



ztC Edge 用户指南



For an **Always-On** World

www.stratus.com

通知

该文件内包含的信息可能会发生修改而不另行通知。

除 **STRATUS TECHNOLOGIES** 授权代表签署的书面协议中有明确规定外，**STRATUS** 没有就本文件内包含的信息提供包括适销性和用途适用性在内的任何保证或陈述。

对于本文件内包含的或与本文件的提供、性能或使用有关的任何错误，**Stratus Technologies** 不承担任何类型的任何责任或义务。**Stratus** 文件中描述的软件 (a) 是 **Stratus Technologies Ireland, Ltd.** 或第三方的财产，(b) 是依照授权提供的，(c) 只能依照授权条款中的明确许可复制或使用的。

Stratus 文件描述了支持的所有用户接口功能和 **Stratus** 开发的应用程序接口 (API)。这些接口的任何无文件支持功能仅供 **Stratus** 人员使用，可能会发生变更而不予告知。

本文件受版权保护。保留所有权利。**Stratus Technologies** 授予您有限许可来下载和打印合理份数的本文件(或其中的任何部分)，但是不得进行修改，仅供您内部使用，而且文件复印件中必须保留所有版权声明和其他限制性说明及/或声明。

版权

Stratus、Stratus 徽标和 Stratus Cloud 是注册商标，Stratus Technologies 徽标、Stratus 24 x 7 徽标和 ztC 是 Stratus Technologies Ireland, Ltd. 的商标。

UNIX 是 The Open Group 在美国和其他国家的注册商标。

Intel 和 Intel Inside 标志是 Intel Corporation 或其子公司在美国和/或其他国家/地区的注册商标，Xeon 是这些公司在这些国家或地区的商标。

Microsoft、Windows、Windows Server 和 Hyper-V 是 Microsoft Corporation 在美国和/或其他国家/地区的注册商标或商标。

VMware、vSphere 和 ESXi 是 VMware, Inc. 在美国和/或其他司法管辖区的注册商标或商标。

注册商标 Linux 是按照该商标的全球所有者 Linus Torvalds 的独家被授权人 Linux Mark Institute 的子授权使用的。

Google 和 Google 标志是 Google Inc. 的注册商标，是已获得使用许可的。Chrome browser 是 Google Inc. 的商标，是已获得使用许可的。

Mozilla 和 Firefox 是 Mozilla Foundation 的注册商标。

Red Hat 是 Red Hat, Inc. 在美国和其他国家的注册商标。

所有其他商标和注册商标都是其各自持有者的财产。

手册名称：*ztC Edge*用户指南

产品版本号：Stratus Redundant Linux版本 2.2.0.0

发布日期：2020年11月25日

Stratus Technologies, Inc.

5 Mill and Main Place, Suite 500

Maynard, Massachusetts 01754-2660

© 2020 Stratus Technologies Ireland, Ltd.。保留所有权利。

目录

部分 1: ztC Edge用户指南	1
第 1章: ztC Edge系统简介	1
ztC Edge系统概述	1
ztC Edge系统描述	2
物理机和虚拟机	2
管理操作	3
警报	3
远程支持	4
无人值守管理	4
第三方管理工具	4
操作模式	5
高可用性操作	5
容错操作	6
ALSR配置	6
ALSR和仲裁服务	7
仲裁服务器	7
网络架构	8
A-Link 和专用网络	8
业务和管理网络	9
网络分段故障检测与修正	9
系统使用限制	10
QEMU	10
访问主机操作系统	10
第 2章: 入门	13
计划	14
安全防范措施	14
系统要求概述	15
系统硬件	15
IP 地址	16
端口	17
空间建议	17
系统规范: ztC Edge 110i系统	18
系统规范: ztC Edge 100i系统	19

DIN 轨和墙壁安装支架装置 : ztC Edge 110i 系统	21
DIN 轨和墙壁安装支架装置 : ztC Edge 100i 系统	23
产品合规性	24
一般网络要求和配置	25
业务和管理网络要求	25
A-Link 和专用网络要求	27
ztC Console 要求	27
兼容 Internet 浏览器	27
电源要求与注意事项	28
部署	28
连接电源	28
UPS(可选)	29
部署系统	30
连接以太网电缆	32
映射您的键盘	33
要在部署之后配置键盘布局:	34
记录管理 IP 地址	34
部署后任务	35
获取系统 IP 信息	36
首次登录 ztC Console	36
注册系统并获取永久授权	38
重新部署 ztC Edge 系统	42
将节点添加到单节点系统	43
连接第二个业务网络	44
第 3 章: 使用 ztC Console	47
ztC Console	47
登录 ztC Console	48
编辑您的用户信息	50
“仪表板”页	51
解决仪表板上的未决警报	52
“系统”页	52
启动系统	53
重启系统	53
关闭系统	54
“首选项”页	55

指定所有者信息	58
管理产品许可证	58
管理软件更新	61
配置 IP 设置	62
配置仲裁服务器	64
配置日期和时间	65
配置邮件服务器	66
配置“用户与组”	68
管理本地用户帐户	69
管理域用户帐户	71
配置活动目录	72
配置安全连接	73
配置 VM 设备	77
管理 IPtables	78
配置登录横幅	82
启用 ztC Advisor	83
保存和还原系统首选项	84
配置电子警报	92
配置 SNMP 设置	93
配置 OPC 设置	98
显示 OPC 输出	100
配置远程支持设置	107
配置 Internet 代理设置	108
“警报历史记录”页	109
“审核日志”页	110
“支持日志”页	110
创建诊断文件	111
上传诊断文件至客户支持	111
删除诊断文件	112
“物理机”页	113
物理机操作	114
物理机状态和活动	115
“虚拟机”页	116
虚拟机操作	117
虚拟机状态和活动	119

“卷”页	121
“网络”页	122
设置 MTU	123
“虚拟 CD”页	124
“升级套件”页	124
创建具有系统软件的 USB 介质	125
第 4 章：升级 Stratus Redundant Linux 软件	127
使用升级套件升级 Stratus Redundant Linux 软件	127
第 5 章：管理物理机	131
维护模式	131
启动物理机	133
重启物理机	133
关闭物理机	134
负载均衡	135
操作模式	136
物理机故障排除	136
恢复故障物理机(手动)	137
第 6 章：管理虚拟机	141
计划虚拟机资源	142
计划虚拟机 vCPU	142
计划虚拟机内存	144
计划虚拟机存储	144
计划虚拟机网络	145
创建和迁移虚拟机	146
创建新虚拟机	146
复制虚拟机	150
将物理机或虚拟机迁移到系统	152
导入 OVF 或 OVA 文件	161
从 OVF 文件替换/还原虚拟机	168
导出虚拟机	172
在 ztC Edge 系统上安装 USB 设备或网络安装的文件夹	176
管理 Windows 驱动器标签	178
配置基于 Windows 的虚拟机	178
更新 VirtIO 驱动程序(基于 Windows 的 VM)	179
创建和初始化磁盘(基于 Windows 的 VM)	182

安装应用程序(基于 Windows 的 VM)	182
配置基于 Linux 的虚拟机	183
创建和初始化磁盘(基于 Linux 的 VM)	183
安装应用程序(基于 Linux 的 VM)	184
管理虚拟机的运行	184
启动虚拟机	185
关闭虚拟机	185
关闭虚拟机电源	187
打开虚拟机控制台会话	187
重命名虚拟机	190
移除虚拟机	191
管理虚拟机资源	192
重新配置虚拟机资源	192
在虚拟机中创建卷	195
将卷附加到虚拟机	196
将卷与虚拟机分离	197
将卷从虚拟机中移除	198
重命名 ztC Edge系统上的卷	199
扩展 ztC Edge系统上的卷	200
恢复虚拟机资源	201
管理虚拟 CD	201
创建虚拟 CD	202
插入虚拟 CD	203
弹出虚拟 CD	204
从虚拟 CD 启动	204
重命名虚拟 CD	205
下载虚拟 CD	206
移除虚拟 CD	206
高级主题(虚拟机)	207
将特定 MAC 地址分配给虚拟机	207
为虚拟机选择首选 PM	208
强制 VM 启动	208
更改虚拟机的保护级别(HA 或 FT)	211
配置虚拟机的启动顺序	212
为故障虚拟机重置 MTBF	213

将USB设备附加到虚拟机	214
第7章：维护物理机	217
替换物理机(自动)	217
更换物理机(手动)	219
第8章：监控系统、基于Windows的VM和应用程序	225
监控ztC Edge系统	225
监控基于Windows的虚拟机	227
监控基于Windows的虚拟机上的应用程序	229
部分2：支持文档	233
第9章：Stratus Redundant Linux版本2.2.0.0版本说明	234
新功能及增强	234
Stratus Redundant Linux	234
Stratus Redundant Linux版本2.1.0.0中的新功能	235
漏洞修复	235
在Stratus Redundant Linux版本2.2.0.0中修复的故障	235
在Stratus Redundant Linux版本2.1.0.0中修复的故障	236
CVE修复	236
重要注意事项	236
升级到版本2.2.0.0	236
确定系统软件的版本	236
在升级过程中，刷新浏览器并接受新证书	236
使用Intel主动管理技术(AMT)获得Lights-Out支持	237
在不同物理站点上部署ztC Edge节点	237
启用ztC Advisor	237
经过测试的客人操作系统	237
在套件升级过程中，单节点系统不能处于维护模式	237
已知问题	237
创建Windows 2008(SP2, 32位)VM后，VirtIO串行驱动程序的安装失败	237
可移动媒体以及使用P2V客户端迁移PM或VM	238
导入VM时的最大路径长度	238
导入OVA文件有时会失败	238
导入Linux VMware OVA文件后，手动配置网络信息	238
“从USB导入”搜索列出各个目录中的OVA文件	239
无法导入RHEL 8.1 VM	239
UEFI VM控制台会话的最大分辨率	239

重启 VM, 以获得 vmgenid 支持	239
使用 Microsoft Edge 控制台浏览器创建 VCD 失败	240
要导入 VMware VM, 则使用操作系统关闭命令	240
在单节点系统中, 添加的 vCPU 的 VM 创建向导显示不正确	240
升级到双节点系统后, VM 显示警告图标	240
在 IE10、IE11 或 Firefox 中针对控制台的日语键盘 106 和 109 的映射可能不正确	240
迁移已设置了监视的 VM 会导致“无响应”	240
当 A-Link 离线时, VM 报告为已损坏, 而不是降级	240
弹出的 VCD 仍显示在基于 Linux 的 VM 控制台中	241
在使用 https 时, 有些浏览器无法连接 VNC	241
更改节点 IP 地址或网络掩码网络设置时需要重新启动	241
文档更新	241
访问 Stratus 知识库文章	241
获取帮助	242
第 10 章: 系统参考信息	244
经过测试的客人操作系统	244
重要物理机和虚拟机注意事项	245
虚拟机建议和限制	246
建议的 CPU 内核数量	246
重要注意事项	246
创建 ALSR 配置	247
创建配置	251
典型 ztC Edge 系统	251
具有仲裁服务器的 ALSR 配置	251
ALSRVLAN 要求	252
从初始部署到完成 ALSR 配置	253
符合网络要求	254
定位和创建仲裁服务器	255
定位仲裁计算机	255
添加备选仲裁计算机	256
仲裁计算机要求	256
下载并安装仲裁服务软件	257
完成配置	257
配置仲裁服务端口	258
验证仲裁服务端口	258

请参阅在 ztC Console中配置仲裁服务器	258
验证此配置并(重新)连接 VM	260
了解仲裁对系统行为的影响	260
示例 1:无仲裁服务器的系统遇到脑裂情况	260
灾难性故障	261
故障处理	261
恢复和修复	262
示例 2:具有仲裁服务器的ALSR系统可避免脑裂情况	262
灾难性故障	263
故障处理	263
恢复和修复	264
示例 2, 已修改:在灾难性故障期间仲裁服务器不可及	264
示例 2, 已修改:在无灾难性故障时仲裁服务器不可及	265
从电源故障中恢复	265
访问知识库文章	265
已修复的 CVE	266
Stratus Redundant Linux版本 2.2.0.0 中已修复的 CVE	266
Stratus Redundant Linux版本 2.1.0.0 中已修复的 CVE	270
Stratus Redundant Linux版本 2.0.1.0 中已修复的 CVE	275
Stratus Redundant Linux版本 2.0.0.0 中已修复的 CVE	278
REST API 调用	279
login	280
overview	280
vms	281
第 11章: 安全性	282
安全性加强	282
安全性指导原则	283
端口和协议	284
网络分段	284
IP 表/防火墙	284
用户帐户创建	284
密码创建	285
最低权限	285
活动目录	285
时间同步	286

安全连接	286
更新 SSL 证书	287
SNMP 配置	287
备份	287
自动本地站点恢复	287
审核	288
升级	288
物理安全性	289
高级安全性指导原则	289
密码质量建议	289
并发用户管理	290
防病毒	290
SSH 访问限制	290
标准组织的最佳实践与标准	292
第 12 章：SNMP	296
使用 snmptable 获取系统信息	296

部分 1: ztC Edge用户指南

*ztC Edge*用户指南描述 ztC Edge 系统、系统部署方法和系统使用方法。

关于系统描述,包括其运行模式、存储和网络架构,请参阅:

- [ztC Edge系统简介](#)

关于规划和部署信息,请参阅:

- [入门](#)

下面的主题描述 ztC Edge系统管理方法:

- [使用 ztC Console](#)
- [升级 Stratus Redundant Linux软件](#)
- [管理物理机](#)
- [管理虚拟机](#)
- [维护物理机](#)
- [监控系统、基于 Windows 的 VM 和应用程序\(在已授权用于此类监控的系统上\)](#)

1

第 1 章：ztC Edge 系统简介

有关 ztC Edge 系统简介，请参阅以下主题：

- [ztC Edge 系统概述](#)
- [操作模式](#)
- [网络架构](#)
- [系统使用限制](#)

ztC Edge 系统概述

ztC Edge 系统提供自动恢复，能够在发生硬件故障时丢失数据。关于系统组件和功能的描述，请参阅如下各主题。

- [ztC Edge 系统描述](#)
- [物理机和虚拟机](#)
- [管理操作](#)
- [警报](#)
- [远程支持](#)
- [无人值守管理](#)
- [第三方管理工具](#)

ztC Edge系统描述

Stratus Redundant Linux软件允许两台单独ztC Edge 计算机(具有相应授权)作为一个高度可用的或能容错的单一系统工作。每一台计算机均称为物理机 (PM) 或节点。

两台 PM:

- 运行相同的主机操作系统 (CentOS)
- 包含复制的虚拟机和存储(通过两台 PM 之间的直接以太网连接同步)
- 支持运行客人操作系统的虚拟机

关于ztC Edge系统中 PM 配置的更多信息, 请参阅[系统要求概述](#)。

当系统已授权用于一个节点时, Stratus Redundant Linux软件也可以在单个 PM 上运行。在此配置中, 系统是单工的, 其没有容错或高可用性, 并且在正常运行过程中, 系统显示网络故障。

相关主题

[系统要求概述](#)

[经过测试的客人操作系统](#)

[网络架构](#)

物理机和虚拟机

具有两个物理机 (PM)(也称为节点)的ztC Edge 系统通过创建在两个节点上运行的冗余虚拟机 (VM) 来透明地保护应用程序。

当具有一个 PM 的系统已授权用于一个节点时, ztC Edge软件也在该系统上运行。有关已授权用于一个节点的系统的信息, 请参阅 [ztC Edge系统描述](#)。本主题其余部分中的信息适用于已授权用于两个节点的系统。

Stratus Redundant Linux管理软件可从头创建客人 VM。其还可从其他环境导入现有 VM, 以及将它们转换成客人 VM。通过创建第二个主机上所选 VM 的相同实例, 管理软件自动提供 VM 的 FT 级保护。系统管理员从称为 ztC Console的基于浏览器的单独管理控制台管理此单个实体。

应用程序和用户都不暴露于两个主机 PM 上的冗余计算资源。应用程序仅看到一个主机名、呈现给 VM 的每个网络接口的一个 MAC 地址, 以及呈现给 VM 的每个 VM 网络接口的一个 IP 地址。系统管理员加载和配置客人 VM 上的应用程序 – 就像是系统管理员正在将它们加载到物理服务器上似的。如果在磁盘或网络设备中出现故障或失败, 该软件会自动将 I/O 重定向到配对的主机 PM, 以实现持续运行。尽管在修复此故障前失去冗余, 但 VM 会继续正常运行。应用程序会持续执行, 就像什么也没发生一样。冗余、故障检测、隔离和管理对 Windows 或 Linux 环境以及在其中

运行的应用程序完全透明。PM 的修复同样是透明和自动的。当修复了 PM 上的故障组件时，软件会自动将修复的组件结合到客人 VM 的受保护环境并透明地恢复冗余。

相关主题

[使用 ztC Console](#)

[“物理机”页](#)

[“虚拟机”页](#)

管理操作

您可以在 ztC Edge 系统上从 ztC Console 执行许多管理操作，这是一个基于浏览器的界面，通过该界面可将系统作为整体进行访问，以及访问物理机 (PM)、虚拟机 (VM) 和其他资源。有关信息，请参阅 [ztC Console](#)。

警报

ztC Edge 系统警报信息通知系统管理员需要关注的问题。警报内容可以是：

- 应执行的配置工作
- 系统运行状态通知
- 需要关注的系统问题

单击左侧导航面板上的 **仪表盘** 来查看警报消息及其说明。单击左侧导航面板上的 **警报** 来查看警报记录。

下面的图标指示警报消息的状态。

-  信息
-  正常或良好状态
-  轻度、警告或不一致状态
-  中度状态
-  损坏、故障或严重状态

远程支持

要访问 ztC Edge 系统的远程支持功能时，点击左侧导航面板上的**首选项**。在这里，您可以选择如下各项来配置支持和代理规格：

- **支持配置**—配置设置来允许您的授权 **Stratus** 服务代表对您的系统进行远程支持访问，并使您的系统能够向您的授权 **Stratus** 服务代表发送健康和状态通知。有关详细信息，请参阅[配置远程支持设置](#)。
- **代理配置**—使您能够为互联网访问配置代理服务器。关于详细信息，请参阅[配置 Internet 代理设置](#)。

无人值守管理

ztC Edge 系统结合了 Intel[®] 主动管理技术 (AMT) Lights-Out 支持，在默认情况下禁用此支持。当在系统启动过程中显示 BIOS 初始屏幕时按 **Ctrl-P** 可启用和配置此支持。有关 AMT 配置和限制的其他信息，请访问知识库，搜索文章 *ztC Edge* 中的 *AMT 和远程访问 (KB-8219)*。请参阅[访问知识库文章](#)。

可在系统的 **P1** 网络端口上访问 AMT 功能。

第三方管理工具

您可以将第三方管理工具安装到 ztC Edge 系统上。这些工具的示例包括厂商特有的管理/监控实用程序、企业管理/监控实用程序，以及其他管理/监控软件。请注意如下问题：

- 一般来说，在主机操作系统 (CentOS) 上运行的管理工具应在 ztC Edge 系统上运行。可能的例外是管理/监控基于 CentOS KVM 的虚拟化的工具。要管理/监控 ztC Edge 虚拟化时，请使用集成的 ztC Edge 管理工具。
- **Stratus** 建议，在部署您的 ztC Edge 系统之前，确认在安装并且运行管理工具的条件下系统能够正确运行。
- **Stratus** 建议您为第三方管理工具设置一个非根账户。
- 您可以通过管理网络使用在安装过程中指定的(或者如果在安装过程中为 DHCP 配置了接口，则由 DHCP 服务器指定)IP 地址访问 ztC Edge 系统。
- 如果您在物理机 (PM) 的主机操作系统中安装第三方管理工具，并且未来需要更换 PM，则记得在更换的 PM 上安装这些工具。



注意：第三方管理工具可能会使主机操作系统和系统软件的环境变得不稳定。您可能需要删除消耗过多 RAM 或磁盘空间或者怀疑会使本产品变得不稳定的管理工具。请遵循您授权 Stratus 服务代表的建议。

关于主机操作系统访问的信息，请参阅[访问主机操作系统](#)。

相关主题

[入门](#)

[系统参考信息](#)

操作模式

ztC Edge系统提供了两个操作模式来为 VM 设置用户定义的可用性级别：

- [高可用性操作](#)
- [容错操作](#)

HA 操作和 FT 操作均通过使用一对物理机 (PM) 来实现它们各自的冗余级别。FT 操作消耗更多的系统资源，这可能会减慢应用程序的处理速度。

Stratus 建议对 HA 操作和 FT 操作配置仲裁服务。此仲裁服务可防止出现脑裂情况 (HA 操作和 FT 操作对的两台 PM 彼此独立运行)；有关信息，请参阅[仲裁服务器](#)。

高可用性操作

ztC Edge 软件为 VM 提供了两个用户定义的可用性级别：高可用性 (HA) 和容错 (FT)。

在 HA 操作中，Stratus Redundant Linux 会自动检测、隔离和处理大多数硬件故障，从而使您的应用程序保持运行。凭借 HA 远程支持技术，软件会向 Stratus 支持中心通知各种问题，并且指示故障类型及其位置。自动故障检测、隔离和远程支持技术的这种组合可确保快速获得专家级支持技术人员并快速解决问题。

当您使用 ztC Console 创建或导入 VM 时，选择一个 VM 可用性级别。

在启用时，HA 操作可提供基本故障转移和恢复，一些故障需要 (自动) VM 重启才能恢复并返回 HA 操作：

- 可消除因许多 (但非所有) CPU、内存、I/O 或其他物理机 (PM) 故障导致的停机。
- 在无需 IT 人员干预的情况下处理故障。

- 提供对所有组件的持续、主动验证。
- 确保始终实现全面冗余和恢复。

HA 适用于允许几分钟的偶尔中断的场合。

相关主题

[“虚拟机”页](#)

[使用 ztC Console](#)

容错操作

ztC Edge系统为 VM 提供了两个用户定义的可用性级别:高可用性 (HA) 和容错 (FT)。在 FT 操作中,应用程序在故障期间不间断地持续运行。FT 用于需要最高可用性水平的场合。

当您使用 ztC Console 创建或导入 VM 时,选择一个 VM 可用性级别。

在 FT 操作中,通过为运行于两个物理机间的 VM 创建冗余环境,ztC Edge 软件透明地保护应用程序。凭借第二个主机上所选 VM 的相同实例,ztC Edge 软件提供了 VM 的 FT 级保护。

在启用时,FT 操作可在所有故障中保护 VM,无需停机,并且 FT 操作:

- 可消除因任何 CPU、内存、I/O 或其他物理机 (PM) 故障导致的停机。
- 在无需 IT 人员干预的情况下处理故障。
- 确保无数据丢失。
- 提供对所有组件的持续、主动验证。
- 确保始终实现全面冗余和恢复。

相关主题

[“虚拟机”页](#)

[使用 ztC Console](#)

ALSR 配置

*自动本地站点恢复 (ALSR) 配置*连接不同站点中的两台物理机。它是一种容灾部署,既保持硬件冗余又保持物理计算机室及其所在建筑物的冗余。由于地理上的分离,ALSR 配置需要仔细的组件布局规划和较复杂的网络拓扑。由于 ALSR 配置使 A-Link 网络可能出现其他潜在故障条件,因此对于 ALSR 配置,Stratus 强烈建议您使用仲裁服务。(ALSR 配置不适用于已授权用于一个节点的系统。)

[符合网络要求](#) 列出了 ALSR 配置的网络要求。

ALSR和仲裁服务

在ALSR配置中，按照建议的仲裁部署最佳做法(参阅[仲裁服务器](#)和[定位和创建仲裁服务器](#))。在任何ALSR配置中，首选仲裁服务计算机位置是第三方设施内，替代位置是第四方位置(或者谨慎地放在第三方位置)。网络是互联的。

仲裁服务计算机应尽可能是隔离的。当两台计算机必须放在相同(第三方)位置时，必须确保它们不使用共同的电源。

ztC Edge PM与仲裁服务计算机之间的物理连接不得穿过另一台PM的位置。

把一台仲裁服务计算机与一台ztC Edge PM放在同一位置来确保数据完整性。不过，这样的话，对于某些位置故障，在手动恢复之前可能需要关闭VM。

管理网络为ztC Edge PM与仲裁服务计算机之间提供物理连接。为确保工作正常，您必须把每一台ztC Edge PM配置为使用不同网关连接仲裁服务计算机。当两台PM使用相同网关连接仲裁服务计算机时，可以保证发生故障时的数据完整性。不过，这样的话，对于某些位置故障，在手动恢复之前可能需要关闭VM。

相关主题

[创建ALSR配置](#)

[网络架构](#)

仲裁服务器

*仲裁服务*是一种基于Windows操作系统的服务，其部署于与两个服务器(物理机或PM)完全不同的服务器上。仲裁服务器对于ztC Edge环境中的特定故障提供数据完整性保证和自动重启功能。

Stratus强烈建议使用仲裁服务器，尤其是ALSR操作。您可以配置具有0、1或2个仲裁服务器的ztC Edge PM对。

仲裁服务器保证VM的完整性，能够预防包括脑裂在内的多种网络故障条件，并在特定故障下提供无人照管的VM启动。仲裁服务器通讯通过管理网络进行。

仲裁服务器在ALSR配置中尤为重要。ALSR的最佳做法是将首选仲裁计算机放在第三个设施内，并将替代仲裁服务器放在第四个设施内。但您还可以将替代仲裁服务计算机与首选仲裁计算机放在一起，并且仍能获得令人满意的服务。有关更多信息，请参阅[ALSR配置](#)。

如果只有两个站点可用(因而无法采用上述最佳做法配置)，并且如果一个PM已经停机，而幸存的PM无法与仲裁服务器进行通讯(例如，因为它与停机的PM位于同一站点)，则幸存站点处的VM会自动关闭，以避免在脑裂情况下运行。

相关主题

[创建ALSR配置](#)，其讨论仲裁服务器

[配置仲裁服务器](#)

网络架构

以太网为系统通信提供途径。以太网的主要类型：

- **可用性链路网络或 A-Link 网络**(在蓝色(A2 或 •)和黄色(A1 或 ••)网络端口上)在已授权用于两个节点的ztC Edge 系统上是分配给虚拟机 (VM) 的,用于在两个 PM 之间同步数据或迁移 VM。一个 A-Link 网络(在蓝色(A2 或 •)网络端口上)还是必须是连接两台 ztC Edge PM 的**专用网络 (priv0)**。有关更多信息,请参阅[A-Link 和专用网络](#)。(已授权用于一个节点的系统不提供 A-Link 网络功能。)
- **业务网络**(在 P1 网络端口上,以及在 P2 上,如果启用) 在所有 ztC Edge 系统上均可使您的应用程序连接到您的现有网络。一个业务网络(在 P1 网络端口上)还。有关更多信息,请参阅[业务和管理网络](#)。

ztC Edge系统还提供网络分段检测机制。有关信息,请参阅[网络分段故障检测与修正](#)。

A-Link 和专用网络

已授权用于两台物理机(PM, 也称为节点)的每ztC Edge 个系统都需要一个用于在这两个 PM 之间传输专用管理流量的网络。此专用网络称为 *priv0*, 这是一个物理直连以太网, 或者两个节点之间的 VLAN 式连接。*Priv0* 用于对等节点发现, 上面可以没有响应 IPv4 广播的其他实体。

除了 *priv0* 外, 已授权用于两个节点的每个系统还有一个 A-Link 网络, 用于提高 PM 之间的数据复制性能。A-Link 网络可用来同步磁盘、分流网络、迁移 VM、执行心跳检查和同步容错内存。

A-link 与 *priv0* 以相同方式连接在这些 PM 之间。这些 A-link 连接在每个 PM 的蓝色和黄色网络端口之间, 其中 *priv0* 是与蓝色网络上的 A-link 共享的。

最简单的 *priv0* 由直接连接各服务器上的内嵌以太网端口的单根以太网电缆(交叉连接或直连)组成。当 *priv0* 使用除单根以太网电缆之外的网络设备时, 请参阅 [ALSR配置](#)。

相关主题

[业务和管理网络](#)

[A-Link 和专用网络要求](#)

[网络架构](#)

业务和管理网络

除 A-Link 网络和专用网络使用的端口之外的所有以太网端口都属于业务网络端口，供客人操作系统用来连接您的网络。

业务网络是一个管理网络，负责访问 **ztC Console** 和处理各种管理任务和仲裁服务器。每个 PM 都有一个称为 *ibiz0* 的单一管理网络，其使用标记为 **P1** 的网络。

当您部署系统时，设置管理网络。您还可以为部署过程中物理连接的所有业务网络端口安装业务网络。要在部署完成后设置第二个业务网络，请参阅[连接第二个业务网络](#)。

相关主题

[A-Link 和专用网络](#)

[业务和管理网络要求](#)

[网络架构](#)

网络分段故障检测与修正

如果出现某种网络故障致使共享网络的两端无法互相通信，但每一端仍有外部网络连接，则该网络故障称为网络分段故障。

ztC Edge系统提供了一种网络分段检测机制，当系统检测到此故障时，该机制会将活动 VM 放在具有最外部网络连接的节点上。作为此功能的一部分，ztC Edge系统在活动与备用节点之间通过业务网络接口不断发送 UDP 数据包。如果两端在仍有活动网络链路时此数据包流被中断，系统的网络分段逻辑会检测到故障。在这种故障情况下，两个节点仍有活动网络连接，因此该故障在于 ztC Edge系统外部的交换机。

当检测到这种情况时，ztC Edge系统会根据确定哪一端有更好外部连接的逻辑来处理该故障。ztC Edge系统通过不断监测传入的广播/多播流量来确定哪个节点具有最多传入流量，从而作出这种故障处理决定。在这种故障情况下，如果 VM 在具有最多传入网络流量的节点上尚未处于活动状态，则 ztC Edge系统会将此 VM 网络故障转移到此节点。这种故障检测功能不需要用户配置，因为它基于任何系统上正常发生的流量作出决定。

相关主题

[网络架构](#)

系统使用限制

遵守如下主题中描述的系统使用限制：

- [QEMU](#)
- [访问主机操作系统](#)

QEMU

Stratus ztC Edge 系统支持开放源管理程序 QEMU ("Quick EMUlator")，该程序执行硬件虚拟化。用作虚拟化程序时，QEMU 直接在主机 CPU 上执行客人代码，从而获得较高性能水平。

ztC Edge用户不应修改 QEMU 虚拟化引擎或其配置。

访问主机操作系统

完成了 ztC Edge 部署后，您可以在 PM 的物理控制台本地访问、也可以通过使用安全外壳 (SSH) 客户端远程访问主机操作系统 (CentOS)。

要通过 SSH 客户端登录主机操作系统，则使用在部署过程中指定的(或者，当部署过程中把接口配置为 DHCP 时，由 DHCP 服务器提供的)管理 IP 地址。如果需要，您可以按照本主题中的描述查找每个 PM 的管理 IP 地址。



小心：不要从除 ztC Edge外的任何来源更新Stratus 系统的 CentOS 主机操作系统。仅使用与 Stratus Redundant Linux软件一同安装的 CentOS 版本。



注意：为确保管理命令正常工作，登录到主 PM 的物理控制台或 IP 地址(除非您具体需要在从 PM 中的组件上进行操作)。不要连接到系统 IP 地址，因为这个地址可以从 PM 到 PM 迁移。



注意：根帐户的默认密码是 **KeepRunning**。为保护系统，尽快更改每个 PM 上的根密码。首次以根用户身份登录 PM 时，系统会自动提示您更改密码。要在未来再次更改密码，则在每个 PM 上发出 `passwd` 命令。

关于 CentOS 上使用第三方管理工具的信息，请参阅[第三方管理工具](#)。

要查找 ztC Console中每个 PM 的 IP 地址。

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**系统**下，单击**IP 配置**。

3. 记录每个 PM 的 IP 地址，**node0** 和 **node1**。
4. 单击左侧导航面板中的**物理机**，打开**物理机**页。
5. 记录哪个 PM 是系统的主节点，其显示为 **noden(主)**。在大多数情况下，登录到主节点的 IP 地址，确保管理命令将正常工作。

要从基于 Windows 的系统访问主机操作系统

您可以下载并使用 PuTTY，这是一个开源 SSH 客户端套件：

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

尤其是，`putty.exe` 客户端可使您访问在主机操作系统的命令行上执行程序的外壳程序。PuTTY 还包括 `pscp.exe` 命令行实用程序，该实用程序可使您将文件从远程系统安全地传输到主机操作系统。

如果您喜欢具有图形用户界面的安全副本 (SCP) 客户端，也可以尝试使用开源 WinSCP 实用程序：

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

要从基于 Linux 的系统访问主机操作系统

在许多基于 Linux 和 UNIX 的系统上，默认情况下已安装并启用了 SSH 实用程序。有关如何使用这些实用程序的信息，请参阅 `ssh(1)` 和 `scp(1)`。

2

第 2 章：入门

下面的主题描述 **ztC Edge** 规划、部署和部署后任务：

- [计划](#)
- [部署](#)
- [部署后任务](#)

计划

有关计划您系统配置的信息，请参阅以下主题。

- [安全防范措施](#)
- [系统要求概述](#)
- [空间建议](#)
- [系统规范: ztC Edge 110i系统](#)
- [系统规范: ztC Edge 100i系统](#)
- [DIN 轨和墙壁安装支架装置: ztC Edge 110i系统](#)
- [DIN 轨和墙壁安装支架装置: ztC Edge 100i系统](#)
- [产品合规性](#)
- [一般网络要求和配置](#)
- [业务和管理网络要求](#)
- [A-Link 和专用网络要求](#)
- [ztC Console要求](#)
- [兼容 Internet 浏览器](#)
- [电源要求与注意事项](#)
- [创建ALSR配置\(如果适用于您的配置\)](#)

在您已计划了该系统配置后，继续进行[部署](#)。

安全防范措施

开始前，请阅读以下重要安全防范措施。



警告: 连接本产品前，确保电源电压正确。



警告: 应由合格的服务人员进行维修，没有用户可维修的组件。

警告: 如果更换的电池类型不正确, 则有爆炸危险。按照说明处理用过的电池。



IL Y A RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UNE BATTERIE DE TYPE INCORRECT. METTRE AU REBUT LES BATTERIES USAGÉES CONFORMÉMENT AUX INSTRUCTIONS



警告: 表面热, 不要触摸。

以下信息仅适用于 **ztC Edge110i** 系统:

- 这些设备为开放式设备, 应将它们安装在适用于相关环境且只能使用工具才能进入内部隔间的外壳中。
- 仅适用于 I 类, 2 区, A、B、C 和 D 组危险位置, 或仅适用于非危险位置。



警告: 爆炸危险 - 请勿在电路带电时断开设备的连接, 除非已知该区域无可点燃的浓度。

系统要求概述

ztC Edge 系统能够支持多个虚拟机 (VM) 和一台能够运行 **ztC Console** 的远程管理计算机 (即, 通用 PC)。

对于每种类型的物理机 (PM), **ztC Edge 系统硬件** 规范和要求总结如下。有关 PM 布局的建议, 请参阅 [空间建议](#)。

有关客人操作系统的信息, 请参阅 [经过测试的客人操作系统](#)。

系统硬件

特性	ztC Edge 100i PM	ztC Edge 110i PM
RAM(物理内存)	32 GB	32 GB 或 64 GB
磁盘空间	512 GB 固态驱动器 (SSD), 其中约 475 GB 可用于 VM。	2 TB SSD, 其中约 1.9 TB 可用于 VM。
网络端口	每个 PM 均有四个 1 Gb 以太网端口。	每个 PM 都有八个网络端口: 前面六

特性	ztC Edge 100i PM	ztC Edge 110i PM
	<p>在已授权用于两个节点的系统上：</p> <ul style="list-style-type: none"> • 将蓝色 (•) 用于组合的 A-link 和 priv0 专用网络 • 将黄色 (••) 用于第二个专用 A-link 网络 <p>在已授权用于两个节点或一个节点的系统上：</p> <ul style="list-style-type: none"> • 将 P1 用于组合的业务网络和管理网络 • 将 P2 用于可选业务网络 	<p>个 1-Gb 端口 (P1 至 P6)，后面两个 10-Gb 端口 (A1 和 A2)。</p> <p>在已授权用于两个节点的系统上：</p> <ul style="list-style-type: none"> • 将 A1(黄色标签)用于 A-link 1 • 将 A2(蓝色标签)用于 priv0 <p>在已授权用于两个节点或一个节点的系统上：</p> <ul style="list-style-type: none"> • 将 P1 用于组合的业务网络和管理网络。 • 将 P2 至 P6 用于可选业务网络。
<div style="border: 2px solid #00AEEF; border-radius: 10px; padding: 10px;">  <p>注意： P1 有时称为 network0 或 ibiz0; P2 有时称为 network1 或 ibiz1; P3 有时称为 network3 或 ibiz3; 以此类推。</p> </div>		

支持

该系统还支持 Intel[®] 主动管理技术 (AMT) Lights-Out 支持，您可以在每个 PM 的 P1 端口上访问该支持。

ALSR配置有其他网络要求。有关信息，请参阅[符合网络要求](#)。

关于更多信息，请参阅[网络架构](#)、[A-Link 和专用网络](#)和[业务和管理网络](#)。

IP 地址

必须为各 ztC Edge 系统分配一个静态 IPv4 IP 地址，供管理软件使用。请向 IT 网络管理员索取管理网络的 DNS 主服务器和辅助服务器 IP 地址以及网关和子网掩码信息。关于更多信息，请参阅[获取系统 IP 信息](#)。

端口

ztC Edge系统在本地防火墙中使用端口 443 进行 HTTPS 通讯，使用端口 22 进行 ssh，使用 5900-59nn 用于和每个 VM 关联的每个活动 VNC。防火墙必须允许相应端口的流量通过。防火墙必须允许客人 VM 使用 UDP 端口 4557 联系仲裁服务计算机。有关 TCP 或 UDP 端口的其他信息，请访问知识库，搜索文章 *ztC Edge 使用的 TCP 和 UDP 端口 (KB-9357)*。请参阅[访问知识库文章](#)。

相关主题

[重要物理机和虚拟机注意事项](#)

[虚拟机建议和限制](#)

[计划虚拟机资源](#)

[配置 IP 设置](#)

空间建议

为确保 ztC Edge100i 或 110i 系统的安装站点提供正确安装、冷却且大小合适的环境，请考虑针对您站点的以下空间建议。

位于台面上的节点的空间建议如下：

- 在节点左右两侧至少有 2 in. (5.08 cm) 的空间
- 在节点顶部至少有 3 in. (7.62 cm) 的空间
- 在节点前部和后部至少有 5 in. (12.7 cm) 的空间
- 在节点之间至少有 2 in. (5.08 cm) 的空间

DIN 轨安装式节点的空间建议如下：

- 在节点左右两侧至少有 2 in. (5.08 cm) 的空间
- 在节点的顶部和底部至少有 5 in. (12.7 cm) 的空间
- 在节点之间至少有 2 in. (5.08 cm) 的空间

额外空间要求如下：

- 节点可以水平(在平面上)或垂直(在墙上)安装。如果垂直安装，则带有 Stratus 徽标的面应朝上。
- 为避免损坏系统电缆，所有电缆的弯曲半径均应至少为 2 in.(5.08 cm)。
- 避免在节点下方安装任何类型的发热源。

- 避免超出节点的工作环境限制。
- 为实现最佳热传递，每个节点在散热器上方均应至少有 100 LFM (0.51 m/s) 的气流。

除上述建议外，评估您站点的具体安装需求。如果您需要进一步指导，请联系您的授权 Stratus 服务代表。

系统规范：ztC Edge 110i系统

下表提供了系统规范。

组件	描述
CPU	
CPU	Intel Core i7-8700T 处理器；35W
系统内存	2 个 260 针脚无缓冲 DDR4-2400 MHz SO-DIMM 插座，32 GB，或者共 64 GB
I/O	
显示器	1 个 HDMI 1 个 DVI 端口
以太网	6 个 10/100/1000 以太网端口 2 个 10 Gb 以太网端口
USB 端口	2 个 USB 3.2，第 2 代 (10 Gbps)(先前称为 USB 3.1，第 2 代) 2 个 USB 3.2，第 1 代 (5 Gbps)(先前称为 USB 3.1，第 1 代)
存储	1 个 SATA SSD，2 TB
指示灯	1 个绿色 LED，作为 PWR 状态指示灯 1 个绿色 LED，作为 SYS 状态指示灯 1 个绿色 LED，作为 SSD 活动状态指示灯
开关	1 个电源开关

	1个重置开关
系统	
电源	24VDC 输入 可选交流电源模块, 100 至 240VAC, 50/60 Hz, 5A
典型功率和 BTU	62 W, 213 BTU/hr
环境	
工作温度	-20°C 至 55°C(-4°F 至 131°F)
储存温度	-40°C 至 80°C(-40°F 至 176°F)
湿度	10% 至 95%(无冷凝)
冲击	IEC 60068-2-27(有 SSD:在墙壁安装、半正弦、11 ms 持续时间时为 25G)
耐振性	IEC 60068-2-64(有 SSD:3Grms STD, 随机, 5 - 500 Hz, 1 hr/轴)
物理尺寸	
重量	5.2 kg (11.46 lb), 不含包装 6.2 kg (13.67 lb), 含包装
高度	86.9 mm (3.42 in.)
宽度	280 mm (11.02 in.)
深度	210 mm (8.26 in.)

系统规范: ztC Edge 100i系统

下表提供了系统规范。

组件	描述
----	----

CPU	
CPU	Intel Core I7-6700TE 处理器; 35W
系统内存	2个 260 针脚无缓冲 DDR4-2400 MHz SO-DIMM 插座, 共 32 GB
I/O	
显示器	1 个 HDMI 1 个 DVI 端口
以太网	4 个 10/100/1000 以太网端口
USB 端口	2 个 USB 2.0 6 个 USB 3.2, 第 1 代 (5 Gbps)(先前称为 USB 3.1, 第 1 代)
存储	1 个 SATA SSD, 512 GB
指示灯	1 个绿色 LED, 作为 PWR 状态指示灯 1 个绿色 LED, 作为 SYS 状态指示灯 1 个绿色 LED, 作为 SSD 活动状态指示灯
开关	1 个电源开关 1 个重置开关
系统	
电源	9-36VDC 输入 可选交流电源模块, 100 至 240VAC, 50/60 Hz, 5A
典型功率和 BTU	41 W, 140 BTU/hr
环境	
工作温度	-40°C 至 60°C(-40°F 至 140°F)

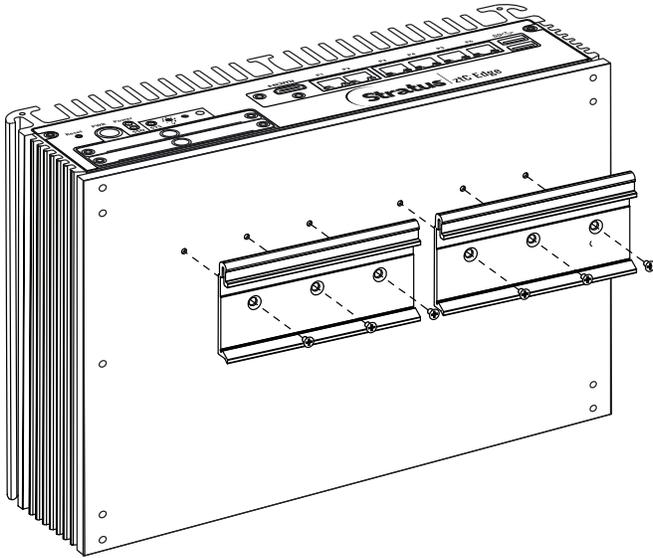
储存温度	-40°C 至 80°C (-40°F 至 176°F)
湿度	10% 至 95%(无冷凝)
冲击	IEC 60068-2-27(有 SSD: 在墙壁安装、半正弦、11 ms 持续时间时为 50G)
耐振性	IEC 60068-2-64(有 SSD: 3Grms STD, 随机, 5 - 500 Hz, 1 hr/轴)
物理尺寸	
重量	4.8 kg (10.58 lb), 不含包装 5.6 kg (12.34 lb), 含包装
高度	75 mm (2.95 in.)
宽度	280 mm (11.02 in.)
深度	190 mm (7.48 in.)

DIN 轨和墙壁安装支架装置: ztC Edge 110i系统

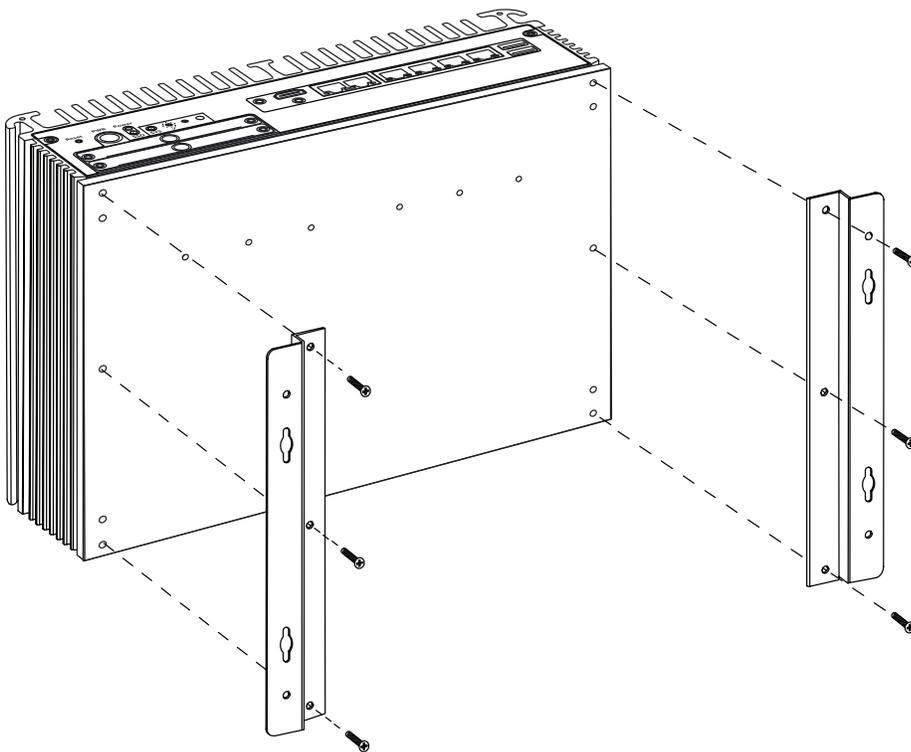


注意: 在将 DIN 轨或墙壁安装套件安装在 ztC Edge 节点上时, 确保带有 Stratus 徽标的面朝上。

要附加 DIN 轨安装套件, 则使用附件盒中的六颗平头 M3 x 6 mm 螺丝。



要附加墙壁安装套件，则卸下位于节点底部的六颗(每侧三颗)圆头 M3 x 12 mm 螺丝。重新使用这六颗螺丝来安装墙壁安装套件。





注意：如果将螺丝安装在干式墙中，则使用空心墙锚，确保不会因电缆和电源连接器上的长时间的张力而导致该装置脱离墙壁。使用最大直径为 0.166 in.(4.2 mm)、头部直径最小为 0.216 in.(5.5 mm) 的螺丝。

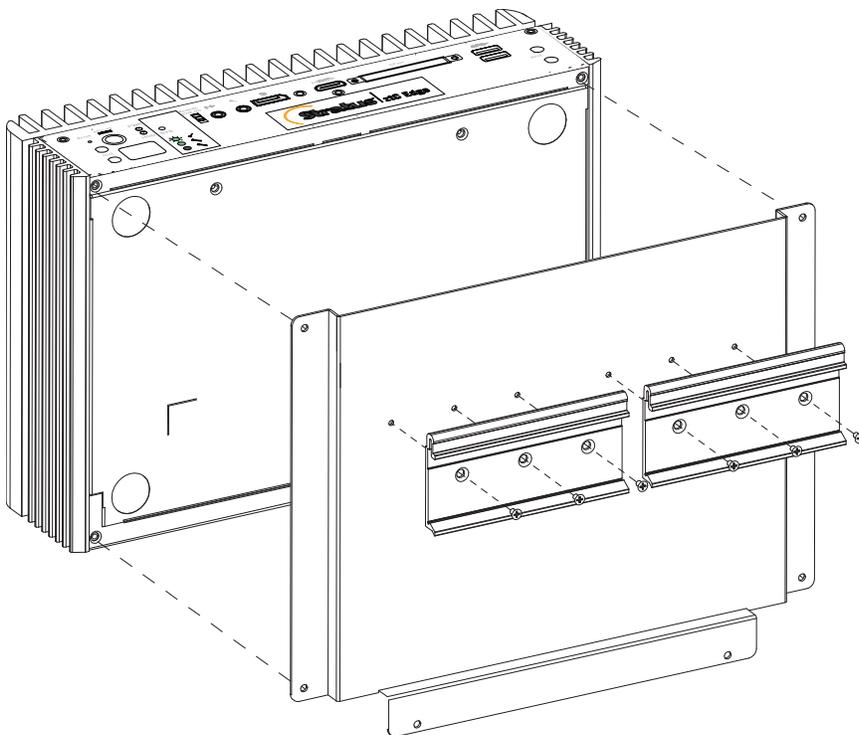
DIN 轨和墙壁安装支架装置：ztC Edge 100i系统



注意：在将 DIN 轨或墙壁安装套件安装在 ztC Edge节点上时，确保带有 Stratus 徽标的面朝上。

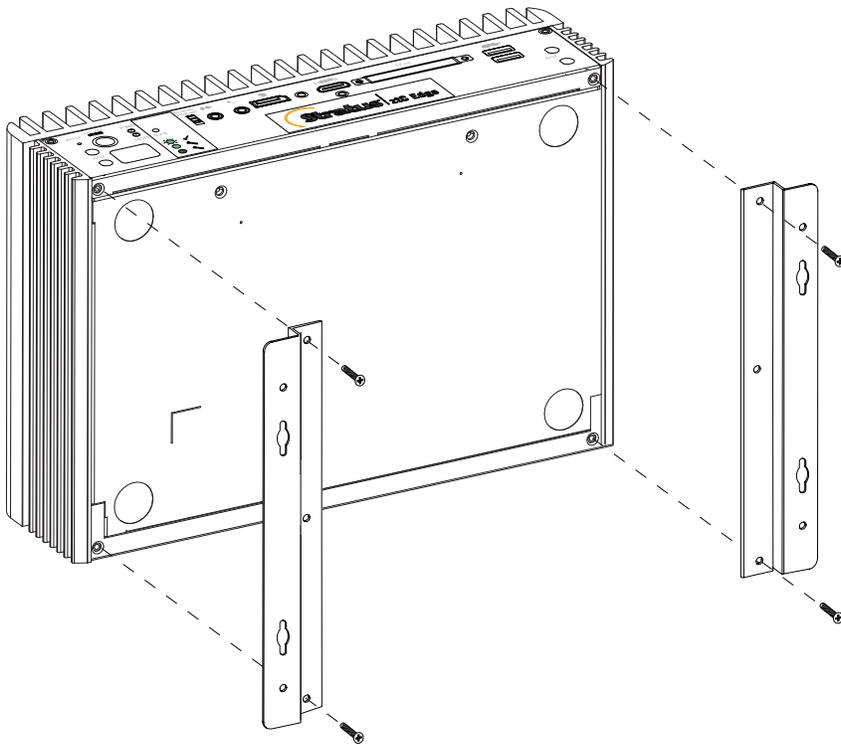
要附加 DIN 轨安装套件：

- 卸下位于节点底部的四颗(每侧两颗)平头 M3 x 6mm 螺丝。
- 使用位于附件盒中的四颗 M3 x 6mm 圆头螺丝，将 DIN 轨安装板附加到节点上。
- 使用位于附件盒中的六颗平头 M3 x 6mm 螺丝，将两个 DIN 轨安装支架附加到 DIN 轨安装板上。



要附加墙壁安装套件：

- 卸下位于节点底部的四颗(每侧两颗)平头 M3 x 6mm 螺丝。
- 使用位于附件盒中的四颗 M3 x 6mm 圆头螺丝, 将墙壁安装支架附加到节点上。



注意: 如果将该装置安装在干式墙或类似材料中, 则使用与此材料兼容的空心墙锚, 确保不会因电缆上的长时间的张力而导致该装置脱离墙壁。使用最小直径为 0.138 in.(3.5 mm)、最小长度为 1.5 in.(38.1 mm) 且头部直径最小为 0.216 in.(5.5 mm) 的螺丝。确保这些螺丝与所选空心墙锚兼容。

产品合规性

以下网站提供了 ztC Edge 100i和 ztC Edge 110i 系统的合规信息:

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

一般网络要求和配置



注意：ALSR网络具有一些额外的不同网络要求和**建议**。除以下信息外，还请参阅[创建 ALSR配置](#)。

在部署 ztC Edge系统前，确保您的网络符合如下要求：

- ztC Edge系统利用完成 IPv4 和 IPv6 协议访问，其中包括 IPv6 多路广播。这种流量受到任何阻碍时都可能会导致无法成功部署，或者降低正在运行的 ztC Edge系统的可用性。

另外，关于各网络类型的特别要求，请参阅如下主题：

- [A-Link 和专用网络要求](#)
- [业务和管理网络要求](#)

业务和管理网络要求

业务和管理网络的要求如下：

- 这些网络使用 IPv6 本地链路地址。
- 这些网络支持最高为 9000 的 MTU 值。
- 这些网络不支持绑定或 VLAN 中继。
- 虚拟机 (VM) 可以使用 IPv4、IPv6 和其他以太网协议。
- 当您的站点启用了 SLAAC 或 DHCPv6 时，所有业务网络都可以用于 IPv6 主机访问。
- 要访问 ztC Console，则使用 ibiz0，这是迁移到主管理物理机 (PM) 上的 IPv4 地址。而且，每一台 PM 在管理网络上都有其自己的 ibiz0 IPv4 地址。
- 每一台 PM 都需要至少一个业务网络(特别是管理网络)。

为了确保两台 PM 上 VM 的出入以太网流量不受阻碍：

- 连接到业务网络的交换端口不应过滤 ARP 数据包，其中包括免费 ARP 数据包。ztC Edge 系统代表客人 VM 发送免费 ARP 数据包来提示以太网交换机更新其端口转发表，以确保把 VM 流量转发到正确 PM 上的正确物理以太网端口。
- 业务网络连接的交换端口必须允许使用以太网类型：0x8807 的 layer2 多路广播(地址：01:E0:09:05:00:02)。
- 如果把 RHEL 或 CentOS 客人配置为在同一个子网络上有多个 NIC，可能会因不对称路由而出现客人网络连接问题。为了避免这个问题，应修改客人虚拟机 (VM) 上的 `/etc/sysctl.conf` 文件来放入如下行，保存该文件，然后重新启动 VM。
 - `net.ipv4.conf.default.rp_filter = 2`
 - `net.ipv4.conf.all.rp_filter = 2`
- 请勿从 PM 的主机 OS 发出 `ifdown` 命令来暂时终止 VM 的商业网络连接 (`ibizx`)。否则会断开物理接口与桥之间的连接，导致无法通过网络访问 VM。应该使用 `ifconfig down` 命令。
- 业务网络连接的交换机不得启用会禁止把 MAC 地址从一个业务链路移动到另一台 PM 上的匹配业务链路的任何 MAC 地址安全功能。
- 为了获得最佳故障转移响应，应把您的系统连接的所有交换器的 MAC 老化超时值设置为不超过一秒。

当不能满足这些要求时，或者在把一个 VM 从一台 ztC Edge PM 迁移到另一台时交换机不能正确更新其转发表时，VM 可能会出现中断，这时无法正确转发出入该 VM 的网络流量。

相关主题

[网络架构](#)

[业务和管理网络](#)

A-Link 和专用网络要求

A-Link 和专用网络的要求如下：

- 这些网络使用 IPv6 本地链路地址。
- ztC Edge 系统的一台 PM 上的所有 A-Link 和专用网络都必须与另一台物理机 (PM) 上的匹配链路位于同一个 L2 广播域内，并且没有任何协议过滤。
- 在系统的两台 PM 之间发送的以太网数据包不应受到阻碍或速率限制。确保这些数据包不经过任何 L3 网络基础设施的路由或转接。
- A-Link 网络的速度应等于或大于业务或管理网络的速度。
- PM 之间的存储复制网络流量是通过 A-Link 网络发送的。
- 除了 ztC Edge 端点外，专用网络中没有连接网络主机。

相关主题

[A-Link 和专用网络](#)

ztC Console 要求

ztC Console 为该 ztC Edge 系统、其物理机 (PM) 和虚拟机 (VM) 提供基于浏览器的远程管理。

- 您的计算机必须能够访问包含 ztC Edge 管理网络 (在标记为 P1 的网络端口上已启用) 的子网。
- 使用支持的浏览器。参阅 [兼容 Internet 浏览器](#)。

关于更多信息，请参阅 [使用 ztC Console](#)。

兼容 Internet 浏览器

需要使用浏览器连接到 ztC Console。必须使用与 ztC Edge 系统兼容的浏览器。使用不兼容的浏览器会导致一些显示问题和略过一些向导。

下面的浏览器与ztC Edge系统兼容。

兼容浏览器	版本
Microsoft Internet Explorer™	11.0.648 或更高版本
Microsoft Edge	42.17134 或更高版本
Mozilla® Firefox®	65.0 或更高版本
Google® Chrome™	73.0 或更高版本

电源要求与注意事项

为保证最高可用性，Stratus强烈建议在采用冗余电源供电的物理机(PM)或节点上运行ztC Edge的容错(FT)软件。另外，两套PM电源应连接到不同电源。

请参阅[连接电源](#)中的一些关于电源连接配置的说明示例。

部署

在第一次部署系统时：



注意：如果您已经部署并配置了某个系统，并且您需要使其准备好在新站点进行部署，请参阅[重新部署ztC Edge系统](#)。

1. 查看网络布线信息。必要时，对您的网络进行更改。参阅[连接以太网电缆](#)。
2. 部署系统。参阅[部署系统](#)。

部署完成后，请参阅[部署后任务](#)。

相关主题

[升级 Stratus Redundant Linux 软件](#)

连接电源

要连接电源，则配置已授权用于两个节点的ztC Edge系统，使其具有连接到单独电源的冗余电源。您可根据情况使用不间断电源(UPS)，如下所示。

连接电源后，返回到[部署系统](#)。

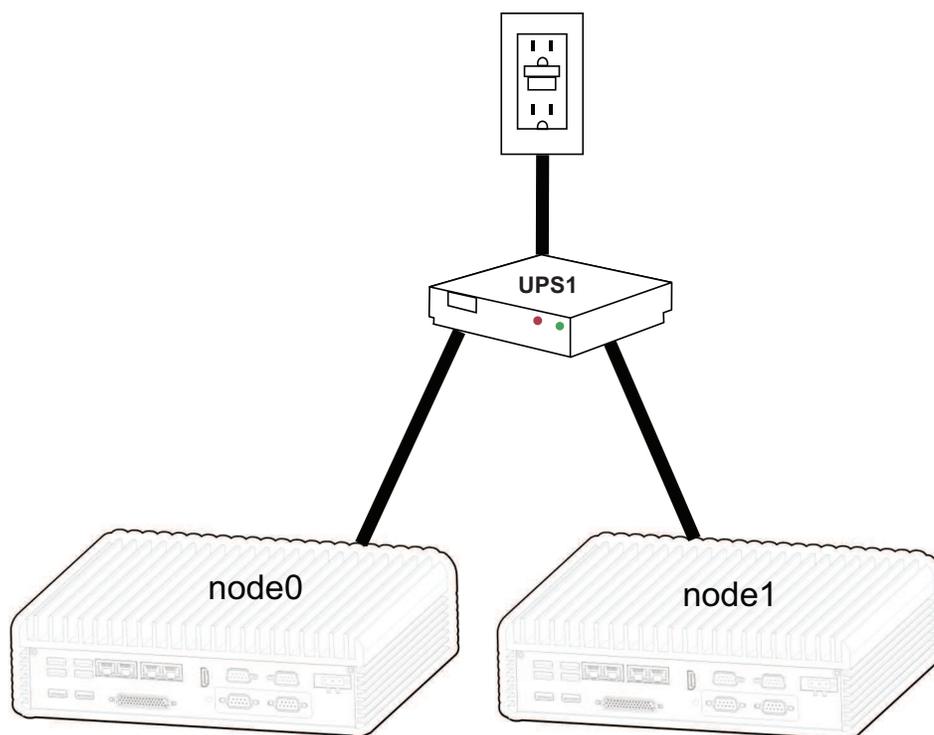
UPS(可选)

这些图显示了如何将一个或两个可选 UPS 装置连接到已授权用于两个节点的 ztC Edge 系统。

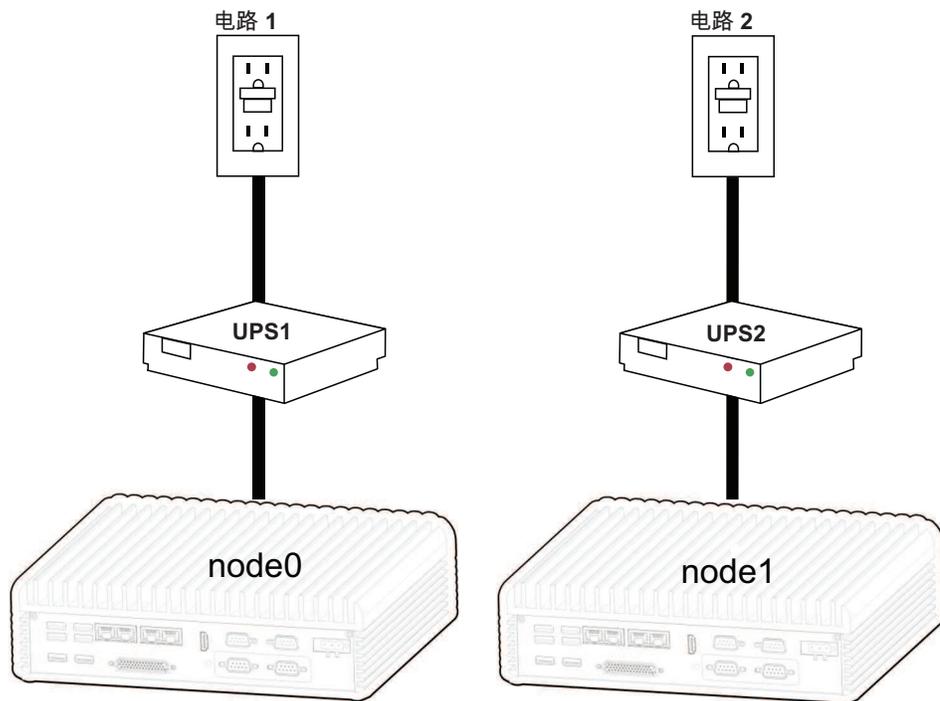


注意：Stratus 建议您使用连接到不同的独立电源的两个 UPS 装置。通过使用两个电源，在一个电源出现故障的情况下，系统会继续获得电力。

单 UPS:



双 UPS:



相关主题

[电源要求与注意事项](#)

