解决方案实践

华为云芯片 EDA 云服务解决方案实践

文档版本1.0发布日期2023-12-07





版权所有 © 华为技术有限公司 2024。 保留一切权利。

非经本公司书面许可,任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部,并不得以任何形式传播。

商标声明

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束,本文档中描述的全部或部分产品、服务或 特性可能不在您的购买或使用范围之内。除非合同另有约定,华为公司对本文档内容不做任何明示或暗示的声 明或保证。

由于产品版本升级或其他原因,本文档内容会不定期进行更新。除非另有约定,本文档仅作为使用指导,本文 档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以"漏洞处理流程"为准,该流程的详细内容请参见如下网址: https://www.huawei.com/cn/psirt/vul-response-process 如企业客户须获取漏洞信息,请参见如下网址: https://securitybulletin.huawei.com/enterprise/cn/security-advisory

1 万案概还	1
2 资源和成本规划	4

2 资源和成本规划	4
3 实施步骤	7
3.1 搭建北鲲云平台运行环境	7
3.1.1 配置云上网络环境	7
3.1.2 购买云资源	12
3.1.3 部署北鲲云平台服务	15
3.2 配置 LDAP 服务	17
3.2.1 部署 ldap 服务端	17
3.2.2 配置 ldap 主从	
3.2.3 配置 ldap 客户端	18
4 修订记录	19

目录



应用场景

- 芯片设计企业弹性上云:整合本地资源和华为云资源,构建混合云集群,弹性按需上云,解决业务高峰期算力存力不足的问题;
- 芯片设计企业轻资产运营:企业IT全面上云,云上构建设计仿真一体化环境,通 过多维度多层次的安全服务,在弹性使用云上算力资源的同时,保证芯片设计各 阶段的数据安全;
- 多地域协同办公的芯片设计企业:结合专线、VPN等技术搭建国内外多团队协同 多地域高可用的EDA设计仿真云平台。

业务痛点及挑战

- 芯片研发全流程对于IT资源的诉求是波动,资源高峰期,本地静态资源无法满足 动态需求,资源低谷期,本地资源只能闲置,整体IT资源利用率低,影响项目进 度;
- 芯片研发随着工艺节点发展,对于IT资源的诉求是翻倍,企业IT部门无法快速做到 无限制扩机房、扩容操作。
- 公有云资源丰富多样,一旦云上资源调度策略不合适,会导致云山仿真任务挂住,无法发挥云上弹性按需的效果,还影响仿真工作稳定性;
- 以传统方式将芯片研发环境迁移云上的解决方案严重改变了芯片设计工程师线下 操作方式,增加了学习成本,降低了工作效率;
- 多地域的研发中心协同能力不足,计算资源调度差;
- 作业、资源监控不直观,作业状态通知不全面、不及时,导致作业运行失败频 发,资源有效利用率不高。

方案架构



图 1-1 华为云芯片设计仿真一体化解决方案架构

- 运维人员和设计人员双通道接入,保护数据网络的互相隔离访问,子网隔离,防 护项目数据安全;
- 2. 静态云上工作站,完善的IC设计仿真环境,仿真作业弹性调度云上集群;

方案优势

- 安全高效的云上EDA设计桌面:设立多个安全分区,使用 ACL和安全组访问控制 技术保障核心数据的安全;
- 不改变原有操作习惯:云上和线下保持一致的EDA软件环境,混合云模式支持本 地设计云上仿真,结合调度系统命令的转译适配,为芯片设计工程师提供无感化 上云的操作体验;
- 无需运维资源最新:管理无压力:无需运维管理线下计算机,线上的硬件资源持续更新,您可以一直使用到最新的配置;
- 联合运营 服务稳定:服务全方位:华为云与北鲲云联合运营,市场合作深度绑定,北鲲云为客户解决云上资源调度、软件工艺库安装、案例脚本调试全方位服务,为客户减负,服务稳定有保障;
- 按需使用 弹性计费:成本更可控:云上计算机资源闲置关闭不计费,按照工作有效时间弹性计费,成本更加可控。

约束与限制

管理平台部署限制

硬件限制:北鲲云管理平台运行环境推荐配置CPU4核、内存16G、系统盘200GB,最少需要三个节点做高可用部署。

• 软件系统限制:北鲲云管理平台运行在CentOS7下,其他Linux发行版本可能出现 兼容问题。

2 资源和成本规划

基于北鲲云平台+华为云搭建芯片设计仿真一体化环境

表 2-1	资源和成本规划
-------	---------

云资源	规格	数量	每月费用 (元)
VPC	公共VPC 红区VPC	2	00.00
子网	设计堡垒机子网 运维堡垒机子网 设计子网 计算子网 存储子网 公共子网	6	00.00
安全组	设计安全组 计算安全组 存储安全组 公共安全组	4	00.00
对等连接	打通公共VPC和红区VPC	1	00.00
云服务器(包月)	北鲲云平台运行服务器 4核16G(高IO 200G存储)	3	1,709
云服务器(按需)	包括设计桌面,如果干台计算节点 配置不固定	弹性	弹性
LICENSE服务器	LDAP服务 主从 EDA软件LICENSE服务 主从 2核4G(高IO 200G存储)	2	439

