die Aktivierung von SNMP-Anfragen und -Traps für die Remotesystemüberwachung. Siehe Konfigurieren der SNMP-Einstellungen.

Voreinstellung	Beschreibung
OPC-Konfiguration	Ermöglicht Ihnen, die Einstellungen für die Open Platform Communication (OPC) zu konfigurieren, damit die OPC-Serverfunktionalität aktiviert wird. Diese erlaubt Ihnen die Überwachung des ztC Edge-Systems zusammen mit anderen industriellen Anlagen. Siehe Konfigurieren der OPC-Einstellungen.
Remotesupport	
Supportkonfiguration	Ermöglicht Ihnen die Konfiguration des Remotezugriffs und der Benachrichtigungen. Der Remotezugriff berechtigt Ihren autorisierten Stratus-Servicemitarbeiter, sich zum Zweck der Fehlerbehebung remote beim System anzumelden. Wenn diese Funktion aktiviert ist, kann das ztC Edge-System Benachrichtigungen an Ihren autorisierten Stratus-Servicemitarbeiter senden, wenn es Probleme mit dem System gibt. Siehe Konfigurieren der Remotesupport-Einstellungen.
Proxykonfiguration	Ermöglicht Ihnen die Konfiguration der Proxyeinstellungen für das ztC Edge-System, falls Ihre Organisation für den Internetzugriff einen Proxyserver erfordert und Sie eine Dienstvereinbarung mit Stratus oder einem anderen autorisierten ztC Edge-Servicevertreter haben. Die Stratus Redundant Linux-Software verwendet Proxyserverinformationen für Supportbenachrichtigungen und den Remotesupportzugriff. Siehe Konfigurieren der Internetproxyeinstellungen.

Verwandte Themen

Die ztC Console

Verwenden der ztC Console

Eingeben der Besitzerinformationen

Geben Sie den Namen und die Kontaktinformationen für einen Administrator oder den Besitzer des ztC Edge-Systems ein, um diese Informationen zu Supportzwecken bereitzustellen.

Diese Kontaktinformationen sind in der ztC Console verfügbar und werden bei Simple Network Management Protocol (SNMP)-Anfragen bereitgestellt.

So geben Sie Systembesitzerinformationen an

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**.
2. Klicken Sie auf der Seite **Voreinstellungen** auf **Besitzerinformationen**.
3. Geben Sie die entsprechenden Informationen in die Felder **Voller Name**, **Rufnummer**, **E-Mail** und **Standortadresse** ein.
4. Klicken Sie auf **Speichern**.

Verwandte Themen

Die Seite „Voreinstellungen“

Die ztC Console

Verwalten der Produktlizenz

Mit den folgenden Aufgaben verwalten Sie die Produktlizenz für das System:

- Beziehen einer dauerhaften Lizenz während oder nach der Bereitstellung.
- Überprüfen des Status einer vorhandenen Lizenz, wodurch sie ggf. aktualisiert wird.
- Anzeigen aktueller Lizenzinformationen wie Status und Ablaufdatum.

Nach der ersten Installation eines Systems gilt für 30 Tage eine befristete Lizenz. (Eine befristete Lizenz wird in der Titelleiste mit **UNREGISTERED_TRIAL** als **Bestandskennung** angezeigt.) Sie müssen das System registrieren, wozu auch das Beziehen einer dauerhaften Lizenz gehört. Sie können das System direkt nach der ersten Bereitstellung oder später registrieren. Informationen zur Registrierung des Systems finden Sie unter Registrieren des Systems und Beziehen einer dauerhaften Lizenz.

Sobald ein System über eine dauerhafte Lizenz verfügt, prüft es alle 24 Stunden, ob auf dem Lizenzserver ein Update verfügbar ist, sofern das System mit dem Internet verbunden ist. Auch wenn das System keine Internetverbindung hat, können Sie die Lizenz aktualisieren und ihren Status überprüfen. Dazu müssen Sie eine Datei zwischen dem Standort der ztC Console (ohne Internetverbindung) und einem Standort mit Internetverbindung kopieren. Neben weiteren Methoden gibt es dafür die folgenden beiden Möglichkeiten:

- Ein USB-Stick – Sie verwenden einen USB-Stick auf einem Verwaltungscomputer (der eine Verbindung zum System herstellen kann) und auf einem Computer mit Internetverbindung.

- Ein mobiles Gerät, zum Beispiel Notebook oder Smartphone – Sie können ein mobiles Gerät zwischen einem Standort, an dem Sie sich bei der ztC Console anmelden können, und einem Standort mit Internetverbindung verwenden.

Wählen Sie unter das Verfahren, das am besten zu Ihren Anforderungen passt (klicken Sie ggf. auf das Dropdownsymbol).

So überprüfen Sie den Status einer Lizenz

Gehen Sie folgendermaßen vor, wenn das System mit dem Internet verbunden ist. Mit diesem Verfahren wird die Lizenz automatisch aktualisiert, falls erforderlich. Wenn das System keine Internetverbindung hat, folgen Sie den Anleitungen unter ***Auf einem System ohne Internetverbindung***. Wenn Sie eine Lizenz manuell aktualisieren müssen, lesen Sie ***So aktualisieren Sie eine neue Lizenz manuell***.

1. Klicken Sie in der Titelleiste der ztC Console auf ***bestandskennung*** (in **Bestandskennung:** ***bestandskennung***).

   Alternativ dazu klicken Sie bei einem registrierten System im Navigationsbereich auf der linken Seite auf **Voreinstellungen** und dann:

   a. Klicken Sie auf der Seite **Voreinstellungen** auf **Produktlizenz**.

   b. Bei **Online-Lizenzüberprüfung** klicken Sie auf **Lizenz jetzt überprüfen**.

2. Die Konsole zeigt den Status der Lizenz an (das Datumsformat variiert je nach Standort):

STATUS	Die Lizenz ist aktiviert und läuft nicht ab.
LETZTE ÜBERPRÜFUNG	*Tag, Monat tt*, 20*jj*, *Uhrzeit*
SERVICEABLAUF	*Tag, Monat tt*, 20*jj*, *Uhrzeit*
BESTANDSKENNUNG	*bestandskennung*
PRODUKT-UUID	*xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx*
FT aktiviert	*Ja_oder_Nein*
ALSR zulässig	*Ja_oder_Nein*
Gastüberwachung zulässig	*Ja_oder_Nein*
Speichern/Wiederherstellen der Systemvoreinstellungen zulässig	*Ja_oder_Nein*

Speichern/Wiederherstellen der Systemvoreinstellungen läuft ab	*Tag, Monat tt, 20jj, Uhrzeit_oder_ Niemals lizenziert*

So aktualisieren Sie eine neue Lizenz für ein registriertes System manuell

Auf einem registrierten System mit Internetverbindung wird die Lizenz automatisch aktualisiert. Sie können eine Lizenz aber auch manuell aktualisieren.

Auf einem System mit Internetverbindung

1. Klicken Sie in der Konsole im Navigationsbereich auf der linken Seite auf **Voreinstellungen**.
2. Klicken Sie auf der Seite **Voreinstellungen** auf **Produktlizenz**.
3. Klicken Sie auf die Leiste **Offline-Lizenzüberprüfung und manuelle Installation der Lizenz**, um verschiedene Optionen anzuzeigen, falls diese nicht bereits eingeblendet sind.
4. Bei **Offline-Lizenzüberprüfung über URL-Datei** klicken Sie auf **URL-Datei herunterladen** und speichern Sie die Datei.
5. Klicken Sie auf den Dateinamen. Ein Webbrowser wird geöffnet und der Stratus-Lizenzserver überprüft den Status der Lizenzdatei. Gegebenenfalls wird eine neue Lizenzschlüsseldatei automatisch heruntergeladen.
6. Klicken Sie dann auf **Hochladen**.

Auf einem System ohne Internetverbindung

Gehen Sie wie nachstehend beschrieben vor, um manuell auf einem registrierten System ohne Internetverbindung eine Lizenz zu überprüfen und eine neue Lizenz zu beziehen. Dazu müssen Sie eine Datei zwischen dem Standort der ztC Console (ohne Internetverbindung) und einem Standort mit Internetverbindung kopieren. Neben weiteren Methoden gibt es dafür die folgende Möglichkeit:

Auf einem Computer oder einem mobilen Gerät mit Zugriff auf die ztC Console

1. Wenn Sie einen Verwaltungscomputer verwenden, schließen Sie einen USB-Stick an einen USB-Anschluss an.

   Wenn Sie ein mobiles Gerät verwenden, stellen Sie sicher, dass es Zugriff auf die ztC Console hat.
2. Melden Sie sich bei der ztC Console an.
3. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**.
4. Klicken Sie auf der Seite **Voreinstellungen** auf **Produktlizenz**.

5. Klicken Sie auf die Leiste **Offline-Lizenzüberprüfung und manuelle Installation der Lizenz**, um verschiedene Optionen anzuzeigen, falls diese nicht bereits eingeblendet sind.
6. Bei **Offline-Lizenzüberprüfung über URL-Datei** klicken Sie auf **URL-Datei herunterladen**. Speichern Sie die Datei auf dem USB-Stick oder auf dem mobilen Gerät. Wenn Sie einen USB-Stick verwenden, trennen Sie ihn vom System. Gehen Sie zu einem Computer mit Internetverbindung.

Auf einem Computer mit Internetverbindung

1. Wenn Sie einen USB-Stick verwenden, schließen Sie ihn an einen USB-Anschluss des Computers mit Internetverbindung an.
2. Navigieren Sie zu der Datei, die Sie gespeichert haben, und klicken Sie auf den Dateinamen.
3. Ein Webbrowser wird geöffnet und der Stratus-Lizenzserver überprüft den Status der Lizenzdatei. Gegebenenfalls wird eine neue Lizenzschlüsseldatei automatisch heruntergeladen. Wenn Sie einen USB-Stick verwenden, kopieren Sie die neue Lizenzschlüssel darauf und nehmen Sie den USB-Stick dann aus dem Anschluss.
4. Gehen Sie wieder zu dem Computer mit Zugriff auf die Konsole.

Auf einem Computer oder einem mobilen Gerät mit Zugriff auf die ztC Console

1. Wenn Sie einen USB-Stick verwenden, schließen Sie ihn an einen USB-Anschluss des Verwaltungscomputers an.

   Wenn Sie ein mobiles Gerät verwenden, stellen Sie sicher, dass es Zugriff auf die ztC Console hat.
2. Klicken Sie in der Konsole im Navigationsbereich auf der linken Seite auf **Voreinstellungen**.
3. Klicken Sie auf der Seite **Voreinstellungen** auf **Produktlizenz**.
4. Klicken Sie auf die Leiste **Offline-Lizenzüberprüfung und manuelle Installation der Lizenz**, um verschiedene Optionen anzuzeigen, falls diese nicht bereits eingeblendet sind.
5. Bei **Aktivierte Lizenz auf dem System installieren** klicken Sie auf **Datei auswählen** und navigieren Sie zum Speicherort, an dem Sie die Datei gespeichert haben.
6. Wählen Sie die Datei aus, klicken Sie auf **Öffnen** und dann auf **Hochladen**, um die Datei an das System hochzuladen.

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Verwalten von Softwareupdates

Sie können Softwareupdates verwalten, indem Sie die aktuelle Versionsnummer der Systemsoftware überprüfen und nachsehen, ob ein Softwareupdate verfügbar ist. Wahlweise können Sie auch Folgendes aktivieren:

- Es wird eine Meldung an die Seite **Alarmverlauf** gesendet wird, wenn ein Update der Systemsoftware verfügbar ist.
- Eine Benachrichtung per E-Mail (e-Alert) wird an einen Systemadministrator gesendet, wenn ein Update der Systemsoftware verfügbar ist.
- Das System lädt das Update automatisch herunter (installiert es aber nicht).

Wenn Sie das System so konfigurieren, dass es automatisch nach Updates suchen soll, prüft das System jeden Tag gegen Mitternacht Ortszeit, ob Updates verfügbar sind. Wenn ein Update verfügbar ist, lädt das System in einen Staging-Bereich des Systems herunter, kurz nachdem verfügbare Updates gesucht wurden. Ist der Download in den Staging-Bereich erfolgreich und wurde dies konfiguriert, sendet das System einen Meldung an die Seite **Alarmverlauf** und/oder einen e-Alert mit dem Hinweis, dass die Software installiert werden kann. Wenn der Download fehlschlägt, wird das Update entfernt.

Voraussetzung: Wenn Sie möchten, dass Systemadministratoren e-Alerts erhalten, wenn ein Update verfügbar ist, müssen Sie den Mail-Server und e-Alerts konfigurieren, falls Sie dies noch nicht getan haben. Siehe Konfigurieren des Mail-Servers und Konfigurieren von e-Alerts.

So verwalten Sie Softwareupdates

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf der Seite **Voreinstellungen** auf **Softwareupdates** (unter **System**).
3. Die Liste **Verfügbare Updates der Systemsoftware** mit den folgenden Informationen wird eingeblendet:

- Versionsnummer der aktuellen Systemsoftware
- Versionsnummer der neuen Version der Systemsoftware, falls verfügbar

Wen eine neu Version der Systemsoftware verfügbar ist, klicken Sie auf einen der folgenden Links:

- **Software herunterladen** – Klicken Sie auf diesen Link, um die verfügbare Version herunterzuladen.
- **Versionshinweise anzeigen** – Klicken Sie auf diesen Link, um die Versionshinweise sowie das vollständige Benutzerhandbuch für die verfügbare Version aufzurufen.

4. **Updates der Systemsoftware verwalten** wird mit den folgenden Optionen eingeblendet:
   - **Benachrichtigung, wenn ein Update der Systemsoftware verfügbar ist** – Wählen Sie diese Option, wenn Sie eine Nachricht über ein verfügbares Update an die Seite **Alarmverlauf** senden möchten. Wenn Sie möchten, dass Systemadministratoren per E-Mail benachrichtigt werden, wenn ein Update der Systemsoftware verfügbar ist, müssen Sie e-Alerts konfigurieren.
   - **Updates der Systemsoftware automatisch herunterladen, sobald sie verfügbar sind. (Sie werden nur heruntergeladen, NICHT installiert)** – Wählen Sie diese Option aus, wenn das System neue Updates der Systemsoftware automatisch herunterladen soll, sobald sie verfügbar sind. Nachdem die Software heruntergeladen wurde, ist sie als Upgrade-Kit auf der Seite **Upgrade-Kits** verfügbar und Sie können sie installieren. Weitere Informationen finden Sie unter Die Seite „Upgrade-Kits“ und Upgrade der Stratus Redundant Linux-Software mit einem Upgrade-Kit.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

Die Seite „Alarmverlauf“

Konfigurieren der IP-Einstellungen

Konfigurieren Sie Internet Protocol (IP)-Einstellungen für das ztC Edge-System, um die IP-Adresse des Systems und der Knoten festzulegen oder zu ändern. Außerdem können Sie so Werte für Einstellungen wie Netzwerkmaske, Gatewayadresse und Domain Name System (DNS)-Server festlegen. (Sie ändern die Netzwerkeinstellungen auch, wenn Sie ein System mit der Schaltfläche **Erneut bereitstellen** erneut bereitstellen wie unter Erneutes Bereitstellen eines ztC Edge-Systems.)

Während und direkt nach der Bereitstellung konfigurieren Sie IP-Adressen für das System. Bei einem System, das für zwei Knoten lizenziert ist, konfigurieren Sie drei IP-Adressen: eine für das System und eine

für jeden Knoten (Knoten0 und Knoten1). Bei einem System, das für einen Knoten lizenziert ist, konfigurieren Sie zwei IP-Adressen: eine für das System und eine für den Knoten (Knoten0). Sie können die IP-Adressen und andere IP-Einstellungen nach der Bereitstellung ändern, indem Sie wie nachstehend beschrieben vorgehen. Sie müssen eine statische IPv4-Adresse für das ztC Edge-System angeben.

Warnungen:

1. Ändern Sie die Einstellungen der IP-Konfiguration, besonders bei Systemen mit laufenden VMs, nicht ohne Beratung und Kenntnis durch Ihren Netzwerkadministrator. Andernfalls könnte der Zugriff auf das System und die VMs unter Umständen nicht mehr möglich sein.
2. Wenn Sie die **Statische System-IP-Adresse** ändern, werden alle MAC-Adressen, die den VMs automatisch zugewiesen wurden, geändert, weil die Stratus Redundant Linux-Software die MAC-Adressen für die VMs basierend auf der System-IP-Adresse generiert. Um Änderungen an der MAC-Adresse einer virtuellen Maschine zu verhindern (zum Beispiel, um Softwareanwendungen zu unterstützen, die basierend auf der MAC-Adresse lizenziert werden), legen Sie eine dauerhafte MAC-Adresse fest wie unter Zuweisen einer spezifischen MAC-Adresse zu einer virtuellen Maschine beschrieben.
3. Sie müssen die ztC Console verwenden, um IP-Adressen zu ändern. Verwenden Sie dazu keine Linux-Tools.

Hinweise:

1. Welches Verfahren Sie zur Konfiguration der IP-Einstellungen verwenden, ist davon abhängig, ob das ztC Edge-System in demselben Subnetz bleibt oder in ein neues Subnetz verschoben wird. Wenn Sie ein ztC Edge-System in ein neues Netzwerk verschieben müssen, stellen Sie das System *erneut bereit*, um die Netzwerkeinstellungen zu entfernen, bevor Sie es verschieben, wie unter Erneutes Bereitstellen eines ztC Edge-Systems beschrieben.
2. Das Ändern der IP-Einstellungen für ein neues Subnetz beinhaltet normalerweise das Ändern der physischen Netzwerkverbindungen des Knotens (zum Beispiel das Trennen und Wiederanschließen von Netzwerkkabeln, falls die PMs an einen anderen Platz versetzt werden). Bevor Sie Kabel von Knoten trennen, müssen Sie die Knoten herunterfahren. Hierfür haben Sie die Option, die Schaltfläche **Speichern und herunterfahren** im Abschnitt **IP-Konfiguration** auf der Seite **Voreinstellungen** zu verwenden.
3. In einem System, das für einen Knoten lizenziert ist, werden auf der Seite **IP-Konfiguration** die Einstellungen für nur einen Knoten angezeigt.

So ändern Sie die System- und/oder Knoten-IP-Einstellungen mit dem System im selben Subnetz

Das ztC Edge-System und alle virtuellen Maschinen (VMs) bleiben während dieses Verfahrens in Betrieb; die ztC Console verliert jedoch kurz die Verbindung zum System, wenn Sie die IP-Adresse des Systems ändern. Nach 1-2 Minuten haben Sie wieder Zugriff auf die ztC Console unter der neuen System-IP-Adresse. (Sie können die IP-Adressen der Knoten einzeln ändern, die Konsolenverbindung geht dabei nicht verloren.)

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf **IP-Konfiguration**.
3. Geben Sie in das Feld **Statische System-IP-Adresse** die statische System-IP-Adresse ein, die Ihnen Ihr Netzwerkadministrator mitgeteilt hat.
4. Klicken Sie auf die Schaltfläche **Statisch** und geben Sie gültige, eindeutige Werte für **Primärer DNS** und **Sekundärer DNS** ein.
5. Überprüfen Sie, ob der angezeigte Wert für **Netzmaske** korrekt ist.

6. Für **Knoten0** und **Knoten1** (falls vorhanden) geben Sie die passenden Werte für **IP-Adresse** und **Gateway-IP** ein.
7. Klicken Sie auf **Speichern**, um die Werte zu übernehmen (oder klicken Sie auf **Zurücksetzen**, um die vorherigen Werte wiederherzustellen).

   Wenn Sie die IP-Adresse des Systems geändert haben, wird die Meldung **System-IP-Adresse wurde aktualisiert** angezeigt. Nach einer kurzen Verzögerung erfolgt automatisch die Umleitung an die neue IP-Adresse des Systems.

Verwandte Themen

Bereitstellung

Beziehen der System-IP-Informationen

Erstmaliges Anmelden bei der ztC Console

Die Seite „Voreinstellungen“

Die ztC Console

Verwenden der ztC Console

Konfigurieren der Quorumserver

Wenn Sie sich zum ersten Mal beim ztC Edge-System anmelden, konfigurieren Sie Quorumserver.

Voraussetzungen:

1. Damit Sie einen Quorumserver konfigurieren können, benötigen Sie ein System, das für zwei Knoten lizenziert ist.
2. Lesen Sie vor der Konfiguration der Quorumserver die Themen Quorumserver und Erstellen einer ALSR-Konfiguration (in denen Quorumserver behandelt werden).

Hinweise:

1. Damit eine VM Änderungen an der Quorumserverkonfiguration erkennt, müssen Sie die VM neu starten, indem Sie sie herunterfahren und dann wieder starten. Siehe Herunterfahren einer virtuellen Maschine und Starten einer virtuellen Maschine.
2. Windows-Updates auf einem Quorumserver können den Serverbetrieb unterbrechen, wovon das Verhalten bei der Wiederherstellung nach einem Ausfall betroffen ist. Auf Quorumservern sollten Sie Windows-Updates so planen, dass sie in Wartungszeiten ausgeführt werden, oder deaktivieren.

So konfigurieren Sie Quorumserver

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf **Quorumserver**.
3. Klicken Sie auf **Quorumserver hinzufügen**.
4. Geben Sie im Dialogfeld **Bevorzugten Quorumserver hinzufügen** die folgenden Werte ein (falls bereits ein bevorzugter Quorumserver vorhanden ist, wird das Dialogfeld **Alternativen Quorumserver hinzufügen** angezeigt):
   - **DNS oder IP-Adresse** - Geben Sie den vollständig qualifizierten **DNS**-Hostnamen oder die **IP-Adresse** für den bevorzugten Quorumserver ein.
   - **Port** (der Standardwert ist 4557) - Geben Sie die Portnummer ein, falls sie sich vom Standardwert unterscheidet.

   Klicken Sie auf **Speichern**, um die Werte zu speichern.
5. Wiederholen Sie die Schritte 4 und 5, um einen zweiten, alternativen Quorumserver zu konfigurieren. Stratus empfiehlt, zwei Quorumserver zu konfigurieren.
6. Um den Quorumdienst zu aktivieren, markieren Sie das Kontrollkästchen **Aktiviert** und klicken Sie auf **Speichern**.

So entfernen Sie einen Quorumserver

Achtung: Wenn Sie den bevorzugten Quorumserver entfernen, wird der alternative Quorumserver zum bevorzugten Quorumserver. Falls kein alternativer Quorumserver vorhanden ist, wird der Quorumdienst beim Entfernen des bevorzugten Quorumservers automatisch deaktiviert.

1. Navigieren Sie zur Seite **Voreinstellungen** der ztC Console.
2. Klicken Sie auf **Quorumserver**.
3. Suchen Sie den Eintrag für den Quorumserver, den Sie entfernen möchten.
4. Klicken Sie in der rechten Spalte auf **Entfernen**.

Hinweis: Falls eine VM den Quorumserver, den Sie entfernen, verwendet, müssen Sie die VM neu starten, sodass sie den Quorumserver nicht mehr erkennt, damit der Vorgang zum Entfernen abgeschlossen werden kann.

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Konfigurieren von Datum und Uhrzeit

Wenn Sie sich zum ersten Mal beim ztC Edge-System anmelden, konfigurieren Sie das Datum und die Uhrzeit, um den NTP-Dienst (Network Time Protocol) zu aktivieren. Wenn Sie den NTP-Dienst verwenden, wird die Systemuhr automatisch eingestellt und somit wird gewährleistet, dass die Systemzeit nicht von der tatsächlichen Zeit abweicht.

Achtung: Wenn Sie die Einstellungen für Datum und Uhrzeit ändern, kann die primäre physische Maschine (PM) neu gestartet und die sekundäre PM (falls vorhanden) heruntergefahren werden, falls die Systemzeit von der tatsächlichen Zeit abweicht. Alle virtuellen Maschinen (VMs) werden beendet und Geschäftsprozesse werden unterbrochen, bis der Neustart abgeschlossen wurde.

Hinweis: Die Uhr wechselt zwischen Zeitzonen, wenn VMs migriert oder neu gestartet werden. So stellen Sie sicher, dass die Zeitzone von VMs nicht geändert wird:

- Legen Sie für alle VMs die Zeitzone fest, die für das ztC Edge-System eingestellt wurde.
- Konfigurieren Sie alle VMs so, dass sie dieselben NTP-Server wie das ztC Edge-System verwenden.

So konfigurieren Sie die Einstellungen für Datum und Uhrzeit

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf der Seite **Voreinstellungen** auf **Datum und Uhrzeit**.
3. Im Bildschirm **Datum und Uhrzeit** ist die Standardeinstellung für **Zeitzone konfigurieren** die Zeitzone **America, New York**. Wählen Sie die für Ihren Standort passende Zeitzone aus.
4. Wählen Sie für **Datum und Uhrzeit konfigurieren** eine der folgenden Optionen:
   - **Automatisch (empfohlen)** aktiviert den NTP-Dienst. Geben Sie die NTP-Serveradressen in den Textbereich ein; jeweils eine pro Zeile. Wenn Sie mehrere NTP-Server angeben, ermöglicht dies Redundanz.
   - **Manuell** ermöglicht Ihnen die manuelle Eingabe der Einstellungen.

     Hinweis: Wenn Sie die Zeit manuell einstellen, kann die ztC Edge-Systemzeit von der tatsächlichen Zeit abweichen.
5. Klicken Sie auf **Speichern** (oder auf **Zurücksetzen**, um die zuvor gespeicherten Werte wiederherzustellen).

Wenn das System wegen einer Zeitabweichung neu gestartet werden muss, wird in der Titelleiste der ztC Console eine entsprechende Meldung angezeigt. In diesem Fall startet die primäre physische Maschine (PM) neu und die sekundäre PM (falls vorhanden) wird heruntergefahren. Während die primäre PM neu gestartet wird, verlieren Sie die Verbindung zur ztC Console. Nach Abschluss des Neustarts stellt die PM die Verbindung zur Konsole wieder her. Sie erhalten dann einen Alarm, der Sie darüber informiert, dass Sie die sekundäre PM neu starten können.

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Konfigurieren des Mail-Servers

Konfigurieren Sie den Mail-Server, damit das ztC Edge-System eine E-Mail senden kann, zum Beispiel wenn ein Benutzer sein Kennwort zurücksetzen muss.

So konfigurieren Sie den Mail-Server

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **System** auf **Mail-Server**.
3. Klicken Sie auf das Feld **Mail-Server aktivieren**. Es werden Felder für die Eingabe oder Auswahl der folgenden Einstellungen eingeblendet:
   - **SMTP-Server** (erforderlich) - Geben Sie den Namen des SMTP-Servers (Simple Mail Transfer Protocol) ein, der in Ihrem Unternehmen zum Versenden von E-Mails verwendet wird.
   - **Portnummer** (optional) - Geben Sie die Portnummer ein, die beim Senden von e-Alerts verwendet werden soll. Wenn keine Portnummer angegeben wird, wird der Standard-SMTP-Port 25 verwendet. (Weitere Informationen zu allen Ports einschließlich des SMTP-Ports finden Sie in der Knowledge Base im Artikel *TCP and UDP ports used by ztC Edge* (KB-9357). Siehe Zugriff auf Artikel in der Knowledge Base.)
   - **E-Mail-Adresse des Absenders** - Aktivieren Sie die Zustellung von e-Alerts, indem Sie eine gültige Absender-E-Mail-Adresse eingeben, falls einer der folgenden Fälle zutrifft:
     - Sie haben keinen DNS-Server im ztC Edge-System angegeben **und** Ihr SMTP-Server ist nicht dafür konfiguriert, Domänenliterale (`Von`-Adressen in der Form `noreply@`*`IP-Adresse`*) zu akzeptieren.
     - Sie möchten e-Alerts von einer anderen E-Mail-Adresse absenden (zum Beispiel noreply@firma.com).

   Jede E-Mail-Adresse, die der SMTP-Server akzeptiert, ist ausreichend.

- **Verschlüsselte Verbindung** - Wählen Sie im Pulldownmenü das Verschlüsselungsprotokoll, dass der SMTP-Server erfordert:
  - **Keine**, wenn keine Verschlüsselung verwendet wird. Standardmäßig wird die Portnummer 25 verwendet.
  - **TLS** für das Protokoll Transport Layer Security (TLS). Für TLS empfiehlt Stratus die Verwendung von 587 als **Portnummer**, obwohl standardmäßig 25 verwendet wird.
  - **SSL** für das Protokoll Secure Sockets Layer (SSL). Für SSL empfiehlt Stratus die Verwendung von 465 als **Portnummer**, obwohl standardmäßig 25 verwendet wird.
- **Authentifizierung aktivieren** - Aktivieren Sie dieses Kontrollkästchen, wenn der SMTP-Server eine Authentifizierung erfordert. Geben Sie den **Benutzernamen** und das **Kennwort** für das SMTP-Konto ein.

  Wenn Sie kein Kennwort eingeben, ist weiterhin das alte Kennwort erforderlich. Falls zuvor kein Kennwort verwendet wurde und Sie kein neues Kennwort eingeben, bleibt das Kennwortfeld leer.

4. Klicken Sie auf **Speichern** (oder auf **Zurücksetzen**, um die zuvor gespeicherten Werte wiederherzustellen).

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Konfigurieren von Benutzern und Gruppen

Auf der Seite **Benutzer und Gruppen** können Sie Benutzerkonten in Ihrem ztC Edge-System hinzufügen, bearbeiten oder entfernen oder Active Directory-Benutzern Zugriff gewähren. Sie können einen Benutzer auswählen und nachsehen, wann sein Kennwort zuletzt geändert wurde. Administratoren können auf dieser Seite auch festlegen, dass ein ausgewählter Benutzer bei der nächsten Anmeldung sein Kennwort ändern muss.

Um diese Seite zu öffnen, klicken Sie im linken Navigationsbereich auf **Voreinstellungen** und wählen dann auf der Seite **Voreinstellungen** unter **Administrative Tools** die Kategorie **Benutzer und Gruppen**.

So verwalten Sie lokale Benutzerkonten

Um einen neuen Benutzer hinzuzufügen, klicken Sie auf **Hinzufügen** rechts im oberen im unteren Fensterbereich. Um einen vorhandenen Benutzer zu bearbeiten, klicken Sie auf den Namen eines Benutzerkontos und dann auf **Bearbeiten** oder **Entfernen**.

Um zu erfahren, wann ein Benutzer zuletzt sein Kennwort geändert hat, sehen Sie in der Spalte **Zeitpunkt der letzten Kennwortänderung** für einen ausgewählten Benutzer nach. Um durchzusetzen, dass ein Benutzer sein Kennwort ändern muss, wenn er sich das nächste Mal anmeldet, kann ein Administrator den Benutzer auswählen und dann auf **Kennwortgültigkeit beenden** klicken.

Weitere Informationen finden Sie unter Verwalten lokaler Benutzerkonten.

So verwalten Sie Domänenbenutzerkonten

Informationen zum Aktivieren des Active Directory-Diensts in Ihrem ztC Edge-System finden Sie unter Konfigurieren von Active Directory. Um Domänenbenutzern die Berechtigung zum Verwalten des ztC Edge-System zu erteilen oder zu entziehen, lesen Sie Verwalten von Domänenbenutzerkonten.

> **Hinweis**: Wenn Sie als Administrator bei einem System angemeldet sind, auf dem Active Directory-Benutzer oder -Gruppen konfiguriert sind, wird die Schaltfläche **Zugriff gewähren** oben rechts auf der Seite **Benutzer und Gruppen** eingeblendet. Mit einem Klick auf die Schaltfläche **Zugriff gewähren** rufen Sie den Assistenten „Zugriff gewähren“ auf. Die Verwendung dieses Assistenten wird unter Verwalten von Domänenbenutzerkonten beschrieben.

So sortieren und suchen Sie Benutzerkonten

Wenn Sie sehr viele Konten haben, können Sie auf eine Spaltenüberschrift klicken, um die Konten nach dem entsprechenden Parameter zu sortieren. Sie können Konten nach **Typ**, **Benutzername**, **Echtname**, **E-Mail-Adresse** oder **Rolle** sortieren.

Verwandte Themen

Verwalten von Domänenbenutzerkonten

Verwalten lokaler Benutzerkonten

Konfigurieren von Active Directory

Sicherheitsverstärkung

Verwalten lokaler Benutzerkonten

Das Hinzufügen, Bearbeiten oder Entfernen von Benutzern, das Festlegen von Kennwörtern und das Zuweisen von Benutzerrollen zu lokalen Benutzerkonten führen Sie auf der Seite **Benutzer und Gruppen** der ztC Console aus. Sie können auch einen Benutzer auswählen und nachsehen, wann sein Kennwort zuletzt geändert wurde. Administratoren können festlegen, dass ein ausgewählter Benutzer bei der nächsten Anmeldung sein Kennwort ändern muss. Sie können einem Benutzer, der kein Administrator ist, die Aufgabe (oder Berechtigung) *Einen Computer zur Domäne hinzufügen* zuweisen. (Informationen zum Erteilen oder Entziehen von Zugriffsberechtigungen für vorhandene Benutzerkonten in einer Active Directory-Domäne finden Sie unter Verwalten von Domänenbenutzerkonten.)

Lokale Benutzerkonten befinden sich auf dem ztC Edge-System statt auf einem zentralen Domänenserver. Sie finden lokale Konten auf der Seite **Benutzer und Gruppen**, indem Sie nach Einträgen mit der Kennzeichnung **Lokaler Benutzer** in der Spalte **Typ** suchen.

Es gibt folgende Benutzerrollen:

- **Administrator**: Vollständige Systemadministratorberechtigungen
- **Plattform-Manager**: Systemadministratorberechtigungen mit Ausnahme der Berechtigungen zum Hinzufügen, Bearbeiten und Entfernen von Benutzern
- **VM-Manager**: Berechtigung zum Verwalten von VMs (siehe Verwalten von virtuellen Maschinen mit ausführlichen Informationen)
- **Schreibgeschützt**: Berechtigung zum Anzeigen, aber nicht zum Ändern der Systemkonfiguration oder zum Installieren der Systemsoftware

Für die unten beschriebenen Verfahren öffnen Sie zunächst die Seite **Benutzer und Gruppen**: Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen, und wählen Sie dann unter „Administrative Tools“ die Kategorie **Benutzer und Gruppen**.

So fügen Sie ein Benutzerkonto hinzu

1. Klicken Sie im unteren Fensterbereich auf **Hinzufügen**.
2. Wählen Sie im Dropdownmenü **Rolle** den Eintrag **Administrator**, **Plattform-Manager**, **VM-Manager** oder **Schreibgeschützt**.
3. Geben Sie Werte in die Felder **Benutzername**, **Kennwort** (und **Kennwort bestätigen**), **E-Mail-Adresse** und **Echtname** ein. Benutzernamen können 1 bis 64 Zeichen enthalten;

Leerzeichen können nicht verwendet werden. Kennwörter müssen der Kennwortrichtlinie des Systems entsprechen.

4. Klicken Sie auf **Speichern**.

So bearbeiten Sie ein Benutzerkonto

1. Wählen Sie das Konto aus, das Sie bearbeiten möchten.
2. Klicken Sie im unteren Fensterbereich auf **Bearbeiten**.
3. Bearbeiten Sie die Benutzerinformationen wie erforderlich. Beispiel: Um die Rolle eines Benutzers zu ändern, wählen Sie im Dropdownmenü **Rolle** den Eintrag **Administrator**, **Plattform-Manager**, **VM-Manager** oder **Schreibgeschützt**.
4. Klicken Sie auf **Speichern**.

So setzen Sie die Kennwortänderung für einen Benutzer durch

1. Wählen Sie den Benutzer aus, dessen Kennwort ungültig werden soll.
2. Klicken Sie auf **Kennwortgültigkeit beenden**.
3. Klicken Sie im Bestätigungsfenster auf **Ja**.

So weisen Sie einem Benutzer, der kein Administrator ist, „Einen Computer zur Domäne hinzufügen“ zu

1. Fügen Sie einen Benutzer, der kein Administrator ist, zum AD-Server hinzu und delegieren Sie die Aufgabe (oder Berechtigung) **Einen Computer zur Domäne hinzufügen** an den Benutzer. Weitere Informationen finden Sie in der Dokumentation zum AD-Server.
2. Bearbeiten Sie im ztC Edge-System die Datei `/etc/resolv.conf`, um die IP-Adresse des AD-Domaincontrollers hinzuzufügen. Die folgende Zeile ist ein Beispiel:

   ```
   nameserver 123.456.28.910
   ```

3. Aktivieren Sie in der ztC Console AD, falls es nicht schon aktiviert ist. Siehe Konfigurieren von Active Directory.

So entfernen Sie ein Benutzerkonto

1. Wählen Sie das Konto aus, das Sie entfernen möchten.
2. Klicken Sie im unteren Navigationsbereich auf **Entfernen**.
3. Klicken Sie im Bestätigungsfenster auf **Ja**.

Hinweise:

1. Das **Admin**-Standardkonto können Sie nicht löschen, Sie sollten aber den Namen und das Kennwort dieses Kontos ändern, indem Sie das Konto bearbeiten.
2. Sie müssen für jedes Benutzerkonto, auch **admin**, eine E-Mail-Adresse angeben, damit die Funktion zum Zurücksetzen des Kennworts verwendet werden kann. Wenn ein Benutzerkonto keine E-Mail-Adresse enthält und der betreffende Benutzer in der Konsole auf den Link **Kennwort vergessen?** klickt, sendet das System eine E-Mail an **benutzer@beispiel.com**.

Verwandte Themen

Konfigurieren von Active Directory

Verwalten von Domänenbenutzerkonten

Konfigurieren von Benutzern und Gruppen

Verwalten von Domänenbenutzerkonten

Sie können Benutzerkonten einer Active Directory-Domäne (AD) Zugriffsrechte für die ztC Console erteilen. Domänenbenutzerkonten werden auf einem zentralen AD-Domänenserver verwaltet statt im lokalen ztC Edge-System.

Nachdem Sie Domänenkonten Zugriffsrechte erteilt haben, können Sie den Assistenten „Zugriff gewähren“ (auf der Seite „Benutzer und Gruppen“) verwenden, um die AD-Konten mit Zugriffsberechtigung anzuzeigen, zu verwalten und zu sortieren.

Voraussetzungen: Sie müssen das ztC Edge-System zur Active Directory-Domäne hinzufügen, bevor Sie Domänenkonten verwalten können. (Siehe Konfigurieren von Active Directory.) Falls Active Directory nicht konfiguriert ist oder wenn der Benutzer, der sich bei der Benutzeroberfläche angemeldet hat, keine Administratorrechte hat, erscheint die Schaltfläche „Zugriff gewähren“ auf der Seite „Benutzer und Gruppen“ abgeblendet.

Öffnen Sie für die folgenden Verfahren den **ztC Edge-Assistenten „Zugriff gewähren“**:

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.

2. Klicken Sie unter „Administrative Tools“ auf **Benutzer und Gruppen**.
3. Klicken Sie auf **Zugriff gewähren**.

So erteilen Sie einem Domänenbenutzerkonto Zugriffsrechte

1. Geben Sie im Assistenten **ztC Edge - Zugriff gewähren** den Suchbereich im Menü **Suchen** an.
2. Geben Sie den gesuchten Namen oder die Gruppe ein. Unvollständige Namen sind zulässig.
3. Klicken Sie auf **Suchen**.
4. Klicken Sie auf das grüne Pluszeichen (**+**) neben den Benutzern oder Gruppen, die Sie als globale Benutzer oder Gruppen für die ztC Console des Systems hinzufügen möchten.
5. Verwenden Sie die Dropdownmenüs in der Spalte „Rolle“, um den Benutzern oder Gruppen, denen Sie gerade Zugriff gewährt haben, eine Rolle zuzuweisen. Sie können die folgenden Rollen zuweisen:
   - **Administrator** - Ermöglicht die Ausführung sämtlicher Aufgaben für die Systemverwaltung.
   - **Plattformadministrator** - Aktiviert Administratorberechtigungen mit Ausnahme der Berechtigung zum Verwalten von Benutzerkonten.
   - **VM-Manager** - Berechtigt zum Verwalten von VMs (siehe Verwalten von virtuellen Maschinen mit ausführlichen Informationen)
   - **Schreibgeschützt** - Erlaubt den Lesezugriff, aber nicht die Ausführung von Verwaltungsaufgaben.
6. Klicken Sie auf **Fertigstellen**. Die neuen Domänenbenutzer werden im Assistenten „Zugriff gewähren“ angezeigt.

So entfernen Sie Zugriffsrechte von einem Domänenbenutzerkonto

1. Klicken Sie im Assistenten **ztC Edge - Zugriff gewähren** auf das Kontrollkästchen neben den Benutzern oder Gruppen, die Sie entfernen möchten.
2. Klicken Sie auf **Zugriff verweigern** und dann auf **Fertigstellen**.

Verwandtes Thema

Konfigurieren von Active Directory

Konfigurieren von Active Directory

Konfigurieren Sie Active Directory für das ztC Edge-System, um vorhandene Benutzer oder Gruppen aus einer Active Directory-Domäne für die Anmeldung bei der ztC Console mit ihren Active Directory-Anmeldeinformationen zu autorisieren.

Nachdem Sie das ztC Edge-System einer Active Directory-Domäne hinzugefügt haben, können Sie Domänenbenutzern mithilfe des Assistenten **Zugriff gewähren** Administratorrechte zuweisen. Sie starten diesen Assistenten von der Seite **Benutzer und Gruppen** (siehe Konfigurieren von Benutzern und Gruppen).

So fügen Sie das ztC Edge-System einer Active Directory-Domäne hinzu

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf **Benutzer und Gruppen**.
3. Klicken Sie auf die Schaltfläche **Active Directory aktivieren** im unteren Fensterbereich.
4. Geben Sie neben **Active Directory-Domäne** den Namen der zu verwendenden Domäne ein.
5. Klicken Sie auf eine der folgenden Optionen, um die automatische Zuweisung der Rolle „Alle“ zu verhindern oder zuzulassen:
   - **Verhindern, dass allen AD-Benutzern automatisch die Rolle „Alle“ zugewiesen wird** (Standardeinstellung).
   - **Zulassen, dass alle AD-Benutzer authentifiziert werden und ihnen die Rolle „Alle“ zugewiesen wird**.
6. Klicken Sie auf **System zu Active Directory hinzufügen**.
7. Sie müssen den **Benutzernamen** und das **Kennwort** eines Active Directory-Administrators eingeben, um dieses ztC Edge-System zur Domäne hinzuzufügen.
8. Klicken Sie auf **Hinzufügen**.
9. Weisen Sie Domänenbenutzern auf der Seite **Benutzer und Gruppen** Administratorrechte zu wie unter Verwalten von Domänenbenutzerkonten beschrieben.

So entfernen Sie ein ztC Edge-System aus einer Active Directory-Domäne

1. Klicken Sie in der ztC Console im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf **Benutzer und Gruppen**.

3. Klicken Sie auf **System aus Active Directory entfernen** im unteren Fensterbereich.
4. Geben Sie einen **Benutzernamen** und ein **Kennwort** ein, mit denen Sie über Administratorrechte innerhalb der Domäne verfügen.
5. Klicken Sie auf **Entfernen**.

So deaktivieren Sie die Domänenauthentifizierung

1. Klicken Sie in der ztC Console im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf **Benutzer und Gruppen**.
3. Klicken Sie auf **Active Directory deaktivieren** im unteren Fensterbereich.

> **Hinweis**: Indem Sie Active Directory deaktivieren, verhindern Sie, dass die Domänenauthentifizierung für die Autorisierung von Administratoren des ztC Edge-Systems verwendet wird; jedoch wird damit nicht das System aus der Domäne entfernt. Um die Domänenauthentifizierung wiederherzustellen, klicken Sie auf **Active Directory aktivieren**. Sie brauchen den Namen des Controllers nicht erneut einzugeben und müssen auch nicht auf der Seite **Benutzer und Gruppen** Domänenbenutzer wiederherstellen.

Verwandte Themen

Konfigurieren von Benutzern und Gruppen

Verwalten von Domänenbenutzerkonten

Verwalten lokaler Benutzerkonten

Die Seite „Voreinstellungen“

Die ztC Console

Sicherheitsverstärkung

Konfigurieren von sicheren Verbindungen

Aus Sicherheitsgründen lässt das ztC Edge-System standardmäßig nur HTTPS-Verbindungen zu. Wenn Sie HTTP-Verbindungen zulassen möchten, können Sie sichere Verbindungen konfigurieren.

> **Hinweis**:
> Wenn Sie im folgenden Verfahren das Kontrollkästchen neben **Nur HTTPS aktivieren/HTTP deaktivieren** aktivieren oder deaktivieren und dann auf **Speichern** klicken, meldet Sie das System automatisch von der ztC Console ab und Sie müssen sich erneut anmelden.

Wenn HTTPS-Verbindungen aktiviert sind, können Sie ein Skript verwenden, das ein benutzerdefiniertes Zertifikat auf der Hostmaschine installiert. Siehe So installieren Sie benutzerdefiniertes Zertifikat.

So aktivieren Sie HTTP- und HTTPS-Verbindungen

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **Administrative Tools** auf **Sichere Verbindung**.
3. Deaktivieren Sie das Kontrollkästchen neben **Nur HTTPS aktivieren/HTTP deaktivieren**.
4. Klicken Sie auf **Speichern**.

   Das System meldet Sie automatisch von der ztC Console ab und leitet den Browser zur HTTPS-Anmeldeseite. Um die HTTP-Anmeldeseite aufzurufen, müssen Sie **https** in der Adressleiste des Browsers manuell durch **http** ersetzen; dann können Sie sich anmelden.

Wenn das System HTTP- und HTTPS-Verbindungen zulässt und Sie nur HTTPS-Verbindungen erlauben möchten, müssen Sie das Kontrollkästchen aktivieren.

So aktivieren Sie nur HTTPS-Verbindungen

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **Administrative Tools** auf **Sichere Verbindung**.
3. Aktivieren Sie das Kontrollkästchen neben **Nur HTTPS aktivieren/HTTP deaktivieren**.
4. Klicken Sie auf **Speichern**.

   Das System meldet Sie automatisch von der ztC Console ab, leitet den Browser zur HTTPS-Anmeldeseite und Sie müssen sich erneut anmelden.

So installieren Sie ein benutzerdefiniertes Zertifikat

Wenn Sie ein benutzerdefiniertes Zertifikat installieren möchten, verwenden Sie das Skript `certificate_installer`. Mit diesem Skript können Sie ein benutzerdefiniertes SSL-Zertifikat installieren, ein zuvor verwendetes oder integriertes Zertifikat wiederherstellen und Informationen zu

einem aktuell oder zuvor verwendeten Zertifikat anzeigen:

- Ein benutzerdefiniertes Zertifikat installieren (Modus, der nicht „nur HTTPS“ ist):
  i. Kopieren Sie ein Zertifikat in den Ordner `/tmp` auf dem Hostcomputer.
  ii. Führen Sie den folgenden Befehl aus:

  ```
  certificate_installer install -c /tmp/server.crt -k
  /tmp/server.key
  ```

- Ein benutzerdefiniertes Zertifikat installieren (Modus „nur HTTPS“):
  i. Kopieren Sie ein Zertifikat in den Ordner `/tmp` auf dem Hostcomputer.
  ii. Führen Sie den folgenden Befehl aus:

  ```
  certificate_installer install -c /tmp/server.crt -k
  /tmp/server.key -f
  ```

- Das zuvor verwendete benutzerdefinierte Zertifikat wiederherstellen:

  ```
  certificate_installer recover -p
  ```

- Das integrierte benutzerdefinierte Zertifikat wiederherstellen:

  ```
  certificate_installer recover -b
  ```

- Informationen zum zurzeit verwendeten Zertifikat auflisten:

  ```
  certificate_installer list -c
  ```

- Informationen zum zuvor verwendeten Zertifikat auflisten:

  ```
  certificate_installer list -p
  ```

Weitere Informationen zum Installieren eines benutzerdefinierten Zertifikats finden Sie in der Knowledge Base im Artikel *Adding Certificates to ca-bundle.crt in ztC Edge* (KB-9792). Siehe Zugriff auf Artikel in der Knowledge Base.

Das `certificate_installer`-Skript

Verwendung

`certificate_installer` [*Befehl Befehlsoptionen*] [*script_options*]

Befehle und Befehlsoptionen

`install` *Befehlsoptionen*	Installiert das benutzerdefinierte Zertifikat.

	Befehlsoptionen sind: • `-c, --cert=`*`Zertifikatpfad`*: Der Pfad, unter dem das Zertifikat gespeichert wurde. • `-k, --key=`*`Pfad_zum_privaten_Schlüssel`*: Der Pfad, unter dem der Schlüssel gespeichert wurde. • `-f, --[no-]force`: Ersetzen des verwendeten SSL-Zertifikats durchsetzen.
`recover` ***Befehlsoptionen***	Stellt das benutzerdefinierte Zertifikat wieder her. Befehlsoptionen sind: • `-b, --[no-]built-in` (Standard): Integriertes Zertifikat wiederherstellen. • `-p, --[no-]previous`: Zuvor verwendetes Zertifikat wiederherstellen.
`list` ***Befehlsoptionen***	Listet die benutzerdefinierten Zertifikate auf. Befehlsoptionen sind: • `-a, --[no-]all` (Standard): Alle SSL-Zertifikate auf dem Hostcomputer auflisten. • `-c, --[no-]current`: Das zurzeit verwendete Zertifikat anzeigen. • `-p, --[no-]previous`: Das zuvor verwendete Zertifikat anzeigen. • `-L, --location=`*`Speicherort`*: Informationen zu einem Zertifikat an dem angegebenen Speicherort anzeigen.

Skriptoptionen

`-v, --[no_]verbose`	Im ausführlichen Modus zeigt das Skript alle Informationen an.
`-l, --log=`*Protokolldatei*	Schreibt Protokolle in die Datei *Protokolldatei* statt in `STDOUT`.

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Sicherheitsverstärkung

Konfigurieren von VM-Geräten

Konfigurieren Sie VM-Geräte, um das Einlegen von virtuellen CDs (VCDs) oder das Anschließen von USB-Geräten bei allen VMs zu deaktivieren oder zu aktivieren. Standardmäßig ist beides aktiviert. Sie können die Konfiguration auf der Seite **Voreinstellungen** unter **VM-Gerätekonfiguration** ändern.

Wenn das Einlegen von VCDs oder das Anschließen von USG-Geräten bei VM-Geräten aktiviert ist (Standardeinstellung), können Sie VCDs in alle VMs einlegen oder USB-Geräte an die VMs anschließen. Wenn das Einlegen von VCDs oder das Anschließen von USG-Geräten bei VMs deaktiviert ist, können Sie diese Medien bzw. Geräte nicht einlegen bzw. anschließen.

So deaktivieren Sie das Einlegen oder Anschließen bei allen VM-Geräten

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf der Seite **Voreinstellungen** unter **Administrative Tools** auf **VM-Gerätekonfiguration**.
3. Aktivieren Sie das Kontrollkästchen für eine oder beide der folgenden Optionen:
   - **Einlegen von CDs auf allen VMs deaktivieren** - Aktivieren Sie dieses Kontrollkästchen, wenn Sie das Einlegen von CDs in VMs deaktivieren möchten.

- **Anschluss von USB-Geräten auf allen VMs deaktivieren** - Aktivieren Sie dieses Kontrollkästchen, wenn Sie das Anschließen von USB-Geräten an VMs deaktivieren möchten.

4. Klicken Sie auf **Speichern**.

So aktivieren Sie das Einlegen oder Anschließen bei allen VM-Geräten

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf der Seite **Voreinstellungen** unter **Administrative Tools** auf **VM-Gerätekonfiguration**.
3. Deaktivieren Sie das Kontrollkästchen für eine oder beide der folgenden Optionen:
   - **Einlegen von CDs auf allen VMs deaktivieren** - Deaktivieren Sie dieses Kontrollkästchen, wenn Sie das Einlegen von CDs in VMs aktivieren möchten.
   - **Anschluss von USB-Geräten auf allen VMs deaktivieren** - Deaktivieren Sie dieses Kontrollkästchen, wenn Sie das Anschließen von USB-Geräten an VMs aktivieren möchten.
4. Klicken Sie auf **Speichern**.

Verwandte Themen

Einlegen einer virtuellen CD

Anschließen eines USB-Geräts an eine virtuelle Maschine

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Verwalten von IPtables

Das administrative Tool zum Verwalten der IP-Paketfilterung für das Betriebssystem Linux wird als *iptables* bezeichnet. Für ztC Edge-Systeme wurde die Arbeit mit iptables vereinfacht und optimiert. Auf der Seite **IPtables-Sicherheit** können Sie die verschiedenen Filtertabellenketten sowie die zugrunde liegenden Regeln einrichten, verwalten und untersuchen. Sie haben Zugriff auf die drei Hauptketten (**INPUT**, **OUTPUT** und **FORWARD**), um die Paketfilterungsregeln anzuwenden, die Sie benötigen. Bei ztC Edge-Systemen werden die Regeln auf das Hostbetriebssystem jeder physischen Maschine (PM) angewendet, sowohl für IPv4- als auch IPv6-Pakete, und die Regeln bleiben auch nach einem Neustart bestehen.

Wenn Sie eine Regel einfügen, geben Sie eine Kette (**INPUT**, **OUTPUT** oder **FORWARD**) und eine **Regelkennung** an. Bei der Verarbeitung von eingehenden Paketen wendet der Kernel die Regeln an, die mit

der **INPUT**-Kette verknüpft sind, und bei der Verarbeitung von ausgehenden Paketen die mit der **OUTPUT**-Kette verknüpften Regeln. Der Kernel wendet die Regeln, die mit der **FORWARD**-Kette verknüpft sind, an, wenn eingehende Pakete empfangen werden, die an einen anderen Host geleitet werden müssen. Regeln werden in der Reihenfolge ihrer **Regelkennung** angewendet. (Eine **Regelkennung** ähnelt einer Zeilenkennung, wobei zum Beispiel **Regelkennung** 1 Zeile 1 entspricht.) Anstatt selbst Regeln zu erstellen, können Sie jedoch auch Standardeinstellungen für die Regeln laden.

Auf der Seite **IPtables-Sicherheit** wird eine separate Tabelle für jede der drei Ketten mit den jeweils verknüpften Regeln angezeigt. Die Regeln einer bestimmten Kette sind nach **Regelkennung** sortiert. In den Spalten werden der Netzwerkname, der Netzwerktyp, das Protokoll und weitere Informationen angezeigt. Verwenden Sie ggf. die Bildlaufleiste an der rechten Seite, um alle Regeln anzuzeigen, und die Bildlaufleisten am unteren Rand, um alle Spalten zu sehen. Weitere Informationen zu den iptables-Funktionen finden Sie im Linux-Handbuch auf den Seiten für iptables.

Sie können optional auch festlegen, dass die Regeln nicht nur auf das Hostbetriebssystem, sondern auch auf das Gastbetriebssystem angewendet werden. Standardmäßig gelten die Regeln nur für das Hostbetriebssystem, nicht für die Gastbetriebssysteme. Wenn Sie festlegen, dass die Regeln auch für die Gäste gelten sollen, werden alle vorhandenen Regeln, importierten Regeln und neu eingefügten Regeln auch auf alle Gastbetriebssysteme angewendet (das gilt für Regeln, die auf demselben Unternehmensnetzwerk basieren, das dem Gast zugewiesen wurden).

Hinweise:

1. Informationen zu den Ports, die die ztC Edge-Software verwendet, finden Sie unter Übersicht über die Systemanforderungen.
2. Weitere Informationen zu ztC Edge TCP- und UDP-Ports finden Sie in der Knowledge Base im Artikel *TCP and UDP ports used by ztC Edge* (KB-2123). Siehe Zugriff auf Artikel in der Knowledge Base.

Um die IPtables zu verwalten, müssen Sie zuerst die IPtables-Sicherheit aktivieren, falls Sie dies noch nicht getan haben.

So aktivieren Sie die IPtables-Sicherheit

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf der Seite **Voreinstellungen** auf **IPtables-Sicherheit**.

3. Aktivieren Sie das Kontrollkästchen neben **IPtables-Sicherheit aktivieren**.

   Das Fenster **IPtables-Sicherheit aktivieren** wird einige Minuten lang grau. Wenn das Fenster wieder aktiv wird, ist **IPtables-Sicherheit aktivieren** ausgewählt.

Standardmäßig werden Regeln nur auf den Host angewendet. Es ist aber möglich, die Regeln auch auf Gäste anzuwenden.

So wenden Sie Regeln nicht nur auf den Host, sondern auch auf Gastbetriebssysteme an

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf der Seite **Voreinstellungen** auf **IPtables-Sicherheit**.

   Vergewissern Sie sich, dass **IPtables-Sicherheit aktivieren** ausgewählt ist.
3. Standardmäßig ist **Auf Host anwenden** ausgewählt:

   Wählen Sie **Auf Host und Gäste anwenden**, um die Regeln sowohl auf das Hostbetriebssystem als auch auf Gastbetriebssysteme anzuwenden. Das Fenster **Portverwaltung aktivieren** wird einige Minuten lang grau.

   Wenn **Auf Host und Gäste anwenden** ausgewählt ist, werden alle vorhandenen Regeln, importierten Regeln und neu eingefügten Regeln auch auf alle Gastbetriebssysteme angewendet (das gilt für Regeln, die auf demselben Unternehmensnetzwerk basieren, das dem Gast zugewiesen wurden).

Fahren Sie fort, indem Sie eine neue Regel einfügen, eine Regel entfernen, Standardeinstellungen laden, Regeln importieren oder Regeln exportieren.

So fügen Sie eine neue Regel ein

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf der Seite **Voreinstellungen** auf **IPtables-Sicherheit**.

   Vergewissern Sie sich, dass **IPtables-Sicherheit aktivieren** ausgewählt ist.
3. Klicken Sie auf die Schaltfläche **Neue Regel einfügen**, um das Popupfenster **Neue Regel einfügen** zu öffnen.
4. Legen Sie im Popupfenster **Neue Regel einfügen** Werte für Folgendes fest:

- **Kette** - Wählen Sie in der Dropdownliste **INPUT**, **OUTPUT** oder **FORWARD** aus.
- **Regelkennung** - Geben Sie eine Zahl ein, um die Reihenfolge für die Verarbeitung der Regeln festzulegen. Beginnen Sie mit 1 und geben Sie höchstens den Wert ein, welcher der Gesamtzahl der Regeln in der Kette entspricht. Jede **Regelkennung** darf nur einmal vorkommen.

  Wenn Sie eine Zahl eingeben, die bereits einer Regel zugewiesen ist, wird der Wert der bestehenden Regel um 1 erhöht (sowie ggf. auch der aller folgenden Regeln), und die eingegebene Zahl wird der neuen Regel zugewiesen. Wenn zum Beispiel **Regelkennung 1** bereits vorhanden ist und Sie **1** für die neue Regel eingeben, wird die vorhandene **Regelkennung 1** zu **Regelkennung 2**, die vorhandene **Regelkennung 2** (falls es sie gibt) wird zu **Regelkennung 3** usw.
- **Gemeinsames Netzwerk** - Wählen Sie ein Netzwerk aus der Dropdownliste aller verfügbaren freigegebenen Netzwerke aus.
- **Protokoll** - Wählen Sie **udp**, **tcp** oder **alle**.

  Wenn Sie **alle** wählen, werden die Felder **Gruppierung** und **Portnummer** inaktiv (grau), weil in diesem Fall kein Bereich von Portnummern angegeben werden muss.
- **Ziel** - Wählen Sie **auslassen**, **akzeptieren** oder **ablehnen** als Aktion, die auf die Pakete angewendet werden soll, welche die Regelkriterien erfüllen.
- **Portnummer (ab)** - Geben Sie für den ersten Port des Bereichs eine Zahl zwischen 0 und 65535 ein, die nicht größer ist als **Portnummer (bis)**.
- **Portnummer (bis)** - Geben Sie für den letzten Port des Bereichs eine Zahl zwischen 0 und 65535 ein, die nicht kleiner ist als **Portnummer (ab)**.
- **IP-Adresse (ab)** - Geben Sie für die erste IPv4-Adresse des Bereichs eine Adresse zwischen 0.0.0.0 und 255.255.255.255 ein, die nicht größer ist als **IP-Adresse (bis)**.
- **IP-Adresse (bis)** - Geben Sie für die letzte IPv4-Adresse des Bereichs eine Adresse zwischen 0 und 255.255.255.255 ein, die nicht kleiner ist als **IP-Adresse (ab)**.
- **IPv6-Adresse (ab)** - Geben Sie für die erste IPv6-Adresse des Bereichs eine Adresse zwischen 0000:0000:0000:0000:0000:0000:0000:0000 und ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff ein, die nicht größer ist als **IPv6-Adresse (bis)**.

- **IPv6-Adresse (bis)** - Geben Sie für die letzte IP-Adresse des Bereichs eine Adresse zwischen 0000:0000:0000:0000:0000:0000:0000:0000 und ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff ein, die nicht kleiner ist als **IPv6-Adresse (ab)**.

Klicken Sie auf **Einfügen**, um die neue Regel einzufügen.

5. Standardmäßig werden neu eingefügte Regeln nur auf den Host angewendet. Wenn die Regeln für den Host und die Gastbetriebssysteme gelten sollen, lesen Sie So wenden Sie Regeln nicht nur auf den Host, sondern auch auf Gastbetriebssysteme an.
6. Klicken Sie unten auf der Seite auf **Speichern** oder auf **Zurücksetzen**, um nicht gespeicherte Änderungen zu verwerfen, womit die Regeln auf die der zuletzt gespeicherten Sitzung zurückgesetzt werden.

   Nachdem die neue Regel gespeichert wurde, wird sie auf der Seite **IPtables-Sicherheit** in der entsprechenden Kette angezeigt.

So entfernen Sie eine Regel

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf der Seite **Voreinstellungen** auf **IPtables-Sicherheit**.

   Vergewissern Sie sich, dass **IPtables-Sicherheit aktivieren** ausgewählt ist.

   (**Auf Host anwenden** und **Auf Host und Gäste anwenden** haben keinen Effekt beim Entfernen von Regeln.)
3. Wählen Sie die Regel aus, die Sie entfernen möchten.
4. Klicken Sie (in der Spalte ganz rechts) für die ausgewählte Regel auf **Entfernen**.
5. Klicken Sie unten auf der Seite auf **Speichern** oder auf **Zurücksetzen**, um nicht gespeicherte Änderungen zu verwerfen, womit die Regeln auf die der zuletzt gespeicherten Sitzung zurückgesetzt werden.

   Nachdem die Regel entfernt wurde, wird sie auf der Seite **IPtables-Sicherheit** nicht mehr angezeigt.

So laden Sie die Standardeinstellungen

Achtung: Wenn Sie die Standardeinstellungen laden, werden die aktuellen Einstellungen überschrieben.

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf der Seite **Voreinstellungen** auf **IPtables-Sicherheit**.

   Vergewissern Sie sich, dass **IPtables-Sicherheit aktivieren** ausgewählt ist.
3. Klicken Sie unten auf der Seite auf **Standardeinstellungen laden**.

   Es wird eine Warnung angezeigt: *Die aktuellen Einstellungen werden von den ursprünglichen Einstellungen überschrieben!* Klicken Sie auf **OK**, wenn Sie die Standardeinstellungen laden möchten, oder klicken Sie auf **Abbrechen**, um das Laden der Standardeinstellungen abzubrechen. Wenn Sie auf **OK** klicken, bleibt das Fenster **Portverwaltung aktivieren** einige Minuten lang grau und die Meldung *Laden der Standardeinstellungen....* wird angezeigt.
4. Standardmäßig werden Standardregeln nur auf den Host angewendet. Wenn die Regeln für den Host und die Gastbetriebssysteme gelten sollen, lesen Sie So wenden Sie Regeln nicht nur auf den Host, sondern auch auf Gastbetriebssysteme an.

So importieren oder exportieren Sie Regeln

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie auf der Seite **Voreinstellungen** auf **IPtables-Sicherheit**.

   Vergewissern Sie sich, dass **IPtables-Sicherheit aktivieren** ausgewählt ist.
3. Klicken Sie unten auf der Seite auf **Importieren** oder **Exportieren**.
   - **Importieren** – Der **Assistent zum Importieren/Wiederherstellen der IPtables-Sicherheitsregeln** wird eingeblendet. Navigieren Sie zu der XML-Datei, die Sie importieren möchten, und wählen Sie sie aus. Alle Regeln, die in der importierten XML-Datei mit dem Typ eines gemeinsamen Netzwerks verknüpft sind, werden für jedes vorhandene gemeinsame Netzwerk im System, das denselben Typ aufweist, generiert.

     Nachdem Sie eine XML-Datei ausgewählt haben, wird die folgende Meldung angezeigt:

     ***Mit Anhängen** bleibt der aktuelle Regelsatz erhalten. Wählen Sie **Überschreiben**, um alle aktuellen Regeln zu löschen.*

     Klicken Sie auf die entsprechende Schaltfläche:

     - **Anhängen** – Die ausgewählte XML-Datei wird an die vorhandene XML angehängt, wobei die vorhandenen Regeln erhalten bleiben.

- **Überschreiben** - Die ausgewählte XML-Datei überschreibt die vorhandene XML, wobei die vorhandenen Regeln gelöscht werden.

- **Exportieren** - Es wird ein Dateiexplorer-Fenster eingeblendet. Navigieren Sie zu einem Speicherort auf Ihrem lokalen System, an dem Sie die Datei mit den exportierten Regeln speichern wollen. Alle Regeln in der Tabelle werden in eine XML-Datei exportiert, die dann zum ausgewählten Speicherort heruntergeladen wird.

4. Standardmäßig werden importierte Regeln nur auf den Host angewendet. Wenn die Regeln für den Host und die Gastbetriebssysteme gelten sollen, lesen Sie So wenden Sie Regeln nicht nur auf den Host, sondern auch auf Gastbetriebssysteme an.
5. Wenn Sie eine Datei importiert haben, klicken Sie auf **Speichern** (oder auf **Zurücksetzen**, um die zuvor gespeicherten Werte wiederherzustellen).

Verwandte Themen

Die Seite „Voreinstellungen“

Die ztC Console

Sicherheitsverstärkung

Konfigurieren des Anmeldebanners

Sie können ein Anmeldebanner konfigurieren, um auf der ztC Console-Anmeldeseite benutzerdefinierten Inhalt anzuzeigen. Sie können zum Beispiel einen Text hinzufügen.

So konfigurieren Sie das Anmeldebanner

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **Administrative Tools** auf **Anmeldebanner-Hinweis**.
3. Aktivieren Sie das Kontrollkästchen **Anmeldebanner-Hinweis aktivieren**. Es wird ein Feld angezeigt.

   Geben Sie in dieses Feld die Informationen ein, die auf der Anmeldeseite der Konsole angezeigt werden sollen. Sie können zum Beispiel den Namen Ihres Unternehmens oder eine Nachricht eingeben.
4. Klicken Sie auf **Speichern** (oder auf **Zurücksetzen**, um die zuvor gespeicherten Werte wiederherzustellen).

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Aktivieren von ztC Advisor

Aktivieren Sie ztC Advisor für ein ztC Edge-System, damit Administratoren die Integrität des Systems remote im ztC Advisor-Dashboard beobachten können.

ztC Advisor ist ein sicheres, webbasiertes Portal, das zentrale Sichtbarkeit Ihrer gesamten Flotte von ztC Edge-Systemen bietet. Über ein intuitives und benutzerfreundliches Dashboard können Sie die Integrität, die Ressourcennutzung und die Softwareversion jedes Systems auf einen Blick beurteilen. Weitere Informationen über die Registrierung für und Verwendung von ztC Advisor finden Sie auf der folgenden Webseite: https://www.stratus.com/solutions/ztc-advisor.

Voraussetzung: Das ztC Edge-System muss bei Stratus registriert und mit dem Internet verbunden sein, damit es in ztC Advisor überwacht werden kann. Sie können ztC Advisor jederzeit aktivieren, die Informationen zum Systemzustand werden jedoch nur dann im Dashboard angezeigt, wenn das System bei Stratus registriert und mit dem Internet verbunden ist.

Nach Aktivieren von ztC Advisor, wie im folgenden Verfahren beschrieben, können Sie sich am ztC Advisor-Dashboard anmelden und den Status Ihres Systems auf der folgenden Webseite anzeigen: https://ztcadvisor.stratus.com.

So aktivieren Sie ztC Advisor für ein ztC Edge-System

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **Administrative Tools** auf **ztC Advisor**.
3. Aktivieren Sie das Kontrollkästchen neben **ztC Advisor aktivieren**.
4. Geben Sie optional einen **Aliasnamen** für das System ein.

   Standardmäßig listet das Dashboard jedes System nach seiner Bestandskennung auf; Sie können dem System jedoch einen aussagekräftigen Aliasnamen zuweisen, sodass es in Filtern und Suchen

leichter zu identifizieren ist. Der Aliasname kann bis zu 64 Zeichen lang sein und eine beliebige Kombination aus Buchstaben, Ziffern und Sonderzeichen enthalten.

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und die Überwachung zu aktivieren.

Innerhalb einiger Minuten nach dem Speichern ist das System im ztC Advisor-Dashboard zu sehen.

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Speichern und Wiederherstellen der Systemvoreinstellungen

In einem ztC Edge-System mit der entsprechenden Lizenz kann ein Benutzer mit vollständigen Systemadministratorberechtigungen die Einstellungen der Seite ztC Console**Voreinstellungen** speichern, indem er eine Wiederherstellungsdatei (manchmal als Backupdatei oder Sicherungsdatei bezeichnet) erstellt. Sie können diese Datei in einem Zielordner auf einem lokalen Computer oder in einem Ordner in der Cloud speichern. Sollte es später einmal erforderlich sein, können Sie dann diese gespeicherte Datei auswählen, um die **Voreinstellungen** auf demselben Knoten, auf einem Ersatzknoten oder auf einem oder mehreren anderen Knoten wiederherzustellen. Mit dieser Funktion können Sie schnell ein oder mehrere Systeme einrichten. Wenn Sie zum Beispiel bereits bei Ihrem Cloud-Account angemeldet sind, in dem eine Wiederherstellungsdatei für Ihr System gespeichert ist, können Sie die Systemvoreinstellungen des Knotens mit einem Klick wiederherstellen.

Hinweise:

- Sie können pro ztC Edge-System bis zu 50 Dateien in der Cloud speichern.
- Damit Sie eine Datei in der Cloud speichern oder eine Datei aus der Cloud wiederherstellen können, muss das System mit dem Internet verbunden sein und Sie müssen sich mit gültigen Anmeldeinformationen bei einem Cloud-Account anmelden.

Das System benötigt die entsprechende Lizenz, damit die Einstellungen der **Voreinstellungen** gespeichert und wiederherstellt werden können. Bei der erstmaligen Installation des Systems ist diese Funktion deaktiviert. Die Fenster **Systemvoreinstellungen speichern** und **Systemvoreinstellungen wiederherstellen** der Seite **Voreinstellungen** zeigen eine Meldung an, dass Sie die Lizenz zum Speichern

und Wiederherstellen der **Voreinstellungen** aktivieren müssen. Sie müssen die Lizenz aktivieren, wenn Sie diese Funktion verwenden möchten.

So aktivieren Sie die Lizenz

Voraussetzungen: Sie benötigen die folgenden Informationen, um die Lizenz zu aktivieren:

- **First Name** (Vorname) und **Last Name** (Nachname)
- **Company Email** (E-Mail-Adresse des Unternehmens) - Geben Sie die E-Mail-Adresse des Unternehmens ein, dem das System gehört. Geben Sie keine persönliche E-Mail-Adresse ein.
- **Company Name** (Name des Unternehmens) - Geben Sie den Namen des Unternehmens ein, dem das System gehört.
- **Company Phone Number** (Telefonnummer des Unternehmens) - Geben Sie die Telefonnummer des Unternehmens ein, dem das System gehört. Geben Sie keine private Telefonnummer ein.
- **Asset ID** (Bestandskennung) - Geben Sie die BESTANDSKENNUNG ein, die Sie auf dem Stratus-Registrierungsblatt finden.

Wenn Ihr System Internetzugang hat, fahren Sie mit Schritt 1 weiter unten fort. Bei einem System ohne Internetverbindung müssen Sie die Lizenzdatei zwischen einem Standort mit Internetverbindung und dem Standort der ztC Console (ohne Internetverbindung) kopieren. Im nachstehend beschriebenen Verfahren wird dazu ein USB-Stick verwendet, es gibt aber auch andere Möglichkeiten. Wenn Sie einen USB-Stick verwenden, schließen Sie diesen an einen USB-Port am Remote-Verwaltungscomputer an, auf dem die ztC Console ausgeführt wird.

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **Administrative Tools** auf **Systemvoreinstellungen speichern** oder **Systemvoreinstellungen wiederherstellen**.
3. Das Fenster zeigt eine Meldung an, dass Sie eine separate Lizenz zum Speichern und Wiederherstellen der **Voreinstellungen** aktivieren müssen.
4. Lesen Sie die Meldung. Wenn Ihr System Internetzugang hat, klicken Sie auf den Link, um die Webseite für die Lizenzierung zu öffnen.

> **Hinweis**: Wenn Sie das System auch registrieren und eine dauerhafte Lizenz für das System erwerben müssen, lesen Sie Registrieren des Systems und Beziehen einer dauerhaften Lizenz.

Wenn das System keine Internetverbindung hat, gehen Sie wie nachstehend beschrieben vor, um die Webseite für die Lizenzierung zu öffnen.

Auf einem System ohne Internetverbindung

a. Klicken Sie auf den Link, um die Webseite für die Lizenzierung zu öffnen, und kopieren Sie die URL der Webseite für die Lizenzierung mit einer der in Ihrem Browser verwendeten Methoden.

b. Fügen Sie die URL in eine Textdatei ein und speichern Sie diese auf dem USB-Stick.

c. Trennen Sie den USB-Stick vom Port und gehen Sie zu einem Computer mit Internetzugang.

d. Schließen Sie den USB-Stick an einen USB-Port des Computers an.

e. Gehen Sie zu der Textdatei auf dem USB-Stick, öffnen Sie sie und kopieren Sie die URL der Webseite für die Lizenzierung.

f. Öffnen Sie einen Webbrowser, fügen Sie URL in die Adressleiste ein und öffnen Sie die Webseite.

5. Geben Sie die erforderlichen Informationen auf der Webseite ein und klicken Sie auf **Submit** (Senden).

6. Klicken Sie auf die Schaltfläche **Download License** (Lizenz herunterladen), wenn diese eingeblendet wird. Wenn Ihr System Internetzugang hat, fahren Sie mit dem nächsten Schritt fort.

   Wenn das System keinen Internetzugang hat, speichern Sie die heruntergeladene Lizenzdatei auf dem USB-Stick und trennen Sie diesen vom Computer. Kehren Sie zum Remote-Verwaltungscomputer zurück, auf dem die Konsole ausgeführt wird, und schließen Sie den USB-Stick an.

7. Laden Sie die Lizenz auf das System hoch, indem Sie zuerst auf **Produktlizenz** auf der Seite **Voreinstellungen** klicken. Führen Sie dann je nach Ihrem System einen der folgenden Schritte aus:

- Um die Lizenz auf einem System mit Internetverbindung automatisch hochzuladen, klicken Sie zuerst auf **Produktlizenz** auf der Seite **Voreinstellungen** und dann auf **Lizenz jetzt überprüfen** für **Online-Lizenzüberprüfung**. Die neu heruntergeladene Datei wird automatisch auf das System angewendet.
- Um die Lizenz manuell auf einem System ohne Internetzugang hochzuladen:
    a. Klicken Sie auf der Seite **Voreinstellungen** auf **Produktlizenz**.
    b. Klicken Sie auf die Leiste **Offline-Lizenzüberprüfung und manuelle Installation der Lizenz**, um verschiedene Optionen anzuzeigen, falls diese nicht bereits eingeblendet sind.
    c. Bei **Aktivierte Lizenz auf dem System installieren** klicken Sie auf **Datei auswählen** und navigieren Sie zum Speicherort, an dem Sie die Datei gespeichert haben.
    d. Wählen Sie die Datei aus, klicken Sie auf **Öffnen** und dann auf **Hochladen**, um die Datei an das System hochzuladen.

Das System verfügt jetzt über die entsprechende Lizenz, damit die Einstellungen der **Voreinstellungen** gespeichert und wiederherstellt werden können.

Standardmäßig sind in der gespeicherten Datei die folgenden Einstellungen der Voreinstellungen enthalten:

Besitzerinformationen	VM-Gerätekonfiguration
Softwareupdates	IPtables-Sicherheit
IP-Konfiguration	Anmeldebanner-Hinweis
Quorum-Server (nur bei Systemen mit zwei Knoten)	ztC Advisor
	e-Alerts
Datum und Uhrzeit	SNMP-Konfiguration
Mail-Server	OPC-Konfiguration
Benutzer und Gruppen	Supportkonfiguration
Sichere Verbindung	Proxykonfiguration

So speichern Sie die Systemvoreinstellungen

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **Administrative Tools** auf **Systemvoreinstellungen speichern**.
3. Wählen Sie unter **Systemvoreinstellungen speichern** eine der folgenden Optionen:
   - **Systemvoreinstellungen in einer Datei auf diesem Computer speichern**
   - **Systemvoreinstellungen in der Cloud speichern** – Bei dieser Auswahl wird die folgende Meldung angezeigt, wenn der Remoteverwaltungscomputer (auf dem die ztC Console ausgeführt wird) mit dem Internet verbunden ist:

     Melden Sie sich beim Stratus Customer Service Portal an, um Ihr Konto zu authentifizieren.

     Geben Sie den Benutzernamen und das Kennwort für Ihr Stratus-Kundendienstkonto ein. Falls der Remoteverwaltungscomputer nicht mit dem Internet verbunden ist, werden die Anmeldefelder nicht angezeigt. Stattdessen erscheint eine Meldung, die angibt, dass keine Internetverbindung verfügbar ist und dass Sie die Datei nicht speichern können.

     Nachdem Sie sich beim Cloud-Account angemeldet haben, werden der Name des angemeldeten Benutzers und die Anzahl der in der Cloud gespeicherten Dateien angezeigt. Sie können pro System bis zu 50 Dateien speichern. Wenn Sie 50 Dateien gespeichert haben, lässt sich keine weitere speichern. Da Sie selbst keine Dateien löschen können, müssen Sie sich an Ihren Stratus-Servicemitarbeiter wenden, wenn Dateien gelöscht werden sollen.