部署系统

该主题描述如何部署 ztC Edge 系统。它补充了针对您系统的 [部署指南](#) 中的信息。(对于已授权用于一个节点的系统,如果您的系统已经在运行,并且您需要添加第二个节点,请参阅 [将节点添加到单节点系统](#)。)

要部署系统

1. 将键盘、监视器和电源连接到一个节点(针对您系统的 [部署指南](#) 的第 1 步)。您可以根据情况连接一个或两个可选不间断电源 (UPS)。有关信息,请参阅 [连接电源](#)。
2. 该节点自动启动。如果没有,则按电源按钮(针对您系统的 [部署指南](#) 的第 2 步)。

当监视器屏幕显示说明时,执行以下操作之一:

- 对于已授权用于两个节点的系统,按 **[1]** 键部署第一个节点。
- 对于已授权用于一个节点的系统,按 **[s]** 键部署一个节点。

- 对于已为您预配置的系统，按 **[c]** 键可继续重新部署该系统。

仅当系统集成商已为您配置了系统，然后清除了网络设置以便在您站点进行重新部署时，才会显示 **[c]** 选项。当您重新部署系统时，将保留预先配置的双节点或单节点选择、VM 和其他系统设置。

3. 将显示一个窗口，要求您选择一个键盘布局。使用 **Tab**、箭头或 **Esc** 键选择下列之一：

- 德国布局 = DE
- 日本布局 = JP106
- 美国布局 = US(默认)

使用 **Tab** 键导航到**确定**，然后按 **Enter**。



注意：初始部署后，您可以选择或更改键盘布局。有关信息，请参阅[映射您的键盘](#)。

4. 屏幕上的消息指导您选择配置该节点网络地址的方法。使用 **Tab**、箭头或 **Esc** 键选择下列之一：

- **通过 DHCP 自动配置(默认)**—选择此方法可将 P1 配置为动态 IP 配置。
- **手动配置(静态地址)**—选择此方法可为 P1 提供 IP 地址。将显示一个对话框，您可以在其中键入从网络管理员那里获得的值(您可能已在针对您系统的[部署指南](#)的**用户提供的组件部分**中写入这些地址)：
 - 该节点的 IP 地址
 - 该节点的子网掩码
 - 默认网关(可选)

如果您输入的信息无效，则该对话框将重新显示，直到您输入了有效信息为止。

使用 **Tab** 键导航到**确定(或返回)**，然后按 **Enter**。

5. 将显示确认对话框。使用箭头键或 **Tab** 键导航到**保存(默认)**，以保存显示的值(或导航到**返回**，以返回到上一窗口)。然后按 **Enter**。

如果您保存了这些值，蓝色屏幕将显示几秒钟。

6. 对于已授权用于两个节点的系统，将显示一条消息，指示解压缩第二个节点。

对于已授权用于一个节点或两个节点的系统，按照屏幕上的消息操作，该消息还指导您连接网络电缆，对于已授权用于两个节点的系统，启动第二个节点(针对您系统的[部署指南](#)的第 3 步)。有关网络配置的更多信息，请参阅[连接以太网电缆](#)。

对于已授权用于两个节点的系统，各个状态消息在屏幕上最多继续显示 15 分钟，对于已授权用于一个节点的系统，这些信息在屏幕上最多显示 5 分钟。

7. 此屏幕显示连接到网络浏览器中 IP 地址的消息(针对您系统的[部署指南](#)的第 4 步)。记下此 IP 地址，因为您将用它来登录 ztC Console。

连接到第一个节点的监视器没有显示更多额外提示。如果您将 P1 配置成了动态 IP 配置(对于节点的网络地址，选择以上[通过 DHCP 自动配置](#))，则按照[记录管理 IP 地址](#)中的描述记录其 IP 地址。



注意：如果您配置了错误的网络设置(例如，您错误键入了 IP 地址)，您可以通过按 **[1]** 键重新开始，以纠正此问题。

要完成此部署，请参阅[首次登录 ztC Console](#)。

部署指南

[ztC Edge100i/110i 系统: 部署单节点系统 \(R012Z\)](#)

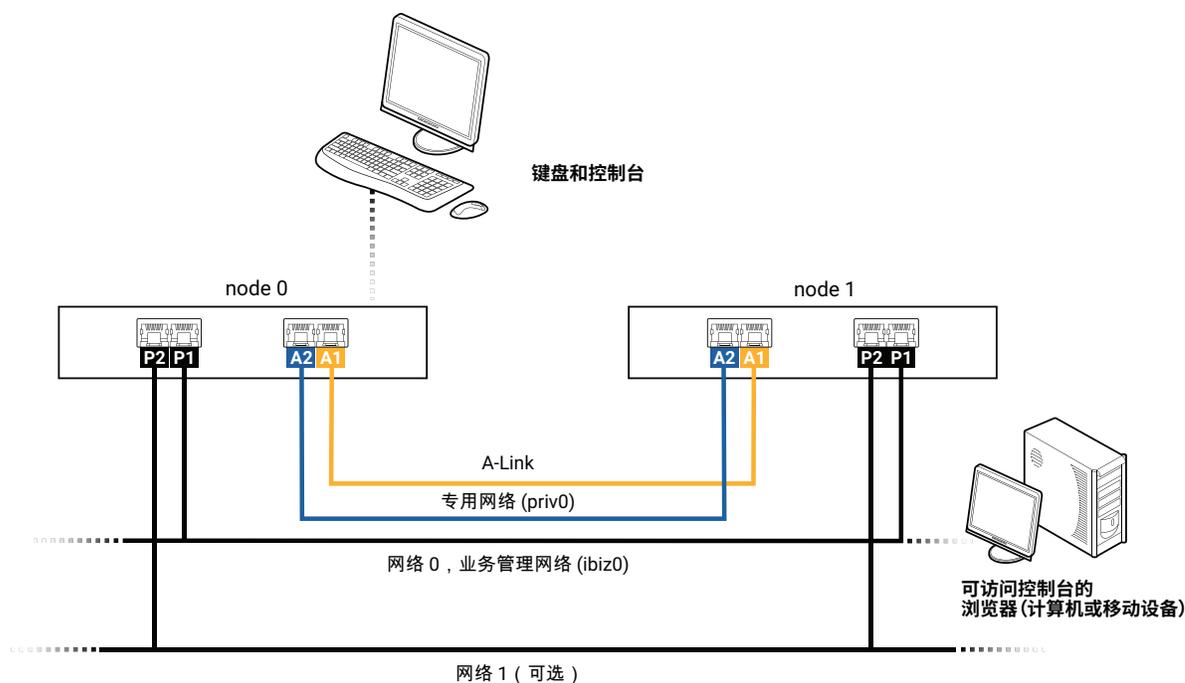
[ztC Edge100i/110i 系统: 部署单节点系统 \(R014Z\)](#)

连接以太网电缆

当部署 ztC Edge 系统时，您需要连接以太网电缆。下图显示的以太网电缆连接针对已授权用于两个节点的系统网络配置。(键盘和控制台可连接到 node0 或 node1。该图显示了到 node0 的连接。)在已授权用于一个节点的系统上，按照(以下)说明将以太网电缆连接到 **P1**(针对 network0 (ibiz0)) 和 **P2**(针对 network1 (ibiz1))。



注意：根据节点型号，以太网端口 **P1** 和 **P2** 以及端口 **A1** 和 **A2** 位于节点的前面或后面。



当您部署该系统时(请参阅[部署系统](#)), 连接:

- 蓝色电缆针对 **priv0**, 其从 **node0** 上的嵌入式端口 **A2** 连接到 **node1** 上的相同嵌入式端口。
- 黄色电缆针对 **A-Link1**, 其从 **node0** 上的嵌入式端口 **A1** 连接到 **node1** 上的相同嵌入式端口。

对于 **network0 (biz0)**, 将以太网电缆从每个节点上的 **P1** 连接到远程管理计算机能够访问的网络。

对于可选的 **network1 (biz1)**, 可将以太网电缆从每个节点上的 **P2** 连接到其他网络。

在您的网络中进行任何更改(如果需要), 以便为这些连接做准备。然后, 执行[部署系统](#)的下一步。

相关主题

[部署](#)

[A-Link 和专用网络要求](#)

[业务和管理网络要求](#)

[ztC Console要求](#)

映射您的键盘

部署后, 您可以针对不同布局配置键盘。

支持的键盘布局包括:

布局	语言
de	德语
de-latin1	德语 (latin1)
de-latin1-nodeadkey	德语 (无死键的 latin1)
dvorak	Dvorak
jp106	日语
sg	瑞士德语
sg-latin1	瑞士德语 (latin1)
uk	英国
us	美国英语
us-acentos	美国国际

要在部署之后配置键盘布局：

1. 作为根登录到第一个 PM。
2. 从该命令行发出 `localectl` 命令，以便配置正确的键盘布局。以下为配置德语键盘布局的示例：

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

3. 在第二个 PM(如果存在)上重复先前步骤。

相关主题

[部署后任务](#)

记录管理 IP 地址

您的网络管理员可能需要每台物理机 (PM) 的管理 IP 地址才能配置系统 IP 地址。如果已将管理网络配置为具有动态 IP 地址，则执行这个程序。(如果管理网络有静态 IP 地址，那么，您的网络管理员就已经有了这些信息。)

1. PM 完成了其安装并重启后，系统将显示与下面所示相似的屏幕：

```
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. 记录屏幕上显示的 IPv4 地址。
3. 将此 IP 地址提供给您的网络管理员。

返回到 [部署系统](#)，继续部署。

相关主题

[业务和管理网络要求](#)

部署后任务

完成系统部署后，还必须完成多项部署后任务，其中包括：

- [获取系统 IP 信息](#)
- [首次登录 ztC Console](#)
- [注册系统并获取永久授权](#)
- 配置所需的系统首选项：
 - [配置日期和时间](#)
 - [配置远程支持设置](#)
 - [配置仲裁服务器](#)
 - [指定所有者信息](#)
- [配置活动目录](#)
- [管理本地用户帐户](#)



注意：要启用忘记密码功能，您必须为每个用户帐户均指定一个电子邮件地址，包括**管理员**。如果用户帐户不包含电子邮件地址，并且用户单击控制台登录页面上的**忘记密码？**链接，则系统会向 **user@example.com** 发送电子邮件。**管理本地用户帐户**描述如何添加用户以及如何编辑用户帐户，包括如何添加电子邮件地址。

- [解决仪表板上的未决警报](#)
- [连接第二个业务网络](#)

在某些情况下，您可能需要执行以下额外任务：

- [重新部署 ztC Edge系统](#)
- [将节点添加到单节点系统](#)

获取系统 IP 信息

在部署系统后，您在首次登录 **ztC Console**时需要使用 **node0** IP 地址(参阅[首次登录 ztC Console](#))。在完成初次登录时，您还需要系统 IP 系统，网络管理员将提供这些信息。向网络管理员提供 **node0** 和 **node1**(如果存在) IP 地址(参阅[记录管理 IP 地址](#))，这有助于网络管理员确定系统 IP 信息。系统 IP 地址必须为静态 IP 地址。不要使用动态 IP 地址。

相关主题

[部署](#)

[部署后任务](#)

首次登录 ztC Console

在部署系统时，登录到**ztC Console**来接受最终用户授权协议 (EULA) 以及提供网络信息。您还可以注册系统并立即获取永久授权，但您可以稍后执行此操作。当首次安装系统时，其具有临时授权，该授权将在 30 天内到期。

首次登录 ztC Console

1. 在联网的 PC 或笔记本上，在浏览器地址栏内输入 **node0**(主)的 IP 地址(针对您系统的[部署指南](#)的第 5 步)。



注意：如果显示安全消息，继续访问该网站。您可以稍后添加安全例外，以允许站点在没有此消息的情况下加载(请参阅[配置安全连接](#))。

屏幕将显示 ztC Console 的登录页。

2. 输入用户名 **admin** 和密码 **admin**(或其他凭据, 如果提供), 然后单击 **登录**。

将显示 Stratus ztC Edge 最终用户授权协议 (EULA)。

3. 阅读 EULA, 然后, 适宜时, 单击 **接受** 来接受该协议。如果您没有接受 EULA, 部署会终止。

初始配置页将显示在 **配置** 下。

4. 缺省条件下, **通知** 中的 **启用支持通知** 复选框是选中的。如果您不想让 ztC Edge 系统向您的授权 Stratus 服务代表发送健康与状态通知, 则取消选中该复选框。您以后也可以修改该设置(参阅 [配置远程支持设置](#))。
5. 在 **系统 IP** 下, 对于 **静态系统 IP**, 输入您从您的网络管理员获得的静态系统 IP 地址(在针对您系统的 [部署指南](#) 中, 请参阅 [用户提供的组件部分](#))。(系统 IP 地址有时称为群集 IP 地址。)
6. 还在 **系统 IP** 下, 选择 **DHCP**(默认) 或 **静态**。对于 **DHCP**, 您无需提供额外信息。

如果您选择 **静态**, 将显示您在部署期间输入的 node0 静态 IP 地址。提供以下值(在针对您系统的 [部署指南](#) 中, 请参阅 [用户提供的组件部分](#)):

- 主和从 DNS
- 网络掩码
- node0 的网关地址
- node1 的 IP 地址(如果存在)
- node1 的网关地址(如果存在)

输入了网络配置后, 单击 **继续**。短暂延迟后, 将显示 **授权信息** 窗口。

7. 您可以注册系统并立即(针对您系统的 [部署指南](#) 的第 6 步) 或稍后安装永久授权。请参阅 [注册系统并获取永久授权](#)。
8. 注册完成后, 单击 **完成**。将显示 **帐户安全** 窗口。
9. 对于 **帐户安全** 中的 **新密码**, 为用户 **admin** 键入一个新密码。在 **确认密码** 中再次键入此密码。密码必须符合系统的密码策略(有关信息, 请参阅 [密码策略](#))。

注释：



- 为安全起见，您必须立即更改 **admin** 密码。您也可以稍后再次更改此密码，并且您应更改 **admin** 帐户的默认用户登录名。您可以在[用户与组](#)页面上进行这些更改(请参阅[配置“用户与组”](#)页面)。
- 此外为提高安全性，在部署后尽快更改每个 PM 的主机操作系统中 **root** 用户的密码(请参阅[访问主机操作系统](#))。

10. 单击**完成**。

将显示ztC Console，初始登录完成。使用书签标记或者记录系统 IP 地址，以便将来登录控制台时使用。

必要时，在[部署后任务](#)中执行额外任务。

相关主题

[部署](#)

[ztC Console](#)

[使用ztC Console](#)

[部署指南](#)

[ztC Edge100i/110i 系统: 部署单节点系统 \(R012Z\)](#)

[ztC Edge100i/110i 系统: 部署单节点系统 \(R014Z\)](#)

注册系统并获取永久授权

您必需注册系统，这包括获取永久授权。当首次部署系统时，其具有临时授权，该授权将在 30 天内到期。(对于刊头中的**资产 ID**，临时授权显示为 **UNREGISTERED_TRIAL**。)当您首次登录ztC Console时，您可以注册系统，或者稍后注册。您可以在具有或无 Internet 接入的系统上执行此操作。

在没有 Internet 接入的系统上，您需要在控制台的位置(没有 Internet 接入)与具有 Internet 接入的位置之间移动文件。两个方法如下，但也可使用其他方法：

- **USB 闪存驱动器**—在管理 PC(可连接到系统)与具有 Internet 接入的计算机之间移动 USB 闪存驱动器。
- **笔记本电脑或智能手机等移动设备**—在您可以登录 ztC Console 的位置与具有 Internet 接入的位置之间移动移动设备。

先决条件：

- 要注册系统，您需要 **Stratus** 提供的 **重要注册信息** 插页，这是与该系统一同提供的。此插页包含 **ztC Edge** 系统的资产 ID。如果您不再拥有 **ASSET ID**，请联系您的授权 **Stratus** 服务代表以获取它。
- 在您注册系统前，请阅读 [要完成注册门户步骤](#)，确保您获得了所有必需的信息。

要完成注册门户步骤**第 1 步：一般信息**—输入以下信息：

- **名字和姓氏**
- **公司电子邮件**—提供作为最终部署站点的公司的电子邮件地址。不要提供个人电子邮件地址。
- **资产 ID**—提供 **Stratus** 注册插页中的资产 ID。

您还需要查看并接受 **服务条款**。

第 2 步：位置信息—输入以下信息：

- **公司电子邮件** 和 **重新键入电子邮件**—提供作为最终部署站点的公司的电子邮件地址。不要提供个人电子邮件地址。
- **部署收货地址**—提供完整的更换部件收货地址。使用作为最终部署场点的公司的地址。不要提供邮政信箱。字段为：
 - **地址 1 和地址 2**
 - **城市、州、邮政编码和国家/地区**
 - **特殊说明** (例如“始终交付至装货码头 2”)

第 3 步：详细联系信息—输入以下信息：

- **主要技术联系人** 和 **次要技术联系人**—提供将与您的授权 **Stratus** 服务代表沟通的技术联系人的姓名。
- **服务续约合同**—提供负责处理每年服务协议续约的人员的姓名。

对于每个联系人，均输入 **名字、姓氏、电子邮件地址、座机和手机(可选)**。稍后您可以使用以下添加更多联系人：此 **Stratus 客户服务门户** 在 <https://support.stratus.com>。

单击页面底部的 **下一步** 后，**Stratus** 验证这些信息。

如果这些信息有问题，则将显示**遇到问题**窗格，其将描述此问题。单击**后退**可修复此问题(如果可能)。如果问题仍然存在，则单击**下一步**，继续，从而使您能够下载可使您完成注册的文件。为帮助解决此问题，以及确保正确设置您的账户，您的授权 **Stratus** 服务代表将联系您。

将显示**信息验证**页，从而使您能够查看这些信息。单击**后退**可更改任何信息。单击**下一步**可提交这些信息并完成注册。

第 4 步: 授权密钥—单击**完成**，下载授权密钥文件，此文件将安装在 ztC Edge 系统上。记下您将此文件下载到的位置。

要注册系统并获取永久授权

在具有 Internet 接入的系统上

1. 如果当您首次登录控制台时您注册系统，则从下一步开始。如果您在部署后注册系统，则执行以下步骤：
 - a. 在 ztC Console 中，单击左侧导航面板中的**首选项**。
 - b. 在**首选项**页面上，单击**产品授权**。
2. 对于**在线授权注册和激活**，单击**在线注册**，打开一个具有 Stratus 注册门户网站的新浏览器标签页。然后完成**注册门户网站步骤**。
在**第 4 步**，下载永久授权文件，然后将其保存到您的计算机。
3. 在控制台中，单击**安装授权栏**。
4. 单击**选择文件**，然后导航到您保存此文件的位置。
5. 选择该文件，单击**打开**，然后单击**上传**，将该文件上传到系统。

在无 Internet 接入的系统上

如果系统没有 Internet 接入，您需要在 ztC Console 的位置(没有 Internet 接入)与具有 Internet 接入的位置之间移动文件。以下操作程序描述了一种方法，但也可使用其他方法。

在能够访问 ztC Console 的计算机或移动设备上

1. 如果使用管理 PC，则将 USB 闪存驱动器插入 USB 端口中。
如果使用移动设备，则确保其能够访问 ztC Console。
2. 如果当您首次登录控制台时您注册系统，则继续执行下一步。如果您在部署后注册系统，则执行以下步骤：

- a. 登录到 ztC Console。
 - b. 单击左侧导航面板中的**首选项**。
 - c. 在**首选项**页面上，单击**产品授权**。
3. 对于第 1 步通过 URL 文件的离线授权注册(在**离线授权注册**和**手动授权安装**栏下)，单击**下载 URL 文件**，然后将 `register_site_file.html` 文件保存到 USB 闪存驱动器或移动设备。如果使用 USB 闪存驱动器，则拔掉它。
 4. 转到具有 Internet 接入的位置。

在具有 Internet 接入的位置

1. 如果使用 USB 闪存驱动器，则将其插入具有 Internet 接入的计算机的 USB 端口中。
2. 导航到您保存的文件，然后单击该文件名。浏览器会打开此文件，并被重定向到 Stratus 注册门户网站。完成**注册门户网站步骤**。

在**第 4 步**，下载永久授权密钥文件，然后将其保存到 USB 闪存驱动器或移动设备。如果使用 USB 闪存驱动器，则拔掉它。

3. 返回到可访问控制台的位置。

在能够访问 ztC Console 的计算机或移动设备上

1. 如果使用 USB 闪存驱动器，则将其插入管理 PC 上的 USB 端口中。
如果使用移动设备，则确保其能够访问 ztC Console。
2. 在控制台中，单击左侧导航面板中的**首选项**。
3. 在**首选项**页面上，单击**产品授权**。
4. 对于第 2 步，**将已激活的授权密钥安装到该系统**(在**离线授权注册**和**手动授权安装**栏下)，单击**选择文件**，然后导航到您保存此授权密钥文件的位置。
5. 选择该文件，单击**打开**，然后单击**上传**，将该文件上传到系统。

如果您首次登录控制台，则在您上传了授权后，返回到**首次登录 ztC Console**中的最后一步。

相关主题

[首次登录 ztC Console](#)

[管理产品许可证](#)

重新部署 ztC Edge系统

如果您已经部署并配置了系统，但您需要重新设置其网络设置，以便使其准备好在其他网络或子网上(可能是在一个新位置)进行部署，则重新部署 ztC Edge系统。

如果您需要利用设置和虚拟机 (VM) 使新 ztC Edge系统为最终用户做好准备，但后来您需要重新设置网络设置，以便最终用户能够首次在他们场点部署该系统(采用的方式类似于使用 Windows Sysprep 实用程序使 Windows 系统为其首次最终用户部署或全新体验 (OOBE) 做好准备)，则通常重新部署该系统。

为最终用户配置了该系统后，在 ztC Console 中开始重新部署。随后系统会清除系统和节点网络设置，关闭正在运行的任何 VM，以及关闭系统。系统保留其非网络系统设置和您配置的 VM，但现在其已准备好了进行部署，如针对您系统的 [部署指南](#) 中所述。

注释：

当您重新部署 ztC Edge系统时，注意以下限制和规避方法：

- 在重新部署系统前禁用任何 NFS/CIFS 共享。

活动 NFS/CIFS 共享会干扰重新部署功能。在新网络上配置完网络设置前，禁用这些共享。

- 在设置新的静态系统 IP 地址时需要重启系统。



如果您重新部署并关闭系统，在新位置启动系统，然后配置新的静态系统 IP 地址，则系统将无法访问辅助节点。要重新获得对辅助节点的访问权限，则打开 **系统** 页，单击 **重启**，重启系统。重启系统会刷新辅助节点上的网关设置，并使其连接到系统。

- 如果您已将系统移至新网络，但忘记首先重新部署它，请参阅 [KB-8283](#)，了解重新部署系统的说明。
- 如果您需要重新部署单个已使用的节点作为新系统中的第一个节点，或者作为其他系统中的辅助节点，请参阅 [KB-9391](#)，了解有关说明。

要重新部署 ztC Edge 系统

1. 使该系统为最终用户做好准备。配置 ztC Edge 系统设置并根据需要创建 VM。(当您重新部署系统时，将仅清除这些网络设置。)
2. 当系统准备完成时，打开 ztC Console 中的 **首选项** 页，单击 **IP 配置**，然后单击 **重新部署**。
3. 系统会清除系统和节点网络设置，关闭正在运行的任何 VM，以及关闭系统。

4. 系统准备由最终用户部署。要部署系统，请参阅针对您系统的[部署指南](#)。(如果需要，请参阅[部署系统](#)，了解其他详细信息。)

相关主题

[部署](#)

[ztC Console](#)

[使用 ztC Console](#)

[部署指南](#)

[ztC Edge100i/110i 系统: 部署单节点系统 \(R012Z\)](#)

[ztC Edge100i/110i 系统: 部署单节点系统 \(R014Z\)](#)

将节点添加到单节点系统

本主题描述如何将第二个节点添加到已授权用于一个节点的系统，以便创建冗余系统。它补充了为您系统[添加节点指南](#)中的信息。(如果您需要初始部署系统，请参阅[部署](#)。)

先决条件: 要完成此程序，您需要：



- 与正在运行的节点的型号和资产 ID 匹配的第二个 ztC Edge 节点，以及为获得双节点支持而更新的产品授权。如果需要，请联系您的授权 Stratus 服务代表以获得帮助。
- 如果已使用静态 IP 地址配置了第一个节点，则需要第二个节点的静态 IP 地址。
(您可以在 ztC Console 的[首选项页](#)的 **IP 配置** 下检查当前网络配置。)

要添加节点

1. 确认正在运行的节点正常 - SYS LED 正在闪烁，并且 ztC Console **仪表板** 页显示无未决问题的绿色标记。解决任何问题，然后再添加第二个节点。
2. 在 ztC Console 中，打开[首选项页](#)，然后单击 **产品授权**。单击 **立即检查授权**，更新您的当前授权，以获得双节点支持。在成功更新后，**仪表板** 页会指示双节点升级挂起。



注意: 考虑将后续步骤延迟到计划的维护窗口执行，因为在第 6 步中重新启动 VM 前，VM 性能会变慢。

3. 将第二个节点的 P1 端口连接到现有 LAN，并将蓝色和黄色网络电缆从第一个节点连接到第二个节点(A2 和 A1 端口)。将电源线连接到第二个节点，然后确认开启了此节点。有关网络配置的更多信息，请参见[连接以太网电缆](#)。



注意： ztC 控制台可开始显示有关第二个节点的警报。在第 6 步中完成同步前，您可以安全地忽略这些警报。

4. 在连接第二个节点后，等待最多 30 分钟，一直等到第二个节点上的 SYS LED 闪烁，并且物理机页上的**添加 PM**按钮变为活动状态。单击**添加 PM**。(如果该按钮保持不活动状态，则验证产品授权是否已更新，网络电缆和电源电缆是否已连接，以及第二个节点是否已启动。)



注意： 系统添加新节点时，管理控制台将最多 15 分钟不可用。

5. 在 ztC 控制台中，打开**首选项**页，然后单击**IP 配置**，以验证网络设置。如果需要，输入第二个节点 (**node1**) 的静态 IP 地址，然后单击**保存**。
6. VM 可同步数小时，之后必须重新启动 VM 才能启用冗余并清除警告。对于支持容错 (FT) 操作的系统，考虑在 VM 关闭时更新它们的保护级别 (HA/FT) 设置，如[更改虚拟机的保护级别 \(HA 或 FT\)](#) 中所述。当系统已同步并且 VM 正在运行时，**仪表板**显示绿色勾号，并且无未解决的问题。

添加节点指南

ztC Edge100i/110i 系统: 添加节点 (R015Z)

连接第二个业务网络

当您首次部署 ztC Edge 系统时，将网络电缆从每个节点的 P1 端口连接到您的现有网络，以便创建称为 **network0** 的共享业务/管理网络。

如果在部署后您要添加第二个专用业务网络 (**network1**)，您可以将网络电缆从每个节点的 P2 端口连接到您的现有网络。

添加第二个业务网络可帮助在具有两个或更多 VM 的系统上改进负载均衡，因为您能够将虚拟机 (VM) 分配到单独业务网络。减少 **network0** 上的负载还有助于提高性能，因为 **network0** 承载管理流量和业务流量。

要连接第二个业务网络

1. 将网络电缆从每个节点的 **P2** 端口连接到您的现有网络。
2. 在 ztC Console 中，进入 **网络** 页面。
 - a. 一分钟左右后应显示新的 **network1** 连接。
 - b. 确认新的 **network1** 连接显示一个绿色对勾。
3. 根据需要使用 **重新配置虚拟机** 向导为每个 VM 启用 **network1** (并且可禁用 **network0**)。有关更多信息，请参阅 [重新配置虚拟机资源](#)。

相关主题

[连接以太网电缆](#)

[A-Link 和专用网络要求](#)

[业务和管理网络要求](#)

[一般网络要求和配置](#)

3

第 3 章：使用 ztC Console

ztC Console 是一个基于浏览器的界面，其从远程管理计算机提供对 ztC Edge 系统的管理和监控。有关控制台的概述，请参阅 [ztC Console](#)。

关于 ztC Console 内页面的信息，请参阅如下主题：

- [“仪表板”页](#)
- [“系统”页](#)
- [“首选项”页](#)
- [“警报历史记录”页](#)
- [“审核日志”页](#)
- [“支持日志”页](#)
- [“物理机”页](#)
- [“虚拟机”页](#)
- [“卷”页](#)
- [“网络”页](#)
- [“虚拟 CD”页](#)
- [“升级套件”页](#)

ztC Console

ztC Console 是一个基于浏览器的界面，其从远程管理计算机提供对 ztC Edge 系统的管理和监控。您可以从该控制台执行许多管理操作，因为通过该控制台可将系统作为整体进行访问，以及访问

物理机 (PM)、虚拟机 (VM) 和其他资源。

有关运行 ztC Console 的远程管理计算机的要求的信息，请参阅 [ztC Console 要求](#)。

您可以使用 ztC Console 执行各种管理功能：

- 从仪表板读取系统警报。请参阅 [“仪表板”](#) 页。
- 查看 VM、CPU、内存和存储统计信息，以及从“系统”页重启或关闭系统。请参阅 [“系统”](#) 页。
- 设置系统的首选项、通知(电子警报和 SNMP 配置)和远程支持(通知和访问)；以及访问可使您创建安全连接的管理工具。系统首选项包括所有者信息和 IP 地址的配置值、仲裁服务、日期与时间等。请参阅 [“首选项”](#) 页。
- 查看警报和审核日志。请参阅 [“警报历史记录”](#) 页、[“审核日志”](#) 页和 [“支持日志”](#) 页。
- 监控、管理和维护资源：
 - PM 状态、存储(包括磁盘)、网络、VM 和 USB 设备：请参阅 [“物理机”](#) 页。
 - VM 状态和管理任务，例如创建、导入/恢复、管理和维护 VM：请参阅 [“虚拟机”](#) 页。
 - 卷，包括它们的状态、名称、数据同步状态、大小、状态和其他信息：请参阅 [“卷”](#) 页。
 - 网络，包括状态、链路情况、名称、内部名称、类型(例如 A-Link)、VM、速度、MAC 地址和网络带宽：请参阅 [“网络”](#) 页。
 - 虚拟 CD，包括它们的状态、名称、大小，以及是否能够移除 VCD：请参阅 [“虚拟 CD”](#) 页。
- 监控和管理升级套件。请参阅 [“升级套件”](#) 页。

您还可以编辑您的用户信息(请参阅 [编辑您的用户信息](#))以及配置用户和组(请参阅 [配置“用户与组”](#))。

相关主题

[首次登录 ztC Console](#)

[登录 ztC Console](#)

[使用 ztC Console](#)

登录 ztC Console

登录 ztC Console，以管理 ztC Edge 系统。您可以使用该控制台管理此系统，包括其物理机 (PM)、虚拟机 (VM)、存储和网络。您还可以查看警报和日志，以及执行其他管理任务。

注释：

1. 如果未使用，登录会话将在一小时后超时。
2. 系统具有 10 次登录会话的限制。
3. 密码必须符合系统的 [密码策略](#)。
4. 您可以配置登录横幅，以便为 ztC Console 登录页面提供自定义内容。请参阅 [配置登录横幅](#)。

要登录 ztC Console

1. 将 ztC Edge 系统的 IP 地址或者作为完全限定的域名 (FQDN) 的名称键入浏览器地址栏中：

`http://IP_address`

或

`http://FQDN_name`

IP_address 是在部署过程中提供的 ztC Edge 系统的静态 IP 地址。

FQDN_name 是与该 IP 地址相应的 FQDN。

2. 当显示登录页时，输入您的 **用户名** 和 **密码**。

如果您忘记密码，则单击 **忘记密码?**，此时将显示 **重置密码** 页面。输入请求的信息，以重置密码。



注意：重置密码要求您在系统上拥有电子邮件帐户，以及电子邮件地址，如在您的本地用户帐户中配置的(请参阅[管理本地用户帐户](#))。如果您无法接收电子邮件，则必须联系您的系统管理员，其将为您请求密码重置。(系统管理员需要请求主机 OS 管理员更改密码。主机 OS 管理员在主节点上使用命令更改密码。)

重置您的密码

注意：要在重置您密码时接收电子邮件，则必须配置邮件服务器。请参阅[配置邮件服务器](#)。

- a. 当显示 **重置密码** 页面时，输入您的 **用户名**，然后单击 **继续**。此时将向与您本地用户帐户一同列出的电子邮件地址发送电子邮件。该电子邮件包含可转向重置密码页面的链接。

- b. 在您的电子邮件帐户中，打开具有 `reset-password` 链接的电子邮件，然后单击该链接。将再次显示**重置密码**页面。
- c. 对于**新密码**和**确认密码**，键入您的新密码。新密码必须符合系统的**密码策略**。单击**继续**。
- d. 将显示一个页面，同时显示一条消息，说明重置成功，您可以使用新密码登录系统。单击**完成**。

3. 单击**登录**。

密码策略

系统的密码策略要求您的密码符合以下条件：

- 其最小长度为 **8** 个字符。
- 其必须包含大写和小写字符。
- 其不能为用户名。



注意：登录尝试的间隔为 **500 ms**，因此，在登录尝试后，您必须等待至少半秒钟才能再次登录。

相关主题

[首次登录 ztC Console](#)

[ztC Console](#)

[使用 ztC Console](#)

编辑您的用户信息

通过更改您的用户名、电子邮件地址、实名或密码来编辑您的用户信息(即，您的用户配置文件)。

编辑您的用户信息

1. 单击控制台右上角中您的用户名。

将打开**编辑用户**对话框。

2. 输入或修改以下项的值：

- **用户名**
- **电子邮件地址**

- 实名
- 密码



注意：密码必须符合系统的**密码策略**。

- 确认密码

3. 单击**保存**。(或者单击**取消**，取消更改。)

相关主题

[ztC Console](#)

[使用 ztC Console](#)

“仪表板”页

仪表板页显示 ztC Edge 系统上未决警报的摘要。要打开此页，则单击左侧导航面板中的**仪表板**。

要显示有关未决警报的更多信息，则单击 ztC Edge 系统图表中的警报符号(例如，)，或者单击以下系统图表的警报列表中的一个条目。警报列表可能显示在**全部**、**系统**或**已忽略**等选项卡中，根据警报，这些选项卡可能显示在系统图表下。这些警报信息包括：

- 与该问题相关的组件(例如 ztC Edge 系统、物理机 (PM) 或虚拟机 (VM))。
- 需要关注的活动或任务的描述。
- 应解决此问题的原因(如果可获得)。

应尽快处理活动警报(参阅[解决仪表板上的未决警报](#))。

了解 ztC Edge 系统图表。

仪表板页上的系统图表显示系统状态的图示。星形符号指示主 PM。警报符号(如果显示)表示需要关注的信息或关键警报。单击警报符号可显示有关此警报的信息。

相关主题

[“物理机”页](#)

[“系统”页](#)

[“虚拟机”页](#)

解决仪表板上的未决警报

在系统部署完成后，解决仪表板页面上显示的未处理警报。

解决未处理警报

在 ztC Console 仪表板页面上，查看页面下部列出的警报。您的选项如下：

- 解决警报。

例如，如果看到消息应启用支持服务，以确保尽量从 **Stratus** 获得最佳支持，则启用支持通知服务。

- 单击 **忽略** (在 **操作** 列下面) 来忽略该警报，并将其从列表中移除。可以忽略而不解决轻度警报。单击 **忽略** 来隐藏该警报。

要恢复列表中被忽略的警报时，单击警报列表上方的 **已忽略**，然后单击 **操作** 列下面的 **恢复**。

相关主题

[“仪表板”页](#)

“系统”页

系统 页显示有关 ztC Edge 系统的信息，并可使您重启或关闭该系统。此页还显示 ztC Edge 系统的 **统计信息** 和资源分配。要打开此页，则单击左侧导航面板中的 **系统**。

您可以使用 **系统** 页执行管理任务，包括：

- [重启系统](#)
- [关闭系统](#)

要启动系统 (在 PM 的物理控制台上)，请参阅 [启动系统](#)。

ztC Edge 系统上的其他许多任务都可使用 ztC Console 来执行。有关信息，请参阅 [ztC Console](#)。

查看统计

系统 页包含这些部分，这些部分显示系统使用率以及 PM 和 VM 的信息和统计：

- **系统名称**—圆形图指示系统的 CPU 分配、内存分配、磁盘 (R/W) 和网络利用率。
- **Node0** 和 **Node1** (如果存在)—圆形图指示每个节点的 CPU 利用率、内存利用率、磁盘利用率和网络利用率。对于磁盘利用率和网络利用率，您可以选择您要显示其统计的逻辑磁盘或网络。

相关主题

[使用 ztC Console](#)

启动系统

在每个物理机 (PM) 或节点的物理控制台上启动系统。这样做可执行有序启动: 首先启动系统软件, 然后启动系统上的虚拟机 (VM)。(要关闭系统, 请参阅[关闭系统](#)。)



小心: 如果您正在首次启动系统来部署它, 则遵循针对您系统的部署指南中的说明。(如果需要, 请参阅[部署系统](#), 了解其他详细信息。)



注意: 如果因为您断开电源线或因交流主电源断电而使 PM 断电, 则将 ztC Edge 系统中的每个 PM 均设为在电力一恢复便自动启动。系统软件和 VM 自动重启。

要启动 ztC Edge 系统

1. 确保已将所有必需的网络电缆连接到了两个 PM。
2. 按下系统中每个 PM 前面板上的电源按钮。
3. 确保每个 PM 前面板上的 PWR LED 亮起。

相关主题

[ztC Console](#)

[“系统”页](#)

[使用 ztC Console](#)

重启系统

使用 ztC Console 重启 ztC Edge 系统可安全地重启两个 PM, 同时不会影响 VM。



小心: 使用除下面所列之外的其他任何方法重启 ztC Edge 系统(例如分别从 PM 重启)都可能会导致数据丢失。



注意: 仅在两个 PM 都在正常运行且都不处于维护模式时才能重启已授权用于两个 PM 的系统。



先决条件: 在已授权用于两个 PM 的系统上, 确认这两个 PM 都在运行, 然后再重启。

要重启 ztC Edge系统

1. 在左侧导航面板中选择**系统**。
2. 单击**重启**按钮。将显示一条消息, 要求您确认重启。单击**是**, 继续。

重启可能最多需要 15 分钟。您可以在**仪表板**和**ztC Console**的刊头中观察此过程。系统的 PM 按顺序进入然后退出维护模式(有关维护模式的信息, 请参阅[维护模式](#))。

3. 验证这些 PM 是否重启, 以及所有 VM 是否按预计的那样继续运行。

在您启动重启后, 刊头中会出现一条消息, 显示此重启的状态。必要时, 您可以通过单击刊头中的**取消重启**, 取消重启。



小心: 如果您取消了重启, 系统会保持在当前状态, 您需要手动将其恢复到正常状态。

相关主题

[ztC Console](#)

[“系统”页](#)

[使用 ztC Console](#)

关闭系统

使用 **ztC Console**关闭 ztC Edge 系统。这样做可执行有序关闭: 首先关闭虚拟机 (VM), 然后关闭物理机 (PM)。仅使用此方法关闭 ztC Edge 系统。对于已授权用于两个 PM 的系统, 确保这两个 PM 均在运行, 然后再关闭。

小心:



1. 关闭 ztC Edge 系统会使 VM 脱机, 因此仅在计划的维护期间关闭该系统。
2. 通过其他任何方法关闭 ztC Edge 系统(例如分别拔下两个 PM 的电源)都可能导致数据丢失。



注意: 当您关闭系统时, 待机电源仍开启, 以实现无人值守管理, 除非您断开了电源线的连接或交流主电源已关闭。

要关闭 ztC Edge系统

1. 在已授权用于两个节点的系统上，确认这两个 PM 都在运行，以便使磁盘能够在节点间进行同步。
2. 在左侧导航面板中选择**系统**。
3. 单击**关闭**按钮。将显示警告：*其将关闭整个系统，并且停止一个或多个 VM!* 单击**是**，关闭，或者单击**否**，取消关闭。单击**是**后将显示一条消息，要求您确认关闭。再次单击**是**，关闭，或者单击**否**，取消关闭。

当该系统的 PM 按顺序进入维护模式时，您可以在**仪表板**和**ztC Console**的刊头中观察部分关闭过程(有关维护模式的信息，请参阅[维护模式](#))。但当该系统完全关闭时，**ztC Console**不可用，并且刊头显示**失去通信**。

该系统关闭后，您会失去与控制台的连接。如果ztC Edge系统无法完全关闭，则 VM 可能未正常关闭。执行以下操作之一来关闭 VM:

- 使用 VM 控制台或远程桌面应用程序登录 VM。使用操作系统命令关闭 VM。
- 登录到ztC Console。单击左侧导航面板中的**虚拟机**，选择 VM，然后单击**关机**。

相关主题

[管理虚拟机的运行](#)

[ztC Console](#)

[“系统”页](#)

[使用ztC Console](#)

“首选项”页

首选项页可使您配置ztC Edge 系统设置。要打开此页，则单击左侧导航面板中的**首选项**。

下表列出并描述了这些首选项。

首选项	描述
系统	
所有者信息	可使您指定然后查看ztC Edge系统管理员的姓名和联系信息。提供这些信息也是为了响应简单网络管理协议 (SNMP) 请求。请参阅 指定所

首选项	描述
	有者信息 。
产品授权	可使您查看和管理 ztC Edge 产品授权。请参见 管理产品许可证 。
软件更新	可使您检查系统软件的当前版本以及是否可获得新版本。如果可获得新版本，您可下载它并阅读发行说明。您还可以指定在可获得更新时发送警报，以及自动下载可用更新。请参见 管理软件更新 。
IP 配置	可使您查看和指定系统的 Internet 协议 (IP) 地址和网络设置；以及部署系统。请参见 配置 IP 设置 。
仲裁服务器	可使您查看现有和新仲裁服务器。仲裁服务器对于 ztC Edge 环境中的特定故障提供数据完整性保证和自动重启功能。请参见 仲裁服务器 和 配置仲裁服务器 。
日期与时间	可使您查看系统时间、指定网络时间协议 (NTP) 的值(推荐)，或者在系统上手动设置时间和日期。请参见 配置日期和时间 。
邮件服务器	可使您配置邮件服务器，以便使 ztC Edge 系统能够在例如某人需要重置密码时发送电子邮件。请参见 配置邮件服务器 。
管理工具	
用户与组	可使您在 ztC Edge 系统上添加、修改或移除用户帐户；启用活动目录(然后授予它)，以及选择一个用户并查看上次更新该用户密码的时间。管理员还可使用该页面强制所选用户在下次登录时更改该用户的密码。请参见 配置“用户与组”
安全连接	可使您仅启用与系统之间的 HTTPS 连接。请参见 配置安全连接 。
VM 设备配置	可使您禁止或允许在所有 VM 中插入虚拟 CD (VCD)，或者将 USB 设备附加到所有 VM。请参见 配置 VM 设备 。
IPtables 安全性	可使您使用管理工具 IPtables 管理 IP 数据包过滤。请参见 管理 IPtables 。

首选项	描述
登录横幅通知	可使您配置登录横幅。请参阅 配置登录横幅 。
ztC Advisor	可使您启用 ztC Advisor ，以便使管理员能够在 ztC Advisor 仪表板中远程监控系统的运行状况。请参阅 启用 ztC Advisor 。
保存首选项	可使您将 首选项 页设置保存到本地计算机或云中的文件。请参阅 保存和还原系统首选项 。
还原首选项	可使您从备份文件还原 首选项 页。请参阅 保存和还原系统首选项 。
通知	
电子警报	可使您启用面向系统管理员的电子邮件警报(电子警报)。请参阅 配置电子警报 。
SNMP 配置	可使您启用简单网络管理协议 (SNMP) 请求和自陷，以实现远程系统监控。请参阅 配置 SNMP 设置 。
OPC 配置	可使您配置开放式平台通信 (OPC) 设置以启用 OPC 服务器功能，该功能可使您监控 ztC Edge 系统和其他工业设备。请参阅 配置 OPC 设置 。
远程支持	
支持配置	可使您配置远程访问和通知。远程访问可使您的授权 Stratus 服务代表远程登录系统，以进行故障排除。启用时， ztC Edge 系统可向您的授权 Stratus 服务代表发送有关系统问题的通知。请参阅 配置远程支持设置 。
代理配置	可使您为 ztC Edge 系统配置代理设置，如果您的组织需要使用代理服务器接入 Internet，并且您与 Stratus 或另一个授权 ztC Edge 服务代表签订了服务协议。 Stratus Redundant Linux 软件使用代理服务器信息来实现支持通知消息传递和远程支持访问功能。请参阅 配置 Internet 代理设置 。

相关主题

[ztC Console](#)

[使用 ztC Console](#)

指定所有者信息

指定 ztC Edge 系统的管理员或所有者的姓名和联系方法，以便使用这些信息提供支持。

此联系信息可在 ztC Console 中找到，并会在响应简单网络管理协议 (SNMP) 请求时提供。

指定系统所有者的信息

1. 单击左侧窗格中的 **首选项**。
2. 在 **首选项** 页面上，单击 **所有者信息**。
3. 提供的信息应包括 **全名**、**电话号码**、**电子邮件** 和 **网址** 字段。
4. 单击 **保存**。

相关主题

[“首选项”页](#)

[ztC Console](#)

管理产品许可证

使用如下方法管理系统的产品授权：

- 在部署过程中或之后获取永久授权。
- [检查现有授权的状态，必要时对其进行更新](#)。
- 查看当前授权信息，例如状态和过期日期。

当首次安装系统时，其具有临时授权，该授权将在 30 天内到期。（对于刊头中的 **资产 ID**，临时授权显示为 **UNREGISTERED_TRIAL**。）您必需注册系统，这包括获取永久授权。您可以在初始部署之后立即或稍后注册系统。有关注册系统的信息，请参阅 [注册系统并获取永久授权](#)。

系统具有了永久授权后，如果系统有 **Internet** 连接，系统会每 24 小时向授权服务器核实，以了解是否有更新。如果系统没有 **Internet** 接入，您仍可更新授权并查看其状态。要执行此操作，您需要在 **ztC Console** 的位置（没有 **Internet** 接入）与具有 **Internet** 接入的位置之间移动文件。两个方法如下，但也可使用其他方法：

- USB 闪存驱动器—在管理 PC(可连接到系统)与具有 Internet 接入的计算机之间移动 USB 闪存驱动器。
- 笔记本电脑或智能手机等移动设备—在您可以登录 ztC Console 的位置与具有 Internet 接入的位置之间移动移动设备。

对于适用于您需求的操作程序，选择以下菜单(如果适用，单击下拉列表)。

要检查授权的状态时

如果系统具有 Internet 接入，则使用以下操作程序。必要时，此操作程序还可自动更新授权。如果系统没有 Internet 接入，则使用 [在无 Internet 接入的系统上](#) 操作程序。如果您需要手动更新授权，请参阅 [手动更新授权](#)。

1. 在 ztC Console 中，单击刊头中的 **asset_ID(资产 ID: asset_ID)**。

或者，在已注册的系统上，单击控制台左侧导航面板中的**首选项**，然后：

 - a. 在**首选项**页面上，单击**产品授权**。
 - b. 对于**在线授权检查**，单击**立即检查授权**。
2. 控制台显示授权的状态(日期格式因位置而异)：

状态	授权已激活，未过期。
上次检查	日，月 dd, 20yy, 时间
服务过期	日，月 dd, 20yy, 时间
资产 ID	asset_ID
产品 UUID	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
FT 已启用	Yes_or_No
允许 ALSR	Yes_or_No
允许客人监控	Yes_or_No
允许保存/还原系统首选项	Yes_or_No
保存/还原系统首选项过期	日，月 dd, 20yy, 时间_或_从未授权

为已注册的系统手动更新新授权

在具有 Internet 连接的注册系统上会自动更新授权。必要时，您还可以手动更新授权。

在具有 Internet 接入的系统上

1. 在控制台中，单击左侧导航面板中的**首选项**。
2. 在**首选项**页面上，单击**产品授权**。
3. 单击**离线授权检查和手动授权安装**栏，以显示其选项(如果尚未显示它们)。
4. 在**通过 URL 文件的离线授权检查**下，单击**下载 URL 文件**，然后保存该文件。
5. 单击文件名。将打开网络浏览器，**Stratus**授权服务器查看该授权文件的状态。必要时将自动下载新授权 **.key** 文件。
6. 然后，单击**上传**。

在无 Internet 接入的系统上

使用以下操作程序来检查此授权，必要时在没有 Internet 接入的已注册系统上手动获取新授权。您需要在 ztC Console 的位置(没有 Internet 接入)与具有 Internet 接入的位置之间移动文件。以下操作程序描述了一种方法，但也可使用其他方法。

在能够访问 ztC Console 的计算机或移动设备上

1. 如果使用管理 PC，则将 USB 闪存驱动器插入 USB 端口中。
如果使用移动设备，则确保其能够访问 ztC Console。
2. 登录到 ztC Console。
3. 单击左侧导航面板中的**首选项**。
4. 在**首选项**页面上，单击**产品授权**。
5. 单击**离线授权检查和手动授权安装**栏，以显示其选项(如果尚未显示它们)。
6. 在**通过 URL 文件的离线授权检查**下，单击**下载 URL 文件**，并将该文件保存到移动设备或 USB 闪存驱动器。如果使用 USB 闪存驱动器，则拔掉它。转到具有 Internet 接入的位置。

在具有 Internet 接入的位置

1. 如果使用 USB 闪存驱动器，则将其插入具有 Internet 接入的计算机的 USB 端口中。
2. 导航到您保存的文件，然后单击该文件名。
3. 将打开网络浏览器，**Stratus**授权服务器查看该授权文件的状态。必要时将自动下载新授权 **.key** 文件。如果使用 USB 闪存驱动器，则将该新授权 **.key** 文件复制到它上，然后拔掉 USB 闪存驱动器。
4. 返回到可访问控制台的位置。

在能够访问 ztC Console 的计算机或移动设备上

1. 如果使用 USB 闪存驱动器，则将其插入管理 PC 上的 USB 端口中。
如果使用移动设备，则确保其能够访问 **ztC Console**。
2. 在控制台中，单击左侧导航面板中的**首选项**。
3. 在**首选项**页面上，单击**产品授权**。
4. 单击**离线授权检查和手动授权安装**栏，以显示其选项(如果尚未显示它们)。
5. 对于**将已激活的授权密钥安装到该系统**，单击**选择文件**，然后导航到您保存此文件的位置。
6. 选择该文件，单击**打开**，然后单击**上传**，将该文件上传到系统。

相关主题

[ztC Console](#)

[“首选项”页](#)

[使用 ztC Console](#)

管理软件更新

您可以通过检查系统软件的当前版本号以及检查软件更新是否可获得来管理软件更新。您还可以选择启用以下功能：

- 在可获得系统软件更新时将发送到**警报历史记录**页的消息。
- 在可获得系统软件更新时将发送给系统管理员的电子邮件警报(电子警报)。
- 系统将自动下载(但不安装)更新。

如果将系统配置为自动检查是否有更新，则系统将每天在当地时间午夜前后检查一次。在可获得更新时，系统会在检查是否有更新的软件后立即将其下载到系统上的暂存区域。如果成功下载到暂存区域并且已配置为这样做，则系统会向**警报历史记录**页发送消息和/或发送电子警报，说明该软件已准备好安装。如果下载失败，则会删除此更新。



先决条件：如果您希望系统管理员在可获得更新时收到电子警报，则必须配置邮件服务器和电子警报(如果尚未配置)。请参阅[配置邮件服务器](#)和[配置电子警报](#)。

要管理软件更新

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**首选项**页面上，单击**软件更新(在系统下)**。

3. 将显示**可用系统软件更新**，并且显示以下信息：

- 当前系统软件的版本号。
- 新版本系统软件的版本号(如果可获得)。

如果可获得新版本的系统软件，则在适用于您需求时，单击下列一个或两个链接：

- **下载软件**—单击此链接可下载可用版本。
- **查看发行说明**—单击此链接可查看发行说明以及可用版本的整个用户指南。

4. 将显示**管理系统软件更新**，并且具有以下选项：

- **当可获得系统软件更新时提醒我**—如果要将在可获得更新这一消息发送到**警报历史记录**页，则选择该选项。如果要向系统管理员发送电子邮件，从而在可获得更新时通知他们，您必须配置电子警报。
- **当可获得系统软件更新时自动下载它们。(仅下载到系统，不安装)**—如果您要在可获得新系统软件更新时使系统自动下载它，则选择此选项。下载该软件后，可在**升级套件**页上将其作为升级套件，并且您可以安装该软件。有关其他信息，请参阅[“升级套件”](#)页和[使用升级套件升级 Stratus Redundant Linux软件](#)。

5. 单击**保存**。

相关主题

[“警报历史记录”](#)页

配置 IP 设置

配置ztC Edge系统的网络协议 (IP) 设置来设置或修改此系统和节点的 IP 地址，以及网络掩码、网关地址和域名系统 (DNS) 服务器等适用设置的值。(您还可以在使用**重新部署**按钮重新部署系统时修改网络设置，如[重新部署 ztC Edge系统](#)。)

部署过程中和部署后，您可以为系统配置 IP 地址。对于已授权用于两个节点的系统，需要配置三个 IP 地址：系统一个，每个节点(`node0` 和 `node1`) 各一个。对于已授权用于一个节点的系统，需要配置两个 IP 地址：系统一个，节点 (`node0`) 一个。在部署后，可以使用下面的适宜步骤修改 IP 地址和其他 IP 设置。您必须为ztC Edge系统指定一个静态 IPv4 地址。

警告：

1. 在未通知网络管理员并获得其指导的情况下，特别是当系统正在运行 VM 时，不要修改 IP 配置设置。否则可能会导致系统及其所有 VM 无法访问。
2. 如果您更改**静态系统 IP**地址，在 VM 重启时，自动分配给 VM 的任何 MAC 地址都将更改，因为 Stratus Redundant Linux 软件会根据系统 IP 地址为 VM 生成 MAC 地址。要防止 VM 的 MAC 地址发生更改(例如，支持基于 MAC 地址授权的软件应用程序)，则按照**将特定 MAC 地址分配给虚拟机**中的说明设置永久 MAC 地址。
3. 您必须使用 ztC Console 修改 IP 地址。切勿使用 Linux 工具。

注释：

1. IP 设置配置步骤取决于 ztC Edge 系统是留在同一个子网络上还是迁移到一个新的子网络上。如果您需要将 ztC Edge 系统移至新子网，则**重新部署**该系统，以便清除其网络设置，然后再移动它，如**重新部署 ztC Edge 系统**中所述。
2. 更改新子网的 IP 设置一般包括更改节点的物理网络连接(例如：断开连接，然后如果移动 PM，即重新连接网络电缆)。从节点处断开电缆前，必须先关闭节点。为此，您可以选择使用**首选项页 IP 配置**部分中的**保存和关闭**按钮。
3. 在已授权用于一个节点的系统中，**IP 配置**页面仅显示一个节点的设置。

要使用同一个子网上的系统修改系统和/或节点 IP 设置

在这套步骤中，ztC Edge 系统和所有虚拟机 (VM) 继续运行；不过，当修改了系统 IP 地址时，ztC Console 将短时失去与系统的连接。1-2 分钟后，就可以使用新系统 IP 地址访问 ztC Console。(您可以分别在各节点上修改节点 IP 地址，这种情况下控制台连接不会断开。)

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 单击**IP 配置**。
3. 在**静态系统 IP**框中，键入您从您的网络管理员获得的静态系统 IP 地址。
4. 单击**静态**按钮，然后为主 DNS 和从 DNS 键入有效的、独一无二的值。
5. 确认所显示的**子网掩码**值正确无误。
6. 对于**Node0** 和 **Node1**(如果存在)，为**IP 地址**和**网关 IP**输入适当的值。
7. 单击**保存**来保存数值(或单击**重置**来恢复以前的数值)。

当修改了系统 IP 地址时，将显示**已更新系统 IP**消息框。短暂延迟后，浏览器将自动重定向到新的系统 IP 地址。

相关主题

[部署](#)

[获取系统 IP 信息](#)

[首次登录 ztC Console](#)

[“首选项”页](#)

[ztC Console](#)

[使用 ztC Console](#)

配置仲裁服务器

在首次登录到 ztC Edge 系统时，配置仲裁服务器。

先决条件：



1. 您必须有已授权用于两个节点的系统才能配置仲裁服务器。
2. 在配置仲裁服务器前，请阅读[仲裁服务器](#)和[创建ALSR配置](#)(其讨论仲裁服务器)。

注释：



1. 为使 VM 识别仲裁服务器配置更改，必须关闭该 VM，然后将其重新开启，以重启该 VM。请参阅[关闭虚拟机](#)和[启动虚拟机](#)。
2. 仲裁服务器上的“Windows 更新”会中断服务器的运行，这会影响故障恢复行为。在仲裁服务器上，您应计划在维护期间进行 Windows 更新，或者禁用“Windows 更新”。

要配置仲裁服务器

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 单击**仲裁服务器**。
3. 单击**添加仲裁服务器**。
4. 在**添加首选仲裁服务器**对话框中，输入以下值(如果首选仲裁服务器已经存在，**添加首选仲裁服务器**对话框将出现)：

- **DNS 或 IP 地址**-为优选仲裁服务器输入完全符合条件的 **DNS 主机名称或 IP 地址**。
- **端口**(缺省值是 4557)-如果端口号与缺省值不同,则输入端口号。

单击 **保存**,保存这些值。

5. 重复步骤 4 和 5,配置第二个即替代仲裁服务器。**Stratus**建议配置两个仲裁服务器。
6. 要启用仲裁服务器时,选择 **已启用**复选框后单击 **保存**。

要移除仲裁服务器



小心: 如果移除了优选仲裁服务器,替代仲裁服务器将变成优选仲裁服务器。如果不存在替代仲裁服务器,则删除优选仲裁服务器后将自动禁用仲裁服务。

1. 导航到ztC Console的**首选项**页面。
2. 单击**仲裁服务器**。
3. 找到要删除的仲裁服务器项。
4. 在最右列,单击**移除**。



注意: 如果某 VM 使用的是正在移除的仲裁服务器,则必须重启该 VM,以令其无法识别该仲裁服务器,从而令移除流程得以完成。

相关主题

[ztC Console](#)

[“首选项”页](#)

[使用ztC Console](#)

配置日期和时间

当您首次登录ztC Edge系统时,配置日期和时间,以便启用网络时间协议 (NTP) 服务。使用 NTP 服务可自动设置系统时钟,并确保其不会偏离实际时间。



小心: 当您更改日期和时间设置时,如果系统时间已偏离实际时间,则主物理机 (PM) 可能重启,从 PM(如果存在)可能关闭。在重启完成前,所有虚拟机 (VM) 均停止,并且业务处理会中断。

注意：只要 VM 迁移或重启，时钟便在不同时区之间进行切换。为确保 VM 中的时区不会更改，



- 将所有 VM 中的时区设置为与为 ztC Edge系统配置的时区相对应。
- 将所有 VM 中的时区配置为使用为 ztC Edge系统配置的同一直 NTP 服务器。

要配置日期和时间设置

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**首选项**页面，单击**日期和时间**。
3. 在**日期和时间**显示中，**配置时区**的默认设置为**美国，纽约**。必要时选择一个适合您位置的时区。
4. 对于**配置日期和时间**，选择下列之一：
 - **自动(建议)**可启用 NTP 服务。在文本区域中键入 NTP 服务器地址，每行一个。指定多个 NTP 服务器可提供冗余。
 - **手动**可使您手动输入设置。



注意：如果您手动配置时间，ztC Edge系统的时间可能会偏离实际时间。

5. 单击**保存**(或者单击**重置**，以便还原先前保存的值)。

如果因时间偏离系统要求重启，则会在 ztC Console 刊头显示一条消息，告诉您系统将重启。在这种情况下，主物理机 (PM) 将重启，从 PM(如果存在)将关闭。在主 PM 重启时，您会失去与 ztC Console 的连接。当重启完成时，PM 会重新建立与该控制台的连接，并且您将收到一条警报，告诉您重启从 PM。

相关主题

[ztC Console](#)

[“首选项”页](#)

[使用 ztC Console](#)

配置邮件服务器

配置邮件服务器，以便使 ztC Edge 系统能够在例如某人需要重置密码时发送电子邮件。

要配置邮件服务器

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**系统**下，单击**邮件服务器**。
3. 单击 **Enable Mail Server(启用邮件服务器)** 框。此时将显示用于指定或选择以下设置的框：
 - **SMTP 服务器(必填)**—输入您所在公司用于发送电子邮件的简单邮件传输协议 (SMTP) 服务器的名称。
 - **端口号(可选)**—输入在发送电子警报时将使用的端口号。如果未指定端口号，则将使用默认 SMTP 端口 25。(有关 SMTP 端口等所有端口的其他信息，请访问知识库，搜索文章 *ztC Edge 使用的 TCP 和 UDP 端口 (KB-9357)*。请参阅 [访问知识库文章](#)。)
 - **发送者电子邮件地址**—通过在下列任何一种情况下指定有效的发送者电子邮件地址，启用电子警报：
 - 您尚未在 **ztC Edge**系统上指定 DNS 服务器，并且未将您的 SMTP 服务器配置成接受域文本(发件人地址采用 `noreply@IP_address` 的形式)。
 - 您想让电子警报提供不同的发送者电子邮件地址(例如，`noreply@company.com`)。SMTP 服务器接受的任何电子邮件地址即可。
 - **加密的连接**—从 SMTP 服务器所需的加密协议下拉菜单中选择一个值：
 - **无**表示无加密。默认情况下使用端口号 25。
 - **TLS**表示传输层安全 (TLS) 协议。对于 TLS，尽管默认情况下使用 25，但 **Stratus** 建议您对**端口号**指定 587。
 - **SSL**表示安全套接字层 (SSL) 协议。对于 SSL，尽管默认情况下使用 25，但 **Stratus**建议您对**端口号**指定 465。
 - **启用身份验证**—如果 SMTP 服务器要求进行身份验证来发送电子邮件，则单击此框。然后，键入 SMTP 帐户的**用户名**和**密码**。

如果您没有键入密码，则仍需要键入先前密码。如果先前密码为空，并且您没有输入新密码，则密码仍为空。
4. 单击**保存**(或者单击**重置**，以便还原先前保存的值)。

相关主题

[ztC Console](#)

[“首选项”页](#)

[使用 ztC Console](#)

配置“用户与组”

利用[用户与组](#)页添加、修改或删除 ztC Edge 系统上的用户帐户，或者为活动目录用户授予访问权。您可以选择一个用户并查看上次更新该用户密码的时间。管理员还可使用该页面强制所选用户在下次登录时更改该用户的密码。

要打开此页面，则单击左侧导航面板中的[首选项](#)，然后在[首选项](#)页面上，选择[管理工具](#)下的[用户与组](#)。

要管理本地用户帐户时

要添加新用户时，单击下部窗格右侧的[添加](#)。要修改原有用户，单击用户帐户名，然后单击[编辑](#)或[移除](#)。

要查看用户上次更改用户密码的时间，则查看所选用户的 **Last Password Update Time(上次密码更新时间)**列。要强制用户在下次登录时更改用户密码，管理员将选择该用户，然后单击 **Expire Password(密码过期)**。

关于更多信息，请参阅[管理本地用户帐户](#)。

要管理域用户帐户时

关于在您的 ztC Edge系统上启用活动目录的信息，请参阅[配置活动目录](#)。要授予或移除域用户对 ztC Edge系统的管理访问权，请参阅[管理域用户帐户](#)。



注意：如果您以管理员身份登录了已配置活动目录用户或组的系统，则[授予访问权](#)按钮将显示在[用户与组](#)页的右上角。单击[授予访问权](#)按钮可启动“授予访问权”向导。[管理域用户帐户](#)主题探讨“授予访问权”向导的使用。

要排序和查找用户帐户时

当您有大量帐户时，可以单击列标题来按参数对帐户进行排序。您可以按[类型](#)、[用户名](#)、[实名](#)、[电子邮件地址](#)或[角色](#)对帐户进行排序。

相关主题

[管理域用户帐户](#)

[管理本地用户帐户](#)

[配置活动目录](#)

[安全性加强](#)

管理本地用户帐户

可以在 **ztC Console**的**用户与组**页上为本地用户帐户添加、编辑或移除用户、指定密码和分配用户角色。您还可以选择一个用户并查看上次更新该用户密码的时间，并且管理员可强制所选用户在下次登录时更改用户密码。您能够为不是管理员的用户分配任务(或权限) *将计算机加入域*。(关于活动目录域中已有用户帐户访问权的授予和拒绝，请参阅[管理域用户帐户](#)。)

本地用户帐户驻留在**ztC Edge**系统本身，而不是中央域服务器上。可以在**用户和组**页面上查看本地用户，方法是查找在**类型**列标有**本地用户**的项。

用户角色为：

- **管理员**：完整系统管理员权限
- **平台管理员**：除了用户添加、移除和修改之外的系统管理员权限
- **VM 管理员**：能够管理 VM(有关详细信息，请参阅[管理虚拟机](#))
- **只读**：能够查看但不能修改系统配置或安装系统软件

对于以下程序，首先打开**用户与组**页面：单击左侧导航面板中的**首选项**，打开**首选项**页面，然后在“管理工具”下，选择**用户与组**。

要添加一个用户帐户时

1. 在上部窗格中，单击**添加**。
2. 在**角色**下拉窗口中，选择**管理员**、**平台管理员**、**VM 管理员**或**只读**。
3. 提供**用户名**、**密码**(和**确认密码**)、**电子邮件地址**和**实名字段**的值。用户名的长度可以为 1 到 64 个字符，但不得包含空格。密码必须符合系统的**密码策略**。
4. 单击**保存**。

要编辑一个用户帐户时

1. 选择要编辑的帐户。
2. 在上部窗格中，单击**编辑**。
3. 必要时更改用户信息。例如，要更改一个用户的角色，在**角色**下拉窗口中，选择**管理员**、**平台管理员**、**VM 管理员**或**只读**。
4. 单击**保存**。

强制用户更改用户密码

1. 选择要使其密码过期的用户。
2. 单击**密码过期**。
3. 在确认对话框中单击**是**。

要为管理员分配“将计算机加入域”

1. 将不是管理员的用户添加到 AD 服务器，并向该用户委派任务(或权限)**将计算机加入域**。有关详细信息，请参阅针对 AD 服务器的文档。
2. 在 ztC Edge 系统上，编辑 `/etc/resolv.conf` 文件，以便添加 AD 域控制器的 IP 地址。例如以下行：