云资源	规格	数量	每月费用 (元)
主机安全服务(包 月)	企业版 10台 以实际数量为准	弹性	900
云审计服务	基础功能免费 可查看7天内数据	1	00.00
云日志服务	500M以内免费	1	00.00
云堡垒机(包月)	华为云堡垒机标准版100资产	1	3,780
弹性文件服(包月)	SFS turbo 标准型增强版10TB,增加的 容量按需购买	1	4,096
文件系统备份	SFS Turbo备份存储库 20TB	1	7168
VPN网关	IPsec 10M	1	775
北鲲云平台 LICENSE	以商务合同为准,以调用核数进行收费	1	弹性
正式阶段:	该价格仅为参考,实际需要以控制台显 示为准, 且仅包含固定费用,不包含弹 性资源费用	合计	81931.4

表 2-2 网络规划

云资源	名称	网段	说明
VPC	公共VPC	172.16.0.0/20	和本地建立VPN连接
	芯片研发VPC	172.17.0.0/20	EDA黑盒环境
子网	设计堡垒机子网	172.16.0.0/24	/
	运维堡垒机子网	172.16.1.0/24	/
	设计子网	172.17.0.0/24	VDI设计桌面
	计算子网	172.17.0.1/24	弹性计算资源
	存储子网	172.17.0.2/24	SFS存储
	公共子网	172.17.0.3/24	北鲲云平台服务器
安全组	设计安全组	/	通过堡垒机子网进行跳 转
	计算安全组	/	仅运维堡垒机子网可跳 转
	存储安全组	/	仅运维堡垒机子网可跳 转
	公共安全组	/	仅运维堡垒机子网可跳 转

云资源	名称	网段	说明
对等连接	公共VPC-红区VPC	/	/
路由表	rtb-公共	/	设计堡垒机子网路由至 设计子网 运维堡垒机子网路由至 红区所有子网
	rtb-红区	/	设计子网路由至设计堡 垒机子网
网络ACL	设计子网ACL	/	仅可访问红区内部子网 和 设计堡垒机子网
	设计堡垒机子网ACL	/	可访问红区设计子网

表 2-3 数据规划

数据类型	目录	读取频率	备份频率				
用户数据	/home	较高速IOPS读取	备份频率高				
项目数据	/data/project	较高速IOPS读取	备份频率高				
设计工具	/opt/modulefiles	普通高速读取	备份频率低				
IP和工艺库数 据	/public/foundry	普通高速读取	备份频率低				
仿真数据	/data/project/ user/sim	较高速IOPS读写	较少备份或不备份				
推荐与本地目录保持一致减少调试成本							



3.1 搭建北鲲云平台运行环境

3.2 配置LDAP服务

3.1 搭建北鲲云平台运行环境

3.1.1 配置云上网络环境

🗀 说明

以下操作均在虚拟私有云VPC控制台完成

1. 创建VPC

分别创建架构中的公共VPC和红区VPC,创建VPC时注意网段划分。

图 3-1 创建 VPC1

				1 20287	DBARNAP, NERS	ian, menti serat-m	wo-woar Actuaroa	P. AU176				×
M Hann	华为云 🗆 💮 🖻	MD 9							Q x			۳
=	网络控制台		虚拟私有云() •• ####^ •• m#	31 0					○ 1711 D @@@ame	STRUCTURE OF STRUCT	
6	805	- 1	1817412-18	性的关键字统术							Q C C	
۵	道印从有12 1889/PC	1	2543	PHRG		us	子将个数	器由表	服務器个数	操作		
.00.	子用	· 1							1.11			
o	20.00	- 1	-						1.1	-		
0	对等压缩	- 1										
6	卵性同中	- 1	•						1.11	-		
Ô	10/78280											
4	VPC流日志	- 1										0
۲	理性公司户和管理											0
8	NATED:											0
\odot	弹性负载均衡											
	VPG 總續世点											
	222388											
	\$\$\$\$\$\$											

图 3-2 创建 VPC2

🚯 Excelosational, accessive, accessive, accessive analy-analy-analy-analy-analy-analy-									
	参方元 合 12000			19 de					
00080000		基本社立 2151 2157 17-0122 2002王 ・	* ##?** * MIDENDERFACTION (MIDENDERSON), KANNENS, MANNENS, MAN						
4 0 0 0	·	RUATION THES 200 7000-4000 7000-4000 2000-4000 2000-4000	IND 0 IND 1 IND		0				
		do illi felicit							