     Die Anmeldung bei Ihrem Cloud-Account bleibt so lange aktiv, wie Ihre Konsolensitzung aktiv ist. Sie werden automatisch abgemeldet, wenn Sie die Konsolensitzung schließen oder wenn die Sitzung aufgrund einer Zeitüberschreitung bei Inaktivität geschlossen wird.
4. Geben Sie Informationen in die folgenden Felder ein:
   - **Dateiname** – In diesem Feld wird ein Standardname im folgenden Format angezeigt: **ztC_*Bestandskennung*_preferences_*jjjj-mm-tt-hh-mm*.zip**. Falls erforderlich, können Sie den Standardnamen nach dem Speichern der Datei ändern.
   - **Beschreibung** – Geben Sie eine Beschreibung ein (optional).

- **Schlüsselwörter** – Standardmäßig wird das Schlüsselwort *system_ID* verwendet. Sie können das Standardschlüsselwort ändern und maximal zwei weitere Schlüsselwörter hinzufügen.

5. Klicken Sie auf eine der folgenden Schaltflächen:

   - **Speichern** – Die Datei wird mit dem Standarddateinamen gespeichert; Sie können diesen Namen aber auch ändern.

     Wenn Sie die Datei auf einem lokalen Computer speichern, können Sie den Standardspeicherort verwenden oder zu einem anderen Ordner navigieren. (Der Standardspeicherort wird im Dateibrowser festgelegt.)

     Wenn Sie die Datei in der Cloud speichern und der Benutzername und das Kennwort erfolgreich validiert wurden, wird die Datei erstellt und im Cloud-Konto des Benutzers in einem Ordner mit dem Namen ***Bestandskennung*** gespeichert.

   - **Löschen** – Löscht den Text in den Feldern **Beschreibung** und **Tags**. Wenn Sie die Datei in der Cloud speichern, wird außerdem der Dateiname auf den Standardnamen zurückgesetzt und die Angaben für Benutzername und Kennwort werden gelöscht.

   Die Meldung *Systemvoreinstellungen wurden gespeichert.* wird angezeigt, wenn die Datei gespeichert wurde.

Wenn Sie die Einstellungen der Systemvoreinstellungen gespeichert haben und die Einstellungen dann auf demselben System oder auf einem anderen System wiederherstellen möchten, machen Sie sich zunächst mit den Warnhinweisen, Voraussetzungen und Hinweisen vertraut, die die Wiederherstellung betreffen.

So bereiten Sie die Wiederherstellung der Systemvoreinstellungen vor

Lesen Sie sich die folgenden Warnhinweise, Voraussetzungen und Hinweise durch, bevor Sie eine gespeicherte Datei mit Systemvoreinstellungen wiederherstellen.

Achtung: Falls die wiederhergestellten Systemvoreinstellungen eine oder mehrere der folgenden Einstellungen ändern, geht die Verbindung des Systems zur ztC Console verloren:

- IP-Konfiguration
- Sichere Verbindungen (wenn Sie mit aktiviertem HTTP angemeldet sind und die Wiederherstellungsdatei HTTP deaktiviert.)
- Datum und Uhrzeit

Wenn die Verbindung unterbrochen wird, wird der Wiederherstellungsvorgang im Hintergrund weiterhin ausgeführt, Sie können den Fortschritt oder Status jedoch nicht sehen. Wenn Sie die Konsolenverbindung verloren haben, melden Sie sich erneut an. (Informationen zum Einstellen der IP-Konfiguration finden Sie unter Konfigurieren der IP-Einstellungen. Informationen zum Einstellen sicherer Verbindungen finden Sie unter Konfigurieren von sicheren Verbindungen. Informationen zum Einstellen von Datum und Uhrzeit finden Sie unter Konfigurieren von Datum und Uhrzeit.)

Voraussetzungen:

- Active Directory (AD)-Einstellungen: Wenn die wiederhergestellten Voreinstellungen AD aktivieren, müssen Sie bei der Anmeldung die Anmeldedaten für AD angeben. Informationen zum Aktivieren von AD finden Sie unter Konfigurieren von Active Directory.
- Die Einstellung **Quorumserver**:
  - Der Status **Aktiviert** wird wiederhergestellt.
  - Keine VM sollte die vorhandenen Quorumserver verwenden; alle verwendeten VMs müssen ausgeschaltet werden, bevor die Voreinstellungen wiederhergestellt werden. Falls während der Wiederherstellung noch VMs den Quorumserver verwenden, schlägt die Wiederherstellung der Einstellung **Quorumserver** fehl.
  - Diese Einstellung wird in einem System mit nur einem Knoten nicht wiederhergestellt.

  Informationen zum Aktivieren von Quorumservern finden Sie unter Konfigurieren der Quorumserver.

Hinweise: Beachten Sie Folgendes, bevor Sie die Systemvoreinstellungen wiederherstellen:

- Das System, auf dem Sie die Voreinstellungen wiederherstellen, und das System, dessen gespeicherte Datei mit Voreinstellungen Sie verwenden, müssen in folgenden Punkten übereinstimmen:
  - Dasselbe Hardwaremodell - Das System, auf dem Sie die Voreinstellungen wiederherstellen, muss dasselbe Hardwaremodell haben wie das System, dessen gespeicherte Datei mit Voreinstellungen Sie wiederherstellen.
  - Dieselbe Zwei-Knoten- oder Ein-Knoten-Konfiguration - Sie können in einem System mit zwei Knoten nur Voreinstellungen wiederherstellen, die in einem System mit zwei Knoten gespeichert wurden. Sie können in einem System mit einem Knoten nur Voreinstellungen wiederherstellen, die in einem System mit einem Knoten gespeichert wurden.
- Wenn Sie Systemvoreinstellungen in einem System wiederherstellen, auf dem eine frühere oder neuere Version ausgeführt wird als auf dem Originalsystem, können Sie nur die Voreinstellungen wiederherstellen, die von der früheren Version unterstützt werden.
- **IPtables-Sicherheit** - Um IPtables-Einstellungen wiederherzustellen, müssen Sie entweder **Anhängen** auswählen (um die Einstellungen aus der Wiederherstellungsdatei an die vorhandenen Regeln anzuhängen) oder **Überschreiben** (um die vorhandenen Regeln mit den Einstellungen aus der Wiederherstellungsdatei zu überschreiben). (Informationen zu IPtables finden Sie unter Verwalten von IPtables.)
- **IP-Konfiguration** - Wenn Sie diese Option auswählen, werden alle Daten der Netzwerkkonfiguration wiederhergestellt. (Informationen zur finden Sie unter Konfigurieren der IP-Einstellungen.)
- **Datum und Uhrzeit** - Nur die Einstellung **Automatisch** kann sofort wiederhergestellt werden. Wenn Sie die Einstellung **Manuell** sowie Einstellungen mit einer anderen Zeitzone und mehreren NTP-Servern wiederherstellen, werden die physischen Maschinen ausgeschaltet und die wiederhergestellten Einstellungen für Datum und Uhrzeit werden nach dem Neustart des Systems

wirksam. (Informationen hierzu finden Sie unter Konfigurieren von Datum und Uhrzeit.)

- Für **Benutzer und Gruppen** beachten Sie bitte Folgendes:
  - Sie müssen Anmeldedaten für Active Directory angeben, wenn Sie die Einstellung **Benutzer und Gruppen** wiederherstellen möchten.
  - Wenn ein Benutzerkonto im aktuellen System und in der Wiederherstellungsdatei vorhanden ist, betrachtet das aktuelle System das Benutzerkonto als bearbeitet.
  - Wenn ein Benutzerkonto in der Wiederherstellungsdatei, aber nicht im aktuellen System vorhanden ist, betrachtet das aktuelle System das Benutzerkonto als hinzugefügt.
  - In den folgenden Fällen überspringt das aktuelle System einen AD-Eintrag in der Wiederherstellungsdatei:
    - Wenn ein AD-Eintrag in der Wiederherstellungsdatei zum Zeitpunkt der Wiederherstellung im für das aktuelle System konfigurierten AD fehlt.
    - Wenn der AD-Eintrag in der Wiederherstellungsdatei zum Zeitpunkt der Wiederherstellung im für das aktuelle System konfigurierten AD einen anderen Benutzertyp aufweist.

  (Informationen zu **Benutzern und Gruppen** finden Sie unter Konfigurieren von Benutzern und Gruppen.)

Nachdem Sie sich mit den Warnhinweisen, Voraussetzungen und Hinweisen vertraut gemacht haben, die den Wiederherstellungsvorgang betreffen, können Sie die Systemvoreinstellungen wiederherstellen.

So stellen Sie die Systemvoreinstellungen wieder her

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **Administrative Tools** auf **Systemvoreinstellungen wiederherstellen**.
3. Wählen Sie unter **Systemvoreinstellungen wiederherstellen** eine der folgenden Optionen:

- **Systemvoreinstellungen aus einer Datei auf diesem Computer wiederherstellen**:

  a. Klicken Sie auf **Datei auswählen**, um eine Liste mit Dateien im Standardverzeichnis für die Speicherung anzuzeigen, darunter gespeicherte ZIP-Dateien. Falls erforderlich, navigieren Sie zu einem anderen Verzeichnis.

  b. Wählen Sie die Datei mit den **Voreinstellungen** aus, die Sie wiederherstellen möchten, und klicken Sie auf den Dateinamen. Es wird die folgende Tabelle angezeigt:

  Systemvoreinstellungen werden wiederhergestellt aus:

Dateiname	ztC_*Bestandskennung*_preferences_*jjjj-mm-tt-hh-mm-ss*.zip
Softwareversion	*Versionsnummer*
Beschreibung	*Beschreibung*
Schlüsselwörter	*Schlüsselwörter*

  Falls die wiederhergestellten **Voreinstellungen** Benutzer und Gruppen einschließen, werden auch die folgenden Informationen angezeigt:

Anmeldedaten für Active Directory	Sie benötigen Anmeldedaten für Active Directory, wenn Sie **Benutzer und Gruppen** wiederherstellen möchten.

  Klicken Sie auf **Weiter**, um die Einstellungen aus der ausgewählten Datei wiederherzustellen.

- **Systemvoreinstellungen aus einer Datei in der Cloud wiederherstellen** – Bei dieser Auswahl wird *Melden Sie sich beim Stratus Customer Service Portal an, um Ihr Konto zu authentifizieren* zusammen mit Feldern für **Benutzername** und **Kennwort** angezeigt (falls Sie noch nicht in Ihrem Konto angemeldet sind), sofern der Remoteverwaltungscomputer mit dem Internet verbunden ist. Falls der Remoteverwaltungscomputer nicht mit dem Internet verbunden ist, wird eine Meldung zur nicht verfügbaren Internetverbindung angezeigt. (Nachdem Sie sich beim Cloud-

Account angemeldet haben, bleibt die Sitzung so lange geöffnet, wie Ihre Konsolensitzung aktiv ist. Sie werden automatisch abgemeldet, wenn Sie die Konsolensitzung schließen oder wenn die Sitzung aufgrund einer Zeitüberschreitung bei Inaktivität geschlossen wird.)

Geben Sie den Benutzernamen und das Kennwort für Ihr Stratus-Kundendienstkonto ein und klicken Sie auf **ANMELDEN**.

Wenn die Verbindung erfolgreich ist, wird die folgende Tabelle eingeblendet, in der eine oder mehrere Dateien bis zur Gesamtzahl der gespeicherten Dateien aufgeführt sind:

Bestandskennung auswählen *Kennung suchen*	**Datei auswählen, aus der die Systemvoreinstellungen wiederhergestellt werden sollen**	
Bestandskennung	**Dateiname**	**Erstellt am**
bestandskennung	*dateiname*	*uhrzeit*

Die Spalte **Bestandskennung** enthält eine Liste der *bestandskennung*-Ordner. Die Spalte **Dateiname** enthält eine Liste der Dateien im *bestandskennung*-Ordner zusammen mit dem Zeitpunkt, zu dem die Datei gesichert wurde, wie in der Spalte **Uhrzeit** angegeben. Zusätzlich wird die Tabelle Systemvoreinstellungen werden wiederhergestellt aus: angezeigt.

Unter **Bestandskennung** wird die ID des aktuellen Systems als Erste aufgeführt, und unter **Dateiname** wird dessen Wiederherstellungsdatei (sofern vorhanden) als Erste aufgeführt. Klicken Sie in diesem Fall auf den obersten Dateinamen, um die Einstellungen der **Voreinstellungen** im aktuellen System wiederherzustellen.

Um nach einer Datei zu suchen, geben Sie den *Dateinamen* in das Feld *Kennung suchen* ein.

Um eine Datei auszuwählen, klicken Sie auf die gewünschte *Bestandskennung* und dann auf den gewünschten *Dateinamen*. Klicken Sie auf **Weiter**, um die **Voreinstellungen** aus der ausgewählten Datei wiederherzustellen.

4. Das Fenster **Systemvoreinstellungen zum Wiederherstellen auswählen** wird mit einer Liste von Voreinstellungen angezeigt.

Standardmäßig werden die folgenden Einstellungen der Voreinstellungen wiederhergestellt:

Besitzerinformationen Softwareupdates Quorum-Server (nur bei Systemen mit zwei Knoten) Mail-Server VM-Gerätekonfiguration Anmeldebanner-Hinweis	ztC Advisor e-Alerts SNMP-Konfiguration OPC-Konfiguration Supportkonfiguration Proxykonfiguration

Hinweis:
Die folgenden Voreinstellungen sind nicht standardmäßig ausgewählt, da sie dazu führen, dass entweder eine Popup-Meldung eingeblendet oder das System neu gestartet wird:

- **Datum und Uhrzeit** - Wenn sich diese Einstellung ändert, wird das System neu gestartet.
- **Benutzer und Gruppen** - Wenn Active Directory (AD) aktiviert ist, wird ein Fenster für die AD-Anmeldeinformationen eingeblendet.
- **Sichere Verbindung** - Wenn Sie mit HTTP angemeldet sind und die Wiederherstellungsdatei HTTP deaktiviert, verlieren Sie die Verbindung zum System und müssen sich erneut anmelden.
- **IPtables-Sicherheit** - Es wird ein Fenster eingeblendet, in dem Sie gefragt werden, ob Sie die wiederhergestellten Regeln an den aktuellen Regelsatz anhängen oder den aktuellen Regelsatz überschreiben wollen.
- **IP-Konfiguration** - Wenn sich die IP-Konfiguration ändert, verlieren Sie die Verbindung zum System und müssen sich erneut anmelden.

Wenn Sie bestimmte Voreinstellungen nicht wiederherstellen möchten, klicken Sie auf die entsprechenden Kontrollkästchen, um die Auswahl aufzuheben. Wählen Sie ggf. weitere Voreinstellungen aus.

5. Klicken Sie auf **Wiederherstellen**, damit das System die ausgewählten Voreinstellungen wiederherstellt, oder auf **Zurück**, um zum vorherigen Fenster zurückzukehren. Wenn Sie auf **Wiederherstellen** geklickt haben, können Sie den Vorgang nicht mehr abbrechen. Der Wiederherstellungsvorgang dauert etwa eine Minute. Während der Wiederherstellung können Sie nicht zu anderen Bildschirmen im ztC Console-Fenster wechseln. Sie müssen warten, bis der Wiederherstellungsvorgang abgeschlossen ist, bis Sie ein anderes Konsolenfenster anzeigen können.

   In der Spalte **Wiederherstellungsstatus** wird der Status der Wiederherstellung als **In Bearbeitung**, **Abgeschlossen**, **Teilweise abgeschlossen** oder **Fehler** angezeigt. Wenn der Wiederherstellungsvorgang abgeschlossen ist, wird die folgende Meldung eingeblendet:

   > Abgeschlossen! Die oben angezeigten Voreinstellungen wurden erfolgreich wiederhergestellt.

6. Klicken Sie auf **Fertig**. Das Fenster **Systemvoreinstellungen wiederherstellen** wird wieder angezeigt.

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Konfigurieren von e-Alerts

Konfigurieren Sie E-Mail-Alarme (e-Alerts), um dem ztC Edge-System zu ermöglichen, E-Mails an Systemadministratoren zu senden, wenn das System ein Ereignis erkennt, dass das Eingreifen des Administrators erfordert.

Voraussetzung: Damit e-Alerts korrekt funktionieren, müssen Sie den Mail-Server konfigurieren. Siehe Konfigurieren des Mail-Servers.

So aktivieren Sie e-Alerts

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **Benachrichtigung** auf **e-Alerts**.

3. Aktivieren Sie das Kontrollkästchen **e-Alerts aktivieren**. Es werden Felder für die Eingabe oder Auswahl der folgenden Einstellungen eingeblendet:
    - **e-Alerts-Sprache** – Wählen Sie eine Sprache aus dem Pulldownmenü aus.
    - **Empfängerliste** (erforderlich) – Geben Sie die E-Mail-Adressen für alle e-Alert-Empfänger ein.
4. Klicken Sie auf **Speichern** (oder auf **Zurücksetzen**, um die zuvor gespeicherten Werte wiederherzustellen).

> **Hinweis**: Wenn Sie die e-Alert-Konfiguration aktivieren oder aktualisieren, generieren Sie einen Testalarm, um zu überprüfen, ob die Alarme empfangen werden können.

So generieren Sie einen Testalarm

Klicken Sie auf **Testalarm generieren**. Die Stratus Redundant Linux-Software generiert einen Testalarm und sendet eine Beispiel-E-Mail mit dem Betreff „Testalarm“ an alle E-Mail-Empfänger; SNMP sendet Traps an die Empfänger von SNMP-Traps, sofern konfiguriert (siehe Konfigurieren der SNMP-Einstellungen); und „Supportkonfiguration“ sendet eine Benachrichtigung an Ihren autorisierten Stratus-Servicemitarbeiter, sofern konfiguriert (siehe Konfigurieren der Remotesupport-Einstellungen). Sehen Sie im Alarmverlaufsprotokoll (siehe Die Seite „Alarmverlauf“) nach dem Zustellungsstatus.

Sie können e-Alerts auch testen, indem Sie die sekundäre physische Maschine in den Wartungsmodus versetzen (siehe Wartungsmodus) und dann wieder aus dem Wartungsmodus nehmen. Vergewissern Sie sich, dass Sie für beide Wartungsmodusereignisse e-Alerts erhalten.

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Konfigurieren der SNMP-Einstellungen

Konfigurieren Sie Simple Network Management Protocol (SNMP)-Einstellungen für das ztC Edge-System, damit SNMP-Verwaltungsanwendungen Ihre Systeme remote verwalten können. (SNMP-Informationen gelten nur für Systeme, nicht für einzelne PMs.) Sie können SNMP-Anfragen und SNMP-Traps aktivieren:

- SNMP-Anfrage – Eine Anfrage, die an das System gesendet wird, um die Werte von Objekten abzurufen, die in den von der Stratus Redundant Linux-Software unterstützten MIBs (Management

Informationen Bases) aufgelistet sind. Zu diesen MIBs gehört eine systemspezifische MIB, die eine Sammlung von Objekten darstellt, die das ztC Edge-System beschreiben. Sie finden eine Kopie der MIB-Datei zum Herunterladen im Abschnitt **Drivers and Tools** der Seite **Downloads** unter https://www.stratus.com/services-support/downloads/?tab=ztcedge.

- SNMP-Trap - Eine von einem der Knoten im ztC Edge-System generierte Meldung, die nach Eintritt eines bestimmten Ereignisses (z. B. nach einem Alarm) an eine zuvor definierte Empfängerliste gesendet wird, üblicherweise an eine Netzwerkmanagementstation (NMS).

Folgen Sie der entsprechenden Vorgehensweise zum Aktivieren von SNMP-Anfragen oder -Traps.

So aktivieren Sie SNMP-Anfragen

Um SNMP-Anfragen zu aktivieren, führen Sie eines der folgenden Verfahren aus:

- SNMP-Anfragen auf der Seite **Voreinstellungen** aktivieren:
  - Fügen Sie einen SNMPv3-Benutzer hinzu, der SNMPv3-Anfragen aktivieren kann und der Lesezugriff (schreibgeschützt) auf die gesamte MIB im ztC Edge-System hat.
  - Konfigurieren Sie die Zugriffskontrolle für SNMPv1- und SNMPv2-Anfragen und legen Sie fest, dass keine Benutzer (**Eingeschränkt**) oder beliebige Benutzer aus der öffentlichen Standard-Community (**Nicht eingeschränkt**) Anfragen senden dürfen.
- Passen Sie die SNMP-Anfragefunktion an, indem Sie `snmpd.conf`-Dateien bearbeiten. Sie können die Zugriffskontrolle für SNMPv1- und SNMPv2-Anfragen anpassen. Sie können auch die Liste der Benutzer für SNMPv3-Anfragen anpassen. Weitere Informationen finden Sie unter *So passen Sie die SNMP-Anfragefunktion an* (weiter unten).

So aktivieren Sie SNMP-Anfragen auf der Seite „Voreinstellungen“

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **Benachrichtigung** auf **SNMP-Konfiguration**.
3. Aktivieren Sie das Kontrollkästchen neben **SNMP-Anfragen aktivieren**.
4. Die **Liste der Benutzer für SNMP-Anfragen (Version 3)** wird angezeigt.

   Wenn ein Benutzername unter der **Liste der Benutzer für SNMP-Anfragen (Version 3)** aufgeführt ist, wird die Sicherheitsstufe des Benutzers angezeigt und es ist eine schreibgeschützte Ansicht der Datei `snmpd.conf` zu sehen. Der Benutzer hat Lesezugriff

(schreibgeschützt) auf die gesamte MIB. Beachten Sie, dass das System nur einen Benutzer für **SNMP-Anfragen (Version 3)** zulässt.

Wenn kein Benutzername angezeigt wird, können Sie einen SNMPv3-Benutzer hinzufügen.

So fügen Sie einen SNMPv3-Benutzer hinzu

a. Klicken Sie auf die Schaltfläche **Hinzufügen**, um den Assistenten **Benutzer hinzufügen** zu öffnen.

b. Geben Sie Werte für Folgendes ein:

Benutzername – Der Name des Benutzers, der Zugriff auf den SNMPv3-Agent hat. Der Name muss eindeutig sein.

Sicherheitsstufe – Die Sicherheitsstufe des Benutzers. Gültige Werte sind:

- **Keine Authentifizierung und kein Datenschutz**: Es wird keine Sicherheit auf Nachrichten angewendet; Nachrichten werden weder authentifiziert noch verschlüsselt.
- **Authentifizierung und kein Datenschutz**: Nachrichten werden authentifiziert, aber nicht verschlüsselt. Sie müssen Werte für **Authentifizierungstyp** und **Authentifizierungskennwort** eingeben.
- **Authentifizierung und kein Datenschutz**: Nachrichten werden authentifiziert und verschlüsselt. Sie müssen Werte für **Authentifizierungstyp**, **Authentifizierungskennwort**, **Verschlüsselungstyp** und **Verschlüsselungskennwort** eingeben.

Wenn die Sicherheitsstufe Authentifizierung oder Datenschutz beinhaltet, werden die folgenden Felder angezeigt:

Authentifizierungstyp – Die Art der Authentifizierung des Benutzers. Gültige Werte sind:

- **MD5**: Konfigurieren Sie den Message Digest Algorithm (MD5) als Authentifizierungstyp des Benutzers.
- **SHA**: Konfigurieren Sie den Secure Hash Algorithm (SHA) als Authentifizierungstyp des Benutzers.

Authentifizierungskennwort - Das erforderliche Kennwort des Benutzers, das verwendet wird, um den geheimen Authentifizierungsschlüssel zu generieren. Das Kennwort muss mindestens 8 Zeichen enthalten.

Verschlüsselungstyp - Der Verschlüsselungstyp des Benutzers. Gültige Werte sind:

- **AES**: Konfigurieren Sie den Advanced Encryption Standard (AES) als Verschlüsselungstyp des Benutzers.
- **DES**: Konfigurieren Sie den Data Encryption Standard (DES) als Verschlüsselungstyp des Benutzers.

Verschlüsselungskennwort - Das erforderliche Kennwort des Benutzers, das verwendet wird, um den geheimen Verschlüsselungsschlüssel zu generieren. Das Kennwort muss mindestens 8 Zeichen enthalten.

c. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

5. Wählen Sie eine Zugriffsoption:

   Eingeschränkt (Standard) - Kein Benutzer kann SNMPv1- oder SNMPv2-Anfragen senden.

   Nicht eingeschränkt - Alle Benutzer, die die öffentliche Standardcommunity verwenden, können SNMPv1- oder SNMPv2-Anfragen senden.

   Benutzerdefiniert (verfügbar, wenn `snmpd.conf` manuell von einem Benutzer bearbeitet wurde, siehe *So passen Sie die SNMP-Anfragefunktion an* weiter unten) - Erlaubt den benutzerdefinierten Zugriff.

6. Klicken Sie auf **Speichern**. (Oder klicken Sie auf **Zurücksetzen**, um die zuvor gespeicherten Werte wiederherzustellen.)

So passen Sie die SNMP-Anfragefunktion an, indem Sie `snmpd.conf`-Dateien bearbeiten

Passen Sie die SNMP-Anfragefunktion an, indem Sie `snmpd.conf`-Dateien bearbeiten.

Passen Sie die Zugriffskontrolle für SNMPv1- und SNMPv2-Anfragen an, indem Sie die Datei `/etc/snmp/snmpd.conf` bearbeiten:

1. Melden Sie sich beim Host an.
2. Bearbeiten Sie die Standarddatei `/etc/snmp/snmpd.conf` auf beiden Knoten.
3. Speichern Sie die Datei.

4. Starten Sie den `snmpd`-Prozess auf jedem Knoten neu, indem Sie den Befehl **systemctl restart snmpd** eingeben.

Passen Sie die Liste der Benutzer für SNMPv3-Anfragen an, indem Sie die Dateien `/etc/snmp/snmpd.conf` und `/var/lib/net-snmp/snmpd.conf` bearbeiten.

1. Melden Sie sich beim Host an.
2. Bearbeiten Sie die Standarddatei `/etc/snmp/snmpd.conf` auf beiden Knoten.
3. Bearbeiten Sie die Standarddatei `/var/lib/net-snmp/snmp/snmpd.conf` auf beiden Knoten.
4. Speichern Sie die Datei.
5. Starten Sie den `snmpd`-Prozess auf jedem Knoten neu, indem Sie den Befehl **systemctl restart snmpd** eingeben.

So aktivieren Sie SNMP-Traps

Hinweise:

1. Wenn Sie einen Empfänger für **SNMP-Traps (Version 3)** hinzufügen, müssen Sie bestätigen, dass die Engine-ID des Trap-Benutzers auf dem Empfängerserver 0x80001370017F000001 ist.
2. Wenn Sie die SNMP-Trap-Einstellungen aktivieren oder ändern, generieren Sie einen Testalarm, um zu überprüfen, ob die Traps empfangen werden.

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **Benachrichtigung** auf **SNMP-Konfiguration**.
3. Aktivieren Sie das Kontrollkästchen neben **SNMP-Traps aktivieren**.
4. Geben Sie den Namen der SNMP-**Community** ein oder lassen Sie den Standardwert (**public**) unverändert.
5. Unter der **Liste der Empfänger von SNMP-Traps (Version 3)** sehen Sie eine Liste der Trap-Benutzer sowie die IP-Adresse des Empfängerservers, auf dem der Trap-Benutzer eingerichtet ist. Das ztC Edge-System sendet SNMPv3-Traps an den Trap-Benutzer auf dem Empfängerserver. Fügen Sie ggf. einen Empfänger hinzu.

   So fügen Sie einen Empfänger hinzu

a. Klicken Sie auf die Schaltfläche **Hinzufügen**, um den Assistenten **Empfänger hinzufügen** zu öffnen.

b. Geben Sie Werte für Folgendes ein:

Empfängeradresse - Der Hostname oder die IPv4-Adresse des Empfängerservers.

Benutzername - Der Name des Trap-Benutzers auf dem Empfängerserver. Der Name muss für den Empfänger eindeutig sein.

Sicherheitsstufe - Die Sicherheitsstufe des Benutzers. Gültige Werte sind:

- **Keine Authentifizierung und kein Datenschutz**: Es wird keine Sicherheit auf Nachrichten angewendet; Nachrichten werden weder authentifiziert noch verschlüsselt.
- **Authentifizierung und kein Datenschutz**: Nachrichten werden authentifiziert, aber nicht verschlüsselt. Sie müssen Werte für **Authentifizierungstyp** und **Authentifizierungskennwort** eingeben.
- **Authentifizierung und kein Datenschutz**: Nachrichten werden authentifiziert und verschlüsselt. Sie müssen Werte für **Authentifizierungstyp**, **Authentifizierungskennwort**, **Verschlüsselungstyp** und **Verschlüsselungskennwort** eingeben.

Wenn die Sicherheitsstufe Authentifizierung oder Datenschutz beinhaltet, werden die folgenden Felder angezeigt:

Authentifizierungstyp - Die Art der Authentifizierung des Benutzers. Gültige Werte sind:

- **MD5**: Konfigurieren Sie den Message Digest Algorithm (MD5) als Authentifizierungstyp des Benutzers.
- **SHA**: Konfigurieren Sie den Secure Hash Algorithm (SHA) als Authentifizierungstyp des Benutzers.

Authentifizierungskennwort - Das erforderliche Kennwort des Benutzers, das verwendet wird, um den geheimen Authentifizierungsschlüssel zu generieren. Das Kennwort muss mindestens 8 Zeichen enthalten.

Verschlüsselungstyp - Der Verschlüsselungstyp des Benutzers. Gültige Werte sind:

- **AES**: Konfigurieren Sie den Advanced Encryption Standard (AES) als Verschlüsselungstyp des Benutzers.
- **DES**: Konfigurieren Sie den Data Encryption Standard (DES) als Verschlüsselungstyp des Benutzers.

Verschlüsselungskennwort - Das erforderliche Kennwort des Benutzers, das verwendet wird, um den geheimen Verschlüsselungsschlüssel zu generieren. Das Kennwort muss mindestens 8 Zeichen enthalten.

c. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

6. Klicken Sie auf **Speichern**. (Oder klicken Sie auf **Zurücksetzen**, um die zuvor gespeicherten Werte wiederherzustellen.)
7. Konfigurieren Sie die Firewall Ihres Unternehmens so, dass SNMP-Vorgänge zugelassen werden, damit SNMP-Managementsystem Alarme empfangen und Traps an das ztC Edge-System senden können. Öffnen Sie dazu in der Firewall Ihres Unternehmens den SNMP-Port:

   Nachrichtentyp: SNMP
   Protokoll: SNMP
   Port: 161(Get/Walk) 162(Traps)

8. Generieren Sie einen Testalarm, indem Sie auf **Testalarm generieren** klicken.

   Die Stratus Redundant Linux-Software generiert einen Testalarm und „SNMP“ sendet Traps an die Empfänger von SNMP-Traps; „e-Alerts“ sendet eine Beispiel-E-Mail mit dem Betreff „Testalarm“ an alle E-Mail-Empfänger von e-Alerts, sofern konfiguriert (siehe Konfigurieren von e-Alerts); und „Supportkonfiguration“ sendet eine Benachrichtigung an Ihren autorisierten Stratus-Servicemitarbeiter, sofern konfiguriert (siehe Konfigurieren der Remotesupport-Einstellungen). Sehen Sie im Alarmverlaufsprotokoll (siehe Die Seite „Alarmverlauf“) nach dem Zustellungsstatus.

Verwandte Themen

SNMP

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Sicherheitsverstärkung

Konfigurieren der OPC-Einstellungen

Konfigurieren Sie Open Platform Communication (OPC)-Einstellungen, um die OPC-Server-Funktionalität zu aktivieren. Diese veröffentlicht Daten zur ztC Edge-Systemleistung, die dann auf einem OPC-Client empfangen und angezeigt werden können. So können Sie das ztC Edge-System zusammen mit anderen industriellen Anlagen überwachen.

Damit Sie die OPC-Funktionalität nutzen können, müssen Sie OPC-Clientsoftware (Ihrer Wahl) auf einem separaten Computer installieren und dann den OPC-Client konfigurieren (siehe *So installieren und konfigurieren Sie einen OPC-Client*). Der OPC-Client muss so konfiguriert werden, dass er Daten von dem Port des ztC Edge-System empfangen kann, den Sie für OPC konfigurieren. Der Standardport ist 4840, Sie können jedoch auch eine andere Portnummer festlegen.

So konfigurieren Sie OPC-Einstellungen

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **Benachrichtigung** auf **OPC-Konfiguration**.
3. Aktivieren Sie das Kontrollkästchen neben **OPC-Server aktivieren**.
4. Standardmäßig wird die Portnummer **4840** verwendet. Falls nötig, können Sie eine andere Nummer angeben.
5. Aktivieren Sie eines oder beide der folgenden Kontrollkästchen wie für Ihr System geeignet:

   Anonyme OPC-Clientverbindungen zulassen - OPC-Clients können auch ohne Benutzernamen und Kennwort eine Verbindung zum OPC-Server im ztC Edge-System herstellen. (Wenn das Kontrollkästchen nicht aktiviert ist, müssen OPC-Clients einen Benutzernamen und ein Kennwort angeben.)

OPC-Clientverbindungen zulassen, die unter „Benutzer & Gruppen“ konfigurierte Benutzernamen und Kennwörter verwenden - OPC-Clients können sich mit demselben Benutzernamen und Kennwort beim OPC-Server im ztC Edge-System anmelden, die sie auch für die Anmeldung bei der ztC Console verwenden. (Wenn das Kontrollkästchen nicht aktiviert ist, können sich OPC-Clients nicht mit den Benutzernamen und Kennwörtern lokaler Benutzerkonten anmelden, die auf der Seite **Benutzer und Gruppen** angegeben sind. Siehe Verwalten lokaler Benutzerkonten.)

6. Klicken Sie auf **Speichern**. (Oder klicken Sie auf **Zurücksetzen**, um die zuvor gespeicherten Werte wiederherzustellen.)

So installieren und konfigurieren Sie einen OPC-Client

Sie müssen einen separaten Computer verwenden, um die OPC-Clientsoftware zu installieren und einen OPC-Client zu konfigurieren. Sie können eine beliebige OPC-Clientsoftware verwenden; es sind viele Versionen erhältlich. Nachstehend wird beschrieben, wie Sie einen OPC-Client mit der Software UaExpert® von Unified Automation installieren und konfigurieren.

Installieren und Konfigurieren eines OPC-Clients mit UaExpert-Software

> **Hinweis**: Lesen Sie die folgenden Informationen und orientieren Sie sich an den Anweisungen der UaExpert-Software.

1. Laden Sie die Windows-Version der UaExpert-Software herunter. Siehe https://www.unified-automation.com/products/development-tools/uaexpert.html.
2. Wenn Sie die UaExpert-Software zum ersten Mal starten, folgen Sie den Anweisungen der Software für den erstmaligen Start.
3. Führen Sie die UaExpert-Software aus.

   Das Hauptfenster **Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject** wird geöffnet.
4. Klicken Sie in der Menüleiste auf **Server** und wählen Sie **Add** (Hinzufügen). Das Dialogfeld **Add Server** (Server hinzufügen) wird angezeigt.
5. Klicken Sie auf die Registerkarte **Advanced** (Erweitert).
6. Geben Sie in das Feld **Endpoint Url** (Endpunkt-URL) die URL des Endpunkts ein. Dies ist die Cluster-IP-Adresse des ztC Edge-Systems (zum Beispiel **opc.tcp://*tcp_cluster_ip_address*:4840/**).

7. Wählen Sie unter **Security Settings** (Sicherheitseinstellungen) die Option **None** (Ohne) für **Security Policy** (Sicherheitsrichtlinie) und **Message Security Mode** (Meldungssicherheitsmodus).
8. Wählen Sie für **Authentication Settings** (Authentifizierungseinstellungen) eine der folgenden Optionen aus, die zu Ihrer Konfiguration passt:

   Anonymous (Anonym – Wählen Sie diese Option, wenn Sie das Kontrollkästchen aktiviert haben, um anonyme OPC-Clientverbindungen zuzulassen.

   Username (Benutzername) und **Password** (Kennwort) – Geben Sie hier Werte ein, wenn Sie das Kontrollkästchen aktiviert haben, um zuzulassen, dass OPC-Clientverbindungen Benutzernamen und Kennwörter verwenden. Benutzername und Kennwort müssen mit den entsprechenden Daten übereinstimmen, die Sie für einen Benutzer mit Lesezugriff (read-only) im ztC Edge-System für den OPC-Zugriff hinzufügen. Unter Verwalten lokaler Benutzerkonten finden Sie Informationen zum Hinzufügen eines Benutzers zum ztC Edge-System.
9. Klicken Sie auf **OK**, um das Dialogfeld **Add Server** (Server hinzufügen) zu schließen.

   Es wird wieder das Hauptfenster angezeigt. Im Bereich auf der linken Seite wird der Name des Servers im Feld **Project** (Project) unter **Servers** (Server) angezeigt.
10. Wählen Sie den neuen Server aus und klicken Sie dann auf die Verbindungsschaltfläche, die in der Symbolleiste rechts neben dem Minuszeichen angezeigt wird.

    Wenn der Client erfolgreich eine Verbindung zum Server herstellt, wird im Hauptfenster im Feld **Address Spaces** (Adressräume) der Endpunkt des Servers angezeigt.

Im Feld **Address Spaces** (Adressräume) können Sie auf die oberste Ebene klicken, um sie zu erweitern und die verfügbaren Datenwerte zu sehen. Im Feld **Attributes** (Attribute) wird in der Spalte **Value** (Wert) der aktuelle Wert des ausgewählten Elements angezeigt.

Verwandte Themen

Anzeigen der OPC-Ausgabe

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Anzeigen der OPC-Ausgabe

Nachdem Sie die OPC-Serverfunktion auf dem ztC Edge-System aktiviert haben, kann ein OPC-Client (auf einem Computer, der nicht das ztC Edge-System ist) die Performancedaten des Systems anzeigen. Die Daten sind nach Adressraum aufgeteilt, wobei jeder Adressraum wiederum in Unterobjekte mit mehreren Datenelementen unterteilt ist. Die OPC-Serverfunktion auf dem ztC Edge-System übergibt Werte für die Datenelemente an den OPC-Client, der die Daten dann anzeigt.

In diesem Thema wird beschrieben, wie ztC Edge-Systeminformationen über einen OPC-Client angezeigt werden, der mit UaExpert®-Software von Unified Automation erstellt wurde.

So zeigen Sie die OPC-Ausgabe an

1. Öffnen Sie den OPC-Client auf dem Computer, auf dem Sie ihn erstellt haben.
2. Klicken Sie im (linken) Bereich **Project** auf **Project**, **Servers** und dann auf **ztC OPC Server**.

   Im linken Fenster unter **Project** sehen Sie **Address Space** (Adressraum). Nachdem Sie **ztC OPC Server** ausgewählt haben, zeigt der Bereich **Address Space** die **Root**-Hierarchie an.
3. Klicken Sie im Bereich **Address Space** auf **Objects** (unter **Root**). Unter **Objects** können Sie **Server** und **ztC** auswählen.

   - **Server**

     Um Informationen über den Knoten aufzurufen, auf dem der OPC-Server zurzeit ausgeführt wird, zeigen Sie das Unterobjekt **BuildInfo** an: klicken Sie auf **Server** und dann auf **ServerStatus**.

     Das Unterobjekt **BuildInfo** zeigt Werte für die folgenden Datenelemente an:

Datenelemente	Beschreibung
ProductUrl	Zeigt **http://www.stratus.com/** an.
ManufacturerName	Zeigt **Stratus Technologies Ireland, Ltd** an.
ProductName	Zeigt den Produktnamen der Hardware an (**ztC Edge**).
SoftwareVersion	Zeigt die Versionsnummer der Stratus Redundant Linux-Software an.

Datenelemente	Beschreibung
BuildNumber	Zeigt die Buildnummer der Stratus Redundant Linux-Software an.
BuildDate	Zeigt das Datum des Stratus Redundant Linux-Softwarebuilds an.

Weitere Informationen zum **Server**-Objekt finde Sie in *Part 5: Information Model* der *OPC Unified Architecture Specification*. Diese sind verfügbar unter opcfoundation.org.

- **ztC** Das ztC-Objekt teilt den Adressraum in die folgenden Unterobjekte auf, mit den Datenelementen in den jeweiligen Tabellen:

  Anwendungen

  Die Anwendungsdatenelemente bieten Informationen über die Integrität von Anwendungen.

Datenelemente	Beschreibung
AlertedApplicationsCount	Gibt die Anzahl der Anwendungen in der AlertedApplicationsList an. Datentyp: UInt32.
AlertedApplicationsList	Listet die zurzeit überwachten Anwendungen auf, die einen anderen Status als „normal“ haben oder deren Status nicht verfügbar ist (*Wird nicht ausgeführt*, *Antwortet nicht*, *Nicht verfügbar* und *Nicht gefunden*). Diese Liste enthält auch Anwendungen mit einer gestoppten VM. Die Liste enthält keine Überwachungen, die nicht aktiviert sind (Anwendungsüberwachungen, die im Bereich **Anwendungen** der Registerkarte **Überwachen** ohne aktiviertes Kontrollkästchen **Aktiviert** aufgeführt sind).

Datenelemente	Beschreibung
	Datentyp: dynamisches Array von Zeichenfolgen.
AllApplicationsHealthy	Gibt an, ob eine überwachte Anwendung eine Warnung hat oder nicht: *true* zeigt an, dass keine Warnungen vorliegen; *false* gibt an, dass für mindestens eine überwachte Anwendung eine Warnung vorliegt. Datentyp: Boolesch.
ApplicationMonitoringEnabled	Gibt an, ob die Anwendungsüberwachung lizenziert und eingeschaltet ist: *true* zeigt an, dass sie eingeschaltet ist; *false* zeigt an, dass sie nicht eingeschaltet ist. Datentyp: Boolesch.
ApplicationsCount	Gibt an, wie viele Anwendungen zurzeit überwacht werden. Dieser Wert sollte mit der Anzahl der Anwendungen in ApplicationsList übereinstimmen. Datentyp: UInt32.
ApplicationsList	Listet die zurzeit überwachten Anwendungen auf. Es handelt sich um ein eindimensionales Array, das zunimmt oder abnimmt, wenn überwachte Anwendungen hinzugefügt oder entfernt werden. Die Liste enthält keine Überwachungen, die nicht aktiviert sind (Anwendungsüberwachungen, die im Bereich **Anwendungen** der Registerkarte **Überwachen** ohne aktiviertes Kontrollkästchen **Aktiviert** aufgeführt sind). Die aufgeführten Namen enthalten den Namen der VM als Präfix

Datenelemente	Beschreibung
	des Anwendungsnamens (z. B. vm1/testapp.exe). Datentyp: dynamisches Array von Zeichenfolgen.

Physische Maschinen

Die Datenelemente für physische Maschinen geben Informationen zur Integrität der einzelnen Knoten in einem System an.

Datenelemente	Beschreibung
AllPhysicalMachinesHealthy	Gibt an, ob beide Knoten in einem stabilen Zustand sind: *true* zeigt an, dass beide Knoten vorhanden sind, mit grünen Prüfhäkchen laufen und sich nicht im Wartungsmodus befinden; *false* gibt an, dass mindestens ein Knoten nicht vorhanden ist, nicht mit grünen Prüfhäkchen läuft und/oder sich im Wartungsmodus befindet. Datentyp: Boolesch.
Knoten0 *und* Knoten1	Node*n*HostState: Der Hostzustand. Gültige Werte sind *exiled*, *failed*, *firmware*, *imaging*, *lost*, *nfc*, *off*, *proto*, *running*, *starting*, *stopping*, *unlicensed* und *unreachable*.
	Node*n*IPaddress: Die IP-Adresse des Knotens.
	Node*n*MaintenanceMode: Der Wartungsmodus des Hosts. Gültige Werte sind *Evakuierung*, *Wartung* und *normal*.

Datenelemente	Beschreibung
	Node*n*Exists: Gibt an, ob der Knoten im System bekannt ist oder nicht: *true* zeigt ,an, dass der Knoten erfolgreich in das System eingebunden wurde; *false* zeigt an, dass dem System kein zweiter Knoten hinzugefügt wurde oder dass ein zweiter Knoten hinzugefügt, aber später entfernt wurde. Wenn der Wert *false* ist, ignorieren Sie alle anderen Informationen zu Knoten*n*.
	Node*n*VirtualMachineList: Listet die virtuellen Maschinen (VM) auf, die auf diesem Knoten ausgeführt werden.
	Node*n*CombinedState: Zeigt eine Kombination aus Node*n*MaintenanceMode, Node*n*Exists und Node*n*HostState an wie folgt: ◦ Node*n*CombinedState lautet *missing* , wenn Node*n*Exists den Wert *false* hat. ◦ Node*n*CombinedState ist entweder *evacuating* oder *maintenance*, wenn Node*n*Exists den Wert *true* hat, Node*n*HostState den Wert *running* hat und Node*n*MaintenanceMode den Wert *evacuating* oder *maintenance* hat. ◦ Wenn Node*n*CombinedState irgendeinen anderen Wert hat, wird damit der Wert von Node*n*HostState angegeben, wobei der Bereich der Werte von Node*n*HostState dem oben

Datenelemente	Beschreibung
	genannten entspricht.
PhysicalMachinesList	Listet die vorhandenen Knoten auf. Datentyp: dynamisches Array von Zeichenfolgen.
PhysicalMachinesWarningCount	Gibt an, wie viele physische Maschinen nicht mit einem grünen Prüfhäkchen markiert sind. Datentyp: UInt32.
PhysicalMachinesWarningList	Listet die physischen Maschinen auf, die Probleme melden. Hier sind normalerweise beide Knoten aufgeführt; wenn der zweite Knoten zum Beispiel im Wartungsmodus ist, wird der erste als unsicher gekennzeichnet. Datentyp: dynamisches Array von Zeichenfolgen.
PrimaryPhysicalMachine	Zeigt den Namen des aktuellen primären Knotens an. Datentyp: Zeichenfolge.

Virtuelle Maschinen

Die Datenelemente für virtuelle Maschinen geben Informationen zum Status der VMs an, die im System ausgeführt werden.

Datenelemente	Beschreibung
AllVirtualMachinesHealthy	Gibt an, ob irgendeine VM einen Warnungs- oder Fehlerstatus hat: *true* zeigt an, dass alle VMs mit einem grünen Prüfhäkchen markiert sind; *false*

Datenelemente	Beschreibung
	zeigt an, dass mindestens eine VM nicht mit einem grünen Prüfhäkchen markiert ist. Datentyp: Boolesch.
FTVirtualMachinesList	Zeigt die Namen der FT VMs an, die im System vorhanden sind. Datentyp: dynamisches Array von Zeichenfolgen.
GetPhysicalMachine	Gibt an, auf welcher physischen Maschine die angegebene VM ausgeführt wird. Datentyp: Funktion, die eine Zeichenfolge annimmt und eine Zeichenfolge zurückgibt; das Eingabeargument der Funktion ist eine Zeichenfolge, die einem VM-Namen entspricht, und die Ausgabe ist eine Zeichenfolge (Knoten0 oder Knoten1), die angibt, auf welcher physischen Maschine die im Eingabeargument angegebene VM ausgeführt wird).
HAVirtualMachinesList	Zeigt die Namen der HA VMs an, die im System vorhanden sind. Datentyp: dynamisches Array von Zeichenfolgen.
RunningVirtualMachinesCount	Gibt die Anzahl der VMs in RunningVirtualMachinesList an. Datentyp: UInt32.
RunningVirtualMachinesList	Gibt die Namen der VMs mit dem Status *running* (wird ausgeführt) an.

Datenelemente	Beschreibung
	Datentyp: dynamisches Array von Zeichenfolgen.
StoppedVirtualMachinesCount	Gibt die Anzahl der VMs in StoppedVirtualMachinesList an. Datentyp: UInt32.
StoppedVirtualMachinesList	Liste der VMs mit dem Status *stopped* (ignoriert Übergangszustände wie *booting*). Datentyp: dynamisches Array von Zeichenfolgen.
VirtualMachinesCount	Gibt an, wie viele VMs im System vorhanden sind. Datentyp: UInt32.
VirtualMachinesList	Liste der VMs, die im System vorhanden sind. Datentyp: dynamisches Array von Zeichenfolgen.

System

Die Datenelemente für das System geben übergeordnete Statusinformationen sowie Informationen zu den Zugriffsmethoden für das gesamte System an.

Datenelemente	Beschreibung
ManagementConnectionGood	Gibt an, ob der OPC-Server Informationen vom ztC Edge-System abrufen kann: *true* zeigt an, dass der Server Informationen vom System abrufen kann; *false* zeigt an, dass der Server keine Informationen abrufen kann.

Datenelemente	Beschreibung
	Datentyp: Boolesch.
ManagementIP	Gibt die IP-Adresse des ztC Edge-Systems an. Datentyp: Zeichenfolge.
ManagementURL	Gibt die HTTP-Adresse der ztC Console an. Datentyp: Zeichenfolge.
OutstandingSeverity	Entspricht dem Symbol für den allgemeinen Systemstatus auf der Anmeldeseite. Datentyp: Zeichenfolge.
SecureManagementURL	Gibt die HTTPS-Adresse der ztC Console an. Datentyp: Zeichenfolge.

Verwandte Themen

Konfigurieren der OPC-Einstellungen

Konfigurieren der Remotesupport-Einstellungen

Wenn Sie sich zum ersten Mal beim ztC Edge-System anmelden, konfigurieren Sie die Supporteinstellungen, die es dem ztC Edge-System ermöglichen, Supportbenachrichtigungen (Alarme) an Ihren autorisierten Stratus-Servicemitarbeiter zu senden, wenn ein Ereignis ein Eingreifen erfordert.

So konfigurieren Sie die Einstellungen für die Supportkonfiguration

Hinweis: Wenn Sie die Einstellungen für **Zugriff für Remotesupport aktivieren** oder **Benachrichtigungen aktivieren** aktivieren oder ändern, generieren Sie einen Testalarm, um zu überprüfen, ob Sie Meldungen zur Systemintegrität von Ihrem System an Ihren autorisierten Stratus-Servicemitarbeiter senden können.

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.

2. Klicken Sie unter **Remotesupport** auf **Supportkonfiguration**.
3. Modifizieren Sie die Einstellungen passend zu Ihrem System:
   - **Zugriff für Remotesupport aktivieren** berechtigt Ihren autorisierten Stratus-Servicemitarbeiter, zur Fehlerbehebung remote eine Verbindung zum ztC Edge-System herzustellen. Nachdem Sie diese Einstellung aktiviert haben, können Sie sie bei Bedarf deaktivieren.
   - **Benachrichtigungen aktivieren** ermöglicht es dem ztC Edge-System, Integritäts- und Statusbenachrichtigungen an Ihren autorisierten Stratus-Servicemitarbeiter zu senden.
     - **Supportbenachrichtigungen aktivieren** sendet einen Alarm für jedes Ereignis, das ein Eingreifen erfordert. Außerdem wird eine regelmäßige Call-Home-Nachricht („Heartbeat“) an Ihren autorisierten Stratus-Servicemitarbeiter gesendet.
     - **Regelmäßige Berichterstellung aktivieren** sendet eine tagesaktuelle Zusammenfassung der Systeminformationen, damit die Produkt- und Dienstqualität verbessert werden kann.
4. Klicken Sie auf **Speichern** (oder auf **Zurücksetzen**, um die zuvor gespeicherten Werte wiederherzustellen).
5. Konfigurieren Sie die Firewall Ihrer Organisation, um Supportnachrichten zuzulassen.

So konfigurieren Sie Ihre Firewall, um Supportbenachrichtigungen zu ermöglichen

Verwenden Sie die folgenden Informationen, um die Firewall Ihrer Organisation für die Kommunikation mit Ihrem autorisierten Stratus-Servicemitarbeiter zu konfigurieren:

Nachrichtentyp: Call-Home und Lizenzierung
Protokoll: TCP
Port 443
Stratus Support-Server-Adresse: *.stratus.com

Nachrichtentyp: Supportdiagnose
Protokoll: TCP
Port 443
Stratus Support-Server-Adresse: *.stratus.com

Nachrichtentyp: Einwahl
Protokoll: TCP
Port: 443, Standardproxyport: 3128 (Sie können die standardmäßige Proxyportnummer

ändern.)

Stratus Support-Server-Adresse: *.ecacsupport.com

Nachrichtentyp: e-Alert

Protokoll: SMTP

Port 25

(Weitere Informationen zu TCP- und UDP-Ports finden Sie in der Knowledge Base im Artikel *TCP and UDP ports used by ztC Edge* (KB-9357). Siehe Zugriff auf Artikel in der Knowledge Base.)

Damit das SNMP-Verwaltungssystem Alarme empfangen und Traps an das ztC Edge-System senden kann, konfigurieren Sie die Firewall wie folgt:

Nachrichtentyp: SNMP

Protokoll: SNMP

Port: 161(Get/Walk) 162(Traps)

6. Generieren Sie einen Testalarm.

So generieren Sie einen Testalarm

Klicken Sie auf **Testalarm generieren**. Die Stratus Redundant Linux-Software generiert einen Testalarm und „Supportkonfiguration“ sendet eine Benachrichtigung an Ihren autorisierten Stratus-Servicemitarbeiter; „e-Alerts“ sendet eine Beispiel-E-Mail mit dem Betreff „Testalarm“ an alle E-Mail-Empfänger von Testalarmen, sofern konfiguriert (siehe Konfigurieren von e-Alerts); und SNMP sendet Traps an Empfänger von SNMP-Traps, sofern konfiguriert (siehe Konfigurieren der SNMP-Einstellungen). Sehen Sie im Alarmverlaufsprotokoll (siehe Die Seite „Alarmverlauf“) nach dem Zustellungsstatus. Falls die Supportbenachrichtigung fehlschlägt, wird ein Folgealarm generiert.

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Konfigurieren der Internetproxyeinstellungen

Konfigurieren Sie die Proxyeinstellungen für das ztC Edge-System, falls Ihre Organisation für den Internetzugriff einen Proxyserver erfordert und Sie eine Dienstvereinbarung mit Stratus oder einem anderen

autorisierten ztC Edge-Servicerepräsentanten haben.

Ein Proxyserver stellt eine sichere Brücke zwischen dem ztC Edge-System und dem Internet bereit. Stratus Redundant Linux verwendet Proxyserverinformationen für ausgehenden HTTP-Datenverkehr, der mit Supportbenachrichtigungen und der Remotesupport-Funktion zu tun hat.

So konfigurieren Sie Internetproxyeinstellungen

1. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
2. Klicken Sie unter **Remotesupport** auf **Proxykonfiguration**.
3. Um den Proxydienst zu aktivieren, klicken Sie auf das Kontrollkästchen **Proxy aktivieren**.
4. Geben Sie in das Feld **Proxyserver** den vollständig qualifizierten Hostnamen oder die IP-Adresse des Proxyservers ein.
5. Geben Sie in das Feld **Portnummer** die Portnummer ein, falls sie sich von der Standardnummer (3128) unterscheidet.
6. Falls für den Proxyserver eine Authentifizierung erforderlich ist, aktivieren Sie das Kontrollkästchen **Authentifizierung aktivieren** und geben Sie den **Benutzernamen** und das **Kennwort** ein.

   Wenn Sie kein Kennwort eingeben, ist weiterhin das alte Kennwort erforderlich. Falls zuvor kein Kennwort verwendet wurde und Sie kein neues Kennwort eingeben, bleibt das Kennwortfeld leer.
7. Klicken Sie auf **Speichern** (oder auf **Zurücksetzen**, um die zuvor gespeicherten Werte wiederherzustellen).

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Die Seite „Alarmverlauf“

Auf der Seite **Alarmverlauf** werden Meldungen zu Ereignissen im ztC Edge-System angezeigt.

Um die Seite **Alarmverlauf** zu öffnen, klicken Sie im linken Navigationsbereich der ztC Console auf **Alarmverlauf**. (Um ein Protokoll der Benutzeraktivität im ztC Edge-System zu sehen, lesen Sie Die Seite „Auditprotokolle“.)

Hinweis: Supportbenachrichtigungen, e-Alerts und SNMP-Traps werden nur dann generiert, wenn Sie sie in der ztC Console-Konsole aktiviert haben. Weitere Informationen finden Sie unter:

- Konfigurieren der Remotesupport-Einstellungen
- Konfigurieren von e-Alerts
- Konfigurieren der SNMP-Einstellungen

Um Alarminformationen anzuzeigen, blättern Sie durch die Alarme, die standardmäßig in umgekehrter chronologischer Reihenfolge aufgelistet sind. Klicken Sie auf einen Alarm, um den Zeitpunkt, zu dem der Alarm aufgetreten ist, sowie Informationen zu dem Problem und zur Lösung (falls verfügbar) anzuzeigen. Auf diese Weise sehen Sie auch, ob **Supportbenachrichtigungen**, ein **e-Alert** oder eine **SNMP-Trap** für diesen Alarm gesendet wurde. (Sie können Alarminformationen auch mit `snmptable` anzeigen, siehe Beziehen der System-Informationen mit snmptable.)

Um einen Alarm zu entfernen, wählen Sie ihn aus und klicken Sie auf **Entfernen**.

Um alle Alarme zu entfernen, klicken Sie auf **Alle löschen**.

Verwandte Themen

Die ztC Console

Verwenden der ztC Console

Die Seite „Auditprotokolle“

Auf der Seite **Auditprotokolle** wird ein Protokoll der Benutzeraktivitäten in der ztC Console angezeigt. Um diese Seite zu öffnen, klicken Sie im linken Navigationsbereich auf **Auditprotokolle**. (Wie Sie Informationen zu Ereignissen im ztC Edge-System anzeigen, lesen Sie unter Die Seite „Alarmverlauf“.)

Um Protokollinformationen anzuzeigen, blättern Sie durch die Protokolleinträge, die standardmäßig in umgekehrter chronologischer Reihenfolge aufgelistet sind. Die Informationen enthalten Folgendes:

- **Zeit** - Das Datum und die Uhrzeit der Aktion.
- **Benutzername** - Der Name des Benutzers, der die Aktion initiiert hat.
- **Ursprünglicher Host** - Die IP-Adresse des Hosts, auf dem die ztC Console ausgeführt wurde.
- **Aktion** - Die Aktion, die in der ztC Console ausgeführt wurde.

(Sie können Informationen zu Auditprotokollen auch mit `snmptable` anzeigen, siehe Beziehen der System-Informationen mit snmptable.)

Verwandte Themen

Die ztC Console

Verwenden der ztC Console

Sicherheitsverstärkung

Die Seite „Supportprotokolle“

Auf der Seite **Supportprotokolle** können Sie Diagnosedateien erstellen, welche die Protokolldateien des ztC Edge-Systems und Informationen zur Konfiguration zu einem bestimmten Zeitpunkt enthalten. Wenn Sie diese Informationen an Ihren autorisierten Stratus-Servicemitarbeiter senden, kann er Probleme im System leichter beheben.

Weitere Informationen finden Sie unter:

- Erstellen einer Diagnosedatei
- Löschen einer Diagnosedatei
- Hochladen einer Diagnosedatei an den Kundensupport

Verwandte Themen

Die ztC Console

Verwenden der ztC Console

Die Seite „Voreinstellungen“

Erstellen einer Diagnosedatei

Diagnosedateien enthalten die Protokolldateien des ztC Edge-Systems und Informationen zur Konfiguration zu einem bestimmten Zeitpunkt. Sie können eine Diagnosedatei erstellen, um Ihren autorisierten Stratus-Servicemitarbeiter beim Beheben von Problemen mit dem System zu unterstützen.

Hinweis: Die Stratus Redundant Linux-Software weist eine bestimmte Speichermenge für Diagnosedateien zu. Falls beim Erstellen einer Diagnosedatei nicht genügend Speicherplatz vorhanden ist, löscht das System zuvor erstellte Dateien.

So erstellen Sie Diagnosedateien

1. Klicken Sie im linken Navigationsbereich auf **Supportprotokolle**, um die Seite **Supportprotokolle** zu öffnen.
2. Klicken Sie auf **Diagnosedatei generieren**.
3. Laden Sie die Datei an Ihren autorisierten Stratus-Servicemitarbeiter hoch wie unter Hochladen einer Diagnosedatei an den Kundensupport beschrieben.

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Hochladen einer Diagnosedatei an den Kundensupport

Laden Sie eine Diagnosedatei an die Kundensupport-Website von Stratus ztC Edge hoch, damit Probleme mit dem System schneller gelöst werden können. (Informationen zum Erstellen einer Diagnosedatei finden Sie unter Erstellen einer Diagnosedatei.)

So laden Sie eine Diagnosedatei an den Kundensupport hoch

1. Klicken Sie im linken Navigationsbereich auf **Supportprotokolle**, um die Seite **Supportprotokolle** zu öffnen.
2. Führen Sie einen der folgenden Schritte aus:
   - Falls das ztC Edge-System mit dem Internet verbunden ist, laden Sie die Diagnosedatei direkt an die Kundensupport-Website von Stratus ztC Edge hoch, indem Sie auf **Hochladen** klicken. Wenn der Upload erfolgreich ist, wird eine Meldung eingeblendet, die bestätigt, dass die Diagnosedatei erfolgreich hochgeladen wurde.
   - Falls das ztC Edge-System nicht mit dem Internet verbunden ist oder der **Upload** fehlschlägt, können Sie die Diagnosedatei manuell auf die Website „**Stratus Diagnostic Upload**“ hochladen. Klicken Sie in der ztC Console auf **Herunterladen**, um die Diagnosedatei als ZIP-Datei auf den lokalen Computer herunterzuladen. Übertragen Sie die Diagnosedatei (im ZIP-Format) an einen Computer mit Internetverbindung. Öffnen Sie einen Webbrowser und geben Sie die URL http://diags.stratus.com/DiagUpload.html in die Adresszeile ein. Klicken Sie auf

der Seite **Stratus Diagnostic Upload** auf **Choose File** (Datei auswählen), wählen Sie die ZIP-Datei auf dem Computer aus und klicken Sie dann auf **Submit** (Senden).

Wenn Sie dabei Hilfe brauchen, wenden Sie sich telefonisch an den ztC Edge-Kundensupport unter der Nummer, die Sie auf der Seite **ztC Edge Support** unter https://www.stratus.com/services-support/customer-support/?tab=ztcedge finden.

Wenn Sie sicher sind, dass Sie die Datei nicht mehr brauchen (zum Beispiel, wenn der Kundensupport den korrekten Upload bestätigt hat) können Sie sie optional vom ztC Edge-System löschen. Dies wird unter Löschen einer Diagnosedatei beschrieben.

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Löschen einer Diagnosedatei

Löschen Sie eine Diagnosedatei aus dem ztC Edge-System, nachdem Sie sie an Ihren autorisierten Stratus-Servicemitarbeiter hochgeladen haben.

So löschen Sie eine Diagnosedatei

1. Klicken Sie im linken Navigationsbereich auf **Supportprotokolle**, um die Seite **Supportprotokolle** zu öffnen.
2. Wählen Sie die Diagnosedatei aus und klicken Sie auf **Löschen**.

Verwandte Themen

Die ztC Console

Die Seite „Voreinstellungen“

Verwenden der ztC Console

Die Seite „Physische Maschinen“

Auf der Seite **Physische Maschinen** verwalten Sie die physischen Maschinen (PMs) im ztC Edge-System. (PMs werden auch als Knoten bezeichnet.) Um diese Seite zu öffnen, klicken Sie im linken Navigationsbereich auf **Physische Maschinen**.

Die Spalten **Zustand**, **Aktivität**, **Name**, **Modell** und **Anzahl VMs** werden direkt unter der Titelleiste **PHYSISCHE MASCHINEN** angezeigt. Um eine bestimmte PM zu verwalten, klicken Sie auf **Knoten0 (primär)** oder **Knoten1** (falls vorhanden) unter **Name**. Zur Interpretation der PM-Zustände und -Aktivitäten siehe Zustände und Aktivitäten physischer Maschinen. Sie können Informationen zu einem Knoten auch mit dem Befehl `snmptable` anzeigen; siehe Beziehen der System-Informationen mit snmptable.

Im unteren Fensterbereich werden Aktionsschaltflächen und Details zum ausgewählten Knoten angezeigt:

- Aktionsschaltflächen: Je nach Zustand des ausgewählten Knotens werden verschiedene Aktionsschaltflächen angezeigt; nicht aktive Schaltflächen erscheinen abgeblendet. Bei den meisten Wartungsarbeiten müssen Sie auf **Wartung** klicken, wodurch ein Knoten in den Wartungsmodus versetzt wird (siehe Wartungsmodus). Weitere Informationen zu zusätzlichen PM-Aktionen im Wartungsmodus finden Sie unter Aktionen für physische Maschinen oder im Hilfethema für die entsprechende Aufgabe, die Sie ausführen möchten.
- Ausführliche Informationen: Um ausführliche Informationen oder Statistiken zum ausgewählten Knoten anzuzeigen, klicken Sie auf eine der folgenden Registerkarten:
  - **Übersicht** (in der ursprünglichen Anzeige) zeigt Informationen zum Knoten an, zum Beispiel (falls zutreffend) den Hersteller, das Modell, die Seriennummer, den Gesamtzustand, die Aktivität und die Konfiguration (Arbeitsspeicher und logische Laufwerke) für den ausgewählten Knoten.
  - **Beschreibung** zeigt ein Textfeld an, in das Sie Informationen über den Knoten eingeben können.
  - **Speicher** zeigt den Zustand, die logische ID, die Größe und die verwendete Größe des Speichers an. Außerdem wird die verbleibende Lebensdauer von SSD-Laufwerken angezeigt.
  - **Sensoren** zeigt Informationen zum Namen und zum aktuellen Zustand der Sensoren an, darunter Informationen zur Spannung sowie zur Batteriespannungsüberprüfung.
  - **Netzwerk** zeigt den Zustand, den Namen, die Geschwindigkeit und die MAC-Adresse der Netzwerke an.

- **Virtuelle Maschinen** zeigt den Zustand, die Aktivität und den Namen der virtuellen Maschinen an.
- **USB-Geräte** zeigt die USB-Geräte an, die an den Knoten angeschlossen sind.
- **Überwachen** zeigt Informationen zum System an (zum Beispiel CPU-Nutzung und Arbeitsspeicher-Nutzung). Weitere Informationen finden Sie unter Überwachen des ztC Edge-Systems.

Verwandte Themen

Die ztC Console

Verwenden der ztC Console

Aktionen für physische Maschinen

Wenn Sie eine physische Maschine (PM) auswählen, wird je nach Zustand und Aktivität der PM eine oder mehrere der folgenden Aktionsschaltflächen eingeblendet. Inaktive Schaltflächen erscheinen abgeblendet.

> **Achtung**: Auf der Seite **Physische Maschinen** der ztC Console können Sie Wartungsaufgaben für eine PM ausführen. Vermeiden Sie die Verwendung von Schaltern und Tasten am Computer, da die ztC Console das ztC Edge-System vor den meisten Aktionen, die potenziell den Betrieb stören, schützt.

Befehle	Beschreibung
 Wartung	Versetzt eine PM in den Wartungsmodus. Falls VMs auf dieser PM ausgeführt werden, migrieren sie auf die andere PM, falls diese vorhanden und in Betrieb ist. (Andernfalls werden Sie zur erneuten Bestätigung der Anfrage und zum Herunterfahren der VMs aufgefordert.) Wenn VMs migriert oder heruntergefahren werden, zeigt die PM **wird ausgeführt (in Wartung)** an. Siehe Wartungsmodus.
Die folgenden Aktionen sind bei manchen Systemen verfügbar, nachdem Sie auf die Schaltfläche **Wartung** geklickt haben und die PM in den Wartungsmodus versetzt wurde.	
 Abschließen	Nimmt eine PM aus dem Zustand **wird ausgeführt (in Wartung)**. Siehe Wartungsmodus.

Befehle	Beschreibung
 Herunterfahren	Fährt eine PM herunter. Die PM wechselt zu **aus (in Wartung)**. Siehe Herunterfahren einer physischen Maschine.
 Neu starten	Startet die PM neu. Die PM wechselt zu **Vorbereitung auf Neustart (in Wartung)**. Siehe Neustarten einer physischen Maschine.
 Entfernen	Instruiert die Stratus Redundant Linux-Software, die PM aus der Datenbank des ztC Edge-Systems zu löschen, sodass Sie die PM oder eine ihrer Komponenten austauschen können. Siehe Ersetzen von physischen Maschinen (manuell).
Die folgende Aktion ist unter Umständen verfügbar, wenn die Stratus Redundant Linux-Software eine PM wegen einer zu hohen Ausfallrate außer Betrieb genommen und ausgeschaltet hat.	
 Wiederherstellen	Stellt eine ausgefallene PM wieder her. In einigen Fällen zeigt die ztC Console den Zustand einer ausgefallenen PM als **Nicht erreichbar (Synchronisierung/Evakuierung…)** an. Siehe Wiederherstellen einer ausgefallenen physischen Maschine (manuell).

Verwandte Themen

Die ztC Console

Verwenden der ztC Console

Die Seite „Physische Maschinen“

Zustände und Aktivitäten physischer Maschinen

Die folgenden Zustände und Aktivitäten sind bei physischen Maschinen (PMs) möglich. Für die einzelnen Zustände und Aktivitäten sind jeweils nur bestimmte Aktionen verfügbar.

Zustand	Aktivität	Verfügbare Befehle	Beschreibung
	 Wird ausgeführt	**Wartung**	PM wird normal ausgeführt.
	 Evakuierung	**Abschließen**	Virtuelle Maschinen migrieren von dieser PM zu ihrer Partner-PM.
	 Wird ausgeführt	**Wartung**	PM wird vermutlich ausfallen.
	 Wird ausgeführt	**Wartung**	PM ist ausgefallen.
	 Ausgeschaltet	**Wartung**	ztC Edge hat die PM wegen einer übermäßig hohen Ausfallrate ausgeschaltet.
	 Wird gestartet	**Abschließen**	Die PM wird gestartet.
	 Neu starten	**Abschließen**	Die PM wird neu gestartet.
	 Wird ausgeführt	**Abschließen** **Herunterfahren** **Neu starten** **Wiederherstellen** **Ersetzen**	PM läuft im Wartungsmodus. Siehe Wartungsmodus.

Verwandte Themen

Die ztC Console

Verwenden der ztC Console

Die Seite „Physische Maschinen“

Die Seite „Virtuelle Maschinen“

Auf der Seite **Virtuelle Maschinen** können Sie die virtuelle Maschinen (VMs) verwalten, die in Ihrem ztC Edge-System ausgeführt werden. Um diese Seite zu öffnen, klicken Sie im linken Navigationsbereich der ztC Console auf **Virtuelle Maschinen**.

Um eine bestimmte VM zu verwalten, klicken Sie im oberen Bereich der Seite **Virtuelle Maschinen** auf den Namen der VM. Im unteren Fensterbereich werden Steuerungen und Informationen zum Verwalten der VM angezeigt.

Informationen zum Zustand der VMs, der auf der Seite **Virtuelle Maschinen** angezeigt wird, finden Sie unter Zustände und Aktivitäten virtueller Maschinen. Informationen zu den Steuerungen auf dieser Seite finden Sie unter Aktionen für virtuelle Maschinen oder im Hilfethema zu einer bestimmten Aufgabe.

Auf der Seite **Virtuelle Maschinen** können Sie administrative Aufgaben ausführen, darunter:

- Anzeigen von Informationen zu einer VM, darunter Name, Betriebssystem, Beschreibung und Ressourcen auf den Registerkarten im unteren Fensterbereich
- Erstellen, Kopieren, Exportieren, Importieren oder Wiederherstellen von VMs; siehe Erstellen und Migrieren von virtuellen Maschinen
- Öffnen einer VM-Konsolensitzung
- Neuzuweisen von VM-Ressourcen
- Steuern des Stromversorgungszustands einer VM wie in den folgenden Themen beschrieben:
    - Starten einer virtuellen Maschine
    - Herunterfahren einer virtuellen Maschine
    - Ausschalten einer virtuellen Maschine
- Entfernen einer virtuellen Maschine oder Umbenennen einer virtuellen Maschine
- Ausführen von erweiterten Aufgaben oder Fehlerbehebung; siehe Erweiterte Themen (virtuelle Maschinen)
- Bereitstellen (und Aufheben der Bereitstellung) von USB-Geräten oder über das Netzwerk bereitgestellten Ordnern zur Verwendung durch das Gastbetriebssystem wie unter Bereitstellen eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners im ztC Edge-System beschrieben
- Anschließen (und Trennen) von USB-Geräten an eine VM wie unter Anschließen eines USB-Geräts an eine virtuelle Maschine beschrieben

- Überwachen von Windows-basierter VMs und Anwendungen wie unter Überwachen des Systems, Windows-basierter VMs und Anwendungen beschrieben

Benutzer, denen die Rolle **Administrator** oder **Plattform-Manager** zugewiesen wurde, können alle Aufgaben auf der Seite **Virtuelle Maschinen** ausführen. Benutzer, denen die Rolle **VM-Manager** zugewiesen wurde, können alle Aufgaben ausführen, allerdings können **VM-Manager** keine Volumes erweitern. Ausführliche Informationen zu den Berechtigungen von **VM-Managern** finden Sie unter Verwalten von virtuellen Maschinen. Informationen zur Zuweisung dieser Rollen finden Sie unter Verwalten lokaler Benutzerkonten.

Verwandte Themen

Verwalten von virtuellen Maschinen

Verwenden der ztC Console

Aktionen für virtuelle Maschinen

Wenn Sie eine virtuelle Maschine (VM) auswählen, können je nach Zustand und Aktivität der VM die folgenden Aktionsschaltflächen angezeigt werden, wobei die inaktiven Schaltflächen ausgeblendet erscheinen.

Aktion	Beschreibung
 Erstellen	Ruft den Assistenten zum Erstellen von VMs auf. Siehe Erstellen einer neuen virtuellen Maschine.
 Kopieren	Kopiert eine vorhandene VM auf Ihrem System, um eine neue VM zu erstellen oder ein Duplikat für die Fehlerbehebung zu erstellen. Siehe Kopieren einer virtuellen Maschine.
 Importieren/Wiederherstellen	Importiert eine VM aus einem Satz von OVF- und VHD-Dateien. Siehe Erstellen und Migrieren von virtuellen Maschinen. Mit dem Import-Assistenten können Sie eine VM *importieren*, um eine neue Instanz der VM zu erstellen, oder eine VM *wiederherstellen*, um eine identische VM mit denselben Hardware-IDs wie in den OVF- und VHD-Dateien angegeben zu erstellen. OVF (Open Virtual Machine Format) ist ein offener Standard für das

Aktion	Beschreibung
	Verpacken und Verteilen der Daten physischer oder virtueller Maschinen. Das OVF-Format enthält Metadaten zur VM. Eine VHD-Datei enthält die Informationen für den virtuellen Datenträger.
Die folgenden Aktionen sind verfügbar, wenn die VM ausgeführt wird.	
 Bereitstellen	Stellt ein USB-Gerät oder ein über das Netzwerk bereitgestelltes Verzeichnis bereit, damit es für das Gastbetriebssystem verfügbar ist. Sie können dann eine VM an den bereitgestellten Speicherort exportieren. Siehe Bereitstellen eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners im ztC Edge-System.
 Bereitstellung aufheben	Hebt die Bereitstellung eines USB-Geräts oder eine über das Netzwerk bereitgestellten Ordners auf. Siehe Bereitstellen eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners im ztC Edge-System.
 Konsole	Öffnet eine Konsole für die ausgewählte VM. Siehe Öffnen einer VM-Konsolensitzung.
 Herunterfahren	Fährt die ausgewählte VM herunter. Siehe Herunterfahren einer virtuellen Maschine.
 Ausschalten	Beendet sofort die Verarbeitung der ausgewählten VM und zerstört deren Arbeitsspeicherzustand. Verwenden Sie dies nur als letzte Möglichkeit, wenn die VM nicht ordnungsgemäß heruntergefahren werden kann. Siehe Ausschalten einer virtuellen Maschine.
Die folgenden Aktionen sind verfügbar, wenn die VM heruntergefahren oder beendet wurde.	

Aktion	Beschreibung
 Konfig	Ruft den Assistenten **Virtuelle Maschine neu zuweisen** auf. Die VM muss heruntergefahren werden, bevor dieser Assistent gestartet werden kann. Siehe Neuzuweisen von VM-Ressourcen.
 Wiederherstellen	Stellt eine vorhandene VM auf dem ztC Edge-System wieder her, indem die VM mit Daten aus einer früheren Sicherungskopie der OVF- und VHD-Dateien überschrieben wird. Siehe Ersetzen/Wiederherstellen einer virtuellen Maschine aus einer OVF-Datei.
 Exportieren	Speichert das Abbild einer VM in einem Satz von OVF- und VHD-Dateien. Sie können diese Dateien auf einem anderen System importieren oder sie in dasselbe ztC Edge-System zurück importieren, um die ursprüngliche VM wiederherzustellen oder zu duplizieren. Siehe Exportieren einer virtuellen Maschine .
 Starten	Startet die ausgewählte VM. Siehe Starten einer virtuellen Maschine.
 Von CD starten	Startet eine VM von der ausgewählten virtuellen CD. Siehe Starten von einer virtuellen CD.
 Entfernen	Entfernt eine VM. Siehe Entfernen einer virtuellen Maschine.
Die folgende Aktion ist verfügbar, wenn die Stratus Redundant Linux-Software die VM wegen einer übermäßig hohen Ausfallrate außer Dienst genommen und ausgeschaltet hat.	
 Gerät zurücksetzen	Setzt die MTBF (Mean Time Between Failures, mittlere Betriebsdauer zwischen Ausfällen) für eine VM zurück, sodass sie wieder in Betrieb genommen werden kann. Siehe Zurücksetzen der MTBF für eine

Aktion	Beschreibung
	ausgefallene virtuelle Maschine. Wenn eine VM abstürzt, startet die Stratus Redundant Linux-Software sie automatisch neu, sofern sie nicht unter den MTBF-Schwellenwert gefallen ist. Wenn die VM unter dem MTBF-Schwellenwert ist, belässt sie die Stratus Redundant Linux-Software im abgestürzten Zustand. Falls erforderlich, können Sie auf **Gerät zurücksetzen** klicken, um die VM neu zu starten und den MTBF-Zähler zurückzusetzen.