```
nameserver 123.456.28.910
```
3. 在 ztC Console 中，如果尚未启用 AD，则启用它。请参见 [配置活动目录](#)。

要移除一个用户帐户时

1. 选择要移除的帐户。
2. 单击下部窗格中的**移除**。
3. 在确认对话框中单击**是**。

注释：



1. 您无法删除缺省 **admin** 帐户，但可以通过编辑该帐户来修改其名称和密码。
2. 要启用忘记密码功能，您必须为每个用户帐户均指定一个电子邮件地址，包括**管理员**。如果用户帐户不包含电子邮件地址，并且用户单击控制台登录页面上的**忘记密码？**链接，则系统会向 **user@example.com** 发送电子邮件。

相关主题

[配置活动目录](#)

[管理域用户帐户](#)

[配置“用户与组”](#)

管理域用户帐户

您可以为活动目录 (AD) 域用户帐户授予对 **ztC Console** 的访问权限。与本地 **ztC Edge** 系统不同，域用户帐户是在中央 AD 域服务器上管理的。

在为域帐户授予访问权限后，可使用“授予访问权”向导(在“用户与组”页上)查看、管理和排序可访问此系统的 AD 帐户。



先决条件：必须将 **ztC Edge** 系统添加到活动目录域，然后才能管理域帐户。(请参阅 [配置活动目录](#)。)如果未配置活动目录，或者如果已登录到此界面的用户没有管理员权限，则“授予访问权”按钮在“用户与组”页上变灰。

对于以下程序，打开 **ztC Edge- 授予访问权向导**：

1. 在左侧导航面板中，单击**首选项**，打开**首选项**页面。
2. 在管理工具下，选择**用户与组**。
3. 单击**授予访问权**。

授予域用户账户访问权

1. 在 **ztC Edge- 授予访问权向导** 中，在**搜索**菜单中指定搜索范围。
2. 键入要搜索的名称或组。允许使用部分名称和文本。
3. 单击**搜索**。
4. 单击绿色加号 (+)，其位于您要添加为该系统的 **ztC Console** 全局用户或组的用户或组旁边。
5. 使用“角色”列中的下拉菜单为您刚刚授予了访问权的用户或组分配一个角色。您可以分配以下角色：
 - **管理员** – 能够执行所有系统管理活动。
 - **平台管理员** – 启用除用户账户管理之外的管理员权限。

- **VM 管理员** –能够管理 VM(有关详细信息,请参阅[管理虚拟机](#))
- **只读** –启用读访问权,但没有管理功能。

6. 单击**完成**。“授予访问权”向导中将显示新的域用户。

删除域用户账户访问权

1. 在 **ztC Edge- 访问授权向导**中,单击要移除的用户或组旁边的复选框。
2. 单击**拒绝访问**,然后单击**完成**。

相关主题

[配置活动目录](#)

配置活动目录

为 ztC Edge系统配置活动目录来授权活动目录域中的原有用户或组使用自己的活动目录凭据登录到 ztC Console。

将 *ztC Edge* 系统添加到活动目录域后,可使用**授予访问权**向导将管理权限分配给域用户,从**用户与组**页启动此向导(请参见[配置“用户与组”](#))。

在活动目录域中添加 ztC Edge 系统

1. 单击左侧导航面板中的**首选项**,打开**首选项**页。
2. 单击**用户与组**。
3. 单击下方窗格中的**启用活动目录**按钮。
4. 在**活动目录域**旁边,输入要使用的域的名称。
5. 单击下列中的一个,以便阻止或允许“所有人”角色的自动分配:
 - **阻止自动为所有 AD 用户指定“所有人”角色(默认)**。
 - **允许所有 AD 用户进行身份验证,以及获得授权进行“所有人”角色访问**。
6. 单击**向活动目录中添加系统**。
7. 键入活动目录管理员的**用户名**和**密码**后才能把 ztC Edge 系统添加到该域。
8. 单击**添加**。
9. 在**用户和组**页面上按[管理域用户帐户](#)所述为域用户分配管理权限。

从活动目录域中删除一个 ztC Edge 系统

1. 在 ztC Console 中，单击左侧面板中的 **首选项**，打开 **首选项** 页。
2. 单击 **用户与组**。
3. 单击下方窗格中的 **从活动目录中移除系统**。
4. 输入为您提供域中的管理权限的 **用户名和密码**。
5. 单击 **移除**。

要禁用域身份验证时

1. 在 ztC Console 中，单击左侧面板中的 **首选项**，打开 **首选项** 页。
2. 单击 **用户与组**。
3. 单击下方窗格中的 **禁用活动目录**。



注意：禁用活动目录阻止使用 ztC Edge 系统管理员的授权域身份验证；不过，不需要从域中删除该系统。若要恢复使用域身份验证，单击 **启用活动目录**。不需要在 **用户和组** 页面上重新输入控制器名称或恢复域用户。

相关主题

[配置“用户与组”](#)

[管理域用户帐户](#)

[管理本地用户帐户](#)

[“首选项”页](#)

[ztC Console](#)

[安全性加强](#)

配置安全连接

为安全起见，默认情况下 ztC Edge 系统仅允许 HTTPS 连接。如果您要允许 HTTP 连接，可配置安全连接。



注意：

当您在以下程序中激活或取消激活仅启用 **HTTPS/禁用 HTTP** 旁的复选框，然后单击 **保存** 时，系统会自动使您退出 ztC Console，您必须再次登录。

当启用 HTTPS 连接时，您可以使用脚本在主机上安装自定义证书。请参阅[安装自定义证书](#)。

启用 HTTP 和 HTTPS 连接

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**管理工具**下，单击**安全连接**。
3. 取消激活**仅启用 HTTPS/禁用 HTTP**旁边的复选框。
4. 单击**保存**。

系统会自动使您退出 ztC Console，并将浏览器重定向到 HTTPS 登录页。要访问 HTTP 登录页，则在浏览器的地址栏中将 **https** 手动替换成 **http**，然后您便可登录。

如果系统仅允许 HTTP 和 HTTPS 连接，并且您想要允许 HTTPS 连接，则您需要激活此复选框。

仅启用 HTTPS 连接

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**管理工具**下，单击**安全连接**。
3. 激活**仅启用 HTTPS/禁用 HTTP**旁边的复选框。
4. 单击**保存**。

系统会自动使您退出 ztC Console，将浏览器重定向到 HTTPS 登录页，您必须再次登录。

安装自定义证书

要安装自定义证书，则使用 `certificate_installer` 脚本。通过使用此脚本，您可以安装自定义 SSL 证书，恢复先前使用的或内置证书，以及显示有关当前正在使用的或先前使用的证书的信息，如下所示：

- 安装自定义证书(非仅限 HTTPS 的模式)：

- i. 将证书复制到主机的 /tmp 文件夹。
- ii. 发出以下命令：

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

- 安装自定义证书(仅限 HTTPS 的模式)：

- i. 将证书复制到主机的 /tmp 文件夹。
- ii. 发出以下命令：

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

- 将自定义证书恢复到先前使用的证书:

```
certificate_installer recover -p
```

- 将自定义证书恢复到内置证书:

```
certificate_installer recover -b
```

- 列出有关当前使用的证书的信息:

```
certificate_installer list -c
```

- 列出有关先前使用的证书的信息:

```
certificate_installer list -p
```

如果您想要有关安装自定义证书的更多信息, 请访问知识库, 搜索文章在 *ztC Edge* 中将证书添加到 *ca-bundle.crt* (KB-9792)。请参阅[访问知识库文章](#)。

certificate_installer 脚本

使用

```
certificate_installer [command command_options] [script_options]
```

命令和命令选项

install <i>command_options</i>	<p>安装自定义证书。命令选项为：</p> <ul style="list-style-type: none"> • <code>-c, --cert=certificate_path</code>: 保存证书的路径。 • <code>-k, --key=private_key_path</code>: 保存密钥的路径。 • <code>-f, --[no-]force</code>: 强制替换正在使用的 SSL 证书。
recover <i>command_options</i>	<p>恢复自定义证书。命令选项为：</p> <ul style="list-style-type: none"> • <code>-b, --[no-]built-in(默认)</code>: 恢复到内置证书。 • <code>-p, --[no-]previous</code>: 恢复到先前使用的证书
list <i>command_options</i>	<p>列出自定义证书。命令选项为：</p> <ul style="list-style-type: none"> • <code>-a, --[no-]all(默认)</code>: 列出主机上的所有 SSL 证书。 • <code>-c, --[no-]current</code>: 列出当前使用的证书。 • <code>-p, --[no-]previous</code>: 列出先前使用的证书。 • <code>-L, --location=location</code>: 显示指定位置中证书的信息。

脚本选项

<code>-v, --[no_]verbose</code>	在详细模式下，此脚本显示所有信息。
<code>-l, --log=log_file</code>	将日志打印到文件 <i>log_file</i> ，而不是打印到 STDOUT。

相关主题

[ztC Console](#)

[“首选项”页](#)

[使用 ztC Console](#)

[安全性加强](#)

配置 VM 设备

将 VM 设备配置成禁止或允许在所有 VM 中插入虚拟 CD (VCD), 或者将 USB 设备附加到所有 VM。在默认情况下可插入和附加这些 VM 设备。使用**首选项**页上的**VM 设备配置**来更改配置。

当允许(默认)插入或附加 VM 设备时, 您可以在所有 VM 中插入 VCD, 或者将 USB 设备附加到 VM。当禁止插入或附加 VM 设备时, 您无法插入或附加这些设备。

要禁止插入或附加 VM 设备

1. 单击左侧导航面板中的**首选项**, 打开**首选项**页。
2. 在**首选项**页上, 单击**管理工具**下的**VM 设备配置**。
3. 激活下列一个或两个的复选框:
 - **禁止在所有 VM 上插入 CD**—激活此复选框可禁止在所有 VM 中插入 CD。
 - **禁止将 USB 设备附加到所有 VM**—激活此复选框可禁止将 USB 设备附加到 VM。
4. 单击**保存**。

要允许插入或附加 VM 设备

1. 单击左侧导航面板中的**首选项**, 打开**首选项**页。
2. 在**首选项**页上, 单击**管理工具**下的**VM 设备配置**。
3. 取消激活下列一个或两个的复选框:
 - **禁止在所有 VM 上插入 CD**—取消激活此复选框可允许在所有 VM 中插入 CD。
 - **禁止将 USB 设备附加到所有 VM**—取消激活此复选框可允许将 USB 设备附加到 VM。
4. 单击**保存**。

相关主题

[插入虚拟 CD](#)

[将USB设备附加到虚拟机](#)

[“首选项”页](#)

[使用ztC Console](#)

管理 IPtables

用于管理 IP 数据包过滤且支持 Linux 操作系统的管理工具称为 *iptables*。凭借 ztC Edge 系统，使用 *iptables* 的任务已得到简化。通过 **IPtables 安全性** 页，您可以设置、保持和检查各个过滤器表链及其基本规则。您可以访问三个主要链（**输入**、**输出** 和 **转发**），以便应用您需要的数据包过滤。凭借 ztC Edge 系统，这些规则被应用到每个物理机 (PM) 上的主机操作系统以及 IPv4 和 IPv6 数据包，并且在重启后这些规则仍持续使用。

在插入规则时，指定链（**输入**、**输出** 或 **转发**）和 **规则 ID**。当处理入站数据包时，内核应用与 **输入** 链关联的规则，当处理出站数据包时，内核应用与 **输出** 链关联的规则。当处理必须路由到其他主机的已接收入站数据包时，内核应用与 **转发** 链关联的规则。按照 **规则 ID** 的顺序应用规则。（**规则 ID** 类似于行 ID，其中例如 **规则 ID 1** 等于行 1。）但您可以加载针对这些规则的默认设置，而不是创建规则。

IPtables 安全性 页显示针对三个链中每一个的单独表，以及它们关联的规则。这些规则（如果对于特定链存在它们）按 **规则 ID** 排序。列显示网络名称、网络类型、协议和其他信息。如果需要，使用此页右侧的滚动条查看所有规则，以及使用底部的滚动条查看所有列。有关 *iptables* 功能的更多信息，请参阅 *iptables* 的 Linux 手册 (man) 页。

除主机外，您还可以选择使这些规则能够应用于客人操作系统。默认情况下，规则仅应用于主机操作系统，而不应用于客人操作系统。当您使规则也能够应用于客人时，所有现有规则、导入的规则和其他新插入的规则也能够应用于所有客人操作系统（即，针对基于已被分配给客人的同一业务网络的规则）。

注释：



1. 有关 ztC Edge 软件使用的端口的信息，请参阅 [系统要求概述](#)。
2. 有关 ztC Edge TCP 或 UDP 端口的其他信息，请访问知识库，搜索文章 [ztC Edge 使用的 TCP 和 UDP 端口 \(KB-2123\)](#)。请参阅 [访问知识库文章](#)。

要管理 IPtables，首先启用 IPtables 安全性（如果尚未启用）。

要启用 IPtables 安全性

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**首选项**页上，单击**IPtables 安全性**。
3. 激活**启用 IPtables 安全性**旁的复选框。

启用 IPtables 安全性窗口变为灰色并持续几分钟。当此窗口再次处于活动状态时，表明已选择了**启用 IPtables 安全性**

在默认情况下，规则仅应用于主机。但您可将规则应用于客人以及主机。

要将规则应用于客人以及主机。

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**首选项**页上，单击**IPtables 安全性**。
确保选择了**启用 IPtables 安全性**。
3. 默认选择**应用于主机**。

选择**应用于主机和客人**，以便将规则同时应用于主机操作系统和客人操作系统。**启用 IPtables 管理**窗口变为灰色并持续几分钟。

当选择了**应用于主机和客人**时，所有现有规则、导入的规则和其他新插入的规则也将应用于所有客人操作系统(即，针对基于已被分配给客人的同一业务网络的规则)。

在适当时，通过插入新规则，移除规则，加载默认设置，导入规则或导出规则，继续操作。

要插入一个新规则

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**首选项**页上，单击**IPtables 安全性**。
确保选择了**启用 IPtables 安全性**。
3. 单击**插入新规则**按钮，打开**插入新规则**弹出窗口。
4. 在**插入新规则**弹出窗口中，为下列项设置值：

- **链** – 从下拉列表中选择**输入**、**输出**或**转发**。
- **规则 ID** – 输入建立规则处理顺序的编号。输入一个值，从**1**开始，最高到最大值，即该链中规则的总数。每个**规则 ID**值都必须唯一。
如果您输入已经指定给某个规则的编号，则现有规则会增加**1**(后续规则也是如此，如果有)，您输入的编号被指定给新规则。因此，例如如果**规则 ID 1**已经

存在，而您对新规则输入了 **1**，则现有**规则 ID 1** 变为**规则 ID 2**，现有**规则 ID 2** (如果存在)变为**规则 ID 3**，以此类推。

- **共享网络** – 从所有可用共享网络的下拉列表中选择 一个网络。
- **协议** – 选择 **udp**、**tcp** 或 **全部**。

选择**全部**会导致**分组**和**端口号**字段变为非活动状态(灰色)，因为不必设置端口号范围。

- **目标** – 对于您要应用于符合规则规范的数据包的操作，选择**丢弃**、**接受**或**拒绝**。
- **端口号(开始)** – 对于范围的第一个端口，输入小于或等于**端口号(结束)**的数字 0 至 65535。
- **端口号(结束)** – 对于范围的最后一个端口，输入大于或等于**端口号(开始)**的数字 0 至 65535。
- **IP 地址(开始)** – 对于范围的第一个 IPv4 地址，输入小于或等于 **IP 地址(结束)**的地址 0.0.0.0 至 255.255.255.255。
- **IP 地址(结束)** – 对于范围的最后一个 IPv4 地址，输入大于或等于 **IP 地址(开始)**的地址 0.0.0.0 至 255.255.255.255。
- **IPv6 地址(开始)** – 对于范围的第一个 IPv6 地址，输入小于或等于 **IPv6 地址(结束)**的地址 0000:0000:0000:0000:0000:0000:0000:0000 至 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff。
- **IPv6 地址(结束)** – 对于范围的最后一个 IPv6 地址，输入大于或等于 **IPv6 地址(开始)**的地址 0000:0000:0000:0000:0000:0000:0000:0000 至 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff。

单击**插入**，插入此新规则。

5. 在默认情况下，新插入的规则仅应用于主机。如果您想要让这些规则应用于主机和客人，请参阅[要将规则应用于客人以及主机](#)。
6. 单击此页底部的**保存**，或者单击**重置**，取消任何未保存的更改，这会将规则恢复到上次保存的会话的规则。

保存了新规则后，**IPtables 安全性**页会在相应的链中显示它。

要移除规则

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**首选项**页上，单击**IPtables 安全性**。
确保选择了**启用 IPtables 安全性**。
(应用于主机和应用于主机和客人必须对移除规则没有影响。)
3. 选择您要移除的规则。
4. 对于您选择的规则，单击**移除**(位于最右列)。
5. 单击此页底部的**保存**，或者单击**重置**，取消任何未保存的更改，这会将规则恢复到上次保存的会话的规则。
移除了规则后，其从**IPtables 安全性**页消失。

要加载默认设置



小心：加载默认设置将覆盖当前设置。

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**首选项**页上，单击**IPtables 安全性**。
确保选择了**启用 IPtables 安全性**。
3. 单击此页底部的**加载默认设置**。
显示警告：*当前设置将被初始设置覆盖！*如果您要加载默认设置，则单击**确定**，或单击**取消**，取消加载默认设置。如果您单击**确定**，**启用端口管理**窗口变为灰色并持续几分钟，并且会显示**加载默认设置...**消息。
4. 在默认情况下，默认规则仅应用于主机。如果您想要让这些规则应用于主机和客人，请参阅[要将规则应用于客人以及主机](#)。。

要导入或导出规则

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**首选项**页上，单击**IPtables 安全性**。
确保选择了**启用 IPtables 安全性**。
3. 单击此页底部的**导入或导出**。

- **导入—显示导入/还原 IPtables 安全规则向导。**浏览到并选择您要导入的 XML 文件。在已导入的 XML 文件中，对于系统上具有相同类型的每个现有共享网络，都将生成与共享网络类型关联的所有规则。

已选择了 XML 文件后，将显示以下消息：

附加将保留当前规则集。如果您要清除所有当前规则，则选择覆盖。

单击相应按钮：

- **附加**—所选 XML 文件被附加到现有 XML 文件，从而保留现有规则。
- **覆盖**—所选 XML 文件覆盖现有 XML 文件，从而消除现有规则。

- **导出**—显示文件资源管理器窗口。浏览到您本地系统上要保存已导出规则的文件所在的位置。该表中的所有规则都被导出到一个 XML 文件，然后该文件被下载到您选择的位置。

4. 在默认情况下，导入的规则仅应用于主机。如果您想要让这些规则应用于主机和客人，请参阅[要将规则应用于客人以及主机。](#)。
5. 如果您导入了一个文件，则单击**保存**(或者单击**重置**，以便还原先前保存的值)。

相关主题

[“首选项”页](#)

[ztC Console](#)

[安全性加强](#)

配置登录横幅

您可以配置登录横幅，以便为 ztC Console 登录页面提供自定义内容。例如，您可以添加消息。

要配置登录横幅

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**管理工具**下，单击**登录横幅通知**。
3. 激活启用**登录横幅通知**框。将显示一个框。

在该框中，输入您要在控制台登录页面上显示的信息。例如，您可以键入公司名称或提供消息。

4. 单击**保存**(或者单击**重置**，以便还原先前保存的值)。

相关主题

[ztC Console](#)

[“首选项”页](#)

[使用 ztC Console](#)

启用 ztC Advisor

启用支持 ztC Edge 系统的 ztC Advisor，以便使管理员能够在 ztC Advisor 仪表板中远程监控系统的运行状况。

ztC Advisor 是一个基于 Web 的安全门户，其提供对您整个 ztC Edge 系统舰队的集中可见性。通过直观、用户友好的仪表板，您能够一目了然地评估每个系统的运行状况、资源使用情况和软件版本。有关注册和使用 ztC Advisor 的更多信息，请访问以下网页：<https://www.stratus.com/solutions/ztc-advisor>。



先决条件：ztC Edge 系统必须已向 Stratus 注册，并且具有 Internet 连接才能在 ztC Advisor 中进行监控。您可以随时启用 ztC Advisor，但仅在向 Stratus 注册了系统并连接到 Internet 后，仪表板中才会显示系统运行状况信息。

按照以下操作程序的描述启用 ztC Advisor 后，您可以登录 ztC Advisor 仪表板，然后在以下网页上查看您系统的状态：<https://ztcadvisor.stratus.com>。

要启动支持 ztC Edge 系统的 ztC Advisor

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**管理工具**下，单击**ztC Advisor**。
3. 激活启用 **ztC Advisor** 旁边的复选框。
4. 可选择为系统键入一个**别名**。

默认情况下，仪表板按每个系统的资产 ID 列出每个系统；但您还可以为系统分配一个别名，以提供一个更具描述性的名称，并使其更易于在过滤器和搜索中进行查找。别名的最大长度为 64 个字符，可包含字母、数字和特殊字符的任何组合。

5. 单击**保存**，保存设置并启用监控。

保存更改后，几分钟内 ztC Advisor 仪表板中将显示该系统。

相关主题

[ztC Console](#)

“首选项”页

使用 ztC Console

保存和还原系统首选项

在具有相应授权的 ztC Edge系统上，具有完全系统管理员权限的用户可通过创建还原文件(有时称为备份文件)来保存ztC Console首选项页的设置。您可以将此文件保存到本地计算机上的目标文件夹或云中的文件夹。然后，如果以后需要，您可选择此已保存的文件来将首选项设置还原到相同节点、更换节点，或者一个或多个其他节点。此功能可使您快速设置一个或多个系统。例如，如果您已经登录到您的系统具有还原文件的云帐户，则可通过单击来还原该节点的系统首选项设置。

注释：



- 每 ztC Edge系统您最多可将 50 个文件保存到云中。
- 要将文件保存到云或从云还原文件，系统必须具有 Internet 接入，并且您必须使用有效凭据登录云帐户。

系统必须具有相应的授权才能保存和还原首选项设置。最初安装系统时，将禁用此功能。首选项页的保存系统首选项和还原系统首选项窗口会显示一条消息，说明您需要激活此授权才能保存和还原首选项设置。您必须激活许可证才能使用此功能。

激活此授权

先决条件：您需要以下信息才能激活此授权：



- **名字和姓氏**
- **公司电子邮件**—提供拥有接收此授权的系统的公司电子邮件地址。不要提供个人电子邮件地址。
- **公司名称**—提供拥有接收此授权的系统的公司名称。
- **公司电话号码**—提供拥有接收此授权的系统的公司电话号码。不要提供个人电话号码。
- **资产 ID**—提供 Stratus 注册插页中的资产 ID。

如果您的系统有 Internet 接入，则继续执行以下第 1 步。如果您的系统没有 Internet 接入，则需要到有 Internet 接入的位置与 ztC Console(没有 Internet 接入)的位置之间移动授权文件。以下操作程序描述了使用 USB 闪存驱动器的一种方法，但也可使用其他方法。如果您正在使

用 USB 闪存驱动器，则在开始此操作程序前先获取它，然后将其插入正在运行 ztC Console 的远程管理 PC 的 USB 端口中。

1. 在左侧导航面板中，单击**首选项**，打开**首选项**页面。
2. 在**管理工具**下，单击**保存系统首选项**或**还原系统首选项**。
3. 该窗口会显示一条消息，说明您需要激活一个单独授权才能保存和还原**首选项**。
4. 阅读此消息。如果您的系统有 **Internet** 接入，则单击此链接，打开授权网页。



注意：如果您还需要注册该系统并获得针对该系统的永久授权，请参阅[注册系统并获取永久授权](#)。

如果您的系统没有 **Internet** 接入，则执行以下操作程序，打开授权网页。

在无 **Internet** 接入的系统上

- a. 单击此链接，打开授权网页，然后使用浏览器允许的任何方法复制此授权网页的 URL。
 - b. 将此 URL 粘贴到文本文件中，然后将该文本文件保存到 USB 闪存驱动器中。
 - c. 拔下该 USB 闪存驱动器，然后转到具有 **Internet** 接入的计算机。
 - d. 将该 USB 闪存驱动器插入计算机的 USB 端口中。
 - e. 导航到该文本文件，将其打开，然后复制此授权网页的 URL。
 - f. 打开浏览器，将此 URL 粘贴在浏览器地址栏中，然后访问该网页。
5. 在该网页上输入信息，然后单击**提交**。
 6. 当显示**下载授权**按钮时，单击该按钮。如果您的系统有 **Internet** 接入，则继续执行下一步。

如果系统没有 **Internet** 接入，则将下载的授权文件保存到 USB 闪存驱动器中，然后拔下该闪存驱动器。返回运行此控制台的远程管理计算机，然后插入该 USB 闪存驱动器。

7. 首先单击**首选项**页上的**产品授权**，然后将此授权上传到系统。然后在适用于您的系统时，执行下列一个操作程序：
 - 要自动将此授权上传到具有 **Internet** 接入的系统，则单击**首选项**页上的**产品授权**，然后对于**在线授权检查**，单击**立即检查授权**。新下载的授权将自动应用于系

统。

- 要将此授权手动上传到具有或无 Internet 接入的系统：
 - a. 单击**首选项**页上的**产品授权**。
 - b. 单击**离线授权检查和手动授权安装**栏，以显示其选项(如果尚未显示它们)。
 - c. 对于**将已激活的授权密钥安装到该系统**，单击**选择文件**，然后导航到您保存此授权文件的位置。
 - d. 选择该文件，单击**打开**，然后单击**上传**，将该文件上传到系统。

系统现在具有相应的授权来保存和还原**首选项**设置。

默认情况下，以下首选项设置包含在已保存的文件中：

所有者信息	VM 设备配置
软件更新	IPtables 安全性
IP 配置	登录横幅通知
仲裁服务器(仅限双节点系统)	ztC Advisor
日期与时间	电子警报
邮件服务器	SNMP 配置
用户与组	OPC 配置
安全连接	支持配置
	代理配置

保存系统首选项

1. 在左侧导航面板中，单击**首选项**，打开**首选项**页面。
2. 在**管理工具**下，单击**保存系统首选项**。
3. 在**保存系统首选项**下，选择下列一项：
 - **将系统首选项保存到该计算机上的文件**
 - **将系统首选项保存到云中的文件**—选择此选项时，当远程管理计算机(正在运行 ztC Console)连接到 Internet 时，将显示以下消息：

登录到 Stratus 客户服务门户网站，对您的帐户进行身份验证。

输入您 **Stratus** 客户服务帐户的用户名和密码。如果远程管理计算机未连接到 **Internet**，则登录字段不显示，而是显示一条消息，指示 **Internet** 连接不可用，您无法保存该文件。

登录云帐户后，云帐户将显示已登录用户的名称和当前存储在云中的文件数。每系统您最多可将 **50** 个文件保存到云中。如果保存了 **50** 个文件，您将无法保存其他文件。您无法删除文件，因此关于删除文件，您必须联系您的 **Stratus** 服务代表。

只要您的控制台会话处于活动状态，云帐户登录会话就会打开；如果您关闭控制台会话或该会话因不活动而超时，则会将您自动注销。

4. 必要时将信息输入到以下字段：

- **文件名**—此字段显示 **ztC_Asset_ID_preferences_yyyy-mm-dd-hh-mm.zip** 格式的默认文件名。在保存了此文件后，必要时您可以修改默认名称。
- **描述**—输入描述(可选)。
- **关键字**—默认显示关键字 **system_ID**。您可以更改默认关键字并添加其他关键字，总共三个关键字。

5. 单击下列一个按钮：

- **保存**—该文件将使用默认文件名进行保存，或者必要时您需要修改文件名。
如果您正在将文件保存到本地计算机，则使用默认位置，或者导航到其他位置。(在浏览器中设置默认位置。)
如果您正在将文件保存到云，并且已成功确认了用户名和密码，则将在用户的云帐户中创建此文件并将其保存在名为 **Asset_ID** 的文件夹中。
- **清除**—清除**描述**和**标记**字段。此外，如果您正在将文件保存到云，则文件名将被重置为默认名称，并且将清除用户名和密码。

在保存成功后，将显示消息**系统首选项已保存**。

在您保存了系统首选项的设置，并且想要将这些设置还原到同一系统或其他系统后，您首先应熟悉有关此还原操作的注意事项、先决条件和注释，从而做好准备。

准备还原系统首选项

在还原已保存系统首选项文件前，您应了解以下注意事项、先决条件和注释。

小心：如果已还原系统首选项更改了以下任何设置，则该系统与 ztC Console的连接将中断：



- IP 配置
- 安全连接(如果您在启用了 HTTP 时登录，并且还原文件禁用了 HTTP)
- 日期与时间

此连接中断时，还原操作会继续在后台运行，但您无法查看其进度或状态。如果失去连接，则重新登录。(有关设置 IP 配置的信息，请参阅[配置 IP 设置](#)。有关设置安全连接的信息，请参阅[配置安全连接](#)。有关设置日期和时间的信息，请参阅[配置日期和时间](#)。)

先决条件：



- 活动目录 (AD) 设置：如果还原的首选项启用了 AD，您必须在登录时提供 AD 凭据。有关启用 AD 的信息，请参阅[配置活动目录](#)。
- 仲裁服务器设置：
 - 还原了已启用状态。
 - 任何 VM 都不应使用现有仲裁服务器；在还原首选项前，应关闭所有正在使用的 VM 的电源。如果在还原操作过程中有任何虚拟机正在使用仲裁服务器，则**仲裁服务器**的还原将失败。
 - 未将此设置还原到单节点系统。

有关启用仲裁服务器的信息，请参阅[配置仲裁服务器](#)。

注释:还原系统首选项前,请考虑以下信息:

- 您将首选项还原到的系统与您正在使用其已保存首选项文件的系统必须在以下方面保持相同:
 - 相同的硬件型号-您将首选项还原到的系统必须与您正在还原其已保存首选项文件的系统具有相同的硬件型号。
 - 相同的双节点或单节点配置-您只能将保存在双节点系统上的首选项还原到双节点系统。您只能将保存在单节点系统上的首选项还原到单节点系统。
- 如果您在运行比原始备份更早或更晚的版本的系统上还原系统首选项,则只能还原更早版本中支持的首选项。
- **IPtables 安全性**-要还原 IPtables 设置,您必须选择**附加**(将还原文件设置附加到现有规则集)或**覆盖**(使用还原文件设置覆盖现有规则集)。(有关 IPtables 的信息,请参阅[管理 IPtables](#)。)
- **IP 配置**-选择时,将还原所有网络配置数据。(有关信息,请参阅[配置 IP 设置](#)。)
- **日期与时间**-仅还原**自动**设置。在还原**手动**设置以及具有不同时区和多个 NTP 服务器的设置时,物理机将关闭电源,并且还原的日期和时间设置在系统重启后生效。(有关信息,请参阅[配置日期和时间](#)。)
- 对于**用户与组**,请考虑以下方面:
 - 您必须提供 AD 凭据才能还原**用户与组**设置。
 - 如果当前系统上和还原文件中存在用户帐户,则当前系统会认为要编辑该用户帐户。
 - 如果还原文件中存在用户帐户,但当前系统上不存在该用户帐户,则当前系统将认为要添加该用户帐户。
 - 在以下情况下,当前系统会跳过还原文件中的 AD 条目:
 - 如果在还原时为当前系统配置的 AD 中缺少还原文件中的 AD 条目。
 - 如果还原文件中 AD 条目的用户类型与还原时为当前系统配置的 AD 条目的用户类型不匹配。





(有关用户与组的信息, 请参阅配置“用户与组”页面。)

熟悉有关还原操作的注意事项、先决条件、和注释后, 您可以还原系统首选项。

还原系统首选项

1. 在左侧导航面板中, 单击**首选项**, 打开**首选项**页面。
2. 在**管理工具**下, 单击**还原系统首选项**。
3. 在**还原系统首选项**下, 选择下列一项:
 - 从该计算机上保存的文件还原系统首选项:
 - a. 单击**选择文件**可显示默认保存目录中的文件列表, 包括已保存的 zip 文件。必要时, 导航到其他目录。
 - b. 滚动选择具有您要还原的**首选项设置**的文件, 然后单击该文件名。将显示下表:

正在从以下还原系统首选项:

文件名	ztC_Asset_ID_preferences_yyyy-mm-dd-hh-mm-ss.zip
软件版本	version_number
描述	description
关键字	keywords

如果还原的**首选项**包括“用户与组”, 则还将显示以下信息:

活动目录凭据	您需要活动目录凭据才能还原 用户与组 设置。
--------	-------------------------------

要还原所选文件中的设置, 则单击**下一步**。

- 从云中保存的文件还原系统首选项—在选择该选项时, 当远程管理计算机连接到 Internet 时, 将显示登录到 *Stratus* 客户门户以验证您的帐户, 同时显示用户名和密码框(如果您尚未登录到您的帐户)。如果远程管理计算机未连接到 Internet, 则会出现一条消息, 指示 Internet 连接不可用。(登录到云帐户后, 只要您的控制台会话处于活动状态, 该会话就会打开;如果您关闭控制台会话或该

会话因不活动而超时，则会将您自动注销。)

输入您 **Stratus** 客户服务帐户的用户名和密码，然后单击 **登录**。

连接成功后，将显示下表，从而列出一个或多个文件，最多列出已保存文件的总数：

选择资产 ID 搜索 ID	选择从哪个文件还原系统首选项	
资产 ID	文件名	已创建
<i>asset_ID</i>	<i>filename</i>	<i>time</i>

资产 ID 显示 *asset_ID* 文件夹的列表。**文件名** 列列出 *asset_ID* 文件夹中的文件，以及保存文件的时间，如**时间**列中所显示的。此外，显示正在从以下还原系统首选项：表。

在**资产 ID**下，首先列出当前系统的 ID，而在**文件名**下，首先列出其还原文件（如果存在）。在这种情况下，单击顶部文件名可将**首选项**设置还原到当前系统。

要搜索某个文件，则在**搜索 ID**框中输入其文件名。

要选择某个文件，则单击所需的**资产 ID**，然后单击所需的**文件名**。单击**下一步**，从所选文件还原**首选项**设置。

4. 将显示**选择要还原的系统首选项**：窗口，以及首选项列表。

默认情况下，还原以下首选项设置：

所有者信息	ztC Advisor
软件更新	电子警报
仲裁服务器(仅限双节点系统)	SNMP 配置
邮件服务器	OPC 配置
VM 设备配置	支持配置
登录横幅通知	代理配置

注意：

默认情况下不选择以下首选项，因为该首选项会导致显示弹出消息或导致系统重启：



- **日期与时间**—如果这些设置更改，则系统会重启。
- **用户与组**—如果启用了活动目录 (AD)，则会显示一个用于提供 AD 凭据的窗口。
- **安全连接**—如果您使用 HTTP 登录，并且还原文件禁用 HTTP，则与该系统的连接将中断，您必须再次登录。
- **iptables 安全性**—显示一个窗口，询问您想要覆盖当前规则集还是将还原的规则附加到当前规则集。
- **IP 配置**—如果 IP 配置更改，则与该系统的连接将中断，您必须再次登录。

取消选择您不想还原的任何首选项的复选框。选择任何额外首选项(如果尚未选择)。

5. 单击**还原**，使系统还原所选的首选项，或者单击**返回**，返回上一个窗口。单击**还原**后，您无法取消此过程。完成此还原操作将需要约一分钟。在还原操作过程中，您无法导航到ztC Console窗口中的其他屏幕。您必须等待还原操作完成才能显示其他控制台窗口。

还原状态列将还原状态列为**正在进行**、**已完成**、**部分完成**或**失败**。当还原操作完成时，将显示以下消息：

完成！以上显示的首选项已成功还原。

6. 单击**完成**。此时将再次显示初始**还原系统首选项**屏幕。

相关主题

[ztC Console](#)

[“首选项”页](#)

[使用ztC Console](#)

配置电子警报

将电子邮件警报(电子警报)配置成只要系统检测到需要管理员关注的事件，ztC Edge系统便会向系统管理员发送电子邮件。



先决条件: 为使电子警报正常运行,您必须配置邮件服务器。请参阅[配置邮件服务器](#)。

要启用电子警报

1. 单击左侧导航面板中的**首选项**,打开**首选项**页。
2. 在**通知**下,单击**电子警报**。
3. 单击**启用电子警报**框。此时将显示用于指定或选择以下设置的框:
 - **电子警报语言**—从下拉菜单中选择一种语言。
 - **接收者列表(必填)**—输入所有电子警报接收者的电子邮件地址。
4. 单击**保存**(或者单击**重置**,以便还原先前保存的值)。



注意: 当您启用或更新电子警报配置时,生成一个测试警报,以确认您能够收到这些警报。

要生成测试警报

单击**生成测试警报**。Stratus Redundant Linux软件会生成一个测试警报,以及向所有电子邮件接收者发送主题为“测试警报”的示例电子邮件:**SNMP**向**SNMP**自陷的接收者发送自陷(如果配置)(请参阅[配置 SNMP 设置](#);“支持配置”向您的授权**Stratus**服务代表发送通知(如果配置)(请参阅[配置远程支持设置](#))。查看“警报历史记录”日志(请参阅[“警报历史记录”](#)页),了解传送状态。

您还可以通过以下方式测试电子警报:使从物理机进入维护模式(请参阅[维护模式](#)),然后使其退出维护模式。验证对于这两个维护模式事件您是否都收到了电子警报。

相关主题

[ztC Console](#)

[“首选项”](#)页

[使用 ztC Console](#)

配置 SNMP 设置

为ztC Edge系统配置简单网络管理协议(SNMP)设置来使SNMP管理应用程序能够远程监控您的系统。(SNMP信息仅与系统有关,而与个别PM无关。)您可以启用SNMP请求和SNMP自陷:

- **SNMP 请求** - 发送到系统的请求，用以检索 Stratus Redundant Linux 软件支持的管理信息库 (MIB) 中列出的对象的值。这些 MIB 包含作为 ztC Edge 系统描述对象的集合的系统特定 MIB。要下载 MIB 文件的副本，请访问以下项目的 **驱动程序和工具** 部分：此 **下载** 页面在 <https://www.stratus.com/services-support/downloads/?tab=ztcedge>。
- **SNMP 自陷** - 在某一事件 (如警报) 后，ztC Edge 系统中的一个节点启动然后发送到已识别接收者列表 (通常是一个网络管理站 (NMS)) 的消息。

执行相应的程序启用 SNMP 请求或自陷。

要启用 SNMP 请求时

要启用 SNMP 请求，则执行以下操作之一：

- 从 **首选项** 页面启用 SNMP 请求：
 - 添加能够启用 SNMPv3 请求的 SNMPv3 用户，以及对 ztC Edge 系统中的全部 MIB 具有只读访问权限的用户。
 - 在您不允许用户 (**受限制**) 或允许使用默认公共社区的任何用户 (**不受限**) 发送请求的情况下，配置对 SNMPv1 和 SNMPv2 请求的访问控制。
- 通过编辑 snmpd.conf 文件来自定义 SNMP 请求功能。您可以自定义对 SNMPv1 请求和 SNMPv2 请求的访问控制。您还可以自定义可发出 SNMPv3 请求的用户列表。有关信息，请参阅 [自定义 SNMP 请求功能](#) (下文)。

要从“首选项”页面启用 SNMP 请求

1. 单击左侧导航面板中的 **首选项**，打开 **首选项** 页。
2. 在 **通知** 下，单击 **SNMP 配置**。
3. 激活 **启用 SNMP 请求** 旁边的复选框。
4. 将显示 **SNMP 请求的用户列表 (版本 3)**。

如果用户名列表显示在 **SNMP 请求的用户列表 (版本 3)** 下，则会显示用户的安全级别，并且还会显示 snmpd.conf 文件的只读显示。该用户对全部 MIB 具有只读访问权限。注意，系统仅支持一个 **SNMP 请求 (版本 3)** 用户。

如果未显示用户名，您可以添加 SNMPv3 用户。

要添加 SNMPv3 用户

- a. 单击  **添加** 按钮，这会打开 **添加用户** 向导。
- b. 输入以下字段的值：

用户名—对于 SNMPv3 代理具有访问权限的用户的名称。此名称必须是唯一的。

安全级别—用户的安全级别。有效值为：

- **无身份验证且无隐私**：没有对消息应用安全；消息未进行身份验证或加密。
- **身份验证和隐私**：消息进行了身份验证，但未加密。您必须为**身份验证类型**和**身份验证密码**输入值。
- **身份验证和隐私**：消息进行了身份验证和加密。您必须输入**身份验证类型**、**身份验证密码**、**加密类型**和**加密密码**。

当安全级别包括身份验证或隐私时，将显示以下字段：

身份验证类型—用户的身份验证类型。有效值为：

- **MD5**：将消息摘要算法 (MD5) 配置为用户的身份验证类型。
- **SHA**：将安全哈希算法 (SHA) 配置为用户的身份验证类型。

身份验证密码—用户所需的密码，其用于生成身份验证密钥。密码必须至少为八个字符。

加密类型—用户的加密类型。有效值为：

- **AES**：将高级加密标准 (AES) 配置为用户的加密类型。
- **DES**：将数据加密标准 (DES) 配置为用户的加密类型。

加密密码—用户所需的密码，其用于生成加密密钥。密码必须至少为八个字符。

c. 单击**保存**，保存更改。

1. 选择一个访问选项：

受限 (默认)—不允许用户发送 SNMPv1 请求和 SNMPv2 请求。

不受限—许使用默认公共社区的任何用户发送 SNMPv1 请求和 SNMPv2 请求。

自定义(当用户手动编辑 `snmpd.conf` 时可用；请参阅以下 [自定义 SNMP 请求功能](#))—允许自定义访问。

2. 单击**保存**(或者单击**重置**，以便还原先前保存的值)。

通过编辑 `snmpd.conf` 文件来自定义 SNMP 请求功能

通过编辑 `snmpd.conf` 文件来自定义 SNMP 请求功能。

通过编辑 `/etc/snmp/snmpd.conf` 文件来自定义对 **SNMPv1** 请求和 **SNMPv2** 请求的访问控制：

1. 登录主机。
2. 手动编辑两个节点上的标准 `/etc/snmp/snmpd.conf` 文件。
3. 保存文件。
4. 通过输入命令 **systemctl restart snmpd** 在每个节点上重新启动 `snmpd` 进程。

通过编辑 `/etc/snmp/snmpd.conf` 和 `/var/lib/net-snmp/snmpd.conf` 文件来自定义可发出 **SNMPv3** 请求的用户列表。

1. 登录主机。
2. 手动编辑两个节点上的标准 `/etc/snmp/snmpd.conf` 文件。
3. 手动编辑两个节点上的标准 `/var/lib/net-snmp/snmpd.conf` 文件。
4. 保存文件。
5. 通过输入命令 **systemctl restart snmpd** 在每个节点上重新启动 `snmpd` 进程。

要启用 **SNMP** 自陷时

注释：



1. 为 **SNMP 自陷 (版本3)** 添加收件人时，您需要确认收件人服务器上自陷用户的引擎 ID 为 `0x80001370017F000001`。
2. 在启用或修改 **SNMP 自陷** 设置时，将生成一条测试警报来确认已收到自陷。

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**通知**下，单击**SNMP 配置**。
3. 激活启用 **SNMP 自陷** 旁边的复选框。
4. 输入 **SNMP 社区** 的名称，或者保留缺省值(**公共**)。
5. **SNMP 自陷的收件人列表(版本 3)** 下面是自陷用户列表，以及自陷用户所在的收件人服务器的 IP 地址。ztC Edge 系统将 **SNMPv3** 自陷发送到收件人服务器上的自陷用户。必要时，添加一个收件人。

要添加一个收件人

a. 单击  添加按钮，这会打开添加一个收件人向导。

b. 输入以下字段的值：

收件人地址—收件人服务器的主机名或 IPv4 地址。

用户名—收件人服务器上自陷用户的名称。该名称在对于收件人是唯一的。

安全级别—用户的安全级别。有效值为：

- **无身份验证且无隐私**：没有对消息应用安全；消息未进行身份验证或加密。
- **身份验证和隐私**：消息进行了身份验证，但未加密。您必须为**身份验证类型**和**身份验证密码**输入值。
- **身份验证和隐私**：消息进行了身份验证和加密。您必须输入**身份验证类型**、**身份验证密码**、**加密类型**和**加密密码**。

当安全级别包括身份验证或隐私时，将显示以下字段：

身份验证类型—用户的身份验证类型。有效值为：

- **MD5**：将消息摘要算法 (MD5) 配置为用户的身份验证类型。
- **SHA**：将安全哈希算法 (SHA) 配置为用户的身份验证类型。

身份验证密码—用户所需的密码，其用于生成身份验证密钥。密码必须至少为八个字符。

加密类型—用户的加密类型。有效值为：

- **AES**：将高级加密标准 (AES) 配置为用户的加密类型。
- **DES**：将数据加密标准 (DES) 配置为用户的加密类型。

加密密码—用户所需的密码，其用于生成加密密钥。密码必须至少为八个字符。

c. 单击**保存**，保存更改。

6. 单击**保存**(或者单击**重置**，以便还原先前保存的值)。

7. 将您组织的防火墙配置成允许 SNMP 操作，这可使 SNMP 管理系统接收来自 ztC Edge 系统的警报，以及向该系统发送自陷。要执行此操作，则将您组织的防火墙配置成打

开 SNMP 端口：

消息类型：SNMP

协议：SNMP

端口：161(Get/Walk) 162(Traps)

8. 通过单击**生成测试警报**，生成测试警报。

Stratus Redundant Linux软件会生成一个测试警报，并且 SNMP 向 SNMP 自陷的接收者发送自陷；电子警报向电子警报的所有电子邮件接收者发送主题为“测试警报”的示例电子邮件(如果配置)(请参阅[配置电子警报](#)；“支持配置”向您的授权 Stratus 服务代表发送通知(如果配置)(请参阅[配置远程支持设置](#))。查看“警报历史记录”日志(请参阅[“警报历史记录”页](#))，了解传送状态。

相关主题

[SNMP](#)

[ztC Console](#)

[“首选项”页](#)

[使用 ztC Console](#)

[安全性加强](#)

配置 OPC 设置

配置开放式平台通信 (OPC) 设置，以便启用 OPC 服务器功能，该功能发布可使 OPC 客户端接收和显示的 ztC Edge 系统性能数据。这可使您将 ztC Edge 系统与其他工业设备一同进行监控。

为使用 OPC 功能，您必须在单独计算机上安装(您选择的)OPC 客户端软件，然后配置此 OPC 客户端(请参阅[安装和配置 OPC 客户端](#))。必须配置 OPC 客户端，使其为从您要为 OPC 配置的 ztC Edge 系统上的端口接收数据。默认端口为 **4840**，但您可以指定其他端口号。

配置 OPC 设置

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**通知**下，单击**OPC 配置**。
3. 激活启用**OPC 服务器**旁边的复选框。
4. 默认端口号为 **4840**。必要时，指定其他端口号。
5. 在适用于您的系统时，激活下列任何一个或两个复选框：

允许匿名 OPC 客户端连接—在连接到 ztC Edge 系统上的 OPC 服务器时，OPC 客户端不需要提供用户名和密码。(当未激活该复选框时，OPC 客户端必须提供用户名和密码。)

允许使用从用户与组配置的用户名和密码进行 OPC 客户端连接—OPC 客户端能够使用在登录 ztC Edge 时使用的用户名和密码连接到 ztC Console 系统上的 OPC 服务器。(当未激活该复选框时，OPC 客户端无法使用本地用户帐户用户名和密码登录 OPC 服务器，如**用户与组**页面上所指定的。请参阅[管理本地用户帐户](#)。)

6. 单击**保存**(或者单击**重置**，以便还原先前保存的值)。

安装和配置 OPC 客户端

您必须在单独计算机上安装 OPC 客户端软件并配置 OPC 客户端。您可以从市场中存在的许多版本中选择 OPC 客户端软件。以下操作程序描述如何使用 Unified Automation 提供的 UaExpert[®] 软件安装和配置 OPC 客户端。

使用 UaExpert 软件安装和配置 OPC 客户端



注意：除阅读以下操作程序外，还要遵循 UaExpert 软件随附的说明。

1. 下载并安装 Windows 版本的 UaExpert 软件。请参阅 <https://www.unified-automation.com/products/development-tools/uaexpert.html>。
2. 如果首次启动 UaExpert 软件，则按照该软件随附的说明进行初始启动。
3. 运行 UaExpert 软件。

将打开 **Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject** 主窗口。

4. 在菜单栏中，单击**服务器**，然后选择**添加**。将显示**添加服务器**对话框。
5. 单击**高级**选项卡。
6. 在**端点 Url**框中，输入端点的 URL，即 ztC Edge 系统的群集 IP 地址(例如，**opc.tcp://tcp_cluster_ip_address:4840/**)。
7. 对于**安全设置**，对**安全策略**和**消息安全模式**均选择**无**。
8. 对于**身份验证设置**，根据您的配置要求选择下列之一：

匿名—如果您激活了允许匿名 OPC 客户端连接复选框，则选择此选项。

用户名和密码—如果您激活了允许使用用户名和密码进行 OPC 客户端连接的复选框，则输入值。您输入的用户名和密码必须与在 ztC Edge 系统上为使只读用户获得

OPC 访问权而添加的用户名和密码相同。有关将用户添加到 ztC Edge系统的信息，请参阅[管理本地用户帐户](#)。

9. 单击**确定**，关闭**添加服务器**对话框。

将重新显示主窗口。在左侧面板中，服务器的名称显示在**服务器**下的**项目**框中。

10. 选择新服务器，然后单击连接按钮，该按钮显示在减号图标右侧的工具栏中。

当客户端成功连接到服务器时，主窗口的**地址空间**框将显示服务器的端点。

在**地址空间**框中，您可以单击顶层以展开并浏览可用的数据值。在**属性**框中，**值**列显示所选选项的当前值。

相关主题

[显示 OPC 输出](#)

[ztC Console](#)

[“首选项”页](#)

[使用 ztC Console](#)

显示 OPC 输出

在 ztC Edge系统上启用 OPC 服务器功能后，OPC 客户端(在非 ztC Edge 系统的计算机上)可发布系统的性能数据。这些数据被划分为地址空间，其中每个地址空间均被划分为包含多个数据项的子对象。ztC Edge系统上的 OPC 服务器功能将这些数据项的值传递到 OPC 客户端，然后 OPC 客户端会显示这些数据。

本主题描述如何使用通过 Unified Automation 的 UaExpert[®] 软件创建的 OPC 客户端显示 ztC Edge 系统信息。

要显示 OPC 输出

1. 在已创建 OPC 客户端的计算机上，打开此客户端。
2. 在(左侧)项目面板中，单击**项目**、**服务器**，然后单击**ztC OPC 服务器**。

项目下方的左侧面板为**地址空间**。选择了**ztC OPC 服务器**后，**地址空间**面板会显示**根**层级结构。

3. 在**地址空间**面板中，单击**根**下方的**对象**。在**对象**下方，您可以选择**服务器**和**ztC**。

■ 服务器

有关当前正在运行 OPC 服务器的节点的信息，请查看 **BuildInfo** 子对象：单击 **服务器**，然后单击 **ServerStatus**。

BuildInfo 子对象显示以下数据项的值：

数据项	描述
ProductUrl	显示 http://www.stratus.com/ 。
ManufacturerName	显示 Stratus Technologies Ireland, Ltd.
ProductName	显示此硬件的产品名称 (ztC Edge)。
SoftwareVersion	显示 Stratus Redundant Linux 软件的版本号。
BuildNumber	显示 Stratus Redundant Linux 软件的内部版本号。
BuildDate	显示 Stratus Redundant Linux 软件的构建日期。

有关 **服务器** 对象的其他信息，请参阅 *OPC 统一架构规范的第 5 部分：信息模型*，该规范可在 opcfoundation.org 上获得。

- **ztC-ztC** 对象将地址空间划分为以下子对象，每个表中均列出了这些数据项：

应用程序

应用程序数据项提供有关应用程序运行状况的信息。

数据项	描述
AlertedApplicationsCount	在 AlertedApplicationsList 中列出应用程序的数量。 数据类型： UInt32 。
AlertedApplicationsList	列出当前监视的应用程序，这些应用程序具有非正常或不可用的任何状态(未运行、无响应、不可用和未找到)。此列表包含具有已停止的 VM 的应用程序。此列表不包含未激

数据项	描述
	<p>活的监视器(即,在未激活启用框的情况下,监视器选项卡的应用程序面板中所列的应用程序监视器)。</p> <p>数据类型:字符串的动态数组。</p>
AllApplicationsHealthy	<p>指示被监视的应用程序是否有警告:true指示没有警告;false指示一个或多个被监视的应用程序有警告。</p> <p>数据类型:布尔。</p>
ApplicationMonitoringEnabled	<p>指示应用程序监视是否已被授权并已打开:true指示已打开;false指示未打开。</p> <p>数据类型:布尔。</p>
ApplicationsCount	<p>指示当前被监视的应用程序数量。其值应等于 ApplicationsList 中的应用程序数量。</p> <p>数据类型:UInt32。</p>
ApplicationsList	<p>列出当前被监视的应用程序。这是一维数组,其随着被监视应用程序的添加或删除而增加或减少。此列表不包含未激活的监视器(即,在未激活启用框的情况下,监视器选项卡的应用程序面板中所列的应用程序监视器)。列出的名称包含 VM 名称作为应用程序名称的前缀(例如 vm1/testapp.exe)。</p> <p>数据类型:字符串的动态数组。</p>

物理机

物理机的数据项提供有关系统中单个节点是否正常的信息。

数据项	描述
AllPhysicalMachinesHealthy	<p>指示两个节点是否都正常：<i>true</i> 指示两个节点均存在，已绿色选中了“正在运行”，并且任何一个均未处于维护模式下；<i>false</i> 指示一个节点(或两个节点都)不存在，已绿色选中了“未运行”，以及/或者处于维护模式下。</p> <p>数据类型：布尔。</p>
Node0 和 Node1	<p>NodenHostState: 主机状态。有效值包括被逐出、失败、固件、正在映射、丢失、<i>nfc</i>、关闭、原型、正在运行、正在启动、正在停止、未许可和不可及。</p>
	<p>NodenIPAddress: 节点 IP 地址。</p>
	<p>NodenMaintenanceMode: 主机维护模式。有效值包括正在撤出、维护和正常。</p>
	<p>NodenExists: 指示系统是否知道此节点，其中 <i>true</i> 指示此节点已成功加入系统；<i>false</i> 指示未将第二个节点添加到系统，或者已添加了第二个节点，后来又将其移除。如果值为 <i>false</i>，则忽略其他所有 <i>noden</i> 信息。</p>
	<p>NodenVirtualMachineList: 列出正在此节点上运行的虚拟机 (VM)。</p>
	<p>NodenCombinedState: 指示 NodenMaintenanceMode、NodenExists 和 NodenHostState 的组合，如下：</p> <ul style="list-style-type: none"> ◦ 当 NodenExists 为 <i>false</i> 时，

数据项	描述
	<p><code>NodenCombinedState</code> 为丢失。</p> <ul style="list-style-type: none"> 当 <code>NodenExists</code> 为 <code>true</code> 时，<code>NodenCombinedState</code> 为正在撤出或维护，<code>NodenHostState</code> 为正在运行，<code>NodenMaintenanceMode</code> 为正在撤出或维护。 当 <code>NodenCombinedState</code> 为其他任何值时，其指示 <code>NodenHostState</code> 的值，上方列出了 <code>NodenHostState</code> 值的范围。
<code>PhysicalMachinesList</code>	<p>列出存在的节点。</p> <p>数据类型：字符串的动态数组。</p>
<code>PhysicalMachinesWarningCount</code>	<p>列出未绿色选中的物理机数量。</p> <p>数据类型：UInt32。</p>
<code>PhysicalMachinesWarningList</code>	<p>列出正在报告问题的物理机。该列表一般同时包含这两个节点；例如，当辅助节点处于维护模式时，主节点被标记为拉取不安全。</p> <p>数据类型：字符串的动态数组。</p>
<code>PrimaryPhysicalMachine</code>	<p>显示当前主节点的名称。</p> <p>数据类型：字符串。</p>

虚拟机

虚拟机的数据项提供有关系统上运行的 VM 状态的信息。

数据项	描述
AllVirtualMachinesHealthy	指示任何虚拟机具有警告状态还是故障状态： <i>true</i> 指示所有 VM 均已绿色选中； <i>false</i> 指示一个或多个 VM 为已绿色选中“未运行”。 数据类型：布尔。
FTVirtualMachinesList	显示系统上存在的 FT VM 的名称。 数据类型：字符串的动态数组。
GetPhysicalMachine	指示物理机正在运行指定的 VM。 数据类型：接受一个字符串并返回一个字符串的函数(该函数的输入参数是一个作为 VM 名称的字符串，而输出是一个字符串 (node0 或 node1)，其表示当前正在运行输入参数中命名的 VM 的物理机)。
HAVirtualMachinesList	显示系统上存在的 HA VM 的名称。 数据类型：字符串的动态数组。
RunningVirtualMachinesCount	列出 RunningVirtualMachinesList 中的 VM 数。 数据类型：UInt32。
RunningVirtualMachinesList	列出被标记为正在运行的 VM 的名称。 数据类型：字符串的动态数组。
StoppedVirtualMachinesCount	列出 StoppedVirtualMachinesList 中的 VM 数。 数据类型：UInt32。
StoppedVirtualMachinesList	列出被标记为已停止的 VM 的名称(忽略转换状态，例如正在启动)。 数据类型：字符串的动态数组。

数据项	描述
VirtualMachinesCount	列出系统上存在的 VM 数。 数据类型: UInt32。
VirtualMachinesList	列出系统上存在的 VM 的名称。 数据类型: 字符串的动态数组。

系统

系统的数据项提供高级状态信息以及有关整个系统访问方法的信息。

数据项	描述
ManagementConnectionGood	指示 OPC 服务器是否可从 ztC Edge 系统检索信息: <i>true</i> 指示该服务器可从该系统检索信息; <i>false</i> 指示服务器无法检索信息。 数据类型: 布尔。
ManagementIP	指示 ztC Edge 系统的 IP 地址。 数据类型: 字符串。
ManagementURL	指示 ztC Console 的 HTTP URL。 数据类型: 字符串。
OutstandingSeverity	与登录页上的整体系统状态图标相对应。 数据类型: 字符串。
SecureManagementURL	指示 ztC Console 的 HTTPS URL。 数据类型: 字符串。

相关主题

[配置 OPC 设置](#)

配置远程支持设置

当您首次登录 ztC Edge 系统时，配置在事件需要关注时可使 ztC Edge 系统向您的授权 Stratus 服务代表发送支持通知的支持配置设置。

要配置支持配置设置



注意：当您启用或修改启用**远程支持访问**或**启用通知**的设置时，将生成测试警报，以确认您的授权 Stratus 服务代表能够收到从您系统发出的系统运行状况消息。

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**远程支持**下，单击**支持配置**。
3. 在适合您系统时，修改这些设置：
 - **启用远程支持访问**可使您的授权 Stratus 服务代表远程连接到 ztC Edge 系统，以进行故障排除。注意，您可以启用该设置，然后在需要时禁用该设置。
 - **启用通知**可使 ztC Edge 系统向您的授权 Stratus 服务代表发送运行状况和状态通知。
 - **启用支持通知**可针对需要关注的任何事件发送警报。它还向您的授权 Stratus 服务代表发送定期“心跳”自动通报消息。
 - **启用定期报告**可发送每天的系统信息摘要，以帮助改进产品和服务质量。
4. 单击**保存**（或者单击**重置**，以便还原先前保存的值）。
5. 将您组织的防火墙配置成允许支持消息。

要将您的防火墙配置成允许支持消息

使用以下信息将您组织的防火墙配置成允许与您的授权 Stratus 服务代表通讯：

消息类型：自动通报和授权

协议：TCP

端口：443

Stratus 支持服务器地址：*.stratus.com

消息类型：支持诊断

协议：TCP

端口：443

Stratus 支持服务器地址：*.stratus.com

消息类型：拨号

协议：TCP

端口:443, 默认代理端口:3128(您可以更改默认代理端口号。)

Stratus 支持服务器地址:*.ecacsupport.com

消息类型:电子警报

协议:SMTP

端口:25

(有关 TCP 或 UDP 端口的其他信息,请访问知识库,搜索文章 *ztC Edge使用的 TCP 和 UDP 端口 (KB-9357)*。请参阅[访问知识库文章](#)。)

要使 SNMP 管理系统能够接收警报并向 ztC Edge系统发送自陷,请针对以下内容配置防火墙:

消息类型:SNMP

协议:SNMP

端口:161(Get/Walk) 162(Traps)

6. 生成测试警报.

要生成测试警报

单击**生成测试警报**。Stratus Redundant Linux软件会生成测试警报,并且“支持配置”向您的授权 Stratus 服务代表 发送通知;电子警报向电子警报的所有电子邮件接收者发送主题为“测试警报”的示例电子邮件(如果配置)(请参阅[配置电子警报](#));SNMP 向 SNMP 自陷的接收者发送自陷(如果配置)(请参阅[配置 SNMP 设置](#))。查看“警报历史记录”日志(请参阅[“警报历史记录”页](#)),了解传送状态。如果支持通知失败,则将生成后续警报。

相关主题

[ztC Console](#)

[“首选项”页](#)

[使用 ztC Console](#)

配置 Internet 代理设置

为 ztC Edge系统配置代理设置,如果您的组织需要使用代理服务器接入 Internet,并且您与 Stratus 或另一个授权 ztC Edge 服务代表签订了服务协议。

代理服务器在 ztC Edge系统与 Internet 之间提供了一个安全的桥梁。Stratus Redundant Linux软件仅将代理服务器信息用于与支持通知消息传递和远程支持访问功能相关的出站 HTTP 流量。

要配置 Internet 代理设置

1. 单击左侧导航面板中的**首选项**，打开**首选项**页。
2. 在**远程支持**下，单击**代理配置**。
3. 要启用代理服务，则单击**启用代理**框。
4. 在**代理服务器**框中，键入完全限定的代理服务器主机名或 IP 地址。
5. 在**端口号**框中，如果端口号与默认编号 (3128) 不同，则键入此端口号。
6. 如果代理服务器需要进行身份验证，则单击**启用身份验证**框，然后键入**用户名和密码**。

如果您没有键入密码，则仍需要键入先前密码。如果先前密码为空，并且您没有输入新密码，则密码仍为空。

7. 单击**保存**(或者单击**重置**，以便还原先前保存的值)。

相关主题

[ztC Console](#)

[“首选项”页](#)

[使用 ztC Console](#)

“警报历史记录”页

警报历史记录页显示有关 ztC Edge 系统上的事件的消息。

要打开**警报历史记录**页，则单击**警报历史记录** - 位于 ztC Console 的左侧导航面板中。(要查看 ztC Edge 系统上用户活动的日志，请参阅[“审核日志”](#)页。)

注意：仅当您在 ztC Console 控制台中启用支持通知警报、电子警报和 SNMP 自陷时才会生成它们。有关信息，请参阅：



- [配置远程支持设置](#)
- [配置电子警报](#)
- [配置 SNMP 设置](#)

要查看警报信息，则在默认按反向时间序列出的警报中进行滚动。单击警报可显示警报出现的时间以及有关问题和解决方法(如有)的信息，以及是否为该警报发送了**支持通知**、**电子警报**或者**SNMP 自陷**。(您还可以使用 snmptable 显示警报信息；请参阅[使用 snmptable 获取系统信息](#)。)

要移除某条警报，则选择它，然后单击**移除**。

要移除所有警报，则单击**全部清除**。

相关主题

[ztC Console](#)

[使用 ztC Console](#)

“审核日志”页

审核日志页显示 ztC Console 中用户活动的日志。要打开此页，则单击左侧导航面板中的**审核日志**。(要显示有关 ztC Edge系统上的事件的信息，请参阅[“警报历史记录”](#)页。)

要查看日志信息，则在默认按反向时间顺序列出的日志条目中进行滚动。这些信息包括：

- **时间**—操作的日期和时间。
- **用户名**—发起此操作的用户名称。
- **源主机**—正在运行 ztC Console 的主机 IP 地址。
- **操作**—ztC Console 中执行的操作。

您还可以使用 `snmptable` 显示有关审核日志的信息(请参阅[使用 snmptable 获取系统信息](#)。)

相关主题

[ztC Console](#)

[使用 ztC Console](#)

[安全性加强](#)

“支持日志”页

支持日志页可使您生成诊断文件，这包括特定时刻 ztC Edge 系统的日志文件和配置信息。这些信息可使您的授权 Stratus 服务代表解决系统问题。

有关其他信息，请参阅：

- [创建诊断文件](#)
- [删除诊断文件](#)
- [上传诊断文件至客户支持](#)

相关主题

[ztC Console](#)

[使用 ztC Console](#)

[“首选项”页](#)

创建诊断文件

诊断文件提供特定时刻 **ztC Edge** 系统的日志文件和配置信息。创建一个诊断文件，以帮助您的授权 **Stratus** 服务代表解决系统问题。



注意： **Stratus Redundant Linux** 软件为诊断文件分配固定量的存储空间。如果在创建诊断文件时没有足够空间，系统将删除之前创建的文件。

要创建诊断文件

1. 单击左侧导航面板中的 **支持日志**，打开 **支持日志** 页。
2. 单击 **生成诊断文件**。
3. 将此文件上传到您的授权 **Stratus** 服务代表，如 [上传诊断文件至客户支持](#) 中所述。

相关主题

[ztC Console](#)

[“首选项”页](#)

[使用 ztC Console](#)

上传诊断文件至客户支持

把一个诊断文件上传到 **Stratus ztC Edge** 客户支持网站来帮助解决系统的问题。(要创建诊断文件，请参阅 [创建诊断文件](#)。)

把诊断文件上传到客户支持

1. 单击左侧导航面板中的 **支持日志**，打开 **支持日志** 页。
2. 执行以下操作之一：
 - 如果 **ztC Edge** 系统具备互联网连接，则单击 **Stratus 上传 ztC Edge** 来把诊断文件直接上传到客户支持网站。如果上传成功，将显示一条消息，确认此诊断文件已成功上传。

- 如果 ztC Edge系统没有网络连接，或者如果上传失败，您可以手动将诊断文件上传至 **Stratus 诊断上传** 页面。首先，单击 ztC Console 上的 **下载** 来把诊断文件的 .zip 文件下载到本地计算机。将诊断 zip 文件转移到有网络连接的计算机上。打开网络浏览器，在其地址栏中输入 <http://diags.stratus.com/DiagUpload.html>。在 **Stratus 诊断上传** 页上，单击 **选择文件**，选择计算机上的 zip 文件，然后单击 **提交**。

在这个操作程序上需要帮助时，请拨打 **ztC Edge支持** 页在 <https://www.stratus.com/services-support/customer-support/?tab=ztcedge> 上所列的电话号码致电 ztC Edge 客户支持。

确定不再需要该文件(例如:客户支持确认文件已正确上传)后,可按照 **删除诊断文件** 中的描述,选择性地将其从 ztC Edge 系统中删除。

相关主题

[ztC Console](#)

[“首选项”页](#)

[使用 ztC Console](#)

删除诊断文件

从 ztC Edge 系统删除诊断文件(在您已将其上传到您的授权 **Stratus** 服务代表后)。

要删除诊断文件

1. 单击左侧导航面板中的 **支持日志**，打开 **支持日志** 页。
2. 选择此诊断文件，然后单击 **删除**。

相关主题

[ztC Console](#)

[“首选项”页](#)

[使用 ztC Console](#)

“物理机”页

物理机页可使您管理 ztC Edge 系统中的物理机 (PM)。(PM 也称为节点。)要打开此页,则单击左侧导航面板中的**物理机**。

物理机标题和刊头下将立即显示**状态、活动、名称、型号**和**VM**列。要管理一台 PM 时,单击**名称**下的 **node0(主)**或 **node1(如果存在)**。要解释 PM 状态和活动,请参阅[物理机状态和活动](#)。要显示有关节点的信息,您可使用 `snmptable` 命令;请参阅[使用 snmptable 获取系统信息](#)。

下面的窗格显示选定节点的操作按钮和详细信息:

- **操作按钮**:将根据所选节点的状态显示各种操作按钮,不活动按钮变灰。在执行大多数维护工作时,都应点击**维护模式**,系统将把一个节点置于维护模式(关于相关信息,请参阅[维护模式](#))。要了解有关维护模式中可用的其他 PM 操作,请参阅[物理机操作](#)或者有关您要完成的任务的帮助主题。
- **详细信息**:要查看关于选定节点的详细信息或统计数据,应点击如下选项卡之一:
 - **总结**(初始显示),里面将显示有关此节点的信息,例如所选节点的制造商(如果适用)、型号、序列号、总体状态、活动和配置(内存和物理磁盘)。
 - **描述**,里面显示一个窗口,在这里您可以输入关于该节点的信息。
 - **存储**,里面显示存储的状态、逻辑 ID、大小和使用的大小。它还显示 SSD 驱动器的剩余使用时间。
 - **传感器**,其显示有关传感器名称和当前状态的信息,包括有关电压的信息以及有关电池电压检查的信息。
 - **网络**,里面显示网络的状态、名称、速度和 MAC 地址。
 - **虚拟机**,其显示虚拟机的状态、活动和名称。
 - **USB 设备**,其列出节点中插入的任何 USB 设备。
 - **监视器**,其提供有关系统的信息(例如 CPU 使用率和内存使用率)。有关信息,请参阅[监控 ztC Edge 系统](#)。

相关主题

[ztC Console](#)

[使用 ztC Console](#)

物理机操作

当您选择物理机 (PM) 时, 根据此 PM 的状态和活动, 将显示以下部分或所有操作按钮, 不活动按钮变灰。



小心: 在对 PM 进行维护时, 应使用 ztC Console 的 **物理机** 页面。不要使用计算机上的控件, 因为 ztC Console 可阻止大多数对 ztC Edge 系统具有潜在破坏性的操作。

命令	描述
 维护模式	使 PM 进入维护模式。在该 PM 上运行的 VM 会迁移到其他 PM - 如果此 PM 存在并且正在使用。(否则, 将会要求您重新确认请求, 然后关闭 VM。)当迁移或关闭了 VM 时, PM 会显示正在运行(正在维护)。请参阅 维护模式 。
在 PM 进入维护模式时, 单击 维护模式 按钮后在某些系统上可执行以下操作。	
 退出维护	从运行(维护模式)状态移除 PM。请参阅 维护模式 。
 关闭	关闭 PM。PM 转变为关闭(维护模式)。请参阅 关闭物理机 。
 重启	重启 PM。PM 转变为准备重启(维护模式)。参阅 重启物理机 。
 移除	令 Stratus Redundant Linux 软件从 ztC Edge 系统的数据库中删除 PM, 以便替换 PM 或其组件。请参阅 更换物理机 (手动)
在 PM 故障或 Stratus Redundant Linux 软件因故障率过高而停止使用 PM 并将其关闭后, 可以执行以下操作。	
 	恢复故障 PM。有些情况下, ztC Console 会把故障 PM 的状态显示为无法联

命令	描述
恢复	系(同步/撤出...)。请参阅 恢复故障物理机(手动)

相关主题

[ztC Console](#)

[使用 ztC Console](#)

[“物理机”页](#)

物理机状态和活动

以下状态和活动适用于物理机 (PM)。在每个状态和活动过程中仅启用某些操作。

状态	活动	可用命令	描述
	 正在运行	维护模式	PM 正在正常运行。
	 正在撤出	退出维护	虚拟机正在从该 PM 迁移到其配对的 PM。
	 正在运行	维护模式	预计 PM 会出现故障。
	 正在运行	维护模式	PM 已出现故障。
	 的电源已关闭	维护模式	由于过高的故障率，ztC Edge 已关闭了 PM 的电源。
	 正在启动	退出维护	PM 正在启动。
	 正在重启	退出维护	PM 正在重启。
	 正在运行	退出维护 关闭 重启	PM 正在维护模式下运行。请参阅 维护模式 。

状态	活动	可用命令	描述
		恢复 替换	

相关主题

[ztC Console](#)

[使用 ztC Console](#)

[“物理机”页](#)

“虚拟机”页

使用**虚拟机**页可管理在 ztC Edge 系统上运行的虚拟机 (VM)。要打开此页，则单击**虚拟机** - 位于 ztC Console 的左侧导航面板中。

要管理特定 VM，则单击**虚拟机**页顶部窗格中的 VM 名称。底部窗格显示用于管理 VM 的控件和信息。

关于**虚拟机**页面上显示的 VM 状态信息的解释，请参阅[虚拟机状态和活动](#)。欲了解关于该页面上的控件的更多信息，请参阅[虚拟机操作](#)或某项工作的帮助主题。

您可以使用**虚拟机**页执行管理任务，包括：

- 在底部的窗格中查看关于 VM 的信息，包括其名称、操作系统、描述和资源
- 创建、复制、导出、导入或还原 VM，如[创建和迁移虚拟机](#)中所述
- [打开虚拟机控制台会话](#)
- [重新配置虚拟机资源](#)
- 按如下主题中所述控制 VM 的电源开关状态：
 - [启动虚拟机](#)
 - [关闭虚拟机](#)
 - [关闭虚拟机电源](#)
- [移除虚拟机或重命名虚拟机](#)
- 执行高级任务或故障排除，如[高级主题\(虚拟机\)](#)中的汇总信息

- 安装(和卸载)供客人操作系统使用的 USB 设备或网络安装的文件夹, 如在 [ztC Edge系统上安装 USB 设备或网络安装的文件夹](#)中所述
- 作为 USB 设备附加到 VM(以及与 VM 分离), 如[将USB 设备附加到虚拟机](#)中所述。
- 监控基于 Windows 的 VM 和应用程序, 如[监控系统、基于 Windows 的 VM 和应用程序](#)所述

已被分配了**管理员**或**平台管理员**角色的用户可执行**虚拟机**页上的所有任务。已被分配了**VM 管理员**角色的用户可执行所有任务, 除了**VM 管理员**无法展开卷外。有关**VM 管理员**权限的详细信息, 请参阅[管理虚拟机](#)。有关分配这些角色的信息, 请参阅[管理本地用户帐户](#)。

相关主题

[管理虚拟机](#)

[使用ztC Console](#)

虚拟机操作

当您选择虚拟机 (VM) 时, 根据此 VM 的状态和活动, 可能显示以下操作按钮, 不活动按钮变灰。

操作	描述
 创建	启动“创建 VM 向导”。请参阅 创建新虚拟机 。
 复制	复制您系统中的现有 VM, 以创建新的 VM 或创建用于故障排除的副本 VM 请参阅 复制虚拟机 。
 导入/还原	<p>从一系列 OVF 和 VHD 文件导入 VM。请参阅创建和迁移虚拟机。</p> <p>导入向导使您能够导入一个 VM 以创建一个新的 VM 实例, 或恢复一个 VM 以创建一个完全一样的 VM, 并在 OVF 和 VHD 文件中提供相同的硬件 ID。</p> <p>开放式虚拟机格式 (OVF) 是一种打包和分发物理机或虚拟机数据的开放式标准。OVF 格式包含有关 VM 的元数据信息。虚拟硬盘 (VHD) 是一个包含虚拟磁盘信息的文件。</p>
如果 VM 正在运行, 则可使用以下操作。	

操作	描述
 安装	安装 USB 设备 或 网络安装 的文件夹(即, 目录), 以便使其供客人操作系统使用。然后可将 VM 导出到安装的位置。请参阅 在 ztC Edge系统上安装 USB 设备或网络安装的文件夹 。
 卸载	卸载已安装的 USB 设备 或 网络安装 的文件夹。请参阅 在 ztC Edge系统上安装 USB 设备或网络安装的文件夹 。
 控制台	打开针对所选 VM 的控制台。请参阅 打开虚拟机控制台会话 。
 关闭	关闭所选的 VM 。请参阅 关闭虚拟机 。
 关机	立即停止所选 VM 中的处理, 并毁坏其内存状态。仅将这作为在无法成功关闭 VM 时万不得已的方法。请参阅 关闭虚拟机电源 。
如果关闭或停止了 VM , 则可使用以下操作。	
 配置	启动 重新配置虚拟机 向导。在启动此向导之前, 必须关闭 VM 。请参阅 重新配置虚拟机资源 。
 还原	通过从之前的 OVF 和 VHD 文件备份副本覆盖 VM , 在您的 ztC Edge系统上恢复一个现有 VM 。请参阅 从 OVF 文件替换/还原虚拟机 。
	将 VM 的映像保存到一系列 OVF 和 VHD 文件中。您可以将这些文件导入到其他系统, 或者将它们导入回同一 ztC Edge系统, 以便还原或复制原始 VM 。请参

操作	描述
导出	参阅 导出虚拟机 。
 启动	启动所选的 VM。请参阅 启动虚拟机 。
 从 CD 启动	从所选的虚拟 CD 启动 VM。请参阅 从虚拟 CD 启动 。
 移除	移除 VM。请参阅 移除虚拟机 。
如果由于过高的故障率 Stratus Redundant Linux 已停用 VM 并关闭了其电源，则可使用以下操作。	
 重置设备	<p>重置 VM 的平均故障间隔时间 (MTBF) 计数器，以便能够使其恢复使用。请参阅 为故障虚拟机重置 MTBF。</p> <p>当 VM 崩溃时，Stratus Redundant Linux 软件会自动重启该 VM，除非它已低于其 MTBF 阈值。如果 VM 低于此 MTBF 阈值，则 Stratus Redundant Linux 软件会使其保持在崩溃状态。必要时可单击 重置设备 来重启该 VM 并重置 MTBF 计数器。</p>

相关主题

[管理虚拟机的运行](#)

[“虚拟机”页](#)

[使用 zIC Console](#)

虚拟机状态和活动

虚拟机 (VM) 可具有以下状态和活动，在此期间只可启用某些操作。

状态	活动	启用的操作	描述
	 安装		Stratus Redundant Linux软件正在安装新 VM 的启动卷。
	 已停止	启动 复制 配置 导出 从 CD 启动 移除	已关闭 VM 或者已关闭其电源。
	 正在启动	控制台 关机	VM 正在启动。
	 正在运行	控制台 关闭 关机	VM 正在冗余物理机上正常运行
	 正在运行	控制台 关闭 关机	VM 正在正常运行，但不是完全冗余的资源上运行。
	 正在停止	关机 移除	正在关闭 VM 以响应关闭操作，或者由于剩余物理机正在过渡到维护模式，因此正在关闭 VM。
	 已崩溃		VM 已崩溃，并且正在重启。如果已启用，则会发送电子警报和支持通知。
	 已崩溃		VM 崩溃太多次，并且超出了其

状态	活动	启用的操作	描述
			MTBF 阈值。在单击 重置设备 前，VM 保持在崩溃状态。请参阅 为故障虚拟机重置 MTBF 。

相关主题

[管理虚拟机的运行](#)

[“虚拟机”页](#)

[使用 ztC Console](#)

“卷”页

卷页显示有关附加到 ztC Edge 系统中虚拟机 (VM) 的卷的信息。要打开此页，则单击**卷** - 位于 ztC Console 的左侧导航面板中。**卷**页在顶部窗格中显示具有卷信息的以下列：

- 状态
- 名称
- 磁盘同步(如果存在)
- 大小
- 可启动
- 使用者，其显示下列内容之一：
 - 该卷正在由 VM 使用时，到该 VM 的链接。
 - 当该卷是**根**或**交换**卷时，到物理机 (PM) 页面(**node0** 或 **node1**，如果存在)的链接。
 - 对于共享卷 (**shared.fs**)系统。
 - 当卷不是系统卷并且没有被 VM 使用时，显示**无**。

单击**卷**页顶部窗格中的卷名称可在底部窗格中显示有关该卷的其他信息。(您还可以使用 `snmptable` 命令显示有关卷的信息；请参阅[使用 snmptable 获取系统信息](#)。)您可以从底部窗格对卷执行一些管理任务，包括：

- 在**描述**文本框中为每个卷添加描述。
- 重命名卷(请参阅[重命名 ztC Edge 系统上的卷](#))。

- 通过单击**移除**，移除卷。但注意，当 VM 正在使用卷时，**移除**按钮变灰。

可从“虚拟机”页执行其他卷管理任务。这些任务包括：

- [将卷附加到虚拟机](#)
- [在虚拟机中创建卷](#)
- [将卷与虚拟机分离](#)
- [将卷从虚拟机中移除](#)

相关主题

[ztC Console](#)

[使用 ztC Console](#)

“网络”页

网络页显示有关附加到 ztC Edge 系统的共享网络的信息。要打开此页，则单击**网络** - 位于 ztC Console 的左侧导航面板中。

您可以使用**网络**页查看有关特定网络的信息，包括其状态、链路情况、名称、内部名称、类型、连接的虚拟机 (VM) 数、速度和 MTU。您还可以使用底部窗格中的**描述**选项卡添加有网络的描述。

要管理特定网络或只是查看有关它的信息，则单击**网络**页顶部窗格中的**名称**或**内部名称**下的网络名称，或者单击**摘要**选项卡上网络连接图表中的端口。底部窗格显示有关该网络上的节点的额外信息。**摘要**选项卡中的列显示有关节点的状态、物理接口、速度、MAC 地址、插槽和端口的信息。要显示或隐藏列，则将光标移至列标题的右侧，单击显示的下拉箭头，然后单击**列**，从而选择或取消选择您要显示或隐藏的列。

您可以使用**网络**页执行管理任务，包括：

- 在**摘要**选项卡上查看组成网络的物理适配器的列表。
- 在**描述**选项卡上添加网络描述。
- 在**虚拟机**选项卡上查看使用网络的虚拟机的列表。
- 通过双击**名称**列中的名称来更改名称。
- 为 A-Link 和业务网络 [设置 MTU](#)。

有关网络的更多信息，请参阅以下主题：

- [网络架构](#)
- [连接以太网电缆](#)

- [一般网络要求和配置](#)
- [符合网络要求](#) (针对 ALSR 配置)



注意：网络页仅显示在两个物理机上都具有物理连接的网络。如果您期望看到的网络没有显示，则检查两个网络连接是否进行了正确接线，以及它们的 LINK 是否出于活动状态。

相关主题

[ztC Console](#)

[使用 ztC Console](#)

设置 MTU

使用网络能够支持的最高值的最大传输单元 (MTU) 可提高网络性能。您可以使用 ztC Console 的网络页为 A-link 和业务 (biz) 网络指定 MTU 值。



注意：如果您更改任一业务网络 (network0 或 network1) 的 MTU 设置，系统都会自动将 VM 从一个节点迁移到另一个节点。如果您具体更改了 network0 的 MTU，则系统还会自动从主节点故障转移到从节点。要避免此问题，则避免更改业务网络的 MTU 设置，或者仅在计划的维护期间更改 MTU。

要设置 A-Link 或业务网络的 MTU

1. 单击左侧导航面板中的 **网络**，打开网络页。
2. 在顶部窗格中，选择您想要为其设置 MTU 值的 A-link 或业务网络。
3. 单击 **配置**。
4. 在 **配置共享网络** 窗口中，选择 **网络角色** (业务或 A-Link)。
5. 在 **MTU** 下，键入一个从 1280 到 65535。默认值为：
 - 在 100i 系统上，所有以太网端口的默认值均为 1500。
 - 在 110i 系统上，默认值取决于以太网端口：
 - 对于端口 A1 (A-Link1) 和 A2 (priv0)，值为 9000。
 - 对于端口 P1 至 P6 (ibiz0 至 ibiz5)，值为 1500
6. 单击 **保存**。

相关主题

[“网络”页](#)

[ztC Console](#)

[使用 ztC Console](#)

“虚拟 CD”页

使用 **虚拟 CD** 页可创建虚拟 CD (VCD)。使用 VCD 来使软件安装或恢复介质可用于系统上的虚拟机。要打开此页，则单击 **虚拟 CD** - 位于 ztC Console 的左侧导航面板中。

要管理特定 VCD，则单击 **虚拟 CD** 页顶部窗格中的 VCD 名称。底部窗格显示有关 VCD 的描述。

您可以使用 **虚拟 CD** 页执行管理任务，包括：

- [创建虚拟 CD](#)
- [移除虚拟 CD](#)
- [重命名虚拟 CD](#)
- 在 **描述** 文本框中为每个卷添加描述

为完成其他 VCD 管理任务，请参阅 [管理虚拟 CD](#)。

相关主题

[插入虚拟 CD](#)

[弹出虚拟 CD](#)

[使用 ztC Console](#)

“升级套件”页

ztC Edge 升级套件 页使您能够上传和管理用来把系统升级到 Stratus Redundant Linux 软件更新版本的升级套件。您可以检查是否可获得新版本的系统软件，然后下载它(如果可获得)。您还可以将升级套件复制到 USB 介质，以便在重新安装该系统软件时使用此介质。

要打开 **升级套件** 页面时，点击 ztC Console 的左侧导航面板上的 **升级套件**。



注意：您可以指定自动下载可获得的升级套件。您还可以启用向系统管理员发送的电子邮件警报(电子警报)，从而在可获得系统软件更新时通知他们。请参阅 [管理软件更新](#)。

要检查并下载新版本的系统软件

 **注意：**您的用户角色必须为**管理员**或**平台管理员**才能执行此程序。

1. 单击左侧导航面板中的**升级套件**，打开**升级套件**页。
2. 单击刊头下方的**检查更新**。

将显示一个消息框，指示是否可获得新版本的系统软件。

3. 如果可获得更新，则将显示**可获得软件更新**框，您可以单击**下载软件**，下载该软件。您还可以单击**查看发行说明**(英文版本)，阅读有关此更新的信息。

 **注意：****升级套件**页仅允许两个已保存的套件。如果此页列出了两个套件，并且您想要下载另一个套件，则您需要首先删除一个套件。

单击**下载软件**时，将出现以下情况：

- 如果将 **ztC Edge**系统连接到了 **Internet**，则会具有软件更新的 **.kit** 文件直接下载到系统，并将其列在**升级套件**页上。**可获得软件更新**中显示各种状态消息，从而指示下载进度。
- 如果未将系统连接到 **Internet**，则会将 **.kit** 文件下载到正在运行 **ztC Console** 的远程管理计算机。将该文件保存到浏览器的默认下载文件夹，或导航到其他位置。您将收到一条警报(如果已配置)，通知您可获得新版本的系统软件，您需要将其上传到系统。

4. 要继续升级，请参阅[使用升级套件升级 Stratus Redundant Linux 软件](#)。

有关升级 **Stratus Redundant Linux**软件的信息，请参阅[升级 Stratus Redundant Linux 软件](#)。

有关创建 **USB 介质**的信息，请参阅[创建具有系统软件的 USB 介质](#)。

相关主题

[ztC Console](#)

[使用 ztC Console](#)

创建具有系统软件的 USB 介质

您可以使用**升级套件**页创建具有系统软件 **Stratus Redundant Linux** 的部署 ISO 文件副本的 **USB 介质**。然后使用此 **USB 介质**重新安装该软件，如果您需要手动恢复或替换故障节点。



注意：将升级套件复制到 USB 介质会将文件系统(如果有)从该介质中卸除。

要创建具有系统软件的 USB 介质

1. 下载升级套件，如果您尚未这样做。请参阅[使用升级套件升级 Stratus Redundant Linux软件](#)。
2. 将 USB 介质插入主节点中。在**物理机**页上，查看 **USB 设备**选项卡是否列出了此设备。
3. 在ztC Console中，单击左侧导航面板中的**升级套件**。
4. 如果**升级套件**页列出了多个套件，则选择具有您要复制的 ISO 的版本。
5. 单击**创建 USB 介质**按钮(在刊头下方)。

将打开**创建 USB 介质**对话框。

6. 如果节点有多个 USB 介质，您需要从下拉列表中选择一个介质。然后单击**继续**(或单击**取消**，以取消此程序)。

创建 USB 介质对话框显示进度百分比。在复制完成时，此窗口会关闭。

如果您需要手动恢复或替换故障节点，使用此 USB 介质重新安装该软件。请参阅[恢复故障物理机\(手动\)](#)或[更换物理机\(手动\)](#)。

相关主题

[“升级套件”页](#)

4

第 4 章：升级 Stratus Redundant Linux 软件

要升级 Stratus Redundant Linux 软件，则使用升级套件。请参阅 [使用升级套件升级 Stratus Redundant Linux 软件](#)。

相关主题

[管理软件更新](#)

[“升级套件”页](#)

[ztC Console](#)

[使用 ztC Console](#)

使用升级套件升级 Stratus Redundant Linux 软件

该主题描述如何使用 Stratus Redundant Linux 软件的升级套件来升级系统软件。该主题还说明如何下载该套件，然后将其上传到系统(如果您在升级系统前需要这样做)。对于已授权用于两个节点的系统，您可以根据情况通过启用暂停来控制升级(您无法在已授权用于一个节点的系统上启用暂停)。在暂停期间检查系统对于验证或重新配置不由该系统管理的第三方工具或其他服务非常有用。



小心： 不要从除 ztC Edge 外的任何来源更新 Stratus 系统的 CentOS 主机操作系统。仅使用与 Stratus Redundant Linux 软件一同安装的 CentOS 版本。

先决条件：

- 升级该系统软件前，所有 PM 和 VM 都必须处于良好的运行状态。开始升级前，请先检查 **ztC Console**，以确认没有表明 PM 或 VM 出现问题的警报。
- 在升级该系统软件前，从 VM 弹出任何 VCD 或 USB 介质。如果 VCD 或 USB 介质仍与 VM 连接，这会阻止系统迁移 VM，并且会将 PM 置于维护模式以进行该升级过程。
- 要验证系统是否符合此升级套件的要求，则使用**资格验证**按钮，如本主题中所述。
- 在您升级已授权用于一个节点的系统前，应备份 VM。然后，按照以下说明升级并验证该软件。最后，使用**升级已授权用于一个节点的系统**中的操作程序升级系统的一个 PM。在升级操作过程中系统重启时，对 **ztC Console** 的访问至少将中断 15 分钟。

这些步骤为：

- I. 下载升级套件
- II. 将升级套件上传到系统
- III. 验证该软件 (可选)
- IV. 升级系统软件

I. 下载升级套件

在可获得更新时，您可以下载包含新系统软件的升级套件(如果尚未下载)。从**升级套件**页中，单击**可获得软件更新**窗口中的**下载软件**(请参阅“**升级套件**”页)。

或者，您可以从 **Stratus 下载** 页下载该软件。



注意： ztC Console 的**升级套件**页仅允许两个已保存的套件。如果此页列出了两个套件，并且您想要下载另一个套件，则您需要首先删除一个套件。

1. 打开此**下载**页面在 <https://www.stratus.com/services-support/downloads/?tab=ztcedge>。
2. 向下滚动到升级部分，然后单击升级链接，下载该套件。
3. 导航到本地计算机上的某个位置，保存此文件。必要时，将此文件传输到运行 **ztC Console** 的远程管理计算机。

II.将升级套件上传到系统

必要时，将升级套件从运行 **ztC Console**的远程管理计算机上传到 **ztC Edge** 系统。

1. 在**ztC Console**中，单击左侧导航面板中的**升级套件**。
2. 在**升级套件**页上，单击刊头下的**添加套件**按钮，系统将打开**ztC Edge - 套件上传向导**。
3. 在**ztC Edge- 套件上传向导**对话框内，单击**选择文件 (Google Chrome)**或**浏览 (Firefox 或 Internet Explorer)**，然后浏览选择一个 **.kit** 文件。
4. 选择了一个 **.kit** 文件后，单击**上传、导入或完成**(二者功能相同)。在文件上传过程中将显示消息，例如**正在上传文件(不要关闭向导)**。对于本地保存的文件，上传可能需要最长两分钟时间，对于网络上保存的文件，可能需要十分钟或更长时间。如果上传失败，则此向导会显示消息**加载文件失败**。
5. 上传完成后，此向导关闭，**升级套件**页将列出此升级套件的状态和版本号。**资格验证、升级和删除**按钮也将与**添加套件**按钮一起显示。
6. 如果已加载多个升级套件，请选择一个使用。

III.验证该软件

验证该软件，以便验证您的系统是否符合此升级套件的要求。(建议验证该软件，而非必须验证。)

要执行此操作，则在**升级套件**页上选择要进行资格验证的升级套件，然后单击**资格验证**。

资格验证可能需要六分钟。如果资格验证成功，则继续下一步。

如果资格验证失败，则会弹出一个窗口，指示失败原因。这些消息可能指示版本不支持、存储不足、分区问题、需要关闭 **VM**，或者与升级此系统相关的其他信息。例如，如果系统没有足够的磁盘空间来完成升级，则会显示消息可用空间不足，并且报告所需的空间量。如果您在解决资格验证问题时需要帮助，请在**知识库**中搜索资格验证错误消息，位于此**Stratus 客户服务门户**在 <https://support.stratus.com>。

IV.升级系统软件

1. 单击**升级套件**页上的**升级**，开始升级。

将显示**确认**窗口，表示您已选择了升级该系统，并且会显示一条消息，要求您确认升级到所选升级套件。该窗口还包含一个能够使您暂停的复选框，从而使您能够控制升级。可通过单击**单独节点升级后暂停**框来暂停。

2. 单击**是**，继续升级。

升级开始。如果您启用了暂停，说明升级步骤的图表会显示升级的当前状态。当升级暂停时，您必须单击**退出维护**才能继续。

升级了一个节点但另一个节点(如果存在)尚未升级后，这两个节点将运行该软件的不同版本。在此期间，刊头显示消息**系统正在使用不匹配的版本运行**。

升级完成后，在所有基于 Windows 的 VM 上检查是否有更新的 virtIO 驱动程序，如[更新 VirtIO 驱动程序\(基于 Windows 的 VM\)](#)中所述。

要升级已授权用于一个节点的系统

1. 关闭 ztC Edge系统上所有正在运行的 VM。
2. 按照上述步骤中的说明，使用升级套件升级系统。



注意：在升级操作过程中系统重启时，对 ztC Console 的访问至少将中断 15 分钟。

3. 确保系统正在正确运行。
4. 启动所有 VM。

相关主题

[管理软件更新](#)

[“升级套件”页](#)

[ztC Console](#)

[使用 ztC Console](#)

[ztC Edge系统描述](#)

5

第 5 章：管理物理机

管理物理机 (PM) 或节点，以便控制其运行并执行维护。

使用 **物理机** 页面 (ztC Console) 查看和管理 PM；有关信息，请参阅 [“物理机”页](#)。

您从 **物理机** 页执行的许多任务需要使用维护模式；有关信息，请参阅 [维护模式](#)。

要管理 PM 的运行状态 (在维护模式下)，请参阅：

- [重启物理机](#)
- [关闭物理机](#)
- [负载均衡](#)

要启动 PM (在 PM 的物理控制台上)，请参阅 [启动物理机](#)。

要通过恢复故障 PM 或为故障机器重置 MTBF 来进行故障排除，请参阅 [物理机故障排除](#)。

要在 PM 硬件上执行维护任务，例如更换 PM，请参阅 [维护物理机](#)。

要在已授权进行此类监控的系统上监控 ztC Edge 系统的主机操作系统，请参阅 [监控 ztC Edge 系统](#)。

维护模式

当物理机 (PM) 进入维护模式时，其会脱机，以便进行修复。当您完成修复时，PM 会退出维护模式并返回联机状态，从而可用于运行虚拟机 (VM)。

当在已授权用于两个 PM 的系统中，一个 PM 进入维护模式时，PM 会将在它上运行的 VM 迁移到其他 PM，这可防止这些 VM 出现因该修复导致的任何中断。当在已授权用于两个 PM 的系统中，两个 PM 均进入维护模式时，这些 PM 会执行所有 VM 的有序关闭，这可在这些 PM 关闭或重启前保护它们的内存状态。

当主 PM(节点x(主))进入维护模式时,另一个 PM(如果存在)将变成主设备。

当在已授权用于一个节点(即,一个 PM)的系统中,一个 PM 进入维护模式时,该 PM 会关闭 VM。

仅在 PM 处于维护模式时从物理机页关闭 PM,因为 ztC Console 会防止系统受到因手动关闭 PM 而导致的破坏性操作的影响。

小心:



1. 当 PM 处于维护模式时,系统没有容错特性。为实现持续的正常运行,尽快完成修复,以便使 PM 能够退出维护模式并返回联机状态。
2. 仅当您能够关闭所有业务处理时,才将所有 PM 置于维护模式。如果您需要在已授权用于两个 PM 的系统上使 VM 保持运行,则不要使两个 PM 都进入维护模式。为使 VM 保持运行,至少一个 PM 必须启动并正常运行。(如果您需要关闭整个 ztC Edge 系统,请参阅[关闭物理机](#)。)



注意: 如果在已授权用于两个 PM 的系统中,您想让两个 PM 均进入维护模式,则首先使从 PM 进入维护模式,然后使主 PM 进入维护模式。此顺序可避免不必要的 VM 迁移。

要使 PM 进入维护模式

1. 从物理机页选择一个 PM。
2. 单击**维护模式**。

当 PM 进入维护模式时,其状态显示 .

要退出维护并使 PM 退出维护模式

1. 从物理机页选择一个 PM。
2. 单击**退出维护**,这将使 PM 退出维护模式。

相关主题

[ztC Console](#)

[管理物理机](#)

[物理机和虚拟机](#)

[“物理机”页](#)

[“虚拟机”页](#)

启动物理机

在物理机 (PM) 的物理控制台上启动 PM。



注意：如果因为您断开电源线或因交流主电源断电而使 PM 断电，则将 ztC Edge 系统中的每个 PM 均设为在电力一恢复便自动启动。

要启动 PM

1. 按下 PM 前面板上的电源按钮。
2. 确保前面板上的 PWR LED 亮起。

如果要您启动系统，则按系统中每个 PM 的前面板上的电源按钮，如 [启动系统](#) 中所述。

相关主题

[维护模式](#)

[ztC Console](#)

[管理物理机](#)

[“物理机”页](#)

重启物理机

重启物理机 (PM)，以便重启其 Stratus Redundant Linux 软件，以及根据需要使 PM 退出维护模式。(如果在已授权用于两个节点的系统中您需要重启两个 PM，请参阅 [重启系统](#)。)

要重启 PM

1. 确定您要重启哪个 PM (node0 或 node1，如果存在)。
2. 在 ztC Console 中，单击左侧导航面板中的 **物理机**。
3. 选择相应的 PM (node0 或 node1，如果存在)，然后单击 **维护模式**，这会将该 PM 的总体状态更改为 **维护模式**，以及将 **活动状态** 更改为 **正在运行 (维护中)**。
4. 单击 **重启**。当 PM 重启时，将显示 **活动状态**：
 - **准备重启 (维护模式)**
 - **重启 (维护模式)**

- 启动(维护模式)
- 运行(维护模式)。

5. 要使 PM 退出维护模式并使其可用于运行虚拟机，则单击**退出维护**。

相关主题

[维护模式](#)

[ztC Console](#)

[管理物理机](#)

[“物理机”页](#)

关闭物理机

要维修或更换一台物理机 (PM) 或节点时，关闭该 PM 来停止其运行。使用以下操作程序通过使用 ztC Console 或 PM 上的电源按钮关闭一台且仅关闭一台 PM。

小心：



1. 使用以下操作程序关闭具有两个节点的系统上的两台 PM 会导致数据丢失。如果您需要同时停止两个 PM，则关闭 ztC Edge 系统(这也会关闭虚拟机 (VM))，如[关闭系统中](#)所述。
2. 不要将 -f(强制执行)选项与 PM 主机操作系统的 halt、poweroff 或 reboot 命令一同使用。这样做会导致在同一 PM 上处于活动状态的客人挂起。
3. 当您关闭 PM 时，ztC Edge 系统没有容错特性。为实现持续正常运行，尽快使脱机 PM 恢复使用。



注意：当您关闭 PM 时，待机电源仍开启，以实现无人值守管理，除非您断开了电源线的连接或交流主电源已关闭。

要关闭 PM ztC Console 中的

要关闭 PM，您必须使该 PM 进入维护模式，这会将该 PM 上运行的所有 VM 均迁移到剩余 PM(如果存在)上。在具有两个节点的系统中，在此过程中这些 VM 会继续运行，这需要一两分钟。

1. 确定您要关闭哪个 PM。
2. 在 ztC Console 中，单击左侧导航面板中的**物理机**。

3. 选择相应的 PM(`node0` 或 `node1`, 如果存在), 然后单击 **Work On(维护模式)**, 这会将该 PM 的总体状态更改为**维护模式**, 以及将**活动**状态更改为**正在运行(维护中)**。
4. 在 PM 显示**正在运行(正在维护)**后, 单击**关闭**。

PM 已关闭后, 其活动状态为 **✘关闭(维护中)**。您必须手动重启该 PM。

要使用电源按钮关闭 PM

您还可以使用 PM 上的电源按钮关闭 PM。在已授权用于两个节点的系统上, 在此过程中这些 VM 会继续运行, 这需要一两分钟。

1. 当两个 PM 都在运行时, 按下然后松开您要关闭的 PM 的前面板上的电源按钮。
2. 系统会自动使该 PM 进入维护模式, 这会将该 PM 上运行的 VM 迁移到剩余 PM 上。
3. 该 PM 自动关闭。

当 PM 关闭时, 前面板上的 **PWR LED** 熄灭, 但仍有待机电源。您必须手动重启该 PM。

要使用电源按钮强制关闭 PM



小心: 如果在您单击**关闭**或按下电源按钮后 PM 没有关闭, 您可能需要强制关闭 PM。强制关闭 PM 会破坏其内存状态; 因此仅将其用作最后手段。

按住 PM 上的电源按钮几秒钟可强制断电。

当 PM 关闭时, 前面板上的 **PWR LED** 熄灭, 但仍有待机电源。您必须手动重启该 PM。

相关主题

[维护模式](#)

[ztC Console](#)

[管理物理机](#)

[“物理机”页](#)

负载均衡

在已授权用于两个节点的系统上, HA 负载均衡在两台 PM 上分配 VM 来提高性能和可用性。负载均衡是按 VM 配置的, 在 ztC Edge 系统上自动启用。(已授权用于一个节点的系统不提供负载均衡。)

如果某个 PM 停止运行, 所有 VM 将在其余的 PM 上运行。一旦 VM 要在其上运行的目标 PM 恢复运行且完全同步, 它们就会自动迁移回该 PM。

操作模式

VM的负载均衡是在**虚拟机**页面上的**负载均衡**选项卡内设置的。支持以下模式：

- **自动均衡**。这种模式为 VM 提供自动负载均衡。当一个 VM 被设置为自动均衡时，它将在资源最多的可用 PM 上运行。当系统发现可以通过移动一个或多个采用自动设置的 VM 实现更好的负载均衡时，将发出警报。该警报显示在仪表板上，刊头上将显示负载均衡通知。为响应此警报，单击刊头中的**负载均衡**可启动 VM 的自动负载均衡。

当前 PM 列下**虚拟机**页面上的图标指示将立即迁移的 VM。

- **手动放置在节点 N 上**。愿意时，高级用户可以为各个 VM 手动分配首选 PM(节点)，而不是使用自动策略。

虚拟机页上各 VM 的**当前 PM**列内将显示一个图形。该图形指示 VM 的当前负载均衡状态、VM 运行所在 PM 以及其首选项。

在下面的图形示例中，VM 当前正在 PM 0 上运行，其首选项是 PM 1。



ztC Edge策略确保 VM 始终运行。当一台 PM 被预测到将发生故障、正在维修或停止运行时，VM 将在另一台正常 PM 上运行。当两台 PM 都正常时，VM 迁移到其首选 PM。

相关主题

[为虚拟机选择首选 PM](#)

物理机故障排除

以下主题描述 PM 的故障排除方法：

- [恢复故障物理机\(手动\)](#)

如果您无法使用这些基于软件的故障排除程序中的一个恢复PM，请参阅[维护物理机](#)，了解有关更换物理 PM 硬件的信息。

恢复故障物理机(手动)



小心: 如果您需要恢复或替换 **ztC Edge**系统中的 **PM**, 则使用 [ztC Edge 100i/110i 系统: 更换节点 \(R013Z\)](#) 中的说明。(如果需要, 请参阅[替换物理机\(自动\)](#), 了解其他详细信息)。除非您的授权 **Stratus** 服务代表具体说明, 否则不要使用本主题中描述的手动程序。

恢复不能启动或者无法成为 **ztC Edge**系统的物理机 (**PM**) 的物理机或节点。有些情况下, **ztC Console**会把故障 **PM** 的状态显示为**不可及(正在同步/撤出)**。

要恢复一台 **PM**时, 您必须重新安装此 **PM** 一直在运行的 **Stratus Redundant Linux**版本。不过, 故障 **PM** 的恢复与首次安装软件不同。恢复操作保留所有数据, 但只是重新创建 **/boot** 和根文件系统、重新安装 **Stratus Redundant Linux**系统软件并尝试连接已有系统。(如果您需要更换物理 **PM** 硬件, 而不是恢复系统软件, 请参阅[更换物理机\(手动\)](#)。)

要重新安装系统软件, 您可以使系统自动从主 **PM** 上的临时预启动执行环境 (**PXE**) 服务器启动更换节点。只要每个 **PM** 均包含最近安装的软件套件(如在 **ztC Console**的[升级套件](#)页上显示的)的完整副本, 任何一个 **PM** 均能够通过 **PXE** 启动安装开始其配对 **PM** 的恢复。如果需要, 您还可以从 **USB** 安装介质手动启动替换节点。

根据在安装(**PXE** 或 **USB** 安装)中您要使用的介质, 使用以下操作程序之一。



小心: 此恢复程序会删除在 **PM** 的主机操作系统中安装的所有软件, 以及在恢复前输入的所有 **PM** 配置信息。完成此程序后, 您必须手动重新安装所有主机级软件, 并配置 **PM** 以匹配您的初始设置。

先决条件：

1. 确定需要恢复的 PM。
2. 如果您要使用 USB 介质在更换 PM 上安装系统软件，则创建一个可启动 USB 介质，如 [创建具有系统软件的 USB 介质](#) 中所述。



在创建 USB 介质时，确保其包含最近安装的升级套件。例如，如果 ztC Console 窗口刊头中显示的版本为版本 1.2.0-550(其中 550 是创建号)，则在 **升级套件** 页上您选择创建 USB 介质的套件也必需是版本 1.2.0-550。如果系统检测到目标 PM 上有其他版本，系统会自动覆盖此恢复过程，**初始化目标 PM 上的所有数据**，以及使用 PXE 启动安装在该 PM 上重新安装最近安装的软件套件，无需用户交互。

3. 如果使用 USB 介质，则将键盘和监视器连接到更换 PM，以便监视此安装过程并指定设置。

要恢复 PM(使用 PXE 启动安装)

使用以下程序，通过使用 PXE 启动安装从主 PM 上的软件套件重新安装系统软件来恢复 PM。

1. 在 ztC Console 中，单击左侧导航面板中的 **物理机**。
2. 选择相应的 PM(node0 或 node1)，然后单击 **维护模式**，这会将该 PM 的 **总体状态** 更改为 **维护模式**，以及将 **活动状态** 更改为 **正在运行(维护中)**。
3. 在 PM 显示 **正在运行(维护中)** 后，单击 **恢复**。
4. 在提示选择修复类型时，单击 **PXE PM 恢复 - 保护数据**。



小心：务必选择 **PXE PM 恢复：保护数据**；否则安装过程可能会删除目标 PM 上的数据。

5. 单击 **继续**，开始此恢复过程。在准备重新安装系统软件时，系统重启目标 PM。
6. 此恢复过程在无用户交互的情况下继续进行，如下：
 - 目标 PM 开始从临时运行于主节点的 PXE 服务器启动。
 - 目标 PM 自动开始系统软件安装，这是从主节点上的安装套件副本中运行的。
 - 此安装过程会重新安装系统软件，同时保护所有数据。

您无需监视此软件安装进程或响应目标 PM 的物理控制台上的提示。此恢复过程是自动的，在安装过程中，PM 通常会长时间显示空白屏幕。

7. 完成软件安装后，目标 PM 会从最新安装的系统软件重启。
8. 在目标 PM 启动过程中，您可以在 的物理机 ztC Console 页上查看其活动。恢复完成后，**活动列**将该 PM 显示为**(维护中)**。
9. 如果适用，手动重新安装应用程序和任何其他主机级软件，并重新配置 PM 以匹配您的初始配置。
10. 在您准备将目标 PM 联机时，单击**退出维护**，以便退出维护模式。验证这两个 PM 是否均返回到**运行**状态，以及它们是否完成了同步。



注意：当目标 PM 退出维护模式时，系统会禁用曾用于此恢复过程的主节点上的 PXE 服务器。

要恢复 PM(使用 USB 安装)

使用以下操作程序，通过从 USB 介质重新安装系统软件。

1. 在 ztC Console 中，单击左侧导航面板中的**物理机**。
2. 选择相应的 PM(node0 或 node1)，然后单击**维护模式**，这会将该 PM 的**总体状态**更改为**维护模式**，以及将**活动状态**更改为**正在运行(维护中)**。
3. 在 PM 显示**正在运行(维护中)**后，单击**恢复**。
4. 在提示选择修复类型时，单击 **USB PM 恢复 - 保护数据**。



小心：务必选择 **USB PM 恢复：保护数据**；否则安装过程可能会删除目标 PM 上的数据。

5. 单击**继续**，开始此恢复过程。在准备重新安装系统软件时，系统关闭目标 PM。
6. 将可启动 USB 介质连接到目标 PM 上，然后手动启动此 PM。
7. 在目标 PM 启动过程中，进入固件(UEFI)设置实用程序。在**保存并退出菜单**的**直接启动**下，选择 **UEFI** 条目，以便使该 USB 介质在下一个启动顺序中一次从设备启动。此 PM 重启。



注意：使用**直接启动**属性临时更改启动设备，而不是在**启动**菜单中修改永久**启动顺序优先级**。最高启动优先级必须保持**UEFI 网络**(默认)才能支持一般在 ztC Edge 系统上执行的自动节点更换。

8. 在目标 PM 的物理控制台上监视此安装过程。
9. 在**欢迎**屏幕上，使用箭头键为此安装选择国家/地区键盘布局。
10. 在**安装或恢复**屏幕上，选择**恢复 PM, 联合系统:保留数据**，然后按 **Enter** 键。此恢复过程在无用户交互的情况下继续进行。



小心：务必选择**恢复 PM, 联合系统:保留数据**；否则安装过程可能会删除目标 PM 上的数据。

11. 完成软件安装后，目标 PM 会从最新安装的系统软件重启。
12. 在目标 PM 启动过程中，您可以在 的物理机 ztC Console 页上查看其活动。恢复完成后，**活动列**将该 PM 显示为**(维护中)**。
13. 如果适用，手动重新安装应用程序和任何其他主机级软件，并重新配置 PM 以匹配您的初始配置。
14. 在您准备将目标 PM 联机时，单击**退出维护**，以便退出维护模式。验证这两个 PM 是否均返回到**运行**状态，以及它们是否完成了同步。

相关主题

[维护模式](#)

[管理物理机](#)

[ztC Console](#)

[“物理机”页](#)

6

第 6 章：管理虚拟机

管理虚拟机 (VM) 来控制其运行、分配其资源或配置其客人操作系统和应用程序。

您可以在 **ztC Console** 的 **虚拟机** 页面上管理 VM，该页面的访问方法见“[虚拟机](#)”页。关于具体管理工作的执行，请参阅下面的主题。

要管理 VM 运行状态时，请参阅：

- [启动虚拟机](#)
- [关闭虚拟机](#)
- [关闭虚拟机电源](#)
- [打开虚拟机控制台会话](#)
- [重命名虚拟机](#)
- [移除虚拟机](#)

要显示有关 VM 的信息，则使用 `snmptable` 命令(请参阅 [使用 snmptable 获取系统信息](#))。

要创建或配置 VM 时，请参阅：

- [计划虚拟机资源](#)(虚拟 CPU、内存、存储和网络)
- [创建和迁移虚拟机](#)
- [管理虚拟 CD](#)
- [配置基于 Windows 的虚拟机](#)
- [配置基于 Linux 的虚拟机](#)
- [管理虚拟机资源](#)

要将 USB 设备附加到 VM，请参阅[将USB 设备附加到虚拟机](#)。

要执行高级工作时，请参阅：

- [将特定 MAC 地址分配给虚拟机](#)
- [为虚拟机选择首选 PM](#)
- [更改虚拟机的保护级别\(HA 或 FT\)](#)
- [配置虚拟机的启动顺序](#)
- [为故障虚拟机重置 MTBF](#)

VM 管理员的本地用户角色可执行其中许多任务。具体讲，VM 管理员能够：

- 执行“虚拟机”页上的可用功能按钮和操作的任務。
- 查看“虚拟机”页。
- 从“虚拟 CD”页创建和删除 VCD。

有关分配 VM 管理员角色的信息，请参阅[管理本地用户帐户](#)。

计划虚拟机资源

在创建虚拟机时，需要对系统资源的分配进行规划，以最大程度地提高系统性能和连续正常运行时间。

要规划虚拟机的资源分配时，请参阅：

- [计划虚拟机 vCPU](#)
- [计划虚拟机内存](#)
- [计划虚拟机存储](#)
- [计划虚拟机网络](#)

计划虚拟机 vCPU

分配虚拟 CPU (vCPU) 来把计算资源分配给 ztC Edge 系统上的虚拟机 (VM)。

在把 vCPU 分配给 VM 时，必须考虑如下信息和限制：

- 各 vCPU 代表处理能力的一个虚拟单元。系统上的可用 vCPU 总数等于系统的两台物理机 (PM) 提供的硬件线程数中的较少者。例如，假如在一个系统中，一台 PM 有 4 个内核、每个内核 2 个线程(8 个 vCPU)，第二台 PM(在该系统中)有 8 个内核、每个内核 2 个线程(16 个 vCPU)，那么可用 vCPU 总数就是 8 个 vCPU(两台 PM 中的较少线程数)。

- 可用于 VM 的 vCPU 数等于系统上的 vCPU 总数。
- 您可以分配给任何一个 VM 的最大 vCPU 数是系统内的可用 vCPU 总数。
- 基于 Windows 的 VM: 在把分配的 vCPU 数从 1 改为 n 或者从 n 改为 1 时, 在重配(参阅[重新配置虚拟机资源](#))过程结束并重启 VM 后, 您必须再次关闭后重启 VM。这可使 VM 对自身进行正确重新配置, 以实现对称多处理 (SMP)。在重启前, VM 显示奇怪行为, 并且无法使用。
- ztC Console 的 **系统** 页面(参阅[“系统”页](#))上将显示 vCPU 总数、已分配给 ztC Edge 系统软件的 vCPU 数、运行 VM 占用的 vCPU 数和空闲 vCPU 数。
- Stratus Redundant Linux 软件允许超量配给 vCPU。当 **系统** 页面上的空闲 vCPU 数小于零时, 表明您已经超量配给 vCPU; 控制台将指示这种情况, 并显示 vCPU 的估计超量配给程度。
- vCPU 超量配给不会妨碍您创建或启动 VM; 不过, 最好避免在超量配给状态下运行系统。

超量配给虚拟 CPU 时的考虑事项



注意: 一般而言, 应避免超量配给 VM 资源。最好隔离各 VM 的资源来防止 VM 受到其他可能存在资源泄漏或意外性能峰的 VM 的影响。在创建和配置 VM 时, 应分配不允许其他 VM 使用的专用资源。

仅在如下条件下才能超量配给物理 CPU:

- VM 的 vCPU 资源占用总和峰值不超过 ztC Edge 系统的物理资源。
- 有一个或多个 VM 是在不同时间使用的(比如非高峰备份)。
- 在其他虚拟机运行时, 一台或多台 VM 将停止, 比如在 VM 升级时或进行 VM 时间点备份或恢复时。
- VM 的 CPU 使用总量峰值不会影响服务水平协议或要求的响应时间。
- 很好地理解各 VM 的 CPU 使用, 确保其应用不易受资源泄漏影响。当 CPU 超量配给时, 一个 VM 的泄漏可能会影响其他 VM 的性能。

相关主题

[系统要求概述](#)

[创建和迁移虚拟机](#)

[管理虚拟机资源](#)

计划虚拟机内存

分配内存来把物理内存分配给 ztC Edge 系统上的虚拟机 (VM)。

在把内存分配给 VM 时，必须考虑如下信息和限制：

- 可以分配给 VM 的总内存等于 ztC Edge 系统上的可用内存总量(请参阅[系统要求概述](#))减去已分配给 ztC Edge 系统软件。例如，假如内存总量为 32 GB，并且 2 GB，那么，可供 VM 使用的内存就是 30 GB。
- 对于已授权用于两个节点的系统，您可以把可供 VM 使用的全部内存分配给一个 VM。每一个 VM 都占用其请求的内存量外加 20% 的系统开销内存。
- 最小内存分配量为 256 MB，不过，64 位操作系统需要 600 MB 以上。必须确认客人操作系统的内存要求。
- ztC Console 的 **系统** 页面(参阅[“系统”页](#))上显示了内存总量、已分配给 ztC Edge 系统软件的内存量、正在运行的 VM 占用的内存量和空闲内存量。请使用该页面检查内存分配。
- Stratus Redundant Linux 软件不允许为 **运行 VM 过量配给内存**；当超出物理机的总物理内存时，将无法启动 VM。仅当一个或多个 VM **停止**而其他虚拟机在运行时，例如在升级 VM 或进行 VM 时间点备份或恢复时，才有可能安全地过量配给内存。
- 必要时，可以手动重新分配内存：关闭或重新配置一个或多个利用不足的 VM，然后把可用资源再分配给负荷较高的 VM。

相关主题

[系统要求概述](#)

[创建和迁移虚拟机](#)

[管理虚拟机资源](#)

计划虚拟机存储

规划 ztC Edge 系统上的存储分配，以确保具备虚拟机 (VM) 和系统管理所需的空间。

在为您的虚拟机 (VM) 分配存储时，应考虑采取如下措施：

- 遵守存储最大值

Stratus Redundant Linux 软件不允许过量配给存储。所有 VM 和 VCD 所需存储的总和不得超过 ztC Edge 系统内的可用存储总量。
- 为增加更多 VCD 预留存储空间

在预留至少 5 GB 的可用空间，以便为安装更多 VM 和应用程序创建 VCD。(为了节约这种空间，可以在使用完 VCD 后将其删除。)

- 为各 VM 创建单独的启动卷和数据卷

在第一个(启动)卷上安装客人操作系统和应用程序，并为相关数据另外创建卷。把启动卷和数据卷分开有助于保护数据，并且在启动卷崩溃时可以更容易地恢复 VM。

- 创建一个容量足够客人操作系统和内务开销使用的启动卷

遵守客人操作系统的最低空间要求，而且，考虑到卷和空间使用的格式化容量，应分配略多一些空间。例如，假如在创建 VM 时为启动盘分配了 5 GB，启动卷格式化容量在使用前大约为 4.8 GB，这可能不能满足 5 GB 要求。

- 遵循最大卷大小。

当导出、导入或还原卷时，注意最大卷大小，如[重要注意事项](#)中所列。

相关主题

[创建和迁移虚拟机](#)

[管理虚拟机资源](#)

计划虚拟机网络

规划网络资源来确定如何为 ztC Edge 系统上的虚拟机 (VM) 分配可用虚拟网络。

当您部署系统时，在已授权用于两台 PM 的系统上，软件把两台物理机 (PM) 上的物理网络端口对捆绑起来形成冗余虚拟网络。在创建或重配 ztC Edge 系统上的 VM 时，可以把 VM 连接到虚拟网络，而不是物理网络端口。对于已授权用于两个节点的系统，软件把两台物理机 (PM) 上的物理网络端口对捆绑起来形成冗余虚拟网络。

在把 VM 连接到虚拟网络时，必须考虑如下信息和限制：

- 可以把一个 VM 连接到多个虚拟网络时，也可以把多个 VM 连接到同一个虚拟网络。
- Stratus Redundant Linux 软件允许无限超量配给网络资源；所以，在分配虚拟网络时，必须确定 VM 的网络带宽/响应时间要求。
- 当多个 VM 共享同一个虚拟网络时，这些 VM 将平等共享可用网络带宽。与 vCPU 容量不同，没有办法按比例分配带宽资源。所以，当一个 VM 占用大量网络带宽时，会导致网络上所有 VM 的性能下降。当一个 VM 的带宽要求很高时，应考虑为该 VM 连接一个专用虚拟网络。

相关主题

[一般网络要求和配置](#)

[创建和迁移虚拟机](#)

[管理虚拟机资源](#)

创建和迁移虚拟机

通过创建一个新 VM、通过网络直接迁移原有的 VM 或物理机 (PM) 或者从原有 VM 导入一个开放虚拟化格式 (OVF) 文件或开放虚拟化设备 (OVA) 文件在系统上生成一个新的虚拟机 (VM)。

要创建一个新 VM 时(不需要已有的源 VM 或 PM)，请参阅[创建新虚拟机](#)。

要将现有 VM 复制到系统上，以便创建新 VM 或创建用于故障排除的副本 VM，请参阅[复制虚拟机](#)。

要从另一个系统迁移或导入 VM，或者要在同一系统上还原 VM，请参阅下列一个主题：

- [将物理机或虚拟机迁移到系统](#)

使用 P2V 客户端 ([virt-p2v](#)) 通过网络直接把一个 PM 或 VM 转变为系统上的一个新 VM。

- [导出虚拟机](#)

使用 ztC Console 将源 VM 导出到网络共享上的 OVF 和 VHD 文件。

- [导入 OVF 或 OVA 文件](#)

使用 ztC Console 将 OVF 和 VHD 文件从另一个 ztC Edge 系统导入 ztC Edge 系统，或者将 OVF 和 VHD 文件或 OVA 文件从基于 VMware vSphere 的系统导入 ztC Edge 系统。

- [从 OVF 文件替换/还原虚拟机](#)

使用 ztC Console 将 OVF 和 VHD 文件导入回系统，以从之前的备份副本覆盖和还原现有 VM。

相关主题

[管理虚拟机](#)

创建新虚拟机

创建一个新虚拟机，以便在您的 ztC Edge 系统上安装客人操作系统。(您还可以迁移现有 VM 或物理机 (PM)，如在[创建和迁移虚拟机](#)中总结的。)

启动 **VM 创建向导**，操作是单击 **创建** – 在 **虚拟机** 页上。此向导将帮助您逐步完成将资源分配给 VM 的过程。

先决条件：

- 查看将 CPU、内存、存储和网络资源分配给 VM 的前提条件和注意事项，如 [计划虚拟机资源](#) 中所列出的。
- 您可以创建运行支持的客人操作系统和启动界面的 VM，如 [经过测试的客人操作系统](#) 中所述。
- 您可以选择将远程 ISO 或可启动虚拟 CD (VCD) 作为 VM 启动的源。对于远程 ISO，您必须有存储库的 URL 或路径名称，对于共享网络驱动器上的远程 ISO，您必须有用户名和密码。如果您需要 Windows 或 Linux 安装介质的可启动 VCD，则按照 [创建虚拟 CD](#) 中所述的方式创建它。可启动 VCD 必须为单张 CD 或 DVD。不支持多张 CD 或 DVD。
- 确保 ztC Edge 系统的两台 PM 在线并已连接到网络；否则，系统将无法正确创建 VM。

要创建一个新 VM

1. 在已授权用于两个节点的系统的 **物理机** 页面(参阅 [“物理机”](#) 页)上，确认两台 PM 都处于运行状态，并且两台 PM 都不是处于维护模式或正在进行同步。
2. 在 **虚拟机** 页(请参阅 [“虚拟机”](#) 页)上，单击 **创建**，打开 **VM 创建向导**。
3. 在 **名称、描述、保护和 OS** 页上：
 - a. 键入此 VM 的 **名称** 和可选 **描述** – 当它们显示在 ztC Console 中时。

此 VM 名称必须符合以下要求：

- VM 名称的开头必须是单词或数字，并且名称不能包含特殊字符(例如，#、% 或 \$)。
 - VM 名称不能使用带有连字符的前缀，例如 **Zombie-** 或 **migrating-**。
 - VM 名称最多具有 85 个字符。
- b. 选择将对此 VM 使用的保护级别：
 - **容错 (FT)** – 通过为运行于两个物理机间的 VM 创建冗余环境，透明地保护应用程序。对于需要的停机保护比 HA 提供的还要大的应用程序，使用 FT。

- **高可用性 (HA)** – 提供基本故障转移和恢复，一些故障需要(自动)VM 重启才能恢复。对于能够容忍一些停机时间并且不需要 FT 提供的停机保护的应用程序，使用 HA。

关于这些保护水平的更多信息，请参阅[操作模式](#)。

c. 对于**启动界面**，选择下列一项：

- **BIOS**–基本输入/输出系统
- **UEFI**–统一可扩展固件界面

注释：



1. 确保客人操作系统支持您选择的**启动界面**；否则，客人操作系统将无法启动。有关客人操作系统和 ztC Edge系统支持的启动界面的列表，请参阅[经过测试的客人操作系统](#)。
2. 您仅在创建 VM 时才能设置**启动界面**。以后您无法修改此设置。

d. 对于**启动自**，选择下列一项作为启动源：

- **VCD** – 启动源为 VCD。从下拉菜单中选择一个源。
- **通过 Windows 共享的远程 ISO (CIFS/SMB)** – 该启动源为共享网络驱动器上的远程 ISO 文件。您必须为**用户名**和**密码**输入值。对于**存储库**，输入格式为 `\\machine_URL\ShareName` 的值(例如，`\\192.168.1.34\MyISO_Folder`)。
- **通过 NFS 的远程 ISO**– 该启动源为通过 NFS 访问的远程 ISO 文件。对于**存储库**，以 `nnn.nnn.nnn.nnn` 格式(不包含 `http://` 或 `https://`)输入远程系统的 URL。

对于可用 ISO 存储库的列表，则单击**列出 ISO**，然后选择一个 ISO 文件。所选 ISO 文件的完整路径名称显示在**存储库**下。您无法编辑已显示的 ISO URL。

e. 单击**下一步**。

4. 在**VCPU 和内存**页上：

- a. 指定要分配给 VM 的**vCPU**数和**内存**量。有关更多信息，请参阅[计划虚拟机 vCPU](#)和[计划虚拟机内存](#)。
- b. 单击**下一步**。

5. 在卷页上：
 - a. 键入此启动卷的**名称** – 当它们显示在 **ztC Console** 中时。
 - b. 键入**卷大小**，单位为千兆字节 (GB)。有关分配存储的更多信息，请参阅[计划虚拟机存储](#)。
 - c. 如果适用，通过单击**添加新卷**以及为每个卷指定参数，创建额外数据卷。(在创建 VM 后，您还可通过使用**重新配置虚拟机**向导添加卷，如在[虚拟机中创建卷](#)中所述。)
 - d. 单击**下一步**。
6. 在**网络**页上，选择要附加到 VM 的共享网络(有关更多信息，请参阅[计划虚拟机网络](#))。您还可以启用(或禁用)该网络以及指定 MAC 地址。要继续，单击**下一步**。
7. 在**创建摘要**页上：
 - a. 查看创建摘要。如果您需要进行更改，则单击**后退**。
 - b. 如果您想阻止控制台会话自动启动以观察软件安装，则取消选择**启动控制台**。
 - c. 要接受如所配置的 VM 并开始软件安装，则单击**完成**。

VM 创建向导显示创建进度并打开控制台窗口(如果适用)。当控制台窗口打开时，控制台可能需要一分钟才能连接到 VM。

8. 对于基于 Windows 的 VM，当 VM 控制台打开时，单击控制台窗口内部，并准备按任意键，以便从 VCD 或远程 ISO 运行 **Windows 安装程序**。