Verwandte Themen

Verwalten des Betriebs einer virtuellen Maschine

Die Seite „Virtuelle Maschinen“

Verwenden der ztC Console

Zustände und Aktivitäten virtueller Maschinen

Eine virtuelle Maschine (VM) kann die folgenden Zustände und Aktivitäten aufweisen, bei denen jeweils nur bestimmte Aktionen möglich sind.

Zustand	Aktivität	Verfügbare Aktionen	Beschreibung
	 Installation	Zustände und Aktivitäten virtueller Maschinen	Die Stratus Redundant Linux-Software installiert das Startvolume für eine neue VM.
	 Beendet	Starten Kopieren Konfig Exportieren Von CD	Die VM wurde heruntergefahren oder ausgeschaltet.

Zustand	Aktivität	Verfügbare Aktionen	Beschreibung
		starten Entfernen	
	 Wird gestartet	Konsole Ausschalten	Die VM wird gestartet.
	 Wird ausgeführt	Konsole Herunterfahren Ausschalten	Die VM wird normal auf redundanten physischen Maschinen ausgeführt.
	 Wird ausgeführt	Konsole Herunterfahren Ausschalten	Die VM wird normal ausgeführt, läuft jedoch nicht auf vollständig redundanten Ressourcen.
	 Wird beendet	Ausschalten Entfernen	Die VM wird heruntergefahren, weil die Aktion **Herunterfahren** gewählt wurde oder weil die verbleibende physische Maschine in den Wartungsmodus wechselt.
	 Abgestürzt		Die VM ist abgestürzt und wird neu gestartet. Falls die entsprechenden Optionen aktiviert wurden, werden e-Alerts und Supportbenachrichtigungen gesendet.
	 Abgestürzt		Die VM ist zu oft abgestürzt und hat ihren MTBF-Schwellenwert überschritten. Die VM verbleibt im abgestürzten Zustand, bis auf **Gerät zurücksetzen** geklickt wird. Siehe Zurücksetzen der MTBF für eine ausgefallene virtuelle Maschine.

Verwandte Themen

Verwalten des Betriebs einer virtuellen Maschine

Die Seite „Virtuelle Maschinen“

Verwenden der ztC Console

Die Seite „Volumes“

Auf der Seite **Volumes** werden Informationen zu Volumes angezeigt, die mit den virtuellen Maschinen (VMs) im ztC Edge-System verbunden sind. Um diese Seite zu öffnen, klicken Sie im linken Navigationsbereich der ztC Console auf **Volumes**. Die Seite **Volumes** enthält im oberen Fensterbereich die folgenden Spalten mit Informationen über Volumes:

- **Zustand**
- **Name**
- **Datenträgersynchronisierung** (falls vorhanden)
- **Größe**
- **Startfähig**
- **Verwendet von**, worunter eine der folgenden Angaben erscheint:
    - Ein Link zu einer VM, falls das Volume von einer VM verwendet wird.
    - Ein Link zur Seite der physischen Maschine (PM) (**Knoten0** oder **Knoten1**, falls vorhanden), wenn das Volume **root** oder **swap** ist.
    - ***System*** für ein gemeinsam genutztes Volume (**shared.fs**).
    - ***Keine***, wenn das Volume kein Systemvolume ist und nicht von einer VM verwendet wird.

Klicken Sie im oberen Fensterbereich der Seite **Volumes** auf den Namen eines Volumes, um weitere Informationen dazu im unteren Fensterbereich anzuzeigen. (Sie können Informationen zu Volumes auch mit dem Befehl `snmptable` anzeigen, siehe Beziehen der System-Informationen mit snmptable.) Sie können im unteren Fensterbereich einige administrative Aufgaben für Volumes ausführen, darunter:

- Hinzufügen einer Beschreibung für jedes Volume im Textfeld **Beschreibung**
- Umbenennen eines Volumes (siehe Umbenennen eines Volumes im ztC Edge-System)
- Entfernen eines Volumes durch Klicken auf **Entfernen**. Die Schaltfläche **Entfernen** erscheint abgeblendet, wenn ein Volume von einer VM verwendet wird.

Weitere Aufgaben der Volumeverwaltung können Sie auf der Seite „Virtuelle Maschinen“ ausführen, darunter:

- Verbinden eines Volumes mit einer virtuellen Maschine
- Erstellen eines Volumes in einer virtuellen Maschine
- Trennen eines Volumes von einer virtuellen Maschine
- Entfernen eines Volumes von einer virtuellen Maschine

Verwandte Themen

Die ztC Console

Verwenden der ztC Console

Die Seite „Netzwerke“

Auf der Seite **Netzwerke** werden Informationen zu den gemeinsamen Netzwerken angezeigt, die mit dem ztC Edge-System verbunden sind. Um diese Seite zu öffnen, klicken Sie im linken Navigationsbereich der ztC Console auf **Netzwerke**.

Auf der Seite **Netzwerke** können Sie Informationen zu einem bestimmten Netzwerk anzeigen, darunter Angaben zum Zustand, zum Verbindungszustand, zum internen Namen, zum Typ, zur Anzahl der virtuellen Maschinen (VMs), zur Geschwindigkeit und zur MTU. Auf der Registerkarte **Beschreibung** im unteren Fensterbereich können Sie eine Beschreibung für das Netzwerk hinzufügen.

Um ein bestimmtes Netzwerk zu verwalten, klicken Sie im oberen Bereich der Seite **Netzwerke** unter **Name** oder **Interner Name** auf den Namen des Netzwerks oder klicken Sie auf einen Port im Netzwerkkonnektivitätsdiagramm auf der Registerkarte **Übersicht**. Im unteren Fensterbereich werden zusätzliche Informationen zu den Knoten im Netzwerk angezeigt. Die Spalten auf der Registerkarte **Übersicht** enthalten Informationen zum Zustand des Knotens, zur physischen Schnittstelle, zur Geschwindigkeit, zur MAC-Adresse, zum Steckplatz und zum Port. Um Spalten anzuzeigen oder auszublenden, bewegen Sie den Cursor rechts neben eine Spaltenüberschrift, klicken auf den Pfeil nach unten, der dann eingeblendet wird, und klicken dann auf **Spalten**, wobei Sie auswählen können, welche Spalten Sie anzeigen oder ausblenden möchten.

Auf der Seite **Netzwerke** können Sie administrative Aufgaben ausführen, darunter:

- Anzeigen einer Liste der physischen Adapter, aus denen das Netzwerk besteht, auf der Registerkarte **Übersicht**
- Hinzufügen einer Beschreibung für ein Netzwerk auf der Registerkarte **Beschreibung**

- Anzeigen einer Liste der virtuellen Maschinen, die das Netzwerk verwenden, auf der Registerkarte **Virtuelle Maschinen**
- Ändern des Namens durch Doppelklicken auf den Namen in der Spalte **Name**
- Festlegen der MTU für A-Link- und Unternehmensnetzwerke

Weitere Informationen zu Netzwerken finden Sie hier:

- Netzwerkarchitektur
- Verbinden von Ethernet-Kabeln
- Allgemeine Netzwerkanforderungen und -konfigurationen
- Erfüllen der Netzwerkanforderungen für ALSR-Konfigurationen

Hinweis: Auf der Seite **Netzwerke** werden nur die Netzwerke angezeigt, die über eine physische Verbindung zu beiden physischen Maschinen verfügen. Falls Sie in der Liste ein Netzwerk vermissen, überprüfen Sie, ob beide Netzwerkverbindungen korrekt verkabelt sind und ihr LINK aktiv ist.

Verwandte Themen

Die ztC Console

Verwenden der ztC Console

Festlegen der MTU

Die Netzwerkleistung wird mit der höchsten maximalen Übertragungseinheit (MTU), die das Netzwerk unterstützen kann, verbessert. Sie können den MTU-Wert für A-Link und Unternehmensnetzwerke (biz) auf der Seite **Netzwerke** der ztC Console festlegen.

Hinweis: Wenn Sie die MTU-Einstellung eines Unternehmensnetzwerks (`Netzwerk0` oder `Netzwerk1`) ändern, migriert das System die VMs automatisch von einem Knoten auf den anderen. Wenn Sie die MTU für `Netzwerk0` ändern, kommt es automatisch zu einem Failover vom primären Knoten zum sekundären Knoten. Um dieses Problem zu vermeiden, ändern Sie die MTU-Einstellung der Unternehmensnetzwerke nicht oder ändern Sie die MTU nur während eines geplanten Wartungszeitraums.

So legen Sie die MTU für ein A-Link- oder Unternehmensnetzwerk fest

1. Klicken Sie im linken Navigationsbereich auf **Netzwerke**, um die Seite **Netzwerke** zu öffnen.
2. Wählen Sie im oberen Fensterbereich das A-Link- oder Unternehmensnetzwerk aus, dessen MTU-Wert Sie festlegen möchten.
3. Klicken Sie auf **Konfig**.
4. Wählen Sie im Fenster **Gemeinsames Netzwerk konfigurieren** die **Netzwerkrolle** aus (**Unternehmen** oder **A-Link**).
5. Geben Sie unter **MTU** einen Byte-Wert zwischen 1280 und 65535 ein. Die Standardwerte sind:
    - Bei 100i-Systemen ist der Standardwert für alle Ethernet-Ports 1500.
    - Bei 110i-Systemen ist der Standardwert vom Ethernet-Port abhängig:
        - Für Ports A1 (A-Link1) und A2 (priv0) ist der Wert 9000.
        - Für Ports P1 bis P6 (ibiz0 bis ibiz5) ist der Wert 1500
6. Klicken Sie auf **Speichern**.

Verwandte Themen

Die Seite „Netzwerke“

Die ztC Console

Verwenden der ztC Console

Die Seite „Virtuelle CDs“

Auf der Seite **Virtuelle CDs** können Sie virtuelle CDs (VCDs) erstellen. Mit VCDs können Sie Softwareinstallationen oder Wiederherstellungsmedien für die virtuellen Maschinen auf dem System bereitstellen. Um diese Seite zu öffnen, klicken Sie im linken Navigationsbereich der ztC Console auf **Virtuelle CDs**.

Um eine bestimmte VCD zu verwalten, klicken Sie im oberen Bereich der Seite **Virtuelle CDs** auf den Namen der VCD. Im unteren Fensterbereich wird eine Beschreibung der VCD angezeigt.

Auf der Seite **Virtuelle CDs** können Sie administrative Aufgaben ausführen, darunter:

- Erstellen einer virtuellen CD
- Entfernen einer virtuellen CD

- Umbenennen einer virtuellen CD
- Hinzufügen einer Beschreibung für jede VCD im Textfeld **Beschreibung**

Informationen zu anderen VCD-Verwaltungsaufgaben finden Sie unter Verwalten von virtuellen CDs.

Verwandte Themen

Einlegen einer virtuellen CD

Auswerfen einer virtuellen CD

Verwenden der ztC Console

Die Seite „Upgrade-Kits“

Auf der Seite **ztC Edge-Upgrade-Kits** können Sie Upgrade-Kits hochladen und verwalten, mit denen Sie das System auf eine neuere Version der Stratus Redundant Linux-Software aktualisieren können. Sie können prüfen, ob eine neue Version der Systemsoftware verfügbar ist, und diese dann herunterladen. Sie können ein Upgrade-Kit auch auf einen USB-Stick kopieren, um diesen bei der Neuinstallation der Systemsoftware zu verwenden.

Um die Seite **Upgrade-Kits** zu öffnen, klicken Sie im linken Navigationsbereich der ztC Console auf **Upgrade-Kits**.

> **Hinweis**: Sie können festlegen, dass ein verfügbares Upgrade-Kit automatisch heruntergeladen wird. Sie können auch einstellen, dass Systemadministratoren per E-Mail benachrichtigt werden (e-Alert), wenn ein Update der Systemsoftware verfügbar ist. Siehe Verwalten von Softwareupdates.

So können Sie prüfen, ob eine neue Version der Systemsoftware verfügbar ist, und diese herunterladen

> **Hinweis**: Damit Sie dieses Verfahren ausführen können, benötigen Sie die Benutzerrolle **Administrator** oder **Plattform-Manager**.

1. Klicken Sie im linken Navigationsbereich auf **Upgrade-Kits**, um die Seite **Upgrade-Kits** zu öffnen.
2. Klicken Sie unterhalb der Titelleiste auf **Auf Updates prüfen**.

Es wird eine Meldung angezeigt, ob eine neue Version der Systemsoftware verfügbar ist oder nicht.

3. Falls ein Update verfügbar ist, wird das Feld **Softwareupdate verfügbar** eingeblendet und Sie können auf **Software herunterladen** klicken, um die Software herunterzuladen. Wenn Sie mehr über das jeweilige Update erfahren möchten (auf Englisch), klicken Sie auf **Versionshinweise anzeigen**.

   > **Hinweis**: Auf der Seite **Upgrade-Kits** sind höchstens zwei gespeicherte Kits zulässig. Wenn auf der Seite bereits zwei Kits aufgeführt sind und Sie ein weiteres herunterladen wollen, müssen Sie zunächst ein Kit löschen.

   Wenn Sie auf **Software herunterladen** klicken, passiert Folgendes:

   - Wenn das ztC Edge-System mit dem Internet verbunden ist, wird eine **KIT**-Datei mit dem Softwareupdate direkt auf das System heruntergeladen und auf der Seite **Upgrade-Kits** aufgeführt. Im Feld **Softwareupdate verfügbar** werden verschiedene Statusmeldungen angezeigt, die den Fortschritt des Downloads angeben.
   - Hat das System keine Internetverbindung, wird die **KIT**-Datei auf den Remoteverwaltungscomputer heruntergeladen, auf dem die ztC Console ausgeführt wird. Speichern Sie die Datei im Download-Standardordner des Browsers oder navigieren Sie zu einem anderen Speicherort. Sofern Sie dies konfiguriert haben, erhalten Sie eine Benachrichtigung, dass eine neue Version der Systemsoftware verfügbar ist, die Sie auf das System hochladen müssen.

4. Wie Sie dann mit dem Upgrade fortfahren, lesen Sie unter Upgrade der Stratus Redundant Linux-Software mit einem Upgrade-Kit.

Informationen zum Aktualisieren der Stratus Redundant Linux-Software finden Sie unter Aktualisieren der Stratus Redundant Linux-Software.

Informationen zum Erstellen von USB-Medien finden Sie unter Erstellen eines USB-Mediums mit Systemsoftware.

Verwandte Themen

Die ztC Console

Verwenden der ztC Console

Erstellen eines USB-Mediums mit Systemsoftware

Auf der Seite **Upgrade-Kits** können Sie ein USB-Medium mit einer Kopie der Bereitstellungs-ISO-Datei der Systemsoftware, Stratus Redundant Linux, erstellen. Dieses USB-Medium verwenden Sie dann, um die Software neu zu installieren, falls Sie einen ausgefallenen Knoten manuell wiederherstellen oder ersetzen müssen.

> **Hinweis**: Wenn Sie ein Upgrade-Kit auf ein USB-Medium kopieren, werden die Dateisysteme, falls vorhanden, vom Medium entfernt.

So erstellen Sie ein USB-Medium mit Systemsoftware

1. Laden Sie ein Upgrade-Kit herunter, falls Sie dies noch nicht getan haben. Siehe Upgrade der Stratus Redundant Linux-Software mit einem Upgrade-Kit.
2. Schließen Sie ein USB-Medium an den primären Knoten an. Vergewissern Sie sich auf der Seite **Physische Maschinen**, dass das Gerät auf der Registerkarte **USB-Geräte** aufgeführt wird.
3. Klicken Sie in der ztC Console im Navigationsbereich auf der linken Seite auf **Upgrade-Kits**.
4. Wenn auf der Seite **Upgrade-Kits** mehrere Kits aufgeführt sind, wählen Sie die Version mit der ISO-Datei, die Sie kopieren möchten.
5. Klicken Sie auf die Schaltfläche **USB-Medium erstellen** (unterhalb der Titelleiste).

   Das Dialogfeld **USB-Medium erstellen** wird angezeigt.
6. Wenn mehrere USB-Medien an den Knoten angeschlossen sind, müssen Sie eines aus der Dropdownliste auswählen. Klicken Sie dann auf **Weiter** (oder auf **Abbrechen**, um den Vorgang abzubrechen).

   Das Dialogfeld **USB-Medium erstellen** zeigt den Fortschritt des Vorgangs in Prozent an. Nach Abschluss des Kopiervorgangs wird das Fenster geschlossen.

Verwenden Sie das USB-Medium, um die Software neu zu installieren, falls Sie einen ausgefallenen Knoten manuell wiederherstellen oder ersetzen müssen. Weitere Informationen finden Sie unter Wiederherstellen einer ausgefallenen physischen Maschine (manuell) und Ersetzen von physischen Maschinen (manuell).

Verwandte Themen

Die Seite „Upgrade-Kits“

4

Kapitel 4: Aktualisieren der Stratus Redundant Linux-Software

Verwenden Sie ein Upgrade-Kit, um ein Upgrade der Stratus Redundant Linux-Software auszuführen. Siehe Upgrade der Stratus Redundant Linux-Software mit einem Upgrade-Kit.

Verwandte Themen

Verwalten von Softwareupdates

Die Seite „Upgrade-Kits“

Die ztC Console

Verwenden der ztC Console

Upgrade der Stratus Redundant Linux-Software mit einem Upgrade-Kit

In diesem Thema wird beschrieben, wie Sie ein Upgrade-Kit der Stratus Redundant Linux-Software verwenden, um die Systemsoftware zu aktualisieren. Außerdem wird erläutert, wie Sie das Kit herunterladen und dann auf das System hochladen, falls dies vor dem Systemupgrade erforderlich ist. Wenn das System für zwei Knoten lizenziert ist, können Sie wahlweise ein kontrolliertes Upgrade ausführen, indem Sie Pausen aktivieren. (Bei einem System, das nur für einen Knoten lizenziert ist, können Sie keine Pausen aktivieren.) Die Systeminspektion während einer Pause ist hilfreich, um Drittanbieter-Tools oder andere Dienste zu überprüfen oder neu zu konfigurieren, die nicht vom System verwaltet werden.

Achtung: Aktualisieren Sie das CentOS-Hostbetriebssystem auf dem ztC Edge-System nicht aus irgendeiner anderen Quelle als Stratus. Verwenden Sie nur die CentOS-Version, die mit der Stratus Redundant Linux-Software installiert wurde.

Voraussetzungen:

- Alle PMs und VMs müssen sich in einem guten Zustand befinden, bevor ein Upgrade der Systemsoftware ausgeführt wird. Überprüfen Sie vor dem Start eines Upgrades die ztC Console, um sich zu vergewissern, dass keine Alarme vorliegen, die Probleme mit PMs oder VMs anzeigen.
- Entfernen Sie alle VCDs oder USB-Sticks von den VMs, bevor Sie ein Upgrade der Systemsoftware ausführen. Wenn noch eine VCD oder ein USB-Stick mit den VMs verbunden ist, kann das System die VMs nicht migrieren und die PMs nicht in den Wartungsmodus versetzen, was für den Upgradeprozess erforderlich ist.
- Um zu überprüfen, ob Ihr System die Anforderungen des Upgrade-Kits erfüllt, verwenden Sie die Schaltfläche **Qualifizieren** wie in diesem Thema beschrieben.
- Sichern Sie die VMs, bevor Sie ein Upgrade für ein System ausführen, das für einen Knoten lizenziert ist. Aktualisieren und qualifizieren Sie die Software dann, indem Sie wie nachstehend beschrieben vorgehen. Führen Sie zum Schluss ein Upgrade der PM des Systems aus wie unter So aktualisieren Sie ein System, das für einen Knoten lizenziert ist beschrieben. Während des Upgradevorgangs startet das System neu, deshalb kann mindestens 15 Minuten lang nicht auf die ztC Console zugegriffen werden.

Die Schritte im Einzelnen:

I. So laden Sie das Upgrade-Kit herunter

II. So laden Sie das Upgrade-Kit in das System hoch

III. So qualifizieren Sie die Software (optional)

IV. So führen Sie ein Upgrade der Systemsoftware durch

I. So laden Sie das Upgrade-Kit herunter

Wenn ein Update verfügbar ist, können Sie das Upgrade-Kit herunterladen, das die Systemsoftware enthält, falls es nicht automatisch heruntergeladen wurden. Klicken Sie auf der Seite **Upgrade-Kits** auf **Software herunterladen** im Fenster **Softwareupdate verfügbar** (siehe Die Seite „Upgrade-Kits“).

Alternativ dazu können Sie die Software auch von der Stratus **Downloads**-Seite herunterladen.

Hinweis: Auf der Seite **Upgrade-Kits** der ztC Console sind höchstens zwei gespeicherte Kits zulässig. Wenn auf der Seite bereits zwei Kits aufgeführt sind und Sie ein weiteres herunterladen wollen, müssen Sie zunächst ein Kit löschen.

1. Öffnen Sie die Seite **Downloads** unter https://www.stratus.com/services-support/downloads/?tab=ztcedge.
2. Scrollen Sie im Upgradebereich nach unten und klicken Sie dann auf den Upgrade-Link, um das Kit herunterzuladen.
3. Navigieren Sie zu einem Speicherort auf einem lokalen Computer, um die Datei zu speichern. Falls erforderlich, übertragen Sie die Datei auf den Remoteverwaltungscomputer, auf dem die ztC Console ausgeführt wird.

II. So laden Sie das Upgrade-Kit in das System hoch

Falls erforderlich, laden Sie das Upgrade-Kit vom Remoteverwaltungscomputer, auf dem die ztC Console ausgeführt wird, in das ztC Edge-System hoch.

1. Klicken Sie in der ztC Console im Navigationsbereich auf der linken Seite auf **Upgrade-Kits**.
2. Klicken Sie auf der Seite **Upgrade-Kits** oben unter der Titelleiste auf die Schaltfläche **Kit hinzufügen**. Damit wird der **ztC Edge - Assistent zum Hochladen eines Kits aufgerufen**.
3. Klicken Sie im Dialogfeld **ztC Edge - Assistent zum Hochladen eines Kits** auf **Datei auswählen** (in Google Chrome) oder **Durchsuchen** (in Firefox oder Internet Explorer) und wählen Sie eine Datei mit der Erweiterung „.kit“ aus.
4. Nachdem Sie eine Kit-Datei ausgewählt haben, klicken Sie auf **Hochladen**, **Importieren** oder **Fertigstellen** (alle führen dieselbe Funktion aus). Es wird eine Meldung wie **Datei wird hochgeladen (ASSISTENT NICHT SCHLIESSEN)** angezeigt, während die Datei hochgeladen wird. Das Hochladen kann bei einer lokal gespeicherten Datei bis zu zwei Minuten, bei einer im Netzwerk gespeicherten Datei zehn Minuten oder länger dauern. Wenn der Upload fehlschlägt, zeigt der Assistent die Meldung **Datei konnte nicht hochgeladen werden** an.
5. Nach Abschluss des Uploads wird der Assistent geschlossen und auf der Seite **Upgrade-Kits** werden jetzt der Zustand und die Versionsnummer des Upgrade-Kits angezeigt. Außerdem sind jetzt die Schaltflächen **Qualifizieren**, **Upgrade** und **Löschen** neben der Schaltfläche **Kit hinzufügen**

verfügbar.

6. Falls mehrere Upgrade-Kits geladen wurden, wählen Sie das gewünschte aus.

III. So qualifizieren Sie die Software

Qualifizieren Sie die Software, um zu überprüfen, ob Ihr System die Anforderungen des Upgrade-Kits erfüllt. (Die Qualifizierung der Software wird empfohlen, ist aber nicht zwingend erforderlich.)

Wählen Sie dazu das Upgrade-Kit, das Sie qualifzieren wollen, auf der Seite **Upgrade-Kits** aus und klicken Sie auf **Qualifizieren**.

Die Qualifizierung kann bis zu sechs Minuten dauern. Bei erfolgreicher Qualifikation fahren Sie mit dem nächsten Schritt fort.

Falls die Qualifizierung fehlschlägt, wird eine entsprechende Meldung mit der Ursache des Fehlers angezeigt. Die Meldung kann zum Beispiel angeben, dass eine Version nicht unterstützt wird, dass nicht genügend Speicherplatz verfügbar ist, dass es Partitionsprobleme gibt oder dass VMs heruntergefahren werden müssen; oder es werden andere Informationen angezeigt, die mit dem Upgrade des Systems zu tun haben. Wenn zum Beispiel nicht genügend Speicherplatz auf dem Datenträger vorhanden ist, um das Upgrade abzuschließen, erscheint die Meldung `Nicht genügend Speicherplatz` und informiert Sie darüber, wie viel Speicherplatz benötigt wird. Wenn Sie Hilfe bei einem Problem mit der Qualifikation brauchen, suchen Sie die Qualifikationsfehlermeldung in der **Knowledge Base** im **Stratus Customer Service Portal** unter https://support.stratus.com.

IV. So führen Sie ein Upgrade der Systemsoftware durch

1. Starten Sie das Upgrade, indem Sie auf der Seite **Upgrade-Kits** auf die Schaltfläche **Upgrade** klicken.

   Es wird ein Fenster **Bestätigen** angezeigt, in dem Sie auf das Upgrade des Systems hingewiesen werden und aufgefordert werden, das ausgewählte Upgrade-Kit zu bestätigen. Das Fenster enthält auch ein Kontrollkästchen zum Aktivieren von Pausen, damit Sie das Upgrade kontrollieren können. Aktivieren Sie Pausen, indem Sie auf das Kontrollkästchen **Anhalten nach Upgrade eines einzelnen Knotens** klicken.

2. Klicken Sie auf **Ja**, um mit dem Upgrade fortzufahren.

   Das Upgrade beginnt. Wenn Sie Pausen aktiviert haben, zeigt das Diagramm mit den Upgradeschritten den aktuellen Zustand des Upgrades an. Wenn das Upgrade anhält, müssen Sie zum Fortfahren auf **Abschließen** klicken.

Nach dem Upgrade des ersten Knotens, aber vor dem Upgrade des anderen Knotens (sofern vorhanden) werden die beiden Knoten mit unterschiedlichen Versionen der Software ausgeführt. Während dieser Zeit zeigt die Titelleiste die Meldung **System wird mit unterschiedlichen Versionen ausgeführt** an.

Nachdem das Upgrade abgeschlossen ist, prüfen Sie alle Windows-basierten VMs auf aktualisierte VirtIO-Treiber wie unter Aktualisieren der VirtIO-Treiber (Windows-basierte VMs) beschrieben.

So aktualisieren Sie ein System, das für einen Knoten lizenziert ist

1. Fahren Sie alle VMs herunter, die auf dem ztC Edge-System ausgeführt werden.
2. Befolgen Sie die Anleitungen in den oben aufgeführten Schritten, um das System mithilfe eines Upgrade-Kits zu aktualisieren.

   Hinweis: Während des Upgradevorgangs startet das System neu, deshalb kann mindestens 15 Minuten lang nicht auf die ztC Console zugegriffen werden.
3. Vergewissern Sie sich, dass das System korrekt ausgeführt wird.
4. Starten Sie alle VMs.

Verwandte Themen

Verwalten von Softwareupdates

Die Seite „Upgrade-Kits“

Die ztC Console

Verwenden der ztC Console

Beschreibung des ztC Edge-Systems

5

Kapitel 5: Verwalten von physischen Maschinen

Verwalten Sie eine physische Maschine (PM), auch Knoten genannt, um ihren Betrieb zu steuern und Wartungsaufgaben auszuführen.

Sie können PMs auf der Seite **Physische Maschinen** der ztC Console anzeigen und verwalten. Nähere Informationen hierzu finden Sie unter Die Seite „Physische Maschinen“.

Viele Aufgaben auf der Seite **Physische Maschinen** können nur im Wartungsmodus ausgeführt werden; Informationen hierzu finden Sie unter Wartungsmodus.

Um den Betriebszustand einer PM (in Wartung) zu verwalten, siehe:

- Neustarten einer physischen Maschine
- Herunterfahren einer physischen Maschine
- Lastverteilung

Informationen zum Einschalten einer physischen Maschine (an der physischen Konsole der PM) finden Sie unter Einschalten einer physischen Maschine.

Zur Fehlerbehebung bei einer PM durch das Wiederherstellen einer ausgefallenen PM oder das Zurücksetzen der MTBF für eine ausgefallene Maschine lesen Sie Fehlerbehebung bei physischen Maschinen.

Informationen zur Durchführung von Wartungsaufgaben für die PM-Hardware, zum Beispiel zum Ersetzen einer PM, finden Sie unter Warten von physischen Maschinen.

Informationen zur Überwachung des Hostbetriebssystems des ztC Edge-Systems in Systemen, die für diese Art der Überwachung lizenziert sind, finden Sie unter Überwachen des ztC Edge-Systems.

Wartungsmodus

Wenn eine physische Maschine (PM) in den Wartungsmodus versetzt wird, ist sie außer Betrieb, damit Wartungsaufgaben vorgenommen werden können. Beim Abschließen der Arbeiten wechselt die PM aus dem Wartungsmodus zurück und geht wieder in Betrieb, damit virtuelle Maschinen (VM) ausgeführt werden können.

Wenn eine PM in einem System, das für zwei PMs lizenziert ist, in den Wartungsmodus wechselt, migriert sie die auf ihr ausgeführten VMs auf die andere PM, sodass die VMs vor möglichen Unterbrechungen aufgrund der Wartungsarbeiten geschützt sind. Wenn beide PMs in einem System, das für zwei PMs lizenziert ist, in den Wartungsmodus versetzt werden, fahren sie die VMs ordnungsgemäß herunter, sodass ihr Arbeitsspeicherzustand geschützt wird, bevor die PMs heruntergefahren oder neu gestartet werden.

Wenn die primäre PM (**Knoten*x* (primär)**) in den Wartungsmodus wechselt, wird die andere PM (falls vorhanden) zur primären PM.

Wenn eine PM in einem System, das für einen Knoten (eine PM) lizenziert ist, in den Wartungsmodus wechselt, fährt die PM die VMs herunter.

Fahren Sie die PMs nur von der Seite **Physische Maschinen** aus herunter, während sie sich im Wartungsmodus befinden, da die ztC Console das System vor Unterbrechungen schützt, die aus dem manuellen Ausschalten einer PM resultieren.

Achtung:

1. Das System ist nicht fehlertolerant, wenn sich eine PM im Wartungsmodus befindet. Um die kontinuierliche Betriebszeit zu gewährleisten, schließen Sie die Wartungsarbeiten so schnell wie möglich ab, damit die PM den Wartungsmodus verlassen und wieder in Betrieb gehen kann.
2. Versetzen Sie nur dann alle PMs in den Wartungsmodus, wenn Sie alle Geschäftsprozesse herunterfahren können. Wenn Sie VMs in einen System, das für zwei PMs lizenziert ist, laufen lassen müssen, vermeiden Sie es, beide PMs gleichzeitig in den Wartungsmodus zu versetzen. Damit die VMs weiterhin ausgeführt werden, muss mindestens eine PM in Betrieb sein und ordnungsgemäß laufen. (Falls Sie das gesamte ztC Edge-System herunterfahren müssen, lesen Sie Herunterfahren einer physischen Maschine.)

Hinweis: Wenn Sie in einem System, das für zwei PMs lizenziert ist, beide PMs in den Wartungsmodus versetzen möchten, versetzen Sie zuerst die sekundäre, dann die primäre PM in den Wartungsmodus. Diese Reihenfolge verhindert die unnötige Migration von VMs.

So versetzen Sie eine PM in den Wartungsmodus

1. Wählen Sie die PM auf der Seite **Physische Maschinen** aus.
2. Klicken Sie auf **Wartung**.

   Wenn die PM im Wartungsmodus ist, wird ihr Zustand als  angezeigt.

So schließen Sie den Wartungsmodus ab und nehmen eine PM wieder in Betrieb

1. Wählen Sie die PM auf der Seite **Physische Maschinen** aus.
2. Klicken Sie auf **Abschließen**, um den Wartungsmodus zu beenden.

Verwandte Themen

Die ztC Console

Verwalten von physischen Maschinen

Physische Maschinen und virtuelle Maschinen

Die Seite „Physische Maschinen“

Die Seite „Virtuelle Maschinen“

Einschalten einer physischen Maschine

Sie schalten eine physische Maschine (PM) über die physische Konsole der PM ein.

Hinweis: Falls eine PM von der Stromversorgung getrennt wird, weil Sie den Netzwerkstecker ziehen oder es einen Stromausfall gibt, ist jede PM in einem ztC Edge-System so eingestellt, dass sie beim Wiederherstellen der Stromversorgung automatisch eingeschaltet wird.

So schalten Sie eine PM ein

1. Drücken Sie die Einschalttaste vorne an der PM.
2. Vergewissern Sie sich, dass die **PWR**-LED auf der Vorderseite leuchtet.

Wenn Sie das System einschalten möchten, drücken Sie die Ein/Aus-Taste auf der Vorderseite jeder PM im System wie in Einschalten des Systems beschrieben.

Verwandte Themen

Wartungsmodus

Die ztC Console

Verwalten von physischen Maschinen

Die Seite „Physische Maschinen“

Neustarten einer physischen Maschine

Starten Sie eine physische Maschine (PM) neu, um ihre Stratus Redundant Linux-Software neu zu starten, und nehmen Sie sie optional aus dem Wartungsmodus. (Falls Sie beide PMs in einem System, das für zwei Knoten lizenziert ist, neu starten müssen, lesen Sie Neustarten des Systems.)

So starten Sie eine PM neu

1. Stellen Sie fest, welche PM (Knoten0 oder Knoten1, falls vorhanden) Sie neu starten müssen.
2. Klicken Sie in der ztC Console im Navigationsbereich auf der linken Seite auf **Physische Maschinen**.
3. Wählen Sie die entsprechende PM (Knoten0 oder Knoten1, falls vorhanden) und klicken Sie dann auf **Wartung**. Dadurch wird der **Gesamtzustand** der PM in **Wartungsmodus** geändert und der **Aktivität**szustand ändert sich in **wird ausgeführt (in Wartung)**.
4. Klicken Sie auf **Neu starten**. Beim Neustarten der PM wird der **Aktivität**szustand angezeigt:
   - **Vorbereitung auf Neustart (in Wartung)**
   - **Neustart (in Wartung)**
   - **Wird gestartet (in Wartung)**
   - **Wird ausgeführt (in Wartung)**
5. Um die PM aus dem Wartungsmodus zu nehmen und für die Ausführung virtueller Maschinen verfügbar zu machen, klicken Sie auf **Abschließen**.

Verwandte Themen

Wartungsmodus

Die ztC Console

Verwalten von physischen Maschinen

Die Seite „Physische Maschinen“

Herunterfahren einer physischen Maschine

Wenn Sie eine physische Maschine (PM), auch als Knoten bezeichnet, warten oder ersetzen müssen, nehmen Sie sie außer Betrieb, indem Sie sie herunterfahren. Gehen Sie wie nachstehend beschrieben vor, um eine (und nur eine) PM herunterzufahren, indem Sie die ztC Console oder die Ein/Aus-Taste der PM verwenden.

Achtung:

1. Wenn Sie wie nachstehend beschrieben vorgehen, um beide PMs in einem System mit zwei Knoten herunterzufahren, gehen Daten verloren. Wenn Sie beide PMs stoppen müssen, fahren Sie das ztC Edge-System herunter (wobei auch die virtuellen Maschinen (VMs) heruntergefahren werden) wie unter Herunterfahren des Systems beschrieben.
2. Verwenden Sie nicht die Option `-f` (force) mit dem Befehl `halt`, `poweroff` oder `reboot` des Hostbetriebssystems einer PM. Dies würde dazu führen, dass - Gastsysteme, die auf demselben Knoten aktiv sind, hängenbleiben.
3. Das ztC Edge-System ist nicht fehlertolerant, wenn Sie eine PM herunterfahren. Um den Betrieb kontinuierlich fortzusetzen, müssen Sie eine heruntergefahrene PM so schnell wie möglich wieder in Betrieb nehmen.

Hinweis: Wenn Sie eine PM herunterfahren, bleibt die Standby-Stromversorgung für das Lights Out Management (LOM) an, sofern Sie nicht das Stromkabel trennen oder die Stromversorgung ausfällt.

So fahren Sie eine PM herunter (in der ztC Console)

Um eine PM herunterzufahren, müssen Sie sie in den Wartungsmodus versetzen. Dabei werden VMs, die auf dieser PM ausgeführt werden, auf die andere PM migriert (falls vorhanden). Bei einem System mit zwei Knoten bleiben die VMs während dieses Vorgangs, der ein oder zwei Minuten dauert, in Betrieb.

1. Bestimmen Sie, welche PM Sie herunterfahren möchten.
2. Klicken Sie in der ztC Console im Navigationsbereich auf der linken Seite auf **Physische Maschinen**.
3. Wählen Sie die entsprechende PM (Knoten0 oder Knoten1, falls vorhanden) und klicken Sie dann auf **Wartung**. Dadurch wird der **Gesamtzustand** der PM in **Wartungsmodus** geändert und der **Aktivitätszustand** ändert sich in **wird ausgeführt (in Wartung)**.
4. Wenn für die PM der Zustand **wird ausgeführt (in Wartung)** angezeigt wird, klicken Sie auf **Herunterfahren**.

Nachdem die PM heruntergefahren wurde, ist ihre Aktivität ✖ **aus (in Wartung)**. Sie müssen die PM manuell neu starten.

So fahren Sie eine PM mithilfe der Ein/Aus-Taste herunter

Sie können zum Herunterfahren einer PM auch die Ein/Aus-Taste der PM verwenden. Bei einem System, das für zwei Knoten lizenziert ist, bleiben die VMs während dieses Vorgangs, der ein oder zwei Minuten dauert, in Betrieb.

1. Während beide PMs in Betrieb sind, drücken Sie die Ein/Aus-Taste auf der Vorderseite der PM, die Sie herunterfahren möchten, und lassen Sie sie wieder los.
2. Das System versetzt die PM automatisch in den Wartungsmodus. Dabei werden VMs, die auf dieser PM ausgeführt werden, auf die andere PM migriert.
3. Die PM fährt automatisch herunter.

Wenn die PM heruntergefahren wurde, ist die **PWR**-LED auf der Vorderseite aus, obwohl die Standbystromversorgung weiterhin aktiviert ist. Sie müssen die PM manuell neu starten.

So schalten Sie eine PM mithilfe der Ein/Aus-Taste aus

> **Achtung**: Falls die PM nach dem Klicken auf **Herunterfahren** oder nach dem Betätigen der Ein/Aus-Taste nicht ausgeschaltet wird, müssen Sie sie manuell ausschalten. Bei diesem erzwungenen Ausschalten einer PM geht der Arbeitsspeicherzustand verloren. Schalten Sie eine PM deshalb nur als letzte Notlösung manuell aus.

Drücken Sie mehrere Sekunden lang auf die Ein/Aus-Taste der PM, um sie auszuschalten.

Wenn die PM ausgeschaltet wurde, ist die **PWR**-LED auf der Vorderseite aus, obwohl die Standbystromversorgung weiterhin aktiviert ist. Sie müssen die PM manuell neu starten.

Verwandte Themen

Wartungsmodus

Die ztC Console

Verwalten von physischen Maschinen

Die Seite „Physische Maschinen“

Lastverteilung

In Systemen, die für zwei Knoten lizenziert sind, werden bei der HV-Lastverteilung VMs auf beide PMs verteilt, um Leistung und Verfügbarkeit zu verbessern. Die Lastverteilung wird pro VM konfiguriert und ist in ztC Edge-Systemen automatisch aktiviert. (Systeme, die für einen Knoten lizenziert sind, bieten keine Lastverteilung.)

Falls eine PM außer Betrieb ist, werden alle VMs auf der weiter bestehenden PM ausgeführt. Die VMs migrieren automatisch zurück, sobald die PM, auf der sie ausgeführt werden sollen, wieder in Betrieb genommen und vollständig synchronisiert wurde.

Betriebsmodi

Die Lastverteilung für eine VM wird auf ihrer Registerkarte **Lastverteilung** auf der Seite **Virtuelle Maschinen** festgelegt. Die folgenden Modi werden unterstützt:

- **automatisch ausgleichen**. Damit erfolgt die Lastverteilung einer VM automatisch. Wenn für eine VM die automatische Lastverteilung aktiviert ist, wird sie auf der PM mit den meisten Ressourcen ausgeführt. Wenn das System feststellt, dass eine bessere Lastverteilung erzielt werden kann, wenn eine oder mehrere VMs mit der automatischen Einstellung verschoben werden, wird ein Alarm generiert. Der Alarm erscheint auf dem Dashboard, eine entsprechende Benachrichtigung wird in der Titelleiste eingeblendet. Als Reaktion auf den Alarm klicken Sie in der Titelleiste auf **Lastverteilung**, um eine automatische Lastverteilung einer VM zu initiieren.
  Das Symbol auf der Seite **Virtuelle Maschinen** in der Spalte **Aktuelle PM** zeigt VMs an, deren Migration unmittelbar bevorsteht.
- **manuell auf Knoten*N*** platzieren. Fortgeschrittene Benutzer können jeder einzelnen VM eine bevorzugte PM (Knoten) zuweisen, anstatt sich auf die automatische Richtlinie zu verlassen.

Auf der Seite **Virtuelle Maschinen** wird in der Spalte **Aktuelle PM** für jede VM eine Grafik angezeigt. Sie zeigt den aktuellen Status der Lastverteilung der VM, die PM, auf der die VM ausgeführt wird, und die bevorzugte Einstellung an.

Die folgende Beispielgrafik zeigt an, dass die VM zurzeit auf PM 0 ausgeführt wird und PM 1 die bevorzugte PM ist.

ztC Edge-Richtlinien stellen sicher, dass eine VM immer ausgeführt wird. Für den Fall, dass eine PM wahrscheinlich ausfallen wird, gewartet wird oder außer Betrieb genommen wird, wird die VM auf der anderen, stabilen PM ausgeführt. Wenn beide PMs stabil sind, migriert die VM zu ihrer bevorzugten PM.

Verwandtes Thema

Auswählen einer bevorzugten PM für eine virtuelle Maschine

Fehlerbehebung bei physischen Maschinen

Im folgenden Thema werden Verfahren zur Fehlerbehebung bei PMs beschrieben:

- Wiederherstellen einer ausgefallenen physischen Maschine (manuell)

Wenn Sie eine PM mit den beschriebenen Software-basierten Verfahren zur Fehlerbehebung nicht wiederherstellen können, lesen Sie Warten von physischen Maschinen mit Informationen zum Ersetzen der physischen PM-Hardware.

Wiederherstellen einer ausgefallenen physischen Maschine (manuell)

Achtung: Wenn Sie eine PM in einem ztC Edge-System wiederherstellen oder ersetzen müssen, folgen Sie den Anleitungen in *ztC Edge 100i/110i-Systeme: Einen Knoten austauschen* (R013Z). (Lesen Sie bei Bedarf Ersetzen von physischen Maschinen (automatisiert) mit zusätzlichen Informationen.) Vermeiden Sie die Verwendung des in diesem Thema beschriebenen Verfahrens, sofern Sie nicht speziell durch Ihren autorisierten Stratus-Servicemitarbeiter dazu aufgefordert werden.

Stellen Sie eine physische Maschine (PM), auch als Knoten bezeichnet, wieder her, wenn sie nicht gestartet werden kann oder keine PM im ztC Edge-System wird. In einigen Fällen zeigt die ztC Console den Zustand einer ausgefallenen PM als **Nicht erreichbar (Synchronisierung/Evakuierung)** an.

Um eine PM wiederherzustellen, müssen Sie die Stratus Redundant Linux-Version, die auf der PM ausgeführt wurde, erneut installieren. Das Wiederherstellen einer ausgefallenen PM unterscheidet sich jedoch vom

erstmaligen Installieren der Software. Bei der Wiederherstellung bleiben alle Daten erhalten, aber die /boot- und root-Dateisysteme werden neu erstellt, die Stratus Redundant Linux-Software wird neu installiert und es wird versucht, eine Verbindung zum vorhandenen System herzustellen. (Wenn Sie die physische PM-Hardware ersetzen müssen, statt die Systemsoftware wiederherzustellen, lesen Sie Ersetzen von physischen Maschinen (manuell).)

Um die Systemsoftware neu zu installieren, können Sie dem System erlauben, den Ersatzknoten von einem temporären PXE-Server (Preboot Execution Environment) auf der primären PM automatisch zu starten. Solange jede PM eine vollständige Kopie des zuletzt installierten Software-Kits enthält (wie auf der Seite **Upgrade-Kits** der ztC Console angezeigt), kann jede der beiden PMs die Wiederherstellung der jeweils anderen PM mittels PXE-Boot-Installation wiederherstellen. Bei Bedarf starten Sie den Ersatzknoten manuell von einem USB-Installationsmedium.

Verwenden Sie eines der nachstehend beschriebenen Verfahren, je nachdem, welches Medium Sie für die Installation verwenden möchten, **PXE** oder **USB**-Installation.

Achtung: Bei der Wiederherstellung wird sämtliche im Gastbetriebssystem installierte Software auf der PM gelöscht, und alle PM-Konfigurationsinformationen, die Sie vor der Wiederherstellung eingegeben haben, gehen verloren. Nach Abschluss dieses Verfahrens müssen Sie Ihre gesamte Software auf Hostebene manuell neu installieren und die PM-Konfiguration entsprechend Ihren ursprünglichen Einstellungen ändern.

Voraussetzungen:

1. Bestimmen Sie, welche PM wiederhergestellt werden muss.
2. Falls Sie die Systemsoftware mithilfe eines USB-Sticks auf der Ersatz-PM installieren möchten, erstellen Sie einen startfähigen USB-Stick wie unter Erstellen eines USB-Mediums mit Systemsoftware beschrieben.

   Wenn Sie den USB-Stick erstellen, vergewissern Sie sich, dass er das zuletzt installierte Upgrade-Kit enthält. Beispiel: Wenn in der Titelleiste des ztC Console-Fensters die Version `1.2.0-550` angezeigt wird, wobei 550 die Buildnummer ist, dann muss das Kit, das Sie auf der Seite **Upgrade-Kits** zum Erstellen des USB-Sticks auswählen, ebenfalls die Version `1.2.0-550` haben. Wenn das System einen anderen Build auf der Ziel-PM erkennt, wird der Wiederherstellungsprozess automatisch übergangen. Das System **initialisiert alle Daten** auf der Ziel-PM und verwendet die PXE-Boot-Installation, um das zuletzt installierte Software-Kit ohne weiteres Eingreifen des Benutzers auf der PM zu installieren.
3. Wenn Sie einen USB-Stick verwenden, schließen Sie eine Tastatur und einen Monitor an die Ersatz-PM an, um den Installationsprozess zu überwachen und Einstellungen festzulegen.

So können Sie eine PM wiederherstellen (mit PXE-Boot-Installation)

Gehen Sie wie nachstehend beschrieben vor, um eine PM mithilfe der PXE-Boot-Installation wiederherzustellen, indem die Systemsoftware vom Software-Kit auf der primären PM neu installiert wird.

1. Klicken Sie in der ztC Console im Navigationsbereich auf der linken Seite auf **Physische Maschinen**.
2. Wählen Sie die entsprechende PM (Knoten0 oder Knoten1) und klicken Sie dann auf **Wartung**. Dadurch wird der **Gesamtzustand** der PM in **Wartungsmodus** geändert und der **Aktivität**szustand ändert sich in **wird ausgeführt (in Wartung)**.
3. Wenn für die PM der Zustand **wird ausgeführt (in Wartung)** angezeigt wird, klicken Sie auf **Wiederherstellen**.
4. Wenn Sie aufgefordert werden, die Art der Reparatur auszuwählen, klicken Sie auf **PXE-PM-Wiederherstellung - Daten behalten**.

> **Achtung**: Es ist wichtig, **PXE-PM-Wiederherstellung - Daten behalten** auszuwählen, andernfalls können bei der Installation Daten auf der Ziel-PM gelöscht werden.

5. Klicken Sie auf **Weiter**, um mit der Wiederherstellung zu beginnen. Das System führt für die Ziel-PM in Vorbereitung der Neuinstallation der Systemsoftware einen Neustart aus.
6. Der Wiederherstellungsprozess läuft ohne Eingreifen des Benutzers wie folgt ab:
   - Die Ziel-PM beginnt, von einem PXE-Server zu starten, der vorübergehend auf dem primären Knoten ausgeführt wird.
   - Die Ziel-PM beginnt automatisch mit der Installation der Systemsoftware, wofür eine Kopie des Installations-Kits auf dem primären Knoten verwendet wird.
   - Bei der Installation wird die Systemsoftware neu installiert, alle Daten bleiben jedoch erhalten.

   Sie brauchen den Fortschritt der Softwareinstallation nicht an der physischen Konsole der Ziel-PM verfolgen oder auf Eingabeaufforderungen zu reagieren. Der Wiederherstellungsprozess ist automatisiert und es ist ganz normal, dass die PM für einen längeren Zeitraum während der Softwareinstallation nichts auf dem Bildschirm anzeigt.
7. Wenn die Softwareinstallation abgeschlossen ist, wird die Ziel-PM mit der neu installierten Systemsoftware neu gestartet.
8. Während die Ziel-PM neu startet, können Sie die Aktivität auf der Seite **Physische Maschinen** der ztC Console verfolgen. In der Spalte **Aktivität** wird der Zustand der PM als **(in Wartung)** angezeigt, wenn die Wiederherstellung abgeschlossen ist.
9. Installieren Sie ggf. Anwendungen und andere Software auf Hostebene manuell und ändern Sie die PM-Konfiguration auf die ursprünglichen Einstellungen.
10. Wenn Sie bereit sind, die Ziel-PM in Betrieb zu nehmen, klicken Sie auf **Abschließen**, um den Wartungsmodus zu beenden. Vergewissern Sie sich, dass beide PMs in den Zustand **wird ausgeführt** zurückkehren und dass die PMs die Synchronisierung abschließen.

> **Hinweis**: Wenn die Ziel-PM den Wartungsmodus verlässt, deaktiviert das System automatisch den PXE-Server auf dem primären Knoten, der für die Wiederherstellung verwendet wurde.

So können Sie eine PM wiederherstellen (mit USB-Installation)

Gehen Sie wie nachstehend beschrieben vor, um eine PM wiederherzustellen, indem Sie die Systemsoftware von einem USB-Medium neu installieren.

1. Klicken Sie in der ztC Console im Navigationsbereich auf der linken Seite auf **Physische Maschinen**.
2. Wählen Sie die entsprechende PM (Knoten0 oder Knoten1) und klicken Sie dann auf **Wartung**. Dadurch wird der **Gesamtzustand** der PM in **Wartungsmodus** geändert und der **Aktivität**szustand ändert sich in **wird ausgeführt (in Wartung)**.
3. Wenn für die PM der Zustand **wird ausgeführt (in Wartung)** angezeigt wird, klicken Sie auf **Wiederherstellen**.
4. Wenn Sie aufgefordert werden, die Art der Reparatur auszuwählen, klicken Sie auf **USB-PM-Wiederherstellung – Daten behalten**.

   > **Achtung**: Es ist wichtig, **USB-PM-Wiederherstellung – Daten behalten** auszuwählen, andernfalls können bei der Installation Daten auf der Ziel-PM gelöscht werden.

5. Klicken Sie auf **Weiter**, um mit der Wiederherstellung zu beginnen. Das System fährt die Ziel-PM in Vorbereitung der Neuinstallation der Systemsoftware herunter.
6. Schließen Sie das startfähige USB-Medium an die Ziel-PM an und schalten Sie die PM dann manuell ein.
7. Wenn die Ziel-PM hochgefahren wird, rufen Sie das Setup-Utility für die Firmware (UEFI) auf. Wählen Sie im Menü **Save & Exit** unter **Boot Override** den Eintrag **UEFI** für das USB-Medium aus, damit das Gerät bei der nächsten Startsequenz vom USB-Stick gestartet wird. Die PM wird neu gestartet.

   > **Hinweis**: Verwenden Sie die Eigenschaft **Boot Override**, um das Startgerät nur vorübergehend zu ändern, statt dauerhaft mit **BOOT ORDER Priorities** im **Boot**-Menü. Die oberste Priorität muss **UEFI Network** (Standardeinstellung) bleiben, damit der automatisierte Knotenaustausch unterstützt wird, der typischerweise auf ztC Edge-Systemen ausgeführt wird.

8. Überwachen Sie den Fortschritt der Softwareinstallation an der physischen Konsole der Ziel-PM.
9. Wenn der Begrüßungsbildschirm **Welcome** angezeigt wird, wählen Sie mit den Pfeiltasten ein Tastaturlayout für die Installation aus.
10. Wählen Sie im Bildschirm **Install or Recovery** (Installation oder Wiederherstellung) die Option **PM wiederherstellen, System verbinden: Daten werden erhalten** und drücken Sie die **Eingabetaste**. Der Wiederherstellungsprozess läuft ohne Eingreifen des Benutzers wie folgt ab:

    Achtung: Es ist wichtig, **PM wiederherstellen, System verbinden: Daten werden erhalten** auszuwählen, andernfalls können bei der Installation Daten auf der Ziel-PM gelöscht werden.

11. Wenn die Softwareinstallation abgeschlossen ist, wird die Ziel-PM mit der neu installierten Systemsoftware neu gestartet.
12. Während die Ziel-PM neu startet, können Sie die Aktivität auf der Seite **Physische Maschinen** der ztC Console verfolgen. In der Spalte **Aktivität** wird der Zustand der PM als **(in Wartung)** angezeigt, wenn die Wiederherstellung abgeschlossen ist.
13. Installieren Sie ggf. Anwendungen und andere Software auf Hostebene manuell und ändern Sie die PM-Konfiguration auf die ursprünglichen Einstellungen.
14. Wenn Sie bereit sind, die Ziel-PM in Betrieb zu nehmen, klicken Sie auf **Abschließen**, um den Wartungsmodus zu beenden. Vergewissern Sie sich, dass beide PMs in den Zustand **wird ausgeführt** zurückkehren und dass die PMs die Synchronisierung abschließen.

Verwandte Themen

Wartungsmodus

Verwalten von physischen Maschinen

Die ztC Console

Die Seite „Physische Maschinen“

6

Kapitel 6: Verwalten von virtuellen Maschinen

Sie verwalten eine virtuelle Maschine (VM), um ihren Betrieb zu steuern, ihr Ressourcen bereitzustellen oder ihr Gastbetriebssystem und Anwendungen zu konfigurieren.

Sie können virtuelle Maschinen auf der Seite **Virtuelle Maschinen** der ztC Console anzeigen und verwalten. Wie Sie diese Seite aufrufen, wird unter Die Seite „Virtuelle Maschinen“ beschrieben. Zur Ausführung bestimmter Verwaltungsaufgaben lesen Sie die folgenden Themen.

Zum Verwalten des Betriebszustands einer VM lesen Sie:

- Starten einer virtuellen Maschine
- Herunterfahren einer virtuellen Maschine
- Ausschalten einer virtuellen Maschine
- Öffnen einer VM-Konsolensitzung
- Umbenennen einer virtuellen Maschine
- Entfernen einer virtuellen Maschine

Sie können Informationen zu einer VM auch mit dem Befehl `snmptable` anzeigen (siehe Beziehen der System-Informationen mit snmptable.)

Zum Erstellen oder Konfigurieren einer VM lesen Sie:

- Planen von VM-Ressourcen (virtuelle CPUs, Arbeitsspeicher, Speicher und Netzwerke)
- Erstellen und Migrieren von virtuellen Maschinen
- Verwalten von virtuellen CDs
- Konfigurieren von Windows-basierten virtuellen Maschinen

- Konfigurieren von Linux-basierten virtuellen Maschinen
- Verwalten von VM-Ressourcen

Zum Verbinden eines USB-Geräts mit einer virtuellen Maschine lesen Sie Anschließen eines USB-Geräts an eine virtuelle Maschine.

Zum Ausführen erweiterter Aufgaben lesen Sie:

- Zuweisen einer spezifischen MAC-Adresse zu einer virtuellen Maschine
- Auswählen einer bevorzugten PM für eine virtuelle Maschine
- Ändern der Schutzstufe für eine virtuelle Maschine (HV oder FT)
- Konfigurieren der Startreihenfolge für virtuelle Maschinen
- Zurücksetzen der MTBF für eine ausgefallene virtuelle Maschine

Ein lokaler Benutzer mit der Rolle **VM-Manager** kann viele dieser Aufgaben ausführen. Im Einzelnen kann der **VM-Manager**:

- Aufgaben mit den verfügbaren Funktionsschaltflächen und Aktionen auf der Seite „Virtuelle Maschinen“ ausführen (siehe Die Seite „Virtuelle Maschinen“).
- Alle verfügbaren Registerkarten auf der Seite „Virtuelle Maschinen“ anzeigen (siehe Die Seite „Virtuelle Maschinen“.
- Auf der Seite „Virtuelle CDs“ VCDs erstellen und löschen (siehe Die Seite „Virtuelle CDs“).

Informationen zur Zuweisung der Rolle **VM-Manager** finden Sie unter Verwalten lokaler Benutzerkonten.

Planen von VM-Ressourcen

Wenn Sie virtuelle Maschinen erstellen, planen Sie die Zuordnung von Systemressourcen, um Systemleistung und kontinuierliche Betriebszeit zu optimieren.

Informationen zur Planung der Ressourcenzuordnung für virtuelle Maschinen finden Sie in den folgenden Themen:

- Planen von VM-vCPUs
- Planen von VM-Arbeitsspeicher
- Planen von VM-Speicher
- Planen von VM-Netzwerken

Planen von VM-vCPUs

Ordnen Sie virtuelle CPUs (vCPUs) zu, um einer virtuellen Maschine im ztC Edge-System Rechenressourcen zuzuweisen.

Beachten Sie die folgenden Informationen und Einschränkungen, wenn Sie einer VM vCPUs zuordnen:

- Jede vCPU stellt eine virtuelle Einheit von Rechenleistung dar. Die Gesamtzahl der in einem System verfügbaren vCPUs entspricht dem Mindestwert für Hardwarethreads, die durch jede der physischen Maschinen (PMs) im System dargestellt wird. In einem System mit einer PM, die 4 Kerne und 2 Threads pro Kern hat (8 vCPUs), und einer zweiten PM, die 8 Kerne und 2 Threads pro Kern hat (16 vCPUs), beträgt die Gesamtzahl der verfügbaren vCPUs 8 (die kleinste Threadanzahl auf beiden PMs).
- Die Anzahl der vCPUs, die für die VMs verfügbar sind, entspricht der Gesamtzahl der vCPUs im System.
- Die Höchstzahl VCPUs, die Sie einer beliebigen VM zuordnen können, ist die Gesamtzahl der VCPUs im System.
- Windows-basierte VMs: Wenn Sie die Anzahl der zugeordneten VCPUs von 1 zu *n* oder von *n* zu 1 ändern, müssen Sie die VM nach dem Neustarten am Ende der Neuzuweisung (siehe Neuzuweisen von VM-Ressourcen) herunterfahren und ein zweites Mal neu starten. Dadurch kann sich die VM selbst für symmetrisches Multiprocessing (SMP) neu konfigurieren. Die VM verhält sich unerwartet und kann nicht verwendet werden, bis sie neu gestartet wurde.
- Auf der Seite **System** der ztC Console (siehe Die Seite „System“) sind die Gesamtanzahl der VCPUs, die Anzahl der VCPUs, die der ztC Edge-Systemsoftware zugeordnet sind, die Anzahl der von aktiven VMs verwendeten VCPUs sowie die Anzahl der freien VCPUs angegeben.
- Die Stratus Redundant Linux-Software lässt die übermäßige Zuweisung von VCPUs (Over-Provisioning) zu. Wenn die Anzahl der freien VCPUs auf der Seite **System** weniger als null ist, haben Sie zu viele VCPUs zugewiesen (Over-Provisioning); die Konsole zeigt dies an und gibt auch den ungefähren Wert des Over-Provisioning der VCPUs an.
- Das Over-Provisioning der VCPUs verhindert nicht, dass Sie VMs starten oder erstellen; es ist jedoch empfehlenswert, das System nicht in einem Over-Provisioning-Zustand auszuführen.

Überlegungen beim Over-Provisioning virtueller CPUs

> **Hinweis**: Im Allgemeinen sollten Sie das Over-Provisioning von VM-Ressourcen vermeiden. Am besten isolieren Sie die Ressourcen der einzelnen VMs, um sie vor anderen VMs zu schützen, bei denen es möglicherweise Ressourcenlecks oder unerwartete Leistungsspitzen gibt. Wenn Sie VMs erstellen und konfigurieren, weisen Sie dedizierte Ressourcen zu, die nicht von anderen VMs verwendet werden können.

Das Over-Provisioning von physischen CPUs sollte nur unter den folgenden Bedingungen erfolgen:

- Der Höchstwert an von allen VMs verwendeten VCPU-Ressourcen übersteigt nicht die physischen Ressourcen des ztC Edge-Systems.
- Mindestens eine der VMs wird zu unterschiedlichen Zeiten verwendet (zum Beispiel für Sicherungen, die nicht zu Spitzenzeiten ausführt werden).
- Mindestens eine der VMs wird gestoppt, wenn die andere ausgeführt wird, zum Beispiel während VM-Upgrades oder VM-Zeitpunktsicherungen oder -wiederherstellungen.
- Die Spitzenlast aller von VMs verwendeten CPUs beeinträchtigt nicht die Vereinbarungen zum Servicelevel (SLAs) oder Antwortzeitanforderungen.
- Die CPU-Verwendung jeder VM ist klar und ihre Anwendungen sind nicht anfällig für Ressourcenlecks. Beim Over-Provisioning von CPUs kann ein Leck in einer CPU die Leistung der anderen VMs beeinflussen.

Verwandte Themen

Übersicht über die Systemanforderungen

Erstellen und Migrieren von virtuellen Maschinen

Verwalten von VM-Ressourcen

Planen von VM-Arbeitsspeicher

Sie ordnen Arbeitsspeicher zu, um einer virtuellen Maschine (VM) im ztC Edge-System physischen Arbeitsspeicher zuzuweisen.

Beachten Sie die folgenden Informationen und Einschränkungen, wenn Sie einer VM Arbeitsspeicher zuordnen:

- Der Gesamtarbeitsspeicher, den Sie den VMs zuweisen können, entspricht der Größe des Arbeitsspeichers, der im ztC Edge-System verfügbar ist (siehe Übersicht über die Systemanforderungen) abzüglich des Arbeitsspeichers, der der ztC Edge-Systemsoftware zugeordnet ist. Wenn der Arbeitsspeicher insgesamt zum Beispiel 32 GB beträgt und 2 GB für die Systemsoftware zugewiesen werden, sind für die VMs 30 GB Arbeitsspeicher verfügbar.
- Bei Systemen, die für zwei Knoten lizenziert sind, können Sie für eine einzelne VM bei Bedarf den gesamten Arbeitsspeicher bereitstellen, der den VMs insgesamt zur Verfügung steht.Jede VM verbraucht den angeforderten Arbeitsspeicher plus 20 % davon für Overhead (Verwaltungsdaten).
- Die minimale Arbeitsspeicherzuordnung beträgt 256 MB, 64-Bit-Betriebssysteme benötigen jedoch mindestens 600 MB. Überprüfen Sie die Arbeitsspeicheranforderungen der Gastbetriebssysteme.
- Auf der Seite **System** der ztC Console (siehe Die Seite „System“) sind die Gesamtgröße des Arbeitsspeichers, der dem ztC Edge-System zugeordnete Arbeitsspeicher, der von den laufenden VMs verbrauchte Arbeitsspeicher und der freie Arbeitsspeicher angegeben. Auf dieser Seite können Sie Ihre Arbeitsspeicherzuordnungen überprüfen.
- Die Stratus Redundant Linux-Software lässt die übermäßige Zuweisung (Over-Provisioning) von Arbeitsspeicher für **aktive** VMs nicht zu; so wird verhindert, dass Sie VMs starten, die den gesamten physischen Arbeitsspeicher der physischen Maschinen übersteigen. Das Over-Provisioning von Arbeitsspeicher ist nur dann sicher möglich, wenn mindestens eine der VMs **gestoppt** wurde, während die andere weiter ausgeführt wird, zum Beispiel während VM-Upgrades oder bei der Zeitpunktsicherung oder -wiederherstellung von VMs.
- Falls erforderlich, können Sie Arbeitsspeicher manuell neu verteilen, indem Sie eine oder mehrere kaum ausgelastete VMs herunterfahren oder neu konfigurieren und die verfügbaren Ressourcen dann einer stärker ausgelasteten VM zuweisen.

Verwandte Themen

Übersicht über die Systemanforderungen

Erstellen und Migrieren von virtuellen Maschinen

Verwalten von VM-Ressourcen

Planen von VM-Speicher

Planen Sie die Zuordnung von Speicher in Ihrem ztC Edge-System, um sicherzustellen, dass Sie ausreichend Speicherplatz für virtuelle Maschinen (VMs) und Systemverwaltung haben.

Beachten Sie beim Zuordnen von Speicher zu den virtuellen Maschinen (VMs) Folgendes:

- Beachten Sie die Speicherhöchstwerte

  Die Stratus Redundant Linux-Software lässt die übermäßige Bereitstellung (Over-Provisioning) von Speicher nicht zu. Der aggregierte benötigte Speicher für alle VMs und VCDs darf nicht größer sein als der im ztC Edge-System insgesamt verfügbare Speicher.

- Lassen Sie Speicherplatz für zusätzliche VCDs

  Lassen Sie mindestens 5 GB frei, damit Sie VCDs für die Installation weiterer VMs und Anwendungen erstellen können. (Um diesen Speicherplatz verfügbar zu halten, könnten Sie VCDs löschen, wenn Sie sie nicht mehr benötigen.)

- Erstellen Sie separate Start- und Datenvolumes für jede VM

  Installieren Sie das Gastbetriebssystem und Anwendungen im ersten (Start-) Volume und erstellen Sie separate Volumes für die zugehörigen Daten. Wenn Sie Start- und Datenvolumes trennen, lassen sich die Daten leichter aufbewahren und es ist leichter, eine VM wiederherzustellen, falls das Startvolume abstürzt.

- Erstellen Sie ein Startvolume mit ausreichender Kapazität für das Gastbetriebssystem plus Verwaltungsdaten

  Beachten Sie Mindestspeicheranforderungen Ihres Gastbetriebssystems und ziehen Sie in Betracht, etwas mehr Speicher zuzuordnen, um die formatierte Kapazität des Volumes und die Verwendung zu berücksichtigen. Wenn Sie dem Startlaufwerk beim Erstellen der VM zum Beispiel 5 GB zuweisen, liegt die formatierte Kapazität des Startvolumes vor der Verwendung bei ca. 4,8 GB; dies könnte für eine Anforderung von 5 GB zu wenig sein.

- Behalten Sie die maximale Volumegröße im Auge

  Wenn Sie ein Volume exportieren, importieren oder wiederherstellen, notieren Sie die maximale Volumegröße wie unter Wichtige Überlegungen aufgeführt.

Verwandtes Thema

Erstellen und Migrieren von virtuellen Maschinen

Verwalten von VM-Ressourcen

Planen von VM-Netzwerken

Sie planen Netzwerkressourcen, um zu bestimmen, wie Sie die verfügbaren virtuellen Netzwerke den virtuellen Maschinen (VMs) im ztC Edge-System zuordnen.

Wenn Sie das System bereitstellen, verbindet die Software in Systemen, die für zwei physische Maschinen (PMs) lizenziert sind, Paare aus physischen Netzwerk-Ports über zwei PMs, um redundante virtuelle Netzwerke zu bilden. Wenn Sie VMs im ztC Edge-System erstellen oder ihre Ressourcen neu zuweisen, verbinden Sie die VMs mit diesen virtuellen Netzwerken anstatt mit den physischen Netzwerk-Ports. Bei Systemen, die für zwei Knoten lizenziert sind, verbindet die Software Paare aus physischen Netzwerk-Ports über zwei physische Maschinen (PMs), um diese redundanten virtuellen Netzwerke zu bilden.

Beachten Sie beim Verbinden von VMs mit virtuellen Netzwerken die folgenden Informationen und Einschränkungen:

- Sie können eine VM mit mehreren virtuellen Netzwerken verbinden und Sie können mehrere VMs mit demselben virtuellen Netzwerk verbinden.
- Die Stratus Redundant Linux-Software erlaubt das unbegrenzte Zuweisen von Netzwerkressourcen (Over-Provisioning). Deshalb sollten Sie ein Profil der Anforderungen einer VM für Netzwerkbandbreite/Antwortzeit erstellen, wenn Sie virtuelle Netzwerke zuordnen.
- Wenn sich mehrere VMs dasselbe virtuelle Netzwerk teilen, wird die verfügbare Netzwerkbandbreite gleichmäßig unter den VMs aufgeteilt. Anders als bei der vCPU-Kapazität gibt es keine Möglichkeit, Bandbreitenressourcen proportional aufzuteilen. Deshalb kann die starke Auslastung der Netzwerkressourcen durch eine VM die Leistung aller VMs in diesem Netzwerk beeinträchtigen. Wenn eine VM hohe Bandbreitenanforderungen hat, sollten Sie diese VM vielleicht mit einem dedizierten virtuellen Netzwerk verbinden.

Verwandte Themen

Allgemeine Netzwerkanforderungen und -konfigurationen

Erstellen und Migrieren von virtuellen Maschinen

Verwalten von VM-Ressourcen

Erstellen und Migrieren von virtuellen Maschinen

Erstellen Sie eine neue virtuelle Maschine (VM) in einem System, indem Sie eine neue VM erstellen, eine vorhandene VM oder physische Maschine (PM) direkt über das Netzwerk migrieren oder eine OVF-Datei

(Open Virtualization Format) bzw. eine OVA-Datei (Open Virtualization Appliance) aus einer vorhandenen VM importieren.

Zum Erstellen einer neuen VM (ohne vorhandene Quell-VM oder PM) lesen Sie Erstellen einer neuen virtuellen Maschine.

Zum Kopieren einer vorhandenen VM in einem System, um eine neue VM oder ein Duplikat zur Fehlerbehebung zu erstellen, lesen Sie Kopieren einer virtuellen Maschine.

Um eine VM von einem anderen System zu migrieren oder zu importieren oder um eine VM auf demselben System wiederherzustellen, lesen Sie eines der folgenden Themen:

- Migrieren einer physischen oder virtuellen Maschine in ein System

  Verwenden Sie den *P2V-Client* (**virt-p2v**), um eine PM oder VM direkt über das Netzwerk zu einer neuen VM im System zu übertragen.

- Exportieren einer virtuellen Maschine

  Verwenden Sie die ztC Console, um die Quell-VM in OVF- und VHD-Dateien in einer Netzwerkfreigabe zu exportieren.

- Importieren einer OVF- oder OVA-Datei

  Verwenden Sie die ztC Console, um OVF- und VHD-Dateien aus einem anderen ztC Edge-System in das ztC Edge-System oder um OVF- und VHD-Dateien bzw. eine OVA-Datei aus einem VMware vSphere-gestützten System in das ztC Edge-System zu importieren.

- Ersetzen/Wiederherstellen einer virtuellen Maschine aus einer OVF-Datei

  Verwenden Sie die ztC Console, um OVF- und VHD-Dateien zurück auf dasselbe System zu importieren und so eine vorhandene VM mit einer früheren Sicherungskopie zu überschreiben bzw. wiederherzustellen.

Verwandte Themen

Verwalten von virtuellen Maschinen

Erstellen einer neuen virtuellen Maschine

Erstellen Sie eine neue virtuelle Maschine (VM), um ein Gastbetriebssystem in Ihrem ztC Edge-System zu installieren. (Sie können auch eine vorhandene VM oder physische Maschine (PM) migrieren wie unter Erstellen und Migrieren von virtuellen Maschinen beschrieben.)

Starten Sie den **Assistenten zum Erstellen von VMs**, indem Sie auf der Seite **Virtuelle Maschinen** auf **Erstellen** klicken. Der Assistent führt Sie durch den Prozess zum Zuweisen von Ressourcen zur VM.

Voraussetzungen:

- Überprüfen Sie die Voraussetzungen und Überlegungen zum Zuweisen von CPUs, Arbeitsspeicher, Speicher und Netzwerkressourcen zur VM wie unter Planen von VM-Ressourcen aufgeführt.
- Sie können VMs erstellen, die unterstützte Gastbetriebssysteme und Start-Schnittstellen ausführen wie unter Getestete Gastbetriebssysteme beschrieben.
- Sie können eine remote ISO-Datei oder eine startfähige virtuelle CD (VCD) als Quelle auswählen, von der die VM gestartet wird. Für eine remote ISO-Datei benötigen Sie eine URL oder den Pfadnamen für das Repository. Wenn sich die remote ISO-Datei auf einem freigegebenen Netzlaufwerk befindet, benötigen Sie auch einen Benutzernamen und Kennwort. Wenn Sie eine startfähige VCD mit der Installationssoftware für Windows oder Linux benötigen, erstellen Sie sie wie unter Erstellen einer virtuellen CD beschrieben. Die startfähige VCD muss eine einzelne CD oder DVD sein. Mehrere CDs oder DVDs werden nicht unterstützt.
- Stellen Sie sicher, dass beide PMs des ztC Edge-Systems online und mit dem Netzwerk verbunden sind, andernfalls kann das System die VM nicht richtig erstellen.

So erstellen Sie eine neue VM

1. Vergewissern Sie sich, dass auf der Seite **Physische Maschinen** (siehe Die Seite „Physische Maschinen“) eines Systems, das für zwei Knoten lizenziert ist, beide PMs den Status **wird ausgeführt** aufweisen und dass sich keine PM im Wartungsmodus oder im Prozess der Synchronisierung befindet.
2. Klicken Sie auf der Seite **Virtuelle Maschinen** (siehe Die Seite „Virtuelle Maschinen“) auf **Erstellen**, um den **Assistenten zum Erstellen von VMs** zu öffnen.
3. Auf der Seite **Name, Beschreibung, Schutz und Betriebssystem**:
   a. Geben Sie den **Namen** und optional die **Beschreibung** für die VM ein, wie sie in der ztC Console erscheinen sollen.

      Der Name der VM muss die folgenden Anforderungen erfüllen:

- Ein VM-Name muss mit einem Wort oder einer Zahl beginnen, und der Name darf keine Sonderzeichen enthalten (zum Beispiel #, % oder $).
- Ein VM-Name darf keinen Präfix mit Bindestrich enthalten, zum Beispiel Zombie- oder migrieren-.
- Ein VM-Name darf höchstens 85 Zeichen enthalten.

b. Wählen Sie die Schutzstufe für die VM:

- **Fehlertolerant (FT)** - Schützt eine Anwendung transparent, indem eine redundante Umgebung für eine VM erstellt wird, die auf zwei physischen Maschinen ausgeführt wird. Verwenden Sie den FT-Betrieb für Anwendungen, die einen größeren Schutz vor Ausfallzeiten brauchen, als der HV-Betrieb bieten kann.
- **Hohe Verfügbarkeit (HV)** - Bietet grundlegendes Failover und Wiederherstellung, wobei für einige Fehler jedoch ein (automatischer) VM-Neustart zur Wiederherstellung erforderlich ist. Verwenden Sie HV für Anwendungen, die eine gewisse Ausfallzeit tolerieren und nicht den Ausfallschutz benötigen, den FT bietet.

Weitere Informationen zu diesen Schutzstufen finden Sie unter Betriebsmodi.

c. Wählen Sie für **Start-Schnittstelle** eine der folgenden Optionen:

- **BIOS** - Basic Input/Output System
- **UEFI** - Unified Extensible Firmware Interface

Hinweise:

1. Stellen Sie sicher, dass das Gastbetriebssystem die ausgewählte **Start-Schnittstelle** unterstützt, andernfalls kann das Gastbetriebssystem nicht richtig starten. Eine Liste der Gastbetriebssysteme und Start-Schnittstellen, die in ztC Edge-Systemen unterstützt werden, finden Sie unter Getestete Gastbetriebssysteme.
2. Sie können die **Start-Schnittstelle** nur beim Erstellen einer VM festlegen. Später lässt sich diese Einstellung nicht mehr ändern.

d. Wählen Sie für **Starten von** eine der folgenden Startquellen aus:

- **VCD** - Die Startquelle ist eine VCD. Wählen Sie eine Quelle aus dem Pulldownmenü aus.

- **Remote ISO-Datei über Windows-Freigabe (CIFS/SMB)** - Die Startquelle ist eine remote ISO-Datei auf einem freigegebenen Netzlaufwerk. Sie müssen Werte für **Benutzername** und **Kennwort** eingeben. Geben Sie für **Repository** einen Wert im Format ***Maschinen_URL**Freigabename*** ein (zum Beispiel **\\192.168.1.34\MeinISO_Ordner**).
- **Remote ISO-Datei über NFS** - Die Startquelle ist eine remote ISO-Datei, auf die über NFS zugegriffen wird. Für **Repository** geben Sie die URL des Remotesystems im Format ***nnn.nnn.nnn.nnn*** ein (geben Sie nicht **http://** oder **https://** ein).

Um eine Liste der verfügbaren ISO-Repositorys anzuzeigen, klicken Sie auf **ISOs auflisten** und wählen Sie dann eine ISO-Datei aus. Der vollständige Pfadname der ausgewählten ISO-Datei wird unter **Repository** angezeigt. Sie können die angezeigte ISO-URL nicht bearbeiten.

e. Klicken Sie auf **Weiter**.

4. Auf der Seite **vCPUs und Arbeitsspeicher**:
   a. Geben Sie die Anzahl der **vCPUs** und die Größe des **Arbeitsspeichers** an, welcher der VM zugewiesen werden soll. Weitere Informationen finden Sie unter Planen von VM-vCPUs und Planen von VM-Arbeitsspeicher.
   b. Klicken Sie auf **Weiter**.
5. Auf der Seite **Volumes**:
   a. Geben Sie den **Namen** des Startvolumes ein, wie er in der ztC Console erscheinen soll.
   b. Geben Sie die **Volumegröße** des zu erstellenden Volumes in Gigabytes (GB) an. Weitere Informationen zum Zuordnen von Speicher finden Sie unter Planen von VM-Speicher.
   c. Erstellen Sie ggf. weitere Datenvolumes, indem Sie auf **Neues Volume hinzufügen** klicken und die Parameter für die einzelnen Volumes angeben. (Sie können Volumes auch nach dem Erstellen der VM hinzufügen, indem Sie den Assistenten **Virtuelle Maschine neu zuweisen** verwenden wie unter Erstellen eines Volumes in einer virtuellen Maschine beschrieben.)
   d. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Netzwerke** die gemeinsamen Netzwerke aus, die mit der VM verbunden werden sollen (weitere Informationen finden Sie unter Planen von VM-Netzwerken). Sie können das Netzwerk auch aktivieren (oder deaktivieren) und die MAC-Adresse angeben. Klicken Sie zum Fortfahren auf **Weiter**.