```
Press any key to boot from CD or DVD...
```

对于具有 UEFI 启动类型的基于 Windows 的 VM，您需要在一或两秒内按一个键；否则将显示 **UEFI 交互式 Shell**。如果发生这种情况，您可以按照以下方式恢复并运行 **Windows 安装程序**：

- a. 在 **UEFI 交互式 Shell** 中，在 Shell> 提示符下，键入 **exit**，然后按 **Enter**。

```
Shell> exit
```

- b. 使用箭头键选择**继续**，然后按 **Enter**。

```
Select Language
```

```
Device Manager
```

```
Boot Manager
```

```
Boot Maintenance Manager
```

Continue

Reset

- c. 在 VM 重启时，按任何键，从 VCD 或远程 ISO 运行 **Windows 安装程序**。

Press any key to boot from CD or DVD...

- d. 如果您没有按任何键，则会再次显示 **UEFI 交互式 Shell**，重复步骤 a-c。

9. 如果适用，可在 VM 控制台会话中观察操作系统的安装进度(必要时允许在浏览器中弹出)，并对弹出的任何提示做出响应。

10. 安装操作系统后，配置生产使用所需的额外资源和软件，如以下部分中所述：

- [配置基于 Windows 的虚拟机](#)
- [配置基于 Linux 的虚拟机](#)



小心：在安装过程完成后进行最后重启之前，如果主 PM 发生故障或 VM 崩溃，则可能需要重新开始 VM 的安装。

如果中止了以下任何安装，VM 会无法重启：

- 客人操作系统，包括配置步骤
- 操作系统文件的任何中间件或应用程序

相关主题

[复制虚拟机](#)

[重命名虚拟机](#)

[移除虚拟机](#)

[创建和迁移虚拟机](#)

[管理虚拟机资源](#)

[管理虚拟机的运行](#)

复制虚拟机

如果您希望在您的 ztC Edge 系统中克隆现有 VM，则复制虚拟机 (VM)。例如：您可以复制正常 VM，以创建新 VM；或者您可以复制未正确运行的 VM，并使用此副本进行故障排除。(如果您要从其他系统导入或迁移 VM，请参阅 [创建和迁移虚拟机](#) 中的概述。)

要复制 VM，请选择**虚拟机**页面中的 VM，然后单击**复制**。此向导将帮助您逐步完成重命名以及将资源分配到新 VM 的过程。

复制 VM 后将创建具有唯一 SMBIOS UUID、系统序列号、MAC 地址和硬件 ID 的相同 VM。

注释：

- 为防止与源 VM 冲突，复制向导会自动为新 VM 中的每个网络接口分配一个新 MAC 地址；但在需要时您可能需要手动更新任何 IP 地址和主机名称。
- 在复制 VM 的同时，如果 ztC Edge 系统从主 PM 切换到辅助 PM，则复制过程将停止。这不会影响系统的连续正常运行时间，但是您必须删除与已复制的 VM 关联的任何卷，并重启副本。

先决条件：

- 进行复制前，必须关闭 VM。
- ztC Edge 系统的两台 PM 都必须在线，此复制过程才能正确执行。

要在 ztC Edge 系统上复制 VM

1. 在已授权用于两个节点的系统的**物理机**页面(参阅[“物理机”页](#))上，确认两台 PM 都处于运行状态，并且两台 PM 都不是处于维护模式或正在进行同步。
2. 在**虚拟机**页面(请参阅[“虚拟机”页](#))上，选择要复制的 VM，然后单击**关闭**。
3. 此 VM 停止后，单击**复制**，打开复制向导。
4. 在**名称、描述和保护**页上：
 - a. 键入此 VM 的**名称**和可选**描述** – 当它们显示在 ztC Console 中时。
 - b. 选择将对此 VM 使用的保护级别：
 - **容错 (FT)**
 - **高可用性 (HA)**有关这些保护级别的更多信息，请参阅[创建新虚拟机](#)和[操作模式](#)。
 - c. 单击**下一步**。
5. 在**VCPU 和内存**页上：
 - a. 指定要分配给 VM 的 **vCPU** 数和**内存**量。有关更多信息，请参阅[计划虚拟机 vCPU](#)和[计划虚拟机内存](#)。

- b. 单击**下一步**。
6. 在**卷**页上，您可以：
 - 键入**卷名称**。
 - 指定每个卷的**卷大小**。
 - 单击**添加新卷**，以便创建一个新数据卷。(如果没有显示该按钮，则向下滚动到此向导页的底部。)

有关更多信息，请参阅[计划虚拟机存储](#)。要继续，单击**下一步**。

7. 在**网络**页上，激活要附加到 VM 的各共享网络的复选框。
8. 在**复制摘要**页上：
 - a. 查看配置摘要。如果您需要进行更改，则单击**后退**。
 - b. 要继续复制 VM，单击**完成**。

复制过程完成后，ztC Edge系统可能继续同步 PM 之间的数据，以启用高可用性(HA)或容错(FT)操作。

故障排除

必要时，使用如下信息解决在复制过程中遇到的问题。

要在复制过程取消或失败后进行清理

移除与此已复制 VM 关联的任何卷。

相关主题

[创建和迁移虚拟机](#)

[管理虚拟机资源](#)

[管理虚拟机的运行](#)

将物理机或虚拟机迁移到系统

迁移一台物理机 (PM) 或虚拟机 (VM) 来通过网络将其传输到系统上的一个新 VM。(您还可以将开放虚拟化格式 (OVF) 或开放虚拟化设备 (OVA) 文件导入到系统，如[创建和迁移虚拟机](#)中所总结的。)

以下操作程序描述了如何通过网络迁移 PM 或 VM: 下载 **P2V 客户端 (virt-p2v)** ISO 文件，在源 PM 或 VM 上启动此 P2V 客户端 ISO 文件，然后使用该客户端配置、初始化和监视来自源侧的安全网

络传输。在迁移完成之前，系统上不需要配置步骤，不过，当新 VM 的关联卷开始出现时，您可以在 ztC Console 的卷页面上确认迁移正在进行。



小心：考虑在准备迁移之前备份源 PM 或 VM。

注释：

- 此迁移过程支持仅运行以下操作系统的 PM 或 VM：
 - CentOS/RHEL 7.4 或 7.5
 - Microsoft Windows 7、8.x 或 10；或者 Windows Server 2008 R2、2012 或 2016。
 - Ubuntu 18.04 Server—迁移了此 VM 后，您需要执行其他程序。请参阅[完成 Ubuntu VM 的迁移](#)。
 - VMware Release 6.x
- 对于支持休眠或快速启动模式的基于 Windows 的 PM 或 VM，您必须在迁移过程之前禁用这些功能。要完全禁用休眠或快速启动模式，请参阅有关从失败的迁移（在 **Troubleshooting(故障排除)** 下显示错误消息 Failed to mount `'/dev/sda1: Operation not permitted(安装 '/dev/sda1 失败:不允许操作))` 中恢复的说明。
- 对于基于 Linux 的 PM 或 VM，考虑在迁移之前编辑 `/etc/fstab` 文件来注释数据卷项并只允许启动卷加载。由于在 ztC Edge 系统上基于 Linux 的 VM 使用不同设备名称，所以，当系统不能以原始设备名称加载卷时，新 VM 可能会以单用户模式启动。迁移完成后，可以按下面的故障排除所述使用正确设备名称恢复 `/etc/fstab` 项。
- 当迁移 VMware VM 时，除了从 VMware 控制台关闭其电源外，您还必须使用操作系统关闭命令来关闭此 VM。如果您仅使用 VMware 控制台关闭此 VM，则迁移将失败。
- 在迁移过程中，源 PM 或 VM 必须脱机。考虑为迁移安排一段计划维护时间。
- PM 或 VM 迁移所需的时间取决于源系统上卷的大小和数量以及源与目标系统之间的网络带宽。例如，通过 1Gb 的网络传输一个启动卷为 20 GB 的源系统可能需要花费大约 30 分钟。
- 一次可以迁移多个 PM 或 VM，不过，共享网络带宽可能会延长迁移时间。
- 为防止与原始 PM 或 VM 冲突，P2V 客户端会自动为新 VM 中的每个网络接口分配一个新 MAC 地址；但在需要时您必须手动更新任何 IP 地址和主机名称。
- 在迁移期间把系统从主 PM 切换到辅 PM 时，迁移过程将停止。这不影响系统的连续正常运行时间，但是必须在源 PM 或 VM 上重启 P2V 来重新开始。参阅下面的[故障排除](#)来了解更多信息。





- 迁移 PM 或 VM 后，可能没有正确安装网络驱动程序。在这种情况下，手动安装该驱动程序。参阅下面的**故障排除**来了解更多信息。



先决条件：对于已授权用于两个节点的系统，系统的两台 PM 均必须在线，迁移过程才能正确执行。在**物理机 ztC Console**页面上，确认两台 PM 都处于**运行状态**，并且两台 PM 都不是处于维护模式或正在进行同步。

执行以下迁移程序(如果适用，单击下拉菜单)。

要准备把一个 PM 迁移到 ztC Edge 系统时

1. 从以下下载 P2V 客户端 ISO 文件：此**下载**页面在 <https://www.stratus.com/services-support/downloads/?tab=ztcedge>.
 - a. 在**下载**页上，单击**ztC Edge**(如果其尚未显示)，然后选择相应的版本。
 - b. 向下滚动到**驱动程序和工具**，然后继续滚动到**ztC Edge 用于虚拟机或物理机迁移的 P2V 客户端**。
 - c. 选择**P2V Client (virt-p2v)** 文件。

2. 如果您要验证 ISO 映像的完整性，还要下载关联的 fciv 校验和文件，然后从 Microsoft 支持网站下载 Microsoft 文件校验和完整性验证程序 (FCIV) 可执行文件。将这两个文件保存到包含已下载的 ISO 文件的目录中。

打开命令提示符。从包含该 ISO、可执行文件和验证文件的目录，键入与以下类似的命令来验证此 ISO 映像：

```
fciv -v -xml virt-p2v-n.n.n-n.nnnnnnnn.n.el6.centos.xml
```

如果该命令**执行成功**(也就是说，返回消息所有文件均已成功验证)，则转到下一步。如果该命令**执行失败**，则重新下载。

3. 把这个 P2V 客户端 ISO 文件刻录到您将用于启动源 PM 的 CD-ROM。
4. 把 P2V 客户端 CD 插入源 PM 的 CD/DVD 驱动器内。
5. 在准备启动 P2V 客户端时，关闭 PM。

要准备把一个 VM 迁移到 ztC Edge 系统时

1. 从**驱动程序和工具**部分下载 P2V 客户端 ISO 文件此**下载**页面在 <https://www.stratus.com/services-support/downloads/?tab=ztcedge>。请确保您下载的 P2V 客户端版本与您正在将 VM 迁移到 ztC Edge 系统的版本相匹配。

2. 如果您要验证 ISO 映像的完整性, 还要下载关联的 `fciv` 校验和文件, 然后从 Microsoft 支持网站下载 Microsoft 文件校验和完整性验证程序 (FCIV) 可执行文件。将这两个文件保存到包含已下载的 ISO 文件的目录中。

打开命令提示符。从包含该 ISO、可执行文件和验证文件的目录, 键入与以下类似的命令来验证此 ISO 映像:

```
fciv -v -xml virt-p2v-n.n.n-n.nnnnnnnn.n.el6.centos.xml
```

如果该命令 执行成功 (也就是说, 返回消息所有文件均已成功验证), 则转到下一步。如果该命令 执行失败, 则重新下载。

3. 插入或连接 P2V 客户端 ISO 文件至源 VM, 在关联管理程序中把虚拟 CD 驱动器设置为启动设备。
4. 在准备启动 P2V 客户端时, 关闭 VM。

要把一个 PM 或 VM 迁移到 ztC Edge 系统时

1. 打开源 PM 或 VM 来启动 P2V 客户端。一分钟左右之后, 将显示 **virt-p2v** 窗口。
2. P2V 客户端通过 DHCP 自动获取网络设置。该迁移过程不需要进行静态设置, 但是您可以选择性地单击 **配置网络** 以指定这些设置。(必要时, 可稍后在 ztC Edge 系统中配置目标 VM 的网络设置。)
3. 为 **转换服务器** (ztC Edge 系统) 输入连接设置。输入系统的主机名或 IP 地址和 **根** 账户的密码。(您必须按 [访问主机操作系统](#) 所述使用 ztC Edge 主机操作系统的根账户。)
4. 单击 **测试连接**。如果 P2V 客户端连接至 ztC Edge 系统, 则单击 **下一步**, 继续。将显示一个具有以下部分的页面: **Target properties** (目标属性)、**Fixed hard disks** (固定硬盘) 和其他设置。

如果 P2V 客户端未连接, 则验证连接设置并再次尝试连接。

5. 在 **Target properties** (目标属性) 部分中, 输入目标 VM 的 **Name** (名称), 该名称将显示在 ztC Console 中。(这个名称必须不同于 ztC Edge 系统上的任何原有 VM。)
6. **vCPU 的数量** 和 **内存 (MB)** 值是自动检测和填写的, 但如果希望 ztC Edge 系统上的 VM 使用比源 PM 或 VM 多的 CPU 或内存, 您也可以修改这些值。
7. 为目标 VM 指定 **Virt-v2v 输出选项**, 如下所示:

- a. 在 **Output to** (输出至) 旁, 选择 **HA** (高可用性) 或 **FT** (容错) 操作。(有关这些操作选项的信息, 请参阅 [创建新虚拟机](#) 和 [操作模式](#)。

b. 在**输出格式**旁, 选择磁盘映像格式—**原始**或**qcow2**。

8. 如果希望在迁移过程中保存调试消息, 也可选中**启用服务器端调试**复选框。(如果您按照[创建诊断文件](#)所述为您的授权 **Stratus** 服务代表生成诊断文件, 则将包含调试消息。)

9. 通过激活各设备旁的复选框, 选择要包含在迁移中的**固定硬盘**(卷)。

您必须至少选择一个卷, 包括启动卷。(由于 **P2V** 客户端是一个基于 **Linux** 的程序, 所以所有设备都是按 **Linux** 设备名称列出的, 其中 **sda** 或 **vda** 代表启动卷。)

10. 激活各设备旁边的复选框来选择将包含在迁移中的**网络接口**。

如果目标 **ztC Edge** 系统有多个共享网络, 则还可选择将与各网络接口相连接的共享网络。双击网络接口, 打开**配置网络**对话框, 然后从下拉列表中选择共享网络。

在**配置网络**对话框中, 您还可以为特定网络接口指定一个 **MAC** 地址。如果您没有指定地址, 系统会自动为每个网络接口设置 **MAC** 地址。

网络接口配置完成后, 单击**确定**。

11. 在准备好把 **PM** 或 **VM** 迁移到 **ztC Edge** 系统后, 单击**开始转换**。(由于任何原因而需要取消迁移时, 请参阅下面的[故障排除](#)。)

12. 迁移完成后, **P2V** 客户端将显示成功消息。必要时, 您可以弹出 **CD** 或虚拟 **CD** 并单击**关机**来关闭源 **PM** 或 **VM**。



注意: 迁移后, **ztC Edge** 系统上的新 **VM** 将位于主 **PM** 上, 并保持在停机状态。在启动 **VM** 之前, 按后面的程序所述完成迁移。

在 **ztC Edge** 系统上完成迁移

1. 在 **ztC Console** 中打开**虚拟机**页(请参阅[“虚拟机”](#)页)。

2. 按**重配虚拟机资源**所述, 在上部窗格中选择新 **VM**, 单击**配置**来打开**重新配置虚拟机资源**向导。使用这个向导为 **VM** 配置希望的 **vCPU**、内存、存储和网络设置:

- 如果您的源 **PM** 或 **VM** 有多个网络接口, 则配置未包含在迁移过程中的其他网络接口。
- 如果您将继续运行源 **PM** 或 **VM**, 则确保新 **VM** 上各网络接口的 **MAC** 地址与源 **PM** 或 **VM** 不同。

在最后一个向导页面上单击**完成**来实施这些修改。

3. 单击**启动**来启动新 **VM**。

4. 单击**控制台**来打开 VM 控制台，并登录到客人操作系统。(关于控制台的使用的信息，请参阅[打开虚拟机控制台会话](#)。)
5. 禁用 ztC Edge 系统上的操作不需要的任何客人操作系统服务。
 - 从 PM 源迁移时，禁用与硬件直接互动的所有服务。示例包括：
 - Dell OpenManage (OMSA)
 - HP Insight Manager
 - Diskeeper
 - 从 VM 源迁移时，禁用与其他管理程序有关联的所有服务。示例包括：
 - VMware 工具
 - Hyper-V 工具
 - 用于虚拟机的 Citrix 工具

禁用这些服务后，重新启动客人操作系统来实施您的修改。

6. 必要时，更新客人操作系统中的网络配置设置，然后重新启动客人操作系统来启用这些设置。
7. 验证您是否已使用了以下中所述的基于 Windows 或 Linux 的额外系统设置配置了您的客人操作系统：
 - [配置基于 Windows 的虚拟机](#)
 - [配置基于 Linux 的虚拟机](#)

确认新 VM 工作正确后，迁移过程完成；不过，系统可能会继续在 PM 之间同步数据来启用高可用性 (HA) 操作。

完成 Ubuntu VM 的迁移

使用 P2V 从运行某个 Ubuntu 版本的裸机迁移 VM 后，此 VM 可能会出现一些问题，例如没有活动网络。要解决此问题，则在迁移 Ubuntu VM 后执行以下相应步骤。

迁移 Ubuntu 18.04 VM 后

1. 在 ztC Console 中，打开控制台窗口，进入此 VM。
2. 登录此 VM，转到终端。
3. 输入以下命令：`cd /etc/netplan。`
4. 输入以下命令：`sudo vi 01-netcfg.yaml。`

5. 在文件 `01-netcfg.yaml` 中, 将 `eno1` 更改为 `ens3f0`。
6. 输入以下命令:`sudo netplan apply`。
7. 输入以下命令:`ifconfig`。

您无需重启 VM, 因为在发出这些命令后, 此 VM 便使用其配置的 IP 地址连接到网络。

故障排除

必要时, 使用如下信息解决在迁移过程中遇到的问题。

要取消迁移过程时

关闭运行 P2V 客户端的源 PM 或 VM。

迁移取消或失败后的清理

打开 **ztC Console**, 移除已迁移的、与源 PM 或 VM 相关的所有卷。要重新启动迁移过程时, 重新启动源 PM 或 VM 上的 P2V 客户端。

要恢复失败的迁移时

当迁移过程失败时, 源 PM 或 VM 上的 P2V 客户端上将显示一条错误消息。ztC Edge 系统上还可能显示另一条消息。使用这些消息确认问题。

如果迁移仍然失败, 则在提供了相关选项时, 启用服务器侧调试。迁移完毕后, 按 [创建诊断文件](#) 所述生成一个诊断文件并将其发送到您的授权 Stratus 服务代表。这个诊断文件内包含在迁移过程中产生的所有服务器侧调试信息。

要从失败且出现错误消息安装 `'/dev/sda1'` 失败: 不允许操作的迁移中恢复

对于基于 Windows 的 PM 或 VM, 如果该迁移过程失败并出现以下错误消息, 则可能表明已启用休眠或快速启动模式:

安装 `'/dev/sda1'` 失败: 不允许操作

NTFS 分区处于不安全状态。请继续并完全关闭 Windows (非休眠或快速重启), 或者使用 `'ro'` 安装选项安装只读卷。

要解决此问题, 则在源 PM 或 VM 中禁用休眠和快速启动:

1. 登录到源 PM 或 VM 的操作系统。
2. 打开 **Power Options(电源选项)** 控制面板，然后单击 **Choose what the power buttons do(选择电源按钮的功能)**。
3. 在 **When I press the power button(当我按下电源按钮)** 旁，选择 **Shutdown(关闭)** (而不是 **Hibernate(休眠)** 或 **Sleep(睡眠)**，如果存在)。
4. 在 **Shutdown Settings(关闭设置)** 下，清除 **Turn on fast startup (recommended)(启用快速启动(推荐))** 旁的复选框(如果存在)。
5. 单击 **Save changes(保存更改)**。
6. 打开 **Administrator Power Shell(管理员电源外壳)** 并执行以下命令：

```
> powercfg /h off
```
7. 关闭操作系统并重启迁移过程。

在新迁移的基于 Linux 的 VM 陷入“正在启动”状态时进行恢复

如果基于 Linux 的 VM 的网络脱机，则该 VM 可能无法退出正在启动状态(在 ztC Console 中)。

在迁移过程中，P2V 客户端会尝试为每个网络接口设置新的 MAC 地址，以便防止与原始 VM 发生冲突。一些基于 Linux 的操作系统检测到新的 MAC 地址，然后自动为其创建新网络接口，同时仍保留原始接口。客人操作系统启动，但在您手动配置网络设置前网络可能保持脱机状态。

要纠正该问题，则打开 VM 控制台，登录到该客人操作系统，然后更新网络启动脚本。确保对于每个网络接口您仅保留一个条目，以及每个接口均使用唯一 MAC 地址和针对您环境的正确网络设置。

ztC Edge系统上 VM 内丢失数据卷的恢复

在导入后，如果 ztC Edge系统上的 VM 内没有出现数据卷，那么，您可能需要手动恢复这些卷，方法如下：

- 关闭 VM，运行**重配虚拟机**向导，确认**卷**页面上已经有了这些卷。
- 对于基于 Windows 的 VM，使用**磁盘管理**把数据卷联机。
- 对于基于 Linux 的 VM，编辑 `/etc/fstab(/dev/vda 到 /dev/vdh)`。设备名称也可能已经改变，例如，当导入中没有卷时。

ztC Edge系统上 VM 内丢失网络设备的恢复

在导入后, 如果 ztC Edge系统上的 VM 内没有出现这些网络设备, 那么, 您可能需要手动恢复这些网络设备, 方法如下:

- 关闭 VM, 运行**重配虚拟机**向导, 确认**网络**页面上已经有了这些网络。
- 对于基于 Linux 的 VM, 重新配置网络启动脚本来使用网络接口的新设备名称。

要手动安装新的网络驱动程序

迁移 PM 或 VM 后, 可能没有正确安装网络驱动程序(例如, 设备管理器可能列出带有警告  的驱动程序)。在这种情况下, 手动安装该驱动程序:

1. 在 VM 控制台窗口中, 打开客人操作系统中的**设备管理器**。
2. 展开**网络适配器**, 然后右键单击 **Red Hat VirtIO 以太网适配器**(未正确工作的驱动程序)。
3. 选择**更新驱动程序软件**。
4. 在弹出窗口中, 单击**浏览我的计算机以查找驱动程序软件**。
5. 单击**从计算机的设备驱动程序列表中选择**。
6. 选择 **Red Hat VirtIO 以太网适配器**。
7. 单击**下一步**, 安装该网络驱动程序。

安装了该驱动程序后, 在 ztC Console 中查看 VM 的状态。如果状态为正在运行 () , 则该驱动程序正在正确工作。

相关主题

[创建和迁移虚拟机](#)

[配置基于 Windows 的虚拟机](#)

[配置基于 Linux 的虚拟机](#)

[管理虚拟机资源](#)

[管理虚拟机的运行](#)

导入 OVF 或 OVA 文件

要将 VM 从一个系统传输到另一个系统, 或者要将已创建的映像传输回同一系统来恢复或复制原始 VM 时, 可以从一个系统导入开放虚拟化格式 (OVF) 或开放式虚拟设备(或应用程序) (OVA) 文

件。(要把一台物理机 (PM) 或虚拟机 (VM) 迁移到系统而不使用 OVF 或 OVA 文件, 请参阅[将物理机或虚拟机迁移到系统](#)。)

您可以导入或还原此 VM。导入 VM 可为具有唯一硬件 ID 的 VM 创建一个新实例。还原 VM 可创建具有客人操作系统和应用程序进行软件许可时可能需要的相同硬件 ID(SMBIOS UUID、系统序列号和 MAC 地址, 如果在 VM 映像中已提供) 的相同 VM。为防止与原始 VM 发生冲突, 仅在您要将 VM 传输到 ztC Edge 系统并在源系统上停止使用它时才还原该 VM。

本主题说明如何从本地计算机、USB 设备, 或者 NFS 导出或 Windows 共享(也称为 CIFS 共享, 例如 Samba) 等远程文件系统导入 OVF 或 OVA 文件。如果要在同一系统上还原现有 VM 以覆盖此 VM 并从先前备份副本中恢复它, 请参阅[从 OVF 文件替换/还原虚拟机](#)。

注释：

- 如果要尝试从一个黄金映像创建或克隆 VM，则导入 VM，因为在导入 VM 时系统将分配唯一的硬件 ID 和 MAC 地址。(黄金映像一般是为多次复制而创建的模板 VM。)为防止与源 VM 冲突，导入向导会自动为新 VM 中的每个网络接口分配一个新 MAC 地址；但在需要时您可能需要手动更新任何 IP 地址和主机名称。
- 仅在 VM 正在运行支持的客人操作系统和启动界面(如[经过测试的客人操作系统](#))中所述)时您才能导入这些 VM。

当您导入 VM 时，系统会从 OVF 或 OVA 文件导入启动接口设置(BIOS 或 UEFI)；您无法修改此设置。

- 只有当 VMware 源运行 VMware Release 6.x 时，您才能从该源导入 VM。
- 如果您从 VMware OVA 文件导入 VM，则确保您的系统具有足够的磁盘空间来进行此操作。系统需要的磁盘空间量等于 OVA 文件的大小 + 要创建的 VM 卷的总大小 + 100 GB 磁盘空间，该磁盘空间是为扩展和处理压缩的 OVA 文件而临时预留的。例如，如果对于需要 32 GB 卷的 VM 您需要导入 3 GB OVA 文件，则所需的最小存储为 3 GB + 32 GB + 100GB = 135 GB。



您可以在 [ztC Console 系统页的存储分配](#) 下查看您系统上的可用磁盘空间量。如果您的系统缺少导入 VMware OVA 文件所需的磁盘空间量，您可以清理一些磁盘空间，或者直接通过网络(无 OVF 或 OVA 文件)迁移 VM，如[将物理机或虚拟机迁移到系统](#)中所述。

- 当您将 VM 导入回同一系统时，以复制此 VM，则在导出或导入过程中必须重命名此 VM 并复制卷。如果您没有重命名此 VM，则导入向导会自动重命名新 VM 和新卷，以防止与源 VM 发生冲突。该向导在 VM 名称和卷名称后附加一个数字，从而增加 VM 其他副本的数目：**MyVM**、**MyVM0**、**MyVM1** 等等。
- 导入 VM 所需的时间取决于源 VM 上卷的大小和数量以及网络带宽。例如，通过 1Gb 的网络传输一个启动卷为 20 GB 的 VM 可能需要花费大约 30 分钟。
- 在导入期间把系统从主 PM 切换到辅 PM 时，此过程将停止。这不会影响系统的连续正常运行时间，但是您必须删除系统上的未完成 VM 和相关卷后重新导入。
- 迁移 PM 或 VM 后，可能没有正确安装网络驱动程序。在这种情况下，手动安装该驱动程序。参阅下面的[故障排除](#)来了解更多信息。

先决条件：

在从 OVF 文件导入 VM 映像前，使用源系统上的 ztC Console 将 VM(请参阅 [导出虚拟机](#)) 导出到支持的网络共享或 USB 设备上的 OVF 和虚拟硬盘 (VHD) 文件。将这些文件复制到您的管理 PC，或者在目标 ztC Edge 系统上安装此 USB 设备或网络共享，如在 [ztC Edge 系统上安装 USB 设备或网络安装的文件](#) 夹中所述，然后使用目标系统上的 ztC Console 导入 OVF 和 VHD 文件。

从 OVA 文件导入 VM 映像前，在 VMware 系统上创建此 OVA 文件。ztC Edge 系统支持包含一个元数据文件和一个或多个磁盘映像文件的 VMware OVA 文件。

要导入 OVF 或 OVA 文件

1. 登录到 ztC Console(在目标系统上)。
2. 在已授权用于两个节点的系统的 **物理机** 页面(参阅“[物理机](#)”页) 上，确认两台 PM 都处于运行状态，并且两台 PM 都不是处于维护模式或正在进行同步。
3. 如果您正在从 USB 设备或网络共享(而不是运行 ztC Console 的 PC) 导入 VM，则在 ztC Edge 系统上安装此设备或共享，如在 [ztC Edge 系统上安装 USB 设备或网络安装的文件](#) 夹中所述。
4. 在 **虚拟机** 页(请参阅“[虚拟机](#)”页) 上，单击 **导入/还原**，打开 **导入/还原虚拟机** 向导。
5. 选择下列之一：
 - **从我的 PC 导入**—从运行 ztC Console 的 PC 导入 VM。



注意：从 PC 导入时不支持 VMware OVF 和 OVA 的浏览，但您可以使用其余任何方法导入 VMware OVF 和 OVA。

单击 **下一步**，然后单击 **浏览**，在本地计算机上找到相应的文件。

- **从 USB 导入**—从 ztC Edge 系统上安装的 USB 设备导入 VM。

单击 **下一步**，然后从下拉菜单中选择一个分区。单击 **列出 OVF/OVA**，然后从下拉菜单中选择相应的文件。您可以选择在 **搜索文件框** 中输入文件名或部分文件名来搜索文件。

- **从远程/网络 Windows 共享 (CIFS/SMB) 导入**—从您本地网络上的 Windows 共享导入 VM。注意，到 VM 的路径(包括 VM 名称) 的最大长度为 4096 个字符。

单击下一步，然后输入用户名和密码的值。对于存储库，输入格式为 `\\machine_URL\ShareName` 的值(例如，`\\192.168.1.34\MyOVFsForImport`)。然后单击列出 OVF/OVA，从该列表中选择相应的文件。

- **从远程/网络 NFS 导入**—从您本地网络上的 NFS 共享导入 VM。注意，到 VM 的路径(包括 VM 名称)的最大长度为 4096 个字符。

单击下一步，对于存储库，以 `nnn.nnn.nnn.nnn/folder_name` 格式(不包含 `http://` 或 `https://`)输入远程系统的 URL。

单击列出 OVF/OVA，显示远程文件夹中所有文件的列表。选择要导入的相应文件。您可以选择在搜索文件框中输入文件名或部分文件名来搜索文件，也可以通过单击列标题(名称、修改日期或大小)来重新组织该列表。单击文件名以选择文件，然后单击下一步。

如果您已选择了一个 OVA 文件，则继续执行下一步(导入是在使用 OVA 文件时的唯一选项)。

如果您已选择了一个 OVF 文件，则单击下一步。将显示消息，确认这是否是 ztC Edge 创建的文件，以及您是否可选择导入或还原 VM。当选择 ztC Edge 创建的 OVF 文件时，您可以选择导入或还原该文件，并且还可选择显示以下消息：

还原 VM 尝试保留硬件 ID 和所有网络接口的 MAC 地址。仅在以下情况下选择还原：具体尝试还原 VM 的特定实例，并且它将成为在网络上所有系统运行的此 VM 的唯一副本。还原通常用于从以前的备份还原 VM。如果要尝试从一个“黄金”映像创建或克隆 VM，则选择导入，因为这将分配唯一的硬件 ID 和 MAC 地址。

6. 选择导入(必要时，向下滚动该窗口。)(对于 ztC Edge 窗的 OVF，您还可以选择还原。有关信息，请参阅[从 OVF 文件替换/还原虚拟机](#)。)
7. 向导将显示准备导入虚拟机窗口，从而提示您在必要时上传其他文件。在提示时，选择相应的文件，以包含与 VM 关联的每个卷。
8. 如果您已选择了一个 OVF 文件，则可查看它，并在必要时编辑信息(您可能需要向下滚动该窗口)：

- **名称、启动界面、CPU 和内存**

显示 VM 的名称、启动界面、vCPU 数量，以及 VM 可使用的总内存。必要时编辑这些信息。(您无法修改启动界面；系统从 OVF 或 OVA 文件导入此设置。)

■ 存储

显示每个卷的名称和大小。在**创建**列中，为一个卷选择一个框来在系统上为该卷分配存储(需要启动卷)。在**恢复数据**列中，选择一个框，以便从 VHD 文件导入一个卷的数据。

■ 网络

显示可用网络。可以移除网络，也可以添加一个尚未分配的网络。您还可以为选择的每个网络指定一个 MAC 地址。至少需要一个网络。

网络总数不能超过 ztC Edge 系统上的业务网络数。如果从 OVF 文件导入 VM，您可以在向导中选择要移除的网络。如果从 OVA 文件导入 VM，则系统会在导入过程中自动忽略多余的网络。无论哪种情况，您都可在导入 VM 之前或之后将更多业务网络连接到 ztC Edge 系统，以恢复网络连接。

9. 根据情况清除**导入后自动启动虚拟机**复选框，如果您需要在首次启动该 VM 前对其重新配置。

10. 单击**导入**来开始导入 VM。您可以选择单击**取消**，取消此过程。

该向导显示进度信息。传输完成后，单击**完成**，关闭此向导。



注意：在导入仍在进行中时，ztC Console 的卷页面上将开始显示导入卷。在导入窗口报告导入完成之前，不要附加或移除任何导入卷；否则，导入将失败。

11. 适用时，按**重配虚拟机资源**所述使用**重新配置虚拟机资源**向导为 VM 分配更多资源。

完成 VM 重配后，单击**开始**来启动 VM。

12. 单击**控制台**来打开 VM 控制台，并登录到客人操作系统。

13. 对于基于 Windows 的 VM，下载 VirtIO 驱动程序并将它们更新到支持的最新版本，如**更新 VirtIO 驱动程序(基于 Windows 的 VM)**。(基于 Linux 的 VM 中已存在正确的 VirtIO 驱动程序。)



注意：更新了这些驱动程序后，您可能需要重启客人操作系统。

14. 必要时，更新客人操作系统中的网络设置。

确认新 VM 工作正确后，导入过程完成；不过，该系统可能会继续在 PM 之间同步数据来启用高可用性 (HA) 或容错 (FT) 操作。



注意：在数据同步完成并运行 VirtIO 驱动程序之前，新 VM 及其关联卷可能会带有警告标志。

故障排除

必要时，使用如下信息解决在导入或导出过程中遇到的问题。

要在导入取消或失败后进行清理

在目标系统上的 **ztC Console** 中，移除导入的 VM 以及与导入的 VM 关联的所有卷(如果存在)。

要恢复目标 VM 中丢失的数据卷

在导入后，如果目标系统上的 VM 内没有出现数据卷，那么，您可能需要手动恢复这些卷，方法如下：

- 关闭 VM，运行**重配虚拟机**向导，确认**卷**页面上已经有了这些卷。
- 对于基于 Windows 的 VM，使用**磁盘管理**把数据卷联机。
- 对于基于 Linux 的 VM，编辑 `/etc/fstab` 文件，以体现这些存储设备的新设备名称。设备名称可能已经改变，例如，当导入中没有卷时。

ztC Edge 系统上 VM 内丢失网络设备的恢复

在导入后，如果目标系统上的 VM 内没有出现网络设备，那么，您可能需要手动恢复这些网络设备，方法如下：

- 关闭 VM，运行**重配虚拟机**向导，确认**网络**页面上已经有了这些网络。如果 VM 需要的网络数量多于向导中显示的数量，则将额外业务网络连接到 **ztC Edge** 系统，然后重新配置 VM，以包含这些新网络。
- 对于基于 Linux 的 VM，重新配置网络启动脚本来使用网络接口的新设备名称。

要手动安装新的网络驱动程序

导入 PM 或 VM 后，可能没有正确安装网络驱动程序(例如，设备管理器可能列出带有警告  的驱动程序)。在这种情况下，手动安装该驱动程序：

1. 在 VM 控制台窗口中，打开客人操作系统中的**设备管理器**。
2. 展开**网络适配器**，然后右键单击 **Red Hat VirtIO 以太网适配器**(未正确工作的驱动程序)。

3. 选择**更新驱动程序软件**。
4. 在弹出窗口中，单击**浏览我的计算机以查找驱动程序软件**。
5. 单击**从计算机的设备驱动程序列表中选择**。
6. 选择 **Red Hat VirtIO 以太网适配器**。
7. 单击**下一步**，安装该网络驱动程序。

安装了该驱动程序后，在 ztC Console 中查看 VM 的状态。如果状态为正在运行 (✓)，则该驱动程序正在正确工作。

相关主题

[在 ztC Edge 系统上安装 USB 设备或网络安装的文件夹](#)

[创建和迁移虚拟机](#)

[配置基于 Windows 的虚拟机](#)

[配置基于 Linux 的虚拟机](#)

[管理虚拟机资源](#)

[管理虚拟机的运行](#)

从 OVF 文件替换/还原虚拟机

如果您要使用先前备份的副本覆盖 VM 来还原(即,恢复)您 ztC Edge 系统上的 VM, 则从 ztC Edge 创建的开放虚拟化格式 (OVF) 文件替换虚拟机 (VM)。(如果您要从其他系统导入 VM, 请参阅[创建和迁移虚拟机](#)中的概述。)

一般导入 VM 可为具有唯一硬件 ID 的 VM 创建一个新实例。还原 VM 可创建一个相同 VM, 该 VM 具有客人操作系统和应用程序进行软件许可时可能需要的相同 SMBIOS UUID、系统序列号和 MAC 地址(如果在 VM 映像中已提供)。但已还原 VM 的硬件 ID 是唯一的。当 ztC Edge 系统上已经存在一个完全相同的 VM 时, 恢复 VM 使您能够用之前的版本替换 VM 和覆盖它。

只有在以下情况时您才能还原已存在于 ztC Edge 系统上的 VM: 您先前已将 VM(请参阅[导出虚拟机](#))从 ztC Edge 系统导出到了支持的网络共享或 USB 设备上的 OVF 和虚拟硬盘 (VHD) 文件。将这些文件复制到您的管理 PC, 或者在目标 ztC Edge 系统上安装此 USB 设备或网络共享, 如在[ztC Edge 系统上安装 USB 设备或网络安装的文件夹](#)中所述, 然后使用目标 ztC Edge 系统上的 ztC Console 从您的管理 PC 还原 OVF 和 VHD 文件。



小心：在覆盖和还原之前，考虑在 ztC Edge 系统上备份您的现有 VM。如果您导出该 VM 以便创建备份，则确保没有覆盖您要还原的 OVF 和 VHD 文件。

注释：



- 您可以仅从通过 ztC Edge 系统创建的 OVF 还原 VM。您无法从通过第三方系统创建的 OVF 还原 VM。您也无法从 OVA 文件还原 VM。
- 通常还原 VM 是为了从以前的备份恢复 VM。在还原 VM 时，系统尝试保留硬件 ID 和所有网络接口的 MAC 地址。
- 仅在以下情况下还原 VM：具体尝试还原 ztC Edge VM 的特定实例，并且已还原的 VM 将成为在网络上所有 ztC Edge 服务器运行的此 VM 的唯一副本。
- 还原 VM 所需的时间取决于源 VM 上卷的大小和数量以及网络带宽。例如，通过 1Gb 的网络传输一个启动卷为 20 GB 的 VM 可能需要花费大约 30 分钟。
- 如果您覆盖并还原现有 VM，则 ztC Edge。
- 如果在还原 VM 的同时 ztC Edge 系统从主 PM 切换到辅助 PM，则还原过程将停止。这不会影响系统的连续正常运行时间，但是您必须删除 ztC Edge 系统上的未完成 VM 和相关卷后重新还原。

先决条件：



- 在从 ztC Edge 系统替换（即，还原）VM 映像前，使用源 ztC Edge 系统上的 ztC Console 将 VM（请参阅[导出虚拟机](#)）导出到支持的网络共享或 USB 设备上的 OVF 和虚拟硬盘（VHD）文件。将这些文件复制到您的管理 PC，或者在目标 ztC Edge 系统上安装此 USB 设备或网络共享，如在[ztC Edge 系统上安装 USB 设备或网络安装的文件夹](#)中所述，然后使用目标 ztC Edge 系统上的 ztC Console 还原 OVF 和 VHD 文件。
- ztC Edge 系统的两台 PM 都必须在线才能使此还原过程正确执行。

要还原 VM

1. 登录到 ztC Console（在目标 ztC Edge 系统上）。
2. 在已授权用于两个节点的系统的**物理机**页面（参阅[“物理机”页](#)）上，确认两台 PM 都处于运行状态，并且两台 PM 都不是处于维护模式或正在进行同步。

3. 如果您正在从 USB 设备或网络共享(而不是运行 ztC Console的PC)还原 VM, 则在 ztC Edge 系统上安装此设备或共享, 如在 [ztC Edge系统上安装 USB 设备或网络安装的文件夹](#)中所述。
4. 在 [虚拟机](#) 页(请参阅“[虚拟机](#)”页)上, 在上方面板中选择要还原的 VM。
5. 在下方面板中, 单击 **还原** 或顶部窗格附近的 **导入/还原**。
6. 选择下列之一:
 - **从我的 PC 导入**—从运行 ztC Console 的 PC 导入 VM。
 - a. 单击 **下一步**。
 - b. 单击 **浏览**, 在本地计算机上查找相应的文件夹。
 - c. 单击所需文件的名称。
 - d. 单击 **打开**。
 - **从 USB 导入**—从 ztC Edge 系统上安装的 USB 设备导入 VM。

单击 **下一步**, 然后从下拉菜单中选择一个分区。单击 **列出 OVF/OVA**, 然后从下拉菜单中选择相应的 OVF 文件。
 - **从远程/网络 Windows 共享 (CIFS/SMB) 导入**—从您本地网络上的 Windows 共享导入 VM。

单击 **下一步**, 然后输入 **用户名和密码** 的值。对于 **存储库**, 输入格式为 `\\machine_URL\ShareName` 的值(例如, `\\192.168.1.34\MyOVFsForImport`)。然后单击 **列出 OVF/OVA**, 从该列表中选择相应的 OVF 文件。
 - **从远程/网络 NFS 导入**—从您本地网络上的 NFS 共享导入 VM。

单击 **下一步**, 对于 **存储库**, 以 `nnn.nnn.nnn.nnn/folder_name` 格式(不包含 `http://` 或 `https://`)输入远程系统的 URL。

单击 **列出 OVF/OVA**, 显示远程文件夹中所有文件的列表。选择相应的 OVF 文件。您可以选择在 **搜索文件框** 中输入文件名或部分文件名来搜索文件, 也可以通过单击列标题(名称、修改日期或大小)来重新组织该列表。单击文件名以选择文件, 然后单击 **下一步**。
7. 选择 **还原**。(必要时, 向下滚动该窗口。)将显示一条警告消息, 说明 **还原** 将覆盖所有现有数据和配置详细信息, 以及您在操作时应谨慎。
8. 单击 **继续**, 继续操作。

9. 在提示时, 添加 VHD 文件。
10. 审查信息, 必要时进行所需的编辑。

- **名称、启动界面、CPU 和内存**

显示 VM 的名称、启动界面、vCPU 数量, 以及 VM 可使用的总内存。必要时编辑这些信息。(您无法修改**启动界面**; 系统从 OVF 文件导入此设置。)

- **存储**

显示每个卷的名称和大小。在**创建**列中, 为一个卷选择一个框来在 ztC Edge 系统上为该卷分配存储(需要启动卷)。在**恢复数据**列中, 选择一个框, 以便从 VHD 文件导入一个卷的数据。

- **网络**

显示所有可用网络。可以移除网络, 也可以添加一个尚未分配的网络。至少需要一个网络。

网络总数不能超过 ztC Edge 系统上的业务网络数。您可以在向导中选择要移除的网络, 或者在还原 VM 之前或之后将更多业务网络连接到 ztC Edge 系统, 以恢复网络连接。

11. 根据情况清除**还原后自动启动虚拟机**复选框, 如果您需要在首次启动该 VM 前对其重新配置。
12. 单击**还原**, 开始还原 VM。传输完成后, 单击**完成**, 关闭此向导。



注意: 在还原过程仍在进行中时, **卷页/ztC Console** 上开始显示还原的卷。在还原窗口报告此过程完成之前, 不要附加或移除任何已还原的卷; 否则还原过程将失败。

13. 适用时, 按**重配虚拟机资源**所述使用**重新配置虚拟机资源**向导为 VM 分配更多资源。

完成 VM 重配后, 单击**开始**来启动 VM。

确认还原的 VM 工作正确后, 还原过程完成; 不过, ztC Edge 系统可能会继续在 PM 之间同步数据来启用高可用性 (HA) 或容错 (FT) 操作。



注意: 在数据同步完成并运行 VirtIO 驱动程序之前, 还原的 VM 及其关联卷可能会带有警告标志。

故障排除

必要时，使用如下信息解决在还原过程中遇到的问题。

要在还原过程取消或失败后进行清理

在目标系统上的 **ztC Console**中，移除还原的 VM 以及与还原的 VM 关联的所有卷(如果存在)。

相关主题

[创建和迁移虚拟机](#)

[管理虚拟机资源](#)

[管理虚拟机的运行](#)

导出虚拟机

导出系统上的虚拟机 (VM)，以便将 VM 的映像保存到网络加载的文件夹(即，目录)或 USB 设备。从 **ztC Edge**系统导出 VM 可使 VM 映像可用于导入到其他系统或导入回同一 **ztC Edge** 系统，以便还原或复制原始 VM。您可以直接从 **ztC Edge**系统导出 VM，如本主题中所述。

通过创建一个网络加载的文件夹将导出的 VM 存储在您的环境中，为导出快照做好准备。如果您正在使用 USB 设备，则将其插入系统的当前主节点(在**物理机**页上显示为 **noden(主)**)。如果您正在使用文件夹，则创建一个用于 Windows 共享或网络文件系统 (NFS) 导出的文件夹。Windows 共享也称为通用 Internet 文件系统 (CIFS) 共享(例如 Samba)。然后将此文件夹或 USB 设备安装到 **ztC Edge**系统的主机操作系统中，如本主题中所述。当在 **ztC Console**中开始导出时，**ztC Edge** 系统会将 VM 另存为标准开放虚拟化格式 (OVF) 和虚拟硬盘 (VHD) 文件。

注释：

- 因为必须关闭源 VM 才能将其导出，因此考虑为此过程安排一段计划维护时间。
- 导出所需的时间取决于源 VM 上卷的大小和数量以及网络带宽。例如，通过 1Gb 的网络传输一个启动盘为 20 GB 的 VM 可能需要花费大约 30 分钟。
- 如果在导出后将继续使用源 VM，则当您在目标系统上导入它时，记得为此 VM 设置不同的 MAC 地址和 IP 地址。
- 在导出期间将 ztC Edge 系统从主 PM 切换到辅助 PM 时，此过程将停止。这不影响系统的继续正常运行。可将部分导出的文件从网络加载的文件夹中删除，然后再次导出这些文件。
- 您可导入的 vfat 文件最大为 4 GB。如果您尝试导入大于 4 GB 的 vfat 文件，则导出将失败。
- 对于基于 Linux 的 VM，将 VM 导出到其他系统时，您无需修改 /etc/fstab 文件。
- 对于运行某些较早 Ubuntu 版本的基于 Ubuntu 的 VM，在导出 VM 之前，您可能需要编辑 /boot/grub/grub.cfg 文件，把参数 gfxmode 更改为 text(例如，设置 gfxmode=text)；否则，在其他系统上，新 VM 的控制台可能会挂起。在迁移完毕后可以恢复源 VM 上的原始设置。



先决条件：

- 进行导出前，必须关闭 VM。
- 准备导出目标：
 - 如果您正在使用 USB 设备，则将其插入系统的当前主节点(在**物理机**页上显示为 **noden(主)**)。确认系统显示了该 USB 设备。导航到**物理机**页。单击插入了该设备的节点，然后在下部窗格中，选择 **USB 设备** 选项卡。您插入的 USB 设备应显示在该选项卡中。
 - 如果您正在将网络加载的文件夹用于 Windows/CIFS 共享或 NFS 导出，则在您能够保存已导出 VM 的环境中创建此文件夹。在网络加载的文件夹上设置全部读/写权限，以便允许文件传输，或者仅对于 Windows/CIFS 共享，为托管此共享的系统/域上的特定用户指定读/写权限。记录 NFS 导出或 CIFS 共享的 URL 或路径名，以及在您导出 VM 时使用的 CIFS 共享的用户名/密码。



确保您有足够的存储空间来容纳您要导出的 VM。

此外，基于 Windows 的 VM 需要进行 Windows 特定的准备。

准备导出 VM(仅基于 Windows 的 VM)

1. 使用 ztC Console 登录到 ztC Edge 系统。
2. 在**虚拟机**页面上，选择要导出的 VM。
3. 单击**控制台**来打开 VM 控制台，并登录到 Windows 客人操作系统。
4. 确保按**管理 Windows 驱动器标签**所述准确标示所有卷。
5. 运行 Windows 系统准备工具 (Sysprep) 来为重新部署准备客人操作系统。

要导出 VM

1. 使用 ztC Console 登录到 ztC Edge 系统。
2. 在**虚拟机**页上，选择要导出的 VM，然后单击**关闭**。等待 VM 关闭。请参阅“**虚拟机**”页。
3. 在选择了 VM 时，单击**导出**，打开导出向导。
4. 选择下列之一：



注意：如果您已经使用**安装按钮**安装了一个位置(如在 **ztC Edge**系统上安装 **USB 设备或网络安装**的文件夹中所述)，则导出向导会以绿色显示此安装的设备。要更改它，则单击**更改按钮**。

■ 通过 Windows 共享 (CIFS/SMB) 安装设备

导出目标是 CIFS 共享上的文件夹。输入**用户名**、**密码**和**存储库值**。对于**存储库**，输入格式为 `\\machine_URL\ShareName` 的值(例如，`\\192.168.1.34\MyExportVMs`)。

■ 通过 NFS 安装设备

导出目标是通过 NFS 访问的远程系统上的文件夹。输入**存储库值**，其为远程系统的 URL，格式为 `nnn.nnn.nnn.nnn`(不包含 `http://` 或 `https://`)。

■ 安装 USB

对于 **USB 分区列表**，从下拉菜单中选择一个分区。

- 对于**导出路径**：`/mnt/ft-export:`，键入 VM 导出位置的路径以及其 OVF 和 VHD 文件存储位置的路径。例如，如果要将 VM 导出到名为 ocean1 的新文件夹，则键入 ocean1。
- 单击**安装**。

如果安装成功，该存储库会显示在**设备 URL**下，并且**导出 VM**按钮变为活动状态；否则将显示警报。
- 选择要包含在**要导出的启动卷**和**要导出的数据卷**下的卷。(需要启动卷。)
- 单击**导出 VM**，导出 VM。

您可以在正在导出的 VM 的**总结**选项卡内监视**导出状态**。进度是作为对于整个导出或对于每个卷而言完成的百分数(%)。此过程完成后，状态改变为**导出已成功完成**。

要取消导出，则单击**导出进度**百分数旁的**取消**。将打开确认对话框，要求您确认此取消。单击**是**，取消。

ztC Edge系统先导出 VHD 文件(卷)，然后再导出 OVF 文件。当 OVF 文件显示在该文件夹中时，可确认此过程已完成。

在导出过程之后，如果要在 ztC Edge 系统上导入或还原 OVF 和 VHD 文件，请参阅[导入 OVF 或 OVA 文件](#)。

要卸载此设备，请参阅[在 ztC Edge 系统上安装 USB 设备或网络安装的文件夹](#)。

故障排除

必要时，使用如下信息解决在导出过程中遇到的问题。

在取消从 ztC Edge系统中导出或导出失败之后进行清理

移除导出文件夹内的 VM 文件，或者为后面的导出创建一个新文件夹。

相关主题

[将USB 设备附加到虚拟机](#)

[创建和迁移虚拟机](#)

[管理虚拟机资源](#)

[管理虚拟机的运行](#)

在 ztC Edge系统上安装 USB 设备或网络安装的文件夹

您可以使用**虚拟机**页上的**安装(或卸载)**按钮在 ztC Edge 系统上安装(或卸载)USB 设备或网络安装的文件夹(即，目录)。安装某个位置可使其可用于安装点 /mnt/ft-export/ 处的主节点。然后，您可以将主节点上的 VM 导出到安装位置，或将 VM 从安装位置导入 ztC Edge 系统。导出或导入完成后，使用**卸载**按钮可卸载该位置。

(如果需要安装 USB 设备以访问 VM 的客人操作系统中的设备，请参阅[将USB 设备附加到虚拟机](#)。)

注释：



1. 您无法卸载正在使用的已安装位置。例如，当正在导出或导入 VM 时，您无法卸载位置。
2. ztC Edge系统上的Stratus Redundant Linux 软件不支持 exFAT 文件系统。安装 USB 介质前，使用 NTFS 对设备进行格式化。(默认情况下，大多数 USB 介质是使用 FAT 文件系统格式化的，这具有 4 GB 的文件大小限制，对于大多数 VM 而言这可能太小。)

先决条件：准备已安装位置：

- 如果您正在使用 USB 设备导出或导入 VM，则将此设备附加到系统的当前主节点（在物理机页上显示为 **noden(主)**）。确认系统显示此 USB 设备：导航到物理机页，单击附加了该设备的节点，然后在下部窗格中，选择 **USB 设备** 选项卡。您附加的 USB 设备应显示在该选项卡中。
- 如果您正在将网络加载的文件夹用于 Windows/CIFS 共享或 NFS 导出，则在您能够保存已导出 VM 的环境中创建此文件夹。在网络加载的文件夹上设置全部读/写权限，以便允许文件传输，或者仅对于 Windows/CIFS 共享，为托管此共享的系统/域上的特定用户指定读/写权限。记录 NFS 导出或 CIFS 共享的 URL 或路径名，以及在您安装 CIFS 共享的 NFS 导出时使用的 CIFS 共享的用户名/密码。

要安装 USB 设备或网络安装的文件夹

1. 在虚拟机页上，选择一个 VM。
2. 在下部窗格中，单击 **安装** 按钮。
3. 对于安装点 **/mnt/ft-export/**，选择下列之一：

- **通过 Windows 共享 (CIFS/SMB) 安装设备**

安装位置是 CIFS 共享上的文件夹。输入用户名、密码和存储库值。对于存储库，输入格式为 `\\machine_URL\ShareName` 的值（例如，`\\192.168.1.34\MyMountLocation`）。

- **通过 NFS 安装设备**

安装位置是通过 NFS 访问的远程系统上的文件夹。对于存储库，以 `nnn.nnn.nnn.nnn` 格式（不包含 `http://` 或 `https://`）输入远程系统的 URL。

- **安装 USB**

对于 **USB 分区列表**，从下拉菜单中选择一个分区。

4. 单击 **安装**。

该位置安装在主节点上，**安装** 按钮变为 **卸载**。

要卸载 USB 设备或网络安装的文件夹

1. 在虚拟机页上，选择一个 VM。
2. 在下部窗格中，单击 **卸载** 选项卡。
3. 将显示 **确认** 对话框，询问您是否确定要卸载该位置。单击 **是**，卸载它。

该位置已卸载，**卸载**按钮变为**安装**。

相关主题

[导出虚拟机](#)

[管理虚拟机](#)

管理 Windows 驱动器标签

在基于 Windows 的虚拟机中标记卷，以确保在您导出虚拟之前正确映射这些卷。



小心：确保每个卷都有唯一可识别标签，然后再运行 **Sysprep**(以便准备导出)。此过程需要管理员权限。

若要从命令提示符设置标签，请键入：

```
C:\>label C:c-drive
```

要列出和验证所有卷标签，则使用 **diskpart** 实用程序：

```
C:\> diskpart
```

```
DISKPART> list volume
```

```
...
```

```
DISKPART> exit
```

在导入虚拟机后，使用**磁盘管理器**重新分配盘符。在导出之前分配标签有助于识别驱动器。有关在 Windows 系统上重新分配盘符的说明，请搜索 [Microsoft 支持网站](#)。

相关主题

[创建和迁移虚拟机](#)

[配置基于 Windows 的虚拟机](#)

配置基于 Windows 的虚拟机

安装基于 Windows 的虚拟机后，配置生产使用所需的额外资源和软件，如以下部分中所述：

- [更新 VirtIO 驱动程序\(基于 Windows 的 VM\)](#)
- [创建和初始化磁盘\(基于 Windows 的 VM\)](#)
- [安装应用程序\(基于 Windows 的 VM\)](#)

此外,确保配置以下设置:

- 更改客人操作系统中的时区,以便与 **日期和时间** 首选项页 (ztC Console 中) 上配置的时区相对应(请参阅 [配置日期和时间](#)); 否则只要 VM 重启或迁移,VM 的时区就会改变。建议对 VM 和 ztC Edge 系统均使用网络时间协议 (NTP)。
- 禁用休眠(有时在默认情况下启用了休眠),以防止客人操作系统进入省电状态。
- 将客人操作系统中的电源按钮操作配置成关闭客人(并且不使其休眠),以便使 **关闭 VM** 按钮 (ztC Console 中) 正常工作(请参阅 [关闭虚拟机](#))。
- 将客人操作系统配置成在操作系统崩溃时生成故障转储文件。请遵循 Microsoft 文章 [如何在基于 Windows 的系统上使用一个 NMI 生成完整的故障转储文件或内核故障转储文件](#) (文章 ID: 927069) 中的说明。请遵循 **更多信息** 部分中的说明。

有关在已授权用于监控的系统上监控基于 Windows 的 VM 的信息,请参阅 [监控基于 Windows 的虚拟机](#)。

相关主题

[管理虚拟机](#)

更新 VirtIO 驱动程序(基于 Windows 的 VM)

将基于 Windows 的虚拟机 (VM) 中的 Red Hat VirtIO 驱动程序更新到支持的最新版本,以确保这些 VM 的正确运行。例如,在升级了系统软件(升级 [Stratus Redundant Linux 软件](#))或使用 P2V 客户端将 VM 或物理机 (PM) 迁移到 ztC Edge 系统([将物理机或虚拟机迁移到系统](#))后,您应更新 VirtIO 驱动程序。

注释：

- 为正确运行，确保仅从 **ztC Edge支持** 页下载 VirtIO 驱动程序，如以下操作程序中所所述。该支持页上的 VirtIO ISO 文件包含已使用 Stratus Redundant Linux 软件进行了测试的 VirtIO 驱动程序版本，并且已知它们可正常工作。来自其他来源的 VirtIO 驱动程序可能具有兼容性问题。
- 更新 VirtIO 驱动程序时，仅使用 **浏览我的计算机以查找驱动程序软件** 选项，然后选择适用于客人操作系统的特定文件夹或 .inf 文件。如果使用 **自动搜索更新的驱动程序软件** 选项，或者仅选择 VirtIO VCD 的顶层，则 Windows 可能会自动安装错误的驱动程序。
- 在某些情况下，更新了驱动程序后客人操作系统会请求重启。如果是这样，则重启客人操作系统。

更新基于 Windows 的虚拟机中的 VirtIO 驱动程序

1. 从以下下载 VirtIO ISO 文件：此 **下载** 页面在 <https://www.stratus.com/services-support/downloads/?tab=ztcedge>.
 - a. 在 **下载** 页上，单击 **ztC Edge** (如果其尚未显示)，然后选择相应的版本。
 - b. 向下滚动到 **驱动程序和工具**，然后继续滚动到 **ztC Edge VirtIO 驱动程序更新**。
 - c. 单击转到相应文件的链接。

确保下载与您 ztC Edge 系统相匹配的 VirtIO ISO 文件版本。

2. 如果您要验证 ISO 映像的完整性，还要下载关联的 fciv 校验和文件，然后从 Microsoft 支持网站下载 Microsoft 文件校验和完整性验证程序 (FCIV) 可执行文件。将这两个文件保存到包含已下载的 ISO 文件的目录中。

打开命令提示符。从包含该 ISO、可执行文件和验证文件的目录，键入与以下类似的命令来验证此 ISO 映像：

```
fciv -v -xml virtio-win-n.n.nn.xml
```

如果该命令 **执行成功** (也就是说，返回消息所有文件均已成功验证)，则转到下一步。如果该命令 **执行失败**，则重新下载。

3. 打开 ztC Console，创建 VirtIO ISO 文件的 VCD，然后将该 VCD 插入基于 Windows 的 VM 中 (请参阅 [创建虚拟 CD](#) 和 [插入虚拟 CD](#))。
4. 在 VM 控制台窗口中，打开客人操作系统中的 **设备管理器**。

打开设备管理器的方法因客人操作系统的版本而异。一种方法是打开控制面板，然后选择**设备管理器**。另一种方法是打开搜索窗口，然后键入**设备管理器**。

5. 展开**网络适配器**，然后找到**Red Hat VirtIO 以太网适配器**。可能存在多个适配器，具体取决于您的 VM 中的网络接口数量。

如果**Red Hat VirtIO 以太网适配器**不存在，则不会安装 VirtIO 驱动程序。展开**其他设备**，然后找到未知**以太网控制器**设备。更新此设备的驱动程序。

- a. 右键单击**Red Hat VirtIO 以太网适配器(或以太网控制器)**，然后选择**更新驱动程序软件**。单击**浏览我的计算机以查找驱动程序软件**，指定您客人操作系统的 VirtIO 以太网驱动程序(**netkvm**)的位置，然后完成此驱动程序的更新。(例如，要在 Windows Server 2012 R2 客人中更新该驱动程序，则在 VirtIO VCD 上选择 `NetKVM\2k12R2\amd64\netkvm.inf` 文件。)
 - b. 对每个额外**Red Hat VirtIO 以太网适配器(或以太网控制器)**设备均重复此驱动程序更新。
6. 展开**存储控制器**，然后找到**Red Hat VirtIO SCSI 控制器**。可能存在多个控制器，具体取决于您的 VM 中的卷数量。如果**Red Hat VirtIO SCSI 控制器**不存在，则不会安装 VirtIO 驱动程序。查找未知**SCSI 控制器**设备，然后更新此设备的驱动程序：

- a. 右键单击**Red Hat VirtIO SCSI 控制器(或 SCSI 控制器)**，然后选择**更新驱动程序软件**。单击**浏览我的计算机以查找驱动程序软件**，指定您客人操作系统的 VirtIO SCSI 驱动程序(**viosstor**)的位置，然后完成此驱动程序的更新。(例如，要在 Windows Server 2012 R2 客人中更新该驱动程序，则在 VirtIO VCD 上指定 `viosstor\2k12R2\amd64\viosstor.inf` 文件。)
- b. 对每个额外**Red Hat VirtIO SCSI(或 SCSI 控制器)**设备均重复此驱动程序更新。



小心：尽管设备名称为**Red Hat VirtIO SCSI 控制器**，但您必须选择标有**viosstor**的存储驱动程序文件，而不是**vioscsi**(如果存在)。安装**vioscsi**驱动程序可能会使您的 VM 崩溃。

7. 如适用，则重新启动客人操作系统来加载更新后的驱动程序。

相关主题

[配置基于 Windows 的虚拟机](#)

[创建和迁移虚拟机](#)

[管理虚拟机的运行](#)

创建和初始化磁盘(基于 Windows 的 VM)

创建和初始化磁盘，以便使其准备好在基于 Windows 的虚拟机中分区成多个卷。

要在基于 Windows 的虚拟机中创建和初始化磁盘

1. 使用 ztC Console在 ztC Edge 系统上的存储组中创建一个新卷，如在[虚拟机中创建卷](#)中所述。
2. 在 Windows 客人操作系统中，打开**磁盘管理**或者类似实用程序。
3. 初始化新添加的磁盘。(可能提示您此操作会自动执行。)
4. 将该磁盘转换成动态磁盘。
5. 在该磁盘上创建一个或多个简单卷。
6. 重启 Windows 客人操作系统。

有关完整说明，请参阅您的 Windows 文档。



注意：由于 Stratus Redundant Linux软件已经在物理层面上镜像了数据，因此在 Windows 客人操作系统中无需卷冗余。

相关主题

[打开虚拟机控制台会话](#)

[配置基于 Windows 的虚拟机](#)

[创建和迁移虚拟机](#)

[管理虚拟机的运行](#)

安装应用程序(基于 Windows 的 VM)

通过执行下列一个操作，在基于 Windows 的虚拟机中安装应用程序：

- 将安装程序作为可执行文件或 ISO 文件下载到客人操作系统。
- 安装包含此安装程序的网络驱动器。
- 创建并插入包含此安装程序的虚拟 CD (VCD)。请参阅[管理虚拟 CD](#)。

有关在基于 Windows 的 VM 上监控应用程序的信息(在已授权用于此类监控的系统上)，请参阅[监控基于 Windows 的虚拟机上的应用程序](#)。

相关主题

[打开虚拟机控制台会话](#)

[配置基于 Windows 的虚拟机](#)

[创建和迁移虚拟机](#)

[管理虚拟机的运行](#)

配置基于 Linux 的虚拟机

安装基于 Linux 的虚拟机后，配置生产使用所需的额外资源和软件，如以下部分中所述：

- [创建和初始化磁盘\(基于 Linux 的 VM\)](#)
- [安装应用程序\(基于 Linux 的 VM\)](#)

此外，确保配置以下设置：

- 禁用休眠(有时在默认情况下启用了休眠)，以防止客人操作系统进入省电状态。
- 将客人操作系统中的电源按钮操作配置成关闭客人(并且不使其休眠)，以便使**关闭 VM**按钮(**ztC Console**中)正常工作。对于 **Ubuntu Linux** 的最小服务器版本，可根据需要安装 **acpid** 包，以便启用**关闭**按钮。请参阅[关闭虚拟机](#)。
- 安装 **kexec-tools** 包，以及将客人操作系统配置成在系统崩溃时生成故障转储文件。
- 对于 **Ubuntu Linux** 客人操作系统，为了防止出现 VM 控制台在 **ztC Console** 中挂起的问题，编辑 `/boot/grub/grub.cfg` 文件，把 `gfxmode` 参数修改为 `text`(例如，`set gfxmode=text`)。如果在您能够设置此参数前 VM 控制台挂起，请参阅[打开虚拟机控制台会话](#)中的故障排除信息，以解决此问题。

有关这些设置的更多信息，请参阅 **Linux** 文档。

相关主题

[管理虚拟机](#)

创建和初始化磁盘(基于 Linux 的 VM)

创建和初始化磁盘，以便使其可用于保存基于 Linux 的虚拟机中的数据。

要在基于 Linux 的虚拟机中创建和初始化磁盘

1. 在 ztC Console中，在存储组中创建一个新卷，如在[虚拟机中创建卷](#)中所述。
2. 在基于 Linux 的虚拟机中，当需要初始化和安装卷时，使用卷管理工具或者编辑文件。有关完整说明，请参阅您的 Linux 文档。

基于 Linux 的虚拟机的磁盘设备名称是 /dev/vda 到 /dev/vdh，而不是标准的 /dev/sda 到 /dev/sdh。ztC Edge虚拟磁盘卷显示在客人操作系统中，对它们的使用就像使用物理磁盘似的。

相关主题

[打开虚拟机控制台会话](#)

[配置基于 Linux 的虚拟机](#)

[创建和迁移虚拟机](#)

[管理虚拟机的运行](#)

安装应用程序(基于 Linux 的 VM)

通过执行下列一个操作，在基于 Linux 的虚拟机中安装应用程序：

- 将安装包作为可执行文件或 ISO 文件下载到客人操作系统。
- 安装包包含此安装包的网络驱动器。
- 创建并插入包含此安装包的虚拟 CD (VCD)。请参阅[管理虚拟 CD](#)。

相关主题

[打开虚拟机控制台会话](#)

[配置基于 Linux 的虚拟机](#)

[创建和迁移虚拟机](#)

[管理虚拟机的运行](#)

管理虚拟机的运行

管理虚拟机的运行，如以下部分中所述：

- [启动虚拟机](#)
- [关闭虚拟机](#)
- [关闭虚拟机电源](#)

- [打开虚拟机控制台会话](#)
- [重命名虚拟机](#)
- [移除虚拟机](#)

欲了解关于配置和故障排除的更多信息，请参阅[高级主题\(虚拟机\)](#)。

启动虚拟机

启动虚拟机 (VM)，以便启动 VM 的客人操作系统。您还可以配置在 ztC Edge 系统启动时的 VM 启动模式。

要启动虚拟机

1. 在**虚拟机**页上，选择一个 VM。
2. 单击底部面板中的**启动**。

要配置在系统启动时的 VM 启动模式

1. 在**虚拟机**页上，选择一个 VM。
2. 单击下部面板中的**启动**选项卡。
3. 对于**自动启动模式**，选择下列一项：
 - **最后**—在系统关闭时，使 VM 返回到其状态：如果 VM 正在运行，则在系统启动时重启 VM；如果 VM 停止，则在系统启动时不启动 VM。
 - **打开**—在系统启动时启动 VM。
 - **关闭**—在系统启动时不启动 VM。
4. 单击**保存**。

相关主题

[关闭虚拟机](#)

[关闭虚拟机电源](#)

[管理虚拟机的运行](#)

关闭虚拟机

关闭虚拟机 (VM)，以便开始有序关闭客人操作系统。



注意：可通过客人操作系统命令关闭 VM。部分客人可允许(或可配置为允许)您使用 ztC Console 关闭 VM。

在 ztC Console 中关闭 VM 类似于按物理机上的电源按钮，这一般会使操作系统有序关闭。在某些情况下，您可能需要在客人操作系统中显式启用该功能。例如：

- 对于任何客人，验证是否将电源按钮操作设置成了关闭客人操作系统，而不是使其休眠。对于被设置为休眠的客人，如果单击**关闭**(ztC Console 中)，则 VM 仍处于**正在停止**状态，不会正常关闭。
- 在部分访客系统中，除非用户已登录操作系统，否则电源按钮不会关闭系统。您可以根据需要更新安全设置，以便在未登录会话时也能够启用电源按钮。
- 在 Ubuntu 的一些最小服务器版本上，默认安装中不包括可启用电源按钮的 acpid 包。您可以手动安装此包，以便使用以下命令启用电源按钮(或者参见针对您客人操作系统的文档)：

```
sudo apt-get install acpid
```

对于运行桌面的 Ubuntu 版本，ztC Console**关闭**按钮会致使 VM 的 Ubuntu 桌面提示您选择三个图标中的一个：挂起、睡眠或关闭。要使 Ubuntu VM 在没有桌面提示的情况下关闭，您必须修改 powerbtn 文件。

要修改 powerbtn 文件

1. 在 VM 中，编辑 /etc/acpi/events/powerbtn 文件。
2. 对以下行进行注释：

```
event=button[ /]power  
action=/etc/acpi/powerbtn.sh
```

3. 添加以下行：

```
event=button/power (PWR.||PBTN)  
action==/sbin/poweroff
```

4. 发出以下命令来重启 acpid：

```
systemctl restart acpid
```

请参阅您客人操作系统的文档，以配置系统电源按钮的行为，从而使**关闭**按钮能够在 ztC Console 中工作。

要关闭ztC Console中的 VM

1. 在**虚拟机**页上，选择一个 VM。
2. 单击底部面板中的**关闭**。

将显示一条警告消息，要求您确认关闭。单击**是**，关闭，或者单击**否**，停止关闭。

如果 VM 没有响应，您还可以使 VM **关机**，以便在未正确关闭客人操作系统的情况下使其停止。

相关主题

[启动虚拟机](#)

[关闭虚拟机电源](#)

[管理虚拟机的运行](#)

关闭虚拟机电源

关闭虚拟机 (VM) 电源，以便在未正确关闭客人操作系统的情况下使其停止。



小心：仅在以下情况下使用**关机**命令：**关闭**命令或客人操作系统命令失败。关闭 VM 电源类似于拔下电源线，这可能导致数据丢失。

要关闭虚拟机电源

1. 在**虚拟机**页上，选择一个 VM。
2. 单击底部面板中的**关机**。

相关主题

[启动虚拟机](#)

[关闭虚拟机](#)

[管理虚拟机的运行](#)

[高级主题\(虚拟机\)](#)

打开虚拟机控制台会话

打开虚拟机 (VM) 控制台会话，以显示在 VM 中运行的客人操作系统的控制台。

以下过程描述了如何在 ztC Console 中打开 VM 控制台会话，但您还可以使用远程桌面应用程序执行此操作。

要打开 VM 控制台会话

1. 在**虚拟机**页上，选择一个 VM。
2. 确保此 VM 处于运行状态。
3. 单击底部面板中的**控制台** ()。

注意：

单击**控制台**后，如果浏览器与系统建立了 HTTPS 连接，但没有针对它的安全例外，则打开的控制台会话可能为空。在这种情况下，单击此会话窗口右上角的 IP 地址。该 IP 地址的格式为 `https://system_IP_address:8000`，其添加系统 IP 地址以作为浏览器中的安全例外站点。安全例外可使浏览器打开此站点。

根据浏览器，可能显示其他安全窗口或消息。在使用某些浏览器时会显示一条或多条安全消息，您需要单击这些消息。在使用其他浏览器时，地址栏变为红色且没有消息，您需要单击地址才能继续。一些具体示例为：



- 如果地址栏中显示**证书错误**，您需要 (1) 单击此地址；(2) 在显示**网站无法显示该页面**的页面上，单击**更多信息**；然后 (3) 在显示**此站点不安全的**页面上，单击**转到此网页(不推荐)**。
- 如果显示**警告：面临潜在的安全风险**页，则单击**高级**，然后在下一个窗口中，单击**接受风险并继续**。
- 如果显示**错误响应**和**错误代码 405**，则关闭此窗口或选项卡。

然后，此安全例外将应用于所有 VM。对于每个浏览器，只需执行一次这些操作。当未来单击**控制台**时，与 VM 的控制台会话将成功打开。

打开了 VM 控制台会话后，您可以调整浏览器窗口和 VM 控制台会话的大小。您还可以使用键盘快捷键。

要调整浏览器窗口和 VM 会话的大小

1. 打开 VM 控制台会话(请参阅以上程序)。

图标显示在窗口的左边缘。要显示这些图标，您可能需要单击窗口左边缘的选项卡中的箭头。

2. 要将浏览器窗口调整为全屏，则单击全屏图标 ()。

全屏时，再次单击全屏图标 () 可将浏览器调整为较小的窗口。

3. 要在浏览器中调整 VM 会话的大小，则单击“设置”图标 ，然后选择**缩放模式**(单击当前模式可查看具有其他设置的下拉菜单):
 - **远程调整大小**(默认)—当您更改客人 OS 的分辨率时，VM 会话的大小会更改。
 - **局部缩放**—VM 会话的大小自动更改，以便使用原始宽高比填充整个屏幕。

要使用键盘快捷键

1. 打开 VM 控制台会话(请参阅以上程序)。
2. 单击窗口左边缘的 **A** 图标 ，显示键盘快捷键选择图标。
3. 将显示以下图标：
 - —单击可实现 **Ctrl** 键功能。
 - —单击可实现 **Alt** 键功能。
 - —单击可实现 **Tab** 键功能。
 - —单击可实现 **Esc** 键功能。
 - —单击可实现 **Ctrl + Alt + Delete** 键功能。

故障排除

解决 VM 控制台窗口不能打开的问题

请求您的网络管理员打开端口 6900-6999(含)。

解决 VM 控制台窗口空白的问题

确认 VM 已经打开并且不是处于启动过程中。而且，单击控制台窗口后按任意键来关闭屏幕保护程序。

解决显示不止一个 VM 控制台窗口和窗口行为异常的问题

关闭所有控制台窗口，然后只打开一个控制台窗口。

解决 ztC Edge 系统上 VM 控制台窗口挂起的问题

对于基于 Ubuntu 的 VM，VM 控制台将会在 ztC Console 挂起 - 如果您没有正确设置 `gfxmode` 参数。在客人操作系统中，编辑 `/boot/grub/grub.cfg` 文件，将 `gfxmode` 参数更改为 `text`(例如，`set gfxmode=text`)。

如果在您能够设置此参数前控制台挂起，则执行以下操作：

1. 重新启动 ztC Console 中的 VM。
2. 在 GRUB 菜单上, 按 e, 编辑 grub 命令。
3. 在下一屏幕的 gfxmode 行上, 将 \$linux_gfx_mode 更改为 text, 以便使此行显示为:

```
gfxmode text
```

4. 按 **Ctrl-x** 或 **F10**, 启动客人操作系统。
5. 要更新此设置, 以便在每次启动周期中都保持此设置, 则编辑 /boot/grub/grub.cfg 文件, 将 gfxmode 参数更改为 text, 以便使此行显示为:

```
set gfxmode=text
```

6. 保存 /boot/grub/grub.cfg 文件。

在控制台屏幕无法阅读时修改基于 Linux 的 VM 的终端类型

默认情况下, Linux 操作系统将 TERM 变量设置为 vt100-nav, vncterm 程序 (ztC Console 上 VM 控制台的基础) 无法正确支持该设置。如果您使用命令行以外的任何内容, 则屏幕会变得不可读。要解决此问题, 则更改 Linux 客人操作系统中的终端类型:

1. 在客人操作系统中打开 inittab 文件。
2. 在下面的行中, 通过删除行末尾的 -nav, 将 vt100-nav 替换为 vt100。更新的行显示如下:

```
# Run gettys in standard runlevels co:2345:respawn:/sbin/agetty xvc0
9600 vt100
```
3. 保存 **inittab** 文件。

相关主题

[启动虚拟机](#)

[关闭虚拟机](#)

[管理虚拟机的运行](#)

重命名虚拟机

重命名虚拟机 (VM), 以便更改其在 **虚拟机** 页上显示的名称。

如果您需要更改在 VM 中运行的客人操作系统的主机名，则使用客人操作系统工具。



先决条件：要重命名 VM，您必须将其关闭。

要重命名虚拟机

1. 在**虚拟机**页上，选择一个 VM。
2. 单击**关闭**，然后等待该 VM 关闭。
3. 双击此 VM 的名称。
4. 键入新名称。此 VM 名称必须符合以下要求：
 - VM 名称的开头必须是单词或数字，并且名称不能包含特殊字符(例如，#、% 或 \$)。
 - VM 名称不能使用带有连字符的前缀，例如 **Zombie-** 或 **migrating-**。
 - VM 名称最多具有 85 个字符。
5. 按 **Enter**。

相关主题

[移除虚拟机](#)

[创建和迁移虚拟机](#)

[管理虚拟机的运行](#)

移除虚拟机

移除虚拟机 (VM)，以便将其永久删除，以及根据需要将关联的卷从 ztC Edge 系统中删除。



先决条件：ztC Edge 系统的两个 PM 都必须联机才能正确移除 VM。在 ztC Console 的**物理机**页面上，确认两台 PM 都处于**运行**状态，并且两台 PM 都不是处于维护模式或正在进行同步。

要移除虚拟机

1. 在**虚拟机**页上，选择一个 VM。
2. 单击底部面板中的**关闭**。
3. 当 VM 已停止时，单击**移除**。

4. 在**移除虚拟机**对话框中，激活要删除的卷旁边的复选框。取消选中要保存为存档的卷或要为附加到另一个 VM 而保存的卷的复选框。



小心：确认正确选择了要移除的 VM 和卷。单击**删除 VM**后，这些项目将永久删除。

5. 单击**删除 VM**会永久删除此 VM 以及任何选中的卷。

相关主题

[重命名虚拟机](#)

[创建和迁移虚拟机](#)

[管理虚拟机的运行](#)

管理虚拟机资源

管理物理机资源，以便重新配置现有虚拟机的 vCPU、内存、存储或网络资源。

要配置虚拟机资源，则使用**重新配置虚拟机**向导，如以下部分中所述：

- [重新配置虚拟机资源](#)

要配置虚拟机卷，请参阅以下任务特定主题：

- [在虚拟机中创建卷](#)
- [将卷附加到虚拟机](#)
- [将卷与虚拟机分离](#)
- [将卷从虚拟机中移除](#)
- [扩展 ztC Edge系统上的卷](#)

要恢复虚拟机资源，则为新卷或虚拟 CD 释放空间，请参阅：

- [恢复虚拟机资源](#)

重新配置虚拟机资源

重新配置虚拟机 (VM)，以便更改其虚拟 CPU (vCPU)、内存、存储或网络资源的分配。

启动**重新配置虚拟机**向导，操作是单击**配置** – 在**虚拟机**页的底部窗格中。此向导将帮助您逐步完成将资源重新分配给 VM 的过程。

先决条件：

- 查看将 vCPU、内存、存储和网络资源分配给 VM 的前提条件和注意事项，如 [计划虚拟机资源](#) 中所列出的。有关存储资源的更多信息，请参阅 [计划虚拟机存储](#)。
- 要重新配置 VM，您必须关闭 VM。

要重新配置虚拟机

1. 打开 **虚拟机** 页 (请参阅 [“虚拟机”](#) 页)。
2. 选择一个 VM，然后单击 **关闭**。
3. 当此 VM 已停止时，单击 **配置**，以显示 **重新配置虚拟机** 向导。
4. 在 **名称和描述名称、描述和保护** 页上：
 - a. 键入此 VM 的 **名称** 和可选 **描述** – 当它们显示在 ztC Console 中时
此 VM 名称必须符合以下要求：
 - VM 名称的开头必须是单词或数字，并且名称不能包含特殊字符 (例如，#、% 或 \$)。
 - VM 名称不能使用带有连字符的前缀，例如 **Zombie-** 或 **migrating-**。
 - VM 名称最多具有 85 个字符。
 - b. 选择将对此 VM 使用的保护级别：
 - **容错 (FT)**
 - **高可用性 (HA)**有关这些保护级别的更多信息，请参阅 [创建新虚拟机](#) 和 [操作模式](#)。
 - c. 单击 **下一步**。
5. 在 **VCPU 和内存** 页上：
 - a. 指定要分配给 VM 的 **vCPU** 数和 **内存** 量。有关更多信息，请参阅 [计划虚拟机 vCPU](#) 和 [计划虚拟机内存](#)。
 - b. 单击 **下一步**。

6. 在卷页上，您可以：

**注意：**

您无法修改 VM 启动卷，只能修改数据卷.但您可以分离启动卷。

- 单击**启动卷**，分离启动卷。



小心：如果您分离启动卷，VM 会变得不可启动。

将显示一条警告，说明分离启动卷导致 VM 变得不可启动。如果您要撤销分离启动卷，则单击**撤销分离**。

- 单击**分离**，以便将卷与虚拟机分离，并保留它，以供未来使用。
- 单击**删除**，以便将卷从 ztC Edge 系统中永久移除。
- 从下拉菜单(如果显示)中选择一个未附加的卷，然后单击**附加**。

如适用，您还可以单击**添加新卷**，以便创建一个新数据卷。(如果没有显示该按钮，则向下滚动到此向导页的底部。)

对于未附加的卷或新卷，指定卷的参数：

- a. 键入卷的**名称**。
- b. 键入**卷大小**，单位为千兆字节 (GB)。有关分配存储的更多信息，请参阅和[计划虚拟机存储](#)。
- c. 如适用，单击**附加**，将卷连接到 VM。

要继续，单击**下一步**。

7. 在**网络**页上，激活要附加到 VM 的各共享网络的复选框。

对于要附加的各共享网络，您还可以(可选)：

- 设置自定义 **MAC 地址**(有关详细信息，请参阅[将特定 MAC 地址分配给虚拟机](#))。
- 把**状态**设定为**启用**或**禁用**，这个设置用于允许或阻挡到选定网络的网络流量。

有关更多信息，请参阅[计划虚拟机网络](#)。要继续，单击**下一步**。

8. 在**配置摘要**页上：



小心：确保标记为移除的任何卷均是正确的。在单击**完成**时，标记为移除的磁盘上的数据会永久丢失。

- a. 查看配置摘要。如果您需要进行更改，则单击**后退**。
 - b. 要接受如所配置的 VM，则单击**完成**。
9. 单击**启动**，以便重启 VM。
 10. 对于基于 Windows 的 VM，如果您将基于 Windows 的 VM 中分配的虚拟 CPU 数从 1 更改为 n 或者从 n 更改为 1，则在重新配置过程结束时重启 VM 后，您必须关闭并再次重启 VM。这可使 VM 对自身进行正确重新配置，以实现对称多处理 (SMP)。在重启前，VM 显示奇怪行为，并且无法使用。

相关主题

[管理虚拟机资源](#)

[计划虚拟机资源](#)

[管理虚拟机](#)

在虚拟机中创建卷

创建一个卷，以便将新的空白卷附加到虚拟机 (VM)。(您还可以附加未附加的现有卷，如[将卷附加到虚拟机](#)中所述。)



先决条件：在为 VM 创建卷前，您必须关闭 VM。

要在 VM 中创建一个新卷

1. 打开[虚拟机](#)页(请参阅[“虚拟机”](#)页)。
2. 选择一个 VM，然后单击**关闭**。
3. 当此 VM 已停止时，单击**配置**，以显示**重新配置虚拟机**向导。
4. 在每个向导页上单击**下一步**，直到显示**卷**页为止。(如果适用，请参阅[重新配置虚拟机资源](#)，以配置其他 VM 资源。)
5. 在**卷**页上，单击**添加新卷**。(如果没有显示该按钮，则向下滚动到此向导页的底部。)

6. 在**将创建**下，执行以下操作：
 - a. 键入此卷的**名称** – 当它们显示在 **ztC Console** 中时。
 - b. 键入**卷大小**，单位为千兆字节 (GB)。有关分配存储的更多信息，请参阅和 [计划虚拟机存储](#)。
7. 在每个向导页上单击**下一步**，直到显示**配置摘要**页为止。验证配置是否更改。
8. 单击**完成**，以创建此卷。
9. 启动 **VM**，使此卷准备好用于客人操作系统，如以下部分中所述：
 - [创建和初始化磁盘\(基于 Windows 的 VM\)](#)
 - [创建和初始化磁盘\(基于 Linux 的 VM\)](#)

相关主题

[将卷与虚拟机分离](#)

[将卷从虚拟机中移除](#)

[管理虚拟机资源](#)

[计划虚拟机资源](#)

[管理虚拟机](#)

将卷附加到虚拟机

附加卷，以便将当前未使用的卷连接到虚拟机。



注意：如果您将启动卷连接到已经具有启动卷的 **VM**，则新添加的卷将作为数据卷连接。您可能想要以这种方式连接卷，以便诊断其他 **VM** 启动卷中的启动问题或数据损坏。使用客人操作系统工具解决此问题后，分离此卷，然后将其重新连接到其原始 **VM**。



先决条件：在将卷附加到虚拟机前，您必须关闭虚拟机。

要将卷附加到虚拟机

1. 确保其他虚拟机没有使用您要附加的卷；否则您无法附加该卷。打开**卷**页，查找该卷，并确保**使用者**列中的值为**无**。
2. 打开**虚拟机**页(请参阅[“虚拟机”](#)页)。
3. 选择一个 **VM**，然后单击**关闭**。

4. 当此 VM 已停止时，单击 **配置**，以显示 **重新配置虚拟机** 向导。
5. 在每个向导页上单击 **下一步**，直到显示 **卷** 页为止。(如果适用，请参阅 [重新配置虚拟机资源](#)，以配置其他 VM 资源。)
6. 在 **卷** 页上，找到 **添加新卷** 按钮旁的下拉菜单。从该下拉菜单中选择一个未附加的卷，然后单击 **附加**。
(如果没有显示该下拉菜单，则向下滚动到此向导页的底部。仅在 **ztC Edge** 系统上有未附加的卷时才显示该下拉菜单。)
7. 在每个向导页上单击 **下一步**，直到显示 **配置摘要** 页为止。验证配置是否更改。
8. 单击 **完成**，附加所选的卷。

相关主题

[在虚拟机中创建卷](#)

[将卷与虚拟机分离](#)

[将卷从虚拟机中移除](#)

[管理虚拟机资源](#)

[计划虚拟机资源](#)

[管理虚拟机](#)

将卷与虚拟机分离

分离卷，以便断开其与虚拟机的连接，并留待未来使用，或者将其附加到其他虚拟机，如 [将卷附加到虚拟机](#) 中所述。(您还可以将该卷从 **ztC Edge** 系统中永久删除，如 [将卷从虚拟机中移除](#) 中所述。)



注意：如果将启动卷与 VM 分离，您无法启动该 VM；但您可能想要分离启动卷，以便诊断该 VM 中的启动问题或数据损坏。您可以将启动卷作为数据卷临时附加到其他 VM，如 [将卷附加到虚拟机](#) 中所述。使用客人操作系统工具解决此问题后，分离此卷，然后将其重新连接到其原始 VM。



先决条件：在将卷与虚拟机分离前，您必须关闭虚拟机。

要将卷与虚拟机分离

1. 打开[虚拟机](#)页(请参阅“[虚拟机](#)”页)。
2. 选择一个 VM, 然后单击**关闭**。
3. 当此 VM 已停止时, 单击**配置**, 以显示**重新配置虚拟机**向导。
4. 在每个向导页上单击**下一步**, 直到显示**卷**页为止。(如果适用, 请参阅[重新配置虚拟机资源](#), 以配置其他 VM 资源。)
5. 在**卷**页上, 找到要分离的卷。(如果没有显示该卷, 则向下滚动此向导页。)
6. 单击卷名称旁的**分离**, 以标记要分离的卷。



小心: 仔细标记要分离的正确卷, 避免标记当前正在使用的任何卷。

7. 在每个向导页上单击**下一步**, 直到显示**配置摘要**页为止。验证配置是否更改。
8. 单击**完成**, 分离所选的卷。

相关主题

[将卷附加到虚拟机](#)

[将卷从虚拟机中移除](#)

[管理虚拟机资源](#)

[计划虚拟机资源](#)

[管理虚拟机](#)

将卷从虚拟机中移除

移除虚拟机 (VM) 卷, 以便将其从 ztC Edge 系统中永久删除。(您还可以将卷与 VM 分离, 但保留它, 以供未来使用, 如[将卷与虚拟机分离](#)中所述。)



先决条件: 在移除附加到虚拟机的卷前, 您必须关闭虚拟机。

要移除附加到虚拟机的卷

1. 打开[虚拟机](#)页(请参阅“[虚拟机](#)”页)。
2. 选择一个 VM, 然后单击**关闭**。
3. 当此 VM 已停止时, 单击**配置**, 以显示**重新配置虚拟机**向导。

4. 在每个向导页上单击**下一步**，直到显示**卷页**为止。(如果适用，请参阅[重新配置虚拟机资源](#)，以配置其他 VM 资源。)
5. 在**卷页**上，找到要删除的卷。(如果没有显示该卷，则向下滚动此向导页。)
6. 单击卷名称旁的**删除**，以标记要删除的卷。



小心：仔细标记要移除的正确卷，避免标记当前正在使用的任何卷。

7. 在每个向导页上单击**下一步**，直到显示**配置摘要页**为止。验证配置是否更改。
8. 单击**完成**，永久删除所选的卷。

要移除未附加的卷



小心：在移除卷前，确保其他管理员不再需要此卷。

1. 打开**卷页**。
2. 选择一个未附加的卷。(使用者列必须显示**无**，否则不显示**移除**按钮。)
3. 单击**移除**。

相关主题

[将卷与虚拟机分离](#)

[将卷附加到虚拟机](#)

[管理虚拟机资源](#)

[计划虚拟机资源](#)

[管理虚拟机](#)

重命名 ztC Edge系统上的卷

重命名 ztC Edge系统上的卷，以便更改其在**卷页**上显示的名称。

如果您需要更改在虚拟机中运行的客人操作系统中的磁盘或卷的名称，则使用客人操作系统工具。

要重命名 ztC Edge系统上的卷

1. 在**卷页**上找到此卷。
2. 双击此卷的名称。

3. 指定新名称，然后按 **Enter**。

相关主题

[在虚拟机中创建卷](#)

[将卷与虚拟机分离](#)

[将卷从虚拟机中移除](#)

[管理虚拟机资源](#)

[计划虚拟机资源](#)

[管理虚拟机](#)

扩展 ztC Edge系统上的卷

扩展虚拟机 (VM) 卷，以便为客人操作系统中的程序和数据分配更多空间。

您可扩展卷，但无法减小卷的大小。仅当 VM 已停止时，使用以下操作程序扩展卷。

先决条件：



- 在扩展 VM 包含的卷前，必须关闭 VM。
- 确保 ztC Edge 系统的两台 PM 均在线；否则，系统将无法正确扩展卷。

要扩展卷

1. 在已授权用于两个节点的系统的 **物理机** 页面(参阅“[物理机](#)”页)上，确认两台 PM 都处于运行状态，并且两台 PM 都不是处于维护模式或正在进行同步。
2. 在 **虚拟机** 页(请参阅“[虚拟机](#)”页)上，选择包含您要扩展的卷的 VM。确保该 VM 已停止。
3. 在底部窗格中，单击 **卷** 选项卡，然后选择您要扩展的卷。在 **操作** 列中，单击 **扩展卷**。
4. 在 **扩展方式** 旁，键入要添加到卷的存储空间大小(单位为千兆字节 (GB))。在输入数字后，对话框中将显示在完成操作后将获得的 **扩展后卷大小**。



注意：仔细考虑 **扩展方式** 条目，因为在扩展卷后将无法撤消更改，也无法减小卷大小；只允许进一步扩展卷。

5. 单击 **扩展卷** 来执行更改并扩展卷。对话框将显示扩展进度，并在操作完成后自动关闭。

相关主题

[在虚拟机中创建卷](#)

[将卷与虚拟机分离](#)

[将卷从虚拟机中移除](#)

[管理虚拟机资源](#)

[计划虚拟机资源](#)

[管理虚拟机](#)

恢复虚拟机资源

为节约存储空间，当不再需要 VM 资源时，将它们移除。当对于某些任务没有足够的空间时，例如创建卷或 VCD，您可能需要立即恢复存储空间。

要恢复存储空间，则移除未使用的资源，如以下主题所述：

- [移除虚拟机](#)
- [将卷从虚拟机中移除](#)
- [移除虚拟 CD](#)

相关主题

[管理虚拟机资源](#)

[计划虚拟机资源](#)

[管理虚拟机](#)

管理虚拟 CD

创建和管理虚拟 CD (VCD)，以便使软件安装介质能够以 ISO 格式用于您 ztC Edge 系统上的虚拟机。

VCD 是一种驻留在 ztC Edge 系统的存储设备上的只读 ISO 映像文件。使用 [虚拟 CD 创建向导](#) (ztC Console 中) 上传现有 ISO 文件，如 [创建虚拟 CD](#) 中所述。

创建 VCD 后，您可以从它启动来安装 Windows 或 Linux 客人操作系统，或者从可启动的恢复 VCD 启动 VM。您可以将 VCD 下载到您的本地计算机。您还可以将 VCD 插入正在运行的 VM 来安装软件应用程序。

您可以按照如以下部分中所述的那样管理 VCD：

- [创建虚拟 CD](#)
- [插入虚拟 CD](#)
- [弹出虚拟 CD](#)
- [从虚拟 CD 启动](#)
- [重命名虚拟 CD](#)
- [下载虚拟 CD](#)
- [移除虚拟 CD](#)

已被分配了**管理员**或**平台管理员**角色的用户可执行所有 VCD 任务。已被分配了**VM 管理员**角色的用户可执行除重命名 VCD 外的所有 VCD 任务。(有关分配这些角色的信息,请参阅[管理本地用户帐户](#)。)

创建虚拟 CD

创建和管理虚拟 CD (VCD), 以便使软件安装介质可用于您 ztC Edge 系统上的虚拟机 (VM)。

要创建 VCD, 则使用**虚拟 CD 创建向导**, 将 ISO 文件上传或复制到 ztC Edge 系统上的存储设备。此后, 您可以从它启动(请参阅[从虚拟 CD 启动](#))来安装客人操作系统, 或者从可启动的恢复 VCD 启动 VM。您还可以将 VCD 插入正在运行的 VM([插入虚拟 CD](#))来安装软件应用程序。

注释:



1. 除非您经常使用 VCD, 否则在不需要时将其移除。
2. 如果您创建用于安装的可启动 VCD, 则它必须为单张 CD 或 DVD。不支持多张 CD 或 DVD。

要创建 VCD

1. 必要时, 对于您将为其创建 VCD 的任何物理介质, 创建其 ISO 文件。
2. 打开**虚拟 CD**页(在 ztC Console 中)。
3. 单击**创建 VCD**, 打开**虚拟 CD 创建向导**。
4. 为该 VCD 键入一个名称。
5. 选择该 VCD 的来源。
 - **上传 ISO 文件**可从运行 ztC Console 的系统上传文件。单击**浏览**, 选择您系统上的 ISO 文件, 然后单击**打开**。

- **从网络来源复制 CD ISO** 可从 Web URL 复制文件。指定 ISO 文件的 URL。
6. 单击 **完成**，以便从指定的来源上传或复制 ISO 文件。

虚拟 CD 创建向导 显示上传的进度。

您可以通过在 **虚拟 CD** 页面上查看 **状态** 列来确定 VCD 状态：

- 同步图标 (🔄) 表示该 VCD 仍在创建中。
- 破碎图标 (✖) 表示 VCD 创建失败。移除该 VCD，然后尝试重新创建。
- 正常图标 (✔) 表示传输已完成，并且该 VCD 已可以使用。

相关主题

[插入虚拟 CD](#)

[弹出虚拟 CD](#)

[管理虚拟 CD](#)

[创建和迁移虚拟机](#)

插入虚拟 CD

将虚拟 CD (VCD) 插入虚拟机 (VM)，以便在将应用程序安装到客人操作系统中时访问安装介质。(要附加 USB 设备，请参阅 [将 USB 设备附加到虚拟机](#)。要从 VCD 启动虚拟机，请参阅 [从虚拟 CD 启动](#)。)



小心： 当您将 VCD 插入正在运行 VM 中时，其可防止在出现故障时 Stratus Redundant Linux 软件从 VM 迁移到其他物理机。要恢复冗余，则在您一用完此 VCD 时就将其卸载和弹出。



注意： 默认情况下，允许将 VCD 插入 VM。要更改此配置，请参阅 [配置 VM 设备](#)。

要将 VCD 连接到 VM

1. 必要时，为您需要访问的软件安装介质创建一个 VCD(请参阅 [创建虚拟 CD](#))。
2. 在 **虚拟机** 页上，选择一个 VM。
3. 在底部窗格中，单击 **CD 驱动器和 USB 设备** 选项卡。
4. 要选择一个 VCD，则单击 **插入 CD**，然后选择一个 VCD。使用下拉菜单(如果存在)。

当系统已插入了 VCD 时，其名称会显示在 **CD-ROM** 的右侧。

相关主题

[创建虚拟 CD](#)

[弹出虚拟 CD](#)

[从虚拟 CD 启动](#)

[管理虚拟 CD](#)

弹出虚拟 CD

弹出虚拟 CD (VCD)，以便断开它与虚拟机 (VM) 的连接。弹出 VCD 可使您将另一个 VCD 插入 VM 中。这还可使该 VCD 能够插入其他 VM 中。

要将 VCD 从 VM 中弹出

1. 将该 VCD 从客人操作系统中卸载，以确保它未在使用。
2. 在**虚拟机**页上，选择一个 VM。
3. 单击下部框中的 **CD 驱动器和 USB 设备** 选项卡。
4. 在 **CD 驱动器** 选项卡上，单击**弹出 CD**。

相关主题

[创建虚拟 CD](#)

[插入虚拟 CD](#)

[从虚拟 CD 启动](#)

[管理虚拟 CD](#)

从虚拟 CD 启动

从虚拟 CD (VCD) 启动虚拟机，以便安装客人操作系统或执行维护。

在从 VCD 启动前，您必须关闭虚拟机。

要从 VCD 启动虚拟机

1. 必要时从可启动 CD/DVD 创建一个 VCD(请参阅 [创建虚拟 CD](#))。
2. 在**虚拟机**页上，选择一个虚拟机。

3. 如果该虚拟机正在运行，则单击**关闭**。
4. 当虚拟机状态显示**已停止**时，单击下部窗格中的**从 CD 启动**。
5. 选择可启动 VCD，然后单击**启动**。



注意：从 VCD 启动的基于 Windows 的虚拟机可作为硬件虚拟机 (HVM) 启动，并且它只能访问前三个磁盘卷。

相关主题

[创建虚拟 CD](#)

[插入虚拟 CD](#)

[弹出虚拟 CD](#)

[管理虚拟 CD](#)

[创建和迁移虚拟机](#)

[管理虚拟机的运行](#)

重命名虚拟 CD

重命名虚拟 CD (VCD)，以便更改其在**虚拟 CD** 页上显示的名称。

要重命名 VCD

1. 在**虚拟 CD** 页上找到此 VCD。
2. 双击此 VCD 的名称。
3. 指定新名称，然后按 **Enter**。

相关主题

[移除虚拟 CD](#)

[插入虚拟 CD](#)

[弹出虚拟 CD](#)

[创建虚拟 CD](#)

[管理虚拟 CD](#)

下载虚拟 CD

下载虚拟 CD (VCD), 以便使 VCD 上的软件以后可用于进行上传。



先决条件: 如果尚未创建 VCD, 则必须首先创建它。请参阅[创建虚拟 CD](#)。

要下载 VCD

1. 打开**虚拟 CD**页(在 ztC Console 中)。
2. 单击您要下载的 VCD 的名称。
3. 单击**下载**。将打开一个窗口, 显示您本地计算机上的一个文件夹。
4. 为此文件选择一个目的地, 然后单击**保存**。

根据文件大小, 下载可能需要几分钟才能完成。

相关主题

[管理虚拟 CD](#)

移除虚拟 CD

移除虚拟 CD (VCD), 以便将其从 ztC Edge 系统中永久删除。

要移除 VCD

1. 在 ztC Console 中, 单击**虚拟 CD**。
2. 在该列表中找到您要移除的 VCD。
3. 确保此 VCD 的**可移除**列显示**是**。如果该值为**否**, 则表明此 VCD 当前正在使用。
4. 选择此 VCD, 然后在下部窗格中单击**移除**。

相关主题

[重命名虚拟 CD](#)

[插入虚拟 CD](#)

[弹出虚拟 CD](#)

[创建虚拟 CD](#)

[管理虚拟 CD](#)

高级主题(虚拟机)

以下主题描述了针对高级用户的程序和信息：

- [将特定 MAC 地址分配给虚拟机](#)
- [为虚拟机选择首选 PM](#)
- [强制 VM 启动](#)
- [更改虚拟机的保护级别\(HA 或 FT\)](#)
- [配置虚拟机的启动顺序](#)
- [为故障虚拟机重置 MTBF](#)
- [将USB 设备附加到虚拟机](#)

关于虚拟机运行的管理，请参阅[管理虚拟机的运行](#)。

将特定 MAC 地址分配给虚拟机

如果您需要覆盖虚拟机 (VM) 的默认媒体访问控制 (MAC) 地址，则将特定 MAC 地址分配给该虚拟机。

警告：



1. 默认情况下，Stratus Redundant Linux软件自动为 VM 分配 MAC 地址。除非您有特定要求(例如，支持基于 MAC 地址授权的软件应用程序)，负责不要覆盖这些默认设置。
2. 如果您更改静态系统 IP 地址，在 VM 重启时，自动分配给 VM 的任何 MAC 地址都将更改，因为Stratus Redundant Linux软件会根据系统 IP 地址为 VM 生成 MAC 地址。要防止 VM 的 MAC 地址发生更改，则按照以下程序中的说明设置永久 MAC 地址。请联系您的网络管理员，为您的环境生成一个有效 MAC 地址，并且记得根据新 MAC 地址更新任何防火墙规则。



先决条件：在修改虚拟机的 MAC 地址前，您必须关闭 VM。

要将特定 MAC 地址分配给 VM

1. 打开[虚拟机](#)页(请参阅[“虚拟机”](#)页)。
2. 选择一个 VM，然后单击**关闭**。

3. 当此 VM 已停止时，单击 **配置**，以显示 **重新配置虚拟机** 向导。
4. 在每个向导页上单击 **下一步**，直到显示 **网络** 页为止。(如果适用，请参阅 [重新配置虚拟机资源](#)，以配置其他 VM 资源。)
5. 在 **网络** 页上，查找要修改的网络，并且记录当前 **MAC** 地址，以免您需要还原它。
6. 在 **MAC 地址** 列中键入新地址，或者使文本区域留空，以便使 **Stratus Redundant Linux** 软件能够自动分配 **MAC** 地址。
7. 单击 **完成**。

相关主题

[高级主题\(虚拟机\)](#)

[管理虚拟机资源](#)

[管理虚拟机的运行](#)

为虚拟机选择首选 PM

在已授权用于两个节点的系统上，选择首选物理机，以便确保虚拟机在 **ztC Edge** 系统的特定物理机上运行。



注意：在默认情况下，该系统会自动均衡这两个物理机上的虚拟机负载。除非您具有特定负载均衡要求，否则不要修改此设置。

要选择首选物理机

1. 在 **虚拟机** 页上，选择一个虚拟机。
2. 在底部窗格中，单击 **负载均衡** 选项卡。
3. 从下拉列表中选择您的首选项，然后单击 **保存**。

相关主题

[高级主题\(虚拟机\)](#)

[管理虚拟机的运行](#)

强制 VM 启动

您可以使用“虚拟机”页上的 **强制启动** 按钮强制 VM 启动。但仅当 **ztC Console** 报告配对节点已关闭或不可及时，**强制启动** 按钮才处于活动状态。当使用 **强制启动** 使 VM 联机时，手动绕过系统的安全

检查，以保护数据，因此，在使用**强制启动**时必须格外谨慎，并充分了解其使用它的条件和后果。



小心：使用**强制启动**前，请阅读此整个主题，以及咨询您的授权Stratus 服务代表。服务代表可查看您的系统，包括上次卷同步的日期，然后可与您讨论使用**强制启动**的全部影响。然后，您可以与您的服务代表一同决定是否强制 VM 启动。

在使用**强制启动**使 VM 联机时，请选择一个您要强制 VM 启动所在的节点(即，可访问的节点)。无论该节点上数据的实际情况如何(例如，数据的状态、上一次同步、卷的状况等)，所有这些数据均被标记为有效。

在**强制启动**过程中，将使用启动了强制启动过程的日期和时间标记 VM 的卷。VM 的 AX 组件(即，VM 的 AX 对)使用 VM 卷上的数据，并传达这些数据的状态，以确定哪个 AX 包含最新的卷信息。**强制启动**过程会覆盖防止 VM 在脑裂条件下运行的内置逻辑。如果 AX 对无法进行通信，则会发生脑裂情况并破坏数据完整性(有关脑裂情况的信息，请参阅[创建 ALSR 配置](#))。

警告：在以下情况下，请勿使用**强制启动**：

- 一个或多个卷是您将执行**强制启动**所在节点上未完成的镜像副本的目标。
- 未完成的镜像副本的目标不良，即使在使用**强制启动**时也将不可用。
- 未同步这些卷。例如以下两种情况：
 - VM 的两个 AX 必须都有权访问 VM 的所有数据卷。
 - 在具有多个卷的系统上，VM 需要这两个 AX 都在运行，以便使 VM 有权访问其所有卷，因为每个节点都有不同卷的绿色选中复本，并且该卷在相对节点上的镜像副本未被绿色选中。
- 这两个节点都需要，因为多个 VM 已降级，而在相对节点上已被绿色选中(例如，Node0 的启动卷很好，但数据卷不好，而 Node1 的启动卷不好，但数据卷很好)。
- 已授权将该系统用于单节点。

如果您在具有过时卷上执行**强制启动**，则立即联系您的授权Stratus 服务代表。如果这两个节点均已启动并已开始同步数据，则系统将使用您强制启动的 VM 中的数据，并且您无法恢复不可及节点上的数据。

但在某些情况下，在具有过时卷的系统上使用**强制启动**后，您或许能够恢复数据：

- 如果不可及节点仍然关闭，则不要启动它。
- 如果在单击**强制启动**之前关闭了不可及节点的电源，则将保护已关闭节点上 VM 的 AX，并且在以下情况下，您可反向执行**强制启动**，同时不会丢失数据：

- 您强制启动的 VM 没有新数据(即,该 VM 尚未投入生产)。
- 在强制启动此 VM 之前,不可及节点上 VM 的 AX 未与您将强制启动的 VM 的 AX 交换状态。
- 已解决了阻止不可及节点上 VM 的 AX 启动这一问题。
- 两个节点之间的所有 VM 数据均已准确进行了同步。系统没有以下情况的 VM: 在每个 VM 有两个 AX 组件中,一个节点上 VM AX 的数据与另一节点上 VM AX 的数据处于不同状态。

如果您的系统符合以上所有条件,则联系您的授权 Stratus 服务代表,以便获得有关恢复过程的建议。

如果您已决定强制启动某个 VM,则确保通过执行这些先决程序,为其做好准备。

先决条件:



- 手动检查所有卷,以确保您可安全地覆盖它们。例如,应绿色选中卷状态,并且应完成磁盘同步。
- 确定 VM 的两个 AX 组件是否都可进行通信,并可使这些系统进程能够确定每个卷的状态。为防止出现脑裂情况,必须确保 VM 的两个 AX 组件均可传达状态,并可确定哪个 AX 具有良好的数据和良好的启动卷。
- 确保已授权将该系统用于两个节点。
- 请联系您的授权 Stratus 服务代表。

要强制 VM 启动

在您咨询了您的授权 Stratus 服务代表并且已决定强制启动某个 VM 后,请执行以下程序。在这些示例中,node0 已脱机,node1 为主节点,VM-1 已停止。

1. 在已授权用于两个节点的系统的 ztC Console 中,单击左侧面板中的 **虚拟机**。
2. 导航到 **虚拟机** 页。
3. 在 **虚拟机** 页上,选择已停止并且您要强制启动的 VM(例如,VM-1)。
4. 在底部窗格中,单击 **启动** 按钮。

此 VM 开始启动。它会继续启动,直至达到超时限制(可能长达 5 分钟)为止。达到超时限制后,**强制启动** 按钮将变为活动状态。

5. 要强制启动此 VM,则单击 **强制启动**。

此时将显示一条警告，询问您是否确定知道哪个节点具有最新的 VM 数据。该警告还会告诉您注意可能出现数据丢失。此外还会显示一条消息，告诉您可强制此 VM 所在的节点。



小心：如果在**强制启动**过程中选择了错误节点，则会损坏数据。

您必须按照此消息中的指示键入节点(`node0` 或 `node1`)。例如以下命令：

强制启动 VM-1

 不要继续，除非您确定知道哪个节点具有您最新的 VM 数据。请注意，数据可能丢失。

只有 `node1` 可以强制启动。

如果您要在 `node1` 上启动 Vm，则键入 `node1`：

`node1`

[确定按钮] [取消按钮]

- 单击**确定**，强制启动此节点(例如 `node1`)。(单击**取消**，取消此程序。)随着强制启动过程的开始和继续，在 VM 启动之前会显示其他确认消息，并且这些数据会被标记为对系统有效。

此 VM 开始运行。在**虚拟机**页上列出了该 VM 并带有警告，因为该节点(例如，`node0`)仍处于脱机状态。

将辅助节点重新带回系统后，所有数据均从运行此 VM 的节点进行同步。在该示例中，所有数据均从 `node1` 同步到 `node0`。

相关主题

[高级主题\(虚拟机\)](#)

[管理虚拟机的运行](#)

更改虚拟机的保护级别(HA 或 FT)

您可以将客人 VM 的保护级别从高可用性 (HA) 更改为容错 (FT)，反之亦然。

要更改保护级别

1. 在**虚拟机**页上，选择一个已停止的 VM(在**活动**列中标记为“已停止”)。(有关停止 VM 的信息，请参阅[关闭虚拟机](#)。)
2. 在下部窗格，单击**配置**来打开向导**重配虚拟机**
3. 在**名称、描述和保护**页上，选择 **HA** 或 **FT** 按钮。
4. 在这些向导页中继续单击，直至到达最后一页。按**完成**，然后按**确定**(如果重新配置成功)。

相关主题

[操作模式](#)(HA 或 FT)

[高级主题](#)(虚拟机)

[管理虚拟机的运行](#)

配置虚拟机的启动顺序

配置虚拟机的启动顺序，以便设置客人操作系统和应用程序在 **ztC Edge**系统上的启动顺序。

确定所需的启动顺序，然后相应地为每个虚拟机配置启动设置。

要设置虚拟机的启动顺序

1. 在**虚拟机**页上，选择一个虚拟机。
2. 在底部窗格中，单击**启动顺序**选项卡。
3. 配置启动设置，如下所述。
4. 单击 **保存**。

启动设置如下：

- **优先级组**可使用户指定启动 **ztC Edge** 系统后或者故障转移后虚拟机的启动顺序，这需要重启虚拟机。一些业务解决方案要求在启动其他虚拟机前，特定虚拟机正在运行。第 **1** 组具有最高优先级，**无**则是优先级最低。**Stratus Redundant Linux**软件等待 **OS** 和**应用程序启动时间**已过后再启动下一个优先级组中的虚拟机。

启动顺序示例：

VM	优先级组	OS 和应用程序启动时间
DNS	1	2 分钟
App	2	30 秒
DB	2	10 分钟
Web	3	0

- 1 ztC Edge 启动 DNS VM。
 - 2 DNS VM 启动后 2 分钟，ztC Edge 将启动第 2 组中的 APP 和 DB 服务器。
 - 3 DB VM 启动后 10 分钟，ztC Edge 将启动第 3 组中的 Web VM。
- 应将 **OS 和应用程序启动时间** 设置为在客人操作系统和应用程序完全正常运行前启动虚拟机所需的时间。

相关主题

[高级主题\(虚拟机\)](#)

[管理虚拟机的运行](#)

为故障虚拟机重置 MTBF

为故障虚拟机重置平均故障间隔时间 (MTBF) 计数器，以便尝试重启故障虚拟机。

如果虚拟机的客人 OS 崩溃，ztC Edge 会自动重启该虚拟机，除非它已低于其 MTBF 阈值。如果虚拟机低于此 MTBF 阈值，则 ztC Edge 会使其保持在崩溃状态。必要时，您可以重置 MTBF 计数器并重启虚拟机。



小心：除非您的授权 Stratus 服务代表指示您重置 MTBF 计数器，否则不要执行此操作，因为这样做可能影响您系统的持续正常运行时间。

注释：



1. 仅在虚拟机低于其 **MTBF** 阈值时才显示**重置设备**按钮。
2. 仅当在一台物理机上支持 **VM** 的系统软件低于其 **MTBF** 阈值时才显示**清除 MTBF**按钮。

要重置虚拟机的 **MTBF** 计数器

1. 在**虚拟机**页上，选择一个虚拟机。
2. 单击**重置设备**。

如果支持一个物理机上的 **VM** 的系统软件经常出现故障，则执行以下步骤，重置其 **MTBF** 计数器。

重置一台物理机上的一个 **VM** 的 **MTBF** 计数器

1. 在**虚拟机**页上，选择一个虚拟机。
2. 单击**清除 MTBF**。

相关主题

[高级主题\(虚拟机\)](#)

[管理虚拟机的运行](#)

[创建诊断文件](#)

将**USB** 设备附加到虚拟机

将 **USB** 设备附加到虚拟机 (**VM**)，以便使 **VM** 能够使用该设备。例如，当需要基于 **USB** 的许可证以在来宾操作系统中安装应用程序时，可能需要 **USB** 设备。当您不再需要该 **USB** 设备时，将其拔出。

(如果您需要在 **ztC Edge**系统上安装 **USB** 设备来使用此设备导出或导入 **VM**，请参阅在 **ztC Edge**系统上安装 **USB** 设备或网络安装的文件夹。)

小心：



当您将一个 **USB** 设备附加到正在运行的容错 (**FT**) **VM** 时，其可防止在出现故障时 **Stratus Redundant Linux** 软件将该 **VM** 迁移到其他物理机。要恢复容错运行，则在您一用完该 **USB** 设备时就将其分离和移除。

注释：

1. 您只能将受支持的 USB 设备附加到客人操作系统。有关 ztC Edge系统支持的 USB 设备的列表，请参阅适合您系统的规范：

- [系统规范: ztC Edge 110i系统](#)
- [系统规范: ztC Edge 100i系统](#)

注意，ztC Edge系统在客人操作系统中不支持 USB 3.2 第 2 代 (10 Gbps) 或更高版本的设备。但您可以将第 2 代或更高版本的设备插入 USB 3.2 第 1 代 (5 Gbps) 设备主机端口中，这会强制该设备以第 1 代 (5 Gbps) 速度运行；在这种情况下，您可以将该设备连接到客人操作系统。(USB 3.2 第 1 代 (5 Gbps) 设备先前称为 USB 3.1 第 1 代设备，USB 3.2 第 2 代 (10 Gbps) 设备先前称为 USB 3.1 第 2 代设备。)

2. 不要将 USB 3.0(或更高版本)设备连接到运行以下操作系统之一的 VM，因为这些操作系统不支持 USB 3.0 设备：

- Windows 7 Desktop
- Windows Small Business Server 2011
- 较低版本的 Linux 发行版，例如 CentOS 6.6

3. 不要将 USB 连接的符合 SCSI (UAS) 的设备连接到 VM，因为系统不支持 UAS 设备。

4. VM 必须运行您才能将 USB 设备附加到 VM。

5. 默认情况下，允许将 USB 设备附加到 VM。要更改此配置，请参阅[配置 VM 设备](#)。

6. 使用下列任一方法从基于 Windows 的 VM 分离(即，弹出)受支持的 USB 设备：

- 单击文件资源管理器中的“弹出”-如果从文件资源管理器中弹出设备，您必须使用以下操作程序在 ztC Console 中将其分离。然后，在重新连接到相同或其他 VM 前，将其从 ztC Edge 系统中拔掉并重新插入。
- 单击任务栏中的“安全删除硬件并弹出媒体”-如果从任务栏弹出设备，您必须使用以下操作程序在 ztC Console 中将其分离。在将其重新连接到相同或其他 VM 前，您无需将其从 ztC Edge 系统中拔掉。



要将 USB 设备附加 VM

1. 将该 USB 设备插入 VM 的主(活动)节点中。

虚拟机页将每个 VM 的主节点均显示为**当前 PM**。(此节点可能与 ztC Edge系统的当前主节点不同,如**物理机**页上所示。)

确认系统显示此 USB 设备。导航到**物理机**页。单击插入了该设备的节点,然后在下部窗格中,选择**USB 设备**选项卡。您插入的 USB 设备应显示在该选项卡中。

2. 在**虚拟机**页上,选择一个 VM。
3. 在底部窗格中,单击**CD 驱动器**和**USB 设备**选项卡。
4. 在**CD 驱动器**和**USB 设备**选项卡的**USB**上,从下拉菜单中选择一个 USB 设备。
5. 单击**附加 USB**,将该 USB 设备附加到 VM。
6. 将显示**确认**对话框,询问您是否确定要附加该设备,并且显示一条警告,说明在该 USB 设备正在使用时,客人将进入单工模式。单击**是**,附加该设备。

在系统将该 USB 设备附加到 VM 后,USB 设备名称将显示在针对该 VM 的**CD 驱动器**和**USB 设备**选项卡上的 USB 设备列表中。

要将 USB 设备与 VM 分离

1. 在**虚拟机**页上,选择已附加了此 USB 设备的 VM。
2. 在底部窗格中,单击**CD 驱动器**和**USB 设备**选项卡。
3. 在**CD 驱动器**和**USB 设备**选项卡的**USB**行上,单击**分离 USB 设备**。必要时,从下拉菜单中选择该 USB 设备。
4. 将显示**确认**对话框,询问您是否确定要分离该设备。单击**是**,分离该设备。

在系统将该 USB 设备与 VM 分离后,USB 设备名称将不再显示在针对该 VM 的**CD 驱动器**和**USB 设备**选项卡上的 USB 设备列表中。

相关主题

[管理虚拟机](#)

7

第 7 章：维护物理机

要维护 ztC Edge 系统内的物理机 (PM) 或节点，可更换或恢复它们。

要替换故障 PM，则使用下列程序之一：

- [替换物理机\(自动\)](#) (建议)

描述如何利用自动节点替换过程替换故障 PM。此帮助主题补充了每个替换节点中包含的 [ztC Edge100i/110i 系统: 更换节点 \(R013Z\)](#) 中的信息。

- [更换物理机 \(手动\)](#)

描述如何通过用户启动的替换过程替换故障 PM，此过程从 ztC Console 启动和监控。除非您的授权 Stratus 服务代表具体说明，否则不要使用此用户启动的程序。

要恢复故障 PM 上的系统软件，而不是更换 PM 硬件，请参阅 [恢复故障物理机\(手动\)](#)。

要将某个节点添加到已授权用于一个节点的系统，请参阅 [将节点添加到单节点系统](#)。

替换物理机(自动)

本主题描述如何利用自动节点替换过程替换 ztC Edge 系统中的故障物理机 (PM) 或节点。其补充了 [ztC Edge100i/110i 系统: 更换节点 \(R013Z\)](#) 以下中的信息。

在系统正在运行时替换 ztC Edge 节点。

先决条件: 要请求更换 ztC Edge节点, 则登录 **Stratus 客户服务门户**, 展开 **客户支持**, 然后单击 **添加问题**。在创建此问题时, 请准备好以下信息:



- **资产 ID**—在 **窗口中查找您系统的资产 ID** ztC Console。
- **诊断文件**—在 **的支持日志** ztC Console页上生成并下载诊断文件, 如 [创建诊断文件](#) 中所述。将该诊断文件附加到您在服务门户中添加的问题。

客户服务代表将联系您, 以便诊断此问题并在必要时提供更换节点。

要替换 ztC Edge系统中的节点

1. 找到要替换的节点。关闭故障节点(自动), 或者在 **SYS LED** 不亮或常绿(运行状况不正常)时启动故障节点。如果已关闭此节点, 则跳到第 3 步。
2. 如果故障节点仍处于开启状态, 则打开 **ztC Console**, 以解决阻止关机的任何问题。例如, 正常节点上的网络连接故障可能导致对故障节点的依赖。解决任何问题并关闭故障节点。
3. 断开电源线与故障节点的连接, 然后断开网络电缆, 并将节点从系统中移除。
4. 将更换节点添加到系统。重新连接网络电缆, 然后重新连接电源, 以便自动启动节点。节点更换完成。系统开始同步, 无需用户输入。
5. 20 分钟后, **SYS LED** 循环从不亮变为常绿, 以表明更换节点上的软件正在启动。再过 15 分钟后, **SYS LED** 开始闪烁, 以表明系统运行正常。
6. 登录 **ztC Console**, 确认系统运行状况。虚拟机可继续同步数小时。同步成功完成后, **仪表盘** 应显示绿色复选标记, 并且不存在未决问题。

相关主题

[维护模式](#)

[维护物理机](#)

[ztC Console](#)

[物理机和虚拟机](#)

[“物理机”页](#)

更换物理机 (手动)



小心: 如果您需要恢复或替换 ztC Edge 系统中的 PM, 则使用 [ztC Edge 100i/110i 系统: 更换节点 \(R013Z\)](#) 中的说明。(如果需要, 请参阅 [替换物理机\(自动\)](#), 了解其他详细信息)。除非您的授权 Stratus 服务代表具体说明, 否则不要使用本主题中描述的手动程序。

在系统正在运行时更换物理机 (PM) 或节点。(如果需要恢复故障 PM 上的系统软件, 而不是更换 PM 硬件, 请参阅 [恢复故障物理机\(手动\)](#)。)

当移除并更换 PM 时, 系统会完全擦除更换 PM 中的所有磁盘, 以便为 Stratus Redundant Linux 系统软件的完全安装做准备。要安装该软件, 您可以使系统自动从主 PM 上的临时预启动执行环境 (PXE) 服务器启动更换节点。只要每个 PM 均包含最近安装的软件套件(如在 [ztC Console 的升级套件](#) 页上显示的)的完整副本, 任何一个 PM 均能够通过 PXE 启动安装开始其配对 PM 的更换。如果需要, 您还可以从 USB 安装介质手动启动替换节点。

根据在安装 (PXE 或 USB 安装) 中您要使用的介质, 使用以下操作程序之一。



小心: 此更换程序会删除在 PM 的主机操作系统中安装的所有软件, 以及在更换前输入的所有 PM 配置信息。完成此程序后, 您必须手动重新安装所有主机级软件, 并配置 PM 以匹配您的初始设置。



小心: 为防止数据丢失, 如果系统日志指示需要手动干预来组装磁盘镜像, 请联系您的授权 Stratus 服务代表寻求帮助。如果您强制重新同步并覆盖镜像中的最近磁盘, 您可能会丢失宝贵数据。

先决条件: 要请求更换 ztC Edge 节点, 则登录 [Stratus 客户服务门户](#), 展开 [客户支持](#), 然后单击 [添加问题](#)。在创建此问题时, 请准备好以下信息:



- **资产 ID**—在 [窗口中查找您系统的资产 ID](#) ztC Console。
- **诊断文件**—在 [的支持日志](#) ztC Console 页上生成并下载诊断文件, 如 [创建诊断文件](#) 中所述。将该诊断文件附加到您在服务门户中添加的问题。

客户服务代表将联系您, 以便诊断此问题并在必要时提供更换节点。

先决条件: 如果您要使用 USB 介质在更换 PM 上安装系统软件:

- 创建一个可启动 USB 介质, 如在 [创建具有系统软件的 USB 介质](#) 中所述。

在创建 USB 介质时, 确保其包含最近安装的升级套件。例如, 如果 ztC Console 窗口刊头中显示的版本为版本 1.2.0-550(其中 550 是创建号), 则在 [升级套件](#) 页上您选择创建 USB 介质的套件也必需是版本 1.2.0-550。如果系统检测到更换 PM 上有其他版本, 系统会自动重新启动此更换过程, 初始化更换 PM 上的所有数据, 以及使用 PXE 启动安装在该 PM 上重新安装最近安装的软件套件, 无需用户交互。

- 将键盘和监视器连接到更换 PM, 以便监视此安装过程并指定设置。

要拆卸和更换故障 PM (使用 PXE 启动安装)

使用以下操作程序更换故障 PM, 以及通过使用 PXE 启动安装从主 PM 上的软件套件重新安装系统软件。

1. 在 ztC Console 中, 单击左侧导航面板中的 **物理机**。
2. 选择相应的 PM (node0 或 node1), 然后单击 **维护模式**, 这会将该 PM 的 **总体状态** 更改为 **维护模式**, 以及将 **活动状态** 更改为 **正在运行 (维护中)**。
3. 在 PM 显示 **正在运行 (维护中)** 后, 单击 **恢复**。
4. 在提示选择修复类型时, 单击 **PXE PM 替换 - 初始化所有磁盘**。



小心: 选择 **PXE PM 替换 - 初始化所有磁盘** 会删除更换 PM 上的所有数据。

5. 选择下列 PXE 设置之一:

- **仅响应来自当前配对节点的 PXE 请求。**

等待来自当前配对节点 MAC 地址的 PXE 启动请求。如果您正在通过完全擦除并重新安装现有 PM 来恢复它, 则选择此选项。此过程会删除该 PM 上的所有数据, 但会还原其当前网络配置。

- **仅响应来自以下 MAC 地址的 PXE 请求。**

等待来自您指定的 MAC 地址的 PXE 启动请求。如果您正在使用新 PM 来更换该 PM, 则选择此选项。输入将开始 PXE 启动的特定网络适配器的 MAC 地址。

- 接受来自 `priv0` 上任何系统的 PXE 请求。

等待来自连接两个 ztC Edge 节点的专用网络 `priv0` 的 PXE 启动请求。如果您正在使用新 PM 来更换该 PM，但您不知道新 PM 的 MAC 地址，则选择此选项。

6. 单击**继续**，开始此更换过程。系统关机并关闭 PM 的电源。
7. 关闭 PM 的电源后，安装替换 PM(如果适用):
 - a. 断开连接并移除 PM，然后安装更换 PM。
 - b. 将网络电缆重新连接到它们原来的端口，然后重新连接电源。
8. 如果 PM 没有自动启动，则按电源按钮。
9. 此替换过程在无用户交互的情况下继续进行，如下：
 - 更换 PM 开始从临时运行于主节点的 PXE 服务器启动。
 - 系统自动删除更换 PM 中的磁盘上的所有数据。
 - 更换 PM 再次重启并自动开始系统软件安装，这是从主节点上的安装套件副本中运行的。

您无需监视此软件安装进程或响应替换 PM 的物理控制台上的提示。此替换过程是自动的，在安装过程中，PM 通常会长时间显示空白屏幕。

10. 完成软件安装后，更换 PM 会从最新安装的系统软件重启。



注意：安装了系统软件后，更换 PM 可能需要最多 20 分钟加入系统并显示在 ztC Console 中。

11. 在更换 PM 加入系统时，您可以在 的物理机 ztC Console 页上查看其活动。**活动**列将该 PM 显示为**(维护中)**，然后在更换完成后，显示为**正在运行**。该 PM 自动退出维护模式，并对系统上的 VM 进行负载均衡。
12. 如果适用，手动重新安装应用程序和任何其他主机级软件，并重新配置更换 PM 以匹配您的初始配置。



注意：当更换 PM 退出维护模式时，系统会禁用曾用于此更换过程的主节点上的 PXE 服务器。

要拆卸和更换故障 PM (使用 USB 安装)

使用以下操作程序更换故障 PM，以及通过使用 USB 介质重新安装系统软件。

1. 在ztC Console中，单击左侧导航面板中的**物理机**。
2. 选择相应的 PM(node0 或 node1)，然后单击**维护模式**，这会将该 PM 的总体状态更改为**维护模式**，以及将**活动**状态更改为**正在运行(维护中)**。
3. 在 PM 显示**正在运行(维护中)**后，单击**恢复**。
4. 在提示选择修复类型时，单击 **USB PM 替换 - 初始化所有磁盘**。



小心：选择 **USB PM 替换 - 初始化所有磁盘**会删除更换 PM 上的所有数据。

5. 单击**继续**，开始此更换过程。在准备重新安装系统软件时，系统关闭该 PM。
6. 关闭 PM 的电源后，安装替换 PM(如果适用):
 - a. 断开连接并移除 PM，然后安装更换 PM。连接监视器和键盘。
 - b. 将网络电缆重新连接到它们原来的端口。
 - c. 将可启动 USB 介质连接到更换 PM 上，然后重新连接电源线。如果 PM 没有自动启动，则按电源按钮。
7. 在替换 PM 启动过程中，进入固件(UEFI)设置实用程序。在**保存并退出**菜单的**直接启动**下，选择 **UEFI** 条目，以便使该 USB 介质在下一个启动顺序中一次从设备启动。此 PM 重启。



注意：使用**直接启动**属性临时更改启动设备，而不是在**启动**菜单中修改永久启动顺序优先级。最高启动优先级必须保持 **UEFI 网络(默认)**才能支持一般在 ztC Edge 系统上执行的自动节点更换。

8. 在更换 PM 的物理控制台上监视此安装过程。
9. 在**欢迎**屏幕上，使用箭头键为此安装选择国家/地区键盘布局。
10. 在**安装或恢复**屏幕上，选择**更换 PM, 加入系统:初始化数据**，然后按 **Enter** 键。此更换过程在无用户交互的情况下继续进行。



小心：选择**更换 PM, 加入系统:初始化数据**会删除更换 PM 上的所有数据。

11. 完成软件安装后，更换 PM 会从最新安装的系统软件重启。



注意：安装了系统软件后，更换 PM 可能需要最多 20 分钟加入系统并显示在 ztC Console 中。

12. 在更换 PM 加入系统时，您可以在 的物理机 ztC Console 页上查看其活动。**活动**列将该 PM 显示为**(维护中)**，然后在更换完成后，显示为**正在运行**。该 PM 自动退出维护模式，并对系统上的 VM 进行负载均衡。
13. 如果适用，手动重新安装应用程序和任何其他主机级软件，并重新配置更换 PM 以匹配您的初始配置。

相关主题

[维护模式](#)

[维护物理机](#)

[ztC Console](#)

[物理机和虚拟机](#)

[“物理机”页](#)

8

第 8 章：监控系统、基于 Windows 的 VM 和应用程序

在已许可用于监控的系统上，您可以监控有关性能的信息(例如，CPU 利用率)。您可以设置低值和高值，以便创建要监控的参数值范围。您还可以设置在参数值超出配置范围时发送的**自动通报**和/或**电子警报/自陷消息**。

您可以监控有关以下方面的信息：

- ztC Edge系统的主机操作系统 - 请参阅[监控 ztC Edge系统](#)。
- 基于 Windows 的 VM 上的 Windows 操作系统 - 请参阅[监控基于 Windows 的虚拟机](#)。
- 在基于 Windows 的 VM 上运行的应用程序 - 请参阅[监控基于 Windows 的虚拟机上的应用程序](#)。



注意：如果系统未获许可用于监控，则**监控**选项卡内容变灰。有关启用此功能的信息，请与您的客户代表联系。

具有 ztC Advisor的系统是一个基于 Web 的安全门户，其提供对您整个 ztC Edge 系统舰队的集中可见性，有关监控该系统的信息，请参阅[启用 ztC Advisor](#)。

监控 ztC Edge系统

监控 ztC Edge系统的主机操作系统，以便获取有关 OS 性能的信息(例如，CPU 利用率)。设置监视参数后，其值每 30 秒更新一次。

设置和查看用于监控主机操作系统的参数

1. 在 ztC Console 中，单击左侧导航面板中的 **物理机**。

2. 在下部面板中，单击 **监控** 选项卡。

监控 选项卡显示针对正在运行的每个节点的监控信息。

3. 要启用对正在运行的每个节点上的参数的监控，则激活针对该参数的最左侧列中的 **已启用** 框。

4. 设置参数值(如果适用)：

参数—CPU 利用率和内存利用率。显示值(不可设置)。

单位—百分比 (%); 最大值为 100%。显示值(不可设置)。

范围：

低—范围的低阈值。其值可以是 0 或任何正数。该值适用于两个节点。

高—范围的高阈值。其值可以是 0 或任何正数。该值必须大于 **低** 值。该值适用于两个节点。

在默认情况下，范围值为空。要输入值，请单击参数行 **低** 或 **高** 列中的单元格空间。单击此空间后，将显示一个框，您可以在其中键入值。

自动通报—当在任一节点上检测到范围之外的值时，向您的授权 **Stratus** 服务代表发送自动通报消息。

电子警报/自陷—当在任一节点上检测到超出范围的值时，将发送电子邮件警报(电子警报)和 SNMP 自陷。

第一次查看时间—在单个节点上过去 24 小时内首次检测到参数值的日期和时间。显示值(不可设置)。

最后一次查看时间—在单个节点上过去 24 小时内最后检测到参数值的日期和时间。显示值(不可设置)。

最后一个事件—单个节点上最后一次违反阈值的情况：**低** 或 **高**。空单元格表示尚未发生违反阈值的情况。显示值(不可设置)。

事件计数—在一个节点上过去 24 小时内超出范围的次数。显示值(不可设置)。

当前值—表示以下之一(显示值;不可设置)。

- 一个节点的当前值。
- 不可用 = 此值暂时不可用。

状态—在一个节点上参数的状态。显示值(不可设置)。

- 预计 (✓)= 在过去 24 小时内此参数未超出其范围。
- 警告 (⚠)= 在过去 24 小时内此参数超出了其范围,但现在未上报任何事件。
- 超出范围 (✗)= 当前超出范围。

5. 单击**保存**,保存更改,或者单击**重置**,取消任何未保存的更改。

相关主题

[监控系统、基于 Windows 的 VM 和应用程序](#)

[配置电子警报](#)

[配置 SNMP 设置](#)

[管理物理机](#)

监控基于 Windows 的虚拟机

监控基于 Windows 的 VM 上的操作系统,以便获取有关 OS 性能的信息(例如,CPU 利用率)。在运行以下操作系统的 VM 上,监控可用:

- Windows 7 Professional
- Windows 10 Professional
- Windows 10 Enterprise
- Windows Server 2012 R2 Standard
- Windows Server 2016 Standard

创建了基于 Windows 的 VM 后,您可以在**虚拟机**页面的**监控**选项卡上查看和设置监视参数。设置监视参数后,其值每 60 秒更新一次。

您首先需要安装客人监视代理(如果尚未安装)。

要安装客人监视代理

1. 在 ztC Console 中,单击**虚拟 CD**。
2. 确认列出了 **guest_monitoring_agent_n.n.n.n VCD**。
3. 在左侧面板中,单击**虚拟机**。
4. 在**虚拟机**下,选择您要在上面安装客人监视代理的 VM。
5. 插入 VCD。请参阅[插入虚拟 CD](#)。

6. 打开 VM 控制台会话。请参阅[打开虚拟机控制台会话](#)。
7. 在 VM 控制台会话中，打开一个文件资源管理器窗口，然后导航到[监视代理安装 CD](#)。
8. 双击此 CD，打开[监视代理服务设置向导](#)，在该向导中，单击下一步。
向导将安装此代理。安装完成后，单击**完成**。
9. 安装完成后，从 VM 中弹出 VCD。请参阅[弹出虚拟 CD](#)。

注释：

1. 重命名 VM 时，监控参数会消失，但会在一两分钟后再次显示。
2. 您需要确保在客人操作系统中启用了性能计数器，并且其正常运行，以便使客人监视代理获得处理器、内存和磁盘利用率信息。

设置和查看用于监控 VM 的参数

1. 在 ztC Console 中，单击左侧导航面板中的**虚拟机**。
2. 选择相应的 VM。
3. 在下部面板中，单击**监控**选项卡。

在 **Guest OS(客人 OS)** 下，该选项卡显示您可以查看和设置的参数。

4. 要启用对参数的监控，则激活最左侧列中的**已启用**框。
5. 设置参数值(如果适用)：

参数—CPU 利用率、使用的磁盘空间和内存利用率。显示值(不可设置)。

单位—百分比 (%)。显示值(不可设置)。

范围：

低—范围的低阈值。该值必须为介于 0 与 100 之间的正整数(对于 100%)。

高—范围的高阈值。该值必须为介于 0 与 100 之间的正整数(对于 100%)，并且该值必须大于**低**值。

在默认情况下，范围值为空。要输入值，请单击参数行**低**或**高**列中的单元格空间。单击此空间后，将显示一个框，您可以在其中键入值。

自动通报—当检测到范围之外的值时，向您的授权 **Stratus** 服务代表发送自动通报消息。

电子警报/自陷—当检测到超出范围的值时，将发送电子邮件警报(电子警报)和 SNMP 自陷。

第一次查看时间–在过去 24 小时内首次检测到参数值的日期和时间。显示值(不可设置)。

最后一次查看时间–在过去 24 小时内最后检测到参数值的日期和时间。显示值(不可设置)。

最后一个事件–单个节点上最后一次违反阈值的情况：**低**或**高**。空单元格表示尚未发生违反阈值的情况。显示值(不可设置)。

事件计数–在过去 24 小时内超出范围的次数。显示值(不可设置)。

当前值–表示以下之一(显示值;不可设置)：

- 当前值。
- **无响应**= Guest Monitoring Agent 在此 VM 上无响应，因为此代理未安装或已停止。要监控客人，您必须在此 VM 上手动安装或重启 Guest Monitoring Agent。
- **未运行**= 此客人未处于运行状态。
- **不可用**= 此值暂时不可用。

状态–显示值(不可设置)。

- **预计** (✓)= 在过去 24 小时内此参数未超出其范围。
- **警告** (⚠)= 在过去 24 小时内此参数超出了其范围，但现在未上报任何事件。
- **超出范围** (✗)= 当前超出范围。

6. 单击**保存**，保存更改，或者单击**重置**，取消任何未保存的更改。

相关主题

[监控系统、基于 Windows 的 VM 和应用程序](#)

[配置电子警报](#)

[配置 SNMP 设置](#)

[配置基于 Windows 的虚拟机](#)

监控基于 Windows 的虚拟机上的应用程序

监控在基于 Windows 的 VM 上运行的应用程序，以便获取有关应用程序性能的信息(例如，CPU 利用率)。

创建了基于 Windows 的 VM 后，您可以在**虚拟机**页面的**监控**选项卡上添加应用程序。然后查看和设置监控参数。设置监视参数后，其值每 60 秒更新一次。



注意：重命名 VM 时，监控参数会消失，但会在一两分钟后再次显示。

要添加或查看用于监控的应用程序参数，或者删除某个参数，您需要知道应用程序可执行文件的名称(没有例外，例如，在 `mysqld` 中)。从 Windows 实用程序中获得名称。例如，在 **任务管理器** 中，从 **进程** 选项卡上的名称列表中获得相应的名称。

添加、设置或查看应用程序及其参数

1. 在 ztC Console 中，单击左侧导航面板中的 **虚拟机**。
2. 选择正在运行您感兴趣的应用程序的 VM。
3. 在下部面板中，单击 **监控** 选项卡。

应用程序 面板显示在 **客户 OS** 面板下方。应用程序列在具有相关参数的 **应用程序** 列中。该列表下方为添加和移除按钮，可使您将应用程序和参数添加到该列表中，或者删除它们。

4. 添加应用程序和参数(如果适用)：

- a. 单击  **添加** 按钮。

将显示两个框，活动光标位于第一个(左)框中。

- b. 在第一个框中键入应用程序可执行文件的名称(没有例外，例如，在 `mysqld` 中)，或者从下拉列表中选择一个名称。
- c. 从第二个(右侧)框的下拉列表中选择要监控的参数。
- d. 单击 **保存**，保存更改(或者单击 **重置**，取消任何未保存的更改)。保存更改后，新应用程序将显示在 **应用程序** 下的列表中。

短暂延迟后，将显示新应用程序。

5. 要启用对应用程序和参数的监控，则激活最左侧列中的 **已启用** 框。
6. 设置参数值(如果适用)：

应用程序—已在 VM 上运行且已选择用于监控的应用程序。

参数—CPU 利用率和内存利用率。显示值(不可设置)。

单位—百分比 (%)。显示值(不可设置)。

范围：

低—范围的低阈值。该值必须为介于 0 与 100 之间的正整数(对于 100%)。

高—范围的高阈值。该值必须为介于 0 与 100 之间的正整数(对于 100%)，并且该值必须大于**低**值。

在默认情况下，范围值为空。要输入值，请单击参数行**低**或**高**列中的单元格空间。单击此空间后，将显示一个框，您可以在其中键入值。

自动通报—当检测到范围之外的值时，向您的授权 **Stratus** 服务代表 发送自动通报消息。

电子警报/自陷—当检测到超出范围的值时，将发送电子邮件警报(电子警报)和 **SNMP** 自陷。

第一次查看时间—在过去 24 小时内首次检测到参数值的日期和时间。显示值(不可设置)。

最后一次查看时间—在过去 24 小时内最后检测到参数值的日期和时间。显示值(不可设置)。

最后一个事件—单个节点上最后一次违反阈值的情况：**低**或**高**。空单元格表示尚未发生违反阈值的情况。显示值(不可设置)。

事件计数—在过去 24 小时内超出范围的次数。显示值(不可设置)。

当前值—表示以下之一(显示值;不可设置)：

- 当前值。
- 无响应= **Guest Monitoring Agent** 在此 VM 上无响应，因为此代理未安装或已停止。要监控客人上的应用程序，您必须在此 VM 上手动安装或重启 **Guest Monitoring Agent**。
- 未运行= 此客人未处于运行状态。
- 未找到= 在此客人上未找到或未运行此应用程序。
- 不可用= 此值暂时不可用。

状态—显示值(不可设置)。

- 预计 (✓)= 在过去 24 小时内此参数未超出其范围。
- 警告 (⚠)= 在过去 24 小时内此参数超出了其范围，但现在未上报任何事件。
- 超出范围 (✗)= 当前超出范围。

7. 单击**保存**，保存更改，或者单击**重置**，取消任何未保存的更改。短暂延迟后，将显示输入的新值(如果有)。

移除参数

1. 在 ztC Console中，单击左侧导航面板中的**虚拟机**。
2. 选择正在运行您要删除参数的应用程序的 VM。
3. 在下部面板中，单击**监控**选项卡。**应用程序**面板显示在**客户 OS**面板下方。
4. 选择应用程序/参数行。
5. 单击  **移除**按钮。

应用程序/参数行将从应用程序列表中消失。

6. 单击**保存**，保存更改(或者单击**重置**，取消任何未保存的更改)。短暂延迟后，应用程序/参数行将(再次)从应用程序列表中消失。

相关主题

[监控系统、基于 Windows 的 VM 和应用程序](#)

[配置电子警报](#)

[配置 SNMP 设置](#)

[安装应用程序\(基于 Windows 的 VM\)](#)

[配置基于 Windows 的虚拟机](#)

部分 2: 支持文档

关于版本信息、参考资料和故障排除信息，请参阅如下支持文件。

- [Stratus Redundant Linux 版本 2.2.0.0 版本说明](#)
- [系统参考信息](#)
- [安全性](#)
- [SNMP](#)

9

第 9 章：Stratus Redundant Linux 版本 2.2.0.0 版本说明

这些发行说明(更新于 2020/11/25 15:50)针对 Stratus Redundant Linux 版本 2.2.0.0, 其在 ztC Edge 系统上运行。(有关这些发行说明的最新版本, 包括自翻译以来可能的更改列表, 请参阅 [StrataDOC](#) 上提供的英文版本。)参阅如下各部分:

- [新功能及增强](#)
- [漏洞修复](#)
- [CVE 修复](#)
- [重要注意事项](#)
- [已知问题](#)
- [文档更新](#)
- [访问 Stratus 知识库文章](#)
- [获取帮助](#)

新功能及增强

Stratus Redundant Linux

以下功能在 Stratus Redundant Linux 版本 2.2.0.0 中为新功能:

- [ztC Advisor](#)
- 主机 OS 支持—支持作为 ztC Edge 系统的主机操作系统的 CentOS 7.8, 提供 3.10.0-1127.19.1.el7.x86_64 内核。
- 安全性改进:

- 已修复了 215 个 CVE。
- 有关配置系统以实现安全性的整合信息。请参阅[安全性](#)。
- 运行和故障排除—用于监控系统运行状况和统计信息的其他 REST API 调用。请参阅[REST API 调用](#)。

Stratus Redundant Linux版本 2.1.0.0 中的新功能

有关信息，请参阅[Stratus Redundant Linux版本 2.1.0.0 中的新功能](#)。

漏洞修复

在 Stratus Redundant Linux版本 2.2.0.0 中修复的故障

ZTC-3175: Nessus 扫描可识别端口 5560 上已弃用的 SSL。(已移除已弃用的协议。)

ZTC-3171: “SSH 密码”设置未通过所有安全扫描。(已修改设置，以便提高安全性并通过这些扫描。)

ZTC-3017、ZTC-2257: 密码中带有特殊字符的用户无法加入活动目录 (AD)。(在登录到 AD 时，现在已支持包含 “\$”、“!”、“&”和 “<”的 AD 用户名和密码。)

ZTC-2773: lvmetad 守护程序具有已知内存泄漏，已被弃用。(该守护程序已被配置为不再运行。)

ZTC-2395、ZTC-2396: Qualys 扫描未通过 QID 37839 和 QID 38738。(已修改 SSH 设置，以便提高安全性并通过该扫描。)

ZTC-2256: 默认情况下不安装 mcelog 包。(现在默认情况下安装 mcelog 包。)

ZTC-2206: Qualys 扫描未通过 QID 13162。(该会话 cookie 现在包含安全属性，该属性允许此扫描通过。)

ZTC-1298: 由于缺少 hypervclock 设置，Windows 客人遇到性能问题。(通过在该配置中添加 hypervclock 设置，已解决了 Windows 2016 和 Windows 2019 客人性能问题。)

ZTC-962: Stratus 提供的 SSL 证书的到期日期为 2026 年。(已提供了自发布之日起有效期为 10 年 (例如 2030 年) 的新证书。您必须接受新证书，请参阅[在升级过程中，刷新浏览器并接受新证书](#)。)

ZTC-461: 主节点故障转移后无法登录到活动目录。

ZTC-458: 配置有启动优先级顺序的客人可能无法启动。

ZTC-454: 全新安装或节点恢复/替换后，根、交换或 diagdata 可能显示为损坏。

ZTC-453: 客人启动失败时生成警报。

在 Stratus Redundant Linux 版本 2.1.0.0 中修复的故障

有关信息，请参阅 [Stratus Redundant Linux 版本 2.1.0.0 中的故障修复](#)。

CVE 修复

有关 CVE 修复列表，请参阅 [已修复的 CVE](#)。

重要注意事项

升级到版本 2.2.0.0

要升级到 Stratus Redundant Linux 版本 2.2.0.0，则遵循您系统上正在运行的版本的升级路径：

- 版本 2.1.0.0、2.0.1.0 和 2.0.0.0—按照 [使用升级套件升级 Stratus Redundant Linux 软件](#) 中的说明直接升级到版本 2.2.0.0。
- 版本 2.0.0.0 之前的版本—升级到版本 2.0.1.0，然后再升级到版本 2.2.0.0。有关升级到版本 2.0.1.0 的信息，请参阅 [版本 2.0.1.0 发行说明和帮助](#)。

确定系统软件的版本

要确定 ztC Edge 系统上运行的 Stratus Redundant Linux 版本，则登录系统的 ztC Console，然后检查刊头中的系统信息：