7. Auf der Seite **Erstellungsübersicht**:

    a. Überprüfen Sie die Angaben in der Erstellungsübersicht. Klicken Sie auf **Zurück**, falls Sie Änderungen vornehmen müssen.

    b. Wenn Sie verhindern möchten, dass automatisch eine Konsolensitzung gestartet wird, um die Softwareinstallation zu beobachten, deaktivieren Sie das Kontrollkästchen **Konsole starten**.

    c. Um die VM-Zuweisungen zu bestätigen und mit der Softwareinstallation zu beginnen, klicken Sie auf **Fertigstellen**.

    Der **Assistent zum Erstellen von VMs** zeigt den Fortschritt der Erstellung an und öffnet ggf. das Konsolenfenster. Wenn das Konsolenfenster geöffnet wurde, kann es noch bis zu eine Minute dauern, bis die Konsole eine Verbindung zur VM hergestellt hat.

8. Wenn bei einer Windows-basierten VM die VM-Konsole geöffnet wird, klicken Sie in das Konsolenfenster und halten Sie sich bereit, auf eine beliebige Taste zu drücken, um das **Windows-Setup** von der VCD oder Remote-ISO auszuführen.

    ```
    Press any key to boot from CD or DVD...
    ```

    Bei Windows-basierten VMs mit dem Starttyp UEFI müssen Sie innerhalb von ein oder zwei Sekunden eine beliebige Taste drücken, andernfalls erscheint die **UEFI Interactive Shell**. In diesem Fall können Sie folgendermaßen vorgehen, um das **Windows-Setup** auszuführen:

    a. Geben Sie in der **UEFI Interactive Shell** bei der Eingabeaufforderung `Shell>` den Befehl `exit` ein und drücken Sie die **Eingabetaste**.

    ```
    Shell> exit
    ```

    b. Wählen Sie mithilfe der Pfeiltasten **Weiter** aus und drücken Sie die **Eingabetaste**.

    ```
    Select Language

    Device Manager
    Boot Manager
    Boot Maintenance Manager

    Continue
    Reset
    ```

    c. Wenn die VM neu gestartet wird, drücken Sie eine beliebige Taste, um das **Windows-Setup** von der VCD oder der Remote-ISO auszuführen.

```
Press any key to boot from CD or DVD...
```

d. Wenn Sie nicht rechtzeitig auf eine Taste drücken und wieder die **UEFI Interactive Shell** angezeigt wird, wiederholen Sie die Schritte a-c.

9. Falls eine VM-Konsolensitzung gestartet wird, können Sie den Fortschritt der Betriebssysteminstallation überwachen (ggf. müssen Sie Popupfenster in Ihrem Browser zulassen) und etwaigen Eingabeaufforderungen nachkommen.
10. Nach der Installation des Betriebssystems konfigurieren Sie die zusätzlichen Ressourcen und die Software, die für die Produktionsverwendung benötigt wird, wie in den folgenden Themen beschrieben:
    - Konfigurieren von Windows-basierten virtuellen Maschinen
    - Konfigurieren von Linux-basierten virtuellen Maschinen

> **Achtung**: Kommt es vor dem letzten Neustart nach Abschluss des Installationsvorgangs zu einem Ausfall der primären PM oder einem Absturz der VM, muss die Installation der VM ggf. neu gestartet werden.

Wenn der Installationsvorgang für eine der folgenden Komponenten unterbrochen wird, kann die VM keinen Neustart ausführen:

- das Gastbetriebssystem, einschließlich der Konfigurationsschritte
- sämtliche Middleware oder Anwendungen, die Systemdateien verändern

Verwandte Themen

Kopieren einer virtuellen Maschine

Umbenennen einer virtuellen Maschine

Entfernen einer virtuellen Maschine

Erstellen und Migrieren von virtuellen Maschinen

Verwalten von VM-Ressourcen

Verwalten des Betriebs einer virtuellen Maschine

Kopieren einer virtuellen Maschine

Kopieren Sie eine virtuelle Maschine (VM), wenn Sie eine vorhandene VM in Ihrem ztC Edge-System klonen möchten. Sie können zum Beispiel eine stabile VM kopieren, um eine neue VM zu erstellen, oder Sie kopieren

eine VM, die nicht richtig funktioniert, und verwenden die Kopie für die Fehlersuche. (Wenn Sie eine VM aus einem anderen System importieren oder migrieren möchten, lesen Sie den Überblick unter Erstellen und Migrieren von virtuellen Maschinen.)

Um eine VM zu kopieren, wählen Sie auf der Seite **Virtuelle Maschinen** eine VM aus und klicken auf **Kopieren**. Ein Assistent führt Sie durch den Prozess zum Umbenennen und Zuweisen von Ressourcen zur neuen VM.

Beim Kopieren einer VM wird eine identische VM mit einer eigenen, eindeutigen SMBIOS UUID, Systemseriennummer, MAC-Adresse und Hardwarekennung erstellt.

Hinweise:

- Um Konflikte mit der Quell-VM zu vermeiden, weist der Kopier-Assistent jeder Netzwerkschnittstelle auf der neuen VM automatisch eine neue MAC-Adresse zu; möglicherweise müssen Sie jedoch IP-Adressen und Hostnamen manuell aktualisieren.
- Wenn das ztC Edge-System während des Kopierens einer VM von der primären PM zur sekundären PM wechselt, kann der Kopiervorgang nicht abgeschlossen werden. Dies beeinträchtigt nicht die durchgängige Betriebszeit Ihres Systems, Sie müssen jedoch alle Volumes löschen, die mit der kopierten VM verknüpft sind, und die Kopie neu starten.

Voraussetzungen:

- Sie müssen eine VM herunterfahren, bevor Sie sie kopieren.
- Damit der Kopiervorgang korrekt ausgeführt werden kann, müssen beide PMs des ztC Edge-Systems online sein.

So kopieren Sie eine VM im ztC Edge-System

1. Vergewissern Sie sich, dass auf der Seite **Physische Maschinen** (siehe Die Seite „Physische Maschinen“) eines Systems, das für zwei Knoten lizenziert ist, beide PMs den Status **wird ausgeführt** aufweisen und dass sich keine PM im Wartungsmodus oder im Prozess der Synchronisierung befindet.
2. Wählen Sie auf der Seite **Virtuelle Maschinen** (siehe Die Seite „Virtuelle Maschinen“) die VM aus, die Sie kopieren möchten, und klicken Sie auf **Herunterfahren**.
3. Wenn die VM gestoppt wurde, klicken Sie auf **Kopieren**, um den Kopier-Assistenten zu öffnen.

4. Auf der Seite **Name, Beschreibung und Schutz**:
    a. Geben Sie den **Namen** und optional die **Beschreibung** für die VM ein, wie sie in der ztC Console erscheinen sollen.
    b. Wählen Sie die Schutzstufe für die VM:
        - **Fehlertolerant (FT)**
        - **Hochverfügbar (HV)**

        Informationen über diese Schutzlevel finden Sie unter Erstellen einer neuen virtuellen Maschine und Betriebsmodi.
    c. Klicken Sie auf **Weiter**.
5. Auf der Seite **vCPUs und Arbeitsspeicher**:
    a. Geben Sie die Anzahl der **vCPUs** und die Größe des **Arbeitsspeichers** an, welcher der VM zugewiesen werden soll. Weitere Informationen finden Sie unter Planen von VM-vCPUs und Planen von VM-Arbeitsspeicher.
    b. Klicken Sie auf **Weiter**.
6. Auf der Seite **Volumes**:
    - Geben Sie den **Namen** des Volumes ein.
    - Legen Sie die**Volumegröße** jedes Volumes.
    - Klicken Sie auf **Neues Volume hinzufügen**, um ein neues Datenvolume zu erstellen. (Falls Sie diese Schaltfläche nicht sehen, führen Sie einen Bildlauf zum unteren Rand der Assistentenseite durch.)

    Weitere Informationen finden Sie unter Planen von VM-Speicher. Klicken Sie zum Fortfahren auf **Weiter**.
7. Aktivieren Sie auf der Seite **Netzwerke** das Kontrollkästchen für jedes gemeinsame Netzwerk, das Sie an die VM anhängen möchten.
8. Auf der Seite **Kopieübersicht**:
    a. Überprüfen Sie die Angaben in der Konfigurationsübersicht. Klicken Sie auf **Zurück**, falls Sie Änderungen vornehmen müssen.
    b. Um das Kopieren der VM fortzusetzen, klicken Sie auf **Fertigstellen**.

Nachdem der Kopiervorgang abgeschlossen ist, kann das ztC Edge-System damit fortfahren, die Daten zwischen PMs zu synchronisieren, um den hochverfügbaren (HV) oder fehlertoleranten (FT) Betrieb zu ermöglichen.

Fehlerbehebung

Verwenden Sie die folgenden Informationen, falls es beim Kopierprozess zu Problemen kommt.

So räumen Sie nach einem abgebrochenen oder fehlgeschlagenen Kopiervorgang auf

Entfernen Sie alle Volumes, die mit der kopierten VM verknüpft sind.

Verwandte Themen

Erstellen und Migrieren von virtuellen Maschinen

Verwalten von VM-Ressourcen

Verwalten des Betriebs einer virtuellen Maschine

Migrieren einer physischen oder virtuellen Maschine in ein System

Sie migrieren eine physische Maschine (PM) oder virtuelle Maschine (VM), um sie über das Netzwerk zu einer neuen VM in einem System zu übertragen. (Sie können auch eine Open Virtualization Format (OVF)-Datei oder Open Virtualization Appliance (OVA)-Datei in ein System importieren wie unter Erstellen und Migrieren von virtuellen Maschinen zusammengefasst.)

In den folgenden Abschnitten wird beschrieben, wie Sie eine PM oder VM über das Netzwerk migrieren: Laden Sie die ISO-Datei des *P2V-Clients* (**virt-p2v**) herunter, starten Sie die ISO-Datei des P2V-Clients auf der Quell-PM oder -VM und verwenden Sie schließlich den Client, um die sichere Netzwerkübertragung von der Quellseite aus zu konfigurieren, einzuleiten und zu überwachen. Bis zum Abschluss der Migration sind im System keine Konfigurationsschritte erforderlich, Sie können auf der Seite **Volumes** der ztC Console jedoch feststellen, dass die Migration stattfindet, wenn die zur neuen VM gehörigen Volumes nach und nach angezeigt werden.

Achtung: Eventuell sollten Sie die Quell-PM oder -VM sichern, bevor Sie die Migration vorbereiten.

Hinweise:

- Der Migrationsprozess unterstützt nur PMs oder VMs, auf denen eines der folgenden Betriebssysteme ausgeführt wird:
  - CentOS/RHEL 7.4 oder 7.5
  - Microsoft Windows 7, 8.x oder 10; oder Windows Server 2008 R2, 2012 oder 2016.
  - Ubuntu 18.04 Server – Nach der Migration dieser VM müssen Sie weitere Schritte durchführen. Siehe So schließen Sie die Migration einer Ubuntu-VM ab.
  - VMware Version 6.x
- Bei Windows-basierten PMs oder VMs, die den *Ruhezustand* oder den *Schnellstartmodus* unterstützen, müssen Sie diese Funktionen vor dem Migrationsprozess deaktivieren. Um den Ruhezustand oder den Schnellstartmodus vollständig zu deaktivieren, lesen Sie die Anleitungen für die Wiederherstellung nach einer fehlgeschlagenen Migration mit dem Fehler `Failed to mount '/dev/sda1: Operation not permitted` weiter unter im Abschnitt **Fehlerbehebung**.
- Bei Linux-basierten PMs oder VMs sollten Sie in Betracht ziehen, die Datei `/etc/fstab` vor dem Migrationsprozess zu bearbeiten und die Einträge für Datenvolumes auszukommentieren, damit nur das Startvolume bereitgestellt wird. Da Linux-basierte VMs im ztC Edge-System andere Gerätenamen verwenden, startet eine neue VM möglicherweise im Einzelbenutzermodus, wenn Volumes nicht mit ihren ursprünglichen Gerätenamen bereitgestellt werden können. Sie können die `/etc/fstab`-Einträge mit den richtigen Gerätenamen nach der Migration wiederherstellen wie unter **Fehlerbehebung** beschrieben.
- Wenn Sie eine VMware-VM migrieren, müssen Sie die VM nicht nur in der VMware-Konsole ausschalten, sondern auch mit dem Befehl „Herunterfahren“ des Betriebssystems herunterfahren. Wenn Sie die VM nur in der VMware-Konsole ausschalten, schlägt die Migration fehl.
- Die Quell-PM oder -VM muss offline sein, solange der Migrationsprozess läuft. Sie sollten in Betracht ziehen, für die Migration einen Wartungszeitraum einzuplanen.
- Wie lange die Migration der PM oder VM dauert, ist von der Größe und der Anzahl der Volumes im Quellsystem sowie von der Netzwerkbandbreite zwischen dem Quell- und dem

Zielsystem abhängig. Das Übertragen eines Quellsystems mit einem 20-GB-Startvolume über ein 1-Gbit-Netzwerk kann zum Beispiel 30 Minuten dauern.

- Sie können mehrere PMs oder VMs gleichzeitig migrieren, durch das Teilen der Netzwerkbandbreite dauert die Migration dann aber länger.
- Um Konflikte mit der Original-PM oder -VM zu vermeiden, weist der P2V-Assistent jeder Netzwerkschnittstelle auf der neuen VM automatisch eine neue MAC-Adresse zu; Sie müssen jedoch alle IP-Adressen und Hostnamen manuell aktualisieren wie erforderlich.
- Wenn das System während einer Migration von der primären PM zur sekundären PM wechselt, kann der Migrationsprozess nicht abgeschlossen werden. Die kontinuierliche Betriebszeit des Systems wird dadurch nicht beeinträchtigt, Sie müssen den P2V-Client auf der Quell-PM oder -VM jedoch neu starten. Weitere Informationen finden Sie weiter unten im Abschnitt **Fehlerbehebung**.
- Nach der Migration einer PM oder VM ist der Netzwerktreiber möglicherweise nicht korrekt installiert. Installieren Sie den Netzwerktreiber in diesem Fall manuell. Weitere Informationen finden Sie weiter unten im Abschnitt **Fehlerbehebung**.

Voraussetzung: Damit bei einem System, das für zwei Knoten lizenziert ist, der Migrationsprozess korrekt ausgeführt werden kann, müssen beide PMs des Systems online sein. Vergewissern Sie sich, dass auf der Seite **Physische Maschinen** der ztC Console beide PMs den Status **wird ausgeführt** aufweisen und dass sich keine PM im Wartungsmodus oder im Prozess der Synchronisierung befindet.

Führen Sie die folgenden Migrationsverfahren durch (klicken Sie ggf. auf das Dropdownsymbol).

So bereiten Sie die Migration einer PM in das ztC Edge-System vor

1. Laden Sie die P2V-Client-ISO-Datei herunter. Sie ist verfügbar auf der Seite **Downloads** unter https://www.stratus.com/services-support/downloads/?tab=ztcedge.
   a. Klicken Sie auf der Seite **Downloads** auf **ztC Edge** (falls nicht bereits angezeigt) und wählen Sie die richtige Version aus.
   b. Scrollen Sie nach unten zu **Drivers and Tools** (Treiber und Tools) und dann weiter zu **ztC Edge P2V Client for Virtual or Physical Machine Migration**.
   c. Wählen Sie die Datei **P2V Client (virt-p2v)** aus.

2. Wenn Sie die Integrität des ISO-Abbilds überprüfen möchten, laden Sie auch die zugehörige Prüfsummendatei `fciv` herunter und dann die ausführbare Microsoft-Datei „File Checksum Integrity Verifier“ (FCIV) von der Microsoft-Supportwebsite. Speichern Sie beide Dateien in dem Verzeichnis, das die heruntergeladene ISO-Datei enthält.

   Öffnen Sie eine Eingabeaufforderung (Befehlszeile). Geben Sie in dem Verzeichnis, welches das ISO-Abbild, die ausführbare Datei und die Prüfsummendatei enthält, einen Befehl ähnlich dem folgenden ein, um das ISO-Abbild zu überprüfen:

   fciv -v -xml virt-p2v-n.n.n-n.nnnnnnnn.n.el6.centos.xml

   Wenn der Befehl erfolgreich war (also die Meldung `All files verified successfully` (Alle Dateien erfolgreich verifiziert) zurückgibt), fahren Sie mit dem nächsten Schritt fort. Wenn der Befehl fehlschlägt, wiederholen Sie den Download.

3. Brennen Sie die P2V-Client-ISO-Datei auf eine CD-ROM, die Sie zum Starten der Quell-PM verwenden.
4. Legen Sie die CD mit dem P2V-Client in das CD/DVD-Laufwerk der Quell-PM ein.
5. Fahren Sie die PM in Vorbereitung auf das Starten des P2V-Clients herunter.

So bereiten Sie die Migration einer VM in das ztC Edge-System vor

1. Downloaden Sie die P2V-Client-ISO-Datei aus dem Abschnitt **Drivers and Tools** der Seite **Downloads** unter https://www.stratus.com/services-support/downloads/?tab=ztcedge. Achten Sie darauf, die Version des P2V-Clients herunterzuladen, die mit der Version des ztC Edge-Systems übereinstimmt, in das Sie die VM migrieren möchten.
2. Wenn Sie die Integrität des ISO-Abbilds überprüfen möchten, laden Sie auch die zugehörige Prüfsummendatei `fciv` herunter und dann die ausführbare Microsoft-Datei „File Checksum Integrity Verifier“ (FCIV) von der Microsoft-Supportwebsite. Speichern Sie beide Dateien in dem Verzeichnis, das die heruntergeladene ISO-Datei enthält.

   Öffnen Sie eine Eingabeaufforderung (Befehlszeile). Geben Sie in dem Verzeichnis, welches das ISO-Abbild, die ausführbare Datei und die Prüfsummendatei enthält, einen Befehl ähnlich dem folgenden ein, um das ISO-Abbild zu überprüfen:

fciv -v -xml virt-p2v-n.n.n-n.nnnnnnnn.n.el6.centos.xml

Wenn der Befehl erfolgreich war (also die Meldung `All files verified successfully` (Alle Dateien erfolgreich verifiziert) zurückgibt), fahren Sie mit dem nächsten Schritt fort. Wenn der Befehl fehlschlägt, wiederholen Sie den Download.

3. Legen Sie die P2V-Client-ISO-Datei in die Quell-VM ein (bzw. verbinden Sie sie damit) und legen Sie das virtuelle CD-Laufwerk im zugehörigen Hypervisor als Startgerät fest.
4. Fahren Sie die VM in Vorbereitung auf das Starten des P2V-Clients herunter.

So migrieren Sie eine PM oder VM in das ztC Edge-System

1. Schalten Sie die Quell-PM oder -VM ein, um den P2V-Client zu starten. Nach ungefähr einer Minute wird das Fenster **virt-p2v** angezeigt.
2. Der P2V-Client bezieht die Netzwerkeinstellungen automatisch über DHCP. Statische Einstellungen sind für den Migrationsprozess nicht erforderlich, Sie können optional jedoch auf **Netzwerk konfigurieren** klicken, um die Einstellungen festzulegen. (Konfigurieren Sie die Netzwerkeinstellungen auf der Ziel-VM später im ztC Edge-System, falls erforderlich.)
3. Geben Sie die Verbindungseinstellungen für den **Konvertierungsserver** (das ztC Edge-System) ein. Geben Sie den Hostnamen oder die IP-Adresse des Systems und das **Kennwort** für das `root`-Konto ein. (Sie müssen das `root`-Konto des ztC Edge-Host-Betriebssystems verwenden wie unter Zugriff auf das Host-Betriebssystem beschrieben.)
4. Klicken Sie auf **Test connection** (Verbindung testen). Wenn der P2V-Client eine Verbindung zum ztC Edge-System herstellt, klicken Sie auf **Next** (Weiter). Es wird eine Seite mit Bereichen für **Target properties** (Zieleigenschaften), **Fixed hard disks** (Festplatten) und andere Einstellungen angezeigt.

   Wenn der P2V-Client keine Verbindung herstellen kann, überprüfen Sie die Verbindungseinstellungen und versuchen Sie es erneut.
5. Geben Sie in den **Target properties** (Zieleigenschaften) den **Namen** für die Ziel-VM ein, der in der ztC Console angezeigt wird. (Der Name muss sich von ggf. bereits im ztC Edge-System vorhandenen VMs unterscheiden.)
6. Die Werte für **# CPUs** (Anzahl der CPUs) und **Memory (MB)** (Arbeitsspeicher (MB)) werden automatisch erkannt und angezeigt, Sie können sie jedoch bei Bedarf ändern, wenn die VM im ztC Edge-System mehr CPUs oder Arbeitsspeicher als die Quell-PM oder -VM haben soll.

7. Geben Sie die **Virt-v2v-Ausgabeoptionen** für die Ziel-VM wie folgt an:

    a. Neben **Output to** (Ausgabe an) wählen Sie den Betriebsmodus **HA** (HV; hochverfügbar) oder **FT** (fehlertolerant). (Informationen über diese Betriebsmodi finden Sie unter Erstellen einer neuen virtuellen Maschine und Betriebsmodi.)

    b. Neben **Output format** (Ausgabeformat) wählen Sie das Datenträgerabbildformat **raw** oder **qcow2**.

8. Falls Sie Debuggingmeldungen aus dem Migrationsprozess speichern möchten, können Sie das Kontrollkästchen **Enable server-side debugging** (Serverseitiges Debugging aktivieren) aktivieren. (Die Debuggingmeldungen werden einbezogen, wenn Sie eine Diagnosedatei für Ihren autorisierten Stratus-Servicemitarbeiter generieren wie unter Erstellen einer Diagnosedatei beschrieben.)

9. Wählen Sie, welche **Fixed hard disks** (Volumes) in die Migration einbezogen werden sollen, indem Sie die Kontrollkästchen neben den gewünschten Geräten aktivieren.

    Sie müssen mindestens ein Volume einschließlich des Startvolumes auswählen. (Da der P2V-Client ein Linux-basiertes Hilfsprogramm ist, werden alle Geräte nach Linux-Gerätenamen aufgeführt, wobei **sda** oder **vda** das Startvolume ist.)

10. Wählen Sie, welche **Netzwerkschnittstellen** in die Migration einbezogen werden sollen, indem Sie die Kontrollkästchen neben den gewünschten Geräten aktivieren.

    Wenn das ztC Edge-Zielsystem über mehrere gemeinsame Netzwerke verfügt, können Sie auch das gemeinsame Netzwerk auswählen, mit dem jede Netzwerkschnittstelle verbunden werden soll. Doppelklicken Sie auf die Netzwerkschnittstelle, um das Dialogfeld **Netzwerk konfigurieren** zu öffnen, und wählen Sie das gemeinsame Netzwerk aus einer Dropdownliste aus.

    Im Dialogfeld **Netzwerk konfigurieren** können Sie auch für jede spezifische Netzwerkschnittstelle eine MAC-Adresse angeben. Wenn Sie keine Adresse angeben, legt das System automatisch die MAC-Adresse für jede Netzwerkschnittstelle fest.

    Klicken Sie auf **OK**, wenn Sie mit der Konfiguration der Netzwerkschnittstelle fertig sind.

11. Wenn Sie für die Migration der PM oder VM in das ztC Edge-System bereit sind, klicken Sie auf **Start conversion** (Konvertierung starten). (Falls Sie die Migration aus irgendeinem Grund abbrechen müssen, lesen Sie den Abschnitt **Fehlerbehebung** weiter unten.)

12. Nach dem erfolgreichen Abschluss der Migration zeigt der P2V-Client eine entsprechende Meldung an. Sie können ggf. die CD oder virtuelle CD auswerfen und auf **Ausschalten** klicken, um die Quell-PM oder -VM herunterzufahren.

Hinweis: Nach der Migration befindet sich die neue VM im ztC Edge-System auf der primären PM und verbleibt im angehaltenen Zustand. Bevor Sie die VM starten, schließen Sie die Migration ab wie im nächsten Verfahren beschrieben.

So schließen Sie die Migration im ztC Edge-System ab

1. Öffnen Sie die Seite **Virtuelle Maschinen** (siehe Die Seite „Virtuelle Maschinen“) in der ztC Console.
2. Wählen Sie die neue VM im oberen Fensterbereich aus und klicken Sie auf **Konfig**, um den Assistenten **Virtuelle Maschine neu zuweisen** zu öffnen wie unter Neuzuweisen von VM-Ressourcen beschrieben. Verwenden Sie den Assistenten, um die gewünschten Werte für vCPUs, Arbeitsspeicher, Speicher und Netzwerkeinstellungen für die VM zu konfigurieren:
   - Falls die Quell-PM oder -VM über mehrere Netzwerkschnittstellen verfügte, konfigurieren Sie die zusätzlichen Netzwerkschnittstellen, die im Migrationsprozess nicht berücksichtigt wurden.
   - Wenn Sie die Quell-PM oder -VM weiterhin ausführen möchten, stellen Sie sicher, dass sich die MAC-Adresse für jede Netzwerkschnittstelle in der neuen VM von der Quell-PM oder -VM unterscheidet.

   Klicken Sie in der letzten Seite des Assistenten auf **Fertigstellen**, um die Änderungen zu übernehmen.
3. Klicken Sie auf **Start**, um die neue VM zu starten.
4. Klicken Sie auf **Konsole**, um die Konsole der VM zu öffnen, und melden Sie sich beim Gastbetriebssystem an. (Informationen zur Verwendung der Konsole finden Sie unter Öffnen einer VM-Konsolensitzung.)
5. Deaktivieren Sie alle Dienste des Gastbetriebssystems, die für den Betrieb im ztC Edge-System nicht erforderlich sind:
   - Wenn Sie die Migration von einer PM-Quelle ausgeführt haben, deaktivieren Sie alle Dienste, die direkt mit der Hardware interagieren. Beispiele sind u.a.:
     - Dell OpenManage (OMSA)
     - HP Insight Manager
     - Diskeeper
   - Wenn Sie die Migration von einer VM-Quelle ausgeführt haben, deaktivieren Sie alle Dienste, die mit anderen Hypervisoren verknüpft sind. Beispiele sind u.a.:
     - VMware-Tools
     - Hyper-V-Tools

- Citrix-Tools für virtuelle Maschinen

Nachdem Sie diese Dienste deaktiviert haben, starten Sie das Gastbetriebssystem neu, um die Änderungen zu übernehmen.

6. Falls erforderlich, aktualisieren Sie die Netzwerkkonfiguration im Gastbetriebssystem und starten Sie es neu, um die Einstellungen zu aktivieren.
7. Überprüfen Sie, dass Sie das Gastbetriebssystem mit den zusätzlichen Windows- oder Linux-basierten Systemeinstellungen konfiguriert haben, die hier beschrieben sind:
   - Konfigurieren von Windows-basierten virtuellen Maschinen
   - Konfigurieren von Linux-basierten virtuellen Maschinen

Nachdem Sie bestätigt haben, dass die neue VM korrekt funktioniert, ist der Migrationsprozess abgeschlossen. Das System fährt jedoch möglicherweise noch damit fort, Daten zwischen PMs zu synchronisieren, um den hochverfügbaren (HV) Betrieb zu ermöglichen.

So schließen Sie die Migration einer Ubuntu-VM ab

Nach der Migration einer VM mit P2V von einem Bare-Metal-Rechner mit einer Ubuntu-Version gibt es möglicherweise Probleme mit der VM, zum Beispiel kein aktives Netzwerk. Um das Problem zu beheben, führen Sie nach der Migration der Ubuntu-VM das geeignete Verfahren der im Folgenden aufgeführten aus.

Nach der Migration einer Ubuntu 18.04-VM

1. Öffnen Sie von der ztC Console aus ein Konsolenfenster für die VM.
2. Melden Sie sich bei der VM an und gehen Sie zum Terminal.
3. Geben Sie den folgenden Befehl ein: `cd /etc/netplan`.
4. Geben Sie den folgenden Befehl ein: `sudo vi 01-netcfg.yaml`.
5. Ändern Sie in der Datei `01-netcfg.yaml` den Eintrag `eno1` zu `ens3f0`.
6. Geben Sie den folgenden Befehl ein: `sudo netplan apply`.
7. Geben Sie den folgenden Befehl ein: `ifconfig`.

Ein Neustart der VM ist nicht erforderlich, da sich die VM nach Ausführung dieser Befehle mit der konfigurierten IP-Adresse im Netzwerk befindet.

Fehlerbehebung

Verwenden Sie die folgenden Informationen, falls es beim Migrationsprozess zu Problemen kommt.

So brechen Sie den Migrationsprozess ab

Schalten Sie die Quell-PM oder -VM, auf der der P2V-Client ausgeführt wird, aus.

So räumen Sie nach einer abgebrochenen oder fehlgeschlagenen Migration auf

Öffnen Sie die ztC Console und entfernen Sie alle migrierten VMs, die zur Quell-PM oder -VM gehören. Wenn Sie den Migrationsprozess erneut ausführen möchten, starten Sie den P2V-Client auf der Quell-PM oder -VM neu.

So führen Sie nach einer fehlgeschlagenen Migration eine Wiederherstellung aus

Wenn der Migrationsprozess fehlschlägt, wird im P2V-Client auf der Quell-PM oder -VM eine Fehlermeldung angezeigt. Im ztC Edge-System wird möglicherweise eine weitere Meldung angezeigt. Verwenden Sie diese Meldungen, um das Problem zu identifizieren.

Wenn die Migration weiterhin fehlschlägt und die entsprechende Option verfügbar ist, aktivieren Sie das serverseitige Debugging. Generieren Sie nach der Migration eine Diagnosedatei, die Sie an Ihren autorisierten Stratus-Servicemitarbeiter senden können, wie unter Erstellen einer Diagnosedatei beschrieben. Die Diagnosedatei enthält alle serverseitigen Debuggingmeldungen aus dem Migrationsprozess.

So führen Sie nach einer fehlgeschlagenen Migration mit dem Fehler `Failed to mount '/dev/sda1: Operation not permitted` eine Wiederherstellung aus

Falls die Migration bei Windows-basierten PMs oder VMs mit der folgenden Fehlermeldung fehlschlägt, kann es sein, dass der *Ruhezustand* oder der *Schnellstartmodus* aktiviert ist:

```
Failed to mount '/dev/sda1': Operation not permitted
The NTFS partition is in an unsafe state. Please resume and
shutdown Windows fully (no hibernation or fast restarting), or
mount the volume read-only with the 'ro' mount option.
```

Um das Problem zu beheben, deaktivieren Sie den Ruhezustand und den Schnellstartmodus auf der Quell-PM oder -VM:

1. Melden Sie sich beim Betriebssystem der Quell-PM oder -VM an.
2. Öffnen Sie die **Energieoptionen** und klicken Sie auf **Auswählen, was beim Drücken von Netzschaltern geschehen soll**.
3. Wählen Sie neben **Beim Drücken des Netzschalters** die Option **Herunterfahren** (statt **Ruhezustand** oder **Schlafmodus**, falls vorhanden).
4. Deaktivieren Sie unter **Einstellungen für das Herunterfahren** das Kontrollkästchen neben **Schnellstart aktivieren (empfohlen)**, falls verfügbar.
5. Klicken Sie auf **Änderungen speichern**.
6. Öffnen Sie die **Powershell als Administrator** und führen Sie den folgenden Befehl aus:

   ```
   > powercfg /h off
   ```

7. Fahren Sie das Betriebssystem herunter und starten Sie den Migrationsprozess neu.

So führen Sie eine Wiederherstellung aus, wenn eine gerade migrierte Linux-basierte VM im Startstatus hängenbleibt

Eine Linux-basierte VM bleibt in der ztC Console möglicherweise im **Start**-Zustand hängen, wenn das Netzwerk der VM offline ist.

Während des Migrationsprozesses versucht der P2V-Client, jeder Netzwerkschnittstelle eine neue MAC-Adresse zuzuweisen, um Konflikte mit der Original-VM zu vermeiden. Einige Linux-basierte Betriebssysteme erkennen eine neue MAC-Adresse und erstellen automatisch eine neue Netzwerkschnittstelle dafür, während die Originalschnittstelle erhalten bleibt. Das Gastbetriebssystem startet, das Netzwerk bleibt möglicherweise jedoch offline, bis Sie die Netzwerkeinstellungen manuell konfigurieren.

Um das Problem zu beheben, öffnen Sie die VM-Konsole, melden Sie sich beim Gastbetriebssystem an und aktualisieren Sie die Skripts für den Netzwerkstart. Achten Sie darauf, dass Sie nur einen Eintrag für jede Netzwerkschnittstelle behalten und dass jede Schnittstelle eine eindeutige MAC-Adresse und die richtigen Netzwerkeinstellungen für Ihre Umgebung verwendet.

So stellen Sie fehlende Datenvolumes in der VM auf dem ztC Edge-System wieder her

Wenn die Datenvolumes nach dem Import nicht für die VM im ztC Edge-System angezeigt werden, müssen Sie die Volumes wie nachstehend beschrieben manuell wiederherstellen:

- Fahren Sie die VM herunter, führen Sie den Assistenten **Virtuelle Maschine neu zuweisen** aus und überprüfen Sie, dass Sie die Volumes auf der Seite **Volumes** einbezogen haben.
- Verwenden Sie für Windows-basierte VMs die **Datenträgerverwaltung**, um Volumes in Betrieb zu nehmen.
- Bei Linux-basierten VMs bearbeiten Sie die Datei `/etc/fstab`, um die neuen Gerätenamen für die Speichergeräte widerzuspiegeln (`/dev/vda` bis `/dev/vdh`). Gerätenamen können sich auch geändert haben, wenn Volumes nicht im Import enthalten waren.

So stellen Sie fehlende Netzwerkgeräte in der VM auf dem ztC Edge-System wieder her

Wenn die Netzwerkgeräte nach dem Import nicht für die VM im ztC Edge-System angezeigt werden, müssen Sie sie wie nachstehend beschrieben manuell wiederherstellen:

- Fahren Sie die VM herunter, führen Sie den Assistenten **Virtuelle Maschine neu zuweisen** aus und überprüfen Sie, dass Sie die Netzwerke auf der Seite **Netzwerke** einbezogen haben.
- Bei Linux-basierten VMs konfigurieren Sie das Netzwerkstartskript neu, um die neuen Gerätenamen für die Netzwerkschnittstellen widerzuspiegeln.

So installieren Sie einen Netzwerktreiber manuell

Nach der Migration einer PM oder VM ist der Netzwerktreiber möglicherweise nicht korrekt installiert (zum Beispiel zeigt der Geräte-Manager den Treiber mit einer Warnung an, ). Installieren Sie den Treiber in diesem Fall manuell:

1. Öffnen Sie im VM-Konsolenfenster den **Geräte-Manager** in Gastbetriebssystem.
2. Erweitern Sie **Netzwerkadapter** und klicken Sie mit der rechten Maustaste auf **Red Hat VirtIO Ethernet Adapter** (der Treiber, der nicht korrekt funktioniert).
3. Wählen Sie **Treiber aktualisieren**.
4. Klicken Sie im Popupfenster auf **Auf dem Computer nach Treibersoftware suchen**.
5. Klicken Sie auf **Aus einer Liste verfügbarer Treiber auf meinem Computer auswählen**.
6. Wählen Sie **Red Hat VirtIO Ethernet Adapter**.
7. Klicken Sie auf **Weiter**, um den Netzwerktreiber zu installieren.

Nachdem der Treiber installiert wurde, überprüfen Sie den Status der VM in der ztC Console. Wenn der Status „wird ausgeführt“ ist (), funktioniert der Treiber korrekt.

Verwandte Themen

Erstellen und Migrieren von virtuellen Maschinen

Konfigurieren von Windows-basierten virtuellen Maschinen

Konfigurieren von Linux-basierten virtuellen Maschinen

Verwalten von VM-Ressourcen

Verwalten des Betriebs einer virtuellen Maschine

Importieren einer OVF- oder OVA-Datei

Importieren Sie eine OVF-Datei (Open Virtualization Format) oder eine OVA-Datei (Open Virtual Appliance/Application) aus einem System, wenn Sie eine VM von einem System auf ein anderes übertragen möchten oder wenn Sie ein Abbild, das Sie erstellt haben, auf dasselbe System zurück übertragen möchten, um die Original-VM wiederherzustellen oder zu duplizieren. (Um eine physische Maschine (PM) oder virtuelle Maschine (VM) ohne eine OVF- oder OVA-Datei in ein System zu übertragen, lesen Sie Migrieren einer physischen oder virtuellen Maschine in ein System.)

Sie können die VM *importieren* oder *wiederherstellen*. Beim Importieren einer VM wird eine neue Instanz der VM mit eindeutigen Hardware-IDs erstellt. Beim Wiederherstellen einer VM wird eine identische VM mit denselben Hardware-IDs (SMBIOS UUID, Systemseriennummer und MAC-Adressen, falls im VM-Abbild bereitgestellt) erstellt, die das Gastbetriebssystem und Anwendungen möglicherweise für die Softwarelizenzierung benötigen. Um Konflikte mit der Original-VM zu vermeiden, stellen Sie eine VM nur dann wieder her, wenn Sie sie in das ztC Edge-System übertragen und auf dem Quellsystem nicht mehr verwenden möchten.

In diesem Thema wird beschrieben, wie Sie eine OVF- oder OVA-Datei von einem lokalen Computer, einem USB-Gerät oder einem Remotedateisystem wie einem NFS-Export oder einer Windows-Freigabe (CIDS-Freigabe, zum Beispiel Samba) importieren. Wenn Sie eine vorhandene VM auf demselben System wiederherstellen möchten, um die VM zu überschreiben und aus einer früheren Sicherungskopie wiederherzustellen, lesen Sie Ersetzen/Wiederherstellen einer virtuellen Maschine aus einer OVF-Datei.

Hinweise:

- Importieren Sie eine VM, wenn Sie eine VM von einem „Goldabbild“ erstellen oder klonen möchten, da das System beim Importieren einer VM eindeutige Hardwarekennungen und MAC-Adressen zuweist. (Ein Goldabbild ist normalerweise eine Vorlagen-VM, die zum mehrmaligen Kopieren erstellt wurde.) Um Konflikte mit der Quell-VM zu vermeiden, weist

der Import-Assistent jeder Netzwerkschnittstelle auf der neuen VM automatisch eine neue MAC-Adresse zu; möglicherweise müssen Sie jedoch IP-Adressen und Hostnamen manuell aktualisieren.

- Sie können VMs nur dann importieren, wenn sie unterstützte Gastbetriebssysteme und Start-Schnittstellen ausführen wie unter Getestete Gastbetriebssysteme beschrieben.

  Wenn Sie eine VM importieren, importiert das System die Start-Schnittstellen-Einstellung (BIOS oder UEFI) aus der OVF- oder OVA-Datei. Sie können diese Einstellung nicht ändern.

- Sie können eine VM nur dann von einer VMware-Quelle importieren, wenn auf der Quelle VMware Version 6.x ausgeführt wird.

- Wenn Sie eine VM aus einer VMware OVA-Datei importieren, achten Sie darauf, dass auf Ihrem System genügend Speicherplatz für den Vorgang verfügbar ist. Das System benötigt verfügbaren Festplattenspeicherplatz, der der Größe der OVA-Datei plus der Gesamtgröße der zu erstellenden VM-Volumes plus 100 GB (für das Extrahieren und Verarbeiten der komprimierten OVA-Datei) entspricht. Beispiel: Wenn Sie eine 3 GB große OVA-Datei für eine VM, die ein 32 GB großes Volume benötigt, importieren möchten, brauchen Sie mindestens 3 GB + 32 GB + 100 GB = 135 GB Speicherplatz.

  Wie viel **freier** Festplattenspeicherplatz in Ihrem System verfügbar ist, sehen Sie auf der Seite **System** der ztC Console unter **Speicherzuordnung**. Wenn auf Ihrem System nicht genügend Speicherplatz für den Import einer VMware OVA-Datei verfügbar ist, können Sie entweder Speicherplatz freimachen oder die VM direkt über das Netzwerk (ohne OVF- oder OVA-Datei) migrieren. Dies wird unter Migrieren einer physischen oder virtuellen Maschine in ein System beschrieben.

- Wenn Sie eine VM zurück in dasselbe System importieren, um die VM zu duplizieren, müssen Sie die VM und doppelte Volumes entweder während des Exports oder während des Imports umbenennen. Wenn Sie die VM nicht umbenennen, benennt der Import-Assistent die neue VM und die neuen Volumes automatisch um, um Konflikte mit der Quell-VM zu vermeiden. Der Assistent hängt eine Nummer an den VM-Namen und an den Volumenamen an, die für jedes Duplikat der VM um eins erhöht wird: **MyVM**, **MyVM0**, **MyVM1** und so weiter.

- Wie lange der Import dauert, ist von der Größe und der Anzahl der Volumes in der Quell-VM sowie von der Netzwerkbandbreite abhängig. Das Übertragen einer VM mit einem 20-GB-Startvolume über ein 1-Gbit-Netzwerk kann zum Beispiel 30 Minuten dauern.
- Wenn das System während eines Importvorgangs von der primären PM zur sekundären PM wechselt, kann der Vorgang nicht abgeschlossen werden. Dies beeinträchtigt zwar nicht die kontinuierliche Betriebszeit des Systems, Sie müssen die unvollständige VM und die zugehörigen Volumes im System jedoch löschen und erneut importieren.
- Nach der Migration einer PM oder VM ist der Netzwerktreiber möglicherweise nicht korrekt installiert. Installieren Sie den Netzwerktreiber in diesem Fall manuell. Weitere Informationen finden Sie weiter unten im Abschnitt **Fehlerbehebung**.

Voraussetzung:
Bevor Sie ein VM-Abbild aus einer OVF-Datei importieren, verwenden Sie die ztC Console auf dem Quellsystem, um eine VM (siehe Exportieren einer virtuellen Maschine) in OVF- und VHD-Dateien auf einer unterstützten Netzwerkfreigabe oder auf einem USB-Gerät zu exportieren. Kopieren Sie diese Dateien auf Ihren Verwaltungscomputer oder stellen Sie das USB-Gerät oder die Netzwerkfreigabe auf dem ztC Edge-Zielsystem bereit wie unter Bereitstellen eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners im ztC Edge-System beschrieben und verwenden Sie dann die ztC Console auf dem Zielsystem, um die OVF- und VHD-Dateien zu importieren.

Erstellen Sie die OVA-Datei auf einem VMware-System, bevor Sie ein VM-Abbild aus einer OVA-Datei importieren. Das ztC Edge-System unterstützt VMware-OVA-Dateien, die eine Metadatendatei und eine oder mehrere Datenträgerabbilddateien enthalten.

So importieren Sie eine OVF- oder OVA-Datei

1. Melden Sie sich bei der ztC Console auf dem Zielsystem an.
2. Vergewissern Sie sich, dass auf der Seite **Physische Maschinen** (siehe Die Seite „Physische Maschinen“) eines Systems, das für zwei Knoten lizenziert ist, beide PMs den Status **wird ausgeführt** aufweisen und dass sich keine PM im Wartungsmodus oder im Prozess der Synchronisierung befindet.
3. Wenn Sie eine VM von einem USB-Gerät oder aus einer Netzwerkfreigabe importieren (statt vom PC, auf dem die ztC Console ausgeführt wird), stellen Sie das Gerät bzw. die Freigabe auf dem ztC Edge-

System bereit wie unter Bereitstellen eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners im ztC Edge-System beschrieben.

4. Klicken Sie auf der Seite **Virtuelle Maschinen** (siehe Die Seite „Virtuelle Maschinen“) auf **Importieren/Wiederherstellen**, um den **Assistenten zum Importieren/Wiederherstellen virtueller Maschinen** zu öffnen.
5. Wählen Sie eine der folgenden Optionen:
   - **Import von meinem PC** - Importiert die VM vom PC, auf dem die ztC Console ausgeführt wird.

     Hinweis: Beim Import von einem PC können Sie nicht „Durchsuchen“ verwenden, um VMware-OVF- und -OVA-Dateien auszuwählen, Sie können aber alle anderen Methoden verwenden, um VMware-OVF- und -OVA-Dateien zu importieren.

     Klicken Sie auf **Weiter** und dann auf **Durchsuchen**, um die gewünschte Datei auf einem lokalen Computer zu finden.
   - **Import über USB** - Importiert die VM von einem USB-Stick, der im ztC Edge-System bereitgestellt wird.

     Klicken Sie auf **Weiter** und wählen Sie dann eine Partition aus dem Pulldownmenü aus. Klicken Sie auf **OVFs/OVAs auflisten** und wählen Sie die gewünschte Datei aus dem Pulldownmenü aus. Sie können auch nach einer Datei suchen, indem Sie den Dateinamen oder einen Teil davon in das Feld *In Dateien suchen* eingeben.
   - **Import aus Remote-/Netzwerk-Windows-Freigabe (CIFS/SMB)** - Importiert die VM aus einer Windows-Freigabe in Ihrem lokalen Netzwerk. Beachten Sie, dass die maximale Länge des Pfads zur VM, einschließlich VM-Name, 4096 Zeichen beträgt.

     Klicken Sie auf **Weiter** und geben Sie Werte für **Benutzername** und **Kennwort** ein. Geben Sie für **Repository** einen Wert im Format ***Maschinen_URL**Freigabename*** ein (zum Beispiel **\\192.168.1.34\MeineOVFsfürExport**). Klicken Sie dann auf **OVFs/OVAs auflisten** und wählen Sie die gewünschte Datei aus der Liste aus.
   - **Import aus Remote-/Netzwerk-NFS** - Importiert die VM aus einer NFS-Freigabe in Ihrem lokalen Netzwerk. Beachten Sie, dass die maximale Länge des Pfads zur VM, einschließlich VM-Name, 4096 Zeichen beträgt.

Klicken Sie auf **Weiter** und geben Sie für **Repository** die URL des Remotesystems im Format ***nnn.nnn.nnn.nnn/ordnername*** ein (geben Sie nicht **http://** oder **https://** ein).

Klicken Sie auf **OVFs/OVFs/OVAs auflisten**, um eine Liste aller Dateien im Remoteordner zu sehen. Wählen Sie die gewünschte Datei zum Importieren aus. Sie können auch nach einer Datei suchen, indem Sie den Dateinamen oder einen Teil davon in das Feld *In Dateien suchen* eingeben, oder die Liste neu ordnen, indem Sie auf eine Spaltenüberschrift klicken (*Name*, *Geändert am* oder *Größe*). Klicken Sie auf den Dateinamen, um die Datei auszuwählen, und dann auf **Weiter**.

Wenn Sie eine OVA-Datei ausgewählt haben, fahren Sie mit dem nächsten Schritt fort (der Import ist für OVA-Dateien die einzige Option).

Wenn Sie eine OVF-Datei ausgewählt haben, klicken Sie auf **Weiter**. Es werden Meldungen eingeblendet, um zu bestätigen, ob es sich um eine mit ztC Edge erstellte Datei handelt und ob Sie die Option haben, die VM zu importieren oder wiederherzustellen. Wenn Sie eine mit ztC Edge erstellte OVF-Datei auswählen, können Sie die Datei importieren oder wiederherstellen, und Sie können optional die folgende Meldung einblenden:

Bei der Wiederherstellung einer VM wird versucht, die Hardware-ID und die MAC-Adressen aller Netzwerkschnittstellen beizubehalten. Wählen Sie **Wiederherstellen** nur, wenn Sie eine bestimmte Instanz einer VM wiederherstellen möchten und dies die einzige Kopie dieser VM auf allen Systemen in Ihrem Netzwerk sein wird. Eine **Wiederherstellung** erfolgt in der Regel, um eine VM aus einer zuvor erstellten Sicherung wiederherzustellen. Wählen Sie **Importieren**, wenn Sie eine VM von einem Referenzabbild erstellen oder klonen möchten, da dabei eine eindeutige Hardware-ID und eindeutige Mac-Adressen zugewiesen werden.

6. Wählen Sie **Importieren** (scrollen Sie im Fenster nach unten, falls nötig). (Bei einer mit ztC Edge erstellten OVF-Datei können Sie auch **Wiederherstellen** wählen. Weitere Informationen finden Sie unter Ersetzen/Wiederherstellen einer virtuellen Maschine aus einer OVF-Datei.)
7. Der Assistent zeigt das Fenster **Import virtueller Maschine vorbereiten** an und fordert Sie auf, ggf. zusätzliche Dateien hochzuladen. Wenn Sie dazu aufgefordert werden, wählen Sie die entsprechenden Dateien für jedes mit der VM verknüpfte Volume aus.
8. Wenn Sie eine OVF-Datei ausgewählt haben, können Sie die Informationen prüfen und ggf. bearbeiten (möglicherweise müssen Sie im Fenster nach unten scrollen):

- **Name, Start-Schnittstelle, CPU und Arbeitsspeicher**

  Zeigt den Namen der VM, die Start-Schnittstelle, die Anzahl der vCPUs und den Gesamtarbeitsspeicher an, den die VM verwenden kann. Bearbeiten Sie die Informationen, falls nötig. (Sie können die **Start-Schnittstelle** nicht ändern; das System importiert diese Einstellung aus der OVF- oder OVA-Datei.)

- **Speicher**

  Zeigt den Namen und die Größe für jedes Volume an. Wählen Sie in der Spalte **Erstellen** ein Kästchen für ein Volume aus, um Speicher für das Volume im System zuzuweisen (das Startvolume ist erforderlich). Wählen Sie in der Spalte **Daten wiederherstellen** ein Kästchen aus, um Daten für ein Volume aus der VHD-Datei zu importieren.

- **Netzwerk**

  Zeigt die verfügbaren Netzwerke an. Sie können ein Netzwerk entfernen oder ein noch nicht zugeordnetes hinzufügen. Sie können für jedes ausgewählte Netzwerk auch eine MAC-Adresse angeben. Mindestens ein Netzwerk muss immer vorhanden sein.

  Die Gesamtzahl der Netzwerke darf nicht die Anzahl der Unternehmensnetzwerke im ztC Edge-System überschreiten. Wenn Sie die VM aus einer OVF-Datei importieren, können Sie im Assistenten auswählen, welche Netzwerke entfernt werden sollen. Wenn Sie die VM aus einer OVA-Datei importieren, ignoriert das System während des Importvorgangs die überzähligen Netzwerke automatisch. In beiden Fällen können Sie vor oder nach dem Import der VM zum Wiederherstellen der Netzwerkverbindungen weitere Unternehmensnetzwerke zum ztC Edge-System hinzufügen.

9. Deaktivieren Sie wahlweise das Kontrollkästchen **Virtuelle Maschine nach Import automatisch starten**, wenn Sie die Ressourcen der VM vor dem ersten Starten neu zuweisen möchten.
10. Klicken Sie auf **Importieren**, um den Import der VM zu starten. Oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

    Der Assistent zeigt den Fortschritt an. Wenn die Übertragung abgeschlossen ist, klicken Sie auf **Fertig**, um den Assistenten zu schließen.

> **Hinweis**: Importierte Volumes werden bereits auf der Seite **Volumes** der ztC Console angezeigt, während der Importprozess noch ausgeführt wird. Sie sollten keines dieser importierten Volumes verbinden oder entfernen, bis im Importfenster angezeigt wird, dass der Prozess abgeschlossen ist; andernfalls kann der Import nicht korrekt beendet werden.

11. Verwenden Sie ggf. den Assistenten **Virtuelle Maschine neu zuweisen**, um der VM zusätzliche Ressourcen zuzuordnen wie unter Neuzuweisen von VM-Ressourcen beschrieben.

    Klicken Sie nach dem Neuzuweisen von Ressourcen zur VM auf **Start**, um die VM neu zu starten.

12. Klicken Sie auf **Konsole**, um die Konsole der VM zu öffnen, und melden Sie sich beim Gastbetriebssystem an.

13. Laden Sie bei Windows-basierten VMs die VirtIO-Treiber herunter bzw. aktualisieren Sie sie auf die neueste unterstützte Version wie unter Aktualisieren der VirtIO-Treiber (Windows-basierte VMs) beschrieben. (Bei Linux-basierten VMs sind die korrekten VirtIO-Treiber bereits vorhanden.)

    > **Hinweis**: Nach dem Aktualisieren der Treiber müssen Sie das Gastbetriebssystem möglicherweise neu starten.

14. Aktualisieren Sie die Netzwerkeinstellungen im Gastbetriebssystem, falls erforderlich.

Nachdem Sie bestätigt haben, dass die neue VM korrekt funktioniert, ist der Importprozess abgeschlossen. Das System fährt jedoch möglicherweise noch damit fort, Daten zwischen PMs zu synchronisieren, um den hochverfügbaren (HV) oder fehlertoleranten (FT) Betrieb zu ermöglichen.

> **Hinweis**: Die neue VM und die zugehörigen Volumes sind möglicherweise mit Warnsymbolen gekennzeichnet, bis die Daten synchronisiert wurden und die VirtIO-Treiber ausgeführt werden.

Fehlerbehebung

Verwenden Sie die folgenden Informationen, falls es beim Export- oder Importprozess zu Problemen kommt.

So räumen Sie nach einem abgebrochenen oder fehlgeschlagenen Import auf

Entfernen Sie in der ztC Console auf dem Zielsystem die importierte VM und alle zugehörigen Volumes, sofern vorhanden.

So stellen Sie fehlende Datenvolumes auf der Ziel-VM wieder her

Wenn Datenvolumes nach dem Import nicht für die VM im Zielsystem angezeigt werden, müssen Sie die Volumes wie nachstehend beschrieben manuell wiederherstellen:

- Fahren Sie die VM herunter, führen Sie den Assistenten **Virtuelle Maschine neu zuweisen** aus und überprüfen Sie, dass Sie die Volumes auf der Seite **Volumes** einbezogen haben.
- Verwenden Sie für Windows-basierte VMs die **Datenträgerverwaltung**, um Volumes in Betrieb zu nehmen.
- Bearbeiten Sie für Linux-basierte VMs die Datei `/etc/fstab`, um die neuen Gerätenamen für die Speichergeräte anzugeben. Gerätenamen können sich geändert haben, wenn Volumes nicht im Import enthalten waren.

So stellen Sie fehlende Netzwerkgeräte in der VM auf dem ztC Edge-System wieder her

Wenn Netzwerkgeräte nach dem Import nicht für die VM im Zielsystem angezeigt werden, müssen Sie sie wie nachstehend beschrieben manuell wiederherstellen:

- Fahren Sie die VM herunter, führen Sie den Assistenten **Virtuelle Maschine neu zuweisen** aus und überprüfen Sie, dass Sie die Netzwerke auf der Seite **Netzwerke** einbezogen haben. Falls die VM mehr Netzwerke als die im Assistenten aufgeführten benötigt, verbinden Sie zusätzliche Unternehmensnetzwerke mit dem ztC Edge-System und stellen Sie die VM dann erneut bereit, um die neuen Netzwerke einzuschließen.
- Bei Linux-basierten VMs konfigurieren Sie das Netzwerkstartskript neu, um die neuen Gerätenamen für die Netzwerkschnittstellen widerzuspiegeln.

So installieren Sie einen Netzwerktreiber manuell

Nach dem Import einer PM oder VM ist der Netzwerktreiber möglicherweise nicht korrekt installiert (zum Beispiel zeigt der Geräte-Manager den Treiber mit einer Warnung an, ). Installieren Sie den Treiber in diesem Fall manuell:

1. Öffnen Sie im VM-Konsolenfenster den **Geräte-Manager** in Gastbetriebssystem.
2. Erweitern Sie **Netzwerkadapter** und klicken Sie mit der rechten Maustaste auf **Red Hat VirtIO Ethernet Adapter** (der Treiber, der nicht korrekt funktioniert).
3. Wählen Sie **Treiber aktualisieren**.
4. Klicken Sie im Popupfenster auf **Auf dem Computer nach Treibersoftware suchen**.

5. Klicken Sie auf **Aus einer Liste verfügbarer Treiber auf meinem Computer auswählen**.
6. Wählen Sie **Red Hat VirtIO Ethernet Adapter**.
7. Klicken Sie auf **Weiter**, um den Netzwerktreiber zu installieren.

Nachdem der Treiber installiert wurde, überprüfen Sie den Status der VM in der ztC Console. Wenn der Status „wird ausgeführt“ ist (✔), funktioniert der Treiber korrekt.

Verwandte Themen

Bereitstellen eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners im ztC Edge-System

Erstellen und Migrieren von virtuellen Maschinen

Konfigurieren von Windows-basierten virtuellen Maschinen

Konfigurieren von Linux-basierten virtuellen Maschinen

Verwalten von VM-Ressourcen

Verwalten des Betriebs einer virtuellen Maschine

Ersetzen/Wiederherstellen einer virtuellen Maschine aus einer OVF-Datei

Ersetzen Sie eine virtuelle Maschine (VM) aus einer Datei im Open Virtualization Format (OVF), die Sie mit ztC Edge erstellt haben, wenn Sie eine VM in Ihrem ztC Edge-System wiederherstellen möchten, indem Sie die VM mit einer zuvor erstellten Sicherungskopie überschreiben. (Wenn Sie eine VM aus einem anderen System importieren möchten, lesen Sie den Überblick unter Erstellen und Migrieren von virtuellen Maschinen.)

Beim Importieren einer VM wird normalerweise eine neue Instanz der VM mit eindeutigen Hardware-IDs erstellt. Beim Wiederherstellen einer VM wird eine identische VM mit denselben Werten für SMBIOS UUID, Systemseriennummer und MAC-Adressen, falls im VM-Abbild bereitgestellt, erstellt, die das Gastbetriebssystem und Anwendungen möglicherweise für die Softwarelizenzierung benötigen. Die Hardwarekennung der wiederhergestellten VM ist jedoch eindeutig. Wenn im ztC Edge-System bereits eine identische VM vorhanden ist, können Sie die VM durch das Wiederherstellen der VM ersetzen und sie mit der vorherigen Kopie überschreiben.

Sie können eine VM, die bereits in einem ztC Edge-System vorhanden ist, nur dann wiederherstellen, wenn Sie zuvor eine VM (siehe Exportieren einer virtuellen Maschine) aus einem ztC Edge-System in OVF- und VHD-Dateien auf einer unterstützten Netzwerkfreigabe oder einem USB-Gerät exportiert haben. Kopieren Sie diese Dateien auf Ihren Verwaltungscomputer oder stellen Sie das USB-Gerät oder die Netzwerkfreigabe auf

dem ztC Edge-Zielsystem bereit wie unter Bereitstellen eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners im ztC Edge-System beschrieben und verwenden Sie dann die ztC Console auf dem ztC Edge-Zielsystem, um die OVF- und VHD-Dateien von Ihrem Verwaltungscomputer zu importieren.

Achtung: Sichern Sie die vorhandene VM im ztC Edge-System gegebenenfalls, bevor Sie sie überschreiben und wiederherstellen. Wenn Sie die VM exportieren, um die Sicherung zu erstellen, achten Sie darauf, dass Sie nicht versehentlich die OVF- und VHD-Dateien überschreiben, die Sie wiederherstellen möchten.

Hinweise:

- Sie können eine VM nur aus einer OVF-Datei wiederherstellen, die von einem ztC Edge-System erstellt wurde. Sie können eine VM nicht aus einer OVF-Datei wiederherstellen, die von einem Drittanbietersystem erstellt wurde. Es ist auch nicht möglich, eine VM aus einer OVA-Datei wiederherzustellen.
- Normalerweise stellen Sie eine VM aus einer früheren Sicherung wieder her. Bei der Wiederherstellung einer VM versucht das System, die Hardware-ID und die MAC-Adressen aller Netzwerkschnittstellen beizubehalten.
- Stellen Sie eine VM nur dann wieder her, wenn Sie eine bestimmte Instanz einer ztC Edge-VM wiederherstellen möchten und dies die einzige Kopie dieser VM auf allen ztC Edge-Servern in Ihrem Netzwerk sein wird.
- Wie lange die Wiederherstellung dauert, ist von der Größe und der Anzahl der Volumes in der Quell-VM sowie von der Netzwerkbandbreite abhängig. Das Übertragen einer VM mit einem 20-GB-Startvolume über ein 1-Gbit-Netzwerk kann zum Beispiel 30 Minuten dauern.
- Wenn Sie eine vorhandene VM überschreiben und wiederherstellen, entfernt das ztC Edge.
- Wenn das ztC Edge-System während der Wiederherstellung einer VM von der primären PM zur sekundären PM wechselt, kann der Wiederherstellungsprozess nicht abgeschlossen werden. Dies beeinträchtigt zwar nicht die kontinuierliche Betriebszeit des Systems, Sie müssen die unvollständige VM und die zugehörigen Volumes im ztC Edge-System jedoch löschen und erneut wiederherstellen.

Voraussetzungen:

- Bevor Sie ein VM-Abbild aus einem ztC Edge-System ersetzen (wiederherstellen), verwenden Sie die ztC Console auf dem ztC Edge-Quellsystem, um eine VM (siehe Exportieren einer virtuellen Maschine) in OVF- und VHD-Dateien auf einer unterstützten Netzwerkfreigabe oder auf einem USB-Gerät zu exportieren. Kopieren Sie diese Dateien auf Ihren Verwaltungscomputer oder stellen Sie das USB-Gerät oder die Netzwerkfreigabe auf dem ztC Edge-Zielsystem bereit wie unter Bereitstellen eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners im ztC Edge-System beschrieben und verwenden Sie dann die ztC Console auf dem ztC Edge-Zielsystem, um die OVF- und VHD-Dateien wiederherzustellen.
- Damit der Wiederherstellungsprozess korrekt ausgeführt werden kann, müssen beide PMs des ztC Edge-System online sein.

So stellen Sie eine VM wieder her

1. Melden Sie sich bei der ztC Console auf dem ztC Edge Zielsystem an.
2. Vergewissern Sie sich, dass auf der Seite **Physische Maschinen** (siehe Die Seite „Physische Maschinen“) eines Systems, das für zwei Knoten lizenziert ist, beide PMs den Status **wird ausgeführt** aufweisen und dass sich keine PM im Wartungsmodus oder im Prozess der Synchronisierung befindet.
3. Wenn Sie eine VM von einem USB-Gerät oder aus einer Netzwerkfreigabe importieren (statt vom PC, auf dem die ztC Console ausgeführt wird), stellen Sie das Gerät bzw. die Freigabe auf dem ztC Edge-System bereit wie unter Bereitstellen eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners im ztC Edge-System beschrieben.
4. Wählen Sie auf der Seite **Virtuelle Maschinen** (siehe Die Seite „Virtuelle Maschinen“) im oberen Fensterbereich die VM aus, die Sie wiederherstellen möchten.
5. Klicken Sie im unteren Fensterbereich auf **Wiederherstellen** oder klicken Sie auf **Importieren/Wiederherstellen** nahe des oberen Fensterbereichs.
6. Wählen Sie eine der folgenden Optionen:

- **Import von meinem PC** – Importiert die VM vom PC, auf dem die ztC Console ausgeführt wird.
    a. Klicken Sie auf **Weiter**.
    b. Klicken Sie auf **Durchsuchen** und suchen Sie den gewünschten Ordner auf einem lokalen Computer.
    c. Klicken Sie auf den Link für die gewünschte Datei.
    d. Klicken Sie auf **Öffnen**.
- **Import über USB** – Importiert die VM von einem USB-Stick, der im ztC Edge-System bereitgestellt wird.

  Klicken Sie auf **Weiter** und wählen Sie dann eine Partition aus dem Pulldownmenü aus. Klicken Sie auf **OVFs/OVAs auflisten** und wählen Sie die gewünschte OVF-Datei aus dem Pulldownmenü aus.
- **Import aus Remote-/Netzwerk-Windows-Freigabe (CIFS/SMB)** – Importiert die VM aus einer Windows-Freigabe in Ihrem lokalen Netzwerk.

  Klicken Sie auf **Weiter** und geben Sie Werte für **Benutzername** und **Kennwort** ein. Geben Sie für **Repository** einen Wert im Format ***Maschinen_URL**Freigabename*** ein (zum Beispiel **\\192.168.1.34\MeineOVFsfürExport**). Klicken Sie dann auf **OVFs/OVAs auflisten** und wählen Sie die gewünschte OVF-Datei aus der Liste aus.
- **Import aus Remote-/Netzwerk-NFS** – Importiert die VM aus einer NFS-Freigabe in Ihrem lokalen Netzwerk.

  Klicken Sie auf **Weiter** und geben Sie für **Repository** die URL des Remotesystems im Format ***nnn.nnn.nnn.nnn/ordnername*** ein (geben Sie nicht **http://** oder **https://** ein).

  Klicken Sie auf **OVFs/OVAs auflisten**, um eine Liste aller Dateien im Remoteordner zu sehen. Wählen Sie die gewünschte OVF-Datei aus. Sie können auch nach einer Datei suchen, indem Sie den Dateinamen oder einen Teil davon in das Feld *In Dateien suchen* eingeben, oder die Liste neu ordnen, indem Sie auf eine Spaltenüberschrift klicken (*Name*, *Geändert am* oder *Größe*). Klicken Sie auf den Dateinamen, um die Datei auszuwählen, und dann auf **Weiter**.

7. Wählen Sie **Wiederherstellen**. (Scrollen Sie im Fenster nach unten, falls nötig.) Es wird eine Warnung angezeigt, dass mit **Wiederherstellen** alle vorhandenen Daten und Konfigurationseinstellungen verloren gehen und dass Sie mti Vorsicht vorgehen sollen.
8. Klicken Sie auf **Weiter**, um fortzufahren.

9. Wenn Sie dazu aufgefordert werden, fügen VHD-Dateien hinzu.
10. Überprüfen Sie die Informationen und nehmen Sie bei Bedarf die gewünschten Änderungen vor:

    - **Name, Start-Schnittstelle, CPU und Arbeitsspeicher**

      Zeigt den Namen der VM, die Start-Schnittstelle, die Anzahl der vCPUs und den Gesamtarbeitsspeicher an, den die VM verwenden kann. Bearbeiten Sie die Informationen, falls nötig. (Sie können die **Start-Schnittstelle** nicht ändern; das System importiert diese Einstellung aus der OVF-Datei.)

    - **Speicher**

      Zeigt den Namen und die Größe für jedes Volume an. Wählen Sie in der Spalte **Erstellen** ein Kästchen für ein Volume aus, um Speicher für das Volume im ztC Edge System zuzuweisen (das Startvolume ist erforderlich). Wählen Sie in der Spalte **Daten wiederherstellen** ein Kästchen aus, um Daten für ein Volume aus der VHD-Datei zu importieren.

    - **Netzwerk**

      Zeigt alle verfügbaren Netzwerke an. Sie können ein Netzwerk entfernen oder ein noch nicht zugeordnetes hinzufügen. Mindestens ein Netzwerk muss immer vorhanden sein.

      Die Gesamtzahl der Netzwerke darf nicht die Anzahl der Unternehmensnetzwerke im ztC Edge-System überschreiten. Sie können im Assistenten auswählen, welche Netzwerke entfernt werden sollen. Sie können aber auch vor oder nach dem Wiederherstellen der VM weitere Unternehmensnetzwerke zum ztC Edge-System hinzufügen, um die Netzwerkverbindungen wiederherzustellen.

11. Deaktivieren Sie wahlweise das Kontrollkästchen **Virtuelle Maschine nach Wiederherstellung automatisch starten**, wenn Sie die Ressourcen der VM vor dem ersten Starten neu zuweisen möchten.
12. Klicken Sie auf **Wiederherstellen**, um mit der Wiederherstellung der VM zu beginnen. Wenn die Übertragung abgeschlossen ist, klicken Sie auf **Fertig**, um den Assistenten zu schließen.

> **Hinweis**: Wiederhergestellte Volumes werden bereits auf der Seite **Volumes** der ztC Console angezeigt, während der Wiederherstellungsprozess noch ausgeführt wird. Sie sollten keines dieser wiederhergestellten Volumes verbinden oder entfernen, bis im Wiederherstellungsfenster angezeigt wird, dass der Prozess abgeschlossen ist; andernfalls kann die Wiederherstellung nicht korrekt beendet werden.

13. Verwenden Sie ggf. den Assistenten **Virtuelle Maschine neu zuweisen**, um der VM zusätzliche Ressourcen zuzuordnen wie unter Neuzuweisen von VM-Ressourcen beschrieben.

    Klicken Sie nach dem Neuzuweisen von Ressourcen zur VM auf **Start**, um die VM neu zu starten.

Nachdem Sie bestätigt haben, dass die wiederhergestellte VM korrekt funktioniert, ist der Wiederherstellungsprozess abgeschlossen. Das ztC Edge-System fährt jedoch möglicherweise noch damit fort, Daten zwischen PMs zu synchronisieren, um den hochverfügbaren (HV) oder fehlertoleranten (FT) Betrieb zu ermöglichen.

> **Hinweis**: Die wiederhergestellte VM und die zugehörigen Volumes sind möglicherweise mit Warnsymbolen gekennzeichnet, bis die Daten synchronisiert wurden und die VirtIO-Treiber ausgeführt werden.

Fehlerbehebung

Verwenden Sie die folgenden Informationen, falls es beim Wiederherstellungsprozess zu Problemen kommt.

So räumen Sie nach einer abgebrochenen oder fehlgeschlagenen Wiederherstellung auf

Entfernen Sie in der ztC Console auf dem Zielsystem die wiederhergestellte VM und alle zugehörigen Volumes (falls vorhanden).

Verwandte Themen

Erstellen und Migrieren von virtuellen Maschinen

Verwalten von VM-Ressourcen

Verwalten des Betriebs einer virtuellen Maschine

Exportieren einer virtuellen Maschine

Exportieren Sie eine virtuelle Maschine (VM) in einem System, um ein Abbild der VM in einem im Netzwerk bereitgestellten Ordner (einem Verzeichnis) oder auf einem USB-Gerät zu speichern. Wenn Sie eine VM aus

einem ztC Edge-System exportieren, können Sie das VM-Abbild auf ein anderes System importieren oder in dasselbe ztC Edge-System importieren, um die ursprüngliche VM wiederherzustellen oder zu duplizieren. Sie können eine VM direkt aus dem ztC Edge-System exportieren wie hier beschrieben.

Bereiten Sie den Export einer VM vor, indem Sie ein USB-Gerät anschließen oder einen im Netzwerk bereitgestellten Ordner erstellen, in dem eine exportierte VM in Ihrer Umgebung gespeichert werden kann. Wenn Sie ein USB-Gerät verwenden, verbinden Sie es mit dem aktuellen primären Knoten des Systems. (Dieser wird als **Knoten*n* (primär)** auf der Seite **Physische Maschinen** angezeigt). Wenn Sie einen Ordner verwenden, erstellen Sie einen Ordner für eine Windows-Freigabe oder einen NFS-Export (Network File System). Eine Windows-Freigabe wird auch als CIFS-Freigabe bezeichnet, wobei CIFS für Common Internet File System steht (zum Beispiel Samba). Stellen Sie den Ordner oder das USB-Gerät im Hostbetriebssystem des ztC Edge-Systems bereit wie in diesem Thema beschrieben. Wenn Sie einen Export in der ztC Console einleiten, speichert das ztC Edge-System die VM als standardmäßige Dateien im Format Open Virtualization Format (OVF) und Virtual Hard Disk (VHD).

Hinweise:

- Da die Quell-VM beim Export heruntergefahren werden muss, sollten Sie vielleicht einen geplanten Wartungszeitraum für diesen Prozess in Betracht ziehen.
- Wie lange der Export dauert, ist von der Größe und der Anzahl der Volumes in der Quell-VM sowie von der Netzwerkbandbreite abhängig. Das Übertragen einer VM mit einem 20-GB-Startvolume über ein 1-Gbit-Netzwerk kann zum Beispiel 30 Minuten dauern.
- Wenn Sie die Quell-VM nach dem Export weiterhin verwenden werden, denken Sie daran, eine andere MAC-Adresse und IP-Adresse für die VM festzulegen, wenn Sie sie in das Zielsystem importieren.
- Wenn das ztC Edge-System während eines Exports von der primären PM zur sekundären PM wechselt, kann der Vorgang nicht abgeschlossen werden. Dies wirkt sich nicht auf die durchgehende Betriebszeit des Systems aus. Sie können die unvollständig exportierten Dateien aus dem im Netzwerk bereitgestellten Ordner löschen und die Dateien erneut exportieren.
- Eine vfat-Datei, die Sie exportieren, kann höchstens 4 GB groß sein. Wenn Sie versuchen, eine vfat-Datei zu exportieren, die größer als 4 GB ist, schlägt der Export fehl.
- Wenn Sie bei Linux-basierten VMs eine VM in ein anderes System exportieren, brauchen Sie die Datei `/etc/fstab` nicht zu bearbeiten.
- Bei Ubuntu-basierten VMs, die mit einigen älteren Ubuntu-Versionen laufen, müssen Sie die Datei `/boot/grub/grub.cfg` bearbeiten und den Parameter `gfxmode` zu `text` (zum Beispiel `set gfxmode=text`) ändern, bevor Sie die VM exportieren; andernfalls bleibt die Konsole der neuen VM in einem anderen System hängen. Nach der Migration können Sie die ursprüngliche Einstellung in der Quell-VM wiederherstellen.

Voraussetzungen:

- Sie müssen eine VM herunterfahren, bevor Sie sie exportieren.
- Bereiten Sie das Exportziel vor:
  - Wenn Sie ein USB-Gerät verwenden, verbinden Sie es mit dem aktuellen primären Knoten des Systems. (Dieser wird als **Knoten*n* (primär)** auf der Seite **Physische Maschinen** angezeigt). Vergewissern Sie sich, dass das System das USB-Gerät anzeigt. Öffnen Sie die Seite **Physische Maschinen**. Klicken Sie auf den Knoten, an den Sie das Gerät angeschlossen haben, und wählen Sie im unteren Fensterbereich die Registerkarte **USB-Geräte**. Das USB-Gerät, das Sie angeschlossen haben, sollte auf der Registerkarte aufgeführt werden.
  - Wenn Sie einen im Netzwerk bereitgestellten Ordner für eine Windows/CIFS-Freigabe oder einen NFS-Export verwenden, erstellen Sie einen Ordner in Ihrer Umgebung, in dem Sie die exportierte VM speichern können. Legen Sie vollständige Lese-/Schreibberechtigungen für den im Netzwerk bereitgestellten Ordner fest, um Dateiübertragungen zuzulassen. Bei einer Windows/CIFS-Freigabe können Sie die Lese-/Schreibberechtigung auch für einen bestimmten Benutzer in dem System/der Domäne, das/die die Freigabe hostet, festlegen. Notieren Sie sich die URL oder den Speicherort des NFS-Exports oder der CIFS-Freigabe sowie den Benutzernamen/das Kennwort der CIFS-Freigabe. Sie brauchen diese Angaben in einem späteren Schritt.

  Achten Sie darauf, dass genügend Speicherplatz für die zu exportierenden VMs vorhanden ist.

Zusätzlich benötigen Windows-basierte VMs eine Windows-spezifische Vorbereitung.

So bereiten Sie das Exportieren einer VM vor (nur Windows-basierte VMs)

1. Melden Sie sich mit der ztC Console beim ztC Edge-System an.
2. Wählen Sie auf der Seite **Virtuelle Maschinen** die zu exportierende VM aus.
3. Klicken Sie auf **Konsole**, um die Konsole der VM zu öffnen, und melden Sie sich beim Windows-Gastbetriebssystem an.
4. Vergewissern Sie sich, dass alle Volumes korrekt benannt sind wie unter Verwalten von Windows-Laufwerkbezeichnungen zusammengefasst.

5. Führen Sie das Windows-Systemvorbereitungstool (`Sysprep`) aus, um das Gastbetriebssystem für die Neubereitstellung vorzubereiten.

So exportieren Sie eine VM

1. Melden Sie sich mit der ztC Console beim ztC Edge-System an.
2. Wählen Sie auf der Seite **Virtuelle Maschinen** die VM aus, die Sie exportieren möchten, und klicken Sie auf **Herunterfahren**. Warten Sie, bis die VM heruntergefahren wurde. Siehe Die Seite „Virtuelle Maschinen“.
3. Während die VM ausgewählt ist, klicken Sie auf **Exportieren**, um den Exportassistenten zu öffnen.
4. Wählen Sie eine der folgenden Optionen:

   Hinweis: Wenn Sie bereits mit der Schaltfläche **Bereitstellen** einen Speicherort bereitgestellt haben (wie unter Bereitstellen eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners im ztC Edge-System beschrieben), zeigt der Export-Assistent die URL des bereitgestellten Geräts in Grün an. Klicken Sie auf die Schaltfläche **Ändern**, um die Auswahl zu ändern.

   - **Gerät über Windows-Freigabe (CIFS/SMB) bereitstellen**

     Das Ziel des Exports ist ein Ordner in einer CIFS-Freigabe. Geben Sie einen **Benutzernamen**, ein **Kennwort** und ein **Repository** ein. Geben Sie für **Repository** einen Wert im Format ***Maschinen_URL**Freigabename*** ein (zum Beispiel **\\192.168.1.34\MeineExportVMs**).

   - **Gerät über NFS bereitstellen**

     Das Exportziel ist ein Ordner auf einem Remote-System, auf den über NFS zugegriffen wird. Geben Sie einen **Repository**-Wert ein. Dies ist die URL des Remote-Systems im Format ***nnn.nnn.nnn.nnn*** (geben Sie nicht **http://** oder **https://** ein).

   - **USB bereitstellen**

     Wählen Sie für **USB-Partitionsliste** eine Partition aus dem Pulldownmenü aus.

5. Geben Sie für **Exportpfad: `/mnt/ft-export`:** den Pfad zu dem Speicherort ein, an den die VM exportiert und ihre OVF- und VHD-Dateien gespeichert werden sollen. Wenn Sie die VM

zum Beispiel in einen neuen Ordner mit dem Namen `ocean1` exportieren möchten, geben Sie `ocean1` ein.

6. Klicken Sie auf **Bereitstellen**.

   Wenn die Bereitstellung erfolgreich war, wird das Repository unter **Geräte-URL** angezeigt und die Schaltfläche **VM exportieren** wird verfügbar. Andernfalls wird ein Alarm angezeigt.

7. Wählen Sie unter **Zu exportierendes Startvolume** und **Zu exportierende Datenvolumes** die Volumes aus, die Sie einschließen möchten. (Das Startvolume ist erforderlich.)

8. Klicken Sie auf **VM exportieren**, um die VM zu exportieren.

Sie können den **Exportstatus** der VM, die Sie exportieren, auf der Registerkarte **Übersicht** überwachen. Der Fortschritt wird in Prozent (%) für den gesamten Export und für jedes Volume angezeigt. Wenn der Vorgang abgeschlossen ist, ändert sich der Status zu **Export erfolgreich abgeschlossen**.

Um den Export abzubrechen, klicken Sie auf **Abbrechen** neben der Prozentangabe des **Exportfortschritts**. Es wird ein Dialogfeld zur Bestätigung angezeigt, in dem Sie den Abbruch bestätigen können. Klicken Sie zur Bestätigung auf **Ja.**

Das ztC Edge-System exportiert zuerst die VHD-Dateien (Volumes), dann die OVF-Datei. Dass der Vorgang abgeschlossen ist, erkennen Sie daran, dass die OVF-Datei im Ordner angezeigt wird.

Wenn Sie nach dem Exportvorgang die OVF- und VHD-Dateien auf einem ztC Edge-System importieren oder wiederherstellen möchten, lesen Sie Importieren einer OVF- oder OVA-Datei.

Informationen zum Aufheben der Bereitstellung des Geräts finden Sie unter Bereitstellen eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners im ztC Edge-System.

Fehlerbehebung

Verwenden Sie die folgenden Informationen, falls es beim Exportprozess zu Problemen kommt.

So räumen Sie nach einem abgebrochenen oder fehlgeschlagenen Export aus dem ztC Edge-System auf

Entfernen Sie die VM-Dateien aus dem Exportordner oder erstellen Sie für einen späteren Export einen neuen Ordner.

Verwandte Themen

Anschließen eines USB-Geräts an eine virtuelle Maschine

Erstellen und Migrieren von virtuellen Maschinen

Verwalten von VM-Ressourcen

Verwalten des Betriebs einer virtuellen Maschine

Bereitstellen eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners im ztC Edge-System

Sie können ein USB-Gerät oder ein über das Netzwerk bereitgestellte Verzeichnis im ztC Edge-System bereitstellen (oder die Bereitstellung aufheben), indem Sie die Schaltfläche **Bereitstellen** (oder **Bereitstellung aufheben**) auf der Seite **Virtuelle Maschinen** verwenden. Wenn Sie einen Speicherort bereitstellen, ist er für den primären Knoten am Bereitstellungspunkt `/mnt/ft-export/` verfügbar. Sie können dann eine VM auf dem primären Knoten an den bereitgestellten Speicherort exportieren oder eine VM vom bereitgestesllten Speicherort in das ztC Edge-System importieren. Wenn der Export oder Import abgeschlossen ist, können Sie die Bereitstellung des Speicherorts mit der Schaltfläche **Bereitstellung aufheben** aufheben.

(Wenn Sie ein USB-Gerät bereitstellen müssen, um im Gastbetriebssystem einer VM auf das Gerät zuzugreifen, lesen Sie Anschließen eines USB-Geräts an eine virtuelle Maschine.)

Hinweise:

1. Wenn ein Speicherort verwendet wird, können Sie seine Bereitstellung nicht aufheben. Sie können zum Beispiel nicht die Bereitstellung eines Speicherortes aufheben, während eine VM exportiert oder importiert wird.
2. Die Stratus Redundant Linux-Software unterstützt auf ztC Edge-Systemen nicht das exFAT-Dateisystem. Bevor Sie einen USB-Stick bereitstsellen, formatieren Sie das Gerät mit NTFS. (Standardmäßig sind die meisten USB-Medien mit dem FAT-Dateisystem formatiert. Dieses weist eine Dateigrößenbeschränkung von 4 GB auf, was für die meisten VMs zu klein ist.)

Voraussetzung: Bereiten Sie den Bereitstellungsspeicherort vor:

- Wenn Sie ein USB-Gerät verwenden, um eine VM zu exportieren oder importieren, verbinden Sie das Gerät mit dem aktuellen primären Knoten des Systems. (Dieser wird als **Knoten*n* (primär)** auf der Seite **Physische Maschinen** angezeigt). Vergewissern Sie sich, dass das System das USB-Gerät anzeigt: Navigieren Sie zur Seite **Physische Maschinen**, klicken Sie auf den Knoten, an den Sie das Gerät angeschlossen haben, und wählen Sie im unteren Fensterbereich die Registerkarte **USB-Geräte**. Das USB-Gerät, das Sie angeschlossen haben, sollte auf der Registerkarte aufgeführt werden.
- Wenn Sie einen im Netzwerk bereitgestellten Ordner für eine Windows/CIFS-Freigabe oder einen NFS-Export verwenden, erstellen Sie einen Ordner in Ihrer Umgebung, in dem Sie die exportierte VM speichern können. Legen Sie vollständige Lese-/Schreibberechtigungen für den im Netzwerk bereitgestellten Ordner fest, um Dateiübertragungen zuzulassen. Bei einer Windows/CIFS-Freigabe können Sie die Lese-/Schreibberechtigung auch für einen bestimmten Benutzer in dem System/der Domäne, das/die die Freigabe hostet, festlegen. Notieren Sie sich die URL oder den Speicherort des NFS-Exports oder der CIFS-Freigabe sowie den Benutzernamen/das Kennwort der CIFS-Freigabe. Sie brauchen diese Angaben, wenn Sie einen NFS-Export oder eine CIFS-Freigabe bereitstellen.

So stellen Sie ein USB-Gerät oder einen über das Netzwerk bereitgestellten Ordner bereit

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine VM aus
2. Klicken Sie im unteren Fensterbereich auf die Schaltfläche **Bereitstellen**.
3. Wählen Sie für den Bereitstellungspunkt **/mnt/ft-export/** eine der folgenden Optionen:
   - **Gerät über Windows-Freigabe (CIFS/SMB) bereitstellen**

     Der Bereitstellungsort ist ein Ordner in einer CIFS-Freigabe. Geben Sie einen **Benutzernamen**, ein **Kennwort** und ein **Repository** ein. Geben Sie für **Repository** einen Wert im Format ***Maschinen_URL**Freigabename*** ein (zum Beispiel **\\192.168.1.34\MeinBereitstellungsort**).
   - **Gerät über NFS bereitstellen**

     Der Bereitstellungsort ist ein Ordner auf einem Remote-System, auf den über NFS zugegriffen wird. Für **Repository** geben Sie die URL des Remotesystems im Format ***nnn.nnn.nnn.nnn*** ein (geben Sie nicht **http://** oder **https://** ein).

- **USB bereitstellen**

  Wählen Sie für **USB-Partitionsliste** eine Partition aus dem Pulldownmenü aus.

4. Klicken Sie auf **Bereitstellen**.

Der Speicherort wird auf dem primären Knoten bereitgestellt und die Schaltfläche **Bereitstellen** ändert sich zu **Bereitstellung aufheben**.

So heben Sie die Bereitstellung eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners auf

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine VM aus
2. Klicken Sie im unteren Fensterbereich auf die Schaltfläche **Bereitstellung aufheben**.
3. Es wird ein Dialogfeld zur **Bestätigung** angezeigt, in dem Sie gefragt werden, ob Sie die Bereitstellung des Speicherorts wirklich aufheben möchten. Klicken Sie auf **Ja**, um die Bereitstellung aufzuheben.

Die Aufhebung des Speicherorts wird aufgehoben und die Schaltfläche **Bereitstellung aufheben** ändert sich zu **Bereitstellen**.

Verwandte Themen

Exportieren einer virtuellen Maschine

Verwalten von virtuellen Maschinen

Verwalten von Windows-Laufwerkbezeichnungen

Geben Sie Volumes in einer Windows-basierten virtuellen Maschine Bezeichnungen, damit sie korrekt zugeordnet werden können, bevor Sie die virtuelle Maschine exportieren.

> **Achtung**: Achten Sie darauf, dass jedes Volume eine eindeutig identifizierte Bezeichnung hat, bevor Sie **Sysprep** ausführen (zur Vorbereitung eines Exports). Für diesen Prozess benötigen Sie Administratorberechtigungen.

Um die Bezeichnung an der Eingabeaufforderung festzulegen, geben Sie Folgendes ein:

```
C:\>label C:c-drive
```

Verwenden Sie das Hilfsprogramm **diskpart**, um alle Volumebezeichnungen aufzulisten und zu überprüfen:

```
C:\> diskpart

DISKPART> list volume
```

```
...

DISKPART> exit
```

Nachdem Sie die virtuelle Maschine importiert haben, weisen Sie die Laufwerkbuchstaben mit **Datenträgerverwaltung** neu zu. Die Bezeichnungen, die Sie vor dem Export zugewiesen haben, helfen Ihnen bei der Identifizierung der Laufwerke. Anleitungen zur Neuzuweisung von Laufwerkbuchstaben in einem Windows-System finden Sie auf der Microsoft-Supportwebsite.

Verwandte Themen

Erstellen und Migrieren von virtuellen Maschinen

Konfigurieren von Windows-basierten virtuellen Maschinen

Konfigurieren von Windows-basierten virtuellen Maschinen

Nach der Installation einer Windows-basierten virtuellen Maschine konfigurieren Sie die zusätzlichen Ressourcen und die Software, die für die Verwendung in der Produktion erforderlich sind, wie in den folgenden Themen beschrieben:

- Aktualisieren der VirtIO-Treiber (Windows-basierte VMs)
- Erstellen und Initialisieren eines Datenträgers (Windows-basierte VMs)
- Installieren von Anwendungen (Windows-basierte VMs)

Achten Sie zusätzlich darauf, die folgenden Einstellungen zu konfigurieren:

- Ändern Sie die Zeitzone im Gastbetriebssystem, sodass sie der Zeitzone entspricht, die auf der Voreinstellungsseite **Datum und Uhrzeit** in der ztC Console konfiguriert wurde (siehe Konfigurieren von Datum und Uhrzeit); andernfalls ändert sich die Zeitzone der VM jedes Mal, wenn sie neu gestartet oder migriert wird. Network Time Protocol (NTP) wird sowohl für die VM als auch für das ztC Edge-System empfohlen.
- Deaktivieren Sie den Ruhezustand (in einigen Fällen standardmäßig aktiviert), um zu verhindern, dass das Gastbetriebssystem in einen energiesparenden Zustand wechselt.
- Konfigurieren Sie die Netzschalteraktion im Gastbetriebssystem so, dass der Gast heruntergefahren wird (nicht: in den Ruhezustand versetzt wird), damit die Schaltfläche **VM herunterfahren** in der ztC Console korrekt funktioniert (siehe Herunterfahren einer virtuellen Maschine).
- Konfigurieren Sie das Gastbetriebssystem so, dass bei Abstürzen eine Speicherauszugsdatei erstellt wird. Befolgen Sie die Anweisungen im Microsoft-KB-Artikel *How to generate a complete crash dump*

file or a kernel crash dump file by using an NMI on a Windows-based system (Erstellen einer vollständigen Speicherauszugsdatei oder einer Kernel-Speicherauszugsdatei mithilfe eines NMI auf Windows-Systemen, Artikel-ID 927069). Befolgen Sie die Anweisungen im Abschnitt **More Information** (Weitere Informationen).

Informationen zum Überwachen von Windows-basierten VMs in Systemen, die für eine solche Überwachung lizenziert sind, finden Sie unter Überwachen von Windows-basierten virtuellen Maschinen .

Verwandte Themen

Verwalten von virtuellen Maschinen

Aktualisieren der VirtIO-Treiber (Windows-basierte VMs)

Aktualisieren Sie die Red Hat VirtIO-Treiber auf Ihren Windows-basierten virtuellen Maschinen (VMs) auf die neuesten unterstützten Versionen, um den korrekten Betrieb der VMs sicherzustellen. Sie sollten die VirtIO-Treiber zum Beispiel aktualisieren, nachdem Sie ein Upgrade der Systemsoftware ausgeführt haben (Aktualisieren der Stratus Redundant Linux-Software) oder nachdem Sie den P2V-Client verwendet haben, um eine VM auf das ztC Edge-System zu migrieren (Migrieren einer physischen oder virtuellen Maschine in ein System).

Hinweise:

- Um den korrekten Betrieb sicherzustellen, laden Sie die VirtIO-Treiber nur von der **ztC Edge Support**-Seite herunter wie nachstehend beschrieben. Die VirtIO-ISO-Datei auf der Supportseite enthält Versionen der VirtIO-Treiber, die mit der Stratus Redundant Linux-Software auf Funktionsfähigkeit getestet wurden. VirtIO-Treiber von anderen Quellen könnten Kompatibilitätsprobleme aufweisen.
- Wenn Sie die VirtIO-Treiber aktualisieren, verwenden Sie nur die Option **Auf meinem Computer nach Treiber-Software suchen** und wählen Sie den Ordner bzw. die INF-Datei aus, der bzw. die für Ihr Gastbetriebssystem gilt. Wenn Sie die Option **Automatisch nach aktueller Treibersoftware suchen** verwenden oder nur die oberste Ebene der VirtIO VCD auswählen, installiert Windows möglicherweise einen falschen Treiber.
- In einigen Fällen fordert das das Gastbetriebssystem nachdem Aktualisieren der Treiber einen Neustart an. Starten Sie das Gastbetriebssystem in diesem Fall neu.

So aktualisieren Sie die VirtIO-Treiber auf einer Windows-basierten virtuellen Maschine

1. Laden Sie die VirtIO-ISO-Datei herunter. Sie ist verfügbar auf der Seite **Downloads** unter https://www.stratus.com/services-support/downloads/?tab=ztcedge.

    a. Klicken Sie auf der Seite **Downloads** auf **ztC Edge** (falls nicht bereits angezeigt) und wählen Sie die richtige Version aus.

    b. Scrollen Sie nach unten zu **Drivers and Tools** (Treiber und Tools) und dann weiter zu **ztC Edge VirtIO Driver Update**.

    c. Klicken Sie auf den Link für die entsprechende Datei.

    Achten Sie darauf, die Version der VirtIO-ISO-Datei herunterzuladen, die zu der Version Ihres ztC Edge-Systems passt.

2. Wenn Sie die Integrität des ISO-Abbilds überprüfen möchten, laden Sie auch die zugehörige Prüfsummendatei `fciv` herunter und dann die ausführbare Microsoft-Datei „File Checksum Integrity Verifier“ (FCIV) von der Microsoft-Supportwebsite. Speichern Sie beide Dateien in dem Verzeichnis, das die heruntergeladene ISO-Datei enthält.

    Öffnen Sie eine Eingabeaufforderung (Befehlszeile). Geben Sie in dem Verzeichnis, welches das ISO-Abbild, die ausführbare Datei und die Prüfsummendatei enthält, einen Befehl ähnlich dem folgenden ein, um das ISO-Abbild zu überprüfen:

    fciv -v -xml virtio-win-*n.n.nn*.xml

    Wenn der Befehl erfolgreich war (also die Meldung `All files verified successfully` (Alle Dateien erfolgreich verifiziert) zurückgibt), fahren Sie mit dem nächsten Schritt fort. Wenn der Befehl fehlschlägt, wiederholen Sie den Download.

3. Öffnen Sie die ztC Console, erstellen Sie eine VCD der VirtIO-ISO-Datei und legen Sie die VCD in die Windows-basierte VM ein (siehe Erstellen einer virtuellen CD und Einlegen einer virtuellen CD).

4. Öffnen Sie im VM-Konsolenfenster den **Geräte-Manager** in Gastbetriebssystem.

    Wie Sie den Geräte-Manager öffnen, ist von der Version des Gastbetriebssystems abhängig. Eine Methode besteht darin, die Systemsteuerung zu öffnen und **Geräte-Manager** auszuwählen. Sie können auch ein Suchfenster öffnen und **Geräte-Manager** eingeben.

5. Erweitern Sie **Netzwerkadapter** und suchen Sie den **Red Hat VirtIO Ethernet Adapter**. Je nach Anzahl der Netzwerkschnittstellen auf Ihrer VM sind möglicherweise mehrere Adapter vorhanden.

Wenn der **Red Hat VirtIO Ethernet Adapter** nicht aufgeführt ist, wurde der VirtIO-Treiber nicht installiert. Erweitern Sie **Weitere Geräte** und suchen Sie das unbekannte Gerät **Ethernet-Controller**. Aktualisieren Sie den Treiber für dieses Gerät.

a. Klicken Sie mit der rechten Maustaste auf den **Red Hat VirtIO Ethernet Adapter** (oder **Ethernet Controller**) und wählen Sie **Treibersoftware aktualisieren**. Klicken Sie auf **Treibersoftware auf dem Computer suchen**, geben Sie den Speicherort des VirtIO-Ethernet-Treibers (**netkvm**) für Ihr Gastbetriebssystem an und stellen Sie die Aktualisierung des Treibers fertig. (Um den Treiber zum Beispiel auf einem Windows Server 2012 R2-Gast zu aktualisieren, wählen Sie die Datei „NetKVM\2k12R2\amd64**netkvm.inf**“ auf der VirtIO-VCD.)

b. Wiederholen Sie die Treiberaktualisierung für jeden weiteren **Red Hat VirtIO Ethernet Adapter** (oder **Ethernet Controller**).

6. Erweitern Sie **Speichercontroller** und suchen Sie den **Red Hat VirtIO SCSI Controller**. Je nach Anzahl der Volumes auf Ihrer VM sind möglicherweise mehrere Controller vorhanden. Wenn der **Red Hat VirtIO SCSI Controller** nicht aufgeführt ist, wurde der VirtIO-Treiber nicht installiert. Suchen Sie das unbekannte **SCSI Controller**-Gerät und aktualisieren Sie den Treiber für dieses Gerät:

   a. Klicken Sie mit der rechten Maustaste auf den **Red Hat VirtIO SCSI**-Controller (oder **SCSI-Controller**) und wählen Sie **Treibersoftware aktualisieren**. Klicken Sie auf **Treibersoftware auf dem Computer suchen**, geben Sie den Speicherort des VirtIO-SCSI-Treibers (**viostor**) für Ihr Gastbetriebssystem an und stellen Sie die Aktualisierung des Treibers fertig. (Um den Treiber zum Beispiel auf einem Windows Server 2012 R2-Gast zu aktualisieren, geben Sie die Datei „viostor\2k12R2\amd64**viostor.inf**“ auf der VirtIO-VCD an.)

   b. Wiederholen Sie die Treiberaktualisierung für jedes weitere **Red Hat VirtIO SCSI**-Gerät (oder **SCSI-Controller**).

   Achtung: Obwohl der Gerätename der **Red Hat VirtIO SCSI**-Controller ist, müssen Sie die Speichertreiberdatei auswählen, die **viostor** benannt ist, und nicht **vioscsi** (falls vorhanden). Wenn Sie den **vioscsi**-Treiber installieren, stürzt die VM möglicherweise ab.

7. Starten Sie das Gastbetriebssystem ggf. neu, um die aktualisierten Treiber zu laden.

Verwandte Themen

Konfigurieren von Windows-basierten virtuellen Maschinen

Erstellen und Migrieren von virtuellen Maschinen

Verwalten des Betriebs einer virtuellen Maschine

Erstellen und Initialisieren eines Datenträgers (Windows-basierte VMs)

Erstellen und initialisieren Sie einen Datenträger, um ihn für die Partitionierung in Volumes in einer Windows-basierten virtuellen Maschine vorzubereiten.

So erstellen und initialisieren Sie einen Datenträger in einer Windows-basierten virtuellen Maschine

1. Verwenden Sie die ztC Console, um ein neues Volume in einer Speichergruppe im ztC Edge-System zu erstellen wie unter Erstellen eines Volumes in einer virtuellen Maschine beschrieben.
2. Öffnen Sie im Windows-Gastbetriebssystem die **Datenträgerverwaltung** oder ein ähnliches Hilfsprogramm.
3. Initialisieren Sie den neu hinzugefügten Datenträger. (Möglicherweise werden Sie automatisch dazu aufgefordert.)
4. Konvertieren Sie den Datenträger in einen dynamischen Datenträger.
5. Erstellen Sie ein oder mehrere einfache Volumes auf dem Datenträger.
6. Starten Sie das Windows-Gastbetriebssystem neu.

Vollständige Anleitungen finden Sie in Ihrer Windows-Dokumentation.

> **Hinweis**: Da die Stratus Redundant Linux-Software Daten bereits auf der physischen Ebene spiegelt, ist im Windows-Gastbetriebssystem keine Volumeredundanz erforderlich.

Verwandte Themen

Öffnen einer VM-Konsolensitzung

Konfigurieren von Windows-basierten virtuellen Maschinen

Erstellen und Migrieren von virtuellen Maschinen

Verwalten des Betriebs einer virtuellen Maschine

Installieren von Anwendungen (Windows-basierte VMs)

Führen Sie einen der folgenden Schritte aus, um eine Anwendung auf einer Windows-basierten virtuellen Maschine zu installieren:

- Laden Sie das Installationsprogramm als ausführbare Datei oder ISO-Datei in das Gastbetriebssystem herunter.
- Stellen Sie ein Netzlaufwerk bereit, welches das Installationsprogramm enthält.
- Erstellen Sie eine virtuelle CD (VCD), die das Installationsprogramm enthält, und legen Sie sie ein. Siehe Verwalten von virtuellen CDs.

Informationen zum Überwachen von Anwendungen auf Windows-basierten VMs (in Systemen, die für eine solche Überwachung lizenziert sind), finden Sie unter Überwachen von Anwendungen auf Windows-basierten virtuellen Maschinen.

Verwandte Themen

Öffnen einer VM-Konsolensitzung

Konfigurieren von Windows-basierten virtuellen Maschinen

Erstellen und Migrieren von virtuellen Maschinen

Verwalten des Betriebs einer virtuellen Maschine

Konfigurieren von Linux-basierten virtuellen Maschinen

Nach der Installation einer Linux-basierten virtuellen Maschine konfigurieren Sie die zusätzlichen Ressourcen und die Software, die für die Verwendung in der Produktion erforderlich sind, wie in den folgenden Themen beschrieben:

- Erstellen und Initialisieren eines Datenträgers (Linux-basierte VMs)
- Installieren von Anwendungen (Linux-basierte VMs)

Achten Sie zusätzlich darauf, die folgenden Einstellungen zu konfigurieren:

- Deaktivieren Sie den Ruhezustand (in einigen Fällen standardmäßig aktiviert), um zu verhindern, dass das Gastbetriebssystem in einen energiesparenden Zustand wechselt.
- Konfigurieren Sie die Netzschalteraktion im Gastbetriebssystem so, dass der Gast heruntergefahren wird (nicht: in den Ruhezustand versetzt wird), damit die Schaltfläche **VM herunterfahren** in der ztC Console korrekt funktioniert. Für die minimale Serverversion von **Ubuntu Linux** installieren Sie

wahlweise das `acpid`-Paket, um die Schaltfläche **Herunterfahren** zu aktivieren. Siehe Herunterfahren einer virtuellen Maschine.

- Installieren Sie das `kexec-tools`-Paket und konfigurieren Sie das Gastbetriebssystem so, dass ein Absturzspeicherauszug erstellt wird, wenn das System abstürzt.
- Um bei **Ubuntu Linux**-Gastbetriebssystemen ein Problem zu vermeiden, bei dem die VM-Konsole in ztC Console hängenbleibt, bearbeiten Sie die Datei `/boot/grub/grub.cfg` und ändern Sie den Parameter `gfxmode` in `text` (zum Beispiel `set gfxmode=text`). Wenn die VM-Konsole hängenbleibt, bevor Sie den Parameter sehen können, lesen Sie die Informationen zur Fehlerbehebung unter Öffnen einer VM-Konsolensitzung.

Weitere Informationen zu diesen Einstellungen finden Sie in Ihrer Linux-Dokumentation.

Verwandte Themen

Verwalten von virtuellen Maschinen

Erstellen und Initialisieren eines Datenträgers (Linux-basierte VMs)

Erstellen und initialisieren Sie einen Datenträger, um ihn für die Datenspeicherung in einer Linux-basierten virtuellen Maschine verfügbar zu machen.

So erstellen und initialisieren Sie einen Datenträger in einer Linux-basierten virtuellen Maschine

1. Erstellen Sie in der ztC Console ein neues Volume in einer Speichergruppe wie unter Erstellen eines Volumes in einer virtuellen Maschine beschrieben.
2. Verwenden Sie in der Linux-basierten virtuellen Maschine das Tool zum Verwalten von Volumes oder bearbeiten Sie Dateien, um das Volume zu initialisieren und bereitzustellen. Vollständige Anleitungen finden Sie in Ihrer Linux-Dokumentation.

Die Datenträgernamen für eine Linux-basierte virtuelle Maschine sind `/dev/vda` bis `/dev/vdh`, nicht die standardmäßigen `/dev/sda` bis `/dev/sdh`. Die virtuellen Datenträgervolumes des ztC Edge-Systems werden im Gastbetriebssystem aufgeführt und werden wie physische Datenträger verwendet.

Verwandte Themen

Öffnen einer VM-Konsolensitzung

Konfigurieren von Linux-basierten virtuellen Maschinen

Erstellen und Migrieren von virtuellen Maschinen

Verwalten des Betriebs einer virtuellen Maschine

Installieren von Anwendungen (Linux-basierte VMs)

Führen Sie einen der folgenden Schritte aus, um eine Anwendung auf einer Linux-basierten virtuellen Maschine zu installieren:

- Laden Sie das Installationspaket als ausführbare Datei oder ISO-Datei in das Gastbetriebssystem herunter.
- Stellen Sie ein Netzlaufwerk bereit, welches das Installationspaket enthält.
- Erstellen Sie eine virtuelle CD (VCD), die das Installationspaket enthält, und legen Sie sie ein. Siehe Verwalten von virtuellen CDs.

Verwandte Themen

Öffnen einer VM-Konsolensitzung

Konfigurieren von Linux-basierten virtuellen Maschinen

Erstellen und Migrieren von virtuellen Maschinen

Verwalten des Betriebs einer virtuellen Maschine

Verwalten des Betriebs einer virtuellen Maschine

Verwalten Sie den Betrieb einer virtuellen Maschine wie in diesen Themen beschrieben:

- Starten einer virtuellen Maschine
- Herunterfahren einer virtuellen Maschine
- Ausschalten einer virtuellen Maschine
- Öffnen einer VM-Konsolensitzung
- Umbenennen einer virtuellen Maschine
- Entfernen einer virtuellen Maschine

Weitere Informationen zur Konfiguration und Fehlerbehebung finden Sie unter Erweiterte Themen (virtuelle Maschinen).

Starten einer virtuellen Maschine

Starten Sie eine virtuelle Maschine (VM), um das Gastbetriebssystem der VM zu starten. Sie können auch einen Startmodus für eine VM festlegen, der verwendet wird, wenn das ztC Edge-System gestartet wird.

So starten Sie eine virtuelle Maschine

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine VM aus.
2. Klicken Sie im unteren Fensterbereich auf **Starten**.

So konfigurieren Sie einen Startmodus für eine VM, der verwendet wird, wenn das System gestartet wird

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine VM aus.
2. Klicken Sie im unteren Fensterbereich auf die Registerkarte **Starten**.
3. Wählen Sie für **Auto-Start-Modus** eine der folgenden Optionen:
    - **Zuletzt** - Setzen Sie die VM in den Zustand zurück, in dem sie beim Herunterfahren des Systems war: Wenn die VM ausgeführt wurde, wird die VM beim Starten des Systems neu gestartet; wenn die VM beendet war, wird die VM beim Starten des Systems nicht gestartet.
    - **Ein** - Startet die VM, wenn das System gestartet wird.
    - **Aus** - Startet die VM nicht, wenn das System gestartet wird.
4. Klicken Sie auf **Speichern**.

Verwandte Themen

Herunterfahren einer virtuellen Maschine

Ausschalten einer virtuellen Maschine

Verwalten des Betriebs einer virtuellen Maschine

Herunterfahren einer virtuellen Maschine

Fahren Sie eine virtuelle Maschine (VM) herunter, um das ordnungsgemäße Herunterfahren des Gastbetriebssystems einzuleiten.

Hinweis: Sie können eine VM mit Befehlen des Gastbetriebssystems herunterfahren. Einige Gastsysteme lassen es zu, dass VMs mit der ztC Console heruntergefahren werden (bzw. lassen sich konfigurieren, um dies zuzulassen).

Das Herunterfahren einer VM in der ztC Console entspricht dem Betätigen der Ein/Aus-Taste bei einer physischen Maschine, was normalerweise zum ordnungsgemäßen Herunterfahren des Betriebssystems führt. In einigen Fällen müssen Sie diese Funktion eventuell erst im Gastbetriebssystem aktivieren. Beispiel:

- Überprüfen Sie für jedes Gastsystem, dass die Aktion beim Drücken des Netzschalters so eingestellt ist, dass das Gastbetriebssystem heruntergefahren und nicht in den Ruhezustand versetzt wird. Wenn Sie für ein Gastsystem, das auf den Ruhezustand eingestellt ist, in der ztC Console auf **Herunterfahren** klicken, verbleibt die VM im Zustand **wird beendet** und wird niemals richtig heruntergefahren.
- Bei einigen Gastsystemen fährt die Ein/Aus-Taste das System nicht herunter, sofern nicht ein Benutzer beim Betriebssystem angemeldet ist. Sie können die Sicherheitseinstellungen ggf. ändern, um die Ein/Aus-Taste zu aktivieren, auch wenn keine Sitzungsanmeldung präsent ist.
- Bei einigen Minimalserverversionen von Ubuntu ist das `acpid`-Paket, das die Ein/Aus-Taste aktiviert, nicht in der Standardinstallation enthalten. Sie können dieses Paket manuell installieren, um die Ein/Aus-Taste zu aktivieren, indem Sie den folgenden Befehl eingeben (oder lesen Sie die Dokumentation zu Ihrem Gastbetriebssystem):

  ```
  sudo apt-get install acpid
  ```

  Bei Ubuntu-Versionen, die den Desktop ausführen, führt die ztC Console-Schaltfläche **Herunterfahren** dazu, dass auf dem Ubuntu-Desktop der VM drei Symbole zur Auswahl angeboten werden: Suspend, Sleep oder Shutdown. Damit die Ubuntu-VM ohne diese Desktopaufforderungen heruntergefahren werden kann, müssen Sie die Datei `powerbtn` modifizieren.

  So modifizieren Sie die Datei `powerbtn`

  1. Bearbeiten Sie auf der VM die Datei `/etc/acpi/events/powerbtn`.
  2. Diese Zeilen auskommentieren:

     ```
     event=button[ /]power
     action=/etc/acpi/powerbtn.sh
     ```

  3. Diese Zeilen hinzufügen:

     ```
     event=button/power (PWR.||PBTN)
     action==/sbin/poweroff
     ```

4. Geben Sie den folgenden Befehl ein, um `acpid` neu zu starten:

```
systemctl restart acpid
```

Informationen zur Konfiguration des Verhaltens der Ein/Aus-Taste und somit zum Aktivieren der Schaltfläche **Herunterfahren** in der ztC Console finden Sie in der Dokumentation des Gastbetriebssystems.

So fahren Sie eine VM in der ztC Console herunter

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine VM aus.
2. Klicken Sie im unteren Fensterbereich auf **Ausschalten**.

   Mit einer Meldung werden Sie aufgefordert, das Herunterfahren zu bestätigen. Klicken Sie zum Herunterfahren auf **Ja** oder klicken Sie auf **Nein**, um das Herunterfahren abzubrechen.

Falls die VM nicht reagiert, können Sie sie auch **ausschalten**, um sie ohne ordnungsgemäßes Herunterfahren des Gastbetriebssystems zu stoppen.

Verwandte Themen

Starten einer virtuellen Maschine

Ausschalten einer virtuellen Maschine

Verwalten des Betriebs einer virtuellen Maschine

Ausschalten einer virtuellen Maschine

Schalten Sie eine virtuelle Maschine (VM) aus, um sie zu beenden, ohne das Gastbetriebssystem ordnungsgemäß herunterzufahren.

> **Achtung**: Verwenden Sie den Befehl **Ausschalten** nur dann, wenn der Befehl **Herunterfahren** oder die Befehle des Gastbetriebssystems fehlschlagen. Das Ausschalten einer VM entspricht dem Abziehen des Netzsteckers und kann zu Datenverlust führen.

So schalten Sie eine virtuelle Maschine aus

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine VM aus.
2. Klicken Sie im unteren Fensterbereich auf **Ausschalten**.

Verwandte Themen

Starten einer virtuellen Maschine

Herunterfahren einer virtuellen Maschine

Verwalten des Betriebs einer virtuellen Maschine

Erweiterte Themen (virtuelle Maschinen)

Öffnen einer VM-Konsolensitzung

Öffnen Sie eine Konsolensitzung für eine virtuelle Maschine (VM), um die Konsole des Gastbetriebssystems anzuzeigen, das auf der VM ausgeführt wird.

Nachstehend wird beschrieben, wie Sie eine VM-Konsolensitzung in der ztC Console öffnen, Sie können zu diesem Zweck aber auch eine Remotedesktopanwendung verwenden.

So öffnen Sie eine VM-Konsolensitzung

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine VM aus.
2. Vergewissern Sie sich, dass die VM ausgeführt wird.
3. Klicken Sie im unteren Fensterbereich auf **Konsole** ().

> **Hinweis**:
> Nachdem Sie auf **Konsole** geklickt haben, wird eventuell eine leere Konsolensitzung geöffnet, falls der Browser über HTTPS mit dem System verbunden ist, aber keine entsprechende Sicherheitsausnahme festgelegt wurde. Klicken Sie in diesem Fall auf die IP-Adresse oben rechts im Sitzungsfenster. Diese IP-Adresse, die das Format https://*IP_Adresse_des_Systems*:8000 hat, fügt die IP-Adresse des Systems als Sicherheitsausnahme im Browser hinzu. Die Sicherheitsausnahme ermöglicht es dem Browser, die Site zu öffnen.
>
> Je nach Browser werden möglicherweise weitere Sicherheitsfenster oder -meldungen eingeblendet. Bei einigen Browsern werden lediglich Sicherheitsmeldungen angezeigt, die Sie mit einem Klick schließen können. Bei anderen Browsern wird die Adressleiste rot eingefärbt, ohne dass eine Meldung angezeigt wird, und Sie müssen auf die Adresse klicken, um fortzufahren. Dies sind einige spezifische Beispiele:

- Wenn **Zertifikatfehler** in der Adressleiste angezeigt wird, müssen Sie (1) auf die Adresse klicken; (2) auf einer Seite mit der Meldung **Die Webseite kann nicht angezeigt werden** auf **Weitere Informationen** klicken und dann (3) auf einer Seite mit der Meldung **Diese Website ist nicht sicher** auf **Webseite trotzdem laden (nicht empfohlen)** klicken.
- Wenn die Seite **Warnung: Mögliches Sicherheitsrisiko erkannt** angezeigt wird, klicken Sie auf **Erweitert** und im nächsten Fenster auf **Risiko akzeptieren und fortfahren**.
- Wenn ein **Fehler** mit **Fehlercode 405** angezeigt wird, schließen Sie das Fenster oder den Tab.

Diese Sicherheitsausnahme gilt dann für alle VMs. Sie müssen diese Schritte in jedem Browser nur einmal ausführen. Wenn Sie danach auf **Konsole** klicken, wird die Konsolensitzung für die VM erfolgreich geöffnet.

Nachdem Sie die Konsolensitzung geöffnet haben, können Sie die Größe des Browserfensters und der VM-Konsolensitzung ändern. Sie können auch Tastaturbefehle verwenden.

So ändern Sie die Größe des Browserfensters und der VM-Sitzung

1. Öffnen Sie die VM-Konsolensitzung (wie oben beschrieben).

   Am linken Rand des Fensters werden Symbole angezeigt. Um die Symbole anzuzeigen, müssen Sie möglicherweise auf den Pfeil auf der Registerkarte am linken Fensterrand klicken.

2. Um das Browserfenster im Vollbild anzuzeigen, klicken Sie auf das entsprechende Symbol ( ).

   Wenn Sie im Vollbildmodus erneut auf das Vollbild-Symbol ( ) klicken, wird das Browserfenster kleiner angezeigt.

3. Um die Größe der VM-Sitzung innerhalb des Browserfensters zu ändern, klicken Sie auf das Symbol für die Einstellungen ( ) und wählen Sie einen **Skalierungsmodus** (klicken Sie auf den aktuellen Modus, um ein Pulldownmenü mit weiteren Einstellungen zu öffnen):

   - **Remote-Größenänderung** (Standardeinstellung) - Die Größe der VM-Sitzung ändert sich, wenn Sie die Auflösung des Gast-Betriebssystems ändern.

- **Lokale Skalierung** - Die Größe der VM-Sitzung ändert sich automatisch, um mit dem ursprünglichen Seitenverhältnis den Bildschirm auszufüllen.

So verwenden Sie Tastaturbefehle

1. Öffnen Sie die VM-Konsolensitzung (wie oben beschrieben).
2. Klicken Sie auf das Symbol **A** () am linken Fensterrand, um die Symbole für die Auswahl der Tastaturbefehle einzublenden.
3. Es werden die folgenden Symbol angezeigt:
   -  - Klicken, um die Funktion der **Strg**-Taste zu verwenden.
   -  - Klicken, um die Funktion der **Alt**-Taste zu verwenden.
   -  - Klicken, um die Funktion der **Tab**-Taste zu verwenden.
   -  - Klicken, um die Funktion der **Esc**-Taste zu verwenden.
   -  - Klicken, um die Funktion der Tasten **Strg**+**Alt**+**Entf** zu verwenden.

Fehlerbehebung

So lösen Sie das Problem, wenn sich das VM-Konsolenfenster nicht öffnet

Lassen Sie von Ihrem Netzwerkadministrator die Ports 6900 bis einschließlich 6999 öffnen.

So lösen Sie das Problem, wenn das VM-Konsolenfenster leer ist

Vergewissern Sie sich, dass die VM eingeschaltet ist und der Startvorgang abgeschlossen wurde. Klicken Sie im Konsolenfenster und drücken Sie eine beliebige Taste, um den Bildschirmschoner zu deaktivieren.

So lösen Sie das Problem, wenn mehrere VM-Konsolenfenster angezeigt werden und sich nicht wie erwartet verhalten

Schließen Sie alle Konsolenfenster und öffnen Sie nur ein Konsolenfenster.

So beheben Sie das Problem, wenn das VM-Konsolenfenster im ztC Edge-System hängenbleibt

Bei Ubuntu-basierten VMs bleibt das VM-Konsolenfenster in der ztC Console hängen, wenn Sie den Parameter `gfxmode` nicht richtig eingestellt haben. Bearbeiten Sie im Gastbetriebssystem die Datei

`/boot/grub/grub.cfg` und ändern Sie den `gfxmode`-Parameter zu `text` (zum Beispiel `set gfxmode=text`).

Falls die Konsole abstürzt, bevor Sie den Parameter sehen können, führen Sie Folgendes aus:

1. Starten Sie die VM in der ztC Console neu.
2. Drücken Sie im GRUB-Menü auf `e`, um den grub-Befehl zu bearbeiten.
3. Ändern Sie im nächsten Bildschirm in der Zeile `gfxmode` den Eintrag `$linux_gfx_mode` zu `text`, sodass die Zeile nun so aussieht:

   ```
   gfxmode text
   ```

4. Drücken Sie **Strg-X** oder **F10**, um das Gastbetriebssystem zu starten.
5. Um die Einstellung zu aktualisieren, damit sie für jeden Startvorgang verwendet wird, bearbeiten Sie die Datei `/boot/grub/grub.cfg` und ändern Sie den `gfxmode`-Parameter zu `text`, sodass die Zeile nun so aussieht:

   ```
   set gfxmode=text
   ```

6. Speichern Sie die Datei `/boot/grub/grub.cfg`.

So ändern Sie den Terminaltyp bei einer Linux-basierten VM, wenn der Konsolenbildschirm nicht lesbar ist

Linux setzt die `TERM`-Variable standardmäßig auf `vt100-nav`. Dies wird aber vom Programm `vncterm`, der Grundlage der VM-Konsole in der ztC Console, nicht richtig unterstützt. Der Bildschirm wird unlesbar, wenn Sie eine andere Funktion als die Befehlszeile verwenden. Um dieses Problem zu beheben, ändern Sie den Terminaltyp im Linux-Gastbetriebssystem:

1. Öffnen Sie die Datei `inittab` im Gastbetriebssystem.
2. Ersetzen Sie in der folgenden Zeile `vt100-nav` durch `vt100`. Löschen Sie dazu `-nav` am Ende der Zeile. Die geänderte Zeile sieht folgendermaßen aus:

   ```
   # Run gettys in standard runlevels co:2345:respawn:/sbin/agetty xvc0
   9600 vt100
   ```

3. Speichern Sie die Datei **inittab**.

Verwandte Themen

Starten einer virtuellen Maschine

Herunterfahren einer virtuellen Maschine

Verwalten des Betriebs einer virtuellen Maschine

Umbenennen einer virtuellen Maschine

Sie können eine virtuelle Maschine (VM) umbenennen, damit sie auf der Seite **Virtuelle Maschinen** mit einem anderen Namen angezeigt wird.

Wenn Sie den Hostnamen des Gastbetriebssystems, das auf einer VM ausgeführt wird, ändern möchten, verwenden Sie dazu die Tools des Gastbetriebssystems.

Voraussetzung: Um eine VM umzubenennen, müssen Sie sie herunterfahren.

So benennen Sie eine virtuelle Maschine um

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine VM aus.
2. Klicken Sie auf **Herunterfahren** und warten Sie, bis die VM heruntergefahren wurde.
3. Doppelklicken Sie auf den Namen der VM.
4. Geben Sie den neuen Namen ein. Der Name der VM muss die folgenden Anforderungen erfüllen:
    - Ein VM-Name muss mit einem Wort oder einer Zahl beginnen, und der Name darf keine Sonderzeichen enthalten (zum Beispiel #, % oder $).
    - Ein VM-Name darf keinen Präfix mit Bindestrich enthalten, zum Beispiel Zombie- oder migrieren-.
    - Ein VM-Name darf höchstens 85 Zeichen enthalten.
5. Drücken Sie die **Eingabetaste**.

Verwandte Themen

Entfernen einer virtuellen Maschine

Erstellen und Migrieren von virtuellen Maschinen

Verwalten des Betriebs einer virtuellen Maschine

Entfernen einer virtuellen Maschine

Entfernen Sie eine virtuelle Maschine (VM), um sie dauerhaft zu löschen und optional die mit ihr verknüpften Volumes aus dem ztC Edge-System zu löschen.

> **Voraussetzung**: Beide PMs des ztC Edge-Systems müssen online sein, damit eine VM entfernt werden kann. Vergewissern Sie sich, dass auf der Seite **Physische Maschinen** der ztC Console beide PMs den Status **wird ausgeführt** aufweisen und dass sich keine PM im Wartungsmodus oder im Prozess der Synchronisierung befindet.

So entfernen Sie eine virtuelle Maschine

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine VM aus.
2. Klicken Sie im unteren Fensterbereich auf **Ausschalten**.
3. Wenn die VM gestoppt wurde, klicken Sie auf **Entfernen**.
4. Aktivieren Sie im Dialogfeld **Virtuelle Maschine entfernen** das Kontrollkästchen neben den Volumes, die Sie löschen möchten. Lassen Sie Kontrollkästchen leer, wenn Sie die entsprechenden Volumes als Archiv behalten oder für die Verbindung mit einer anderen VM aufheben möchten.

   > **Achtung**: Vergewissern Sie sich, dass Sie die richtige VM und die richtigen Volumes zum Entfernen ausgewählt haben. Wenn Sie auf **VM löschen** klicken, werden diese Objekte unwiderruflich entfernt.

5. Klicken Sie auf **VM löschen**, um die VM und alle ausgewählten Volumes dauerhaft zu löschen.

Verwandte Themen

Umbenennen einer virtuellen Maschine

Erstellen und Migrieren von virtuellen Maschinen

Verwalten des Betriebs einer virtuellen Maschine

Verwalten von VM-Ressourcen

Verwalten Sie VM-Ressourcen, um die vCPUs, den Arbeitsspeicher, den Speicher oder die Netzwerkressourcen einer vorhandenen virtuellen Maschine neu zu konfigurieren.

Zum Neukonfigurieren von VM-Ressourcen verwenden Sie den Assistenten **Virtuelle Maschine neu zuweisen** wie in diesem Thema beschrieben:

- Neuzuweisen von VM-Ressourcen

Informationen zur Neukonfiguration der Volumes von virtuellen Maschinen finden Sie in diesen aufgabenspezifischen Themen:

- Erstellen eines Volumes in einer virtuellen Maschine
- Verbinden eines Volumes mit einer virtuellen Maschine
- Trennen eines Volumes von einer virtuellen Maschine
- Entfernen eines Volumes von einer virtuellen Maschine
- Erweitern eines Volumes im ztC Edge-System

Informationen zum Wiederherstellen von VM-Ressourcen, Freigeben von Speicher für neue Volumes oder virtuelle CDs finden Sie hier:

- Wiederherstellen von VM-Ressourcen

Neuzuweisen von VM-Ressourcen

Sie können die Zuweisung von virtuellen CPUs (vCPUs), Arbeitsspeicher, Speicher oder Netzwerkressourcen zu einer virtuellen Maschine (VM) ändern; dieser Vorgang wird auch „Reprovisioning“ genannt.

Starten Sie den Assistenten **Virtuelle Maschine neu zuweisen**, indem Sie im unteren Fensterbereich der Seite **Virtuelle Maschinen** auf **Konfig** klicken. Der Assistent führt Sie durch den Prozess zum Neuzuweisen von Ressourcen zur VM.

Voraussetzungen: Neuzuweisen von VM-Ressourcen

- Überprüfen Sie die Voraussetzungen und Überlegungen zum Zuweisen von vCPUs, Arbeitsspeicher, Speicher und Netzwerkressourcen zur VM wie unter Planen von VM-Ressourcen aufgeführt. Weitere Informationen zu Speicherressourcen finden Sie unter Planen von VM-Speicher.
- Um die Ressourcen einer VM neu zuzuweisen, müssen Sie die VM herunterfahren.

So ändern Sie die Zuweisung einer virtuellen Maschine

1. Öffnen Sie die Seite **Virtuelle Maschinen** (siehe Die Seite „Virtuelle Maschinen“).
2. Wählen Sie eine VM aus und klicken Sie auf **Herunterfahren**.

3. Wenn die VM beendet wurde, klicken Sie auf **Konfig**, um den Assistenten **Virtuelle Maschine neu zuweisen** anzuzeigen.
4. Auf der Seite **Name und Beschreibung Name, Beschreibung und Schutz**:
    a. Geben Sie den **Namen** und optional die **Beschreibung** für die VM ein, wie sie in der ztC Console erscheinen sollen.

    Der Name der VM muss die folgenden Anforderungen erfüllen:

    - Ein VM-Name muss mit einem Wort oder einer Zahl beginnen, und der Name darf keine Sonderzeichen enthalten (zum Beispiel #, % oder $).
    - Ein VM-Name darf keinen Präfix mit Bindestrich enthalten, zum Beispiel Zombie- oder migrieren-.
    - Ein VM-Name darf höchstens 85 Zeichen enthalten.

    b. Wählen Sie die Schutzstufe für die VM:

    - **Fehlertolerant (FT)**
    - **Hochverfügbar (HV)**

    Informationen über diese Schutzlevel finden Sie unter Erstellen einer neuen virtuellen Maschine und Betriebsmodi.

    c. Klicken Sie auf **Weiter**.
5. Auf der Seite **vCPUs und Arbeitsspeicher**:
    a. Geben Sie die Anzahl der **vCPUs** und die Größe des **Arbeitsspeichers** an, welcher der VM zugewiesen werden soll. Weitere Informationen finden Sie unter Planen von VM-vCPUs und Planen von VM-Arbeitsspeicher.

    b. Klicken Sie auf **Weiter**.
6. Auf der Seite **Volumes**:

> **Hinweis**:
> Sie können nicht das VM-Startvolume ändern, sondern nur Datenvolumes. Sie können das Startvolume jedoch trennen.

- Klicken Sie auf **Startvolume**, um das Startvolume zu trennen.

  Achtung: Wenn Sie das Startvolume trennen, kann die VM nicht gestartet werden.

  Es wird eine entsprechende Warnung angezeigt. Wenn Sie das Trennen des Startvolumes rückgängig machen wollen, klicken Sie auf **Trennen rückgängig machen**.

- Klicken Sie auf **Trennen**, um ein Volume von einer VM zu trennen und zur späteren Verwendung zu behalten.
- Klicken Sie auf **Löschen**, um ein Volume dauerhaft aus dem ztC Edge-System zu entfernen.
- Wählen Sie ein nicht verbundenes Volume aus dem Pulldownmenü (falls es angezeigt wird) und klicken Sie auf **Verbinden**.

  Sie können ggf. auch auf **Neues Volume hinzufügen** klicken, um ein neues Datenvolume zu erstellen. (Falls Sie diese Schaltfläche nicht sehen, führen Sie einen Bildlauf zum unteren Rand der Assistentenseite durch.)

  Geben Sie für ein nicht angeschlossenes Volume oder ein neues Volume die Parameter des Volumes an:

  a. Geben Sie den **Namen** des Volumes ein.

  b. Geben Sie die **Volumegröße** des Volumes in Gigabytes (GB) an. Weitere Informationen zum Zuordnen von Speicher finden Sie unter und Planen von VM-Speicher.

  c. Klicken Sie ggf. auf **Anschließen**, um ein Volume an eine VM anzuschließen.

Klicken Sie zum Fortfahren auf **Weiter**.

7. Aktivieren Sie auf der Seite **Netzwerke** das Kontrollkästchen für jedes gemeinsame Netzwerk, das Sie an die VM anhängen möchten.

   Für jedes gemeinsame Netzwerk, das Sie anhängen, können Sie optional

   - Legen Sie eine benutzerdefinierte MAC-Adresse fest (siehe Zuweisen einer spezifischen MAC-Adresse zu einer virtuellen Maschine).
   - den **Zustand** auf **Aktiviert** oder **Deaktiviert** setzen, wodurch Sie Netzwerkdatenverkehr zum ausgewählten Netzwerk zulassen oder blockieren können

   Weitere Informationen finden Sie unter Planen von VM-Netzwerken. Klicken Sie zum Fortfahren auf **Weiter**.

8. Auf der Seite **Konfigurationsübersicht**:

   Achtung: Vergewissern Sie sich, dass Sie die richtigen Volumes zum Entfernen gekennzeichnet haben. Wenn Sie auf **Fertigstellen** klicken, gehen die Daten auf den zum Entfernen markierten Volumes dauerhaft verloren.

   a. Überprüfen Sie die Angaben in der Konfigurationsübersicht. Klicken Sie auf **Zurück**, falls Sie Änderungen vornehmen müssen.

   b. Um die Zuweisung der VMs zu bestätigen, klicken Sie auf **Fertigstellen**.

9. Klicken Sie auf **Start**, um die VM neu zu starten.

10. Wenn Sie bei Windows-basierten VMs die Anzahl der zugewiesenen virtuellen CPUs von 1 zu *n* oder von *n* zu 1 ändern, müssen Sie nach dem Neustarten der VM am Ende der Neuzuweisung die VM ein zweites Mal herunterfahren und neu starten. Dadurch kann sich die VM selbst für symmetrisches Multiprocessing (SMP) neu konfigurieren. Die VM verhält sich unerwartet und kann nicht verwendet werden, bis sie neu gestartet wurde.

Verwandte Themen

Verwalten von VM-Ressourcen

Planen von VM-Ressourcen

Verwalten von virtuellen Maschinen

Erstellen eines Volumes in einer virtuellen Maschine

Erstellen Sie ein Volume, um eine virtuelle Maschine (VM) mit einem neuen, leeren Volume zu verbinden. (Sie können auch ein vorhandenes, nicht verbundenes Volume verbinden wie unter Verbinden eines Volumes mit einer virtuellen Maschine beschrieben.)

Voraussetzung: Vor dem Erstellen eines Volumes für eine VM müssen Sie die VM herunterfahren.

So erstellen Sie ein neues Volume in einer VM

1. Öffnen Sie die Seite **Virtuelle Maschinen** (siehe Die Seite „Virtuelle Maschinen“).

2. Wählen Sie eine VM aus und klicken Sie auf **Herunterfahren**.

3. Wenn die VM beendet wurde, klicken Sie auf **Konfig**, um den Assistenten **Virtuelle Maschine neu zuweisen** anzuzeigen.
4. Klicken Sie auf jeder Seite des Assistenten auf **Weiter**, bis die Seite **Volumes** angezeigt wird. (Lesen Sie ggf. Neuzuweisen von VM-Ressourcen, um weitere VM-Ressourcen zu konfigurieren.)
5. Klicken Sie auf der Seite **Volumes** auf **Neues Volume hinzufügen**. (Falls Sie diese Schaltfläche nicht sehen, führen Sie einen Bildlauf zum unteren Rand der Assistentenseite durch.)
6. Führen Sie unter **Zu erstellen** Folgendes aus:
    a. Geben Sie den **Namen** des Volumes ein, wie er in der ztC Console erscheinen soll.
    b. Geben Sie die **Volumegröße** des zu erstellenden Volumes in Gigabytes (GB) an. Weitere Informationen zum Zuordnen von Speicher finden Sie unter und Planen von VM-Speicher.
7. Klicken Sie auf jeder Seite des Assistenten auf **Weiter**, bis die Seite **Konfigurationsübersicht** angezeigt wird. Überprüfen Sie die Konfigurationsänderungen.
8. Klicken Sie auf **Fertigstellen**, um das Volume zu erstellen.
9. Starten Sie die VM und bereiten Sie das Volume für die Verwendung im Gastbetriebssystem vor wie in den folgenden Themen beschrieben:
    - Erstellen und Initialisieren eines Datenträgers (Windows-basierte VMs)
    - Erstellen und Initialisieren eines Datenträgers (Linux-basierte VMs)

Verwandte Themen

Trennen eines Volumes von einer virtuellen Maschine

Entfernen eines Volumes von einer virtuellen Maschine

Verwalten von VM-Ressourcen

Planen von VM-Ressourcen

Verwalten von virtuellen Maschinen

Verbinden eines Volumes mit einer virtuellen Maschine

Verbinden Sie ein Volume, um ein zurzeit nicht genutztes Volumes mit einer virtuellen Maschine zu verbinden.

Hinweis: Wenn Sie ein Startvolume mit einer VM verbinden, die bereits ein Startvolume hat, wird das neu hinzugefügte Volume als Datenvolume verbunden. Sie können ein Volume auf diese Weise verbinden, um ein Startproblem oder Datenschäden im Startvolume einer anderen VM zu diagnostizieren. Nachdem Sie das Problem mit den Tools des Gastbetriebssystems behoben haben, trennen Sie das Volume und verbinden es dann wieder mit der ursprünglichen VM.

Voraussetzung: Bevor Sie ein Volume mit einer virtuellen Maschine verbinden, müssen Sie die virtuelle Maschine herunterfahren.

So verbinden Sie ein Volume mit einer virtuellen Maschine

1. Stellen Sie sicher, dass das Volume, das Sie verbinden möchten, nicht von einer anderen virtuellen Maschine verwendet wird; andernfalls können Sie es nicht verbinden. Öffnen Sie die Seite **Volumes**, suchen Sie das Volume und stellen Sie sicher, dass in der Spalte **Verwendet von** der Wert **Keine** angezeigt wird.
2. Öffnen Sie die Seite **Virtuelle Maschinen** (siehe Die Seite „Virtuelle Maschinen“).
3. Wählen Sie eine VM aus und klicken Sie auf **Herunterfahren**.
4. Wenn die VM beendet wurde, klicken Sie auf **Konfig**, um den Assistenten **Virtuelle Maschine neu zuweisen** anzuzeigen.
5. Klicken Sie auf jeder Seite des Assistenten auf **Weiter**, bis die Seite **Volumes** angezeigt wird. (Lesen Sie ggf. Neuzuweisen von VM-Ressourcen, um weitere VM-Ressourcen zu konfigurieren.)
6. Suchen Sie auf der Seite **Volumes** das Pulldownmenü neben der Schaltfläche **Neues Volume hinzufügen**. Wählen Sie ein nicht verbundenes Volume aus dem Pulldownmenü und klicken Sie auf **Verbinden**.

   (Falls Sie das Pulldownmenü nicht sehen, führen Sie einen Bildlauf zum unteren Rand der Assistentenseite durch. Das Pulldownmenü wird nur dann angezeigt, wenn es nicht verbundene Volumes im ztC Edge-System gibt.)
7. Klicken Sie auf jeder Seite des Assistenten auf **Weiter**, bis die Seite **Konfigurationsübersicht** angezeigt wird. Überprüfen Sie die Konfigurationsänderungen.
8. Klicken Sie auf **Fertigstellen**, um das ausgewählte Volume zu verbinden.

Verwandte Themen

Erstellen eines Volumes in einer virtuellen Maschine

Trennen eines Volumes von einer virtuellen Maschine

Entfernen eines Volumes von einer virtuellen Maschine

Verwalten von VM-Ressourcen

Planen von VM-Ressourcen

Verwalten von virtuellen Maschinen

Trennen eines Volumes von einer virtuellen Maschine

Trennen Sie ein Volume von einer virtuellen Maschine und behalten Sie es zur späteren Verwendung oder verbinden Sie es mit einer anderen virtuellen Maschine wie unter Verbinden eines Volumes mit einer virtuellen Maschine beschrieben. (Sie können das Volume auch dauerhaft aus dem ztC Edge-System löschen wie unter Entfernen eines Volumes von einer virtuellen Maschine beschrieben.)

Hinweis: Wenn Sie ein Startvolume von einer VM trennen, können Sie die VM nicht starten; Sie können das Startvolume jedoch trennen, um ein Startproblem oder Datenbeschädigungen im Volume zu untersuchen. Sie können das Startvolume dazu als Datenvolume mit einer anderen VM verbinden wie unter Verbinden eines Volumes mit einer virtuellen Maschine beschrieben. Nachdem Sie das Problem mit den Tools des Gastbetriebssystems behoben haben, trennen Sie das Volume und verbinden es dann wieder mit der ursprünglichen VM.

Voraussetzung: Bevor Sie ein Volume von einer virtuellen Maschine trennen, müssen Sie die virtuelle Maschine herunterfahren.

So trennen Sie ein Volume von einer virtuellen Maschine

1. Öffnen Sie die Seite **Virtuelle Maschinen** (siehe Die Seite „Virtuelle Maschinen“).
2. Wählen Sie eine VM aus und klicken Sie auf **Herunterfahren**.
3. Wenn die VM beendet wurde, klicken Sie auf **Konfig**, um den Assistenten **Virtuelle Maschine neu zuweisen** anzuzeigen.
4. Klicken Sie auf jeder Seite des Assistenten auf **Weiter**, bis die Seite **Volumes** angezeigt wird. (Lesen Sie ggf. Neuzuweisen von VM-Ressourcen, um weitere VM-Ressourcen zu konfigurieren.)

5. Suchen Sie auf der Seite **Volumes** das Volume, das Sie trennen möchten. (Wenn das Volume nicht sichtbar ist, führen Sie einen Bildlauf zum unteren Rand der Assistentenseite aus.)
6. Klicken Sie neben dem Volumenamen auf **Trennen**, um das Volume für das Trennen zu markieren.

   Achtung: Achten Sie darauf, das richtige Volume zum Trennen zu markieren, damit nicht versehentlich ein zurzeit verwendetes Volume gekennzeichnet wird.
7. Klicken Sie auf jeder Seite des Assistenten auf **Weiter**, bis die Seite **Konfigurationsübersicht** angezeigt wird. Überprüfen Sie die Konfigurationsänderungen.
8. Klicken Sie auf **Fertigstellen**, um das ausgewählte Volume zu trennen.

Verwandte Themen

Verbinden eines Volumes mit einer virtuellen Maschine

Entfernen eines Volumes von einer virtuellen Maschine

Verwalten von VM-Ressourcen

Planen von VM-Ressourcen

Verwalten von virtuellen Maschinen

Entfernen eines Volumes von einer virtuellen Maschine

Entfernen Sie ein VM-Volume, um es dauerhaft aus dem ztC Edge-System zu löschen. (Sie können ein Volume auch von der VM trennen, es aber zur späteren Verwendung behalten wie unter Trennen eines Volumes von einer virtuellen Maschine beschrieben.)

Voraussetzung: Bevor Sie ein mit einer virtuellen Maschine verbundenes Volume entfernen, müssen Sie die virtuelle Maschine herunterfahren.

So entfernen Sie ein Volume, das mit einer virtuellen Maschine verbunden ist

1. Öffnen Sie die Seite **Virtuelle Maschinen** (siehe Die Seite „Virtuelle Maschinen“).
2. Wählen Sie eine VM aus und klicken Sie auf **Herunterfahren**.
3. Wenn die VM beendet wurde, klicken Sie auf **Konfig**, um den Assistenten **Virtuelle Maschine neu zuweisen** anzuzeigen.

4. Klicken Sie auf jeder Seite des Assistenten auf **Weiter**, bis die Seite **Volumes** angezeigt wird. (Lesen Sie ggf. Neuzuweisen von VM-Ressourcen, um weitere VM-Ressourcen zu konfigurieren.)
5. Suchen Sie auf der Seite **Volumes** das Volume, das Sie löschen möchten. (Wenn das Volume nicht sichtbar ist, führen Sie einen Bildlauf zum unteren Rand der Assistentenseite aus.)
6. Klicken Sie neben dem Volumenamen auf **Löschen**, um das Volume für das Löschen zu markieren.

   Achtung: Achten Sie darauf, das richtige Volume zum Löschen zu markieren, damit nicht versehentlich ein zurzeit verwendetes Volume gekennzeichnet wird.
7. Klicken Sie auf jeder Seite des Assistenten auf **Weiter**, bis die Seite **Konfigurationsübersicht** angezeigt wird. Überprüfen Sie die Konfigurationsänderungen.
8. Klicken Sie auf **Fertigstellen**, um das ausgewählte Volume dauerhaft zu löschen.

So entfernen Sie ein nicht verbundenes Volume

Achtung: Bevor Sie ein Volume entfernen, vergewissern Sie sich, dass es nicht mehr von anderen Administratoren benötigt wird.

1. Öffnen Sie die Seite **Volumes**.
2. Wählen Sie ein nicht verbundenes Volume aus. (Der Wert in der Spalte **Verwendet von** muss ***Keine*** lauten, andernfalls wird die Schaltfläche **Entfernen** nicht angezeigt.)
3. Klicken Sie auf **Entfernen**.

Verwandte Themen

Trennen eines Volumes von einer virtuellen Maschine

Verbinden eines Volumes mit einer virtuellen Maschine

Verwalten von VM-Ressourcen

Planen von VM-Ressourcen

Verwalten von virtuellen Maschinen

Umbenennen eines Volumes im ztC Edge-System

Sie können ein Volume im ztC Edge-System umbenennen, damit es auf der Seite **Volumes** mit einem anderen Namen angezeigt wird.

Wenn Sie den Namen eines Datenträgers oder Volumes im Gastbetriebssystem, das auf einer virtuellen Maschine ausgeführt wird, ändern möchten, verwenden Sie dazu die Tools des Gastbetriebssystems.

So benennen Sie ein Volume im ztC Edge-System um

1. Suchen Sie das Volume auf der Seite **Volumes**.
2. Doppelklicken Sie auf den Namen des Volumes.
3. Geben Sie den neuen Namen ein und drücken Sie die **Eingabetaste**.

Verwandte Themen

Erstellen eines Volumes in einer virtuellen Maschine

Trennen eines Volumes von einer virtuellen Maschine

Entfernen eines Volumes von einer virtuellen Maschine

Verwalten von VM-Ressourcen

Planen von VM-Ressourcen

Verwalten von virtuellen Maschinen

Erweitern eines Volumes im ztC Edge-System

Erweitern Sie das Volume einer virtuellen Maschine (VM), um mehr Speicherplatz für Programme und Daten im Gastbetriebssystem zuzuordnen.

Sie können ein Volume vergrößern, aber nicht verkleinern. Verwenden Sie das folgende Verfahren zum Erweitern eines Volumes nur dann, wenn die VM gestoppt wurde.

Voraussetzungen:

- Sie müssen die VM herunterfahren, bevor Sie ein darin enthaltenes Volume erweitern.
- Stellen Sie sicher, dass beide PMs des ztC Edge-Systems online sind, andernfalls kann das System das Volume nicht richtig erweitern.

So erweitern Sie ein Volume

1. Vergewissern Sie sich, dass auf der Seite **Physische Maschinen** (siehe Die Seite „Physische Maschinen“) eines Systems, das für zwei Knoten lizenziert ist, beide PMs den Status **wird ausgeführt** aufweisen und dass sich keine PM im Wartungsmodus oder im Prozess der Synchronisierung befindet.
2. Wählen Sie auf der Seite **Virtuelle Maschinen** (siehe Die Seite „Virtuelle Maschinen“) die VM aus, die das Volume enthält, das Sie erweitern möchten. Stellen Sie sicher, dass die VM **gestoppt** wurde.
3. Klicken Sie im unteren Fensterbereich auf die Registerkarte **Volumes** und wählen Sie das Volume aus, das Sie erweitern möchten. Klicken Sie in der Spalte **Aktion** auf **Volume erweitern**.
4. Geben Sie neben **Erweitern um** die Größe des Speicherplatzes ein, den Sie diesem Volume hinzufügen möchten (in Gigabytes (GB)). Wenn Sie die Zahl eingeben, zeigt das Dialogfeld die **Erweiterte Volumegröße** an, die sich ergibt, wenn Sie den Vorgang abschließen.

   Hinweis: Geben Sie den Wert für **Erweitern um** mit Bedacht ein, denn nachdem Sie ein Volume erweitert haben, können Sie die Änderung nicht rückgängig machen und das Volume auch nicht verkleinern; es ist nur eine weitere Vergrößerung möglich.
5. Klicken Sie auf **Volume erweitern**, um die Änderung zu übernehmen und das Volume zu erweitern. Das Dialogfeld zeigt den Erweiterungsfortschritt an und wird automatisch geschlossen, wenn der Vorgang abgeschlossen ist.

Verwandte Themen

Erstellen eines Volumes in einer virtuellen Maschine

Trennen eines Volumes von einer virtuellen Maschine

Entfernen eines Volumes von einer virtuellen Maschine

Verwalten von VM-Ressourcen

Planen von VM-Ressourcen

Verwalten von virtuellen Maschinen

Wiederherstellen von VM-Ressourcen

Um Speicherplatz zu sparen, entfernen Sie VM-Ressourcen, wenn sie nicht mehr gebraucht werden. Unter Umständen müssen Sie auch unverzüglich Speicherplatz wiederherstellen, wenn nicht genügend Platz für

bestimmte Aufgaben vorhanden ist, zum Beispiel zum Erstellen eines Volumes oder einer VCD.

Zum Wiederherstellen von Speicherplatz entfernen Sie die nicht benötigten Ressourcen wie in den folgenden Themen beschrieben:

- Entfernen einer virtuellen Maschine
- Entfernen eines Volumes von einer virtuellen Maschine
- Entfernen einer virtuellen CD

Verwandte Themen

Verwalten von VM-Ressourcen

Planen von VM-Ressourcen

Verwalten von virtuellen Maschinen

Verwalten von virtuellen CDs

Erstellen und verwalten Sie virtuelle CDs (VCDs), um Softwareinstallationsmedien für die virtuellen Maschinen in Ihrem ztC Edge-System im ISO-Format bereitzustellen.

Eine VCD ist eine schreibgeschützte ISO-Abbilddatei, die sich auf einem Speichergerät im ztC Edge-System befindet. Verwenden Sie den **Assistenten zum Erstellen von virtuellen CDs** (in ztC Console), um eine vorhandene ISO-Datei hochzuladen wie unter Erstellen einer virtuellen CD beschrieben.

Nachdem Sie eine VCD erstellt haben, können Sie von dieser VCD starten, um ein Windows- oder Linux-Gastbetriebssystem zu installieren, oder eine VM von einer startfähigen Wiederherstellungs-VCD starten. Sie können eine VCD auf Ihren lokalen Computer herunterladen. Sie können eine VCD auch in eine laufende VM einlegen, um Softwareanwendungen zu installieren.

Das Verwalten von VCDs wird in den folgenden Themen beschrieben:

- Erstellen einer virtuellen CD
- Einlegen einer virtuellen CD
- Auswerfen einer virtuellen CD
- Starten von einer virtuellen CD
- Umbenennen einer virtuellen CD
- Herunterladen einer virtuellen CD
- Entfernen einer virtuellen CD

Benutzer, denen die Rolle **Administrator** oder **Plattform-Manager** zugewiesen wurde, können diese Aufgaben ausführen. Benutzer, denen die Rolle **VM-Manager** zugewiesen wurde, können alle VCD-Aufgaben ausführen, ausgenommen das Umbenennen einer VCD. (Informationen zur Zuweisung dieser Rollen finden Sie unter Verwalten lokaler Benutzerkonten.)

Erstellen einer virtuellen CD

Erstellen Sie eine virtuelle CD (VCD), um den virtuellen Maschinen (VM) im ztC Edge-System Softwareinstallationsmedien zur Verfügung zu stellen.

Um eine VCD zu erstellen, verwenden Sie den Assistenten zum **Erstellen von virtuellen CDs**, um eine ISO-Datei auf ein Speichergerät im ztC Edge-System hochzuladen oder zu kopieren. Danach können Sie von der VCD starten (siehe Starten von einer virtuellen CD), um ein Gastbetriebssystem zu installieren oder eine VM von einer startfähigen Wiederherstellungs-VCD zu starten. Sie können eine VCD auch in eine laufende VM einlegen (siehe Einlegen einer virtuellen CD), um Softwareanwendungen zu installieren.

Hinweise:

1. Falls Sie eine VCD nicht regelmäßig verwenden, sollten Sie sie entfernen, wenn sie nicht mehr gebraucht wird.
2. Wenn Sie eine startfähige VCD für die Installation erstellen, muss es sich um eine einzelne CD oder DVD handeln. Mehrere CDs oder DVDs werden nicht unterstützt.

So erstellen Sie eine VCD

1. Falls erforderlich, erstellen Sie ISO-Dateien der physischen Medien, für die Sie VCDs erstellen.
2. Öffnen Sie die Seite **Virtuelle CDs** in der ztC Console.
3. Klicken Sie auf **VCD erstellen**, um den **Assistenten zum Erstellen virtueller CDs** zu öffnen.
4. Geben Sie einen Namen für die VCD ein.
5. Wählen Sie eine Quelle für die VCD aus:
   - **ISO-Datei hochladen** lädt eine Datei vom System hoch, in dem die ztC Console ausgeführt wird. Klicken Sie auf **Durchsuchen**, wählen Sie die ISO-Datei im System aus und klicken Sie auf **Öffnen**.
   - **CD-ISO aus Netzwerkquelle kopieren** kopiert die Datei von einer Web-URL. Geben Sie die URL der ISO-Datei ein.

6. Klicken Sie auf **Fertigstellen**, um die ISO-Datei von der ausgewählten Quelle hochzuladen oder zu kopieren.

   Der **Assistent zum Erstellen virtueller CDs** zeigt den Fortschritt des Uploads an.

Sie können den Status einer VCD in der Spalte **Zustand** auf der Seite **Virtuelle CDs** überprüfen:

- Das Symbol „Synchronisierung“ ( ) zeigt an, dass die VCD noch erstellt wird.
- Das Symbol „Beschädigt“ ( ) zeigt an, dass die VCD nicht erstellt werden konnte. Nehmen Sie die VCD aus dem Laufwerk und versuchen Sie erneut, sie zu erstellen.
- Das Symbol „Normal“ ( ) zeigt an, dass die Übertragung abgeschlossen und die VCD einsatzbereit ist.

Verwandte Themen

Einlegen einer virtuellen CD

Auswerfen einer virtuellen CD

Verwalten von virtuellen CDs

Erstellen und Migrieren von virtuellen Maschinen

Einlegen einer virtuellen CD

Legen Sie eine virtuelle CD (VCD) in eine virtuelle Maschine (VM) ein, um auf ein Installationsmedium zuzugreifen, wenn Sie Anwendungen in einem Gastbetriebssystem installieren. (Zum Anschließen eines USB-Geräts lesen Sie Anschließen eines USB-Geräts an eine virtuelle Maschine. Informationen zum Starten einer virtuellen Maschine von einer VCD finden Sie unter Starten von einer virtuellen CD.)

Achtung: Wenn Sie eine VCD in eine laufende VM einlegen, wird verhindert, dass die Stratus Redundant Linux-Software die VM auf eine andere physische Maschine migriert, falls es zu einem Ausfall kommt. Um die Redundanz wiederherzustellen, heben Sie die Bereitstellung der VCD auf und werfen Sie sie aus, sobald Sie mit ihrer Verwendung fertig sind.

Hinweis: Standardmäßig ist das Einlegen von VCDs bei VMs aktiviert. Wenn Sie diese Konfiguration ändern möchten, lesen Sie Konfigurieren von VM-Geräten.

So verbinden Sie eine VCD mit einer VM

1. Erstellen Sie ggf. eine VCD (siehe Erstellen einer virtuellen CD) für das Softwareinstallationsmedium, das Sie brauchen.
2. Wählen Sie auf der Seite **Virtuelle Maschinen** eine VM aus.
3. Klicken Sie im unteren Fensterbereich auf die Registerkarte **CD-Laufwerke und USB-Geräte**.
4. Um eine VCD auszuwählen, klicken Sie auf **CD einlegen** und wählen Sie eine VCD aus. Verwenden Sie ggf. das Pulldownmenü.

Wenn das System die VCD eingelegt hat, wird der Name rechts neben **CD-ROM** angezeigt.

Verwandte Themen

Erstellen einer virtuellen CD

Auswerfen einer virtuellen CD

Starten von einer virtuellen CD

Verwalten von virtuellen CDs

Auswerfen einer virtuellen CD

Werfen Sie einen virtuelle CD (VCD) aus, um sie von einer virtuellen Maschine (VM) zu trennen. Wenn Sie eine VCD auswerfen, können Sie eine andere VCD in die VM einlegen. Außerdem wird die VCD dann verfügbar, um sie in eine andere VM einzulegen.

So werden Sie eine VCD aus einer VM aus

1. Heben Sie die Bereitstellung der VCD im Gastbetriebssystem auf, um sicherzustellen, dass sie nicht verwendet wird.
2. Wählen Sie auf der Seite **Virtuelle Maschinen** eine VM aus.
3. Klicken Sie im unteren Fensterbereich auf die Registerkarte **CD-Laufwerke und USB-Geräte**.
4. Klicken Sie auf der Registerkarte **CD-Laufwerke** auf **CD auswerfen**.

Verwandte Themen

Erstellen einer virtuellen CD

Einlegen einer virtuellen CD

Starten von einer virtuellen CD

Verwalten von virtuellen CDs

Starten von einer virtuellen CD

Starten Sie eine virtuelle Maschine von einer virtuellen CD (VCD), um ein Gastbetriebssystem zu installieren oder Wartungsaufgaben auszuführen.

Vor dem Starten von einer VCD müssen Sie die virtuelle Maschine herunterfahren.

So starten Sie eine virtuelle Maschine von einer VCD

1. Falls erforderlich, erstellen Sie eine VCD von einer startfähigen CD/DVD (siehe Erstellen einer virtuellen CD).
2. Wählen Sie auf der Seite **Virtuelle Maschinen** eine virtuelle Maschine aus.
3. Falls die virtuelle Maschine ausgeführt wird, klicken Sie auf **Herunterfahren**.
4. Wenn der Status der virtuellen Maschine als **Beendet** angezeigt wird, klicken Sie im unteren Fensterbereich auf **Von CD starten**.
5. Wählen Sie die startfähige VCD aus und klicken Sie auf **Starten**.

Hinweis: Eine Windows-basierte virtuelle Maschine, die von einer VCD gestartet wird, startet als Hardware-VM (HVM) und kann nur auf die ersten drei Datenträgervolumes zugreifen.

Verwandte Themen

Erstellen einer virtuellen CD

Einlegen einer virtuellen CD

Auswerfen einer virtuellen CD

Verwalten von virtuellen CDs

Erstellen und Migrieren von virtuellen Maschinen

Verwalten des Betriebs einer virtuellen Maschine

Umbenennen einer virtuellen CD

Sie können eine virtuelle CD (VCD) umbenennen, damit sie auf der Seite **Virtuelle CDs** mit einem anderen Namen angezeigt wird.

So benennen Sie eine VCD um

1. Suchen Sie die VCD auf der Seite **Virtuelle CDs**.
2. Doppelklicken Sie auf den Namen der VCD.
3. Geben Sie den neuen Namen ein und drücken Sie die **Eingabetaste**.

Verwandte Themen

Entfernen einer virtuellen CD

Einlegen einer virtuellen CD

Auswerfen einer virtuellen CD

Erstellen einer virtuellen CD

Verwalten von virtuellen CDs

Herunterladen einer virtuellen CD

Laden Sie eine virtuelle CD (VCD) herunter, um die Software auf der VCD für den Upload zu einem späteren Zeitpunkt zur Verfügung zu stellen.

Voraussetzung: Zunächst müssen Sie eine VCD erstellen, falls Sie dies noch nicht getan haben. Siehe Erstellen einer virtuellen CD.

So laden Sie eine VCD herunter

1. Öffnen Sie die Seite **Virtuelle CDs** in der ztC Console.
2. Klicken Sie auf den Namen der VCD, die Sie herunterladen möchten.
3. Klicken Sie auf **Herunterladen**. Es wird ein Fenster eingeblendet, in dem ein Ordner auf Ihrem lokalen Computer angezeigt wird.
4. Wählen Sie einen Speicherort für die Datei und klicken Sie auf **Speichern**.

Je nach Größe der Datei kann es einige Minuten dauern, bis der Download abgeschlossen ist.