```
ocean.abc.com
IP: 123.109.50.34 | Asset ID: ze-12345
Version: n.n.n-nnn
```

或者，您可以单击 [首选项](#) 页上的 [软件更新](#)，其还会显示您系统上 Stratus Redundant Linux 软件的当前版本号。

如果软件版本低于版本 2.2.0.0，请从此 [下载](#) 页面在 <https://www.stratus.com/services-support/downloads/?tab=ztcedge> 下载 Stratus Redundant Linux 2.2.0.0 升级套件，然后按照 [使用升级套件升级 Stratus Redundant Linux 软件](#) 中的描述在系统上升级该软件。

在升级过程中，刷新浏览器并接受新证书

升级到版本 2.2.0.0 的过程中，在第一个节点已升级并成为新主节点后，浏览器可能将此升级显示为已暂停。如果该浏览器具有来自 Stratus 的需要接受的新证书，则会出现这个错误的浏览器显示。您应刷新该浏览器，并在提示时接受新证书。接受了新证书后，该浏览器将显示正确的升级状态。

使用 Intel 主动管理技术 (AMT) 获得 Lights-Out 支持

ztC Edge系统结合了对远程电源管理、远程控制台和远程媒体的 Intel 主动管理技术 (AMT) Lights-Out 支持。有关 AMT 配置和限制的重要信息，请参阅 [KB-8219](#)。

在不同物理站点上部署 ztC Edge节点

在部署 ztC Edge系统时，您必须在同一站点部署两个节点，以及在每个节点的蓝色 (A2) 和黄色 (A1) 网络端口之间直接连接 A-link。如果您要在自动本地站点恢复 (ALSR) 配置(其中每个节点均位于单独的物理站点，以增加冗余)中设置 ztC Edge 系统，请联系您的授权Stratus 服务代表寻求帮助。由于地理上的分离，ALSR配置需要仔细的组件布局规划和网络拓扑。

启用 ztC Advisor

Stratus Redundant Linux版本 2.2.0.0 或更高版本引入了对 ztC Advisor的支持，后者是一个基于 Web 的安全门户，其提供对您整个ztC Edge 系统舰队的集中可见性。通过直观、用户友好的仪表板，您能够一目了然地评估每个系统的运行状况、资源使用情况和软件版本。

有关注册和使用 ztC Advisor的信息，请访问以下网页：<https://www.stratus.com/solutions/ztc-advisor>。要启用或禁用对系统的 ztC Advisor，请参阅[启用 ztC Advisor](#)。

经过测试的客人操作系统

有关使用当前版本测试的客人操作系统的列表，请参阅[经过测试的客人操作系统](#)。

在套件升级过程中，单节点系统不能处于维护模式

在单节点系统上开始套件升级前，确保系统未处于维护模式。如果在开始套件升级时单节点系统处于维护模式，则系统无法退出维护模式。

已知问题

创建 Windows 2008 (SP2, 32 位) VM 后，VirtIO 串行驱动程序的安装失败

创建 Windows 2008 SP2(32 位) VM 后，VirtIO 串行驱动程序的安装失败。在这种情况下，您必须手动安装该驱动程序：要执行此操作，则从此[下载](#)页面在<https://www.stratus.com/services-support/downloads/?tab=ztcedge>下载 VirtIO ISO 文件。继续按照[更新 VirtIO 驱动程序\(基于 Windows 的 VM\)](#)中的说明进行操作，但选择串行驱动程序 (vioser)。注意，Windows 2008 SP2 的 64 位版本不会发生此问题。

可移动媒体以及使用 P2V 客户端迁移 PM 或 VM

在使用可启动的 P2V 客户端 (**virt-p2v**) ISO 文件迁移 PM 或 VM 前, 检查源映像是否附加了任何可移动媒体(例如, 软盘、DVD 驱动器或外部 USB 磁盘)。如果在您尝试迁移 PM 或 VM 时源映像附加了可移动媒体, 则会显示错误消息**转换失败**。因此, 开始迁移前, 在 **virt-p2v** 窗口中取消选择该媒体。要执行此操作, 则访问 **virt-p2v** 窗口, 该窗口具有两个部分, **目标属性**和**固定硬盘**, 然后在**固定硬盘**下, 取消选中可移动媒体旁**转换**列中的框。有关使用 **virt-p2v** 的更多信息, 请参阅[将物理机或虚拟机迁移到系统](#), 尤其是[将 PM 或 VM 迁移到 ztC Edge 系统](#)一节。

导入 VM 时的最大路径长度

在您使用**导入/还原虚拟机**向导来导入 VM 时, 对于**从远程/网络 Windows 共享 (CIFS/SMB)** 导入和**从远程/网络 NFS** 导入这两个导入选项, 到此 VM 的最大路径长度(包括 VM 名称)为 4096 个字符。

导入 OVA 文件有时会失败

如果您开始导入 OVA 文件, 然后将该节点置于维护模式下或断电, 则 OVA 导入将失败, 并且未来导入 OVA 文件的任何尝试都将失败。有关规避此问题的信息, 请参阅 [KB-10034](#)。

导入 Linux VMware OVA 文件后, 手动配置网络信息

导入 Linux VMware OVA 文件会改变网络接口和 `networks-scripts` 文件。在您导入此文件后, 您需要使用以下程序手动配置网络信息。

1. 在**虚拟机**页上, 选择此 VM。
2. 单击底部面板中的**控制台**, 打开 VM 登录页(有关其他信息, 请参阅[打开虚拟机控制台会话](#))。
3. 登录此 VM。
4. 打开命令提示符窗口。
5. 发出 `ifconfig` 命令。在命令输出中, 检查是否将 IP 地址分配给了虚拟网络接口 `eth0`。
6. 如果未将 IP 地址分配给 `eth0`, 则列出 `/etc/sysconfig/network-scripts` 目录的内容。
7. 记录 `ifcfg-xxxx`(但不是 `ifcfg-lo`) 的值。
8. 将 `ifcfg-xxxx` 重命名为 `ifcfg-eth0`。
9. 编辑 `ifcfg-eth0` 文件, 从而更改 `DEVICE` 和 `ONBOOT` 的值, 如下所示:

```
DEVICE=eth0
```

```
ONBOOT=yes
```

保存文件。

10. 发出以下命令来重启网络服务：

```
systemctl restart network
```

11. 通过发出 `ifconfig` 命令来验证 IP 分配。在命令输出中，确认已将 IP 地址分配给了 `eth0`。

“从 USB 导入”搜索列出各个目录中的 OVA 文件

当您在 **导入/还原虚拟机** 向导中选择从 **USB 导入** 来导入 OVA 文件时，您可以在 *搜索文件框* 中输入文件名或部分文件名。该框会列出名称与在该框中输入的名称相匹配且位于各个目录中的 OVA 文件：

- 将父(根)目录作为搜索目录时，除了父(根)目录外，列出的文件还位于子目录中。
- 将子目录作为搜索目录时，除了子目录外，列出的文件还位于父(根)目录中。

有关导入 OVA 文件的完整信息，请参阅 [导入 OVF 或 OVA 文件](#)。

无法导入 RHEL 8.1 VM

您无法将运行 RHEL 8.1(具有 BIOS 启动固件)的 VM 从 VMware ESXi 6.7.0 服务器导入到 ztC Edge 系统。

UEFI VM 控制台会话的最大分辨率

在 ztC Console 的 **虚拟机** 页上，您可以打开一个 VM 控制台会话，以显示在 VM 中运行的客人操作系统的控制台。当您打开一个控制台会话以便访问具有 UEFI 启动类型的客人 VM 时，该控制台会话的最大分辨率为 800x600。要获得更高分辨率，则使用“远程桌面连接”连接到 VM。

重启 VM，以获得 vmgenid 支持

使用升级套件将系统从版本 2.0.1.0(或更低版本)升级到 Stratus Redundant Linux 版本 2.2.0.0 后，直到重启了运行 Windows Server 2019、Windows Server 2016 或 Windows Server 2012 的 VM 后才支持这些 VM 上的 `vmgenid`。因此，您必须重启此类 VM 才能在升级后实现 `vmgenid` 支持。当您正在从版本 2.1.0.0 升级时，如果先前已在运行版本 2.1.0.0 的系统上重新启动了此类 VM，您无需重新启动它们。

使用 Microsoft Edge 控制台浏览器创建 VCD 失败

当您使用 Microsoft Edge 作为 ztC Console 的浏览器时，您无法创建 VCD：该过程将失败。使用其他兼容的浏览器(请参阅[兼容 Internet 浏览器](#))。

要导入 VMware VM，则使用操作系统关闭命令

当导入 VMware VM 时，除了从 VMware 控制台关闭其电源外，您还必须使用操作系统关闭命令来关闭此 VM。如果您仅使用 VMware 控制台关闭此 VM，则导入将失败。

在单节点系统中，添加的 vCPU 的 VM 创建向导显示不正确

当您在已授权用于一个节点的系统上创建 VM 时，**VM 创建向导**显示其正在将两个 vCPU 添加到您指定的 vCPU 数量中。但在创建了此 VM 后，会将用户指定数量的 vCPU 附加到此 VM。未添加其他两个(未正确显示)vCPU。

升级到双节点系统后，VM 显示警告图标

当您将已授权用于一个节点的系统升级到授权用于两个节点的系统时，这些 VM 仍在运行，但仪表盘显示带有警告图标 (⚠️) 的 VM 状态。该警告指示这些 VM 仅在使用一个或未使用 A-Link 运行，因为在升级过程中，系统未添加 A-Link1。

要避免此问题，则在升级前停止这些 VM，然后在升级后重新启动它们。如果遇到此问题，则在升级后停止并重新启动这些 VM。

在 IE10、IE11 或 Firefox 中针对控制台的日语键盘 106 和 109 的映射可能不正确

使用 IE10、IE11 或 Firefox 访问 ztC Console 时，日语键盘 106 和 109 的映射可能不正确。请改用 Chrome 或远程连接软件(VNC 或 RDP)。

迁移已设置了监视的 VM 会导致“无响应”

当在 VM 上设置了针对所有三个参数(CPU、内存和磁盘)的监视，并且已将此 VM 迁移到其他节点时，**监视器**选项卡显示**客人代理未响应**。客人代理重新连接可能需要几分钟。

当 A-Link 离线时，VM 报告为已损坏，而不是降级

如果在一个节点上断开了 A-link 电缆或网络，则该节点上的 VM 的状态在 ztC Console 中也可能被报告为已损坏 (❌)，即使此 VM 仍有另一个活动 A-link 连接也是如此。VM 的可用性不受影响。

弹出的 VCD 仍显示在基于 Linux 的 VM 控制台中

如果您使用 ztC Console 从运行基于 Linux 的客人操作系统的 VM 弹出 VCD，则该 VCD 可能仍显示在客人操作系统中。如果需要，您可以在客人操作系统中弹出该 VCD，以停止显示该 VCD。

在使用 https 时，有些浏览器无法连接 VNC

如果您已使用 **https** URL 在 Microsoft Internet Explorer 或 Mozilla[®] FireFox[®] 浏览器中连接到了 ztC Console，并且在从虚拟机页选择了正在运行的 VM 后单击了**控制台**，则可能显示消息 **VNC: 无法连接，请在 n 秒内重试**。要启用 VNC 连接，则单击刊头右上角中可转到 VNC 控制台页的 **https** 链接，然后继续执行以下相应步骤(在您浏览器中的操作步骤可能会有所不同，具体取决于您浏览器的版本)：

- 在 Internet Explorer 中，将显示**安全警报**向导：
 - a. 单击**继续到此网站(不建议)**。
 - b. 单击**确定**。
- 在 FireFox 中，将显示您的**连接不安全**窗口：
 - a. 单击**高级**。显示有关无效安全证书的消息。
 - b. 单击**添加例外**。将显示**添加安全例外**对话框，并且控制台的位置在**位置**中。
 - c. 单击**确认安全例外**。

将显示 VNC 控制台。

更改节点 IP 地址或网络掩码网络设置时需要重新启动

当您按照 [配置 IP 设置](#) 的描述更改节点的 IP 地址或网络掩码设置时，在重启该节点前，新设置和旧设置均有效。使这两个设置均处于活动状态可能导致路由或连接问题。

文档更新

从版本 2.0.0.0 开始，帮助采用德语、日语、中文和葡萄牙语。

访问 Stratus 知识库文章

Stratus 客户服务门户将提供可搜索的**知识库**，其中有包括 ztC Edge 系统和 Stratus Redundant Linux 软件在内的所有 **Stratus** 产品相关技术文章。在某些情况下，版本说明直接引用这些知识库文章(例如，KB-*nnnn*)。如下所示，您可以通过使用现有服务门户凭据或通过创建新的用户帐户访问客户服务门户和知识库文章。

要访问知识库

1. 登录到此 **Stratus 客户服务门户** 在 <https://support.stratus.com>。

如下所示，根据需要，创建新的帐户：

- a. 单击 **注册帐户**。
- b. 输入您公司的电子邮件地址以及联系信息，然后单击 **注册**。

您公司的电子邮件地址必须包括公司 (**Stratus 注册客户**) 的域名 (例如：**stratus.com**)。

- c. 单击您从 **Stratus** 收到的电子邮件中的链接。
- d. 输入新密码，然后完成您帐户的配置。

如果您在创建帐户时需要协助，请联系您的授权 **Stratus** 服务代表。

2. 在服务门户中，单击左侧窗格中的 **知识库**。
3. 在 **关键字搜索** 框中，输入与您需要的信息相关的关键字，然后单击 **搜索**。

要按 **KB-nnnn** 编号搜索文章，则单击 **高级搜索**。在 **按 ID 搜索** 旁，键入文档 ID 号 (**nnnn**)，然后单击 **显示**。

获取帮助

如果存在关于 **ztC Edge** 系统的技术疑问，请到如下位置查找最新技术信息以及在线文档：此 **下载** 页面在 <https://www.stratus.com/services-support/downloads/?tab=ztcedge>。您还可以搜索 **知识库**，位于此 **Stratus 客户服务门户** 在 <https://support.stratus.com>。

如果无法使用这些在线资源解决您的问题，并且您的系统有服务协议，请联系您的授权 **Stratus** 服务代表。有关信息，请参阅 **ztC Edge 支持** 页在 <https://www.stratus.com/services-support/customer-support/?tab=ztcedge>。

10

第 10 章：系统参考信息

关于参考信息，请阅读下面的主题

- [经过测试的客人操作系统](#)
- [重要物理机和虚拟机注意事项](#)
- [访问知识库文章](#)
- [创建 ALSR 配置](#)
- [已修复的 CVE](#)
- [REST API 调用](#)

经过测试的客人操作系统

下表列出了 Stratus 已在当前版本 Stratus Redundant Linux 软件上测试的虚拟机 (VM) 的客人操作系统。未列出的客人操作系统尚未经过 Stratus 测试，必须在本地进行测试。

操作系统	版本	启动固件接口
CentOS 7	CentOS 7.5、7.6、7.7、7.8(全 64 位)	BIOS
CentOS 6	Cent 6.9、6.10(均为 64 位)	BIOS

操作系统	版本	启动固件接口
Microsoft Windows Server 2019(标准版、数据中心版)	64 位	BIOS UEFI ¹
Microsoft Windows Server 2016(标准版、数据中心版)	64 位	BIOS UEFI ²
Microsoft Windows Server 2012(标准版、数据中心版)	64 位 R2	BIOS
Microsoft Windows 10 Desktop	64 位	BIOS
Red Hat Enterprise Linux 8(工作站、服务器)	Red Hat 8.1(64 位)	BIOS
Red Hat Enterprise Linux 7(工作站、服务器)	Red Hat 7.5、7.6、7.7、7.8 (全 64 位)	BIOS
Red Hat Enterprise Linux 6(工作站、服务器)	Red Hat 6.10(64 位)	BIOS
SUSE Linux 企业版服务器	SLES 12 SP2 64 位	BIOS
Ubuntu	18.042 Server(64 位)	BIOS

重要物理机和虚拟机注意事项

为最佳实施物理机和虚拟机，请了解以下章节中所述的配置最大值和要求：

¹仅当从运行 vSphere Release 6.7 的 VMware 服务器导出 VM 时，才可具有 UEFI 启动固件界面且运行 Windows Server 2019 的 VMware VM 导入运行 Stratus Redundant Linux 版 2.2.0.0(或更高版本)的系统。

²仅当从运行 vSphere Release 6.7 的 VMware 服务器导出 VM 时，才可具有 UEFI 启动固件界面且运行 Windows Server 2016 的 VMware VM 导入运行 Stratus Redundant Linux 版 2.2.0.0(或更高版本)的系统。

- [虚拟机建议和限制](#)
- [重要注意事项](#)

虚拟机建议和限制

虚拟机 (VM) 需要一定 [CPU 内核资源](#)。

建议的 CPU 内核数量

Stratus 建议仅将与 ztC Edge 系统上的物理线程一样多的线程用于工作负荷。ztC Edge100i 系统共有 8 个物理线程。ztC Edge110i 系统共有 12 个物理线程。

建议的 ztC Edge 工作负荷用内核数量取决于各 VM 的 vCPU 数量及 VM 类型，如下所述：

项目	物理线程数量
每个有 n 个 vCPU 的 FT 客人	$n + 2$ (典型)
每个有 n 个 vCPU 的 HA 客人	n (典型)

示例

以下示例适用于 ztC Edge 100i 系统：

- 四个 2-vCPU HA 客人通常共需要 8 个线程。
- 两个 3-vCPU HA 客人和一个 2-vCPU HA 客人通常共需要 8 个线程。
- 两个 4-vCPU HA 客人通常共需要 8 个线程。
- 一个 8-vCPU HA 客人通常共需要 8 个线程。

除上述示例外，以下示例也适用于 ztC Edge 110i 系统：

- 一个 4-vCPU FT 客人通常共需要 6 个线程。
- 六个 2-vCPU HA 客人通常共需要 12 个线程。
- 一个 2-vCPU FT 客人需要 4 个线程，两个 2-vCPU HA 客人需要 4 个线程，共需要 8 个线程。

重要注意事项

注意以下重要注意事项。

特性	注释
USB 设备	支持使用 USB 键盘、CD/DVD 驱动器、磁盘驱动器和 U 盘导入/导出 VM 以及进行系统还原。
控制台连接	每个 PM 的文本控制台均可用于 CentOS 操作系统。不过，不支持 VGA 模式；也就是说，PM 必须在运行等级 3 上运行，而不能在运行等级 5 上运行。参阅下面的“系统管理”。
系统管理	ztC Edge 系统管理不能运行在运行等级 5 上。
卷	对于导出、导入或还原卷，最大卷大小为 2TB。

创建 ALSR 配置

本主题及其子主题描述如何创建自动本地站点恢复 (ALSR) 配置。有关仲裁服务器的一般信息，请参阅 [仲裁服务器](#) 以及 [ALSR 和仲裁服务](#)。



注意：在创建前 ALSR，请阅读本主题及其所有子主题，然后按照这些主题中的描述计划您的 ALSR 配置。仅在您确定已计划的配置符合本主题及其子主题中的信息后，才能创建此配置。

如果符合下列任一条件，则存在 ALSR 配置：如果符合下列任一条件，则存在

- 系统的两个节点使用网络基础设施进行连接，而不是使用直接电缆。
- 连接这两个节点的 A-Link(直接连接)电缆的长度大于 10 米(例如，在园区内的两个独立建筑物中)。

这些配置可提供更出色的容灾和硬件冗余，以及物理计算机室及其所在建筑物的冗余。

Stratus 建议 ALSR 配置包含第三台计算机，该计算机为仲裁服务器。仲裁服务器位于从 node0 和 node1 的物理位置中移除的物理位置。



注意：本主题及其子主题描述了具有仲裁服务器的 ALSR 配置。Stratus 强烈建议 ALSR 配置包含仲裁服务器。如果您要考虑创建没有仲裁服务器的 ALSR 配置，请访问知识库，搜索文章在 [无仲裁的情况下部署 ALSR 时的注意事项 \(Kb-9682\)](#)，并且联系您的授权 Stratus 服务代表。有关访问知识库文章的信息，请参阅 [访问知识库文章](#)。

由于这些物理机地理上的分离，创建 ALSR 配置需要仔细的组件布局规划和较复杂的网络拓扑。

以下主题描述了如何创建ALSR配置。要执行这些主题中的程序，您应熟悉 **ztC Edge**软件以及运行该软件所在的硬件，并且应熟悉您系统的网络基础设施及其位置。



注意：这些主题无法描述网络交换机、路由器和其他硬件的每个供应商和型号。如果您需要有关如何根据这些“帮助”主题中的要求配置您基础设施的更多信息，请参阅与您基础设施相关的文档。

- [创建配置](#)
- [符合网络要求](#)
- [定位和创建仲裁服务器](#)
- [完成配置](#)
- [了解仲裁对系统行为的影响](#)

下表列出并定义了与创建ALSR配置相关的术语。

术语	含义
活动节点	客人 VM 当前正运行于的节点。每个客人 VM 都可具有不同的活动节点。与活动相反的是备用(请参阅 备用节点)。
A-Link	可用性链接。组成 ztC Edge 系统的两台计算机之间的直接网络连接。(系统的计算机也称为物理机 (PM) 或节点。) A-Link 必须为点对点连接，并且 A-Link 流量不能路由。 ztC Edge 系统需要两个 A-Link。在某些系统上，这些连接具有蓝色和黄色电缆(和端口)。您可以在分布式本地站点部署中对 A-Link 使用 VLAN 连接(请参阅 VLAN)。
备选仲裁服务器	当首选仲裁服务器不可用时，将使用备选仲裁服务器(请参阅 首选仲裁服务器)。
自动本地站点恢复 (ALSR)	如果符合下列任一条件，则存在 ALSR 配置： <ul style="list-style-type: none"> • ztC Edge系统的两个节点使用网络基础设施进行连接，而不是使用直接电缆。 • 连接这两个节点的 A-Link(直接连接)电缆的长度大于 10 米(例如，在园区内的两个独立建筑物中)。

	ALSR 配置通常用于提供更出色的容灾，其代价是更多的网络设置和更广泛的配置选项。ALSR 配置需要第三台计算机，该计算机为仲裁服务器(请参阅 仲裁服务器)。
AX	驻留在 ztC Edge 系统中并控制客人 VM 行为的容器层。AX 负责在活动节点与备用节点之间保持 VM 同步。每个 VM 都有自己的 AX 对(请参阅 VM 、 活动节点 和 备用节点)
业务网络 (ibiz)	从 ztC Edge 系统到 LAN 的网络连接，其还具有可包括管理消息的其他流量，以及用于应用程序和其他客户端及服务器的流量。ztC Edge 系统通常有两个用于业务网络连接的端口。可将业务网络分配给一个或多个客人 VM 供其使用，或者不分配给客人 VM。您必须将第一个业务网络 (ibiz0) 连接到 LAN，以便您能够从 Web 浏览器管理系统。
故障	系统执行客人 VM 的能力可能降低(请参阅 VM)。磁盘故障、网络中断或断电均为系统检测到的故障示例。
node0 或 node1	组成 ztC Edge 系统的两台计算机在内部标记为 node0 和 node1。(这些计算机有时也称为物理机或 PM。)node0 和 node1 的选择是任意的，并且是在首次配置系统时进行的。在 node0 和 node1 之间流动的持续流量传递系统以及正在运行的每个客人 VM 的状态信息(请参阅 VM)。
首选仲裁服务器	当(首选仲裁服务器)可用时，将使用首选仲裁服务器。如果首选仲裁服务器不可用，则使用备选仲裁服务器(如果存在)(请参阅 备选仲裁服务器)。
主节点	当对系统的计算机进行配对时，只有一台计算机响应管理消息。此计算机是主节点。最初部署系统时分配的系统 IP 地址适用于主节点。当发生不同故障情况时，主节点可在 node0 和 node1 之间进行切换(请参阅 故障)。注意，对于客人 VM 而言，主节点不一定是活动节点(请参阅 活动节点 和 VM)。
priv0	用于两个节点之间的专用管理流量的网络。有关更多信息，请参阅

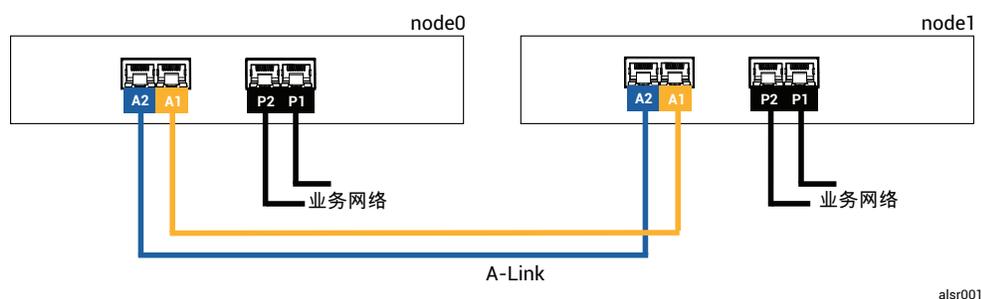
	A-Link 和专用网络。
仲裁服务器	第三台计算机，其帮助仲裁对于每个客人 VM 而言应处于活动状态的 AX(请参阅 活动节点 和 VM)。正确使用仲裁服务器是防止脑裂情况的唯一有保证的方式(请参阅 脑裂)。
RTT	往返时间。网络消息从起点到目的地再返回来所需的时间。此时间通常以毫秒 (ms) 为单位。
脑裂	当客人 VM 的 AX 对的两个 AX 同时处于活动状态时发生的情况，这会在每个活动的客人中生成不同的数据副本(请参阅 AX 和 VM)。当 node0 和 node1 之间的所有通信路径都断开时，可能会发生脑裂(请参阅 node0 或 node1)。使用仲裁服务可防止出现脑裂情况(请参阅 仲裁服务器)。
备用节点	对客人 VM 而言不是活动节点的节点。备用节点通过 AX 通信经 A-Link 连接保持同步(请参阅 AX 和 A-Link)。每个客人 VM 的 AX 对均确定哪个节点处于活动状态，哪个节点处于备用状态(请参阅 活动节点)。
系统管理	系统管理是 Stratus Redundant Linux 软件中负责维护系统整体状态的层。确定哪个节点是主节点是系统管理的一部分(请参阅 主节点)。系统管理还负责显示 ztC Console 中的信息。
UPS	不间断电源供应。用于电气设备的外部备用电池，可防止短暂停电对可用性产生影响。
VLAN	虚拟 LAN。VLAN 是一个或多个 LAN 上的一组设备，这些 LAN 被配置为好像它们连接到同一有线网络中那样进行通信，而实际上此时它们位于不同的 LAN 网段上。VLAN 是在网络基础设施层面上配置的，而不是在 ztC Edge 系统内配置的。在 自动本地站点恢复 (ALSR) 配置中，A-Link 被实现为隔离 VLAN(请参阅 A-Link)。
VM	虚拟机(也称为客人)。系统通常具有已分配的并且正在通过客人操作系统运行应用程序的一个或多个 VM(或客人)。

创建配置

要创建ALSR配置，则首先考虑典型 ztC Edge 系统配置的配置和ALSR 配置的 VLAN 要求。然后，遵循计划周全的包含一个仲裁服务器的ALSR配置，以及熟悉此配置的 VLAN 要求。您还必须熟悉部署典型 ztC Edge 系统然后创建ALSR 配置的整个过程。以下章节提供了这些信息。

典型 ztC Edge 系统

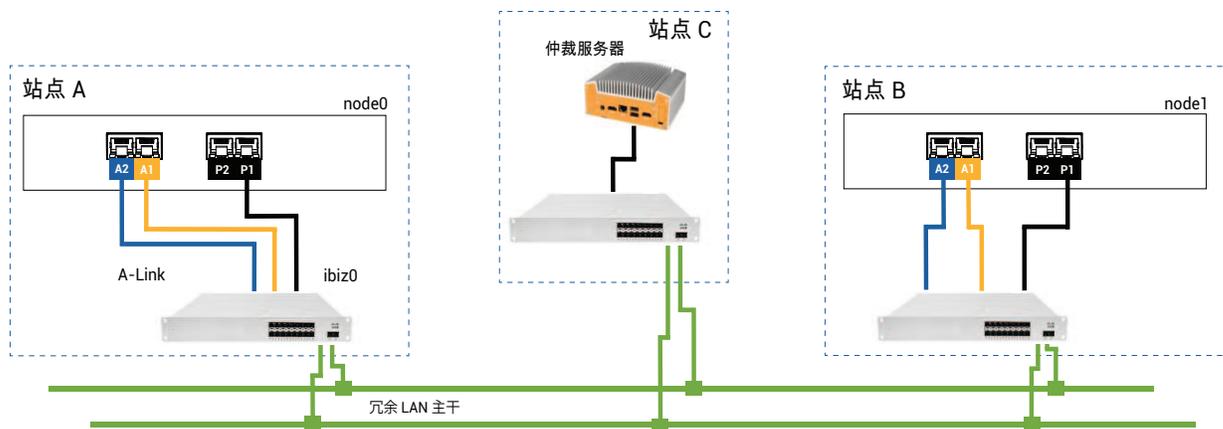
在典型ztC Edge 系统配置中，两个 PM 通过一对用于 A-Link 的网络电缆直接进行连接。一个 A-Link 一般作为设置为专用网络 (priv0)。这两个 PM 具有用于业务网络的额外网络连接，系统托管的ztC Console和客人 VM 使用这些网络连接。下图说明了典型配置。



在典型配置中，这些 PM 之间的物理距离受单根 A-Link 网络电缆长度的限制，该网络电缆的长度约为 33 英尺(10 米)。当考虑物理环境和环境电噪声时，该距离可能大幅缩短。

具有仲裁服务器的 ALSR 配置

计划周全的ALSR 配置由位于两个不同位置的两个节点以及在第三个位置上运行仲裁服务的第三台计算机组成。所有这些计算机均与相应的网络交换设备进行联网，因此在ALSR配置中不存在单点故障。下图说明了这种配置，此配置由站点 A 的 node0、站点 B 的 node1 和站点 C 的仲裁服务器组成。



alsr002

注释：

1. 应将每个 A-Link 均连接在交换机 A 与交换机 B 之间配置的自己 VLAN 上。
2. 为了清楚起见，这些图中未包含 DNS 服务器和网关，但您必须确保 ALSR 配置包含到 DNS 服务器和网关的连接，以防发生网络故障。
3. 为实现最大保护，您应在每个站点安装冗余交换机，尽管该图中未显示这些交换机。对于图示的配置，站点 A 和站点 B 将各包含两个交换机。A-Link 通过一个交换机进行路由，业务网络通过另一个交换机进行路由。如果可能，使用不同的电路为交换机供电，或者使用 UPS，以防止发生短暂的断电故障。

ALSRVLAN 要求

交换机 A 与交换机 B 之间的 A-Link 连接需要在这些交换机上进行 VLAN 配置。A-Link 流量不可路由，此连接应模拟单根长网络电缆。每个 A-Link 均必须在各自的 VLAN 上加以隔离。

如果您无法在这些交换设备之间创建 VLAN，则可以使用以太网到光纤介质转换器在两个 PM 之间创建更长的光纤连接。但您不应通过同一物理管道路由这两个 A-Link 光纤连接，因为这会产生单点故障。

此外，仲裁服务计算机不应与 node0 或 node1 共享交换机，因为共享交换机会产生单点故障。

有关 A-Link 和仲裁连接的延迟要求的更多信息，请参阅[符合网络要求](#)。

从初始部署到完成 ALSR 配置

创建 ALSR 配置时，您首先应在最初无 ALSR 配置的情况下部署和注册典型 ztC Edge 系统。[典型 ztC Edge 系统](#) 中的图展示了这个系统。为简单起见，使用提供的电缆并排安装这些节点。请参阅[入门](#)。

ALSR 典型系统正常运行后，创建配置。

1. 阅读[创建 ALSR 配置](#)及其所有子主题(如果尚未这样做)。
2. 安装仲裁计算机并启用仲裁服务器。遵守以下中的所有信息：
 - [具有仲裁服务器的 ALSR 配置](#)
 - [ALSRVLAN 要求](#)
 - [符合网络要求](#)
 - [完成配置](#)
3. 验证此仲裁服务器是否可访问两个节点。
4. 正确关闭一个节点。请参阅[关闭物理机](#)。
5. 将关闭节点重定位到远端站点。
6. 连接基础设施。[上方的 ALSR 配置图](#)显示了这些连接，包括：
 - 与端口 **A2** 的 `priv0` 连接
 - 与端口 **A1** 的第二个 A-Link 连接
 - 与端口 **P1** 的 `ibiz0` 连接
7. 启动并(重新)连接节点。请参阅[启动物理机](#)。
8. 验证配置。确保：
 - 共享网络正确配对 - 在 **ztC Console** 中，导航到**网络**页面，然后确保每个网络的状态均带有绿色勾。必要时，排查任何基础设施问题。
 - 重新创建仲裁连接 - 在控制台中，单击**首选项**，然后单击**仲裁服务器**，导航到**仲裁服务器**页面。确保仲裁服务器的状态带有绿色勾。必要时，排查任何基础设施问题。
 - 主节点可从 `node0` 转换到 `node1`，控制台可在两种配置中连接 - 将每个节点均置于维护模式(请参阅[维护模式](#))。
9. (重新)连接 VM - 在节点间迁移 VM(请参阅[将物理机或虚拟机迁移到系统](#))。验证 VM 联网

的网络故障转移是否正确。

10. 评估网络状态并验证以太网故障转移(请参阅“网络”页)。

符合网络要求

本主题介绍为实现成功 ALSR配置对 A-Link、业务网络、仲裁服务器连接以及管理网络的网络要求和注意事项。(有关这些网络的一般信息,请参阅[网络架构](#)。)



先决条件: 首先阅读[创建ALSR配置](#)并按照其说明操作,计划和创建 ALSR 配置(如果尚未这样做)。

A-Link 网络连接必须符合以下要求:

- 这些 A-Link 使用 IPv6 寻址。
- 每个 A-Link 均必须在各自的 VLAN 上进行连接。A-Link 流量不可路由。
 - FT VM 要求小于 2ms RTT A-Link 延迟(仅适用于 110i 系统)。
 - HA VM 要求小于 10ms RTT A-Link 延迟(适用于所有 ztC Edge 系统。)
 - 您需要提供足够的带宽以满足系统上所有 VM 的需求,并且您需要提供每 A-Link 至少应 1Gb 的速度。
 - 在计划网络基础设施时,您需要考虑交换机与该交换机上正在使用的所有端口中的网络主干之间的上行链路带宽。

如果不符合这些要求,则由于两个节点之间的同步带宽有限,客人 VM 可能运行得更慢。

第一个业务网络 (ibiz0) 用于节点之间以及到仲裁服务器的通信。ibiz0 网络必须符合以下要求:

- 两个节点必须位于同一子网上。
- 网络必须允许两个节点之间的 IPv6 多播流量。
- 两个节点均可使用 IPv4 网络寻址访问仲裁服务器。

仲裁服务器的网络连接必须符合以下要求:

- 必须使用 ibiz0 以及使用 IPv4 网络寻址提供对仲裁服务的访问。
- 两个 UDP 端口必须打开,并且可用于节点与仲裁服务之间的通信,包括在防火墙中。默认情况下,这些端口为 4557 和 4558。如果您要更改这些端口,请参阅[配置仲裁服务端口](#)(位于仲裁计算机上)和[请参阅在 ztC Console 中配置仲裁服务器](#)。
- ztC Edge 节点与仲裁计算机之间的延迟应小于 500ms RTT。

- 吞吐量不是重要考虑因素。10Mb 以太网，甚至 T1 带宽已足够。
- 仲裁计算机对于同一 ztC Edge系统上的所有 VM 都是通用的。
- 可在许多 ztC Edge系统之间共享仲裁计算机。
- 不得将仲裁计算机在使用它的同一 ztC Edge系统上实现为 VM。
- 使用不同的网络基础设施，不要共享。ztC Edge节点不应依赖配对节点站点上的网关或交换机/路由器来获得对仲裁服务计算机的持续访问。



注意：不要在不同节点对上将仲裁服务实现为客人 VM；这些节点上的故障将导致运行仲裁服务的 VM 进行故障转移，这将为网络拓扑和故障管理产生不必要的复杂性。此外还需要第二个仲裁计算机来管理对正在运行仲裁服务的 ztC Edge系统的仲裁。

管理网络连接必须符合以下要求：

- 默认情况下，管理网络与业务网络共享。这种情况下，业务网络的所有要求都适用。
- 为远程管理配置业务 LAN 网关。

定位和创建仲裁服务器

在规划计划的ALSR配置中，第三台计算机托管仲裁服务。仲裁服务处理要求较低，因此符合所有网络和运行要求的其他任何现有计算机或 VM 都可托管仲裁服务。高效的仲裁服务器取决于网络中仲裁计算机的位置。

在确定了仲裁计算机(和备选仲裁计算机，如果需要)的有效位置并确保该计算机符合仲裁服务的要求后，您便可创建仲裁服务器。



先决条件：首先阅读[创建ALSR配置](#)并按照其说明操作，计划和创建 ALSR 配置(如果尚未这样做)。

定位仲裁计算机

将第一个仲裁计算机定位在网络中的第三个站点，如[具有仲裁服务器的 ALSR 配置](#)所示。如果第三个站点不可用，则使仲裁计算机的放置位置不同于 node0 和 node1 的物理位置。将仲裁计算机置于唯一站点可使系统在发生导致节点和仲裁计算机均丢失的问题(例如，瞬态电气、管道，或者导致网络连接中断的其他问题)时有更大的机会幸免于难。

您将仲裁计算机连接到的电路应不同于为 node0 或 node1 供电的电路。此外，您还应将仲裁计算机连接到 UPS 设备。

小心：如果两个 AX 与仲裁服务器的连接均中断，则它们将尝试选择备选仲裁服务器。如果无法选择仲裁服务器，则 VM 会被降级为单工模式，以防止在发生其他故障时出现脑裂情况。



如果一个节点关闭并且剩余节点上的 VM (AX) 无法访问仲裁服务器或其对等节点，其将自行关闭，以避免脑裂情况的风险。

定位仲裁计算机时：

- 确保仲裁计算机不与 `node0` 或 `node1` 共享交换机(或路由器)。
- 不要在 `ztC Edge`

有关系统行为和故障模式的说明，请参阅[了解仲裁对系统行为的影响](#)。

添加备选仲裁计算机

您可以将另一个仲裁计算机(及其交换机)添加到系统中，以创建备选仲裁服务。备选仲裁服务器的最常见用途是，例如将操作系统更新应用于首选仲裁计算机时。当首选仲裁计算机重新启动时，将选择备选仲裁计算机，并且不会发生降级。当恢复首选仲裁时，该选择将移回原始首选仲裁计算机。

在创建第二个仲裁服务时，您必须遵循有关网络和仲裁位置的所有要求。如果两个节点能够互通信并与相同仲裁服务器(首选或备选仲裁服务器)通信，则即使一个仲裁连接中断，系统也能够保持 VM 冗余。当两个节点可互相访问并且可访问首选仲裁服务器时，将进行首选仲裁服务器选择。因此，如果首选仲裁服务是在节点丢失的同时丢失的，则即使第二个非首选仲裁服务可用，其余节点也会关闭 VM。但如果首选仲裁服务是在节点丢失前丢失的，并且两个节点都能够继续联系备选仲裁服务器，则该选择将被移至备选仲裁服务器。故障处理仅在所选仲裁服务器环境下进行。

如果创建备选仲裁服务，您需要在将该仲裁服务添加到 `ztC Console` 时添加第二个仲裁 IP 地址。

仲裁计算机要求

您可以在运行 Windows 操作系统并符合以下要求的任何通用计算机、笔记本电脑或 VM 上安装仲裁服务软件：

- 计算机可持续保持开机状态以及与网络的连接，以便 `ztC Edge`
- 计算机具有静态 IPv4 网络地址。不使用 DHCP。

- 操作系统为 Windows Server 2016、Windows Server 2012、Windows Server 2008、Windows 7 或 Windows 10; 不支持嵌入式版本的 Windows 操作系统。
- 至少有 100 MB 的可用磁盘空间。
- 两个 UDP 端口必须打开, 并且可用于节点与仲裁服务之间的通信, 包括在防火墙中。默认情况下, 这些端口为 4557 和 4558。要更改这些端口, 请参阅 [配置仲裁服务端口](#) (位于仲裁计算机上) 和 [请参阅在 ztC Console 中配置仲裁服务器](#)。

下载并安装仲裁服务软件

确定了仲裁计算机的适当位置后, 下载并安装创建仲裁服务器所需的软件。

下载并安装仲裁服务器软件

1. 打开此 [下载](https://www.stratus.com/services-support/downloads/?tab=ztcedge) 页面在 <https://www.stratus.com/services-support/downloads/?tab=ztcedge>。
2. 向下滚动到 **驱动程序和工具** 部分, 然后单击 **仲裁服务**, 将仲裁服务器软件安装程序文件下载到仲裁服务器。
3. 在仲裁服务器上, 双击安装程序文件。
4. 将下载的文件移到可访问位置。
5. 登录仲裁计算机。
6. 导航到仲裁服务安装程序, 然后双击它。
7. 按照提示完成安装。

在安装仲裁服务时可能显示产品名称 *everRun*。



注意: 升级至较新版本的仲裁服务器软件时, 您不需要卸载先前的版本。

完成配置

创建了 ALSR 配置后, 必要时更改仲裁服务端口。然后在 **ztC Console** 内启用仲裁。最后, 验证此配置并(重新)连接 VM。



先决条件: 首先阅读 [创建 ALSR 配置](#) 并按照其说明操作, 计划和创建 ALSR 配置(如果尚未这样做)。



注意：在仲裁计算机上为仲裁服务配置的端口与在 **ztC Console** 中为仲裁服务器配置的端口必须是相同端口号。如果更改仲裁计算机上的仲裁服务端口，您必须更改连接到该仲裁计算机的所有 **ztC Edge** 系统(使用 **ztC Console**)上的仲裁服务端口，以便仲裁计算机和 **ztC Edge** 系统均使用相同端口号。请参阅 [请参阅在 ztC Console 中配置仲裁服务器](#)。

配置仲裁服务端口

在默认情况下，仲裁服务在 **UDP** 端口 **4557** 上进行侦听。

在大多数情况下，您无需更改默认端口。但如果网络配置要求您这样做，您可以更改此端口：

要更改仲裁服务器上的端口号

1. 使用具有管理权限的帐户登录仲裁计算机。
2. 在管理模式打开命令窗口。
3. 键入以下命令停止仲裁服务：
`net stop sraqserver`
4. 键入以下命令更改此端口(将 *nnnn* 替换为新端口号)：
`sraqserver -install nnnn`
5. 键入以下命令重启仲裁服务：
`net start sraqserver`

验证仲裁服务端口

如果需要验证仲裁服务端口，则检查此 **Windows** 注册表键值：