Verwandte Themen

Verwalten von virtuellen CDs

Entfernen einer virtuellen CD

Entfernen Sie eine virtuelle CD (VCD), um sie dauerhaft aus dem ztC Edge-System zu löschen.

So entfernen Sie eine VCD

1. Klicken Sie in der ztC Console auf **Virtuelle CDs**.
2. Suchen Sie die VCD, die Sie entfernen möchten, in der Liste.
3. Vergewissern Sie sich, dass in der Spalte **Kann entfernt werden** für die VCD **Ja** angezeigt wird. Wenn der Wert **Nein** ist, wird die VCD zurzeit verwendet.
4. Wählen Sie die VCD im unteren Fensterbereich aus und klicken Sie auf **Entfernen**.

Verwandte Themen

Umbenennen einer virtuellen CD

Einlegen einer virtuellen CD

Auswerfen einer virtuellen CD

Erstellen einer virtuellen CD

Verwalten von virtuellen CDs

Erweiterte Themen (virtuelle Maschinen)

Die folgenden Themen beschreiben Verfahren und Informationen für erfahrene Benutzer:

- Zuweisen einer spezifischen MAC-Adresse zu einer virtuellen Maschine
- Auswählen einer bevorzugten PM für eine virtuelle Maschine
- Erzwungenes Starten einer VM
- Ändern der Schutzstufe für eine virtuelle Maschine (HV oder FT)
- Konfigurieren der Startreihenfolge für virtuelle Maschinen
- Zurücksetzen der MTBF für eine ausgefallene virtuelle Maschine
- Anschließen eines USB-Geräts an eine virtuelle Maschine

Informationen zum Betrieb einer virtuellen Maschine finden Sie unter Verwalten des Betriebs einer virtuellen Maschine.

Zuweisen einer spezifischen MAC-Adresse zu einer virtuellen Maschine

Weisen Sie einer virtuellen Maschine (VM) eine spezifische MAC-Adresse zu, wenn Sie die Standard-MAC-Adresse überschreiben müssen.

Warnungen:

1. Standardmäßig weist die Stratus Redundant Linux-Software den VMs automatisch MAC-Adressen zu. Übergehen Sie die Standardeinstellungen nicht, wenn Sie keine spezifischen Anforderungen haben (zum Beispiel, um Softwareanwendungen zu unterstützen, die auf Grundlage der MAC-Adresse lizenziert werden).
2. Wenn Sie die **Statische System-IP-Adresse** ändern, werden alle MAC-Adressen, die den VMs automatisch zugewiesen wurden, geändert, weil die Stratus Redundant Linux-Software die MAC-Adressen für die VMs basierend auf der System-IP-Adresse generiert. Um zu verhindern, dass die MAC-Adresse einer VM geändert wird, legen Sie eine dauerhafte MAC-Adresse fest wie nachstehend beschrieben. Wenden Sie sich an Ihren Netzwerkadministrator, um eine gültige MAC-Adresse für Ihre Umgebung zu generieren. Vergessen Sie nicht, ggf. Firewallregeln zu ändern, damit die neue MAC-Adresse zugelassen wird.

Voraussetzung: Bevor Sie die MAC-Adresse einer virtuellen Maschine ändern, müssen Sie die VM herunterfahren.

So weisen Sie einer VM eine spezifische MAC-Adresse zu

1. Öffnen Sie die Seite **Virtuelle Maschinen** (siehe Die Seite „Virtuelle Maschinen“).
2. Wählen Sie eine VM aus und klicken Sie auf **Herunterfahren**.
3. Wenn die VM beendet wurde, klicken Sie auf **Konfig**, um den Assistenten **Virtuelle Maschine neu zuweisen** anzuzeigen.
4. Klicken Sie auf jeder Seite des Assistenten auf **Weiter**, bis die Seite **Netzwerke** angezeigt wird. (Lesen Sie ggf. Neuzuweisen von VM-Ressourcen, um weitere VM-Ressourcen zu konfigurieren.)

5. Suchen Sie auf der Seite **Netzwerke** das Netzwerk, das Sie ändern möchten, und notieren Sie sich die aktuelle MAC-Adresse für den Fall, dass Sie sie wiederherstellen müssen.
6. Geben Sie die neue Adresse in der Spalte **MAC-Adresse** ein oder lassen Sie den Textbereich leer, damit die Stratus Redundant Linux-Software die MAC-Adresse automatisch zuweist.
7. Klicken Sie auf **Fertigstellen**.

Verwandte Themen

Erweiterte Themen (virtuelle Maschinen)

Verwalten von VM-Ressourcen

Verwalten des Betriebs einer virtuellen Maschine

Auswählen einer bevorzugten PM für eine virtuelle Maschine

Wählen Sie bei Systemen, die für zwei Knoten lizenziert sind, eine bevorzugte physische Maschine aus, um sicherzustellen, dass eine virtuelle Maschine auf einer bestimmten physischen Maschine im ztC Edge-System ausgeführt wird.

> **Hinweis**: Standardmäßig verteilt das System die Last der virtuellen Maschinen automatisch gleichmäßig auf die beiden physischen Maschinen. Ändern Sie diese Einstellung nur dann, wenn Sie bestimmte Anforderungen an die Lastverteilung haben.

So wählen Sie eine bevorzugte physische Maschine aus

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine virtuelle Maschine aus.
2. Klicken Sie im unteren Fensterbereich auf **Lastverteilung**.
3. Treffen Sie eine Auswahl in der Pulldownliste und klicken Sie auf **Speichern**.

Verwandte Themen

Erweiterte Themen (virtuelle Maschinen)

Verwalten des Betriebs einer virtuellen Maschine

Erzwungenes Starten einer VM

Wenn Sie den Start einer VM erzwingen möchten, können Sie die Schaltfläche **Erzwungenes Starten** auf der Seite VIRTUELLE MASCHINEN verwenden. Die Schaltfläche **Erzwungenes Starten** ist jedoch nur

dann aktiv, wenn die ztC Console meldet, dass der Partnerknoten ausgeschaltet oder aus anderem Grund nicht erreichbar ist. Wenn Sie **Erzwungenes Starten** verwenden, um eine VM online zu bringen, umgehen Sie manuell die Sicherheitsprüfungen des Systems zum Schutz Ihrer Daten. Verwenden Sie **Erzwungenes Starten** also mit Bedacht und nur, wenn Ihnen die Konsequenzen vollkommen bewusst sind.

Achtung: Lesen Sie dieses gesamte Thema aufmerksam durch und beraten Sie sich mit Ihrem autorisierten Stratus-Servicemitarbeiter, bevor Sie auf **Erzwungenes Starten** klicken. Der Servicemitarbeiter kann Ihr System prüfen, darunter auch das Datum der letzten Volumesynchronisierung, und dann die Auswirkungen des **Erzwungenen Startens** mit Ihnen besprechen. Sie können dann gemeinsam mit Ihrem Servicemitarbeiter entscheiden, ob der Start der VM erzwungen werden soll oder nicht.

Wenn Sie eine VM über die Schaltfläche **Erzwungenes Starten** online bringen, wählen Sie einen Knoten aus (d. h. den erreichbaren Knoten), auf dem die VM erzwungenermaßen starten soll. Alle Daten auf diesem Knoten werden als gültig markiert, unabhängig vom tatsächlichen Zustand der Daten (Status der Daten, letzte Synchronisierung, Zustand des Volumes usw.).

Während des **erzwungenen Startens** werden die Volumes der VM mit dem Datum und der Uhrzeit gekennzeichnet, zu dem das erzwungene Starten eingeleitet wurde. Die AX-Komponenten der VM (also das AX-Paar der VM) verwenden die Daten auf den Volumes der VM und melden den Status der Daten, um zu ermitteln, welche AX die aktuellen Volume-Informationen enthält. Der Prozess **Erzwungenes Starten** übergeht die eingebaute Logik, die verhindert, dass eine VM in einem Split-Brain-Zustand ausgeführt wird. Wenn das AX-Paar nicht kommunizieren kann, tritt eine Split-Brain-Bedingung auf und schädigt die Datenintegrität (Informationen zur Split-Brain-Bedingung finden Sie unter Erstellen einer ALSR-Konfiguration).

Warnungen: Verwenden Sie **Erzwungenes Starten** nicht in den folgenden Situationen:

- Mindestens ein Volume ist das Ziel einer nicht abgeschlossenen Spiegelkopie auf dem Knoten, auf dem Sie das **erzwungene Starten** ausführen wollen.
- Das Ziel einer unvollständigen Spiegelkopie ist in keinem guten Zustand und ist auch nach einem **erzwungenen Starten** nicht verfügbar.
- Die Volumes sind nicht synchronisiert. Die folgenden zwei Situationen sind Beispiele:
  - Beide AX der VMs müssen Zugriff auf alle Datenvolumes der VM haben.
  - Bei einem System mit mehreren Volumes ist es erforderlich, dass beide AX ausgeführt werden, damit die VM Zugriff auf alle ihre Volumes hat, da jeder Knoten eine Kopie eines anderen Volumes mit grünem Prüfhäkchen hat und die Spiegelkopie des Volumes auf dem jeweils anderen Knoten kein grünes Prüfhäkchen hat.
- Beide Knoten sind erforderlich, da mehrere VMs verschlechtert sind, aber trotzdem auf dem jeweils anderen Knoten ein grünes Prüfhäkchen haben. (Zum Beispiel: Knoten0 hat ein gutes Startvolume, aber ein schlechtes Datenvolume, während Knoten1 ein schlechtes Startvolume, aber ein gutes Datenvolume hat.)
- Das System ist für einen Knoten lizenziert.

Wenn Sie das **erzwungene Starten** auf einem System mit veralteten Volumes ausführen, wenden Sie sich unverzüglich an Ihren autorisierten Stratus-Servicemitarbeiter. Wenn beide Knoten eingeschaltet sind und mit der Synchronisierung der Daten begonnen haben, verwendet das System Daten von der VM, deren Start Sie erzwungen haben, und Sie können die Daten auf dem Knoten, der nicht erreichbar war, nicht wiederherstellen.

Unter bestimmten Umständen ist es eventuell möglich, dass Sie Daten wiederherstellen können, nachdem Sie das **erzwungene Starten** auf einem System mit veralteten Volumes ausgeführt haben:

- Wenn der nicht erreichbare Knoten noch ausgeschaltet ist, schalten Sie ihn nicht ein.
- Wenn der nicht erreichbare Knoten ausgeschaltet war, bevor Sie auf **Erzwungenes Starten** geklickt haben, bleibt die AX der VM auf dem ausgeschalteten Knoten erhalten. Unter den folgenden Bedingungen können Sie den Vorgang **Erzwungenes Starten** dann ohne Datenverlust rückgängig machen:

- Die VM, deren Start Sie erzwungen haben, hat keine neuen Daten (d. h., die VM wurde nicht in die Produktion genommen).
- Bevor Sie den Start der VM erzwungen haben, hat die AX der VM auf dem nicht erreichbaren Knoten nicht den Status mit der AX auf der VM, deren Start Sie erzwingen wollen, ausgetauscht.
- Das Problem, das den Start der VM-AX auf dem nicht erreichbaren Knoten verhindert hat, wurde behoben.
- Alle VM-Daten zwischen den beiden Knoten werden korrekt synchronisiert. Das System hat keine VMs, bei denen sich die Daten der VM-AX auf dem einen Knoten in einem anderen Zustand als die Daten der VM-AX auf dem anderen Knoten befinden.

Wenn Ihr System alle genannten Bedingungen erfüllt, wenden Sie sich an Ihren autorisierten Stratus-Servicemitarbeiter, um Unterstützung zum Wiederherstellungsprozess zu erhalten.

Wenn Sie sich entschieden haben, den Start einer VM zu erzwingen, bereiten Sie den Vorgang mit den entsprechenden erforderlichen Verfahren vor.

Voraussetzungen:

- Prüfen Sie alle Volumes manuell, um sicherzustellen, dass Sie sie sicher übergehen können. Zum Beispiel muss der Volumezustand ein grünes Prüfhäkchen aufweisen und die Datenträgersynchronisierung muss abgeschlossen sein.
- Vergewissern Sie sich, dass beide AX-Komponenten der VM miteinander kommunzieren können und zulassen, dass die Systemprozesse den Zustand jedes Volumes ermitteln. Um einen Split-Brain-Zustand zu verhindern, müssen Sie sicherstellen, dass die beiden AX-Komponenten der VM ihren Status kommunizieren und ermitteln können, welche AX gute Daten- und gute Startvolumes hat.
- Stellen Sie sicher, dass das System für zwei Knoten lizenziert ist.
- Wenden Sie sich an Ihren autorisierten Stratus-Servicemitarbeiter.

So führen Sie den erzwungenen Start einer VM durch

Nachdem Sie sich mit Ihrem autorisierten Stratus-Servicemitarbeiter beraten und entschieden haben, den Start einer VM zu erzwingen, gehen Sie wie nachstehend beschrieben vor. In den Beispielen ist Knoten0 offline, Knoten1 ist der primäre Knoten und VM-1 wurde gestoppt.

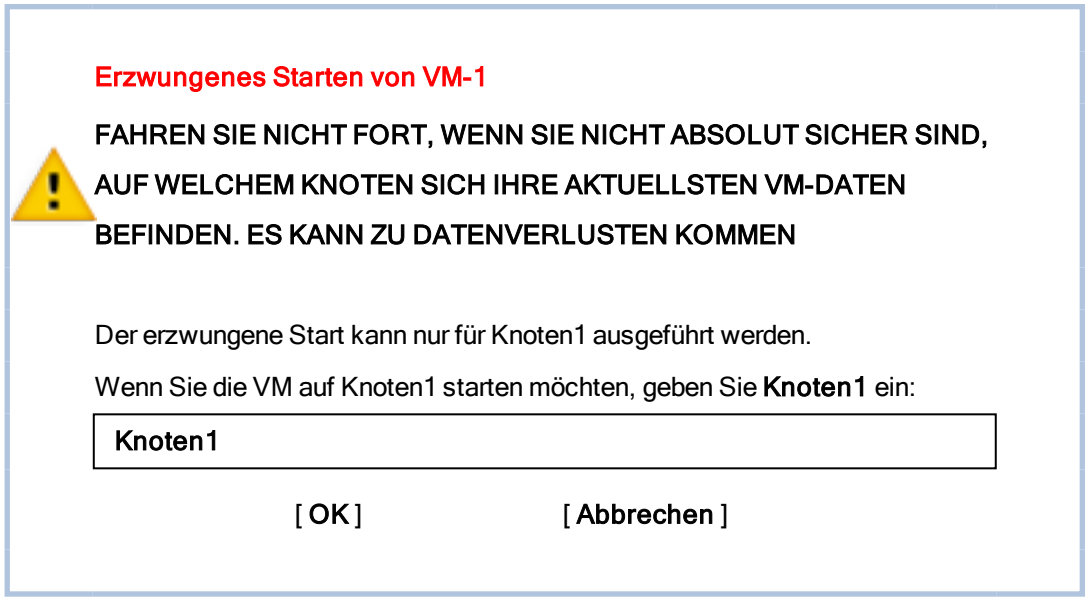
1. Klicken Sie in der ztC Console eines Systems mit zwei Knoten auf der linken Seite auf **Virtuelle Maschinen**.
2. Öffnen Sie die Seite **Virtuelle Maschinen**.
3. Wählen Sie auf der Seite **Virtuelle Maschinen** die gestoppte VM aus, deren Start Sie erzwingen möchten (im Beispiel VM-1).
4. Klicken Sie im unteren Fensterbereich auf die Schaltfläche **Starten**.

   Die VM beginnt zu starten. Der Start wird fortgesetzt, bis die Zeitüberschreitung erreicht wird, dies können 5 Minuten sein. Nach Erreichen der Zeitüberschreitung wird die Schaltfläche **Erzwungenes Starten** verfügbar.
5. Klicken Sie auf **Erzwungenes Starten**, um den Start der VM zu erzwingen.

   Es wird eine Warnung angezeigt, in der Sie gefragt werden, ob Sie ganz sicher wissen, auf welchem Knoten sich die aktuellsten VM-Daten befinden. In der Warnung werden Sie auch darauf hingewiesen, dass es zu einem Datenverlust kommen kann. Außerdem wird in einer Meldung angegeben, auf welchem Knoten Sie den Start der VM erzwingen können.

   Achtung: Wenn Sie für den Vorgang **Erzwungenes Starten** den falschen Knoten wählen, werden Daten beschädigt.

   Sie müssen den Knoten (Knoten0 oder Knoten1) angeben wie in der Meldung angezeigt. Die folgende Meldung ist ein Beispiel:

6. Klicken Sie auf **OK**, um den Start des Knotens (im Beispiel Knoten1) zu erzwingen. (Oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.) Während der Prozess zum erzwungenen Starten beginnt und fortgesetzt wird, werden weitere Bestätigungsmeldungen angezeigt, bevor die VM startet und die Daten für das System als gültig markiert werden.

   Die VM wird ausgeführt. Auf der Seite **Virtuelle Maschinen** wird die VM mit einer Warnung angezeigt, da der Knoten (im Beispiel Knoten0) immer noch offline ist.

   Nachdem der sekundäre Knoten ins das System zurückgebracht wurde, werden alle Daten vom Knoten, der die VM ausführt, synchronisiert. In unserem Beispiel werden also alle Daten von Knoten1 zu Knoten0 synchronisiert.

Verwandte Themen

Erweiterte Themen (virtuelle Maschinen)

Verwalten des Betriebs einer virtuellen Maschine

Ändern der Schutzstufe für eine virtuelle Maschine (HV oder FT)

Sie können die Schutzstufe von Gast-VMs von hoher Verfügbarkeit (HV) zu fehlertolerant (FT) ändern oder umgekehrt.

So ändern Sie die Schutzstufe

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine beendete VM (mit der Markierung „Beendet“ in der Spalte **Aktivität**). (Informationen zum Beenden einer VM finden Sie unter Herunterfahren einer virtuellen Maschine.)
2. Klicken Sie im unteren Fensterbereich auf **Konfig**, um den Assistenten **Virtuelle Maschine neu zuweisen** zu öffnen.
3. Wählen Sie auf der Seite **Name, Beschreibung und Schutz** die Option **HV** oder **FT**.
4. Klicken Sie sich durch den Assistenten, bis Sie die letzte Seite erreichen. Klicken Sie auf **Fertigstellen** und dann auf **OK** (falls die Neukonfiguration erfolgreich war).

Verwandte Themen

Betriebsmodi (HV oder FT)

Erweiterte Themen (virtuelle Maschinen)

Verwalten des Betriebs einer virtuellen Maschine

Konfigurieren der Startreihenfolge für virtuelle Maschinen

Konfigurieren Sie die Startreihenfolge virtueller Maschinen, um die Reihenfolge festzulegen, in der Gastbetriebssysteme und Anwendungen auf dem ztC Edge-System gestartet werden.

Bestimmen Sie die erforderliche Startreihenfolge und konfigurieren Sie die Starteinstellungen für die einzelnen virtuellen Maschinen dann entsprechend.

So legen Sie die Startreihenfolge für eine virtuelle Maschine fest

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine virtuelle Maschine aus.
2. Klicken Sie im unteren Fensterbereich auf die Registerkarte **Startreihenfolge**.
3. Konfigurieren Sie die Starteinstellungen wie nachstehend beschrieben.
4. Klicken Sie auf **Speichern**.

Es gibt folgende Starteinstellungen:

- Die **Prioritätsgruppe** ermöglicht es Benutzern, die Reihenfolge anzugeben, in der virtuelle Maschinen nach dem Einschalten des ztC Edge-Systems oder nach einem Failover, bei dem ein Neustart virtueller Maschinen erforderlich ist, gestartet werden. Einige Unternehmenslösungen erfordern, dass bestimmte virtuelle Maschinen laufen, bevor andere gestartet werden. Gruppe **1** bezeichnet die höchste Priorität und **Keine** die geringste. Die Stratus Redundant Linux-Software wartet, bis die **Betriebssystem- und Anwendungsstartzeit** abgelaufen ist, bevor die virtuellen Maschinen in der nächsten Prioritätsgruppe gestartet werden.

  Startsequenzbeispiel:

VM	Prioritätsgruppe	Betriebssystem und Anwendung Startzeit
DNS	1	2 Min.
Anw.	2	30 Sek.
DB	2	10 Min.
Web	3	0

1. ztC Edge startet die DNS-VM.
2. 2 Minuten nach dem Start der DNS-VM startet ztC Edge die Anwendungs- und DB-Server in Gruppe 2.
3. 10 Minuten nach dem Start der DB-VM startet ztC Edge die Web-VM in Gruppe 3.

- Die **Betriebssystem- und Anwendungsstartzeit** sollte auf die Zeit eingestellt werden, die es ab dem Starten der virtuellen Maschine dauert, bis das Gastbetriebssystem und die Anwendungen vollständig einsatzbereit sind.

Verwandte Themen

Erweiterte Themen (virtuelle Maschinen)

Verwalten des Betriebs einer virtuellen Maschine

Zurücksetzen der MTBF für eine ausgefallene virtuelle Maschine

Setzen Sie den MTBF-Zähler für eine virtuelle Maschine (VM) zurück, um zu versuchen, eine ausgefallene VM neu zu starten. (MTBF = mean time between failures, mittlere Betriebsdauer zwischen Ausfällen)

Wenn das Gastbetriebssystem einer virtuellen Maschine abstürzt, startet ztC Edge es automatisch neu, sofern es nicht unter den MTBF-Schwellenwert gefallen ist. Wenn die VM unter dem MTBF-Schwellenwert ist, belässt sie die ztC Edge-Software im abgestürzten Zustand. Falls erforderlich, können Sie den MTBF-Zähler zurücksetzen und die VM neu starten.

Achtung: Setzen Sie den MTBF-Zähler nur nach Aufforderung durch Ihren autorisierten Stratus-Servicemitarbeiter zurück, da die kontinuierliche Betriebszeit Ihres Systems dadurch beeinträchtigt werden kann.

Hinweise:

1. Die Schaltfläche **Gerät zurücksetzen** wird nur angezeigt, wenn die VM unter den MTBF-Schwellenwert gefallen ist.
2. Die Schaltfläche **MTBF löschen** wird nur angezeigt, wenn die Systemsoftware, die eine VM auf einer physischen Maschine unterstützt, unter den MTBF-Schwellenwert fällt.

So setzen Sie den MTBF-Zähler einer VM zurück

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine virtuelle Maschine aus.
2. Klicken Sie auf **Gerät zurücksetzen**.

Wenn die Systemsoftware, die eine VM auf einer physischen Maschine unterstützt, zu oft ausfällt, führen Sie die folgenden Schritte aus, um den MTBF-Zähler zurückzusetzen.

So setzen Sie den MTBF-Zähler für eine VM auf einer physischen Maschine zurück

1. Wählen Sie auf der Seite **Virtuelle Maschinen** eine virtuelle Maschine aus.
2. Klicken Sie auf **MTBF löschen**.

Verwandte Themen

Erweiterte Themen (virtuelle Maschinen)

Verwalten des Betriebs einer virtuellen Maschine

Erstellen einer Diagnosedatei

Anschließen eines USB-Geräts an eine virtuelle Maschine

Schließen Sie ein USB-Gerät an eine virtuelle Maschine (VM) an, damit die VM das Gerät verwenden kann. Ein USB-Gerät kann zum Beispiel erforderlich sein, wenn eine USB-basierte Lizenz benötigt wird, um eine Anwendung unter einem Gastbetriebssystem zu installieren. Wenn das USB-Gerät nicht mehr benötigt wird, können Sie es trennen.

(Wenn Sie ein USB-Gerät auf dem ztC Edge-System bereitstellen müssen, um es zum Exportieren oder Importieren von VMs zu verwenden, lesen Sie Bereitstellen eines USB-Geräts oder eines über das Netzwerk bereitgestellten Ordners im ztC Edge-System.)

Achtung:
Wenn Sie ein USB-Gerät an eine laufende, fehlertolerante (FT) VM anschließen, wird verhindert, dass die Stratus Redundant Linux-Software die VM auf eine andere physische Maschine migriert, falls es zu einem Ausfall kommt. Um den fehlertoleranten Betrieb wiederherzustellen, trennen und entfernen Sie das USB-Gerät, sobald Sie sie es nicht mehr benötigen.

Hinweise:

1. Es lassen sich nur unterstützte USB-Geräte an ein Gastbetriebssystem anschließen. Eine Liste der USB-Geräte, die von ztC Edge-Systemen unterstützt werden, finden Sie in den Spezifikationen für Ihr System:
   - Systemspezifikationen: ztC Edge 110i-Systeme
   - Systemspezifikationen: ztC Edge 100i-Systeme

   Beachten Sie, dass ztC Edge-Systeme keine Geräte gemäß USB 3.2 Gen 2 (10 Gbit/s) oder höher im Gastbetriebssystem unterstützen. Sie können jedoch ein Gen 2-Gerät (oder höher) an einen USB 3.2 Gen 1 (5 Gbit/s)-Host-Port anschließen, der das Gerät zum Betrieb gemäß Gen 1 (5 Gbit/s) zwingt; in diesem Fall können Sie das Gerät mit einem Gastbetriebssystem verbinden. (USB 3.2 Gen 1 (5 Gbit/)-Geräte wurden früher als USB 3.1 Gen 1-Geräte bezeichnet. USB 3.2 Gen 2 (10 Gbit/s)-Geräte wurden früher als USB 3.1 Gen 2-Geräte bezeichnet.)
2. Schließen Sie kein USB-3.0-Gerät (oder höher) an eine VM an, auf der eines der folgenden Betriebssysteme ausgeführt wird, da diese Betriebssysteme keine USB-3.0-Geräte unterstützen:
   - Windows 7 Desktop
   - Windows Small Business Server 2011
   - Eine ältere Linux-Distribution wie CentOS 6.6
3. Schließen Sie kein UAS-konformes Gerät (USB Attached SCSI) an eine VM an, da das System keine UAS-Geräte unterstützt.
4. Die VM muss ausgeführt werden, damit Sie ein USB-Gerät daran anschließen können.
5. Standardmäßig ist das Anschließen von USB-Geräten an VMs aktiviert. Wenn Sie diese Konfiguration ändern möchten, lesen Sie Konfigurieren von VM-Geräten.

6. Verwenden Sie eine der folgenden Methoden, um ein unterstütztes USB-Gerät von einer Windows-basierten VM zu trennen (auszuwerfen):
   - Im Datei-Explorer auf Auswerfen klicken – Wenn Sie das Gerät im Datei-Explorer auswerfen, müssen Sie es wie nachstehend beschrieben in der ztC Console trennen. Trennen Sie das Gerät danach physisch vom ztC Edge-System und schließen Sie es wieder an, bevor Sie es mit derselben oder einer anderen VM verbinden.
   - In der Taskleiste auf „Hardware sicher entfernen und Medium auswerfen“ klicken – Wenn Sie das Gerät über das Symbol in der Taskleiste auswerfen, müssen Sie es wie nachstehend beschrieben in der ztC Console trennen. Sie brauchen das Gerät nicht physisch vom ztC Edge-System zu trennen, bevor Sie es wieder mit derselben oder einer anderen VM verbinden.

So verbinden Sie ein USB-Gerät mit einer VM

1. Schließen Sie das USB-Gerät an den primären (aktiven) Knoten der VM an.

   Auf der Seite **Virtuelle Maschinen** wird der primäre Knoten für jede VM als die **Aktuelle PM** angezeigt. (Dieser Knoten kann sich vom aktuellen Knoten für das ztC Edge-System unterscheiden, wie er auf der Seite **Physische Maschinen** angezeigt wird.)

   Vergewissern Sie sich, dass das System das USB-Gerät anzeigt. Navigieren Sie zur Seite **Physische Maschinen**. Klicken Sie auf den Knoten, an den Sie das Gerät angeschlossen haben, und wählen Sie im unteren Fensterbereich die Registerkarte **USB-Geräte**. Das USB-Gerät, das Sie angeschlossen haben, sollte auf der Registerkarte aufgeführt werden.
2. Wählen Sie auf der Seite **Virtuelle Maschinen** eine VM aus.
3. Klicken Sie im unteren Fensterbereich auf die Registerkarte **CD-Laufwerke und USB-Geräte**.
4. Wählen Sie in der Zeile **USB** der Registerkarte **CD-Laufwerke und USB-Geräte** ein USB-Gerät aus dem Dropdownmenü aus
5. Klicken Sie auf **USB-Gerät verbinden**, um das USB-Gerät mit der VM zu verbinden.
6. Es wird ein Dialogfeld zur **Bestätigung** angezeigt, in dem Sie gefragt werden, ob Sie das Gerät anschließen möchten. Außerdem enthält es eine Warnung, dass das Gastsystem im Simplexmodus läuft, während das USB-Gerät verwendet wird. Klicken Sie auf **Ja**, um das Gerät zu verbinden.

Nachdem das System das USB-Gerät mit der VM verbunden hat, wird der Name des USB-Geräts in der Liste der USB-Geräte auf der Registerkarte **CD-Laufwerke und USB-Geräte** für die VM aufgeführt.

So trennen Sie ein USB-Gerät von einer VM

1. Wählen Sie auf der Seite **Virtuelle Maschinen** die VM aus, an die das USB-Gerät angeschlossen ist.
2. Klicken Sie im unteren Fensterbereich auf die Registerkarte **CD-Laufwerke und USB-Geräte**.
3. Klicken Sie in der Zeile **USB** der Registerkarte **CD-Laufwerke und USB-Geräte** auf **USB-Gerät trennen**. Wählen Sie das USB-Gerät ggf. aus dem Pulldownmenü aus.
4. Es wird ein Dialogfeld zur **Bestätigung** angezeigt, in dem Sie gefragt werden, ob Sie das USB-Gerät wirklich trennen möchten. Klicken Sie auf **Ja**, um das Gerät zu trennen.

   Nachdem das System das USB-Gerät von der VM getrennt hat, wird der Name des USB-Geräts nicht länger in der Liste der USB-Geräte auf der Registerkarte **CD-Laufwerke und USB-Geräte** für die VM aufgeführt.

Verwandte Themen

Verwalten von virtuellen Maschinen

7

Kapitel 7: Warten von physischen Maschinen

Sie können physische Maschinen (PMs), auch als Knoten bezeichnet, in einem ztC Edge-System warten, indem Sie sie ersetzen oder wiederherstellen.

Um eine ausgefallene PM zu ersetzen, führen Sie eines der folgenden Verfahren aus:

- Ersetzen von physischen Maschinen (automatisiert) (empfohlen)

  In diesem Thema wird beschrieben, wie Sie eine ausgefallene PM mithilfe des automatisierten Knotenaustausches ersetzen. Dieses Hilfethema ergänzt die Informationen im Dokument *ztC Edge 100i/110i-Systeme: Einen Knoten austauschen* (R013Z), das mit jedem Ersatzknoten geliefert wird.

- Ersetzen von physischen Maschinen (manuell)

  In diesem Thema wird beschrieben, wie Sie eine ausgefallene PM mit dem vom Benutzer eingeleiteten Prozess ersetzen. Dieser Prozess wird in der ztC Console gestartet und überwacht. Dieses vom Benutzer eingeleitete Verfahren sollten Sie vermeiden, sofern Sie nicht speziell durch Ihren autorisierten Stratus-Servicemitarbeiter dazu aufgefordert werden.

Um die Systemsoftware auf einer ausgefallenen PM wiederherzustellen anstatt die PM-Hardware zu ersetzen, lesen Sie Wiederherstellen einer ausgefallenen physischen Maschine (manuell).

Wenn Sie einen Knoten zu einem System hinzufügen möchten, das nur für einen Knoten lizenziert ist, lesen Sie Hinzufügen eines Knotens zu einem Einzelknotensystem.

Ersetzen von physischen Maschinen (automatisiert)

In diesem Thema wird beschrieben, wie Sie eine ausgefallene physische Maschine (PM), auch als Knoten bezeichnet, in einem ztC Edge-System mithilfe des automatisierten Knotenaustausches ersetzen. Dies ergänzt die Informationen in *ztC Edge 100i/110i-Systeme: Einen Knoten austauschen* (R013Z).

Sie ersetzen einen ztC Edge-Knoten, während das System in Betrieb ist.

Voraussetzung: Um einen ztC Edge-Ersatzknoten anzufordern, melden Sie sich beim **Stratus Customer Service Portal** an, erweitern Sie **Customer Support** (Kundensupport) und klicken Sie auf **Add Issue** (Fall hinzufügen). Wenn Sie den Fall erstellen, halten Sie die folgenden Informationen bereit:

- **Bestandskennung** - Sie finden die **Bestandskennung** für Ihr System in der Titelliste der ztC Console.
- Diagnosedatei - Generieren Sie auf der Seite **Supportprotokolle** der ztC Console eine Diagnosedatei und laden Sie sie herunter wie unter Erstellen einer Diagnosedatei beschrieben. Fügen Sie die Diagnosedatei als Anhang dem Fall hinzu, den Sie im Service Portal erstellen.

Ein Kundenservice-Mitarbeiter wird sich bei Ihnen melden, um das Problem zu diagnostizieren und bei Bedarf einen Ersatzknoten bereitzustellen.

So ersetzen Sie einen Knoten in einem ztC Edge-System

1. Bestimmen Sie den zu ersetzenden Knoten. Der fehlerhafte Knoten ist entweder ausgeschaltet (automatisch) oder eingeschaltet mit der SYS-LED aus oder durchgehend grün (nicht in Ordnung). Ist der Knoten bereits ausgeschaltet, fahren Sie mit Schritt 3 fort.
2. Ist der fehlerhafte Knoten noch eingeschaltet, öffnen Sie die ztC Console, um Probleme zu beheben, die das Herunterfahren verhindern. Zum Beispiel kann eine ausgefallene Netzwerkverbindung beim stabilen Knoten eine Abhängigkeit am fehlerhaften Knoten verursachen. Beheben Sie die Probleme und fahren Sie den fehlerhaften Knoten herunter.
3. Trennen Sie das Netzkabel vom fehlerhaften Knoten, trennen Sie dann das Netzwerkkabel und entfernen Sie den Knoten physisch aus dem System.
4. Fügen Sie den Ersatzknoten zum System hinzu. Schließen Sie die Netzwerkkabel wieder an und dann das Stromkabel, um den Knoten automatisch einzuschalten. Der Knotenaustausch ist abgeschlossen. Das System beginnt ohne Benutzeraktion mit der Synchronisierung.
5. Nach 20 Minuten wechselt die SYS-LED von aus zu durchgehend grün, um anzuzeigen, dass die Software auf dem Ersatzknoten startet. Nach weiteren 15 Minuten blinkt die SYS-LED, um anzuzeigen, dass das System in Ordnung ist.

6. Melden Sie sich bei der ztC Console an, um die Systemintegrität zu überprüfen. Die Synchronisierung der virtuellen Maschinen kann einige Stunden dauern. Nach dem erfolgreichen Abschluss der Synchronisierung sollte das **Dashboard** grüne Häkchen ohne Probleme anzeigen.

Verwandte Themen

Wartungsmodus

Warten von physischen Maschinen

Die ztC Console

Physische Maschinen und virtuelle Maschinen

Die Seite „Physische Maschinen“

Ersetzen von physischen Maschinen (manuell)

Achtung: Wenn Sie eine PM in einem ztC Edge-System wiederherstellen oder ersetzen müssen, folgen Sie den Anleitungen in *ztC Edge 100i/110i-Systeme: Einen Knoten austauschen* (R013Z). (Lesen Sie bei Bedarf Ersetzen von physischen Maschinen (automatisiert) mit zusätzlichen Informationen.) Vermeiden Sie die Verwendung des in diesem Thema beschriebenen Verfahrens, sofern Sie nicht speziell durch Ihren autorisierten Stratus-Servicemitarbeiter dazu aufgefordert werden.

Sie ersetzen eine physische Maschine (PM), auch als Knoten bezeichnet, während das System in Betrieb ist. (Wenn Sie die Systemsoftware auf einer ausgefallenen PM wiederherstellen möchten anstatt die PM-Hardware zu ersetzen, lesen Sie Wiederherstellen einer ausgefallenen physischen Maschine (manuell).)

Wenn Sie eine PM entfernen und ersetzen, löscht das System alle Datenträger auf der Ersatz-PM vollständig, um die Installation der Stratus Redundant Linux-Systemsoftware vorzubereiten. Um die Software zu installieren, können Sie dem System erlauben, den Ersatzknoten von einem temporären PXE-Server (Preboot Execution Environment) auf der primären PM automatisch zu starten. Solange jede PM eine vollständige Kopie des zuletzt installierten Software-Kits enthält (wie auf der Seite **Upgrade-Kits** der ztC Console angezeigt), kann jede der beiden PMs die Ersetzung der jeweils anderen PM mittels PXE-Boot-Installation einleiten. Bei Bedarf starten Sie den Ersatzknoten manuell von einem USB-Installationsmedium.

Verwenden Sie eines der nachstehend beschriebenen Verfahren, je nachdem, welches Medium Sie für die Installation verwenden möchten, **PXE** oder **USB**-Installation.

Achtung: Bei der Ersetzung wird sämtliche im Gastbetriebssystem installierte Software auf der PM gelöscht, und alle PM-Konfigurationsinformationen, die Sie vor der Ersetzung eingegeben haben, gehen verloren. Nach Abschluss dieses Verfahrens müssen Sie Ihre gesamte Software auf Hostebene manuell neu installieren und die PM-Konfiguration entsprechend Ihren ursprünglichen Einstellungen ändern.

Achtung: Um Datenverlust zu vermeiden, sollten Sie Ihren autorisierten Stratus-Servicemitarbeiter um Unterstützung bitten, wenn das Systemprotokoll angibt, dass ein manuelles Eingreifen erforderlich ist, um eine Datenträgerspiegelung zu erstellen. Sie können wertvolle Daten verlieren, wenn Sie eine Neusynchronisierung erzwingen und den neuesten Datenträger im Spiegel überschreiben.

Voraussetzung: Um einen ztC Edge-Ersatzknoten anzufordern, melden Sie sich beim **Stratus Customer Service Portal** an, erweitern Sie **Customer Support** (Kundensupport) und klicken Sie auf **Add Issue** (Fall hinzufügen). Wenn Sie den Fall erstellen, halten Sie die folgenden Informationen bereit:

- **Bestandskennung** - Sie finden die **Bestandskennung** für Ihr System in der Titelliste der ztC Console.
- Diagnosedatei - Generieren Sie auf der Seite **Supportprotokolle** der ztC Console eine Diagnosedatei und laden Sie sie herunter wie unter Erstellen einer Diagnosedatei beschrieben. Fügen Sie die Diagnosedatei als Anhang dem Fall hinzu, den Sie im Service Portal erstellen.

Ein Kundenservice-Mitarbeiter wird sich bei Ihnen melden, um das Problem zu diagnostizieren und bei Bedarf einen Ersatzknoten bereitzustellen.

Voraussetzungen: Falls Sie die Systemsoftware mithilfe eines USB-Sticks auf der Ersatz-PM installieren möchten:

- Erstellen Sie einen startfähigen USB-Stick wie unter Erstellen eines USB-Mediums mit Systemsoftware beschrieben.

  Wenn Sie den USB-Stick erstellen, vergewissern Sie sich, dass er das zuletzt installierte Upgrade-Kit enthält. Beispiel: Wenn in der Titelleiste des ztC Console-Fensters die Version `1.2.0-550` angezeigt wird, wobei 550 die Buildnummer ist, dann muss das Kit, das Sie auf der Seite **Upgrade-Kits** zum Erstellen des USB-Sticks auswählen, ebenfalls die Version `1.2.0-550` haben. Wenn das System einen anderen Build auf der Ersatz-PM erkennt, wird der Ersetzungsprozess automatisch neugestartet. Das System initialisiert alle Daten auf der Ersatz-PM und verwendet die PXE-Boot-Installation, um das zuletzt installierte Software-Kit ohne weiteres Eingreifen des Benutzers auf der PM zu installieren.

- Schließen Sie eine Tastatur und einen Monitor an die Ersatz-PM an, um den Installationsprozess zu überwachen und Einstellungen festzulegen.

So können Sie eine ausgefallene PM wiederherstellen (mit PXE-Boot-Installation)

Gehen Sie wie nachstehend beschrieben vor, um eine ausgefallene PM zu ersetzen und die Systemsoftware neu zu installieren, indem Sie die PXE-Boot-Installation aus dem Software-Kit auf der primären PM verwenden.

1. Klicken Sie in der ztC Console im Navigationsbereich auf der linken Seite auf **Physische Maschinen**.
2. Wählen Sie die entsprechende PM (Knoten0 oder Knoten1) und klicken Sie dann auf **Wartung**. Dadurch wird der **Gesamtzustand** der PM in **Wartungsmodus** geändert und der **Aktivität**szustand ändert sich in **wird ausgeführt (in Wartung)**.
3. Wenn für die PM der Zustand **wird ausgeführt (in Wartung)** angezeigt wird, klicken Sie auf **Wiederherstellen**.
4. Wenn Sie aufgefordert werden, die Art der Reparatur auszuwählen, klicken Sie auf **PXE-PM-Wiederherstellung - Alle Datenträger initialisieren**.

   Achtung: Wenn Sie **PXE-PM-Ersetzung - Alle Datenträger initialisieren** wählen, werden alle Daten auf der Ersatz-PM gelöscht.

5. Wählen Sie eine der folgenden PXE-Einstellungen:

   - **Nur auf PXE-Anfragen vom aktuellen Partnerknoten antworten.**

     Wartet auf eine PXE-Anfrage von der MAC-Adresse des aktuellen Partnerknotens. Wählen Sie diese Option aus, wenn Sie die vorhandene PM wiederherstellen, indem Sie sie vollständig löschen und eine Neuinstallation ausführen. Bei diesem Prozess werden alle Daten auf der PM gelöscht, die aktuelle Netzwerkkonfiguration wird jedoch wiederhergestellt.

   - **Nur auf PXE-Anfragen von der folgenden MAC-Adresse antworten.**

     Wartet auf eine PXE-Anfrage von der MAC-Adresse, die Sie angeben. Wählen Sie diese Option aus, wenn Sie die PM durch eine neue PM ersetzen. Geben Sie die MAC-Adresse des spezifischen Netzwerkadapters ein, der den PXE-Startvorgang einleitet.

   - **PXE-Anfragen von allen Systemen auf priv0 akzeptieren.**

     Wartet auf eine PXE-Anfragen von priv0, dem privaten Netzwerk, das die beiden ztC Edge-Knoten verbindet. Wählen Sie diese Option, wenn Sie die PM durch eine neue PM ersetzen, aber die MAC-Adresse der neuen PM nicht kennen.

6. Klicken Sie auf **Weiter**, um mit der Ersetzung zu beginnen. Das System fährt die PM herunter und schaltet sie ab.
7. Wenn die PM ausgeschaltet ist, installieren Sie die Ersatz-PM, falls erforderlich:
   a. Trennen und entfernen Sie die alte PM und installieren Sie dann die Ersatz-PM.
   b. Bringen Sie die Netzwerkkabel an ihren ursprünglichen Anschlüssen an und schließen Sie dann die Stromversorgung wieder an.
8. Falls die PM nicht automatisch eingeschaltet wird, betätigen Sie die Ein/aus-Taste.
9. Der Austauschprozess läuft ohne Eingreifen des Benutzers wie folgt ab:
   - Die Ersatz-PM beginnt, von einem PXE-Server zu starten, der vorübergehend auf dem primären Knoten ausgeführt wird.
   - Das System löscht automatisch alle Daten auf Datenträgern in der Ersatz-PM.

- Die Ersatz-PM wird erneut neu gestartet und beginnt automatisch mit der Installation der Systemsoftware, wofür eine Kopie des Installations-Kits auf dem primären Knoten verwendet wird.

Sie brauchen den Fortschritt der Softwareinstallation nicht an der physischen Konsole der Ersatz-PM zu verfolgen oder auf Eingabeaufforderungen zu reagieren. Der Ersetzungsprozess ist automatisiert und es ist ganz normal, dass die PM für einen längeren Zeitraum während der Softwareinstallation nichts auf dem Bildschirm anzeigt.

10. Wenn die Softwareinstallation abgeschlossen ist, wird die Ersatz-PM mit der neu installierten Systemsoftware neu gestartet.

> **Hinweis**: Nach der Installation der Systemsoftware kann es bis zu 20 Minuten dauern, bis die PM in das System eingebunden ist und in der ztC Console zu sehen ist.

11. Während die Ersatz-PM in das System integriert wird, können Sie die Aktivität auf der Seite **Physische Maschinen** der ztC Console anzeigen. In der Spalte **Aktivität** wird der Zustand der PM als **(in Wartung)** und nach Abschluss der Ersetzung als **wird ausgeführt** angezeigt. Die PM verlässt den Wartungsmodus automatisch und beginnt mit der Lastverteilung der VMs im System.
12. Installieren Sie ggf. Anwendungen und andere Software auf Hostebene manuell und ändern Sie die Ersatz-PM-Konfiguration auf die ursprünglichen Einstellungen.

> **Hinweis**: Wenn die Ersatz-PM den Wartungsmodus verlässt, deaktiviert das System automatisch den PXE-Server auf dem primären Knoten, der für die Ersetzung verwendet wurde.

So können Sie eine ausgefallene PM wiederherstellen (mit USB-Installation)

Gehen Sie wie nachstehend beschrieben vor, um eine ausgefallene PM zu ersetzen und die Systemsoftware neu zu installieren, indem Sie einen USB-Stick verwenden.

1. Klicken Sie in der ztC Console im Navigationsbereich auf der linken Seite auf **Physische Maschinen**.

2. Wählen Sie die entsprechende PM (Knoten0 oder Knoten1) und klicken Sie dann auf **Wartung**. Dadurch wird der **Gesamtzustand** der PM in **Wartungsmodus** geändert und der **Aktivität**szustand ändert sich in **wird ausgeführt (in Wartung)**.
3. Wenn für die PM der Zustand **wird ausgeführt (in Wartung)** angezeigt wird, klicken Sie auf **Wiederherstellen**.
4. Wenn Sie aufgefordert werden, die Art der Reparatur auszuwählen, klicken Sie auf **USB-PM-Ersetzung - Alle Datenträger initialisieren**.

   Achtung: Wenn Sie **USB-PM-Ersetzung - Alle Datenträger initialisieren** wählen, werden alle Daten auf der Ersatz-PM gelöscht.
5. Klicken Sie auf **Weiter**, um mit der Ersetzung zu beginnen. Das System fährt die PM in Vorbereitung der Neuinstallation der Systemsoftware herunter.
6. Wenn die PM ausgeschaltet ist, installieren Sie die Ersatz-PM, falls erforderlich:
   a. Trennen und entfernen Sie die alte PM und installieren Sie dann die Ersatz-PM. Schließen Sie Monitor und Tastatur an.
   b. Bringen Sie die Netzwerkkabel an ihren ursprünglichen Anschlüssen an.
   c. Schließen Sie das startfähige USB-Medium an die Ersatz-PM an und schließen Sie das Stromkabel wieder an. Falls die PM nicht automatisch eingeschaltet wird, betätigen Sie die Ein/aus-Taste.
7. Wenn die Ersatz-PM hochgefahren wird, rufen Sie das Setup-Utility für die Firmware (UEFI) auf. Wählen Sie im Menü **Save & Exit** unter **Boot Override** den Eintrag **UEFI** für das USB-Medium aus, damit das Gerät bei der nächsten Startsequenz vom USB-Stick gestartet wird. Die PM wird neu gestartet.

   Hinweis: Verwenden Sie die Eigenschaft **Boot Override**, um das Startgerät nur vorübergehend zu ändern, statt dauerhaft mit **BOOT ORDER Priorities** im **Boot**-Menü. Die oberste Priorität muss **UEFI Network** (Standardeinstellung) bleiben, damit der automatisierte Knotenaustausch unterstützt wird, der typischerweise auf ztC Edge-Systemen ausgeführt wird.
8. Überwachen Sie den Fortschritt der Softwareinstallation an der physischen Konsole der Ersatz-PM.

9. Wenn der Begrüßungsbildschirm **Welcome** angezeigt wird, wählen Sie mit den Pfeiltasten ein Tastaturlayout für die Installation aus.
10. Wählen Sie im Bildschirm **Install or Recovery** (Installation oder Wiederherstellung) die Option **Replace PM, Join system: Initialize Data** (PM ersetzen, Mit System verbinden: Daten initialisieren) und drücken Sie die **Eingabetaste**. Der Ersetzungsprozess läuft ohne Eingreifen des Benutzers ab.

> **Achtung**: Wenn Sie **Replace PM, Join system: Initialize Data** (PM ersetzen, Mit System verbinden: Daten initialisieren) wählen, werden alle Daten auf der Ersatz-PM gelöscht.

11. Wenn die Softwareinstallation abgeschlossen ist, wird die Ersatz-PM mit der neu installierten Systemsoftware neu gestartet.

> **Hinweis**: Nach der Installation der Systemsoftware kann es bis zu 20 Minuten dauern, bis die PM in das System eingebunden ist und in der ztC Console zu sehen ist.

12. Während die Ersatz-PM in das System integriert wird, können Sie die Aktivität auf der Seite **Physische Maschinen** der ztC Console anzeigen. In der Spalte **Aktivität** wird der Zustand der PM als **(in Wartung)** und nach Abschluss der Ersetzung als **wird ausgeführt** angezeigt. Die PM verlässt den Wartungsmodus automatisch und beginnt mit der Lastverteilung der VMs im System.
13. Installieren Sie ggf. Anwendungen und andere Software auf Hostebene manuell und ändern Sie die Ersatz-PM-Konfiguration auf die ursprünglichen Einstellungen.

Verwandte Themen

Wartungsmodus

Warten von physischen Maschinen

Die ztC Console

Physische Maschinen und virtuelle Maschinen

Die Seite „Physische Maschinen“

8

Kapitel 8: Überwachen des Systems, Windows-basierter VMs und Anwendungen

Auf Systemen, die für die Überwachung lizenziert sind, können Sie Informationen zur Leistung überwachen, zum Beispiel die CPU-Auslastung. Sie können Tiefst- und Höchstwerte festlegen, um einen Bereich von Parametern für die Überwachung zu erstellen. Außerdem können Sie eine Meldung für die Funktionen **Call-Home** und/oder **e-Alert** festlegen. Diese wird gesendet, wenn der Wert eines Parameters außerhalb des konfigurierten Bereichs liegt.

Sie können Informationen zu folgenden Elementen überwachen:

- Hostbetriebssystem des ztC Edge-Systems – siehe Überwachen des ztC Edge-Systems.
- Windows-Betriebssystem von Windows-basierten VMs – siehe Überwachen von Windows-basierten virtuellen Maschinen .
- Anwendungen, die auf Windows-basierten VMs laufen – siehe Überwachen von Anwendungen auf Windows-basierten virtuellen Maschinen.

Hinweis: Wenn das System nicht für die Überwachung lizenziert ist, werden die Inhalte der Registerkarte **Überwachen** grau angezeigt. Wenden Sie sich an Ihren Kundenbetreuer, um sich über die Aktivierung dieser Funktion zu informieren.

Informationen über die Überwachung eines Systems mit ztC Advisor, einem sicheren, webbasierten Portal, das zentrale Sichtbarkeit Ihrer gesamten Flotte von ztC Edge-Systemen bietet, finden Sie unter Aktivieren von ztC Advisor.

Überwachen des ztC Edge-Systems

Überwachen Sie das Hostbetriebssystem des ztC Edge-Systems auf Informationen zur Performance des Betriebssystems (zum Beispiel CPU-Auslastung). Nachdem Sie einen Überwachungsparameter festgelegt haben, wird der entsprechende Wert alle 30 Sekundenn aktualisiert.

So können Sie Parameter für die Überwachung des Hostbetriebssystems festlegen und anzeigen

1. Klicken Sie in der ztC Console im Navigationsbereich auf der linken Seite auf **Physische Maschinen**.
2. Klicken Sie im unteren Fensterbereich auf die Registerkarte **Überwachen**.

   Auf der Registerkarte **Überwachen** werden Informationen zu jedem laufenden Knoten angezeigt.
3. Um die Überwachung eines Parameters auf jedem laufenden Knoten zu aktivieren, wählen Sie das Kontrollkästchen **Aktivieren** für den entsprechenden Parameter in der Spalte ganz links aus.
4. Legen Sie ggf. die Parameterwerte fest:

   Parameter – **CPU-Nutzung** und **Arbeitsspeicher-Nutzung**. Anzeigewert (kann nicht festgelegt werden).

   Einheiten – Prozentwert (%), der maximale Wert ist 100 %. Anzeigewert (kann nicht festgelegt werden).

   Bereich:

   Niedrig – Der untere Grenzwert des Bereichs. Der Wert kann 0 oder eine beliebige positive Zahl sein. Der Wert gilt für beide Knoten.

   Hoch – Der obere Grenzwert des Bereichs. Der Wert kann 0 oder eine beliebige positive Zahl sein. Der Wert muss größer als der Wert für **Niedrig** sein. Der Wert gilt für beide Knoten.

   Standardmäßig sind beide Bereichswerte leer. Um einen Wert einzugeben, klicken Sie auf die Zelle in der Spalte **Niedrig** oder **Hoch** der Parameterzeile. Nachdem Sie auf die Zelle geklickt haben, wird ein Feld angezeigt, in das Sie einen Wert eingeben können.

   CallHome – Es wird eine Call-Home-Nachricht an Ihren autorisierten Stratus-Servicemitarbeiter gesendet, wenn an einem Knoten ein Wert außerhalb des Bereichs erkannt wird.

   e-Alert/Trap – Es wird ein E-Mail-Alarm (e-Alert) und eine SNMP-Trap gesendet, wenn an einem Knoten ein Wert außerhalb des Bereichs erkannt wird.

Zuerst gesehen - Datum und Uhrzeit des Zeitpunkts, zu dem der Parameter zum ersten Mal innerhalb der letzten 24 Stunden an einem einzelnen Knoten erkannt wurde. Anzeigewert (kann nicht festgelegt werden).

Zuletzt gesehen - Datum und Uhrzeit des Zeitpunkts, zu dem der Parameter zum letzten Mal innerhalb der letzten 24 Stunden an einem einzelnen Knoten erkannt wurde. Anzeigewert (kann nicht festgelegt werden).

Letztes Ereignis - Die letzte Schwellenwertüberschreitung an einem Knoten: **Niedrig** oder **Hoch**. Wenn die Zelle leer ist, wurde der Schwellenwert nicht über- bzw. unterschritten. Anzeigewert (kann nicht festgelegt werden).

Anzahl Vorkommnisse - Wie oft der Schwellenwert innerhalb der letzten 24 Stunden an einem Knoten über- bzw. unterschritten wurde. Anzeigewert (kann nicht festgelegt werden).

Aktueller Wert - Zeigt eine der folgenden Angaben an (Anzeigewert; kann nicht festgelegt werden).

- Aktueller Wert für einen Knoten.
- **Nicht verfügbar** = Dieser Wert ist zurzeit nicht verfügbar.

Status - Status des Parameters an einem Knoten. Anzeigewert (kann nicht festgelegt werden).

- Erwartungsgemäß () = Der Parameter lag innerhalb der letzten 24 Stunden nicht außerhalb des Bereichs.
- Warnung () = Der Parameter lag innerhalb der letzten 24 Stunden außerhalb des Bereichs, im Moment ist dies aber nicht der Fall.
- Außerhalb des Bereichs () = Zurzeit außerhalb des Bereichs.

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder klicken Sie auf **Zurücksetzen**, um die noch nicht gespeicherten Änderungen zu verwerfen.

Verwandte Themen

Überwachen des Systems, Windows-basierter VMs und Anwendungen

Konfigurieren von e-Alerts

Konfigurieren der SNMP-Einstellungen

Verwalten von physischen Maschinen

Überwachen von Windows-basierten virtuellen Maschinen

Überwachen Sie das Betriebssystem auf Windows-basierten VMs auf Informationen zur Performance des Betriebssystems (zum Beispiel CPU-Nutzung). Die Überwachung ist auf VMs mit den folgenden Betriebssystemen möglich:

- Windows 7 Professional
- Windows 10 Professional
- Windows 10 Enterprise
- Windows Server 2012 R2 Standard
- Windows Server 2016 Standard

Nachdem Sie Windows-basierte VMs erstellt haben, können Sie auf der Registerkarte **Überwachen** der Seite **Virtuelle Maschinen** Überwachungsparameter hinzufügen. Nachdem Sie einen Überwachungsparameter festgelegt haben, wird der entsprechende Wert alle 60 Sekundenn aktualisiert.

Falls der Gast-Überwachungs-Agent noch nicht installiert wurde, müssen Sie diesen als Erstes installieren.

So installieren Sie den Gast-Überwachungs-Agent

1. Klicken Sie in der ztC Console auf **Virtuelle CDs**.
2. Vergewissern Sie sich, die VCD **guest_monitoring_agent_*n.n.n.n*** aufgeführt wird.
3. Klicken Sie im linken Fensterbereich auf **Virtuelle Maschinen**.
4. Wählen Sie unter **Virtuelle Maschinen** die VM aus, auf der Sie den Gast-Überwachungs-Agent installieren möchten.
5. Legen Sie die VCD ein. Siehe Einlegen einer virtuellen CD.
6. Öffnen Sie eine VM-Konsolensitzung. Siehe Öffnen einer VM-Konsolensitzung.
7. Öffnen Sie in der VM-Konsolensitzung ein Dateiexplorer-Fenster und navigieren Sie zur CD *Monitoring Agent Installation*.
8. Doppelklicken Sie auf die CD, um den **Monitoring Agent Service Setup-Assistenten** zu öffnen, und klicken Sie im Assistenten auf **Weiter**.

   Der Assistent installiert den Agent. Klicken Sie nach Abschluss der Installation auf **Fertigstellen**.
9. Werfen Sie die VCD nach Abschluss der Installation aus der VM aus. Siehe Auswerfen einer virtuellen CD.

Hinweise:

1. Wenn eine VM umbenannt wird, sind die Überwachungsparameter für eine oder zwei Minuten nicht zu sehen, werden dann aber wieder angezeigt.
2. Im Gastbetriebssystem müssen Performancezähler aktiviert und funktionsfähig sein, damit der Gast-Überwachungs-Agent Informationen zu Prozessor-, Arbeitsspeicher- und Datenträgernutzung abrufen kann.

So können Sie Parameter für die Überwachung einer VM festlegen und anzeigen

1. Klicken Sie in der ztC Console im Navigationsbereich auf der linken Seite auf **Virtuelle Maschinen**.
2. Wählen Sie die gewünschte VM aus.
3. Klicken Sie im unteren Fensterbereich auf die Registerkarte **Überwachen**.

   Unter **Gast-Betriebssystem** werden auf der Registerkarte Parameter angezeigt, die Sie anzeigen und festlegen können.
4. Um die Überwachung eines Parameters zu aktivieren, wählen Sie das Kontrollkästchen **Aktivieren** in der Spalte ganz links aus.
5. Legen Sie ggf. die Parameterwerte fest:

   Parameter - **CPU-Nutzung**, **Belegter Speicherplatz** und **Arbeitsspeicher-Nutzung**. Anzeigewert (kann nicht festgelegt werden).

   Einheiten - Prozentwert (%). Anzeigewert (kann nicht festgelegt werden).

   Bereich:

   Niedrig - Der untere Grenzwert des Bereichs. Der Wert muss einen positive Ganzzahl zwischen 0 und 100 (für 100 %) sein.

   Hoch - Der obere Grenzwert des Bereichs. Der Wert muss eine positive Ganzzahl zwischen 0 und 100 (für 100 %) sein, und der Wett muss größer als der Wert für **Niedrig** sein.

   Standardmäßig sind beide Bereichswerte leer. Um einen Wert einzugeben, klicken Sie auf die Zelle in der Spalte **Niedrig** oder **Hoch** der Parameterzeile. Nachdem Sie auf die Zelle geklickt haben, wird ein Feld angezeigt, in das Sie einen Wert eingeben können.

   CallHome - Es wird eine Call-Home-Nachricht an Ihren autorisierten Stratus-Servicemitarbeiter gesendet, wenn ein Wert außerhalb des Bereichs erkannt wird.

e-Alert/Trap - Es wird ein E-Mail-Alarm (e-Alert) und eine SNMP-Trap gesendet, wenn ein Wert außerhalb des Bereichs erkannt wird.

Zuerst gesehen - Datum und Uhrzeit des Zeitpunkts, zu dem der Parameter zum ersten Mal innerhalb der letzten 24 Stunden erkannt wurde. Anzeigewert (kann nicht festgelegt werden).

Zuletzt gesehen - Datum und Uhrzeit des Zeitpunkts, zu dem der Parameter zum letzten Mal innerhalb der letzten 24 Stunden erkannt wurde. Anzeigewert (kann nicht festgelegt werden).

Letztes Ereignis - Die letzte Schwellenwertüberschreitung an einem Knoten: **Niedrig** oder **Hoch**. Wenn die Zelle leer ist, wurde der Schwellenwert nicht über- bzw. unterschritten. Anzeigewert (kann nicht festgelegt werden).

Anzahl Vorkommnisse - Wie oft der Schwellenwert innerhalb der letzten 24 Stunden über- bzw. unterschritten wurde. Anzeigewert (kann nicht festgelegt werden).

Aktueller Wert - Zeigt eine der folgenden Angaben an (Anzeigewert; kann nicht festgelegt werden):

- Aktueller Wert.
- **Antwortet nicht** = Der Gast-Überwachungs-Agent antwortet auf dieser VM nicht, da der Agent entweder beendet oder nicht installiert wurde. Um den Gast zu überwachen, müssen Sie den Gast-Überwachungs-Agent manuell auf dieser VM installieren oder neu starten.
- **Wird nicht ausgeführt** = Der Gast wird nicht ausgeführt.
- **Nicht verfügbar** = Dieser Wert ist zurzeit nicht verfügbar.

Status - Anzeigewert (kann nicht festgelegt werden).

- Erwartungsgemäß () = Der Parameter lag innerhalb der letzten 24 Stunden nicht außerhalb des Bereichs.
- Warnung () = Der Parameter lag innerhalb der letzten 24 Stunden außerhalb des Bereichs, im Moment ist dies aber nicht der Fall.
- Außerhalb des Bereichs () = Zurzeit außerhalb des Bereichs.

6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder klicken Sie auf **Zurücksetzen**, um die noch nicht gespeicherten Änderungen zu verwerfen.

Verwandte Themen

Überwachen des Systems, Windows-basierter VMs und Anwendungen

Konfigurieren von e-Alerts

Konfigurieren der SNMP-Einstellungen

Konfigurieren von Windows-basierten virtuellen Maschinen

Überwachen von Anwendungen auf Windows-basierten virtuellen Maschinen

Überwachen Sie Anwendungen, die auf Windows-basierten VMs ausgeführt werden, auf Informationen zur Anwendungsleistung (zum Beispiel CPU-Nutzung).

Nachdem Sie Windows-basierte VMs erstellt haben, können Sie auf der Registerkarte **Überwachen** der Seite **Virtuelle Maschinen** Anwendungen hinzufügen und dann Überwachungsparameter anzeigen und festlegen. Nachdem Sie einen Überwachungsparameter festgelegt haben, wird der entsprechende Wert alle 60 Sekundenn aktualisiert.

Hinweis: Wenn eine VM umbenannt wird, sind die Überwachungsparameter für eine oder zwei Minuten nicht zu sehen, werden dann aber wieder angezeigt.

Damit Sie Anwendungsparameter für die Überwachung hinzufügen oder anzeigen bzw. einen Parameter entfernen können, muss Ihnen der Name der ausführbaren Datei der Anwendung bekannt sein (ohne die Erweiterung, zum Beispiel mysqld). Den Namen finden Sie in einem Windows-Dienstprogramm. Sie können zum Beispiel im **Task-Manager** auf der Registerkarte **Prozesse** (oder Details) den richtigen Namen einer Anwendung ermitteln.

So können Sie eine Anwendung und ihre Parameter hinzufügen, festlegen oder anzeigen

1. Klicken Sie in der ztC Console im Navigationsbereich auf der linken Seite auf **Virtuelle Maschinen**.
2. Wählen Sie die VM aus, auf der die gesuchte Anwendung ausgeführt wird.
3. Klicken Sie im unteren Fensterbereich auf die Registerkarte **Überwachen**.

   Der Bereich **Anwendungen** wird unter dem Bereich **Gast-Betriebssystem** angezeigt. In der Spalte **Anwendung** sind die Anwendungen mit den zugehörigen Parametern aufgeführt. Unterhalb der Liste befinden sich die Schaltflächen „Hinzufügen“ und „Entfernen“, mit denen Sie der Liste Anwendungen und Parameter hinzufügen bzw. diese entfernen können.
4. **Fügen Sie ggf. eine Anwendung und Parameter hinzu:**

a. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Es werden zwei Felder angezeigt; der Cursor befindet sich im ersten Feld (links).

b. Geben Sie den Namen der ausführbaren Datei der Anwendung (ohne die Dateinamenserweiterung, zum Beispiel mysqld) in das erste Feld ein oder wählen Sie einen Namen aus der Dropdownliste aus.

c. Wählen Sie den Parameter, den Sie überwachen möchten, aus der Dropdownliste im zweiten Feld (rechts) aus.

d. Klicken Sie auf **Speichern**, um die Änderungen zu speichern (oder klicken Sie auf **Zurücksetzen**, um die noch nicht gespeicherten Änderungen zu verwerfen). Nachdem Sie die Änderungen gespeichert haben, wird die neue Anwendung in der Liste unter **Anwendungen** angezeigt.

Es dauert einen kurzen Moment, bis die neue Anwendung aufgeführt wird.

5. Um die Überwachung einer Anwendung und ihrer Parameter zu aktivieren, wählen Sie das Kontrollkästchen **Aktivieren** in der Spalte ganz links aus.
6. Legen Sie ggf. die Parameterwerte fest:

Anwendung - Anwendungen, die auf der VM ausgeführt werden und für die Überwachung ausgewählt wurden.

Parameter - **CPU-Nutzung** und **Arbeitsspeicher-Nutzung**. Anzeigewert (kann nicht festgelegt werden).

Einheiten - Prozentwert (%). Anzeigewert (kann nicht festgelegt werden).

Bereich:

Niedrig - Der untere Grenzwert des Bereichs. Der Wert muss einen positive Ganzzahl zwischen 0 und 100 (für 100 %) sein.

Hoch - Der obere Grenzwert des Bereichs. Der Wert muss eine positive Ganzzahl zwischen 0 und 100 (für 100 %) sein, und der Wett muss größer als der Wert für **Niedrig** sein.

Standardmäßig sind beide Bereichswerte leer. Um einen Wert einzugeben, klicken Sie auf die Zelle in der Spalte **Niedrig** oder **Hoch** der Parameterzeile. Nachdem Sie auf die Zelle geklickt haben, wird ein Feld angezeigt, in das Sie einen Wert eingeben können.

CallHome - Es wird eine Call-Home-Nachricht an Ihren autorisierten Stratus-Servicemitarbeiter gesendet, wenn ein Wert außerhalb des Bereichs erkannt wird.

e-Alert/Trap - Es wird ein E-Mail-Alarm (e-Alert) und eine SNMP-Trap gesendet, wenn ein Wert außerhalb des Bereichs erkannt wird.

Zuerst gesehen - Datum und Uhrzeit des Zeitpunkts, zu dem der Parameter zum ersten Mal innerhalb der letzten 24 Stunden erkannt wurde. Anzeigewert (kann nicht festgelegt werden).

Zuletzt gesehen - Datum und Uhrzeit des Zeitpunkts, zu dem der Parameter zum letzten Mal innerhalb der letzten 24 Stunden erkannt wurde. Anzeigewert (kann nicht festgelegt werden).

Letztes Ereignis - Die letzte Schwellenwertüberschreitung an einem Knoten: **Niedrig** oder **Hoch**. Wenn die Zelle leer ist, wurde der Schwellenwert nicht über- bzw. unterschritten. Anzeigewert (kann nicht festgelegt werden).

Anzahl Vorkommnisse - Wie oft der Schwellenwert innerhalb der letzten 24 Stunden über- bzw. unterschritten wurde. Anzeigewert (kann nicht festgelegt werden).

Aktueller Wert - Zeigt eine der folgenden Angaben an (Anzeigewert; kann nicht festgelegt werden):

- Aktueller Wert.
- **Antwortet nicht** = Der Gast-Überwachungs-Agent antwortet auf dieser VM nicht, da der Agent entweder beendet oder nicht installiert wurde. Um Anwendungen auf dem Gast zu überwachen, müssen Sie den Gast-Überwachungs-Agent manuell auf dieser VM installieren oder neu starten.
- **Wird nicht ausgeführt** = Der Gast wird nicht ausgeführt.
- **Nicht gefunden** = Die Anwendung wurde nicht gefunden oder wird auf dem Gast nicht ausgeführt.
- **Nicht verfügbar** = Dieser Wert ist zurzeit nicht verfügbar.

Status - Anzeigewert (kann nicht festgelegt werden).

- Erwartungsgemäß () = Der Parameter lag innerhalb der letzten 24 Stunden nicht außerhalb des Bereichs.
- Warnung () = Der Parameter lag innerhalb der letzten 24 Stunden außerhalb des Bereichs, im Moment ist dies aber nicht der Fall.
- Außerhalb des Bereichs () = Zurzeit außerhalb des Bereichs.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder klicken Sie auf **Zurücksetzen**, um die noch nicht gespeicherten Änderungen zu verwerfen. Nach einem kurzen Moment werden die neu eingegebenen Werte (falls zutreffend) angezeigt.

So entfernen Sie einen Parameter

1. Klicken Sie in der ztC Console im Navigationsbereich auf der linken Seite auf **Virtuelle Maschinen**.
2. Wählen Sie die VM aus, auf der die Anwendung ausgeführt wird, deren Parameter sie entfernen möchten.
3. Klicken Sie im unteren Fensterbereich auf die Registerkarte **Überwachen**. Der Bereich **Anwendungen** wird unter dem Bereich **Gast-Betriebssystem** angezeigt.
4. Wählen Sie eine Anwendung/Parameter-Zeile aus.
5. Klicken Sie auf die Schaltfläche **Entfernen**.

   Die Zeile mit der Anwendung/dem Parameter wird aus der Liste der Anwendungen entfernt.
6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern (oder klicken Sie auf **Zurücksetzen**, um die noch nicht gespeicherten Änderungen zu verwerfen). Nach einem kurzen Moment wird die Zeile mit der Anwendung/dem Parameter (erneut) aus der Liste der Anwendungen entfernt.

Verwandte Themen

Überwachen des Systems, Windows-basierter VMs und Anwendungen

Konfigurieren von e-Alerts

Konfigurieren der SNMP-Einstellungen

Installieren von Anwendungen (Windows-basierte VMs)

Konfigurieren von Windows-basierten virtuellen Maschinen

Teil 2: Ergänzende Dokumentation

In der folgenden ergänzenden Dokumentation finden Sie Versionshinweise, Referenzen und Informationen zur Fehlerbehebung.

- Stratus Redundant Linux Version 2.2.0.0 Versionshinweise
- Systemreferenzinformationen
- Sicherheit
- SNMP

9

Kapitel 9: Stratus Redundant Linux Version 2.2.0.0 Versionshinweise

Diese Versionshinweise (aktualisiert um 15:21 am 25.11.2020) gelten für Stratus Redundant Linux Version 2.2.0.0 auf ztC Edge-Systemen. (Die neueste Version dieser Versionshinweise einschließlich einer Liste der nach der letzten Übersetzung vorgenommenen Änderungen finden Sie in englischer Sprache unter StrataDOC.) Weitere Informationen finden Sie in den folgenden Abschnitten:

- Neue Funktionen und Verbesserungen
- Bug-Fixes
- CVE-Fixes
- Wichtige Überlegungen
- Bekannte Probleme
- Aktualisierte Dokumentation
- Zugriff auf Artikel in der Stratus Knowledge Base
- Hilfe

Neue Funktionen und Verbesserungen

Neu in Stratus Redundant Linux Version 2.2.0.0

Die folgenden Funktionen sind neu in Stratus Redundant Linux Version 2.2.0.0:

- ztC Advisor
- Host-Betriebssystem-Unterstützung – Unterstützung für CentOS 7.8 als Host-Betriebssystem für das ztC Edge-System unter Bereitstellung des Linux Kernel 3.10.0-1127.19.1.e17.x86_64.

- Sicherheitsverbesserungen:
  - 215 CVEs wurden behoben.
  - Informationen zur Sicherheitskonfiguration des Systems wurden konsolidiert. Siehe Sicherheit.
- Betrieb und Fehlerbehebung – Zusätzliche Aufrufe der REST API zur Überwachung der Systemintegrität und von Statistiken. Siehe REST API-Aufrufe.

Neu in Stratus Redundant Linux Version 2.1.0.0

Weitere Informationen finden Sie unter Neu in Stratus Redundant Linux Version 2.1.0.0.

Bug-Fixes

In Stratus Redundant Linux Version 2.2.0.0 behobene Bugs

ZTC-3175: Der Nessus-Scan identifiziert veraltete SSL-Protokolle an Port 5560. (Die veralteten Protokolle wurden entfernt.)

ZTC-3171: SSH Cipher-Einstellungen bestehen nicht alle Sicherheitsprüfungen. (Die Einstellungen wurden geändert, um mehr Sicherheit zu bieten und diese Prüfungen zu bestehen.)

ZTC-3017, ZTC-2257: Benutzer, deren Kennwort Sonderzeichen enthält, können nicht in Active Directory (AD) aufgenommen werden. (AD-Benutzernamen und Kennwörter, die Sonderzeichen wie „$“, „!“, „&“ und „<“ enthalten, werden jetzt beim Anmelden bei AD unterstützt.)

ZTC-2773: Der `lvmetad`-Daemon hat einen bekannten Speicher-Leak und ist veraltet. (Der Daemon wurde so konfiguriert, dass er nicht mehr ausgeführt wird.)

ZTC-2395, ZTC-2396: Der Qualys-Scan wird für QID 37839 und QID 38738 nicht bestanden. (Die SSH Einstellungen wurden geändert, um mehr Sicherheit zu bieten und diesen Scan zu bestehen.)

ZTC-2256: Das `mcelog`-Paket wird nicht standardmäßig installiert. (`mcelog` wird jetzt standardmäßig installiert.)

ZTC-2206: Der Qualys-Scan wird für QID 13162 nicht bestanden. (Der Session-Cookie enthält jetzt das secure-Attribut, sodass diese Prüfung bestanden wird.)

ZTC-1298: Windows-Gäste erleben Leistungsprobleme wegen einer fehlenden hypervclock-Einstellung. (Leistungsprobleme bei Windows 2016- und Windows 2019-Gästen wurden behoben, indem die hypervclock-Einstellungen zur Konfiguration hinzugefügt wurde.)

ZTC-962: Das von Stratus bereitgestellte SSL-Zertifikat hat ein Ablaufdatum von 2026. (Es wurde ein neues Zertifikat bereitgestellt, das 10 Jahre nach Ausstellungdatum abläuft, zum Beispiel 2030. Sie müssen das

neue Zertifikat akzeptieren, siehe Aktualisieren des Browsers und Akzeptieren des neuen Zertifikats während des Upgrades.)

ZTC-461: Nach einem Failover des primären Knotens ist keine Anmeldung bei Active Directory möglich.

ZTC-458: Gäste mit konfigurierter Startreihenfolge starten eventuell nicht.

ZTC-454: Nach einer Neuinstallation oder Wiederherstellung/Ersatz eines Knotens können root, swap oder diagdata als beschädigt angezeigt werden.

ZTC-453: Wenn ein Gast nicht starten kann, sollte ein Alarm generiert werden.

In Stratus Redundant Linux Version 2.1.0.0 behobene Bugs

Weitere Informationen finden Sie unter In Stratus Redundant Linux Version 2.1.0.0 behobene Bugs.

CVE-Fixes

Eine Liste der CVE-Fixes finden Sie unter Behobene CVEs.

Wichtige Überlegungen

Upgrade auf Version 2.2.0.0

Führen Sie ein Upgrade auf Stratus Redundant Linux Release 2.2.0.0 durch, indem Sie dem Upgrade-Pfad für die aktuell auf Ihrem System ausgeführte Version folgen:

- Versionen 2.1.0.0, 2.0.1.0 und 2.0.0.0 – Aktualisieren Sie direkt auf Version 2.2.0.0 wie unter Upgrade der Stratus Redundant Linux-Software mit einem Upgrade-Kit beschrieben.
- Ältere Versionen als Version 2.0.0.0 – Aktualisieren Sie zunächst auf Version 2.0.1.0 und dann auf Version 2.2.0.0. Informationen zum Upgrade auf Version 2.0.1.0 finden Sie in den Versionshinweisen zu Version 2.0.1.0 und in der Hilfe.

Version der Systemsoftware bestimmen

Um festzustellen, welche Stratus Redundant Linux-Version auf einem ztC Edge-System ausgeführt wird, melden Sie sich bei der ztC Console des Systems an und überprüfen Sie die Systeminformationen in der Titelleiste:

```
ocean.abc.com
IP: 123.109.50.34 | Asset ID: ze-12345
Version: n.n.n-nnn
```

Alternativ dazu können Sie auf **Softwareupdates** auf der Seite **Voreinstellungen** klicken. Dann wird auch die aktuelle Versionsnummer der Stratus Redundant Linux-Software auf Ihrem System angezeigt.

Wenn die Softwareversion niedriger als Version 2.2.0.0 ist, laden Sie das Stratus Redundant Linux 2.2.0.0 Upgrade-Kit von der Seite **Downloads** unter https://www.stratus.com/services-support/downloads/?tab=ztcedge herunter und führen Sie ein Upgrade der Software aus. Dies wird unter Upgrade der Stratus Redundant Linux-Software mit einem Upgrade-Kit beschrieben.

Aktualisieren des Browsers und Akzeptieren des neuen Zertifikats während des Upgrades

Während eines Upgrades auf Version 2.2.0.0 zeigt der Browser das Upgrade möglicherweise als angehalten an, nachdem der erste Knoten aktualisiert und zum neuen primären Knoten wurde. Diese falsche Browseranzeige kann auftreten, wenn der Browser ein neues Zertifikat von Stratus erhalten hat, das akzeptiert werden muss. Sie sollten den Browser aktualisieren und, wenn Sie dazu aufgefordert werden, das neue Zertifikat akzeptieren. Nachdem Sie das neue Zertifikat akzeptiert haben, zeigt der Browser den korrekten Status des Upgrades an.

Verwendung der Intel Active Management Technology (AMT) für die Unterstützung des Lights-Out Managements (LOM)

ztC Edge-Systeme bieten Intel Active Management Technology (AMT) LOM-Unterstützung für die Remote-Energieverwaltung, Remote-Konsole und Remote-Medien. Weitere Informationen zur AMT-Konfiguration und zu entsprechenden Einschränkungen finden Sie unter KB-8219.

Bereitstellen von ztC Edge-Knoten an separaten physischen Standorten

Wenn Sie ein ztC Edge-System bereitstellen, müssen Sie beide Knoten am selben Standort bereitstellen und die A-Links zwischen den blauen (**A2**) und gelben (**A1**) Netzwerkports beider Knoten direkt verbinden. Wenn Sie ein ztC Edge-System in einer ALSR-Konfiguration (Automated Local Site Recovery) einrichten möchten, bei der sich jeder Knoten an einem separaten physischen Standort befindet, um die Redundanz zu verbessern, wenden Sie sich an Ihren autorisierten Stratus-Servicemitarbeiter. Aufgrund der räumlichen Trennung muss in einer ALSR-Konfiguration sorgfältig geplant werden, wo Komponenten platziert werden und wie die Netzwerktopologie gestaltet wird.

Aktivieren von ztC Advisor

Stratus Redundant Linux Version 2.2.0.0 oder höher führt Unterstützung für ztC Advisor, ein sicheres, webbasiertes Portal, das zentrale Sichtbarkeit Ihrer gesamten Flotte von ztC Edge-Systemen bietet, ein.

Über ein intuitives und benutzerfreundliches Dashboard können Sie die Integrität, die Ressourcennutzung und die Softwareversion jedes Systems auf einen Blick beurteilen.

Informationen über die Registrierung für und Verwendung von ztC Advisor finden Sie auf der folgenden Webseite: https://www.stratus.com/solutions/ztc-advisor. Wie Sie ztC Advisor für ein System aktivieren oder deaktivieren, finden Sie unter Aktivieren von ztC Advisor.

Getestete Gastbetriebssysteme

Eine Liste der mit der aktuellen Version getesteten Gastbetriebssysteme finden Sie unter Getestete Gastbetriebssysteme.

Ein Einzelknotensystem kann sich während eines Kit-Upgrades nicht im Wartungsmodus befinden

Vergewissern Sie sich, dass sich das System nicht im Wartungsmodus befindet, bevor Sie auf einem Einzelknotensystem ein Kit-Ugrade starten. Wenn sich ein Einzelknotensystem beim Start des Kit-Upgrades im Wartungsmodus befindet, kann das System den Wartungsmodus nicht beenden.

Bekannte Probleme

Installation des seriellen VirtIO-Treibers schlägt fehl, nachdem eine Windows 2008 (SP2, 32-Bit) VM erstellt wurde

Nachdem eine Windows 2008 SP2 (32-Bit) VM erstellt wurde, kann der serielle VirtIO-Treiber nicht installiert werden. Installieren Sie den Treiber in diesem Fall manuell. Laden Sie dazu die VirtIO-ISO-Datei herunter. Sie ist verfügbar auf der Seite **Downloads** unter https://www.stratus.com/services-support/downloads/?tab=ztcedge. Befolgen Sie Anleitung unter Aktualisieren der VirtIO-Treiber (Windows-basierte VMs), wählen Sie jedoch den seriellen Treiber aus (vioser). Beachten Sie, dass dieses Problem nur mit der 64-Bit-Version von Windows 2008 SP2 auftritt.

Wechselmedien und Migration einer PM oder VM mithilfe des P2V-Clients

Prüfen Sie vor der Migration einer PM oder VM mithilfe einer startfähigen ISO-Datei des P2V-Clients (**virt-p2v**), ob irgendwelche Wechselmedien (zum Beispiel Disketten, DVD-Laufwerke oder externe USB-Datenträger) mit dem Quellenabbild verbunden sind. Falls Wechselmedien mit dem Quellenabbild verbunden sind, wenn Sie die Migration einer PM oder VM versuchen, erscheint die Fehlermeldung **Conversion failed** (Konvertierung fehlgeschlagen). Heben Sie daher die Auswahl des Mediums im Fenster **virt-p2v** auf, bevor Sie die Migration starten. Rufen Sie dazu das Fenster **virt-p2v** mit den Abschnitten **Target properties**

(Zieleigenschaften) und **Fixed hard disks** (Festplatten) auf und entfernen Sie dann unter **Fixed hard disks** (Festplatten) die Markierung des Kästchens in der Spalte **Convert** (Konvertieren) neben dem Wechselmedium. Weitere Informationen zur Verwendung von **virt-p2v** finden Sie unter Migrieren einer physischen oder virtuellen Maschine in ein System, insbesondere im Abschnitt **So migrieren Sie eine PM oder VM in das ztC Edge-System**.

Maximale Pfadlänge beim Importieren einer VM

Wenn Sie eine VM mithilfe des **Assistenten zum Importieren/Wiederherstellen einer VM** importieren, beträgt die maximale Länge des Pfads zur VM einschließlich des VM-Namens 4096 Zeichen für die Importoptionen **Import aus Remote-/Netzwerk-Windows-Freigabe (CIFS/SMB)** und **Import aus Remote-/Netzwerk-NFS**.

Importieren einer OVA-Datei schlägt manchmal fehl

Wenn Sie beginnen, eine OVA-Datei zu importieren, und der Knoten dann in den Wartungsmodus versetzt wird oder von der Stromversorgung getrennt wird, schlägt der OVA-Import fehl wie auch alle weiteren Versuche, eine OVA-Datei zu importieren. Weitere Informationen dazu, wie Sie dieses Problem umgehen, finden Sie in KB-10034.

Manuelle Konfiguration der Netzwerkinformationen nach dem Import einer Linux-VMware-OVA-Datei

Beim Import einer Linux-VMware-OVA-Datei werden die Netzwerkschnittstelle und die `networks-scripts`-Datei geändert. Nachdem Sie die Datei importiert haben, müssen Sie die Netzwerkinformationen manuell konfigurieren. Gehen Sie dabei folgendermaßen vor:

1. Wählen Sie die VM auf der Seite **Virtuelle Maschinen** aus.
2. Klicken Sie im unteren Fensterbereich auf **Konsole**, um die VM-Anmeldeseite zu öffnen (weitere Informationen finden Sie unter Öffnen einer VM-Konsolensitzung).
3. Melden Sie sich bei der VM an.
4. Öffnen Sie eine Eingabeaufforderung (Befehlszeile).
5. Führen Sie den Befehl `ifconfig` aus. Prüfen Sie in der Befehlsausgabe, ob `ip address` der virtuellen Netzwerkschnittstelle `eth0` zugewiesen ist.
6. Wenn `ip address` nicht zu `eth0` zugewiesen ist, listen Sie den Inhalt des Verzeichnisses `/etc/sysconfig/network-scripts` auf.

7. Notieren Sie sich den Wert von `ifcfg-xxxx` (aber nicht von `ifcfg-lo`).
8. Benennen Sie `ifcfg-xxxx` in `ifcfg-eth0` um.
9. Bearbeiten Sie die Datei `ifcfg-eth0`, indem Sie die Werte von `DEVICE` und `ONBOOT` wie folgt ändern:

   ```
   DEVICE=eth0
   ONBOOT=yes
   ```

   Speichern Sie die Datei.
10. Geben Sie den folgenden Befehl ein, um die Netzwerkdienste neu zu starten:

    ```
    systemctl restart network
    ```
11. Überprüfen Sie die IP-Zuweisung, indem Sie den Befehl `ifconfig` ausführen. Prüfen Sie in der Befehlsausgabe, ob `ip address` jetzt `eth0` zugewiesen ist.

Suche bei „Import über USB“ listet OVA-Dateien in verschiedenen Verzeichnissen auf

Wenn Sie im Assistenten **Virtuelle Maschine importieren/wiederherstellen** die Option **Import über USB** auswählen, um eine OVA-Datei zu importieren, können Sie einen Dateinamen (vollständig oder teilweise) in das Feld *In Dateien suchen* eingeben. Es werden OVA-Dateien aufgelistet, deren Name mit Ihrer Eingabe übereinstimmt und die sich in verschiedenen Verzeichnissen befinden:

- Mit dem übergeordneten Verzeichnis (root) als Suchverzeichnis werden Dateien aufgeführt, die sich im übergeordneten Verzeichnis (root) oder in dessen Unterverzeichnissen befinden.
- Mit einem untergeordneten Verzeichnis als Suchverzeichnis werden Dateien aufgeführt, die sich in diesem Unterverzeichnis oder im übergeordneten Verzeichnis (root) befinden.

Ausführliche Informationen zum Importieren von OVA-Dateien finden Sie unter Importieren einer OVF- oder OVA-Datei.

Import von RHEL 8.1-VMs nicht möglich

Sie können eine VM, auf der RHEL 8.1 (mit BIOS-Start-Firmware) ausgeführt wird, nicht von einem VMware ESXi 6.7.0-Server in ein ztC Edge-System importieren.

Maximale Auflösung einer UEFI VM-Konsolensitzung

Auf der Seite **Virtuelle Maschinen** der ztC Console können Sie eine VM-Konsolensitzung öffnen, um die Konsole des Gastbetriebssystems anzuzeigen, das auf der VM ausgeführt wird. Wenn Sie eine

Konsolensitzung öffnen, um auf eine Gast-VM mit dem Starttyp UEFI zuzugreifen, hat die Konsolensitzung eine maximale Auflösung von 800x600. Um eine höhere Auflösung anzuzeigen, verbinden Sie sich über eine Remotedesktopverbindung mit der VM.

VMs für `vmgenid`-Unterstützung neu starten

Nachdem ein System mit einem Upgrade-Kit von Version 2.0.1.0 (oder früher) auf Stratus Redundant Linux Version 2.2.0.0 aktualisiert wurde, ist die Unterstützung für `vmgenid` auf VMs mit Windows Server 2019, Windows Server 2016 oder Windows Server 2012 nicht vorhanden, bis die VMs neu gestartet wurden. Sie müssen diese VMs also neu starten, um die Unterstützung von `vmgenid` nach dem Upgrade zu aktivieren. Wenn Sie ein Upgrade von Version Release 2.1.0.0 ausführen, brauchen Sie solche VMs nicht neu zu starten, falls sie zuvor in dem System mit Version 2.1.0.0 neu gestartet wurden.

VCDs können nicht erstellt werden, wenn Microsoft Edge als Konsolenbrowser verwendet wird

Wenn Sie Microsoft Edge als Browser für die ztC Console verwenden, können Sie keine VCD erstellen; der Prozess schlägt fehl. Verwenden Sie stattdessen einen anderen Browser (siehe Kompatible Internetbrowser).

Zum Importieren einer VMware-VM die Befehle zum Herunterfahren des Betriebssystems verwenden

Wenn Sie eine VMware-VM importieren, müssen Sie die VM nicht nur in der VMware-Konsole ausschalten, sondern auch mit dem Befehl „Herunterfahren“ des Betriebssystems herunterfahren. Wenn Sie die VM nur in der VMware-Konsole ausschalten, schlägt der Import fehl.

In einem Einzelknotensystem ist die Anzeige der hinzugefügten vCPUs im Assistenten zum Erstellen von VMs nicht korrekt

Wenn Sie in einem System, das für einen Knoten lizenziert ist, eine VM erstellen, zeigt der **Assistent zum Erstellen von VMs** an, dass zwei vCPUs zur von Ihnen angegebene Anzahl von vCPUs hinzugefügt werden. Sobald die VM erstellt wurde, wird die vom Benutzer angegebene Anzahl von vCPUs an die CM angeschlossen. Die beiden zusätzlichen (fälschlicherweise angezeigten) vCPUs werden nicht hinzugefügt.

Nach dem Upgrade auf ein Zweiknotensystem zeigen VMs ein Warnsymbol an

Wenn Sie ein System, das für einen Knoten lizenziert ist, auf ein System aktualisieren, das für zwei Knoten lizenziert ist, werden die VMs zwar weiterhin ausgeführt, im Dashboard wird der VM-Zustand jedoch mit einem Warnsymbol (⚠) angezeigt. Die Warnung gibt an, dass die VMs mit nur einem oder ohne A-Link laufen, da das System während des Upgrades A-Link1 nicht hinzufügt.

Um das Problem zu vermeiden, stoppen Sie die VMs vor dem Upgrade und starten Sie die VMs nach dem Upgrade neu. Wenn dieses Problem auftritt, stoppen Sie die VMs und starten Sie sie nach dem Upgrade neu.

Tastenzuordnung von japanischen Tastaturen 106 und 109 für die Konsole sind in IE10, IE11 oder Firefox möglicherweise nicht korrekt

Wenn IE10, IE11 oder Firefox für den Zugriff auf die ztC Console verwendet wird, ist die Tastenzuordnung der japanischen Tastaturen 106 und 109 möglicherweise nicht korrekt. Verwenden Sie stattdessen Chrome oder Software für eine Remoteverbindung (VNC oder RDP).

Migrieren einer VM mit Überwachung führt zu „Keine Antwort“

Wenn die Überwachung auf einer VM für alle drei Parameter (CPU, Arbeitsspeicher und Datenträger) eingestellt ist und die VM auf den anderen Knoten migriert wird, wird auf der Registerkarte **Überwachen** die Meldung **Keine Antwort vom Gast-Agent** angezeigt. Es kann mehrere Minuten dauern, bis der Gast-Agent wieder verbunden ist.

Wenn A-Link offline ist, werden VMs als „Beschädigt“ statt als „Beeinträchtigt“ angezeigt

Wenn ein A-Link-Kabel oder Netzwerk an einem Knoten getrennt wird, wird der Zustand einer VM auf diesem Knoten möglicherweise als „Beschädigt“ (✖) in der ztC Console angezeigt, obwohl die VM immer noch über eine andere aktive A-Link-Verbindung verfügt. Die Verfügbarkeit der VM ist davon nicht betroffen.

Bei einer Linux-basierten VM-Konsole wird eine ausgeworfene VCD immer noch angezeigt

Wenn Sie die ztC Console verwenden, um eine VCD aus einer VM auszuwerfen, die ein Linux-basiertes Gastbetriebssystem ausführt, wird die VCD im Gastbetriebssystem möglicherweise weiterhin angezeigt. Falls erforderlich, können Sie die VCD im Gastbetriebssystem auswerfen, damit sie nicht mehr angezeigt wird.

Einige Browser können keine VNC verbinden, wenn https verwendet wird

Wenn Sie mit der ztC Console verbunden sind und dafür eine **https**-URL in Microsoft Internet Explorer oder Mozilla® Firefox® verwenden und auf **Konsole** klicken, nachdem Sie eine laufende VM auf der Seite **Virtuelle Maschinen** ausgewählt haben, wird möglicherweise die Meldung **VNC: Unable to connect. retrying in *n* seconds** (Es kann keine Verbindung hergestellt werden, erneuter Versuch in n Sekunden) angezeigt. Um die VNC-Verbindung zu aktivieren, klicken Sie auf den HTTPS-Link zur VNC-Konsolenseite oben rechts in der Titelleiste und fahren Sie mit dem passenden unten beschriebenen Verfahren fort (je nach Browserversion ist das Verfahren in Ihrem Browser möglicherweise abweichend):

- Im Internet Explorer wird der Assistent **Sicherheitswarnung** angezeigt:
    a. Klicken Sie auf **Weiter zu dieser Website (nicht empfohlen)**.
    b. Klicken Sie auf **OK**.
- In Firefox wird das Fenster **Die Verbindung ist nicht sicher** angezeigt:
    a. Klicken Sie auf **Erweitert**. Es wird eine Meldung über ein ungültiges Sicherheitszertifikat angezeigt.
    b. Klicken Sie auf **Ausnahme hinzufügen**. Das Dialogfeld **Sicherheitsausnahme hinzufügen** wird angezeigt, wobei als **Speicherort** der Speicherort der Konsole angegeben ist.
    c. Klicken Sie auf **Sicherheitsausnahme bestätigen**.

Die VNC-Konsole wird angezeigt.

Neustart erforderlich, wenn Knoten-IP-Adressen oder Netzmasken-Netzwerkeinstellungen geändert werden

Wenn Sie die IP-Adresse oder Netzmaskeneinstellungen eines Knotens ändern wie unter Konfigurieren der IP-Einstellungen beschrieben, sind sowohl die alten als auch die neuen Einstellungen wirksam, bis Sie den Knoten neu starten. Wenn beide Einstellungen aktiv sind, kann es zu Routing- oder Verbindungsproblemen kommen.

Aktualisierte Dokumentation

Ab Version 2.0.0.0 ist die Hilfe auch auf Deutsch, Japanisch, Chinesisch und Portugiesisch verfügbar.

Zugriff auf Artikel in der Stratus Knowledge Base

Das **Stratus Customer Service Portal** bietet eine durchsuchbare **Knowledge Base** mit technischen Artikeln über alle Stratus-Produkte, darunter ztC Edge-Systeme und Stratus Redundant Linux-Software. In einigen Fällen verweisen die Versionshinweise direkt zu Artikeln in der Knowledge Base (zum Beispiel KB-*nnnn*). Sie können mit Ihren vorhandenen Anmeldedaten für das Serviceportal auf das Customer Service Portal und die Artikel in der Knowledge Base zugreifen, oder Sie erstellen wie nachstehend beschrieben ein neues Konto.

So nutzen Sie die Knowledge Base

1. Melden Sie sich beim **Stratus Customer Service Portal** unter https://support.stratus.com an.

    Erstellen Sie bei Bedarf ein neues Konto:

a. Klicken Sie auf **Register Account** (Konto registrieren).

b. Geben Sie Ihre Firmen-E-Mail-Adresse und Kontaktinformationen ein und klicken Sie auf **Register** (Registrieren).

   Ihre Firmen-E-Mail-Adresse muss einen Domänennamen (z. B. stratus.com) für eine Firma enthalten, die ein registrierter Kunde von Stratus ist.

c. Klicken Sie in der E-Mail, die Sie von Stratus erhalten, auf den Link.

d. Geben Sie ein neues Kennwort ein und schließen Sie die Konfiguration Ihres Kontos ab.

Falls Sie Unterstützung beim Erstellen eines Kontos benötigen, wenden Sie sich an Ihren autorisierten Stratus-Servicemitarbeiter.

2. Klicken Sie im Serviceportal im linken Fenster auf **Knowledge Base**.
3. Geben Sie im Feld **Keyword Search** (Stichwortsuche) Schlagwörter für die gesuchten Informationen ein und klicken Sie auf **Search** (Suchen).

   Um einen Artikel anhand seiner KB-*nnnn*-Nummer zu suchen, klicken Sie auf **Advanced Search** (Erweiterte Suche). Geben Sie neben **Search by ID** (Nach ID suchen) die Artikelnummer (*nnnn*) ein und klicken Sie auf **Display** (Anzeigen).

Hilfe

Bei technischen Fragen zu ztC Edge-Systemen lesen Sie zunächst die neuesten technischen Informationen und die Online-Dokumentation auf der Seite **Downloads** unter https://www.stratus.com/services-support/downloads/?tab=ztcedge. Oder suchen Sie in der **Knowledge Base** im **Stratus Customer Service Portal** unter https://support.stratus.com.

Wenn Sie Ihre Fragen nicht mithilfe der Online-Ressourcen beantworten können und das System durch einen Servicevertrag abgedeckt ist, wenden Sie sich an Ihren autorisierten Stratus-Servicemitarbeiter. Weitere Informationen finden Sie auf der Seite **ztC Edge Support** unter https://www.stratus.com/services-support/customer-support/?tab=ztcedge.

10

Kapitel 10: Systemreferenzinformationen

Weitere Informationen finden Sie in den folgenden Themen

- Getestete Gastbetriebssysteme
- Wichtige Überlegungen für physische Maschinen und virtuelle Maschinen
- Zugriff auf Artikel in der Knowledge Base
- Erstellen einer ALSR-Konfiguration
- Behobene CVEs
- REST API-Aufrufe

Getestete Gastbetriebssysteme

In der folgenden Tabelle sind die Gastbetriebssysteme für virtuelle Maschinen (VMs) aufgeführt, die Stratus in der aktuellen Version der Stratus Redundant Linux-Software getestet hat. Nicht aufgeführte Gastbetriebssysteme wurde nicht von Stratus getestet und müssen lokal getestet werden.

Betriebssystem	Version	Start-Firmware-Schnittstelle
CentOS 7	CentOS 7.5, 7.6, 7.7, 7.8 (jeweils 64 Bit)	BIOS
CentOS 6	Cent 6.9, 6.10 (jeweils 64 Bit)	BIOS

Betriebssystem	Version	Start-Firmware-Schnittstelle
Microsoft Windows Server 2019 (Standard, Datacenter)	64 Bit	BIOS UEFI[1]
Microsoft Windows Server 2016 (Standard, Datacenter)	64 Bit	BIOS UEFI[2]
Microsoft Windows Server 2012 (Standard, Datacenter)	64 Bit R2	BIOS
Microsoft Windows 10 Desktop	64 Bit	BIOS
Red Hat Enterprise Linux 8 (Workstation, Server)	Red Hat 8.1 (64 Bit)	BIOS
Red Hat Enterprise Linux 7 (Workstation, Server)	Red Hat 7.5, 7.6, 7.7, 7.8 (jeweils 64 Bit)	BIOS
Red Hat Enterprise Linux 6 (Workstation, Server)	Red Hat 6.10 (64 Bit)	BIOS
SUSE Linux Enterprise Server	SLES 12 SP2 64 Bit	BIOS
Ubuntu	18.042 Server 64 Bit	BIOS

Wichtige Überlegungen für physische Maschinen und virtuelle Maschinen

Damit die Implementierung physischer Maschinen und virtueller Maschinen optimal erfolgt, beachten Sie die Konfigurationshöchstwerte und Anforderungen, die in den folgenden Abschnitten beschrieben werden:

---

[1]Sie können eine VMware-VM mit einer UEFI-Start-Firmware-Schnittstelle und Windows Server 2019 nur dann in ein System mit Stratus Redundant Linux Version 2.2.0.0 (oder höher) importieren, wenn die VM von einem VMware-Server exportiert wurde, auf dem vSphere Version 6.7 ausgeführt wird.

[2]Sie können eine VMware-VM mit einer UEFI-Start-Firmware-Schnittstelle und Windows Server 2016 nur dann in ein System mit Stratus Redundant Linux Version 2.2.0.0 (oder höher) importieren, wenn die VM von einem VMware-Server exportiert wurde, auf dem vSphere Version 6.7 ausgeführt wird.

Empfehlungen und Einschränkungen für virtuelle Maschinen

Virtuelle Maschinen (VMs) benötigen bestimmte CPU-Kernressourcen.

Empfohlene Anzahl von CPU-Kernen

Stratus empfiehlt, nur so viele Threads für Arbeitslasten zu verwenden, wie es physische Threads in einem ztC Edge-System gibt. Das ztC Edge 100i-System hat insgesamt 8 physische Threads. Das ztC Edge 110i-System hat insgesamt 12 physische Threads.

Die Anzahl der Kerne, die für die ztC Edge-Arbeitsauslastung empfohlen wird, ist von der Anzahl der vCPUs in jeder VM und von den VM-Typen abhängig wie nachstehend beschrieben:

Element	Anzahl physischer Threads
Jeder FT-Gast mit *n* vCPUs	*n* + 2 (typisch)
Jeder HV-Gast mit *n* vCPUs	*n* (typisch)

Beispiele

Die folgenden Beispiele gelten für ztC Edge 100i-Systeme:

- Vier 2-vCPU-HV-Gäste benötigen typischerweise insgesamt 8 Threads.
- Zwei 3-vCPU-HV-Gäste und ein 2-VCPU-HV-Gast benötigen typischerweise insgesamt 8 Threads.
- Zwei 4-vCPU-HV-Gäste benötigen typischerweise insgesamt 8 Threads.
- Ein 8-vCPU-HV-Gast benötigt typischerweise insgesamt 8 Threads.

Die folgenden Beispiele gelten für ztC Edge 110i-Systeme (zusätzlich zu den obigen Beispielen):

- Ein 4-vCPU-FT-Gast benötigt typischerweise insgesamt 6 Threads.
- Sechs 2-vCPU-HV-Gäste benötigen typischerweise insgesamt 12 Threads.
- Ein 2-vCPU-FT-Gast benötigt 4 Threads und zwei 2-vCPU-HV-Gäste benötigen 4 Threads; insgesamt also 8.

Wichtige Überlegungen

Beachten Sie die folgenden wichtigen Punkte.

Funktion	Kommentar
USB-Geräte	USB-Tastaturen, CD/DVD-Laufwerke, Festplatten und USB-Sticks werden für das Importieren/Exportieren von VMs und für die Systemwiederherstellung unterstützt.
Konsolenkonnektivität	Die Textkonsole jeder PM ist für ein CentOS-Betriebssystem verfügbar. Der VGA-Modus wird jedoch nicht unterstützt; die PM muss also auf Runlevel 3 ausgeführt werden und kann nicht auf Runlevel 5 ausgeführt werden. Siehe „Systemverwaltung“ weiter unten.
Systemverwaltung	Die ztC Edge-Systemverwaltung kann **nicht** auf Runlevel 5 ausgeführt werden.
Volumes	Wenn Sie ein Volume exportieren, importieren oder wiederherstellen, beträgt die maximale Volumegröße 2 TB.

Erstellen einer ALSR-Konfiguration

In diesem Thema und seinen Unterthemen wird beschrieben, wie Sie eine ALSR-Konfiguration erstellen. Allgemeine Informationen zu Quorumservern finden Sie unter Quorumserver sowie ALSR und Quorumdienst.

> **Hinweis**: **Bevor** Sie eine ALSR-Konfiguration erstellen, sollten Sie dieses Thema einschließlich aller Unterthemen lesen und dann Ihre ALSR-Konfiguration planen wie in diesen Themen beschrieben. Erstellen Sie die Konfiguration erst, wenn Sie sicher sind, dass Ihre geplante Konfiguration mit den Informationen in diesem Thema und seinen Unterthemen konform ist.

Eine ALSR-Konfiguration (Automated Local Site Recovery) liegt vor, wenn eine der folgenden Bedingungen erfüllt ist:

- Die beiden Knoten des Systems sind über die Netzwerkinfrastruktur statt über direkte Kabel verbunden.

- Die Länge der A-Link-Kabel (direkte Verbindung), die die beiden Knoten verbinden, ist größer als 10 Meter (zum Beispiel in zwei verschiedenen Gebäuden auf einem Gelände).

Diese Konfigurationen bieten eine bessere Notfalltoleranz und Hardwareredundanz sowie die Redundanz physischer Rechenzentren und der Gebäude, die sie enthalten.

Stratus empfiehlt, für eine ALSR-Konfiguration einen dritten Computer zu verwenden, welcher ein Quorumserver ist. Der Quorumserver befindet sich an einem physischen Standort, der einen gewissen Abstand zum physischen Standort von Knoten0 und Knoten1 hat.

Hinweis: In diesem Thema und seinen Unterthemen wird beschrieben, wie Sie eine ALSR-Konfiguration mit einem Quorumserver erstellen. Stratus empfiehlt dringend, für eine ALSR-Konfiguration einen Quorumserver zu verwenden. Wenn Sie in Betracht ziehen, eine ALSR-Konfiguration ohne einen Quorumserver zu erstellen, informieren Sie sich in der Knowledge Base im Artikel *Considerations if deploying ALSR without quorum* (KB-9682) und wenden Sie sich auch an Ihren autorisierten Stratus-Servicemitarbeiter. Informationen zum Zugriff auf Artikel in der Knowledge Base finden Sie unter Zugriff auf Artikel in der Knowledge Base.

Aufgrund der räumlichen Trennung dieser physischen Maschinen muss beim Erstellen einer ALSR-Konfiguration sorgfältig geplant werden, wo die Komponenten platziert werden. Außerdem ist die Netzwerktopologie komplexer.

In den folgenden Themen wird beschrieben, wie Sie eine ALSR-Konfiguration erstellen. Damit Sie die hier beschriebenen Verfahren erfolgreich ausführen können, sollten Sie sich mit der ztC Edge-Software und der verwendeten Hardware auskennen und mit der Netzwerkinfrastruktur Ihres Systems und dem Standort vertraut sein.

Hinweis: Es können an dieser Stelle nicht alle Hersteller und Modelle von Netzwerkswitches, Routern und anderer Hardware beschrieben werden. Lesen Sie die Dokumentation zu Ihrer Infrastruktur, falls Sie weitere Informationen über deren Konfiguration gemäß den Anforderungen in diesen Hilfethemen benötigen.

- Erstellen der Konfiguration
- Erfüllen der Netzwerkanforderungen
- Platzieren und Erstellen des Quorumservers

- Abschließen der Konfiguration
- Quorum-Effekte auf das Systemverhalten

In der folgenden Tabelle sind Begriffe aufgeführt und definiert, denen Sie im Zusammenhang mit der Erstellung einer ALSR-Konfiguration begegnen werden.

Begriff	Bedeutung
Aktiver Knoten	Der Knoten, auf dem eine Gast-VM ausgeführt wird. Jede Gast-VM kann einen anderen aktiven Knoten haben. Das Gegenteil von *aktiv* ist „Standby“ (siehe Standby-Knoten).
A-Link	Availability Link (Verfügbarkeitsverbindung). Eine direkte Netzwerkverbindung zwischen den beiden Computern, die ein ztC Edge-System bilden. (Die Computer eines Systems werden auch als *physische Maschinen* (PMs) oder *Knoten* bezeichnet.) A-Links müssen Punkt-zu-Punkt-Verbindungen sein. Der A-Link-Datenverkehr kann nicht über einen Router laufen. Ein ztC Edge-System benötigt zwei A-Links. Bei einigen Systemen haben diese Verbindungen blaue und gelbe Kabel (und Anschlüsse). Sie können VLAN-Verbindungen für A-Links in einer Bereitstellung an einem verteilten lokalen Standort verwenden (siehe VLAN).
Alternativer Quorumserver	Der alternative Quorumserver wird verwendet, wenn der bevorzugte Quorumserver nicht verfügbar ist (siehe Bevorzugter Quorumserver).
Automated local site recovery (ALSR)	Eine ALSR-Konfiguration (Automated Local Site Recovery) liegt vor, wenn eine der folgenden Bedingungen erfüllt ist: • Die beiden Knoten des ztC Edge-Systems sind über die Netzwerkinfrastruktur statt über direkte Kabel verbunden. • Die Länge der A-Link-Kabel (direkte Verbindung), die die beiden Knoten verbinden, ist größer als 10 Meter (zum Beispiel in zwei verschiedenen Gebäuden auf einem Gelände). Eine ALSR-Konfiguration wird normalerweise verwendet, um eine bessere

	Notfalltoleranz zu bieten. Dies ist jedoch mit einem größeren Aufwand bei der Netzwerkeinrichtung und umfangreicheren Konfigurationsoptionen verbunden. Eine ALSR-Konfiguration erfordert einen dritten Computer, welcher ein Quorumserver ist (siehe Quorumserver).
AX	Die Containerschicht, die sich im ztC Edge-System befindet und das Verhalten der Gast-VM steuert. AX ist für die Synchronisierung einer VM zwischen dem aktiven Knoten und dem Standby-Knoten zuständig. Jede VM hat ihr eigenes AX-Paar (siehe VM, Aktiver Knoten und Standby-Knoten)
Unternehmensnetzwerk (ibiz)	Eine Netzwerkverbindung vom ztC Edge-System zu einem LAN, über die auch anderer Datenverkehr läuft, zum Beispiel Verwaltungsmeldungen oder Datenverkehr für Anwendungen und andere Clients und Server. Das ztC Edge-System hat normalerweise zwei Ports für Unternehmensnetzwerk-Verbindungen. Unternehmensnetzwerke können einer oder mehreren Gast-VMs zugewiesen sein, es ist aber auch möglich, dass sie keiner Gast-VM zugewiesen sind. Sie müssen das erste Unternehmensnetzwerk (ibiz0) mit einem LAN verbinden, damit Sie das System über einen Webbrowser verwalten können.
Fehler (Fault)	Jede potenzielle Verschlechterung der Fähigkeit eines Systems, eine Gast-VM auszuführen (siehe VM). Festplattenfehler, Verlust der Netzwerkverbindung oder Stromausfälle sind Beispiele für Fehler, die vom System erkannt werden.
Knoten0 und Knoten1	Die beiden Computer, die das ztC Edge-System bilden, werden intern als Knoten0 und Knoten1 bezeichnet. (Diese Computer werden auch als physische Maschinen oder PMs bezeichnet.) Die Zuordnung als Knoten0 und Knoten1 ist beliebig und erfolgt bei der erstmaligen Konfiguration des Systems. Der konstante Datenverkehr zwischen Knoten0 und Knoten1 übermittelt Informationen zum Zustand des Systems sowie der ausgeführten Gast-VM (siehe VM).

Bevorzugter Quorumserver	Der bevorzugte Quorumserver wird verwendet, wenn er (der bevorzugte Quorumserver) verfügbar ist. Wenn der bevorzugte Quorumserver nicht verfügbar ist, wird der alternative Quorumserver verwendet (siehe Alternativer Quorumserver).
Primärer Knoten	Wenn die Computer des Systems gekoppelt sind, antwortet nur einer der Computer auf Verwaltungsmeldungen. Dieser Computer ist der primäre Knoten. Die System-IP-Adresse, die bei der erstmaligen Bereitstellung zugewiesen wird, gilt für den primären Knoten. Der primäre Knoten kann zwischen Knoten0 und Knoten1 wechseln, wenn unterschiedliche Fehlerbedingungen auftreten (siehe Fehler (Fault)). Beachten Sie, dass der primäre Knoten nicht unbedingt der aktive Knoten für eine Gast-VM sein muss (siehe Aktiver Knoten und VM).
priv0	Ein Netzwerk für den privaten Verwaltungsdatenverkehr zwischen den beiden Knoten. Weitere Informationen finden Sie unter A-Link- und private Netzwerke.
Quorumserver	Ein dritter Computer, der bei der Bestimmung hilft, welche AX für jede Gast-VM aktiv sein soll (siehe Aktiver Knoten und VM). Der richtige Einsatz eines Quorumservers ist die einzige sicher funktionierende Methode, um Split-Brain-Bedingungen zu verhindern (siehe Split-Brain).
RTT	Roundtripzeit. Die Zeit, die eine Netzwerkmeldung benötigt, um vom Startpunkt zum Ziel und wieder zurück übermittelt zu werden. Diese Zeit wird normalerweise in Millisekunden (ms) angegeben.
Split-Brain	Die Situation, die auftritt, wenn beide AX des AX-Paars einer Gast-VM gleichzeitig aktiv sind, wodurch innerhalb jedes aktiven Gasts abweichende Kopien der Daten produziert werden (siehe AX und VM). Dazu kann es kommen, wenn alle Kommunikationswege zwischen Knoten0 und Knoten1 getrennt sind (siehe Knoten0 und Knoten1). Der Einsatz des Quorumdienstes verhindert Split-Brain-Bedingungen (siehe Quorumserver).

Standby-Knoten	Der Knoten, der nicht der aktive Knoten für eine Gast-VM ist. Der Standby-Knoten wird durch AX-Kommunikation über A-Link-Verbindungen synchronisiert (siehe AX und A-Link). Das AX-Paar der einzelnen Gast-VMs bestimmt, welcher Knoten aktiv ist und welcher im Standby ist (siehe Aktiver Knoten).
Systemverwaltung	Die Systemverwaltung ist die Schicht in der Stratus Redundant Linux-Software, die dafür zuständig ist, den allgemeinen Zustand des Systems aufrechtzuerhalten. Dazu gehört zum Beispiel, zu bestimmen, welcher Knoten der primäre Knoten ist (siehe Primärer Knoten). Die Systemverwaltung ist auch dafür zuständig, Informationen in der ztC Console anzuzeigen.
USV	Unterbrechungsfreie Stromversorgung. Eine externe Sicherungsbatterie für elektrische Geräte, die verhindert, dass sich Stromausfälle auf die Verfügbarkeit auswirken.
VLAN	Virtuelles LAN. Ein VLAN ist eine Gruppe von Geräten in einem oder mehreren LANs, die so konfiguriert sind, dass sie kommunizieren, als befänden sie sich in demselben kabelgebundenen Netzwerk, obwohl sie sich in unterschiedlichen LAN-Segmenten befinden. VLANs werden auf der Ebene der Netzwerkinfrastruktur konfiguriert, nicht im ztC Edge-System. In einerAutomated local site recovery (ALSR)-Konfiguration werden die A-Link-Verbindungen als isolierte VLANs implementiert (siehe A-Link).
VM	Virtuelle Maschine (auch als Gast bezeichnet). Einem System sind normalerweise eine oder mehrere VMs (oder Gäste) zugeordnet, auf denen Anwendungen über Gastbetriebssysteme ausgeführt werden.

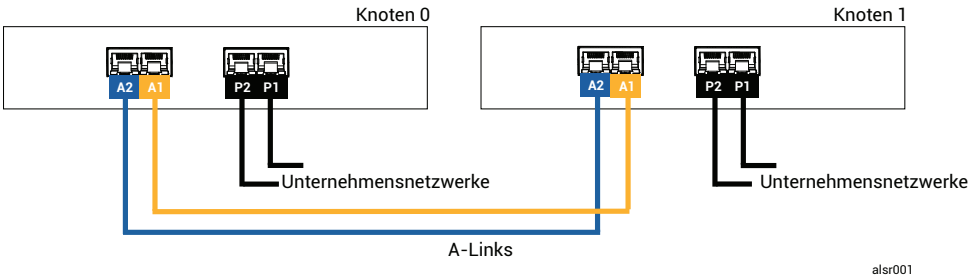
Erstellen der Konfiguration

Um eine ALSR-Konfiguration zu erstellen, überlegen Sie zunächst, wie die Konfiguration eines typischen ztC Edge-Systems aussieht und welche VLAN-Anforderungen für eine ALSR-Konfiguration gelten. Sehen Sie sich dann eine gut geplante ALSR-Konfiguration mit einem Quorumserver an und machen Sie sich mit den

VLAN-Anforderungen der Konfiguration vertraut. Sie müssen sich auch mit dem gesamten Prozess vertraut machen, der die Bereitstellung eines typischen ztC Edge-Systems und die Erstellung einer ALSR-Konfiguration umfasst. In den folgenden Abschnitten finden Sie weitere Informationen.

Ein typisches ztC Edge-System

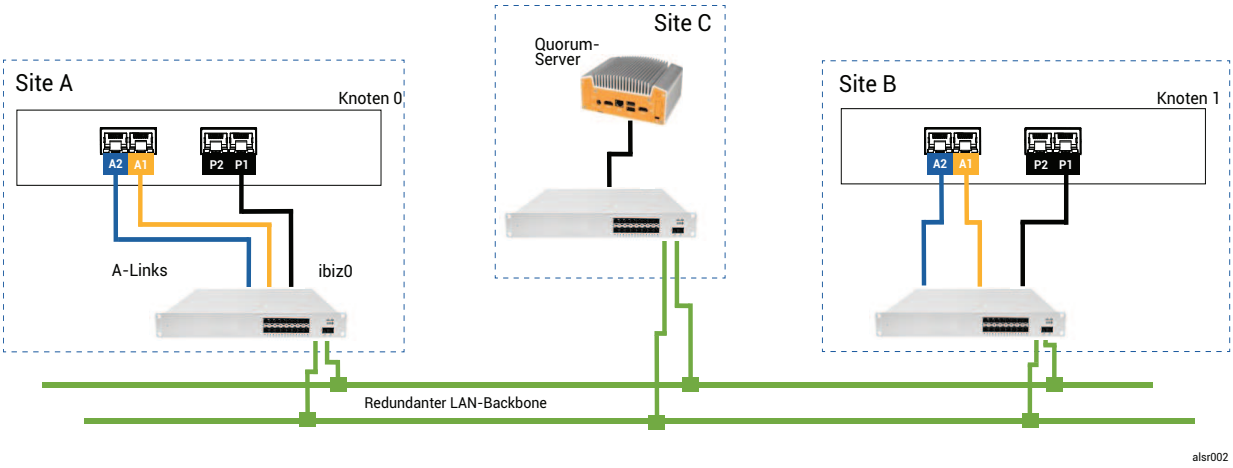
In einer typischen ztC Edge-Systemkonfiguration sind zwei PMs über ein Netzwerkkabelpaar für A-Links direkt verbunden. Ein A-Link wird typischerweise für das private Netzwerk (priv0) verwendet. Die beiden PMs verfügen über zusätzliche Netzwerkverbindungen für Unternehmensnetzwerke, die von der ztC Console und vom System gehosteten Gast-VMs verwendet werden. Die folgende Abbildung zeigt eine typische Konfiguration.



Der physische Abstand zwischen den PMs in einer typischen Konfiguration wird durch die Länge eines einzelnen A-Link-Netzwerkkabels bestimmt, also ungefähr 10 m. Dieser Abstand kann deutlich geringer sein, wenn die Umgebungsbedingungen und elektrisches Rauschen berücksichtigt werden müssen.

Eine ALSR-Konfiguration mit einem Quorumserver

Eine gut geplante ALSR-Konfiguration besteht aus den beiden Knoten an zwei unterschiedlichen Standorten (Sites) sowie einem dritten Computer, der an einem dritten Standort den Quorumdienst ausführt. All diese Computer sind mit den geeigneten Netzwerk-Switching-Geräten in einem Netzwerk verbunden, sodass es keinen Single Point of Failure (SPOF) innerhalb der ALSR-Konfiguration gibt. Die folgende Abbildung zeigt eine solche Konfiguration, zu der Knoten0 an Standort A, Knoten1 an Standort B und der Quorumserver an Standort C gehören.



Hinweise:

1. Jeder A-Link muss mit seinem eigenen VLAN verbunden sein, das zwischen Switch A und Switch B konfiguriert ist.
2. DNS-Server und Gateways sind aus Gründen der Übersichtlichkeit nicht in den Abbildungen dargestellt, Sie müssen aber sicherstellen, dass die ALSR-Konfiguration für den Fall eines Netzwerkausfalls über eine Verbindung zu einem DNS-Server und ein Gateway verfügt.
3. Um den Schutz zu optimieren, sollten Sie redundante Switches an jedem Standort installieren, obwohl diese in den Abbildungen nicht zu sehen sind. Bei der abgebildeten Konfiguration verfügen Standort A *und* Standort B jeweils über zwei Switches. Die A-Links werden über einen Switch geroutet und die Unternehmensnetzwerke werden über den anderen Switch geroutet. Versorgen Sie die Switches nach Möglichkeit über getrennte Schaltkreise mit Strom oder verwenden Sie eine USV, um Ausfälle bei kurzen Stromausfällen zu vermeiden.

ALSR-VLAN-Anforderungen

Die A-Link-Verbindungen zwischen Switch A und Switch B erfordern eine VLAN-Konfiguration an den Switches. A-Link-Datenverkehr kann nicht geroutet werden, und die Verbindung sollte ein einzelnes langes Netzwerkkabel emulieren. Jeder A-Link muss in seinem eigenen VLAN isoliert sein.

Wenn Sie keine VLANs zwischen den Switching-Geräten erstellen können, können Sie Ethernet-zu-Glasfaser-Medienkonverter verwenden. So erstellen Sie eine längere Glasfaserverbindung zwischen den

beiden PMs. Sie dürfen die beiden A-Link-Glasfaserverbindungen jedoch nicht über dieselbe physische Leitung routen, da hiermit ein Single Point of Failure entstehen würde.

Außerdem darf der Computer mit dem Quorumdienst keinen Switch mit Knoten0 oder Knoten1 teilen, da hiermit ein Single Point of Failure entstehen würde.

Lesen Sie Erfüllen der Netzwerkanforderungen, um mehr über die Latenzanforderungen der A-Link- und Quorumverbindungen zu erfahren.

Von der ersten Bereitstellung zum Abschließen der ALSR-Konfiguration

Wenn Sie eine ALSR-Konfiguration erstellen, müssen Sie zunächst ein typisches ztC Edge-System bereitstellen und registrieren, ohne die ALSR-Konfiguration vorzunehmen. Die Abbildung in Ein typisches ztC Edge-System stellt ein solches System dar. Installieren Sie die beiden Knoten der Einfachheit halber Seite an Seite und verwenden Sie dabei die mitgelieferten Kabel. Siehe Erste Schritte.

Wenn das typische System normal läuft, erstellen Sie die ALSR-Konfiguration.

1. Lesen Sie dazu Erstellen einer ALSR-Konfiguration mit allen Unterthemen, falls Sie dies noch nicht getan haben.
2. Installieren Sie den Quorumcomputer und aktivieren Sie den Quorumserver. Achten Sie darauf, dass alle Bedingungen in den folgenden Themen erfüllt sind:
    - Eine ALSR-Konfiguration mit einem Quorumserver
    - ALSR-VLAN-Anforderungen
    - Erfüllen der Netzwerkanforderungen
    - Abschließen der Konfiguration
3. Vergewissern Sie sich, dass der Quorumserver Zugriff auf beide Knoten hat.
4. Fahren Sie einen Knoten ordnungsgemäß herunter. Siehe Herunterfahren einer physischen Maschine.
5. Versetzen Sie den heruntergefahren Knoten an den entfernten Standort.
6. Schließen Sie die Infrastruktur an. Die obige Abbildung zur ALSR-Konfiguration zeigt die Verbindungen. Im Einzelnen sind dies:
    - Die priv0-Verbindung mit Port **A2**
    - Die zweite A-Link-Verbindung mit Port **A1**
    - Die ibiz0-Verbindung mit Port **P1**

7. Schalten Sie die Knoten ein und verbinden Sie sie (erneut). Siehe Einschalten einer physischen Maschine.
8. Überprüfen Sie die Konfiguration. Stellen Sie Folgendes sicher:
    - Die gemeinsamen Netzwerke sind korrekt gekoppelt – Navigieren Sie in der ztC Console zur Seite **Netzwerke** und vergewissern Sie sich, dass der Zustand jedes Netzwerks als grünes Häkchen dargestellt wird. Beheben Sie mögliche Probleme mit der Infrastruktur.
    - Quorumverbindungen wurden wiederhergestellt – Navigieren Sie in der Konsole zur Seite **Quorumserver**, indem Sie auf **Voreinstellungen** und dann auf **Quorumserver** klicken. Vergewissern Sie sich, dass der Zustand des Quorumservers als grünes Häkchen dargestellt wird. Beheben Sie mögliche Probleme mit der Infrastruktur.
    - Der primäre Knoten kann von Knoten0 zu Knoten1 wechseln und die Konsole kann in beiden Konfigurationen eine Verbindung herstellen – Versetzen Sie jeden Knoten einmal in den Wartungsmodus (siehe Wartungsmodus).
9. VMs (erneut) verbinden – Migrieren Sie die VMs von einem Knoten zum anderen (siehe Migrieren einer physischen oder virtuellen Maschine in ein System). Überprüfen Sie das korrekte Netzwerk-Failover für die VM-Netzwerkverbindung.
10. Bewerten Sie den Status des Netzwerks und validieren Sie das Ethernet-Failover (siehe Die Seite „Netzwerke“).

Erfüllen der Netzwerkanforderungen

In diesem Thema werden die Netzwerkanforderungen und Überlegungen für A-Links, Unternehmensnetzwerke, die Quorumserver-Verbindungen und das Verwaltungsnetzwerk beschrieben, die für eine erfolgreiche ALSR-Konfiguration berücksichtigt werden müssen.(Allgemeine Informationen zu diesen Netzwerken finden Sie unter Netzwerkarchitektur.)

Voraussetzung: Planen und erstellen Sie eine ALSR-Konfiguration, indem Sie zunächst Erstellen einer ALSR-Konfiguration lesen und die entsprechenden Anweisungen befolgen, falls Sie dies noch nicht getan haben.

Ein A-Link-Netzwerk muss die folgenden Anforderungen erfüllen:

- Die A-Links verwenden die IPv6-Adressierung.
- Jeder A-Link muss mit seinem eigenen VLAN verbunden sein. A-Link-Datenverkehr kann nicht geroutet werden.
    - FT-VMs erfordern eine A-Link-Latenz von weniger als 2 ms RTT (nur bei 110i-Systemen verfügbar).
    - HV-VMs erfordern eine A-Link-Latenz von weniger als RTT (in allen ztC Edge-Systemen verfügbar).
    - Sie müssen genügend Bandbreite für alle VMs im System bereitstellen, und die Geschwindigkeit pro A-Link muss mindestens 1 Gb betragen.
    - Wenn Sie Ihre Netzwerkinfrastruktur planen, bedenken Sie auch die Uplink-Bandbreite zwischen dem Switch und dem Netzwerk-Backbone über alle Ports, die an diesem Switch verwendet werden.

  Wenn diese Anforderungen nicht erfüllt sind, werden Gast-VMs langsamer ausgeführt. Dies liegt an der eingeschränkten Synchronisierungsbandbreite zwischen den beiden Knoten.

Das erste Unternehmensnetzwerk (ibiz0) wird für die Kommunikation zwischen den Knoten und mit dem Quorumserver verwendet. Das ibiz0-Netzwerk muss die folgenden Anforderungen erfüllen:

- Die beiden Knoten müssen sich in demselben Subnetz befinden.
- Das Netzwerk muss IPv6-Multicast-Datenverkehr zwischen den beiden Knoten zulassen.
- Die beiden Knoten können mit IPv4-Netzwerkadressierung auf den Quorumserver zugreifen.

Netzwerkverbindungen für den Quorumserver müssen die folgenden Anforderungen erfüllen:

- Der Zugriff auf den Quorumdienst muss über ibiz0 mit IPv4-Netzwerkadressierung ermöglicht werden.
- Zwei UDP-Ports müssen für die Kommunikation zwischen den Knoten und dem Quorumdienst offen und verfügbar sein; dies gilt auch für die Firewalls. Standardmäßig sind dies die Ports 4557 und 4558. Wenn Sie diese Ports ändern wollen, lesen Sie Konfigurieren des Quorumdienst-Ports (auf dem Quorumcomputer) und Konfigurieren des Quorumservers über die ztC Console.
- Die Latenz zwischen einem ztC Edge-Knoten und dem Quorumcomputer muss weniger als 500 ms RTT betragen.
- Der Durchsatz spielt keine bedeutende Rolle. 10-Mbit/s-Ethernet oder T1-Bandbreite ist ausreichend.

- Quorumcomputer stehen allen VMs in demselben ztC Edge-System zur Verfügung.
- Quorumcomputer können von zahlreichen ztC Edge-Systemen gemeinsam genutzt werden.
- Quorumcomputer dürfen niemals als VM in demselben ztC Edge-System implementiert werden, das den Quorumcomputer verwendet.
- Verwenden Sie unterschiedliche Netzwerkstrukturen, keine gemeinsamen. Ein ztC Edge-Knoten darf nicht von einem Gateway oder Switch/Router am Standort des Partnerknotens abhängig sein, damit der Zugriff auf eine Quorumdienstcomputer immer gewährleistet ist.

Hinweis: Implementieren Sie den Quorumdienst nicht als Gast-VM auf einem anderen Knotenpaar. Ein Ausfall bei diesen Knoten würde zu einem Failover der VM, auf der der Quorumdienst ausgeführt wird, führen. Dies würde unnötige Komplikationen für die Netzwerktopologie und das Fehlermanagement verursachen. Zusätzlich wird ein zweiter Quorumcomputer für die Quorumverwaltung des ztC Edge-Systems, auf dem der Quorumdienst ausgeführt wird, benötigt.

Verwaltungsnetzwerk-Verbindungen müssen die folgenden Anforderungen erfüllen:

- Standardmäßig wird das Verwaltungsnetzwerk mit einem Unternehmensnetzwerk geteilt. In diesem Fall gelten alle Anforderungen für Unternehmensnetzwerke.
- Konfigurieren Sie Gateways zu einem Unternehmens-LAN für die Remoteverwaltung.

Platzieren und Erstellen des Quorumservers

In einer gut geplanten ALSR-Konfiguration hostet ein dritter Computer den Quorumdienst. Die Anforderungen der Quorumdienstverarbeitung sind gering, sodass ein beliebiger vorhandener Computer oder eine VM den Quorumdienst hosten kann, solange die Netzwerk- und Betriebssystemanforderungen erfüllt sind. Ein effektiver Quorumserver ist von der Platzierung des Quorumcomputers innerhalb des Netzwerks abhängig.

Nachdem Sie einen geeigneten Standort für den Quorumcomputer (und ggf. den alternativen Quorumcomputer) ermittelt und sich vergewissert haben, dass der Computer die Anforderungen des Quorumdienstes erfüllt, können Sie den Quorumserver erstellen.

Voraussetzung: Planen und erstellen Sie eine ALSR-Konfiguration, indem Sie zunächst Erstellen einer ALSR-Konfiguration lesen und die entsprechenden Anweisungen befolgen, falls Sie dies noch nicht getan haben.

Platzieren des Quorumservers

Platzieren Sie den ersten Quorumcomputer an einem dritten Standort innerhalb Ihres Netzwerks wie in der Abbildung Eine ALSR-Konfiguration mit einem Quorumserver veranschaulicht. Falls kein dritter Standort verfügbar ist, platzieren Sie den Quorumserver an einem physischen Standort, der einen gewissen Abstand zum physischen Standort von Knoten0 und Knoten1 hat. Wenn Sie den Quorumcomputer an einem separaten Standort platzieren, ist die Wahrscheinlichkeit höher, dass das System ein Problem übersteht, bei dem beide Knoten und der Quorumcomputer verloren gehen (zum Beispiel ein vorübergehendes Leitungsproblem, dass die Netzwerkkonnektivität unterbricht).

Verbinden Sie den Quorumcomputer mit einem elektrischen Schaltkreis, der getrennt vom Schaltkreis ist, in dem sich Knoten0 und Knoten1 befinden. Außerdem sollten Sie den Quorumcomputer an eine USV anschließen.

Achtung: Wenn beide AX die Verbindung zum Quorumserver verlieren, versuchen sie, einen alternativen Quorumserver auszuwählen. Wenn kein Quorumserver ausgewählt werden kann, wird die VM in den Simplexmodus herabgestuft, damit es im Falle eines Fehlers oder Ausfalls nicht zu einem Split-Brain-Zustand kommt.

Wenn einer der Knoten heruntergefahren wird und die VM (AX) an dem verbleibenden Knoten weder den Quorumserver noch ihren Partner erreichen kann, fährt sie sich selbst herunter, um einen Split-Brain-Zustand zu vermeiden.

Wenn Sie den Quorumserver platzieren:

- Sorgen Sie dafür, dass der Quorumserver weder mit Knoten0 noch mit Knoten1 einen Switch (oder Router) teilt.
- Verwenden Sie **keine** Gast-VM innerhalb des ztC Edge-Systems, um den Quorumdienst auszuführen.

Eine Beschreibung des Systemverhaltens und der Fehlermodi finden Sie unter Quorum-Effekte auf das Systemverhalten.

Hinzufügen eines alternativen Quorumservers

Sie können Ihrem System einen weiteren Quorumcomputer (samt Switch) hinzufügen, um einen alternativen Quorumdienst zu erstellen. Alternative Quorumserver kommen am häufigsten dann zum Einsatz, wenn zum Beispiel Betriebssystem-Updates auf den bevorzugten Quorumserver angewendet werden. Wenn der

bevorzugte Quorumserver nicht verfügbar ist, wird der alternative Quorumserver ausgewählt und es findet keine Herabstufung in den Simplexmodus statt. Sobald der bevorzugte Quorumserver wieder verfügbar ist, wird er wieder verwendet.

Wenn Sie einen zweiten Quorumdienst erstellen, müssen Sie alle Anforderungen für das Netzwerk und die Platzierung des Quorumcomputers berücksichtigen. Wenn beide Knoten miteinander und mit demselben Quorumserver (entweder dem bevorzugten oder dem alternativen Quorumserver) kommunizieren können, kann das System die VM-Redundanz aufrechterhalten, selbst wenn eine Quorumverbindung unterbrochen wird. Wenn beide Knoten Zugriff aufeinander und auf den bevorzugten Quorumserver haben, wird der bevorzugte Quorumserver ausgewählt. Fall der bevorzugte Quorumdienst zur selben Zeit verloren geht wie ein Knoten, fährt der verbleibende Knoten die VM herunter, selbst wenn ein zweiter, nicht bevorzugter Quorumdienst verfügbar ist. Geht der bevorzugte Quorumdienst jedoch verloren, *bevor* ein Knoten verloren geht, und wenn beide Knoten weiterhin den alternativen Quorumserver erreichen können, wird der alternative Quorumserver ausgewählt. Die Fehlerbehandlung erfolgt nur im Zusammenhang mit dem ausgewählten Quorumserver.

Wenn Sie einen alternativen Quorumdienst erstellen, müssen Sie eine zweite Quorum-IP-Adresse hinzufügen, wenn Sie den Quorumdienst in der ztC Console hinzufügen.

Anforderungen für den Quorumcomputer

Sie können die Quorumdienstsoftware auf einem beliebigen Allzweckcomputer, Laptop oder einer VM ausführen, solange das Gerät über ein Windows-Betriebssystem verfügt und die folgenden Anforderungen erfüllt:

- Der Computer kann ständig eingeschaltet und mit dem Netzwerk verbunden sein, damit das ibiz0-Netzwerk des ztC Edge-Systems jederzeit Zugriff auf den Quorumserver hat.
- Der Computer hat eine statische IPv4-Netzwerkadresse. Verwenden Sie nicht DHCP.
- Das Betriebssystem ist Windows Server 2016, Windows Server 2012, Windows Server 2008, Windows 7 oder Windows 10; eingebettete Versionen des Windows-Betriebssystems werden nicht unterstützt.
- Es sind mindestens 100 MB Festplattenspeicherplatz verfügbar.
- Zwei UDP-Ports müssen für die Kommunikation zwischen den Knoten und dem Quorumdienst offen und verfügbar sein; dies gilt auch für die Firewalls. Standardmäßig sind dies die Ports 4557 und 4558. Wenn Sie diese Ports ändern müssen, lesen Sie Konfigurieren des Quorumdienst-Ports (auf dem Quorumcomputer) und Konfigurieren des Quorumservers über die ztC Console.

Herunterladen und Installieren der Quorumdienstsoftware

Nachdem Sie einen geeigneten Standort für den Quorumcomputer ermittelt haben, laden Sie die erforderliche Software herunter und installieren Sie sie, um den Quorumserver zu erstellen.

So laden Sie die Quorumserversoftware herunter und installieren sie

1. Öffnen Sie die Seite **Downloads** unter https://www.stratus.com/services-support/downloads/?tab=ztcedge.
2. Scrollen Sie nach unten zum Abschnitt **Drivers and Tools** (Treiber und Tools) und klicken Sie dann auf **Quorum Service**, um die Installationsdatei für die Quorumserversoftware auf den Quorumserver herunterzuladen.
3. Doppelklicken Sie auf dem Quorumserver auf die Installationsdatei.
4. Verschieben Sie die heruntergeladene Datei auf einen zugänglichen Speicherort.
5. Melden Sie sich beim Quorumcomputer an.
6. Navigieren Sie zur Installationsdatei des Quorumdienstes und doppelklicken Sie darauf.
7. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation abzuschließen.

Bei der Installation des Quorumdienstes wird eventuell der Produktname *everRun* angezeigt.

Hinweis: Wenn Sie ein Upgrade auf eine neuere Version der Quorumserversoftware ausführen, müssen Sie die vorherige Version **nicht** deinstallieren.

Abschließen der Konfiguration

Nachdem Sie die ALSR-Konfiguration erstellt haben, ändern Sie den Port des Quorumdienstes, falls erforderlich. Aktivieren Sie Quorum dann in der ztC Console. Abschließend überprüfen Sie die Konfiguration und verbinden Sie die VMs (erneut).

Voraussetzung: Planen und erstellen Sie eine ALSR-Konfiguration, indem Sie zunächst Erstellen einer ALSR-Konfiguration lesen und die entsprechenden Anweisungen befolgen, falls Sie dies noch nicht getan haben.

Hinweis: Der Port, der für den Quorumdienst auf dem Quorumcomputer konfiguriert wurde, und der Port, der in der ztC Console für den Quorumserver konfiguriert wurde, müssen dieselben Portnummern aufweisen. Wenn Sie den Quorumdienst-Port auf dem Quorumcomputer ändern, müssen Sie die Quorumdienst-Ports in allen ztC Edge-Systemen (über die ztC Console) ändern, die mit diesem Quorumcomputer verbunden sind, damit der Quorumcomputer und die ztC Edge-Systeme dieselben Portnummern verwenden. Siehe Konfigurieren des Quorumservers über die ztC Console.

Konfigurieren des Quorumdienst-Ports

Standardmäßig überwacht der Quorumdienst UDP-Port 4557.

In den meisten Fällen brauchen Sie den Standardport nicht zu ändern. Falls die Netzwerkkonfiguration es erfordert, können Sie den Port jedoch ändern:

So ändern Sie die Portnummer auf dem Quorumserver

1. Melden Sie sich beim Quorumcomputer mit einem Konto an, das über Administratorberechtigungen verfügt.
2. Öffnen Sie ein Befehlseingabefenster im administrativen Modus.
3. Beenden Sie den Quorumdienst, indem Sie Folgendes eingeben:
   ```
   net stop sraqserver
   ```
4. Ändern Sie den Port, indem Sie Folgendes eingeben (ersetzen Sie dabei *nnnn* durch die neue Portnummer):
   ```
   sraqserver -install nnnn
   ```
5. Starten Sie den Quorumdienst neu, indem Sie Folgendes eingeben:
   ```
   net start sraqserver
   ```

Überprüfen des Quorumdienst-Ports

Wenn Sie den Quorumdienst-Port überprüfen müssen, sehen Sie sich diesen Windows-Registrierungsschlüssel an:

```
HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\Services\SraQserver\Parameters\
QSServerPortForReceive
```

Konfigurieren des Quorumservers über die ztC Console

Sobald der Quorumdienst ausgeführt wird, sollten Sie den Quorumdienst in der ztC Console aktivieren. Sie können einen Quorumserver auch entfernen.

So aktivieren Sie den Quorumdienst

1. Melden Sie sich bei der ztC Console mit einem Konto an, das über Administratorberechtigungen verfügt.
2. Klicken Sie im linken Navigationsbereich auf **Voreinstellungen**, um die Seite **Voreinstellungen** zu öffnen.
3. Klicken Sie auf **Quorumserver**. Die Seite „Quorumkonfiguration“ wird angezeigt.
4. Klicken Sie links auf der Seite auf **Quorumserver hinzufügen**.
5. Geben Sie im Dialogfeld **Bevorzugten Quorumserver hinzufügen** die folgenden Werte ein (falls bereits ein bevorzugter Quorumserver vorhanden ist, wird das Dialogfeld **Alternativen Quorumserver hinzufügen** angezeigt):
   - **DNS oder IP-Adresse** - Geben Sie den vollständig qualifizierten **DNS**-Hostnamen oder die **IP-Adresse** für den bevorzugten Quorumserver ein.
   - **Port** - Standardmäßig wird Port 4557 verwendet. Geben Sie eine andere Portnummer ein, falls Sie einen abweichenden Port verwenden. Sie brauchen nur eine Portnummer einzugeben. Der Quorumdienst öffnet die Portnummer für **Port** und den nächsten Port (zum Beispiel 4557 und 4558).

     Hinweis: Die Portnummer muss mit dem Port übereinstimmen, den der Quorumdienst überwacht. (Falls es erforderlich ist, können Sie den Port auf dem Quorumserver ändern.)

   Klicken Sie auf **Speichern**, um die Werte zu speichern.
6. Wiederholen Sie die Schritte 4 und 5, um einen zweiten, alternativen Quorumserver zu konfigurieren. Stratus empfiehlt, zwei Quorumserver zu konfigurieren.
7. Um den Quorumdienst zu aktivieren, markieren Sie das Kontrollkästchen **Aktiviert** und klicken Sie auf **Speichern**.

Änderungen an der Quorumkonfiguration wirken sich nicht auf laufende VMs aus. Sie müssen alle VMs, die ausgeführt werden, beenden und neu starten, nachdem Sie die Quorumkonfiguration geändert haben.

So entfernen Sie einen Quorumserver

Achtung: Wenn Sie den bevorzugten Quorumserver entfernen, wird der alternative Quorumserver zum bevorzugten Quorumserver. Falls kein alternativer Quorumserver vorhanden ist, wird der Quorumdienst beim Entfernen des bevorzugten Quorumservers automatisch deaktiviert.

1. Navigieren Sie zur Seite **Voreinstellungen** der ztC Console.
2. Klicken Sie auf **Quorumserver**.
3. Suchen Sie den Eintrag für den Quorumserver, den Sie entfernen möchten.
4. Klicken Sie in der rechten Spalte auf **Entfernen**.

Hinweis: Falls eine VM den Quorumserver, den Sie entfernen, verwendet, müssen Sie die VM neu starten, sodass sie den Quorumserver nicht mehr erkennt, damit der Vorgang zum Entfernen abgeschlossen werden kann. Die VM läuft im Simplexmodus, bis sie ohne konfigurierte Quorumserver neu gestartet wird.

Überprüfen der Konfiguration und (erneutes) Verbinden der VMs

Überprüfen Sie die Konfiguration und verbinden Sie die VMs (erneut). Folgen Sie den erforderlichen Schritten in Von der ersten Bereitstellung zum Abschließen der ALSR-Konfiguration.

Quorum-Effekte auf das Systemverhalten

Ein Quorumserver in einem ALSR-System wirkt sich auf die Verfügbarkeit und das Wiederherstellungsverhalten des Systems aus. Um den Quorum-Effekt auf das Systemverhalten zu verstehen, muss man sich zunächst klarmachen, wie sich ein System ohne Quorumserver verhält.

Voraussetzung: Planen und erstellen Sie eine ALSR-Konfiguration, indem Sie zunächst Erstellen einer ALSR-Konfiguration lesen und die entsprechenden Anweisungen befolgen, falls Sie dies noch nicht getan haben.

Ein ztC Edge-System ist so konzipiert, dass es hohe Verfügbarkeit für eine oder mehrere Gast-VMs bietet. Dadurch können die VMs weiterhin ausgeführt werden, auch wenn es zu einem Fehler kommt, der andernfalls zum Ausfall der Anwendungen führen würde. Das ztC Edge-System kann Gast-VMs auch dann weiterhin

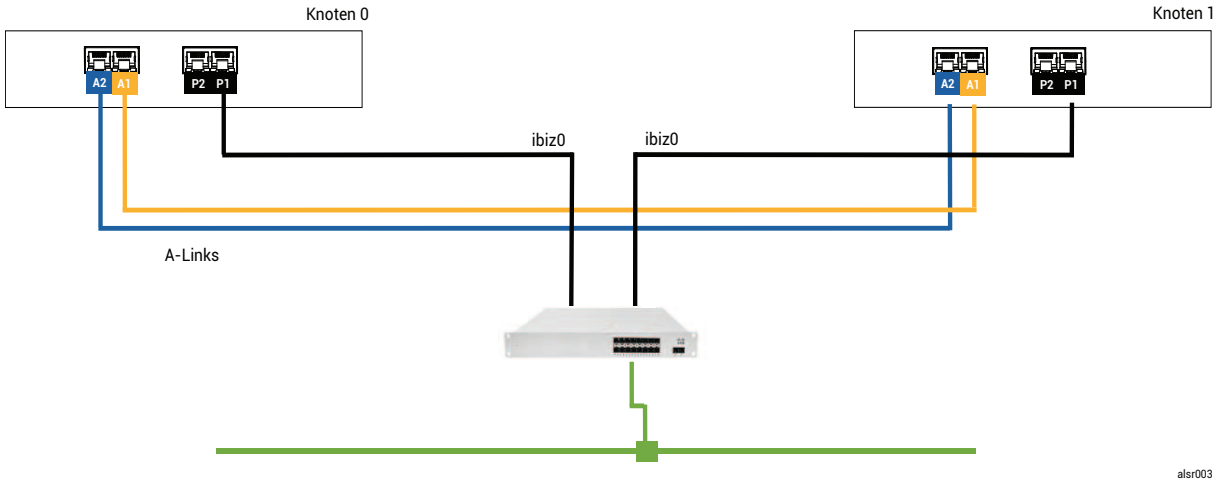
ausführen, wenn zum Beispiel eine einzelne Netzwerkverbindung, eine Festplatte oder sogar ein ganzer Computer ausfällt.

Wenn es jedoch zu einem schwerwiegenderen Fehler kommt (zum Beispiel Ausfall aller Netzwerkpfade), versucht das ztC Edge-System, den allgemeinen Zustand des Gesamtsystems zu bestimmen. Das System führt dann die notwendigen Maßnahmen aus, um die Integrität der Gast-VMs zu schützen.

Die folgenden Beispiele veranschaulichen den Systemprozess bei einem katastrophalen Fehler.

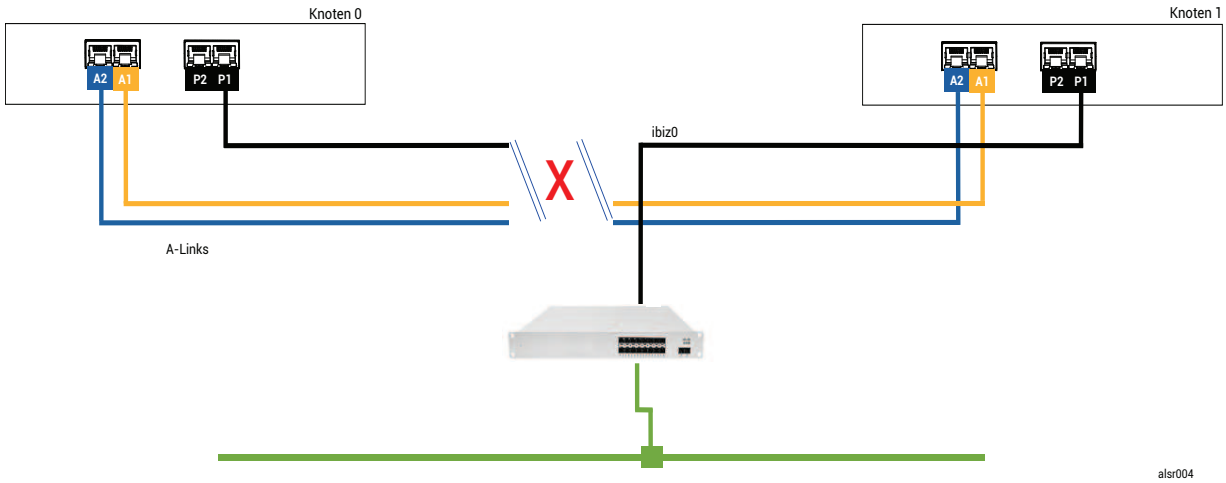
Beispiel 1: Split-Brain-Zustand in einem System ohne Quorumserver

In diesem ALSR-Beispiel enthält das ztC Edge-System Knoten0 und Knoten1, aber keinen Quorumserver. Der Betrieb ist normal, es werden keine Fehler erkannt. Die beiden Knoten kommunizieren ihren Zustand und ihre Verfügbarkeit über die A-Link-Verbindungen, wie immer im normalen (fehlerfreien) Betrieb. Die folgende Abbildung zeigt die normalen Verbindungen.



Ein katastrophaler Fehler

Ein unaufmerksamer Gabelstapler-Fahrer durchstößt eine Wand. Dabei werden alle Netzwerkverbindungen (Unternehmensnetzwerke und A-Links) durchtrennt, während die Stromversorgung intakt bleibt und das System weiterhin läuft. Die folgende Abbildung zeigt den Fehlerzustand.



Fehlerbehandlung

Die beiden Knoten gehen folgendermaßen mit dem Fehler um:

- Knoten0 – Die AX an Knoten0 erkennt den Verlust beider A-Links sowie aller anderen Netzwerkpfade. Da die Knoten0-AX ihren Partner nicht mehr findet, wird die Knoten0-AX aktiv und führt die Gast-VM aus. Die Anwendung innerhalb der Gast-VM wird weiterhin ausgeführt, möglicherweise mit eingeschränkter Kapazität aufgrund des Netzwerkverlusts.
- Knoten1 – Die AX an Knoten1 erkennt ebenfalls den Verlust beider A-Links, ibiz0 bleibt jedoch verfügbar. Da der Partner nicht mehr auf Meldungen in ibiz0 antwortet, ist jetzt die Knoten1-AX aktiv. Die Anwendung innerhalb der Gast-VM wird weiterhin ausgeführt, möglicherweise werden keinerlei Probleme mit dem System erkannt.

Aus der Sicht eines Anwendungs-Clients oder eines externen Beobachters sind beide Gast-VMs aktiv und generieren Netzwerkmeldungen mit derselben Rückgabeadresse. Beide Gast-VMs generieren Daten und erkennen unterschiedliche Mengen an Kommunikationsfehlern. Die Zustände der Gast-VMs weichen im Laufe der Zeit immer mehr voneinander ab.

Wiederherstellung und Reparatur

Nach einiger Zeit ist die Netzwerkkonnektivität wiederhergestellt, die Wand wurde repariert und die Netzwerkkabel wurden erneuert.

Wenn jede AX des AX-Paars erkennt, dass der Partner wieder online ist, wählt das AX-Paar anhand der Fehlerbehandlungsregeln die AX aus, die weiterhin aktiv bleibt. Diese Auswahl ist nicht vorhersagbar und berücksichtigt nicht, welcher Knoten während des Split-Brain-Zustands die genauere Performance zeigte.

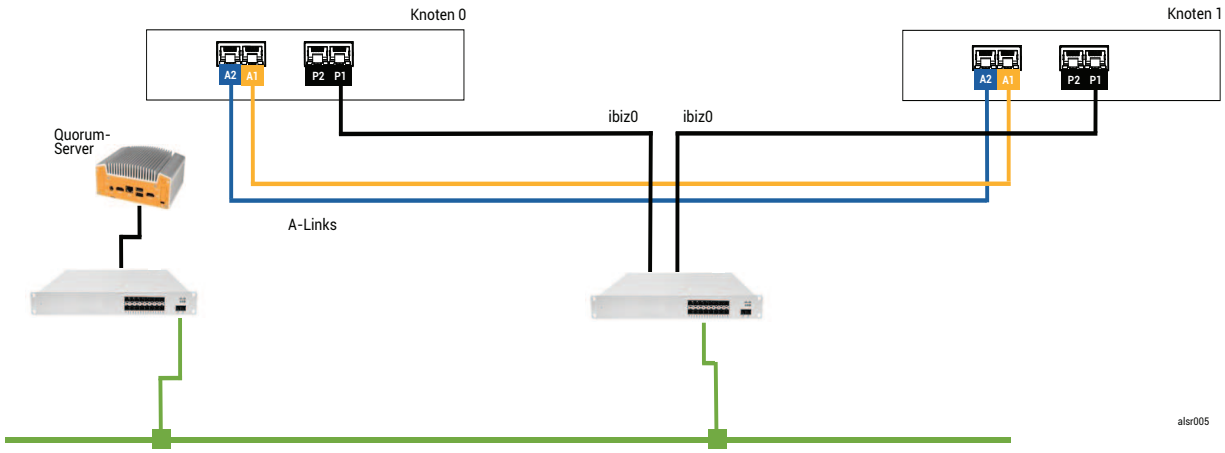
Die Daten, die von dem Knoten, der jetzt der Standby-Knoten ist, generiert wurden, werden durch die Resynchronisierung des aktiven Knotens überschrieben. Somit sind die Daten auf dem (derzeitigen) Standby-Knoten unwiderruflich verloren.

Nach einem Split-Brain-Zustand benötigt das System mehrere Minuten für die Resynchronisierung. Dieser Zeitraum ist davon abhängig, wie viel Festplattenaktivität an den Standby-Knoten übermittelt werden muss. Wenn mehrere Gast-VMs mit unterschiedlichen aktiven Knoten ausgeführt werden, kann Synchronisierungsdatenverkehr in beide Richtungen erfolgen.

Hinweis: Unter Umständen kann das ztC Edge-System nicht ermitteln, wie nach einem katastrophalen Fehler am besten vorzugehen ist. In diesem Fall muss das System manuell wiederhergestellt werden. Die empfohlene Wiederherstellungsmethode ist dann, mit der ztC Console einen Knoten herunterzufahren und neuzustarten, während der andere Knoten weiterhin ausgeführt wird. Diese Methode erzwingt normalerweise, dass der ausgeführte Knoten der primäre Knoten wird und die AX an diesem Knoten aktiv wird. Nachdem der ausgeführte Knoten der primäre Knoten ist, kann der andere Knoten durch einen Mitarbeiter eingeschaltet werden. Wenn die Resynchronisierung bereits ausgeführt wird, darf keiner der beiden Knoten heruntergefahren werden.

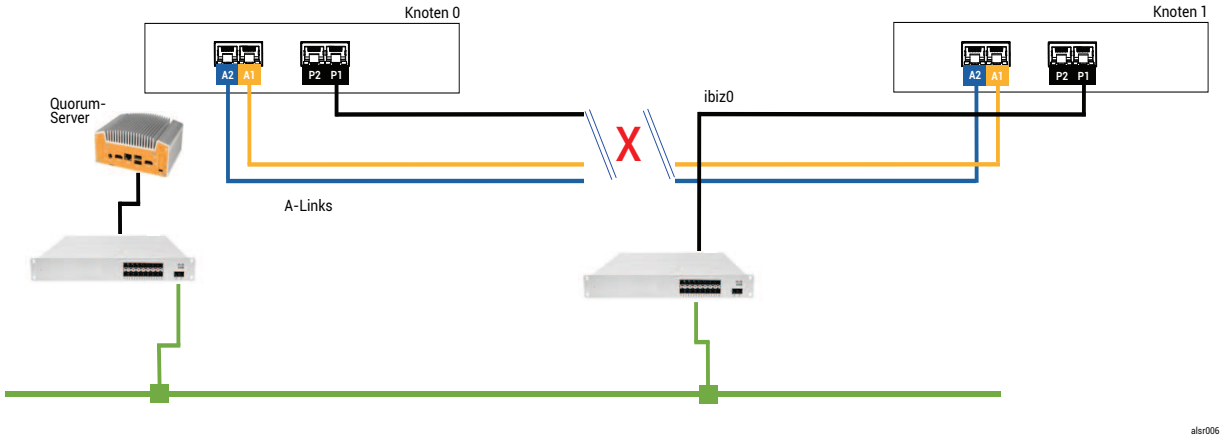
Beispiel 2: Ein ALSR-System mit einem Quorumserver vermeidet einen Split-Brain-Zustand

In diesem ALSR-Beispiel enthält das ztC Edge-System Knoten0 und Knoten1 mit Verbindungen wie beim System in Beispiel 1. Zusätzlich enthält das System in Beispiel 2 jedoch einen Quorumserver. Diese Abbildung veranschaulicht diese Verbindungen.