```
HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\Services\Sraqserver\Parameters\
QSServerPortForReceive
```

请参阅在 **ztC Console** 中配置仲裁服务器

仲裁服务运行后，您应在 **ztC Console** 中启用仲裁服务。您还可以移除仲裁服务器。

要启用仲裁服务：

1. 使用具有管理权限的帐户登录 **ztC Console**
2. 单击左侧导航面板中的**首选项**，打开**首选项**页。
3. 单击**仲裁服务器**。将打开仲裁配置页面。
4. 单击页面左侧的**添加仲裁服务器**。
5. 在**添加首选仲裁服务器**对话框中，输入以下值(如果首选仲裁服务器已经存在，**添加首选仲裁服务器**对话框将出现)：
 - **DNS 或 IP 地址**—为**首选仲裁服务器**输入完全符合条件的 **DNS** 主机名称或 **IP 地址**。
 - **端口**—默认端口为 **4557**。如果您需要一个与默认端口不同的端口，则键入一个端口号。您需要仅键入一个端口号。仲裁服务将打开**端口**和下一个端口的端口号(例如，**4557** 和 **4558**)



注意：端口号必须与仲裁服务侦听时所在的端口匹配。(必要时，您可以更改仲裁服务器上的端口。)

单击**保存**，保存这些值。

6. 重复步骤 4 和 5，配置第二个即替代仲裁服务器。**Stratus**建议配置两个仲裁服务器。
7. 要启用仲裁服务器时，选择**已启用**复选框后单击**保存**。

对仲裁配置的更改不影响正在运行的 **VM**。更改仲裁配置后，您必须停止并重启任何正在运行的 **VM**。

要移除仲裁服务器



小心：如果移除了**首选仲裁服务器**，**替代仲裁服务器**将变成**首选仲裁服务器**。如果不存在**替代仲裁服务器**，则删除**首选仲裁服务器**后将自动禁用仲裁服务。

1. 导航到 **ztC Console**的 **首选项**页面。
2. 单击**仲裁服务器**。
3. 找到要删除的仲裁服务器项。
4. 在最右列，单击**移除**。



注意：如果某 VM 使用的是正在移除的仲裁服务器，则必须重启该 VM，以令其无法识别该仲裁服务器，从而令移除流程得以完成。VM 将降级到单工模式，直到在未配置仲裁服务器的情况下重启它为止。

验证此配置并(重新)连接 VM

验证此配置并(重新)连接 VM。执行从[初始部署到完成 ALSR 配置](#)中的相应步骤。

了解仲裁对系统行为的影响

ALSR系统中的仲裁服务器会改变系统的可用性和恢复行为。要了解仲裁对系统行为的影响，您首先需要了解系统在没有仲裁服务器时的行为。



先决条件：首先阅读[创建 ALSR 配置](#)并按照其说明操作，计划和创建 ALSR 配置(如果尚未这样做)。

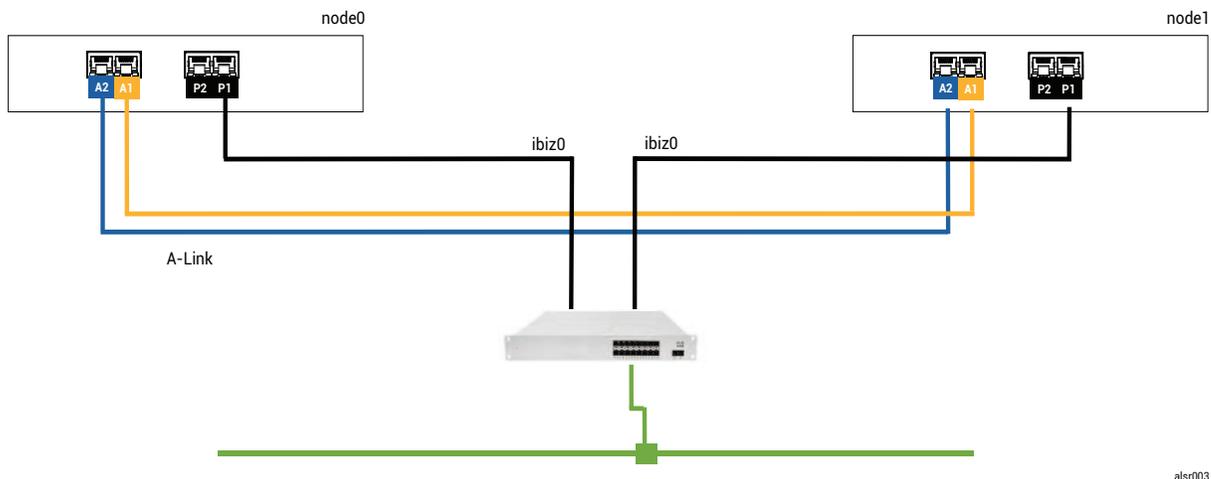
ztC Edge系统旨在为一个或多个客人 VM 提供高可用性，这可使这些 VM 即使在发生将导致应用程序停机的故障期间也能继续运行。例如，即使在失去单个网络连接、一块硬盘甚至整个计算机的情况下，ztC Edge系统也能够继续运行客人 VM。

但如果发生更多灾难性故障(例如，所有可能的网络路径均中断)，ztC Edge系统将尝试确定整个系统的整体状态。然后，系统会采取必要的行动来保护客人 VM 的完整性。

以下示例说明了在灾难性故障期间系统的过程。

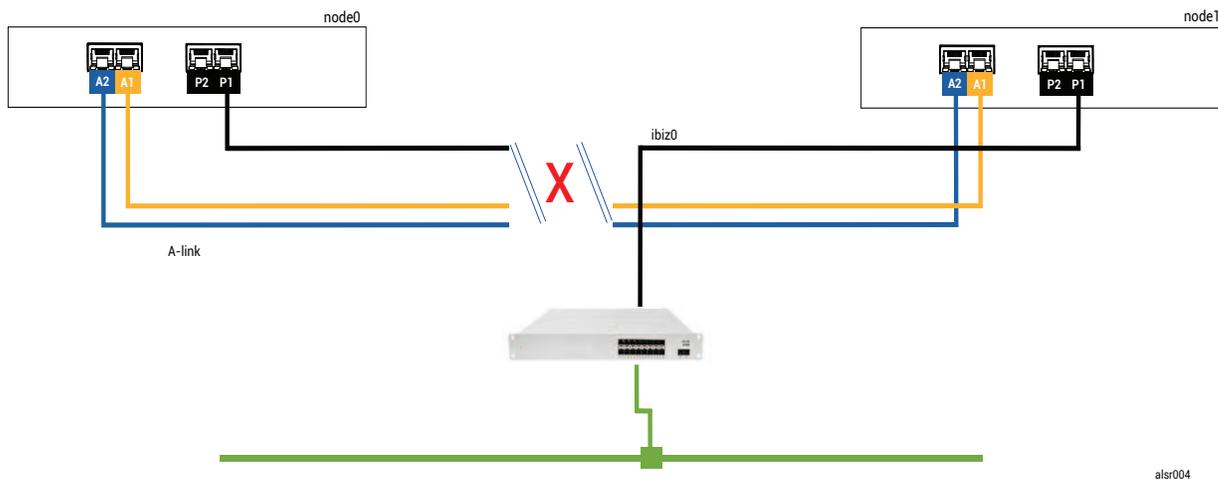
示例 1: 无仲裁服务器的系统遇到脑裂情况

在这个 ALSR示例中，ztC Edge 系统包含 node0 和 node1，但不包含仲裁服务器。操作正常；当前没有检测到任何故障。这两个节点通过 A-Link 连接传达它们的状态和可用性，就像它们在正常(无故障)操作期间那样。下图显示了正常连接。



灾难性故障

一个粗心的叉车操作员将墙撞穿了，切断了所有网络连接(业务和 A-Link)，同时供电仍未中断并且系统正在运行。下图显示了故障情况。



故障处理

这两个节点按照以下方式处理故障：

- node0 – node0 上的 AX 检测到 A-Link 以及其他所有网络路径中断。由于 node0 AX 无法再检测到其配对节点的存在，因此 node0 AX 变为活动状态并运行客人 VM。客人 VM 中的应用程序继续运行，其或许由于网络中断而以有限的容量运行。

- **node1 – node1** 上的 **AX** 也检测到两个 **A-Link** 中断，但 **ibiz0** 仍可用。由于其配对节点未响应 **ibiz0** 上的消息，因此 **node1 AX** 现在处于活动状态。客人 **VM** 中的应用程序继续运行，或许未注意到系统的任何问题。

从应用程序客户端或外部观察者的角度来看，这些客人 **VM** 均处于活动状态，并且生成具有相同返回地址的网络消息。这两个客人 **VM** 均生成数据并看到不同数量的通信故障。这些客人 **VM** 的状态随时间而变得更加不同。

恢复和修复

一段时间后，网络连接恢复：修好了墙壁并更换了网络电缆。

当 **AX** 对的每个 **AX** 均意识到其配对节点重新联机时，具有故障处理程序规则的 **AX** 对选择继续处于活动状态的 **AX**。该选择是不可预测的，并且对于在脑裂情况下哪个节点的性能更准确没有任何考虑。

活动节点的重新同步覆盖了从(现在)备用节点生成的数据，因此(现在)备用节点上的数据永久丢失。

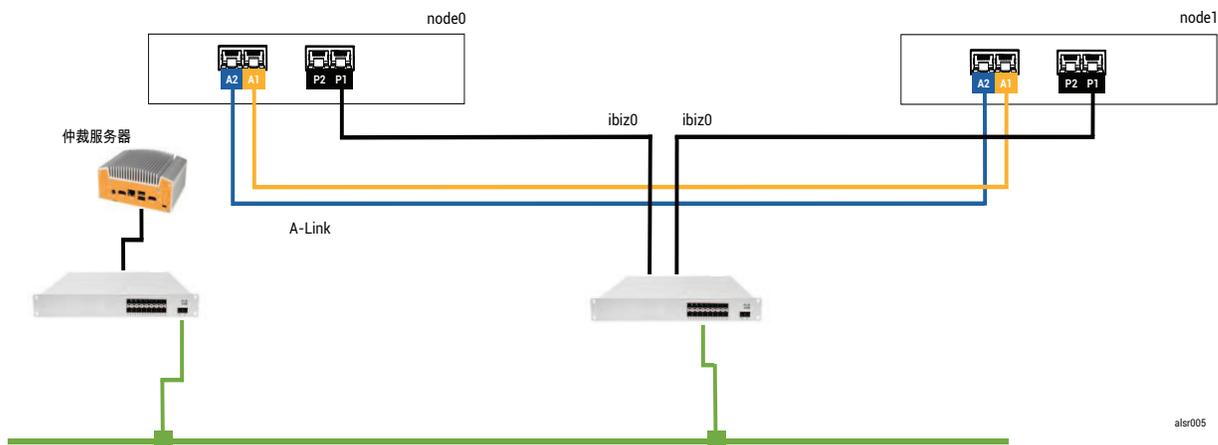
在脑裂情况下，系统需要几分钟的时间进行重新同步，这取决于需要将多少磁盘活动发送到备用节点。如果多个客人 **VM** 正在使用不同的活动节点运行，则可能在两个方向上发生同步流量。



注意：在某些情况下，**ztC Edge**系统可能无法确定在发生灾难性故障后继续运行的最佳方式。在这种情况下需要恢复系统。建议的恢复方法是使用**ztC Console**来关闭并重启一个节点，而另一个节点继续运行。此方法一般会强制正在运行的节点成为主节点，并且该节点上的**AX**变为活动状态。当正在运行的节点变为主节点后，可启动另一个节点。如果重新同步已经在进行，不要关闭任何一个节点。

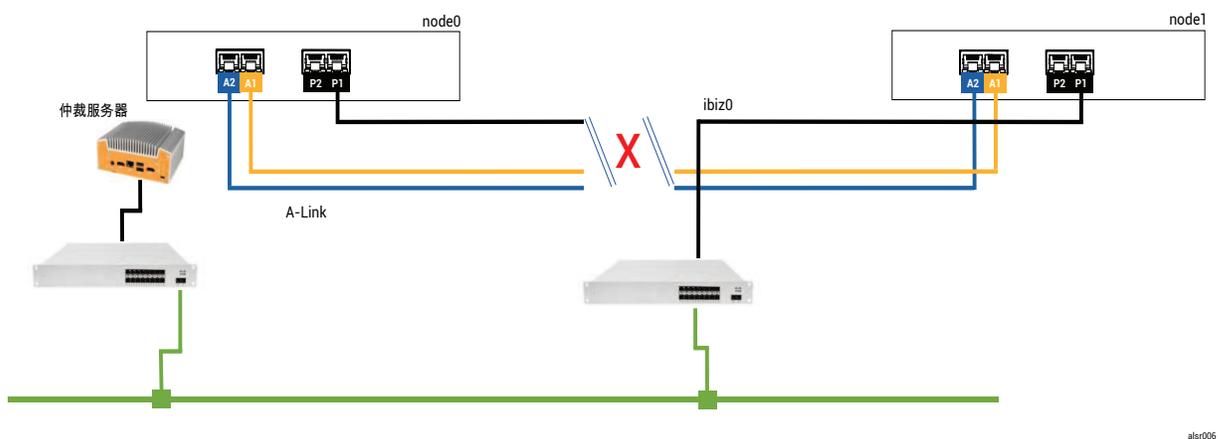
示例 2: 具有仲裁服务器的ALSR系统可避免脑裂情况

在这个 **ALSR**示例中，**ztC Edge** 系统包含 **node0** 和 **node1**，它们的连接与示例 1 中系统的连接相同。此外，示例 2 中的系统还包含仲裁服务器。下图显示了这些连接。



灾难性故障

那个粗心的叉车操作员又将墙撞穿了，切断了所有网络连接，同时供电仍未中断并且系统正在运行。下图显示了故障情况。



故障处理

这两个节点按照以下方式处理故障：

- node0 – node0 上的 AX 检测到 A-Link 以及其他所有网络路径中断。由于 node0 AX 无法再检测到其配对节点的存在，因此 node0 AX 尝试联系仲裁服务器。在这种情况下，仲裁服务器也不可用。因此，node0 AX 决定关闭。此关闭不是正常的 Windows 关闭，而是突然停止，这会导致客人 VM 中的应用程序停止。

- node1 – node1 上的 AX 也检测到两个 A-Link 中断，但 ibiz0 仍可用。node1 AX 尝试联系响应的仲裁服务器，因此 node1 AX 保持活动状态。客人 VM 中的应用程序运行，或许未注意到系统的任何问题。



注意：如果 node1 AX 先前未处于活动状态，并且客人 VM 是 HA VM，则 node1 上的客人 VM 可能需要从 node1 的硬盘驱动器启动。在这种情况下，当客人 VM 启动时，应用程序会经历短暂的停机。(FT VM 继续运行。)

从应用程序客户端或外部观察者的角度来看，node1 上的客人 VM 保持活动状态，并且在 node0 上的 VM 关闭时生成数据。不存在脑裂情况。

恢复和修复

一段时间后，网络连接恢复：修好了墙壁并更换了网络电缆。

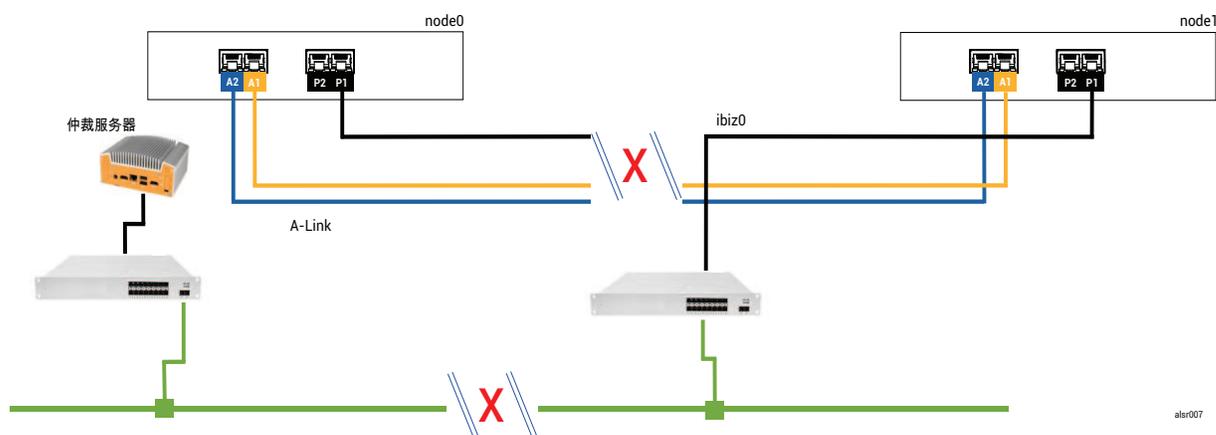
当 node1 AX 意识到其配对节点重新联机时，node0 AX 变为备用节点。由于 node0 先前未运行，因此从 node1 开始将数据同步到 node0。

由于没有发生脑裂情况，因此数据未丢失。

系统需要几分钟进行重新同步，这取决于需要将多少磁盘活动发送到备用节点。

示例 2, 已修改: 在灾难性故障期间仲裁服务器不可及

在具有仲裁服务器的 ALSR 系统中，当灾难性故障切断所有网络连接时，仲裁服务器可能脱机或不可及，但供电仍未中断且系统仍在运行。下图显示了仲裁服务器为脱机状态的这种情况下的系统。



故障处理类似于示例 2 的故障处理，对于 **node1** 而言有一个重要区别：

node1 AX 也检测到两个 A-Link 中断，但 **ibiz0** 仍可用。**node1 AX** 尝试联系仲裁服务器，但通信失败。此 **AX** 终止了客人 **VM**。

在这种情况下，客人 **VM** 在 **node0** 和 **node1** 上均关闭，从而防止发生脑裂。折衷方法是在恢复与 **node0** 或仲裁服务器的连接前，客人 **VM** 不可用。

在这种情况下，确定您不想运行的节点并将其关闭。然后，强制启动您想要运行的节点，之后强制启动 **VM**。有关关闭 **VM** 然后启动它的信息，请参阅[管理虚拟机的运行](#)。)

示例 2, 已修改: 在无灾难性故障时仲裁服务器不可及

在某些情况下，即使没有发生灾难性的物理故障，仲裁服务器也可能不可及。一个示例是当重启仲裁计算机进行例行维护时，例如应用 **OS** 补丁。在这些情况下，**AX** 检测到仲裁服务无响应，因此 **AX** 会暂停同步流量，直至恢复与仲裁服务器的连接为止。当连接中断时，客人 **VM** 继续在处于活动状态的节点上运行。但由于可能会发生其他故障，此客人 **VM** 不移到备用节点。恢复仲裁服务后，只要保持与仲裁服务器的连接，**AX** 就会继续进行同步和正常故障处理。

从电源故障中恢复

如果在断电或系统关闭后重启系统，**ztC Edge** 系统将在启动任何客人 **VM** 前无限期等待其配对系统启动并在做出响应。如果先前处于活动状态的 **AX** 能够联系仲裁服务器，则该 **AX** 会立即启动客人 **VM**，不等待其配对节点启动。如果先前备用的 **AX** 首先启动，则它会等待其配对节点。

如果系统收到来自配对节点或仲裁服务器的响应，则系统将继续正常运行，并且 **VM** 将启动，这需要遵守在其他情况下适用的相同故障处理程序规则。

如果系统未收到来自仲裁服务器的响应，或者系统没有仲裁服务器，则必须强制启动客人 **VM**，这会覆盖 **AX** 或故障处理程序做出的任何决定。您必须确保两个人没有在 **node0** 和 **node1** 上强制启动同一客人 **VM**。无意中这样做会导致脑裂情况。

访问知识库文章

Stratus 客户服务门户 将提供可搜索的**知识库**，其中有包括 **ztC Edge** 在内的所有 **Stratus** 产品相关技术文章。在某些情况下，在线帮助直接引用这些知识库文章(例如，**KB-nnnn**)。如下所示，您可以通过使用现有服务门户凭据，或通过创建新的用户帐户访问客户服务门户和知识库。

要访问知识库

1. 登录到此 **Stratus 客户服务门户** 在 <https://support.stratus.com>。

如下所示，根据需要，创建新的帐户：

- a. 单击**注册帐户**。
- b. 输入您公司的电子邮件地址以及联系信息，然后单击**注册**。
您公司的电子邮件地址必须包括公司 (**Stratus 注册客户**) 的域名 (例如：**stratus.com**)。
- c. 单击您从 **Stratus** 收到的电子邮件中的链接。
- d. 输入新密码，然后完成您帐户的配置。

如果您在创建帐户时需要协助，请联系您的授权 **Stratus** 服务代表。

2. 在服务门户中，单击左侧窗格中的**知识库**。
3. 在**关键字搜索**框中，输入与您需要的信息相关的关键字，然后单击**搜索**。

要按 KB-*nnnn* 编号搜索文章，则单击**高级搜索**。在**按 ID 搜索**旁，键入文档 ID 号 (*nnnn*)，然后单击**显示**。

相关主题

[支持文档](#)

已修复的 CVE

该主题列出了在所列版本中已修复的通用漏洞披露 (CVE)。

Stratus Redundant Linux 版本 2.2.0.0 中已修复的 CVE

下表列出了本版本中已修复的 CVE(存在时，单击下拉图标)

本版本中已修复的 CVE		
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

本版本中已修复的 CVE		
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
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

本版本中已修复的 CVE		
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
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

本版本中已修复的 CVE		
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
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

本版本中已修复的 CVE		
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
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	

Stratus Redundant Linux版本 2.1.0.0 中已修复的 CVE

下表列出了本版本中已修复的 CVE(存在时, 单击下拉图标)

本版本中已修复的 CVE		
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

本版本中已修复的 CVE		
CVE-2018-1122	CVE-2018-1139	CVE-2018-1312
CVE-2018-3058	CVE-2018-3063	CVE-2018-3066
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

本版本中已修复的 CVE		
CVE-2018-12900	CVE-2018-13053	CVE-2018-13093
CVE-2018-13094	CVE-2018-13095	CVE-2018-13346
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

本版本中已修复的 CVE		
CVE-2018-18661	CVE-2018-18897	CVE-2018-19058
CVE-2018-19059	CVE-2018-19060	CVE-2018-19149
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

本版本中已修复的 CVE		
CVE-2019-3846	CVE-2019-3858	CVE-2019-3861
CVE-2019-3880	CVE-2019-3882	CVE-2019-3900
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

本版本中已修复的 CVE		
CVE-2019-1000019	CVE-2019-1000020	CVE-2019-1010238
CVE-2020-2583	CVE-2020-2590	CVE-2020-2593
CVE-2020-2601	CVE-2020-2604	CVE-2020-2654
CVE-2020-2659		

Stratus Redundant Linux版本 2.0.1.0 中已修复的 CVE

以下下拉表列出了本版本中已修复的 CVE(存在时, 单击下拉图标)

本版本中已修复的 CVE		
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

本版本中已修复的 CVE		
CVE-2018-5391	CVE-2018-5407	CVE-2018-5729
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

本版本中已修复的 CVE		
CVE-2018-14646	CVE-2018-14665	CVE-2018-15688
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

本版本中已修复的 CVE		
CVE-2019-3862	CVE-2019-3863	CVE-2019-5953
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

Stratus Redundant Linux版本 2.0.0.0 中已修复的 CVE

以下下拉表列出了本版本中已修复的 CVE(存在时, 单击下拉图标)

本版本中已修复的 CVE		
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

本版本中已修复的 CVE		
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 调用

ztC Edge系统支持以下表述性状态转移 (REST) 应用程序接口 (API) 调用：

- [login](#)
- [overview](#)
- [vms](#)

login

发布登录信息以访问资源信息。此授权调用可防止未授权用户访问该系统。首先发出此调用，然后从响应 JSON 字符串复制 `session-id` 的值，并将此值用作未来调用的标题中的 `JSESSIONID`。

标题	值	必填
内容类型	应用程序/json	是

请求	值	必填
用户名	用于登录到 ztC Console 的用户名。	是
密码	用户名的密码。	是

端点

以下为端点，给定的基 URL 为 `/restapi`：

```
POST /login
```

示例

请求 URL：

```
https://{hostname or IP address}/restapi/login
```

overview

获取系统信息，包括物理机属性、统计信息、系统性能和当前警报列表。响应可能很大(约 14KB)。

标题	值	必填
区域设置	<code>de</code> (德语)、 <code>en-US</code> (英语)、 <code>ja</code> (日语)、 <code>zh-CN</code> (中文) 或 <code>pt-br</code> (葡萄牙语)。默认区域设置是 <code>en-US</code> 。	否
内容类型	应用程序/json	是

端点

GET /system/overview

示例

请求 URL:

`https://{hostname or IP address}/restapi/system/overview`

vms

获取系统中存在的 VM 的列表。

标题	值	必填
JSESSIONID	login 调用响应中的 session-id 值	是
内容类型	应用程序/json	是

端点

GET /v1/vms

示例

请求 URL:

`https://{hostname or IP address}/restapi/v1/vms`

11

第 11 章：安全性

要了解为了给 **ztC Edge** 系统提供最高安全级别您可实施的其他配置设置，请参阅 [安全性加强](#)。

要了解有关安全性的更多信息，请参阅以下主题：

- [已修复的 CVE](#)
- [管理 IPtables](#)
- [配置安全连接](#)
- [配置“用户与组”](#)
- [配置活动目录](#)
- [“审核日志”页](#)

安全性加强

尽管 **Stratus ztC Edge** 系统提供了安全的随取即用体验，但您可按如下所述实施其他配置设置，以提供最高级别的安全性。

安全性通常是保护与易用性之间的平衡。**ztC Edge** 系统配有平衡这些因素的一系列默认设置。为提高安全性，请遵循以下指导原则，并在该系统的整个生命周期(从规划和配置到运行和停用)内不断评估其安全性。

以下信息提供了基于 *CIS Controls 7.1* 版的安全性加强指南，这些是由互联网安全中心 (CIS) 提出的加强建议，互联网安全中心是一家由社区推动的非营利组织，该组织在保护 IT 系统和数据方面处于领先地位，并因其在这方面的最佳实践而获得公认。此外还使用 *CIS 基准* 来验证安全产品并为安全产品创建基线。*CIS Controls* 列表包含在以下 [标准组织的最佳实践与标准](#) 中。

以下信息还提供了基于工业控制系统网络安全标准 ISA/IEC 62443 的加强指南，该标准最初是由国际自动化协会 (ISA) 创建的，然后由国际电工委员会 (IEC) 继续制定。根据数据敏感度或预计威胁方对手，ISA/IEC 62443-4-2 具有不同的安全级别，并且通过实施这些建议和应用缓解控制措施，其有助于符合所需的安全级别。ISA/IEC 62443-4-2 要求的摘要包含在以下[标准组织的最佳实践与标准](#)中。

此帮助主题包含以下章节

- [安全性指导原则](#)
- [高级安全性指导原则](#)
- [标准组织的最佳实践与标准](#)

安全性指导原则

以下章节描述针对 ztC Edge 系统的安全性指导原则。

注意：Stratus 已经过测试，并且支持以下指导原则。未经 Stratus 明确批准的其他任何更新或修改都可能影响该系统的正常运行。



如果您对 these 指导原则有任何问题，并且您的系统有服务协议，请联系您的授权 Stratus 服务代表寻求帮助。有关信息，请参阅 [ztC Edge 支持页](#) 在

<https://www.stratus.com/services-support/customer-support/?tab=ztcedge>

在实施安全性加强指导原则时，请考虑以下方面：

- 这些安全性指导原则是指在 ztC Console 和主机操作系统中执行的管理任务。ztC Console 是一个基于浏览器的界面，其可使您从远程管理计算机管理和监控 ztC Edge 系统的大多数方面(请参见 [ztC Console](#))。主机操作系统在该系统的每个节点上运行。您可以在 PM 的物理控制台上本地访问主机操作系统的命令行，也可以通过使用安全外壳 (SSH) 客户端远程访问主机操作系统的命令行(请参见 [访问主机操作系统](#))。
- 在进行任何配置更改前，记录当前设置，以便在必要时可将还原它们。此外，记录您正在进行的所有修改，以防所需这些信息进行故障排除。
- 更改默认系统设置时，尤其是在主机操作系统中，您必须在两个节点上进行更改，以防止可能影响系统正常运行的不一致问题。同样，在更改主机操作系统的根密码和其他用户帐户设置时，您必须在这两个节点上都进行此操作。以下指导原则需要进行这些更改的时间。

- 当您升级系统软件或更换系统中的节点时，并非为加强系统而进行的所有修改都可继续进行。同样，某些设置在节点之间共享，因此共享资源可能发生冲突。因此，在完成这些操作程序后，您应验证系统中的每个节点是否都具有正确的设置，以及系统是否正在正常工作。
- 在某些情况下，这些安全性指导原则会直接引用具有关于配置 **ztC Edge**系统和 **Stratus Redundant Linux** 软件的更多信息的知识库文章(例如, [KB-nnnn](#))。如下[访问知识库文章](#)中所述，您可以通过使用现有服务门户凭据，或通过创建新的用户帐户访问 **Stratus** 客户服务门户和知识库。

端口和协议

对系统进行网络连接或通信更改的任何管理员都应了解**Stratus Redundant Linux**使用的端口或协议。有关详细信息，请参阅 [KB-9357](#)。

网络分段

仅将**ztC Edge**系统连接到具有受信任设备的网络，或者连接到需要显式权限才能相互通信的网络。有关网络分段的更多信息，请参阅 **NIST** 特别出版物 **800-125B** 和 **800-39**。有关哪些以太网网络可在 **ztC Edge**系统上使用的信息，请参阅[网络架构](#)。

IP 表/防火墙

为系统启用 **IP** 表数据包过滤，以及阻止在正常运行中不使用的所有端口。恶意使用者可利用未使用接口上可能的安全漏洞作为后门。通过启用未用端口的 **IP** 表来限制此暴露。

有关如何实施 **IP** 表的详细信息，请参阅[管理 IPtables](#)。

注释：



- **ICMP** 协议用于在**ztC Edge**系统中执行 **ping**。如果将 **IP** 表设置为丢弃 **ICMP** 流量，则容错或故障转移支持将不会正常工作。
- **SSH** 协议用于连接到主机操作系统。如果将 **IP** 表设置为阻止 **SSH** 流量，则系统管理员将无法访问主机操作系统。

用户帐户创建

为有权访问该系统的每个用户创建单独的用户帐户，并考虑每个用户在设备使用中的角色。保持单独用户帐户还可实现可审核性或不可否认性，这样通过查看日志，可确定哪个用户访问了该设

备或进行了配置更改。

有关如何配置用户设置的详细信息，请参阅[配置“用户与组”](#)。

注释：



- 您无法删除缺省 **admin** 帐户，但可以通过编辑这些帐户设置来修改其名称和密码。
- 要启用忘记密码功能，您必须为每个用户帐户均指定一个电子邮件地址，包括**管理员**。此外，您必须按照[配置邮件服务器](#)中的描述启用邮件服务器；否则，系统无法发送密码重置电子邮件。

密码创建

您必须更改系统的默认密码。

在部署时，**ztC Console**会提示您设置新 **admin** 密码。**ztC Console**的密码策略要求您的密码符合以下条件：

- 其最小长度为 **8** 个字符。
- 其必须包含大写和小写字符。
- 其不能为用户名。

在首次登录时，主机操作系统会提示您设置新根密码。在更改主机操作系统的根密码时，您必须在这两个节点上手动更改此密码。有关详细信息，请参阅[访问主机操作系统](#)。

有关控制主机操作系统中密码质量的更多信息，请参阅[高级安全性指导原则](#)。

最低权限

限制每个用户对适用于他们职位或角色的功能的访问。

实施最低权限可防止无权限用户访问高于他们角色的服务。

有关如何配置可为每个用户定义权限的角色的详细信息，请参阅[配置“用户与组”](#)。

活动目录

活动目录集成提供单个集中式身份验证和授权点。凭借活动目录，您能够创建根据您的本地安全策略执行的组策略，以实现密码复杂性。

有关如何将 **ztC Edge**系统添加到活动目录域的详细信息，请参阅[配置活动目录](#)。

时间同步

时间同步很重要，因为它提供了一个集中式参考点，以确保运行和安全性流程在同一时间范围内工作。时间引用可使您在更新应用程序时对检查时间和使用时间有信心，以及根据时间和日期确保密钥和证书仍然有效。

当您首次登录 **ztC Edge** 系统时，启用网络时间协议 (NTP) 服务，以便自动设置系统时钟。将 NTP 配置为引用已知和可信任 NTP 服务器。有关详细信息，请参阅 [配置日期和时间](#)。



注意：仅使用 **ztC Console** 来正确配置 NTP 设置；不要在主机操作系统中手动配置它们。

安全连接

默认情况下，**ztC Console** 被配置为仅支持使用 HTTPS 协议的安全连接。

在 **ztC Edge** 系统上启用 HTTPS 可防止常见的 Web 安全攻击，以便为每个 Web 会话提供一个保密级别。HTTPS 对 Web 会话流量进行加密，提供数据完整性，以及提高 Web 流量的整体安全性。

启用 HTTPS 时，其仅支持 TLSv1.2，这是当前推荐的最强加密套件。密码包括：

TLSv1.2:

密码：

```
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
```

此外，在使用邮件服务器或其他类型的服务器软件时，启用安全的已加密连接。有关在 **ztC Edge** 系统上为邮件服务器配置和启用已加密连接的信息，请参阅 [配置邮件服务器](#)。

更新 SSL 证书

ztC Edge系统带有自签名 SSL 证书，但可将其更新为任何购买的或提供的证书。通过更改 SSL 证书可将信任根更新为客户规范。有关详细信息，请参阅 [KB-9792](#)。

SNMP 配置

简单网络管理协议 (SNMP) 是用于接收警报，发送自陷和监控系统状态的标准协议。SNMP 利用在分层配置的管理信息库 (MIB) 中保存的系统定义信息。

出于安全原因，客户可能想要以 ztC Edge 系统的主机级别禁用 SNMP。如果需要，可通过向 IPtables 添加规则来禁用所有 SNMP 连接(请参阅[管理 IPtables](#))，以阻止 UDP 端口 162、161 和 199 以及 TCP 端口 162 和 199。

或者，您可以使用 SNMP 受限配置，该配置在 SNMP 配置文件中禁用 SNMP v1 和 v2，并且仅配置 SNMPv3。有关详细信息，请参阅[配置 SNMP 设置](#)。



注意：默认情况下 ztC Edge 系统已启用了 SNMP v1 和 v2。出于安全目的，应禁用这些版本，并且仅应启用版本 3。

备份

为防止发生安全事件，具有备份非常重要；可将装置恢复到已知良好状态以实现持续运行。获取的所有备份均应存储在安全位置。

要备份 VM 及其客人操作系统，请参阅[导出虚拟机](#)。要还原具有与原始 VM 相同的 SMBIOS UUID、系统序列号和 MAC 地址的相同 VM，请参阅[从 OVF 文件替换/还原虚拟机](#)。

要备份在[首选项](#)页上配置的 ztC Edge 系统首选项，可将这些设置保存到本地存储设备或云中。有关详细信息，请参阅[保存和还原系统首选项](#)。

在冗余双节点 ztC Edge 系统上，每个节点还作为另一个节点的备份。如果某个节点出现故障，您可以替换当前已授权系统中的节点，然后系统会使用正在运行的节点上的 Stratus Redundant Linux 软件和虚拟机的准确副本自动还原该节点。

自动本地站点恢复

自动本地站点恢复 (ALSR) 配置连接位于两个独立站点的两台物理机。它是一种容灾部署，既保持硬件冗余又保持物理计算机室及其所在建筑物的冗余。由于地理上的分离，ALSR 配置需要仔细的组件布局规划和较复杂的网络拓扑。由于 ALSR 配置使 A-Link 网络可能出现其他潜在故障条

件，因此对于 ALSR 配置，Stratus 强烈建议您使用仲裁服务。(ALSR 配置不适用于已授权用于一个节点的系统。)

有关详细信息，请参阅[创建 ALSR 配置](#)。

审核

通过本地策略实施审核，以便定期收集和管理检测、了解网络攻击以及从网络攻击中恢复所需的事件日志。

审核日志页显示 ztC Console 中用户活动的日志。要打开此页，则单击左侧导航面板中的**审核日志**。(要显示有关 ztC Edge 系统上的事件的信息，请参阅[“警报历史记录”](#)页。)

日志信息包含：

- 时间—操作的日期和时间。
- 用户名—发起此操作的用户的名称。
- 源主机—正在运行 ztC Console 的主机的 IP 地址。
- 操作—ztC Console 中执行的操作。

您还可以使用 `snmptable` 显示有关审核日志的信息(有关详细信息，请参阅[使用 snmptable 获取系统信息](#)。)

使用日志持续监控 ztC Edge 系统。为确保在接到服务电话时迅速提供服务，还应为您的系统启用支持通知和定期报告，以便使 Stratus 随时了解您系统的运行状况。有关详细信息，请参阅[配置远程支持设置](#)。

升级

定期升级 Stratus Redundant Linux，防止因组件过时而出现安全漏洞被利用的情况。有关频率和方法的信息，请参阅您的本地安全策略。



小心：不要从除 Stratus 外的任何来源更新 ztC Edge 系统的 CentOS 主机操作系统。仅使用与 Stratus Redundant Linux 软件一同安装的 CentOS 版本。

ztC Console 中的**升级套件**页使您能够上传和管理用来把系统升级到 Stratus Redundant Linux 软件更新版本的升级套件。您还可以将升级套件复制到 USB 介质，以便在重新安装该系统软件时使用此介质。

要打开**升级套件**页面时，点击 ztC Console 的左侧导航面板上的**升级套件**。

有关升级 Stratus Redundant Linux软件的信息，请参阅[使用升级套件升级 Stratus Redundant Linux软件](#)。有关创建 USB 介质的信息，请参阅[创建具有系统软件的 USB 介质](#)。

物理安全性

将每个 ztC Edge系统均安装在安全位置，以防止恶意用户访问这些节点。

使用可审核系统保护每个位置，以识别进入该区域的人员，从而识别恶意用户。

物理安全性是对任何设备(包括 ztC Edge节点)的篡改检测和警报的重要补充。

高级安全性指导原则

以下章节描述针对 ztC Edge系统的高级安全性指导原则。

密码质量建议

当设置密码时，建议包括：

- 设置最小密码长度至少为 8 个字符，其中需要以下四个特征中的三个：一个大写字母、一个小写字母、一个数字和一个特殊字符。
- 要求用户定期重置密码，例如每 30、60 或 90 天重置一次。对于数量可变的密码更新历史记录，您还可以禁止重用密码。

要在主机操作系统中手动更新密码质量设置



注意：在该系统中的两个节点上均应用密码质量设置。

1. 登录主机操作系统，如[访问主机操作系统](#)中所述。
2. 使用文本编辑器打开 /etc/pam.d/system-auth 文件。
3. 使用相应的设置修改 pam_pwquality.so 模块。例如，使用与以下类似的设置：

```
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
```

上个示例设置以下值：

minlen=8 设置 8 个字符的最小密码长度。

lcredit=-1 将密码中小写字母的最小数量设置为 1。

`ucredit=-1` 将密码中大写字母的最小数量设置为 1。

`dcredit=-1` 将密码中数字的最小数量设置为 1。

`ocredit=-1` 将密码中 `@`、`#`、`!`、`$`、`%` 等其他字符的最小数量设置为 1。

`enforce_for_root` 确保即使根用户正在设置密码，也应执行复杂性策略。

4. 要限制密码历史记录，则使用相应的设置修改 `pam_pwhistory.so` 模块。例如，使用与以下类似的设置：

```
password requisite pam_pwhistory.so debug use_authok
remember=10 retry=3
```

5. 保存 `/etc/pam.d/system-auth` 文件。

有关主机操作系统中密码策略的更多信息，请参阅 **CentOS** 文档：

https://wiki.centos.org/HowTos/OS_Protection#Password_Policies

并发用户管理

持续监控审核日志，以查看哪些用户已登录该计算机，以及他们是否仍处于活动状态。

标识当前正在操作该系统的用户，以使他们的使用合法化并审核他们的使用情况。

防病毒

持续执行基于网络的分析，以便进行防病毒或恶意软件检测。

基于网络的入侵检测系统补充了支持对安全功能的预期操作进行验证的 **ztC Edge** 功能。该检测系统应搜索异常网络流量，并要求进行调查，以便验证任何恶意意图。

SSH 访问限制

多个 `/etc/ssh/sshd_config` 参数限制可通过 **SSH** 访问系统的用户和组。如果该文件中没有以下任何参数，则编辑该文件，以便设置其中一个或多个参数来限制访问：

`AllowUsers`

`AllowUsers` 参数使系统管理员可选择允许特定用户使用 **SSH** 来访问系统。此列表由空格分隔的用户名组成。此参数不识别数字用户 ID。要通过仅允许已被允许的用户从主机登录来进一步限制用户访问，可采用 `user@host` 的形式来指定条目。

`AllowGroups`

AllowGroups 参数使系统管理员可选择允许特定用户组使用 **SSH** 来访问系统。此列表由空格分隔的组名称组成。此参数不识别数字组 ID。

DenyUsers

DenyUsers 参数使系统管理员可选择拒绝特定用户使用 **SSH** 来访问系统。此列表由空格分隔的用户名组成。此参数不识别数字用户 ID。如果系统管理员要通过具体拒绝来自主机的用户访问来进一步限制用户访问，则可采用 `user@host` 的形式来指定条目。

DenyGroups

DenyGroups 参数使系统管理员可选择拒绝特定用户组使用 **SSH** 来访问系统。此列表由空格分隔的组名称组成。此参数不识别数字用户 ID。

限制哪些用户能够使用 **SSH** 来远程访问系统将有助于确保只有授权用户才能访问该系统。

MaxAuthTries

MaxAuthTries 参数指定每连接允许的最大身份验证尝试次数。当登录失败计数达到此数目的一半时，错误消息将被写入 `syslog` 文件，从而详细说明此登录失败。

将 MaxAuthTries 参数设置为较小的数值将最大程度降低对 **SSH** 服务器成功进行暴力攻击的风险。当建议设置为 4 时，根据站点策略设置此数值。例如：

```
MaxAuthTries 4
```

IgnoreRhosts

IgnoreRhosts 参数指定 `.rhosts` 和 `.shosts` 文件将不用于 `RhostsRSAAuthentication` 或 `HostbasedAuthentication`。

设置此参数会强制用户在使用 **SSH** 进行身份验证时输入密码。例如：

```
IgnoreRhosts yes
```

HostbasedAuthentication

HostbasedAuthentication 参数指定是否允许将 `.rhosts` 或 `/etc/hosts.equiv` 与成功的公钥客户端主机身份验证结合使用，从而通过可信任主机进行身份验证。此选项仅适用于 **SSH** 协议版本 2。

即使当在 `/etc/pam.conf` 禁用支持时 `.rhosts` 文件无效，禁用在 **SSH** 中使用 `.rhosts` 文件的功能也可提供额外的保护层。例如：

```
HostbasedAuthentication no
```

有关 `sshd_config` 参数的更多信息，请参阅 `sshd_config(5)` 手册页。

标准组织的最佳实践与标准

本主题中的信息基于以下最佳实践和标准。

CIS Controls 版本 7.1

CIS 控制是一系列已排列优先级的最佳实践，其旨在阻止当今最普遍、最危险的威胁。这是由全球领先的安全专家开发的，每年都会对其进行改进和验证。有关更多详细信息，请访问 CIS 网站：<https://www.cisecurity.org>。

CIS 控制为：

基本

1. 硬件资产的库存和控制
2. 软件资产的库存和控制
3. 并发漏洞管理
4. 管理权限的受控使用
5. 移动设备、笔记本电脑、工作站和服务器的安全配置
6. 审核日志的维护、监控和分析

基础

7. 电子邮件和 Web 浏览器保护
8. 恶意软件防御
9. 网络端口、协议和服务的限制和控制
10. 数据恢复功能
11. 防火墙、路由器和交换机等网络设备的安全配置
12. 边界防御
13. 数据保护
14. 基于需要了解的内容的受控访问
15. 无线接入控制
16. 帐户监视和控制

组织

17. 实施安全意识和培训计划
18. 应用程序软件安全
19. 事件响应和管理
20. 渗透测试和红队练习

ISA/IEC 62443-4-2

ISA/IEC 62443-4-2 详细说明了与符合控制系统功能安全级别的七个基本要求 (FR) 相关的技术组件要求 (CR)。有关更多详细信息，请访问 IEC 网站：<https://www.iec.ch/>。

这些基本要求为：

1. 身份识别和身份验证控制 (IAC)
2. 使用控制 (UC)
3. 系统完整性 (SI)
4. 数据机密性 (DC)
5. 受限数据流 (RDF)
6. 及时响应事件 (TRE)
7. 资源可用性 (RA)

1. 身份识别和身份验证控制 (IAC)

将用户的身份识别与授权机制结合使用，以实施对组件的访问控制。必须验证请求访问的用户的身份，以防止未授权用户获得组件访问权限。授权来自访问控制列表，这些列表针对登录 ztC Edge 系统并使用密码进行身份验证以进入该系统的不同用户。

2. 使用控制 (UC)

已对用户进行识别和身份验证后，该组件必须将允许的操作限制为对该组件的已授权使用。ztC Edge 系统已定义了实施最低权限概念的角色。创建具有不同级别访问控制的多个用户还定义了对该组件的已授权使用。

3. 系统完整性 (SI)

设备的完整性不应受到影响，无论是运行和非运行状态下的软件还是物理组件。ztC Edge 系统实施安全启动，这可验证该装置是否正在从受信任状态引导和启动，以及在升级前是否验证了软件组件的数字签名。确保系统完整性对于防止未授权操纵或修改数据或系统非常重要。

4. 数据机密性 (DC)

其目的是确保通信通道中的信息和存储在存储库中的数据的机密性，以防止未经授权披露。ztC Edge系统具有带 TLS v1.2(用于 Web 通信)的 HTTPS，以及具有加密功能的 SSH 和 SMTP，从而确保信息不会被恶意人员访问。

5. 受限数据流 (RDF)

受限数据流是控制系统通过区域和管道进行的分段，旨在限制不必要的数据流。ztC Edge网络架构支持如网络配置确定的路由和交换，以便管理如安装系统工程师确定的信息流。充分利用 ztC Edge系统的网络功能可进行网络分段，以限制数据流。

6. 及时响应事件 (TRE)

尽管系统可在安全状态下开始运行，但可能会发生漏洞和安全事件。ztC Edge系统具有产品安全事件响应 (PSIR) 团队，该团队旨在以对安全事件作出反应并报告调查结果，同时及时解决问题。ztC Edge系统具有警报日志，在发生可能指示安全事件的配置更改时，这些日志可用于通知相应的通道。这些日志包含足够的取证信息，并且会通过电子邮件发送这些电子警报通知。

7. 资源可用性 (RA)

该控制的目的是确保组件能够弹性地应对各种类型的拒绝服务事件。ztC Edge系统的高可用性是“始终在线”状态的基础。工业控制系统必须保持高可用性状态，因为可能存在对系统的生命安全影响。凭借内置的虚拟化和可用性层、自动数据保护以及应用程序恢复，当在边缘位置进行虚拟化计算时，Stratus Redundant Linux可极大降低对 IT 的依赖。其自我保护和自我监控功能有助于缩短计划外停机时间，以及确保关键业务工业应用程序的持续可用性。

12

第 12章：SNMP

简单网络管理协议 (SNMP) 是用于接收警报，发送自陷和监控系统状态的标准协议。SNMP 利用在分层配置的管理信息库 (MIB) 中保存的系统定义信息。

要将 ztC Edge 系统配置成使用 SNMP，请参阅 [配置 SNMP 设置](#)。

有关使用 `snmptable` 命令获取系统相关信息的信息，具体讲是有关警报、审核日志、节点、VM 和卷的信息，请参阅 [使用 snmptable 获取系统信息](#)。

要下载 MIB 文件的副本，请访问以下项目的 [驱动程序和工具](#) 部分：此 [下载](https://www.stratus.com/services-support/downloads/?tab=ztcedge) 页面在 <https://www.stratus.com/services-support/downloads/?tab=ztcedge>。

使用 `snmptable` 获取系统信息

您可以发出 `snmptable` 命令来获取系统相关信息，具体讲是有关警报、审核日志、节点、VM 和卷的信息。

要显示警报信息

要显示有关警报的信息，则发出以下命令：

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c  
public localhost ztCEdgeAlertTable
```

该命令输出显示以下内容：

字段	描述
ztCEdgeAlertIndex	警报号。

字段	描述
ztCEdgeAlertSeverity	<p>警报严重性(有关数字值, 请参阅 ztCEdgeAlertSeverityNum)。值为:</p> <p>清除 </p> <p>信息 </p> <p>轻度 </p> <p>重大 </p> <p>严重 </p> <p>极其严重 </p>
ztCEdgeAlertType	<p>警报类型。示例为:</p> <ul style="list-style-type: none"> • node_singleSystemDisk • 节点维护 • 该装置未进行很好的负载均衡
ztCEdgeAlertSource	<p>警报的来源。示例为:</p> <ul style="list-style-type: none"> • node0 或 node1 • ztC Edge系统网络名称 • 网络主机名
ztCEdgeAlertDateTime	<p>警报的日期和时间, 格式为 <i>yyyy-mm-dd hh:mm:ss</i>, 其中 <i>yyyy</i> 是年, <i>mm</i> 是月, <i>dd</i> 是日期, <i>hh</i> 是小时, <i>mm</i> 是分钟, <i>ss</i> 是秒(例如, 2017-11-03 23:49:45)。</p>
ztCEdgeAlertCallHomeSent	<p>如果为 true, 则自动通报已发送; 如果为 false, 则自动通报未发送</p>
ztCEdgeAlertEAlertSent	<p>如果为 true, 则电子警报已发送; 如果为 false, 则电子警报未发送</p>

字段	描述																		
ztCEdgeAlertSNMPTrapSent	如果为 true, 则 SNMP 自陷已发送; 如果为 false, 则 SNMP 自陷未发送																		
ztCEdgeAlertInformation	有关警报的信息。示例为: <ul style="list-style-type: none"> • 节点 节点 1 正在维护 • node0 具有单个系统磁盘: 策略假定此磁盘为冗余 - 如果不是, 请添加另一个内置磁盘 • 业务网络 net_728 正在报告链路降级情况 • 该装置未进行很好的负载均衡 																		
ztCEdgeAlertSNMPTrapOID	SNMP 自陷对象标识符 (OID)(例如, COMPANY-MIB::nodeSingleSystemDisk)																		
ztCEdgeAlertSeverityNum	ztCEdgeAlertSeverity 号。值为: <table> <tbody> <tr> <td>0</td> <td>清除</td> <td></td> </tr> <tr> <td>1</td> <td>信息</td> <td></td> </tr> <tr> <td>2</td> <td>轻度</td> <td></td> </tr> <tr> <td>3</td> <td>重大</td> <td></td> </tr> <tr> <td>4</td> <td>严重</td> <td></td> </tr> <tr> <td>5</td> <td>极其严重</td> <td></td> </tr> </tbody> </table>	0	清除		1	信息		2	轻度		3	重大		4	严重		5	极其严重	
0	清除																		
1	信息																		
2	轻度																		
3	重大																		
4	严重																		
5	极其严重																		

要显示审核日志信息

要显示有关审核日志的信息, 则发出以下命令:

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c
public localhost ztCEdgeAuditTable
```

该命令输出显示以下内容:

字段	描述
ztCEdgeAuditIndex	将指示显示了信息的审核日志的递增数字(1、2等)。
ztCEdgeAuditDateTime	生成审核的日期和时间, 格式为 <i>yyyy-mm-dd hh:mm:ss</i> , 其中 <i>yyyy</i> 是年, <i>mm</i> 是月, <i>dd</i> 是日期, <i>hh</i> 是小时, <i>mm</i> 是分钟, <i>ss</i> 是秒(例如, 2017-11-03 23:49:45)。
ztCEdgeAuditUsername	致使此审核生成的用户的名称(例如, audit 或 admin)。
ztCEdgeAuditOriginatingHost	发起了此审核的主机的 IP 地址。
ztCEdgeAuditAction	正在审核的操作的描述。示例为: <ul style="list-style-type: none"> "Login user \"audit" "Start virtual machine \"manager1" "Remove all cleared alert"

要显示节点信息

要显示节点信息, 则发出以下命令:

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c
public localhost ztCEdgeNodeTable
```

该命令输出显示以下内容:

字段	描述
ztCEdgeNodeIndex	指示显示了信息的节点的数字(一般为 1 或 2)。
ztCEdgeNodeId	节点的主机 ID(例如, host:o34)。

字段	描述
ztCEdgeNodeDisplayName	节点名称, node0 或 node1。
ztCEdgeNodeIsPrimary	如果为 true, 则该节点为主节点。如果为 false, 则该节点为从节点。
ztCEdgeNodeStateNum	节点状态为: 0 正常 (✓) 1 警告 (⚠) 2 忙碌 (🔄) 3 已损坏 (✖) 4 维护 (🛠)
ztCEdgeNodeActivityNum	节点活动为: 0 正在映像 1 正在启动 2 正在运行 3 正在停止 4 正在重启 5 电源已关闭 6 失败 7 固件更新 8 丢失 9 被逐出 10 不可及 11 Proto(正在初始化) 12 正在撤出

要显示 VM 信息

要显示 VM 信息, 则发出以下命令:

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c
public localhost ztCEdgeVMTable
```

该命令输出显示以下内容：

字段	描述
ztCEdgeVMIndex	将指示显示了信息的 VM 的递增数字(1、2 等)。
ztCEdgeVMId	VM ID(例如, vm:01467)。
ztCEdgeVMDisplayName	VM 名称(例如, MyVM)。
ztCEdgeVMRunningNode	正在运行 VM 的节点, node0 或 node1。
ztCEdgeVMAvailability	VM 可用性, HA(高可用性)或 FT(容错)。
ztCEdgeVMStateNum	<p>VM 状态为:</p> <ul style="list-style-type: none"> 0 正常 (✓) 1 警告 (⚠) 2 忙碌或正在同步 (🔄) 3 已损坏或已列入黑名单 (✗)
ztCEdgeVMActivityNum	<p>VM 活动为:</p> <ul style="list-style-type: none"> 0 安装 1 正在启动 2 正在运行 3 正在移动 4 正在停止 5 已停止 6 正在导出 8 已暂停 9 正在加载 10 正在崩溃

字段	描述
	11 已崩溃
	12 正在转储
	13 正在等待

要显示卷信息

要显示卷信息，则发出以下命令：

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c
public localhost ztCEdgeVolumeTable
```

该命令输出显示以下内容：

字段	描述
ztCEdgeVolumeIndex	将指示显示了信息的卷的递增数字(1、2等)。
ztCEdgeVolumeId	卷 ID(例如, volume:o588)。
ztCEdgeVolumeDisplayName	卷名称(例如, root)。
ztCEdgeVolumeSyncPercentage	已同步的卷的百分比。
ztCEdgeVolumeUsedBy	正在使用该卷的 VM 或主机的名称(例如, MyVM);无指示未在使用卷。
ztCEdgeVolumeStateNum	卷状态为： 0 正常 (✓) 1 警告 (⚠) 2 忙碌或正在同步 (🔄) 3 已损坏 (✗)