Ein katastrophaler Fehler

Der unaufmerksame Gabelstapler-Fahrer durchstößt schon wieder eine Wand. Dabei werden alle Netzwerkverbindungen durchtrennt, während die Stromversorgung intakt bleibt und das System weiterhin läuft. Die folgende Abbildung zeigt den Fehlerzustand.



Fehlerbehandlung

Die beiden Knoten gehen folgendermaßen mit dem Fehler um:

- Knoten0 – Die AX an Knoten0 erkennt den Verlust beider A-Links sowie aller anderen Netzwerkpfade. Da die Knoten0-AX ihren Partner nicht mehr findet, versucht die Knoten0-AX , den Quorumserver zu erreichen. In diesem Fall ist der Quorumserver jedoch ebenfalls nicht verfügbar. Deshalb fährt die Knoten0-AX herunter. Dabei handelt es sich nicht um ein ordnungsgemäßes Windows-Herunterfahren,

sondern um einen abrupten Stopp, der auch die Anwendung innerhalb der Gast-VM stoppt.

- Knoten1 – Die AX an Knoten1 erkennt ebenfalls den Verlust beider A-Links, ibiz0 bleibt jedoch verfügbar. Die Knoten1-AX versucht, den Quorumserver zu erreichen. Dieser antwortet, deshalb bleibt die Knoten1-AX aktiv. Die Anwendung innerhalb der Gast-VM wird ausgeführt, möglicherweise werden keinerlei Probleme mit dem System erkannt.

> **Hinweis**: Falls die Knoten1-AX zuvor nicht aktiv war und die Gast-VM eine HV-VM ist, muss die Gast-VM auf Knoten1 möglicherweise von der Festplatte von Knoten1 gestartet werden. In diesem Fall kommt es bei der Anwendung zu einem kurzen Ausfall, während die Gast-VM gestartet wird. (FT-VMs werden weiterhin ausgeführt.)

Aus der Sicht eines Anwendungs-Clients oder eines externen Beobachters bleibt die Gast-VM auf Knoten1 aktiv und generiert Daten, während die VM auf Knoten0 heruntergefahren wird. Es kommt zu keinem Split-Brain-Zustand.

Wiederherstellung und Reparatur

Nach einiger Zeit ist die Netzwerkkonnektivität wiederhergestellt, die Wand wurde repariert und die Netzwerkkabel wurden erneuert.

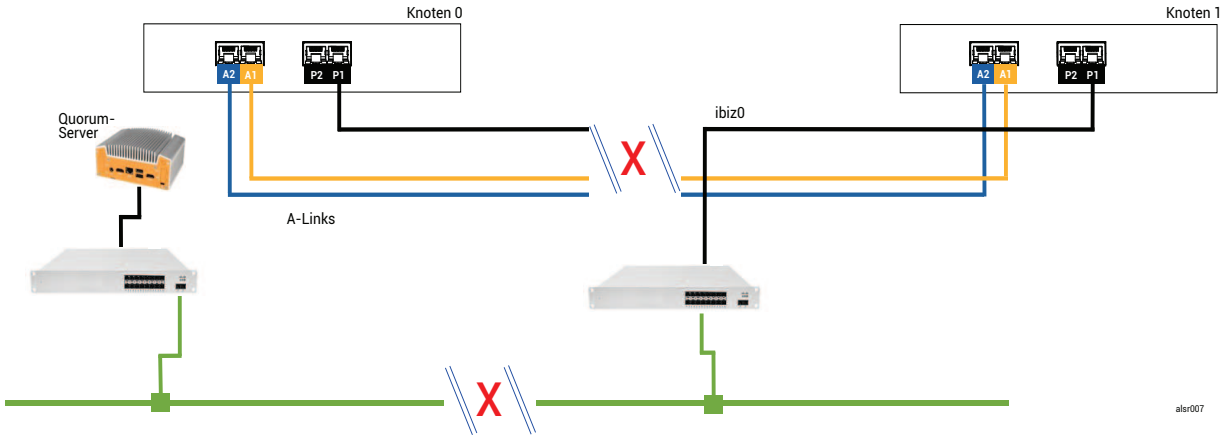
Wenn die Knoten1-AX erkennt, dass der Partner wieder online ist, wird die Knoten0-AX zum Standby-Knoten. Da Knoten0 zuvor nicht ausgeführt wurde, beginnt die Datensynchronisierung von Knoten1 zu Knoten0.

Da es nicht zu einer Split-Brain-Situation kam, sind keine Daten verloren gegangen.

Das System benötigt mehrere Minuten für die Resynchronisierung. Dieser Zeitraum ist davon abhängig, wie viel Festplattenaktivität an den Standby-Knoten übermittelt werden muss.

Beispiel 2, Variante: Der Quorumserver ist während des katastrophalen Fehlers nicht erreichbar

In einem ALSR-System mit einem Quorumserver ist der Quorumserver möglicherweise offline oder aus anderen Gründen nicht erreichbar, wenn bei dem katastrophalen Fehler alle Netzwerkverbindungen getrennt werden, obwohl die Stromversorgung erhalten bleibt und das System weiterhin läuft. Die folgende Abbildung zeigt ein System in dieser Situation, während der Quorumserver offline ist.



Die Fehlerbehandlung ist ähnlich wie in Beispiel 2 – mit einem wichtigen Unterschied für Knoten1:

> Die AX an Knoten1 erkennt ebenfalls den Verlust beider A-Links, ibiz0 bleibt jedoch verfügbar. Die Knoten1-AX versucht, den Quorumserver zu erreichen, die Kommunikation gelingt jedoch nicht. Die AX beendet die Gast-VM.

In diesem Fall wird die Gast-VM auf Knoten0 und Knoten1 heruntergefahren. Somit kommt es nicht zu einem Split-Brain-Zustand. Der Nachteil dabei ist, dass die Gast-VM nicht verfügbar ist, solange die Verbindung zu Knoten0 oder zum Quorumserver nicht wiederhergestellt wird.

In diesem Fall müssen Sie den Knoten bestimmen, der nicht in Betrieb sein soll, und ihn herunterfahren. Starten Sie den Knoten, der in Betrieb sein soll, und dann die VM. Informationen zum Herunterfahren und Starten einer VM finden Sie unter Verwalten des Betriebs einer virtuellen Maschine.

Beispiel 2, Variante: Der Quorumserver ist nicht erreichbar, ohne dass ein katastrophaler Fehler auftritt

Unter Umständen ist der Quorumserver nicht erreichbar, ohne dass ein katastrophaler Hardwarefehler aufgetreten ist. Dies ist zum Beispiel der Fall, wenn für Quorumcomputer aufgrund routinemäßiger Wartungsarbeiten (z. B. Anwendung von Betriebssystem-Patches) ein Neustart ausgeführt werden muss. In diesem Fall erkennt die AX, dass der Quorumserver nicht antwortet, und setzt den Synchronisierungsdatenverkehr aus, bis die Verbindung zum Quorumserver wiederhergestellt wird. Die Gast-VM wird weiterhin auf dem Knoten ausgeführt, der aktiv war, als die Verbindung unterbrochen wurde. Die Gast-VM wechselt jedoch nicht in den Standby-Modus, da möglicherweise weitere Fehler auftreten können. Nachdem der Quorumserver wiederhergestellt wurde, setzt die AX die Synchronisierung und die normale Fehlerbehandlung fort, solange die Verbindung zum Quorumserver erhalten bleibt.

Wiederherstellung nach einem Stromausfall

Wenn die Stromversorgung nach einem Stromausfall oder dem Ausschalten des Systems wiederhergestellt wird, wartet das ztC Edge-System für unbegrenzte Zeit darauf, dass sein Partner startet und antwortet, bevor das System Gast-VMs startet. Wenn die AX, die zuvor aktiv war, den Quorumserver erreichen kann, startet die AX die Gast-VM sofort, ohne darauf zu warten, dass der Partnerknoten gestartet wird. Wenn die AX, die zuvor der Standby-Knoten war, zuerst startet, wartet sie auf ihren Partnerknoten.

Falls das System eine Antwort vom Partnerknoten oder vom Quorumserver erhält, wird der normale Betrieb aufgenommen und die VM startet. Dabei gelten dieselben Fehlerbehandlungsregeln wie in anderen Situationen.

Falls das System keine Antwort vom Quorumserver erhält oder das System über keinen Quorumserver verfügt, muss ein Mitarbeiter eine Gast-VM starten und damit alle Entscheidungen der AX oder der Fehlerbehandlung übergehen. Sie müssen dafür sorgen, dass nicht zwei Personen gleichzeitig dieselbe Gast-VM auf Knoten0 und Knoten1 starten. Dies würde unbeabsichtigt einen Split-Brain-Zustand schaffen.

Zugriff auf Artikel in der Knowledge Base

Das **Stratus Customer Service Portal** bietet eine durchsuchbare **Knowledge Base** mit technischen Artikeln über alle Stratus-Produkte, darunter ztC Edge. In einigen Fällen verweist die Onlinehilfe direkt auf Artikel in der Knowledge Base (zum Beispiel KB-*nnnn*). Sie können mit Ihren vorhandenen Anmeldedaten für das Serviceportal auf das Customer Service Portal und die Knowledge Base zugreifen, oder Sie erstellen wie nachstehend beschrieben ein neues Benutzerkonto.

So nutzen Sie die Knowledge Base

1. Melden Sie sich beim **Stratus Customer Service Portal** unter https://support.stratus.com an.

   Erstellen Sie bei Bedarf ein neues Konto:

   a. Klicken Sie auf **Register Account** (Konto registrieren).

   b. Geben Sie Ihre Firmen-E-Mail-Adresse und Kontaktinformationen ein und klicken Sie auf **Register** (Registrieren).

      Ihre Firmen-E-Mail-Adresse muss einen Domänennamen (z. B. stratus.com) für eine Firma enthalten, die ein registrierter Kunde von Stratus ist.

   c. Klicken Sie in der E-Mail, die Sie von Stratus erhalten, auf den Link.

   d. Geben Sie ein neues Kennwort ein und schließen Sie die Konfiguration Ihres Kontos ab.

Falls Sie Unterstützung beim Erstellen eines Kontos benötigen, wenden Sie sich an Ihren autorisierten Stratus-Servicemitarbeiter.

2. Klicken Sie im Serviceportal im linken Fenster auf **Knowledge Base**.
3. Geben Sie im Feld **Keyword Search** (Stichwortsuche) Schlagwörter für die gesuchten Informationen ein und klicken Sie auf **Search** (Suchen).

   Um einen Artikel anhand seiner KB-*nnnn*-Nummer zu suchen, klicken Sie auf **Advanced Search** (Erweiterte Suche). Geben Sie neben **Search by ID** (Nach ID suchen) die Artikelnummer (*nnnn*) ein und klicken Sie auf **Display** (Anzeigen).

Verwandte Themen

Ergänzende Dokumentation

Behobene CVEs

Hier sind CVEs (Common Vulnerabilities and Exposures) aufgeführt, die in den folgenden Versionen behoben wurden.

In Stratus Redundant Linux Version 2.2.0.0 behobene CVEs

Die folgende Tabelle führt die in dieser Version behobenen CVEs auf (klicken Sie ggf. auf das Dropdownsymbol)

In dieser Version behobene CVEs		
CVE-2015-2716	CVE-2015-8035	CVE-2015-9289
CVE-2016-5131	CVE-2017-6519	CVE-2017-11166
CVE-2017-12805	CVE-2017-12806	CVE-2017-15412
CVE-2017-15710	CVE-2017-17807	CVE-2017-18251
CVE-2017-18252	CVE-2017-18254	CVE-2017-18258
CVE-2017-18271	CVE-2017-18273	CVE-2017-18595
CVE-2017-1000476	CVE-2018-1116	CVE-2018-1301

In dieser Version behobene CVEs		
CVE-2018-4180	CVE-2018-4181	CVE-2018-4300
CVE-2018-4700	CVE-2018-5712	CVE-2018-5745
CVE-2018-7191	CVE-2018-7418	CVE-2018-7584
CVE-2018-8804	CVE-2018-9133	CVE-2018-10177
CVE-2018-10360	CVE-2018-10547	CVE-2018-10804
CVE-2018-10805	CVE-2018-11362	CVE-2018-11439
CVE-2018-11656	CVE-2018-12599	CVE-2018-12600
CVE-2018-13139	CVE-2018-13153	CVE-2018-14340
CVE-2018-14341	CVE-2018-14368	CVE-2018-14404
CVE-2018-14434	CVE-2018-14435	CVE-2018-14436
CVE-2018-14437	CVE-2018-14567	CVE-2018-15518
CVE-2018-15587	CVE-2018-15607	CVE-2018-16057
CVE-2018-16328	CVE-2018-16749	CVE-2018-16750
CVE-2018-17199	CVE-2018-18066	CVE-2018-18544
CVE-2018-18751	CVE-2018-19622	CVE-22018-19869
CVE-2018-19870	CVE-2018-19871	CVE-2018-19872
CVE-2018-19873	CVE-2018-19985	CVE-2018-20169
CVE-2018-20467	CVE-2018-20852	CVE-2018-21009
CVE-2019-2737	CVE-2019-2739	CVE-2019-2740

In dieser Version behobene CVEs		
CVE-2019-2805	CVE-2019-3820	CVE-2019-3880
CVE-2019-3890	CVE-2019-3901	CVE-2019-5436
CVE-2019-6465	CVE-2019-6477	CVE-2019-7175
CVE-2019-7397	CVE-2019-7398	CVE-2019-9024
CVE-2019-9503	CVE-2019-9924	CVE-2019-9956
CVE-2019-9959	CVE-2019-10131	CVE-2019-10197
CVE-2019-10207	CVE-2019-10218	CVE-2019-10638
CVE-2019-10639	CVE-2019-10650	CVE-2019-10871
CVE-2019-11190	CVE-2019-11459	CVE-2019-11470
CVE-2019-11472	CVE-2019-11487	CVE-2019-11597
CVE-2019-11598	CVE-2019-11884	CVE-2019-12293
CVE-2019-12382	CVE-2019-12779	CVE-2019-12974
CVE-2019-12975	CVE-2019-12976	CVE-2019-12978
CVE-2019-12979	CVE-2019-13133	CVE-2019-13134
CVE-2019-13135	CVE-2019-13232	CVE-2019-13233
CVE-2019-13295	CVE-2019-13297	CVE-2019-13300
CVE-2019-13301	CVE-2019-13304	CVE-2019-13305
CVE-2019-13306	CVE-2019-13307	CVE-2019-13309
CVE-2019-13310	CVE-2019-13311	CVE-2019-13454

In dieser Version behobene CVEs		
CVE-2019-13648	CVE-2019-14283	CVE-2019-14815
CVE-2019-14980	CVE-2019-14981	CVE-2019-15090
CVE-2019-15139	CVE-2019-15140	CVE-2019-15141
CVE-2019-15221	CVE-2019-15605	CVE-2019-15916
CVE-2019-16056	CVE-2019-16708	CVE-2019-16709
CVE-2019-16710	CVE-2019-16711	CVE-2019-16712
CVE-2019-16713	CVE-2019-16746	CVE-2019-16865
CVE-2019-17041	CVE-2019-17042	CVE-2019-17540
CVE-2019-17541	CVE-2019-17666	CVE-2019-18634
CVE-2019-18660	CVE-2019-19338	CVE-2019-19527
CVE-2019-19768	CVE-2019-19948	CVE-2019-19949
CVE-2020-0543	CVE-2020-0548	CVE-2020-0549
CVE-2020-1938	CVE-2020-2754	CVE-2020-2755
CVE-2020-2756	CVE-2020-2757	CVE-2020-2773
CVE-2020-2781	CVE-2020-2800	CVE-2020-2803
CVE-2020-2805	CVE-2020-2830	CVE-2020-2922
CVE-2020-5208	CVE-2020-5260	CVE-2020-5312
CVE-2020-7039	CVE-2020-8112	CVE-2020-8597
CVE-2020-8608	CVE-2020-8616	CVE-2020-8617

In dieser Version behobene CVEs		
CVE-2020-9484	CVE-2020-10188	CVE-2020-10531
CVE-2020-10711	CVE-2020-10757	CVE-2020-10772
CVE-2020-11008	CVE-2020-12049	CVE-2020-12351
CVE-2020-12352	CVE-2020-12653	CVE-2020-12654
CVE-2020-12662	CVE-2020-12663	CVE-2020-12888
CVE-2020-14364	CVE-2020-14556	CVE-2020-14577
CVE-2020-14578	CVE-2020-14579	CVE-2020-14583
CVE-2020-14593	CVE-2020-14621	

In Stratus Redundant Linux Version 2.1.0.0 behobene CVEs

Die folgende Tabelle führt die in dieser Version behobenen CVEs auf (klicken Sie ggf. auf das Dropdownsymbol)

In dieser Version behobene CVEs		
CVE-2016-3186	CVE-2016-3616	CVE-2016-10713
CVE-2016-10739	CVE-2017-5731	CVE-2017-5732
CVE-2017-5733	CVE-2017-5734	CVE-2017-5735
CVE-2017-14503	CVE-2017-17742	CVE-2018-0495
CVE-2018-0734	CVE-2018-1050	CVE-2018-1111
CVE-2018-1122	CVE-2018-1139	CVE-2018-1312
CVE-2018-3058	CVE-2018-3063	CVE-2018-3066

In dieser Version behobene CVEs		
CVE-2018-3081	CVE-2018-3282	CVE-2018-3613
CVE-2018-5383	CVE-2018-5407	CVE-2018-5741
CVE-2018-6790	CVE-2018-6914	CVE-2018-6952
CVE-2018-7159	CVE-2018-7409	CVE-2018-7456
CVE-2018-7485	CVE-2018-7755	CVE-2018-8087
CVE-2018-8777	CVE-2018-8778	CVE-2018-8779
CVE-2018-8780	CVE-2018-8905	CVE-2018-9363
CVE-2018-9516	CVE-2018-9517	CVE-2018-10689
CVE-2018-10779	CVE-2018-10853	CVE-2018-10858
CVE-2018-10904	CVE-2018-10907	CVE-2018-10911
CVE-2018-10913	CVE-2018-10914	CVE-2018-10923
CVE-2018-10926	CVE-2018-10927	CVE-2018-10928
CVE-2018-10929	CVE-2018-10930	CVE-2018-10963
CVE-2018-11212	CVE-2018-11213	CVE-2018-11214
CVE-2018-11645	CVE-2018-11813	CVE-2018-12015
CVE-2018-12121	CVE-2018-12181	CVE-2018-12327
CVE-2018-12404	CVE-2018-12641	CVE-2018-12697
CVE-2018-12900	CVE-2018-13053	CVE-2018-13093
CVE-2018-13094	CVE-2018-13095	CVE-2018-13346

In dieser Version behobene CVEs		
CVE-2018-13347	CVE-2018-14348	CVE-2018-14498
CVE-2018-14598	CVE-2018-14599	CVE-2018-14600
CVE-2018-14625	CVE-2018-14647	CVE-2018-14651
CVE-2018-14652	CVE-2018-14653	CVE-2018-14654
CVE-2018-14659	CVE-2018-14660	CVE-2018-14661
CVE-2018-14734	CVE-2018-15473	CVE-2018-15594
CVE-2018-15686	CVE-2018-15853	CVE-2018-15854
CVE-2018-15855	CVE-2018-15856	CVE-2018-15857
CVE-2018-15859	CVE-2018-15861	CVE-2018-15862
CVE-2018-15863	CVE-2018-15864	CVE-2018-16062
CVE-2018-16396	CVE-2018-16402	CVE-2018-16403
CVE-2018-16646	CVE-2018-16658	CVE-2018-16838
CVE-2018-16842	CVE-2018-16866	CVE-2018-16881
CVE-2018-16885	CVE-2018-16888	CVE-2018-17100
CVE-2018-17101	CVE-2018-17336	CVE-2018-18074
CVE-2018-18281	CVE-2018-18310	CVE-2018-18384
CVE-2018-18520	CVE-2018-18521	CVE-2018-18557
CVE-2018-18661	CVE-2018-18897	CVE-2018-19058
CVE-2018-19059	CVE-2018-19060	CVE-2018-19149

In dieser Version behobene CVEs		
CVE-2018-19519	CVE-2018-19788	CVE-2018-20060
CVE-2018-20481	CVE-2018-20650	CVE-2018-20662
CVE-2018-20856	CVE-2018-20969	CVE-2018-1000073
CVE-2018-1000074	CVE-2018-1000075	CVE-2018-1000076
CVE-2018-1000077	CVE-2018-1000078	CVE-2018-1000079
CVE-2018-1000132	CVE-2018-1000876	CVE-2018-1000877
CVE-2018-1000878	CVE-2019-0154	CVE-2019-0155
CVE-2019-0160	CVE-2019-0161	CVE-2019-0217
CVE-2019-0220	CVE-2019-1125	CVE-2019-1387
CVE-2019-1559	CVE-2019-2503	CVE-2019-2529
CVE-2019-2614	CVE-2019-2627	CVE-2019-2945
CVE-2019-2949	CVE-2019-2962	CVE-2019-2964
CVE-2019-2973	CVE-2019-2975	CVE-2019-2978
CVE-2019-2981	CVE-2019-2983	CVE-2019-2987
CVE-2019-2988	CVE-2019-2989	CVE-2019-2992
CVE-2019-2999	CVE-2019-3459	CVE-2019-3460
CVE-2019-3811	CVE-2019-3827	CVE-2019-3840
CVE-2019-3846	CVE-2019-3858	CVE-2019-3861
CVE-2019-3880	CVE-2019-3882	CVE-2019-3900

In dieser Version behobene CVEs		
CVE-2019-5010	CVE-2019-5489	CVE-2019-6470
CVE-2019-7149	CVE-2019-7150	CVE-2019-7222
CVE-2019-7310	CVE-2019-7664	CVE-2019-7665
CVE-2019-9200	CVE-2019-9500	CVE-2019-9506
CVE-2019-9631	CVE-2019-9740	CVE-2019-9824
CVE-2019-9947	CVE-2019-9948	CVE-2019-10086
CVE-2019-10126	CVE-2019-10216	CVE-2019-11043
CVE-2019-11135	CVE-2019-11236	CVE-2019-11599
CVE-2019-11729	CVE-2019-11745	CVE-2019-11810
CVE-2019-11833	CVE-2019-12155	CVE-2019-13616
CVE-2019-13638	CVE-2019-13734	CVE-2019-14287
CVE-2019-14378	CVE-2019-14744	CVE-2019-14811
CVE-2019-14812	CVE-2019-14813	CVE-2019-14816
CVE-2019-14817	CVE-2019-14821	CVE-2019-14835
CVE-2019-14869	CVE-2019-14895	CVE-2019-14898
CVE-2019-14901	CVE-2019-14906	CVE-2019-15239
CVE-2019-17133	CVE-2019-18397	CVE-2019-18408
CVE-2019-1000019	CVE-2019-1000020	CVE-2019-1010238
CVE-2020-2583	CVE-2020-2590	CVE-2020-2593

In dieser Version behobene CVEs		
CVE-2020-2601	CVE-2020-2604	CVE-2020-2654
CVE-2020-2659		

In Stratus Redundant Linux Version 2.0.1.0 behobene CVEs

Die folgende Dropdowntabelle führt die in dieser Version behobenen CVEs auf (klicken Sie ggf. auf das Dropdownsymbol)

In dieser Version behobene CVEs		
CVE-2015-8830	CVE-2015-9262	CVE-2016-4913
CVE-2016-9396	CVE-2017-0861	CVE-2017-3735
CVE-2017-10661	CVE-2017-16997	CVE-2017-17805
CVE-2017-18198	CVE-2017-18199	CVE-2017-18201
CVE-2017-18208	CVE-2017-18232	CVE-2017-18267
CVE-2017-18344	CVE-2017-18360	CVE-2017-1000050
CVE-2018-0494	CVE-2018-0495	CVE-2018-0732
CVE-2018-0737	CVE-2018-0739	CVE-2018-1050
CVE-2018-1060	CVE-2018-1061	CVE-2018-1092
CVE-2018-1094	CVE-2018-1113	CVE-2018-1118
CVE-2018-1120	CVE-2018-1130	CVE-2018-1139
CVE-2018-1304	CVE-2018-1305	CVE-2018-5344
CVE-2018-5391	CVE-2018-5407	CVE-2018-5729

In dieser Version behobene CVEs		
CVE-2018-5730	CVE-2018-5742	CVE-2018-5743
CVE-2018-5803	CVE-2018-5848	CVE-2018-6485
CVE-2018-6764	CVE-2018-7208	CVE-2018-7568
CVE-2018-7569	CVE-2018-7642	CVE-2018-7643
CVE-2018-7740	CVE-2018-7757	CVE-2018-8014
CVE-2018-8034	CVE-2018-8781	CVE-2018-8945
CVE-2018-9568	CVE-2018-10322	CVE-2018-10372
CVE-2018-10373	CVE-2018-10534	CVE-2018-10535
CVE-2018-10733	CVE-2018-10767	CVE-2018-10768
CVE-2018-10844	CVE-2018-10845	CVE-2018-10846
CVE-2018-10852	CVE-2018-10858	CVE-2018-10878
CVE-2018-10879	CVE-2018-10881	CVE-2018-10883
CVE-2018-10902	CVE-2018-10906	CVE-2018-10911
CVE-2018-10940	CVE-2018-11236	CVE-2018-11237
CVE-2018-11784	CVE-2018-12126	CVE-2018-12127
CVE-2018-12130	CVE-2018-12180	CVE-2018-12910
CVE-2018-13033	CVE-2018-13405	CVE-2018-13988
CVE-2018-14526	CVE-2018-14618	CVE-2018-14633
CVE-2018-14646	CVE-2018-14665	CVE-2018-15688

In dieser Version behobene CVEs		
CVE-2018-15908	CVE-2018-15909	CVE-2018-15911
CVE-2018-16395	CVE-2018-16511	CVE-2018-16539
CVE-2018-16540	CVE-2018-16541	CVE-2018-16802
CVE-2018-16863	CVE-2018-16864	CVE-2018-16865
CVE-2018-16871	CVE-2018-16884	CVE-2018-17183
CVE-2018-17456	CVE-2018-17961	CVE-2018-17972
CVE-2018-18073	CVE-2018-18284	CVE-2018-18311
CVE-2018-18397	CVE-2018-18445	CVE-2018-18559
CVE-2018-18690	CVE-2018-19134	CVE-2018-19409
CVE-2018-19475	CVE-2018-19476	CVE-2018-19477
CVE-2018-1000007	CVE-2018-1000026	CVE-2018-1000120
CVE-2018-1000121	CVE-2018-1000122	CVE-2018-1000301
CVE-2019-2422	CVE-2019-2602	CVE-2019-2684
CVE-2019-2698	CVE-2019-2745	CVE-2019-2762
CVE-2019-2769	CVE-2019-2786	CVE-2019-2816
CVE-2019-2842	CVE-2019-3813	CVE-2019-3815
CVE-2019-3835	CVE-2019-3838	CVE-2019-3839
CVE-2019-3855	CVE-2019-3856	CVE-2019-3857
CVE-2019-3862	CVE-2019-3863	CVE-2019-5953

In dieser Version behobene CVEs		
CVE-2019-6116	CVE-2019-6133	CVE-2019-6454
CVE-2019-6778	CVE-2019-6974	CVE-2019-7221
CVE-2019-8322	CVE-2019-8323	CVE-2019-8324
CVE-2019-8325	CVE-2019-9636	CVE-2019-10132
CVE-2019-10160	CVE-2019-10161	CVE-2019-10166
CVE-2019-10167	CVE-2019-10168	CVE-2019-11085
CVE-2019-11091	CVE-2019-11477	CVE-2019-11478
CVE-2019-11479	CVE-2019-11811	CVE-2019-12735

In Stratus Redundant Linux Version 2.0.0.0 behobene CVEs

Die folgende Dropdowntabelle führt die in dieser Version behobenen CVEs auf (klicken Sie ggf. auf das Dropdownsymbol)

In dieser Version behobene CVEs		
CVE-2016-2183	CVE-2017-3636	CVE-2017-3641
CVE-2017-3651	CVE-2017-3653	CVE-2017-10268
CVE-2017-10378	CVE-2017-10379	CVE-2017-10384
CVE-2017-11600	CVE-2017-13215	CVE-2018-1336
CVE-2018-2562	CVE-2018-2622	CVE-2018-2640
CVE-2018-2665	CVE-2018-2668	CVE-2018-2755
CVE-2018-2761	CVE-2018-2767	CVE-2018-2771

In dieser Version behobene CVEs		
CVE-2018-2781	CVE-2018-2813	CVE-2018-2817
CVE-2018-2819	CVE-2018-2952	CVE-2018-3133
CVE-2018-3136	CVE-2018-3139	CVE-2018-3149
CVE-2018-3169	CVE-2018-3180	CVE-2018-3183
CVE-2018-3214	CVE-2018-3620	CVE-2018-3639
CVE-2018-3646	CVE-2018-3665	CVE-2018-3693
CVE-2018-5390	CVE-2018-5740	CVE-2018-7550
CVE-2018-7566	CVE-2018-8088	CVE-2018-10194
CVE-2018-10675	CVE-2018-10873	CVE-2018-10897
CVE-2018-10915	CVE-2018-11235	CVE-2018-11806
CVE-2018-12020	CVE-2018-12384	CVE-2018-14634
CVE-2018-15910	CVE-2018-16509	CVE-2018-16542
CVE-2018-1002200		

REST API-Aufrufe

Das ztC Edge-System unterstützt die folgenden REST API-Aufrufe (REST = Representational State Transfer; API = Application Program Interface):

- login
- overview
- vms

`login`

Stellt die Anmeldeinformationen für den Zugriff auf Ressourceninformationen bereit. Dieser Autorisierungsaufruf verhindert, dass nicht autorisierte Benutzer auf das System zugreifen. Geben Sie zuerst diesen Aufruf aus, kopieren Sie den Wert von `session-id` aus der JSON-Zeichenfolge der Antwort und verwenden Sie diesen Wert als JSESSIONID im Header zukünftiger Aufrufe.

Header	Wert	Erforderlich
Inhaltstyp	application/json	Ja

Anfrage	Wert	Erforderlich
Benutzername	Der Benutzername für die Anmeldung bei der ztC Console.	Ja
Kennwort	Das Kennwort für Benutzername.	Ja

Endpunkt

Das Folgende ist der Endpunkt mit einer Basis-URL `/restapi`:

```
POST /login
```

Beispiel

Anfrage-URL:

```
https://{hostname or IP address}/restapi/login
```

`overview`

Ruft Systeminformationen ab, darunter Eigenschaften der physischen Maschine, Statistiken, Systemleistung sowie eine aktuelle Meldungsliste. Die Antwort kann relativ groß sein (ca. 14 KB).

Header	Wert	Erforderlich
Sprache	de (Deutsch), en-US (Englisch), ja (Japanisch), zh-CN (Chinesisch) oder pt-br (Portugiesisch). Die	Nein

	Standardsprachversion ist en-US.	
Inhaltstyp	application/json	Ja

Endpunkt

```
GET /system/overview
```

Beispiel

Anfrage-URL:

```
https://{hostname or IP address}/restapi/system/overview
```

vms

Ruft eine Liste der im System vorhandenen VMs ab.

Header	Wert	Erforderlich
JSESSIONID	Wert von `session-id` in der Antwort auf den `login`-Aufruf	Ja
Inhaltstyp	application/json	Ja

Endpunkt

```
GET /v1/vms
```

Beispiel

Anfrage-URL:

```
https://{hostname or IP address}/restapi/v1/vms
```

11

Kapitel 11: Sicherheit

Mehr über zusätzliche Konfigurationseinstellungen, die Sie für das höchste Sicherheitsniveau eines ztC Edge-Systems implementieren können, finden Sie unter Sicherheitsverstärkung.

Zusätzliche Informationen zur Sicherheit finden Sie in den folgenden Themen:

- Behobene CVEs
- Verwalten von IPtables
- Konfigurieren von sicheren Verbindungen
- Konfigurieren von Benutzern und Gruppen
- Konfigurieren von Active Directory
- Die Seite „Auditprotokolle“

Sicherheitsverstärkung

Obwohl Stratus ztC Edge-Systeme ein sicheres Out-of-Box-Erlebnis bieten, können Sie für das höchste Sicherheitsniveau Konfigurationseinstellungen wie unten beschrieben implementieren.

Sicherheit ist häufig ein Kompromiss zwischen Schutz und Benutzerfreundlichkeit. ztC Edge-Systeme werden mit einer Reihe von Standardeinstellungen geliefert, die diese Faktoren in Einklang bringen. Für eine sicherere Positionierung befolgen Sie die nachstehenden Richtlinien und werten Sie die Sicherheit des Systems während des gesamten Lebenszyklus, von der Planung und Konfiguration bis zum Betrieb und der Außerbetriebnahme, aus.

Die folgenden Informationen liefern eine Anleitung für die Sicherheitsverstärkung auf Basis von Version 7.1 der *CIS Controls*, eine Empfehlung des Center for Internet Security (CIS), einer gemeinnützigen Organisation,

die bei besten Vorgehensweisen für den Schutz von IT-Systemen und Daten führend und anerkannt ist. *CIS Benchmarks* werden ebenfalls zur Validierung und Erstellung eines Ausgangspunkts für ein sicheres Produkt verwendet. Eine Liste von CIS Controls finden Sie unter Beste Vorgehensweisen und Normen der Normungsorganisationen.

Die folgenden Informationen liefern auch eine Anleitung für die Sicherheitsverstärkung auf Basis des Cybersicherheitsstandards für industrielle Kontrollsysteme ISA/IEC 62443, der ursprünglich durch die International Society of Automation (ISA) entwickelt wurde und von der International Electrotechnical Commission (IEC) weiterentwickelt wird. ISA/IEC 62443-4-2 hat verschiedene Sicherheitsstufen auf Basis der Sensibilität der Daten oder der zu bekämpfenden Bedrohung und hilft durch Implementierung der Empfehlungen und Anwendung von Abmilderungskontrollen bei der Erreichung der Einhaltung der erforderlichen Sicherheitsstufe. Eine Zusammenfassung der ISA/IEC 62443-4-2-Anforderungen finden Sie unter Beste Vorgehensweisen und Normen der Normungsorganisationen.

Dieses Hilfethema enthält die folgenden Abschnitte

- Sicherheitsrichtlinien
- Erweiterte Sicherheitsrichtlinien
- Beste Vorgehensweisen und Normen der Normungsorganisationen

Sicherheitsrichtlinien

Die folgenden Abschnitte beschreiben Sicherheitsrichtlinien für ztC Edge-Systeme.

> **Hinweis**: Stratus hat die folgenden Richtlinien getestet und unterstützt diese. Alle anderen Aktualisierungen oder Änderungen, die von Stratus nicht ausdrücklich genehmigt sind, könnten den normalen Betrieb des Systems beeinflussen.
>
> Wenn Sie Fragen zu diesen Richtlinien haben und das System durch einen Servicevertrag abgedeckt ist, wenden Sie sich an Ihren autorisierten Stratus-Servicemitarbeiter. Weitere Informationen finden Sie auf der Seite **ztC Edge Support** unter https://www.stratus.com/services-support/customer-support/?tab=ztcedge

Berücksichtigen Sie bei Implementierung der Richtlinien zur Sicherheitsverstärkung Folgendes:

- Die Sicherheitsrichtlinien beziehen sich auf Verwaltungsaufgaben, die in der ztC Console und im Host-Betriebssystem durchgeführt werden. Die ztC Console ist eine browserbasierte Benutzeroberfläche, die die Verwaltung und Überwachung der meisten Aspekte eines ztC Edge-Systems von einem

Remoteverwaltungscomputer aus ermöglicht (siehe Die ztC Console). Das Host-Betriebssystem wird auf jedem Knoten des Systems ausgeführt. Sie können auf die Befehlszeile des Host-Betriebssystem lokal an der physischen Konsole der PM oder remote durch Verwendung eines Secure Shell (SSH)-Clients zugreifen (siehe Zugriff auf das Host-Betriebssystem).

- Notieren Sie die aktuellen Einstellungen, bevor Sie Konfigurationsänderungen vornehmen, damit Sie diese bei Bedarf wiederherstellen können. Notieren Sie außerdem alle Änderungen, die Sie vornehmen, falls diese Informationen zur Fehlerbehebung benötigt werden.
- Beim Ändern der Standardsystemeinstellungen, insbesondere des Host-Betriebssystems, müssen Sie die Änderungen an beiden Knoten vornehmen, um Inkonsistenzen zu verhindern, die den normalen Betrieb des Systems beeinflussen könnten. Ähnlich müssen Sie, wenn Sie das `root`-Kennwort und andere Benutzerkontoeinstellungen für das Host-Betriebssystem ändern, dies an beiden Knoten tun. Die folgenden Richtlinien geben an, wann diese Änderungen nötig sind.
- Wenn Sie die Systemsoftware aktualisieren oder einen Knoten im System ersetzen, kann es sein, dass nicht alle Änderungen für die Sicherheitsverstärkung übertragen werden. Außerdem sind einige Einstellungen für alle Knoten gleich, damit es keine Konflikte bei gemeinsam genutzten Ressourcen gibt. Daher sollten Sie nach Abschluss dieser Verfahren prüfen, ob jeder Knoten im System die korrekten Einstellungen hat und dass das System ordnungsgemäß funktioniert.
- In einigen Fällen verweisen die Sicherheitsrichtlinien direkt auf Artikel in der Knowledge Base (zum Beispiel KB-*nnnn*) mit mehr Informationen über das Konfigurieren von ztC Edge-Systemen und der Stratus Redundant Linux-Software. Sie können mit Ihren vorhandenen Anmeldedaten für das Serviceportal auf das Stratus Customer Service Portal und die Knowledge Base zugreifen, oder Sie erstellen wie in Zugriff auf Artikel in der Knowledge Base beschrieben ein neues Benutzerkonto.

Ports und Protokolle

Administratoren, die Netzwerk- oder Kommunikationsänderungen am System vornehmen, sollten die durch Stratus Redundant Linux verwendeten Ports oder Protokolle kennen. Ausführliche Informationen finden Sie in KB-9357.

Netzwerksegmentierung

Verbinden Sie das ztC Edge-System nur mit Netzwerken mit vertrauenswürdigen Geräten oder mit Netzwerken, in denen Geräte eine ausdrückliche Genehmigung für die Kommunikation miteinander benötigen. Weitere Informationen zur Netzwerksegmentierung finden Sie in den speziellen NIST-Publikationen 800-125B

und 800-39. Informationen darüber, welche Ethernet-Netzwerke in ztC Edge-Systemen verfügbar sind, finden Sie unter Netzwerkarchitektur.

IP-Tabellen/Firewall

Aktivieren Sie IP-Tabellen-Paketfilterung für das System und blockieren Sie alle Ports, die im normalen Betrieb nicht verwendet werden. Böswillige Akteure können eine potenzielle Sicherheitsschwachstelle an einer nicht verwendeten Schnittstelle als Hintertür nutzen. Begrenzen Sie das Risiko, indem Sie IP-Tabellen für nicht verwendete Ports aktivieren.

Ausführliche Informationen dazu, wie Sie IP-Tabellen implementieren, finden Sie unter Verwalten von IPtables.

Hinweise:

- Das ICMP-Protokoll wird für Ping-Befehle im ztC Edge-System verwendet. Wenn Sie IP-Tabellen so einstellen, dass ICMP-Datenverkehr ausgelassen wird, funktionieren Fehlertoleranz oder Failover-Unterstützung nicht ordnungsgemäß.
- Das SSH-Protokoll wird für das Verbinden mit dem Host-Betriebssystem verwendet. Wenn Sie IP-Tabellen so einstellen, dass SSH-Datenverkehr blockiert wird, können Systemadministratoren nicht auf das Host-Betriebssystem zugreifen.

Erstellung von Benutzerkonten

Erstellen Sie individuelle Benutzerkonten für jeden Benutzer, der autorisiert ist, auf das System zuzugreifen, und berücksichtigen Sie die Rolle jedes Benutzers bei der Nutzung des Geräts. Die Pflege individueller Benutzerkonten erlaubt auch die Prüfbarkeit oder Nachweisführung, da durch Überprüfung des Protokolls festgestellt werden kann, welcher Benutzer auf das Gerät zugegriffen oder Konfigurationsänderungen vorgenommen hat.

Ausführliche Informationen dazu, wie Benutzereinstellungen konfiguriert werden, finden Sie unter Konfigurieren von Benutzern und Gruppen.

Hinweise:

- Das **Admin**-Standardkonto können Sie nicht löschen, Sie sollten aber den Namen und das Kennwort dieses Kontos ändern, indem Sie die Kontoeinstellungen bearbeiten.
- Sie müssen für jedes Benutzerkonto, auch **admin**, eine E-Mail-Adresse angeben, damit die Funktion zum Zurücksetzen des Kennworts verwendet werden kann. Außerdem müssen Sie den Mail-Server wie in Konfigurieren des Mail-Servers beschrieben aktivieren, da das System sonst keine E-Mails zum Zurücksetzen des Kennworts senden kann.

Kennworterstellung

Sie müssen die Standardkennwörter für das System ändern.

Die ztC Console fordert Sie bei Bereitstellung zur Eingabe eines neuen **admin**-Kennworts auf. In der Kennwortrichtlinie der ztC Console ist festgelegt, dass Ihr Kennwort die folgenden Bedingungen erfüllen muss:

- Es muss mindestens acht Zeichen enthalten.
- Es muss Groß- und Kleinbuchstaben enthalten.
- Es darf nicht mit dem Benutzernamen übereinstimmen.

Das Host-Betriebssystem fordert Sie beim erstmaligen Anmelden zur Eingabe eines neuen `root`-Kennworts auf. Wenn Sie das `root`-Kennwort für das Host-Betriebssystem ändern, müssen Sie es manuell auf beiden Knoten ändern. Details hierzu finden Sie unter Zugriff auf das Host-Betriebssystem.

Weitere Informationen zum Kontrollieren der Qualität von Kennwörtern in einem Host-Betriebssystem finden Sie unter Erweiterte Sicherheitsrichtlinien.

„Least Privilege“

Begrenzen Sie den Zugriff jedes Benutzers auf Funktionen, die für seine Position oder Rolle gelten.

Die Implementierung des „Least Privilege“-Zugriffs verhindert, dass nicht berechtigte Benutzer auf Dienste zugreifen, die über ihre Rolle hinaus gehen.

Ausführliche Informationen dazu, wie Rollen konfiguriert werden, die die Berechtigungen für jeden Benutzer definieren, finden Sie unter Konfigurieren von Benutzern und Gruppen.

Active Directory

Die Active Directory-Integration stellt eine einzige Stelle für die zentrale Authentifizierung und Autorisierung bereit. Mit Active Directory können Sie Gruppenrichtlinien für die Komplexität von Kennwörtern erstellen, die auf Basis Ihrer lokalen Sicherheitsrichtlinie durchgesetzt werden.

Ausführliche Informationen dazu, wie Sie ein ztC Edge-System zu einer Active Directory-Domäne hinzufügen, finden Sie unter Konfigurieren von Active Directory.

Zeitsynchronisierung

Die Synchronisierung der Zeit ist wichtig, da sie einen zentralen Referenzpunkt bereitstellt, um sicherzustellen, dass Betriebs- und Sicherheitsprozesse im selben Zeitrahmen arbeiten. Der Zeitbezug ermöglicht Vertrauen in den Zeitpunkt der Prüfung und den Zeitpunkt der Verwendung bei Aktualisierung von Anwendungen und die Sicherstellung, dass Schlüssel und Zertifikate auf Basis von Uhrzeit und Datum noch gültig sind.

Wenn Sie sich zum ersten Mal bei einem ztC Edge-System anmelden, aktivieren Sie den NTP-Dienst (Network Time Protocol), um die Systemuhr automatisch einzustellen. Konfigurieren Sie NTP, um auf einen bekannten und vertrauenswürdigen NTP-Server Bezug zu nehmen. Details hierzu finden Sie unter Konfigurieren von Datum und Uhrzeit.

> **Hinweis**: Verwenden Sie nur die ztC Console, um die NTP-Einstellungen ordnungsgemäß zu konfigurieren, und konfigurieren Sie diese nicht manuell im Host-Betriebssystem.

Sichere Verbindungen

Standardmäßig ist die ztC Console so konfiguriert, dass sie nur sichere Verbindungen mit dem HTTPS-Protokoll unterstützt.

Die Aktivierung von HTTPS auf dem ztC Edge-System verhindert häufige Websicherheitsangriffe und bietet einen Grad der Vertraulichkeit für jede Websitzung. HTTPS verschlüsselt den Websitzungsdatenverkehr, bietet Datenintegrität und erhöht die gesamte Sicherheit des Webdatenverkehrs.

Wenn HTTPS aktiviert ist, unterstützt es nur TLSv1.2, was zurzeit das stärkste empfohlene Verschlüsselungspaket darstellt. Chiffren sind u.a.:

TLSv1.2:
Chiffren:
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 4096) - A

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 4096) - A
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 4096) - A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 4096) - A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 4096) - A
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 4096) - A
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 4096) - A
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 4096) - A
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A

Aktivieren Sie außerdem sichere, verschlüsselte Verbindungen, wenn Sie einen Mail-Server oder andere Arten von Serversoftware verwenden. Informationen zum Konfigurieren und Aktivieren einer verschlüsselten Verbindung für den Mail-Server auf einem ztC Edge-System finden Sie unter Konfigurieren des Mail-Servers.

Aktualisierung des SSL-Zertifikats

Das ztC Edge-System wird mit einem selbstsignierten SSL-Zertifikat geliefert, dieses kann aber auf jedes gekaufte oder gelieferte Zertifikat aktualisiert werden. Die Änderung des SSL-Zertifikats ermöglicht die Aktualisierung des Vertrauensankers gemäß Kundenspezifikation. Ausführliche Informationen finden Sie in KB-9792.

SNMP-Konfigurationen

SNMP (Simple Network Management Protocol) ist ein Standardprotokoll, das für den Empfang von Alarmen, das Senden von Traps und das Überwachen des Systemstatus verwendet wird. SNMP verwendet systemdefinierende Informationen, die in hierarchisch konfigurierten Management Informationen Bases (MIBs) gespeichert sind.

Aus Sicherheitsgründen kann es sein, dass ein Kunde SNMP auf Hostebene in ztC Edge-Systemen deaktivieren möchte. Falls nötig, können Sie alle SNMP-Verbindungen durch Hinzufügen von Regeln zu IPtables deaktivieren (siehe Verwalten von IPtables), um UDP-Ports 162, 161 und 199 und TCP-Ports 162 und 199 zu blockieren.

Alternativ können Sie die **eingeschränkte** SNMP-Konfiguration verwenden, die SNMP v1 und v2 in den SNMP-Konfigurationsdateien deaktiviert und nur SNMPv3 konfiguriert. Details finden Sie unter Konfigurieren der SNMP-Einstellungen.

> **Hinweis**: Standardmäßig werden ztC Edge-Systeme mit aktiviertem SNMP v1 und v2 geliefert. Zur Sicherheit sollten diese Versionen deaktiviert und es sollte nur Version 3 aktiviert werden.

Sicherungen

Sicherungen sind für den Fall wichtig, dass ein Sicherheitsereignis auftritt, um ein Gerät für den fortgesetzten Betrieb auf einen bekannten guten Zustand zurückzusetzen. Alle durchgeführten Sicherungen sollten an einem sicheren Ort aufbewahrt werden.

Wie Sie eine VM und ihr Gastbetriebssystem sichern, finden Sie unter Exportieren einer virtuellen Maschine . Wie Sie die identische VM mit derselben SMBIOS UUID, derselben Systemseriennummer und denselben MAC-Adressen wie die ursprüngliche VM wiederherstellen, finden Sie unter Ersetzen/Wiederherstellen einer virtuellen Maschine aus einer OVF-Datei.

Um die ztC Edge-Systemvoreinstellungen, die Sie auf der Seite **Voreinstellungen** konfiguriert haben, zu sichern, können Sie die Einstellungen auf einem lokalen Speichergerät oder in der Cloud sichern. Details finden Sie unter Speichern und Wiederherstellen der Systemvoreinstellungen.

Auf redundanten ztC Edge-Systemen mit zwei Knoten dient jeder Knoten auch als Sicherung für den anderen Knoten. Wenn ein Knoten ausfällt, können Sie einen Knoten in einem System, das zurzeit lizenziert ist, ersetzen, und das System stellt automatisch den Knoten mit einer exakten Kopie der Stratus Redundant Linux-Software und den virtuellen Maschinen aus dem laufende Knoten her.

Automated Local Site Recovery

Eine Automated Local Site Recovery (ALSR)-Konfiguration verbindet zwei physische Maschinen an zwei separaten Standorten. Es handelt sich um eine notfalltolerante Implementierung, die Hardwareredundanz sowie die Redundanz physischer Rechenzentren und der Gebäude, die sie enthalten, bereitstellt. Aufgrund der räumlichen Trennung muss in einer ALSR-Konfiguration sorgfältig geplant werden, wo Komponenten platziert werden, und die Netzwerktopologie ist komplexer. Für ALSR-Konfigurationen empfiehlt Stratus dringend, den Quorumdienst zu verwenden, da die Link-Netzwerke in einer ALSR-Konfiguration dem Risiko weiterer potenzieller Ausfallszenarien ausgesetzt sind. (ALSR-Konfigurationen sind bei Systemen, die für einen Knoten lizenziert sind, nicht verfügbar.)

Ausführliche Informationen finden Sie unter Erstellen einer ALSR-Konfiguration.

Prüfung

Implementieren Sie eine Prüfung durch eine lokale Richtlinie, um regelmäßig Protokolle von Ereignissen zu sammeln und zu verwalten, die zum Erkennen und Verstehen von und Wiederherstellen nach einem Cyberangriff nötig sind.

Auf der Seite **Auditprotokolle** wird ein Protokoll der Benutzeraktivitäten in der ztC Console angezeigt. Um diese Seite zu öffnen, klicken Sie im linken Navigationsbereich auf **Auditprotokolle**. (Wie Sie Informationen zu Ereignissen im ztC Edge-System anzeigen, lesen Sie unter Die Seite „Alarmverlauf“.)

Protokollinformationen enthalten:

- Zeit – Das Datum und die Uhrzeit der Aktion.
- Benutzername – Der Name des Benutzers, der die Aktion initiiert hat.
- Ursprünglicher Host – Die IP-Adresse des Hosts, auf dem die ztC Console ausgeführt wurde.
- Aktion – Die Aktion, die in der ztC Console ausgeführt wurde.

Sie können Informationen zu Auditprotokollen auch durch Verwendung von `snmptable` anzeigen (Details siehe Beziehen der System-Informationen mit snmptable.)

Verwenden Sie Protokolle für die kontinuierliche Überwachung des ztC Edge-Systems. Um umgehenden Service bei einem Serviceanruf sicherzustellen, sollten Sie auch Supportbenachrichtigungen und regelmäßige Berichterstellung für Ihr System aktivieren, um Stratus über den Zustand des Systems auf dem Laufenden zu halten. Details finden Sie unter Konfigurieren der Remotesupport-Einstellungen.

Upgrades

Aktualisieren Sie Stratus Redundant Linux regelmäßig, um das Ausnutzen von Sicherheitsschwachstellen aufgrund veralteter Komponenten zu verhindern. Zur Information über Häufigkeit und Methoden verweisen wir Sie auf Ihre lokalen Sicherheitsrichtlinien.

> **Achtung**: Aktualisieren Sie das CentOS-Host-Betriebssystem auf dem ztC Edge-System nicht aus irgendeiner anderen Quelle als Stratus. Verwenden Sie nur die CentOS-Version, die mit der Stratus Redundant Linux-Software installiert wurde.

Auf der Seite **-Upgrade-Kits** in der ztC Console können Sie Upgrade-Kits hochladen und verwalten, mit denen Sie das System auf eine neuere Version der Stratus Redundant Linux-Software aktualisieren können.

Sie können ein Upgrade-Kit auch auf einen USB-Stick kopieren, um diesen bei der Neuinstallation der Systemsoftware zu verwenden.

Um die Seite **Upgrade-Kits** zu öffnen, klicken Sie im linken Navigationsbereich der ztC Console auf **Upgrade-Kits**.

Informationen zum Aktualisieren der Stratus Redundant Linux-Software finden Sie unter Upgrade der Stratus Redundant Linux-Software mit einem Upgrade-Kit. Informationen zum Erstellen von USB-Medien finden Sie unter Erstellen eines USB-Mediums mit Systemsoftware.

Physische Sicherheit

Installieren Sie jedes ztC Edge-System an einem sicheren Ort, um zu verhindern, dass böswillige Benutzer auf die Knoten zugreifen.

Schützen Sie jeden Ort mit einem prüfbaren System, um zu identifizieren, welche Personen den Bereich betreten haben, und so böswillige Benutzer zu identifizieren.

Physische Sicherheit ist eine wichtige Ergänzung der Manipulationserkennung und Warnung für jedes Gerät, einschließlich ztC Edge-Knoten.

Erweiterte Sicherheitsrichtlinien

Die folgenden Abschnitte beschreiben erweiterte Sicherheitsrichtlinien für ztC Edge-Systeme.

Empfehlungen zur Kennwortqualität

Empfehlungen zum Festlegen von Kennwörtern:

- Einstellung einer Mindestlänge für Kennwörter von 8 Zeichen, die drei von vier der folgenden Eigenschaften erfüllen: ein Großbuchstabe, ein Kleinbuchstabe, eine Zahl und ein Sonderzeichen.
- Forderung, dass Benutzer Kennwörter regelmäßig zurücksetzen, zum Beispiel alle 30, 60 oder 90 Tage. Sie können die erneute Verwendung von Kennwörtern auf Basis der Kennwortaktualisierungshistorie für einen variablen Zeitraum verbieten.

So aktualisieren Sie die Kennwortqualitätseinstellungen im Host-Betriebssystem

Hinweis: Wenden Sie die Kennwortqualitätseinstellungen auf beide Knoten im System an.

1. Melden Sie sich am Host-Betriebssystem an, wie unter Zugriff auf das Host-Betriebssystem beschrieben.
2. Öffnen Sie die Datei `/etc/pam.d/system-auth` mit einem Texteditor.
3. Ändern Sie das Modul `pam_pwquality.so` mit den entsprechenden Einstellungen. Verwenden Sie zum Beispiel ähnliche Einstellungen wie die folgenden:

   ```
   password requisite pam_pwquality.so try_first_pass local_
   users_only retry=3 authtok_type= minlen=8 lcredit=-1
   ucredit=-1 dcredit=-1 ocredit=-1 enforce_for_root
   ```

   Im vorherigen Beispiel werden die folgenden Werte eingestellt:

   `minlen=8` stellt die Mindestlänge für das Kennwort auf 8 Zeichen ein.

   `lcredit=-1` stellt die mindestens erforderliche Anzahl von Kleinbuchstaben in einem Kennwort auf eins ein.

   `ucredit=-1` stellt die mindestens erforderliche Anzahl von Großbuchstaben in einem Kennwort auf eins ein.

   `dcredit=-1` stellt die mindestens erforderliche Anzahl von Zahlen in einem Kennwort auf eins ein.

   `ocredit=-1` stellt die mindestens erforderliche Anzahl von anderen Symbolen wie @, #, ! $ % in einem Kennwort auf eins ein.

   `enforce_for_root` stellt sicher, dass auch wenn der `root`-Benutzer das Kennwort festlegt, die Komplexitätsrichtlinien durchgesetzt werden sollen.
4. Um die Kennworthistorie einzuschränken, fügen Sie das Modul `pam_pwhistory.so` mit den entsprechenden Einstellungen hinzu oder ändern Sie es. Zum Beispiel durch Verwendung ähnlicher Einstellungen wie der folgenden:

   ```
   password requisite pam_pwhistory.so debug use_authtok
   remember=10 retry=3
   ```
5. Speichern Sie die Datei `/etc/pam.d/system-auth`.

Weitere Informationen über Kennwortrichtlinien im Host-Betriebssystem finden Sie in der CentOS-Dokumentation:

https://wiki.centos.org/HowTos/OS_Protection#Password_Policies

Verwaltung gleichzeitiger Benutzer

Überprüfen Sie die Auditprotokolle regelmäßig, um zu sehen, welche Benutzer sich an der Maschine angemeldet haben und ob sie noch aktiv sind.

Identifizieren Sie die Benutzer, die das System zurzeit betreiben, um ihre Nutzung zu legitimieren und zu prüfen.

Antivirus

Führen Sie regelmäßig eine netzwerkbasierte Analyse der Viren- und Malware-Erkennung durch.

Ihr netzwerkbasiertes Angrifferkennungssystem ergänzt die ztC Edge-Fähigkeit zur Unterstützung der Verifizierung des beabsichtigten Betriebs der Sicherheitsfunktionen. Das Erkennungssystem sollte nach ungewöhnlichem Netzwerkdatenverkehr suchen und eine Untersuchung fordern, um böswillige Absichten zu validieren.

SSH-Zugriffsbeschränkungen

Mehrere `/etc/ssh/sshd_config`-Parameter beschränken, welche Benutzer und Gruppen durch SSH auf das System zugreifen können. Wenn keiner der folgenden Parameter in der Datei vorhanden ist, bearbeiten Sie die Datei, um ein oder mehrere davon einzustellen und so den Zugriff zu beschränken.

`AllowUsers`

Der Parameter `AllowUsers` bietet Systemadministratoren die Möglichkeit, spezifischen Benutzern die Verwendung von SSH für den Zugriff auf das System zu erlauben. Die Liste besteht aus Benutzernamen, die durch Leerzeichen getrennt sind. Dieser Parameter erkennt keine numerischen Benutzer-IDs. Um den Benutzerzugriff weiter einzuschränken, indem es nur den zulässigen Benutzern erlaubt wird, sich von einem Host anzumelden, kann der Eintrag in der Form benutzer@host spezifiziert werden.

`AllowGroups`

Der Parameter `AllowGroups` bietet Systemadministratoren die Möglichkeit, spezifischen Gruppen von Benutzern die Verwendung von SSH für den Zugriff auf das System zu erlauben. Die Liste besteht aus Gruppennamen, die durch Leerzeichen getrennt sind. Dieser Parameter erkennt keine numerischen Gruppen-IDs.

`DenyUsers`

Der Parameter `DenyUsers` bietet Systemadministratoren die Möglichkeit, spezifischen Benutzern die Verwendung von SSH für den Zugriff auf das System zu verweigern. Die Liste besteht aus Benutzernamen,

die durch Leerzeichen getrennt sind. Dieser Parameter erkennt keine numerischen Benutzer-IDs. Wenn ein Systemadministrator den Benutzerzugriff weiter einschränken möchte, indem er den Zugriff eines Benutzers von einem Host speziell verweigert, kann der Eintrag in der Form benutzer@host spezifiziert werden.

`DenyGroups`

Der Parameter `DenyGroups` bietet Systemadministratoren die Möglichkeit, spezifischen Gruppen von Benutzern die Verwendung von SSH für den Zugriff auf das System zu verweigern. Die Liste besteht aus Gruppennamen, die durch Leerzeichen getrennt sind. Dieser Parameter erkennt keine numerischen Benutzer-IDs.

Die Einschränkung, welche Benutzer mithilfe von SSH remote auf das System zugreifen können, trägt dazu bei, sicherzustellen, dass nur autorisierte Benutzer auf das System zugreifen.

`MaxAuthTries`

Der Parameter `MaxAuthTries` gibt die maximale Anzahl an Authentifizierungsversuchen an, die pro Verbindung erlaubt sind. Wenn die Zahl fehlerhafter Anmeldungen die Hälfte der Anzahl erreicht, werden Fehlermeldungen mit einer genaueren Angabe des Anmeldefehlers in die Datei `syslog` geschrieben.

Die Einstellung des Parameters `MaxAuthTries` auf eine niedrige Zahl minimiert die Gefahr erfolgreicher Brute-Force-Angriffe auf den SSH-Server. Die empfohlene Einstellung ist 4, Sie sollten die Zahl jedoch auf Basis der Standortrichtlinie einstellen. Beispiel:

```
MaxAuthTries 4
```

`IgnoreRhosts`

Der Parameter `IgnoreRhosts` gibt an, dass die Dateien `.rhosts` und `.shosts` nicht in `RhostsRSAAuthentication` oder `HostbasedAuthentication` verwendet werden.

Die Einstellung dieses Parameters zwingt Benutzer, bei der Authentifizierung mit SSH ein Kennwort einzugeben. Beispiel:

```
IgnoreRhosts yes
```

`HostbasedAuthentication`

Der Parameter `HostbasedAuthentication` gibt an, ob Authentifizierung über vertrauenswürdige Hosts durch Verwendung von `.rhosts` oder `/etc/hosts.equiv` mit erfolgreicher Client-Hostauthentifizierung mit öffentlichem Schlüssel erlaubt ist. Diese Option gilt nur für SSH-Protokoll Version 2.

Auch wenn `.rhosts`-Dateien unwirksam sind, wenn Unterstützung in `/etc/pam.conf` deaktiviert ist, bietet die Deaktivierung der Fähigkeit, `.rhosts`-Dateien in SSH zu verwenden, eine zusätzliche Schutzebene. Beispiel:

```
HostbasedAuthentication no
```

Weitere Informationen zu den `sshd_config`-Parametern finden Sie auf der Handbuchseite `sshd_config(5)`.

Beste Vorgehensweisen und Normen der Normungsorganisationen

Die Informationen in diesem Thema basieren auf den folgenden besten Vorgehensweisen und Standards.

CIS Controls Version 7.1

CIS Controls sind ein priorisierter Satz bester Vorgehensweisen, die erstellt wurden, um die verbreitetsten und gefährlichsten Bedrohungen von heute zu stoppen. Sie wurden durch führende Sicherheitsexperten aus der ganzen Welt entwickelt und werden jedes Jahr verfeinert und validiert. Nähere Informationen finden Sie auf der CIS-Website: https://www.cisecurity.org.

Die CIS Controls sind:

Basic

1. Inventarisierung und Kontrolle der Hardware
2. Inventarisierung und Kontrolle der Software
3. Kontinuierliches Schwachstellenmanagement
4. Kontrollierte Nutzung von Administratorrechten
5. Sichere Konfiguration für Hardware und Software auf mobilen Geräten, Laptops, Workstations und Servern
6. Wartung, Überwachung und Analyse von Auditprotokollen

Foundational

7. E-Mail- und Webbrowser-Sicherheit
8. Malware-Abwehr
9. Begrenzung und Kontrolle von Ports, Protokollen und Diensten
10. Datenwiederherstellungsfähigkeiten

11. Sichere Konfiguration von Netzwerkgeräten wie Firewalls, Routern und Switches
12. Verteidigung an den Netzwerkgrenzen
13. Datenschutz
14. Zugangskontrolle nach dem „Need to know“-Prinzip
15. Kontrolle der drahtlosen Zugriffe
16. Überwachung und Kontrolle von Nutzerkonten

Organizational

17. Implementierung von Security Awareness und Schulungsprogrammen
18. Sicherheit für Anwendungssoftware
19. Incident Response and Management
20. Penetrationstests und Red-Team-Übungen

ISA/IEC 62443-4-2

ISA/IEC 62443-4-2 beschreibt technische Komponentenanforderungen (Component Requirements, CRs), die mit den sieben grundlegenden Anforderungen (Foundational Requirements, FRs) für die Erfüllung der Sicherheitsstufen der Kontrollsystemfähigkeit verbunden sind, genauer. Nähere Informationen finden Sie auf der IEC-Website: https://www.iec.ch/

Die grundlegenden Anforderungen sind:

1. Identifizierung und Authentifizierung (Identification and authentication control, IAC)
2. Nutzungskontrolle (Use control, UC)
3. Systemintegrität (System integrity, SI)
4. Vertraulichkeit der Daten (Data confidentiality, DC)
5. Eingeschränkter Datenfluss (Restricted data flow, RDF)
6. Rechtzeitige Reaktion auf Ereignisse (Timely response to events, TRE)
7. Verfügbarkeit der Ressourcen (Resource availability, RA)

1. Identifizierung und Authentifizierung (Identification and authentication control, IAC)

Die Identifizierung von Benutzern wird zusammen mit Autorisierungsmechanismen verwendet, um Zugriffskontrolle für eine Komponente zu implementieren. Eine Verifizierung der Identität von Benutzern, die Zugriff anfordern, damit nicht autorisierte Benutzern keinen Zugriff auf die Komponente erhalten. Die

Autorisierung erfolgt von Zugriffskontrolllisten für verschiedene Benutzer, die sich mit Kennwörtern am ztC Edge-System anmelden und authentifizieren.

2. Nutzungskontrolle (Use control, UC)

Sobald der Benutzer identifiziert und autorisiert ist, muss die Komponente die erlaubten Aktionen auf die autorisierte Verwendung der Komponente beschränken. Das ztC Edge-System hat definierte Rollen, die das „Least Privilege“-Konzept implementieren. Durch Erstellung mehrerer Benutzer mit verschiedenen Zugriffskontrollstufen wird außerdem die autorisierte Verwendung der Komponente definiert.

3. Systemintegrität (System integrity, SI)

Die Integrität des Geräts sollte nicht gefährdet werden, dies gilt sowohl für die Software als auch die physischen Komponenten im Betriebs- und Nicht-Betriebszustand. Das ztC Edge-System implementiert sicheres Booten, was dafür sorgt, dass das Gerät aus einem vertrauenswürdigen Zustand gebootet oder gestartet wird, wobei digitale Signaturen der Softwarekomponenten vor einem Upgrade validiert werden. Die Sicherstellung der Systemintegrität ist für den Schutz vor unbefugter Manipulation oder Änderung der Daten oder des Systems wichtig.

4. Vertraulichkeit der Daten (Data confidentiality, DC)

Zweck ist die Sicherstellung der Vertraulichkeit von Informationen auf Kommunikationskanälen und in Daten, die in Repositorys gespeichert sind, zum Schutz vor unbefugter Offenlegung. Das ztC Edge-System hat HTTPS mit TLS v1.2 für die Webkommunikation sowie SSH und SMTP mit Verschlüsselung zur Sicherstellung, dass Informationen vor böswilligen Personen geschützt sind.

5. Eingeschränkter Datenfluss (Restricted data flow, RDF)

Eingeschränkter Datenfluss ist die Segmentierung des Kontrollsystems durch Zonen und Kanäle zur Begrenzung des unnötigen Flusses von Daten. Die ztC Edge-Netzwerkarchitektur unterstützt Routing und Switching wie durch die Konfiguration der Vernetzung für die Verwaltung des Informationsflusses durch den installierenden Systemtechniker bestimmt. Die Nutzung der Vernetzungsfähigkeiten des ztC Edge-Systems ermöglicht eine Begrenzung des Datenflusses durch Netzwerksegmentierung.

6. Rechtzeitige Reaktion auf Ereignisse (Timely response to events, TRE)

Auch wenn ein System den Betrieb in einem sicheren Zustand beginnt, können Schwachstellen und Sicherheitsereignisse auftreten. Das ztC Edge-System hat ein Product Security Incident Response (PSIR)-Team, um auf Sicherheitsvorfälle und Berichtserkenntnisse zu reagieren und gleichzeitig Probleme zeitnah zu beheben. Das ztC Edge-System hat Alarmprotokolle, die verwendet werden können, um die entsprechenden Kanäle über Konfigurationsänderungen zu informieren, die auf einen Sicherheitsvorfall hinweisen können. Die

Protokolle enthalten genug Informationen für die Forensik und diese E-Alert-Benachrichtigungen werden per E-Mail versendet.

7. Verfügbarkeit der Ressourcen (Resource availability, RA)

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Komponente gegenüber verschiedenen Arten von Denial-of-Service-Ereignissen resistent ist. Die hohe Verfügbarkeit des ztC Edge-Systems ist die Grundlage eines „Always on"-Zustands. Es ist äußerst wichtig, dass industrielle Kontrollsysteme einen hohen Verfügbarkeitszustand aufrechterhalten, da es mögliche lebensrettende Auswirkungen auf Systeme gibt. Mit einer integrierten Virtualisierungs- und Verfügbarkeitsschicht, automatischem Datenschutz und Anwendungswiederherstellung verringert Stratus Redundant Linux die Abhängigkeit von der IT beim virtuellen Edge Computing erheblich. Die selbstschützenden und selbstüberwachenden Funktionen helfen bei der Reduzierung ungeplanter Ausfallzeiten und stellen die kontinuierliche Verfügbarkeit geschäftskritischer industrieller Anwendungen sicher.

12

Kapitel 12: SNMP

SNMP (Simple Network Management Protocol) ist ein Standardprotokoll, das für den Empfang von Alarmen, das Senden von Traps und das Überwachen des Systemstatus verwendet wird. SNMP verwendet systemdefinierende Informationen, die in hierarchisch konfigurierten Management Informationen Bases (MIBs) gespeichert sind.

Informationen zum Konfigurieren eines ztC Edge-Systems für die Verwendung von SNMP finden Sie unter Konfigurieren der SNMP-Einstellungen.

Informationen zur Verwendung des `snmptable`-Befehls zum Abrufen von Informationen zum System, speziell zu Alarmen, Auditprotokollen, Knoten, VMs und Volumes, finden Sie unter Beziehen der System-Informationen mit snmptable.

Sie finden eine Kopie der MIB-Datei zum Herunterladen im Abschnitt **Drivers and Tools** der Seite **Downloads** unter https://www.stratus.com/services-support/downloads/?tab=ztcedge.

Beziehen der System-Informationen mit snmptable

Sie können den `snmptable`-Befehl zum Abrufen von Informationen zum System, speziell zu Alarmen, Auditprotokollen, Knoten, VMs und Volumes verwenden.

So zeigen Sie Informationen zu Alarmen an

Geben Sie den folgenden Befehl ein, um Informationen zu Alarmen anzuzeigen:

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c
public localhost ztCEdgeAlertTable
```

Die Befehlsausgabe zeigt Folgendes an:

Feld	Beschreibung
`ztCEdgeAlertIndex`	Die Alarmnummer.
`ztCEdgeAlertSeverity`	Der Schweregrad des Alarms (numerische Werte siehe `ztCEdgeAlertSeverityNum`). Werte sind: `gelöst`  `zur Information`  `geringfügig`  `schwer`  `ernst`  `kritisch` 
`ztCEdgeAlertType`	Die Art des Alarms. Beispiele sind: • `node_singleSystemDisk` • `Knoten in Wartung` • `Die Last ist auf der Einheit nicht gut verteilt`
`ztCEdgeAlertSource`	Die Quelle des Alarms. Beispiele sind: • `Knoten0` oder `Knoten1` • ztC Edge System-Netzwerkname • Netzwerk-Hostname
`ztCEdgeAlertDateTime`	Datum und Uhrzeit des Alarms im Format *jjjj-mm-tt hh:mm:ss*, dabei sind *jjjj* das Jahr, *mm* der Monat, *tt* der Tag, *hh* die Stunde, *mm* die Minute und *ss* die Sekunde (z. B. `2017-11-03 23:49:45`).
`ztCEdge`	Falls `true` (wahr) wurde ein Call-Home gesendet; falls

Feld	Beschreibung
AlertCallHomeSent	false (falsch), wurde kein Call-Home gesendet
ztCEdgeAlertEAlertSent	Falls true (wahr) wurde ein e-Alert gesendet; falls false (falsch), wurde kein e-Alert gesendet
ztCEdge AlertSNMPTrapSent	Falls true (wahr) wurde ein SNMP-Trap gesendet; falls false (falsch), wurde kein SNMP-Trap gesendet
ztCEdgeAlertInformation	Informationen zum Alarm. Beispiele sind: • Knoten Knoten1 befindet sich in Wartung • Knoten0 hat einen einzelnen Datenträger: Die Richtlinie geht davon aus, dass dieser Datenträger redundant ist - falls nicht, fügen Sie einen weiteren internen Datenträger hinzu • UNTERNEHMENS-Netzwerk net_728 meldet einen verschlechterten Verbindungszustand • Die Last ist auf der Einheit nicht verteilt
ztCEdgeAlertSNMPTrapOID	SNMP Trap-Objektkennung (OID) (zum Beispiel COMPANY-MIB::nodeSingleSystemDisk)
ztCEdgeAlertSeverityNum	ztCEdgeAlertSeverity-Nummer. Werte sind: 0 Gelöst 1 Zur Information

Feld	Beschreibung
	2 Geringfügig  3 Schwer  4 Schwerwiegend  5 Kritisch 

So zeigen Sie Informationen zu Auditprotokollen an

Geben Sie den folgenden Befehl ein, um Informationen zu Auditprotokollen anzuzeigen:

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c
public localhost ztCEdgeAuditTable
```

Die Befehlsausgabe zeigt Folgendes an:

Feld	Beschreibung
`ztCEdgeAuditIndex`	Eine schrittweise erhöhte Zahl (`1`, `2` usw.), um anzugeben, aus welchem Auditprotokoll Informationen angezeigt werden.
`ztCEdgeAuditDateTime`	Datum und Uhrzeit der Auditgenerierung im Format *jjjj-mm-tt hh:mm:ss*, dabei sind *jjjj* das Jahr, *mm* der Monat, *tt* der Tag, *hh* die Stunde, *mm* die Minute und *ss* die Sekunde (z. B. `2017-11-03 23:49:45`).
`ztCEdgeAuditUsername`	Der Name des Benutzers, der die Generierung des Audits veranlasst hat (zum Beispiel `audit` oder `admin`).
`ztCEdge AuditOriginatingHost`	Die IP-Adresse des Hosts, von dem das Audit ausgeht.
`ztCEdgeAuditAction`	Eine Beschreibung der Aktion, für die ein Audit

Feld	Beschreibung
	ausgeführt wird. Beispiele sind: • "Benutzer anmelden: \"audit" • "Virtuelle Maschine starten: \"manager1" • "Alle gelöschten Alarme entfernen"

So zeigen Sie Informationen zu Knoten an

Geben Sie den folgenden Befehl ein, um Informationen zu Knoten anzuzeigen:

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c
public localhost ztCEdgeNodeTable
```

Die Befehlsausgabe zeigt Folgendes an:

Feld	Beschreibung
ztCEdgeNodeIndex	Eine schrittweise erhöhte Zahl (1, 2 usw.), um anzugeben, zu welchem Knoten Informationen angezeigt werden.
ztCEdgeNodeId	Die Host-ID des Knotens (zum Beispiel host:o34).
ztCEdge NodeDisplayName	Der Name des Knotens, Knoten0 oder Knoten1.
ztCEdgeNodeIsPrimary	Falls true (wahr), ist der Knoten primär. Falls false (falsch), ist der Knoten sekundär.
ztCEdgeNodeStateNum	Knotenzustand ist: 0 Normal (✓) 1 Warnung (⚠) 2 Beschäftigt (↻) 3 Beschädigt (✖)

Feld	Beschreibung
	4 Wartung ()
ztCEdge NodeActivityNum	Knotenaktivität ist: 0 Abbild wird erstellt 1 Wird gestartet 2 Wird ausgeführt 3 Anhalten 4 Neu starten 5 Ausgeschaltet 6 Fehler 7 Firmwareaktualisierung 8 Verloren 9 Getrennt 10 Nicht erreichbar 11 Proto (Initialisierung) 12 Evakuierung

So zeigen Sie Informationen zu VMs an

Geben Sie den folgenden Befehl ein, um Informationen zu einer VM anzuzeigen:

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c
public localhost ztCEdgeVMTable
```

Die Befehlsausgabe zeigt Folgendes an:

Feld	Beschreibung
ztCEdgeVMIndex	Eine schrittweise erhöhte Zahl (1, 2 usw.), um anzugeben, zu welcher VM Informationen angezeigt werden.
ztCEdgeVMId	Die VM-ID (zum Beispiel vm:o1467).

Feld	Beschreibung
`ztCEdgeVMDisplayName`	Der Name der VM (zum Beispiel `MeineVM`).
`ztCEdgeVMRunningNode`	Der Name des Knotens, auf dem die VM läuft, `Knoten0` oder `Knoten1`.
`ztCEdgeVMAvailability`	Die Verfügbarkeit der VM, `HA` (Hochverfügbar) oder `FT` (Fehlertolerant).
`ztCEdgeVMStateNum`	VM-Zustand ist: `0` Normal () `1` Warnung () `2` Beschäftigt oder Synchronisierung () `3` Beschädigt oder auf Blacklist ()
`ztCEdgeVMActivityNum`	VM-Aktivität ist: `0` Installation `1` Wird gestartet `2` Wird ausgeführt `3` Verschieben `4` Anhalten `5` Gestoppt `6` Exportvorgang `8` Angehalten `9` Laden `10` Absturz `11` Abgestürzt `12` Speicherauszug `13` Wartet

So zeigen Sie Informationen zu Volumes an

Geben Sie den folgenden Befehl ein, um Informationen zu einem Volume anzuzeigen:

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c
public localhost ztCEdgeVolumeTable
```

Die Befehlsausgabe zeigt Folgendes an:

Feld	Beschreibung
`ztCEdgeVolumeIndex`	Eine schrittweise erhöhte Zahl (`1`, `2` usw.), um anzugeben, zu welchem Volume Informationen angezeigt werden.
`ztCEdgeVolumeId`	Die Volume-ID (zum Beispiel `volume:o588`).
`ztCEdgeVolumeDisplayName`	Der Name des Volumes (zum Beispiel `root`).
`ztCEdge VolumeSyncPercentage`	Der prozentuale Anteil des Volumes, der synchronisiert ist.
`ztCEdgeVolumeUsedBy`	Der Name der VM oder des Hosts, von der/dem das Volume verwendet wird (zum Beispiel `MeineVM`); `keine` zeigt an, dass das Volume nicht verwendet wird.
`ztCEdgeVolumeStateNum`	Volume-Zustand ist: `0` Normal (✓) `1` Warnung (⚠) `2` Beschäftigt oder Synchronisierung (🔄) `3` Beschädigt (✖)