2. 创建子网

在公共VPC和红区VPC中分别创建以下子网,操作演示见截图。

云资源	名称	网段	说明
子网	设计堡垒机子网	172.16.0.0/24	跳转
	运维堡垒机子网	172.16.1.0/24	运维
	设计子网	172.17.0.0/24	VDI设计桌面
	计算子网	172.17.0.1/24	弹性计算资源
	存储子网	172.17.0.2/24	SFS存储
	公共子网	172.17.0.3/24	北鲲云平台服务 器

表 3-1 创建子网

图 3-3 创建子网 1

					Finansenan, Arten	958. 45 81 5993-6	stan-ange Aus	stanse, suma						
	単方云 二 〇 1110						22							
Ξ	网络绘彩台		子間 ① ● ※※ * ● ※※***									⊖ #0	687	FR
0	22 2010/42		BUNDERSTR									a	i 0 (G
9	5825VPC		830	虚彩私有云	PHR	PVORES (1)	800	988 ①	RMACL	算点者	滑作			
.00	子用		本地子网	#8	10.110.0.0/24	- 7183Pv6	12.00	可用区2		10-33 2038:00	RNBAR	209		
0	20.40%		subnel-2	68	172.15.95.0119	- Habirvo	可用	可用区2		rib-hpc BCU20000	Exans	231		
0	7786338		subset-6	68	172.15.64.019	- 7180Pv6	12.00	时用田4		nto-hajo Biol Statute	2238A8	20		
<u>ه</u>	98±53+		subnet-6	628	172.16.32.0/19	- 7161Pv6	12月	17.19.12.5		10-800 2013/2020	EMBOR	89		
0	05/70246		5+82/2+	2 R	10.86.17.9/24	- HillPv6	花用	可用区2		(1)公共 取以因由表	ENDOR	234		
	WPCIEBH		至20至1月11 (1)	22	10.05.15.0.24	- Halanda	可用	可用区2	No.	10-公共 取以出出版	Exans	20		
	理由公司の日本開発		C-lordun	CE	172.15.0.0/19	- HRIPVS	利用	可用包3		rtb-hpc Bici Strinte	ZMBAS	20		
	100902	÷	約39 7网	head	10.05.03.0.24	- Hatave	可用	可用区2		ris-transit Ris-Internet	XMBOS	239		
~	unc assenta													
	0-0-0-9445													
	20808													
	成初步用用地													
	276	ø												
	元1938	8												
	神性云照异静	e												

图 3-4 创建子网 2

					🚯 BARTING	inge. waxefdi. 2000 cedi-wain-inge Towainge. 🕫	;∓ s t		×
*									IN BOOKS MOUND 🖂 🖄 🔯
≡	网络控制台		子問 ⑦ ♥ 855 80 ♥ 255	819					() (FI) (1887)
0	222 2103/102		通过和这是他的大概学说来		创建子网		×		QCD
۲	REEVEC		20	虚别私购云	* 虚拟彩海云	28 · C	RMACL	Bala	190
.001	78		*地子科	#30		Pv4R(2): 10.110.0.020 Pv4R(2): 1	-	18-338 默认指由获	ENDOR BR
0	nes.		subret-2	SIIS.	NHX.	1000 / 10 / 10 / 10 / 10 / 10 / 10 / 10	-	10-100 2013/38/87/87	ESECT DR
0	对导致感		subret-6	828			-	rtb-hpc 取以助性限	Radama (Bio
9	弹性同手		subret-5	ALK .	· 96.57	LEDBE-OF/4	-	10-100 2013/02/20	RMAR IN
0	10/97241		至全省政府会	公共	* 7RPvRR	10 · 110 · 0 · 0 / 24 ·	-	18-公共 家以路会表	ENDER DR
4	VPCRBE		型杂婚王用卡	\$A		FROMEMER. FRANKLARK	293	(10-公共 取以指出来	Roman into
0	弹性公司的存在	- 1	submet-3	SIR.	子用Pvi用度	Tillerve ①	-	10-7pc 2013/06/06	ENDER BR
0	NATE:	Ť	RMFR	tansk	英联络白苏	Ru. 💿	-	Th-buest BLUE BER	ENDER BR
.04	VPC HINER								
	212296				电位配器 •	Ret DNSERNERSE NTHERENDE DHCHGEDHIE GES SES			
	全议系统器								U D
	出现中国网络	8				400 KON			0
	2002	ø							
	Ease	ø							
	弹性宫颈脊髓	e							

3. 创建对等连接

打通红区VPC和公共VPC的对等连接,使得公共VPC可以跳转至红区VPC。

					() 200.470.0092/060-1	nioena. Nexu cena-ans	an-sander Andesander. 🕬 🕬					×
	\$\$752 ④ ##						RR Q BE					
=	和62%35		对等连接 ① ※ ■###☆	0.593 0							0 #0	eibreas
0	8%								8462	* 88	 目標入意図的文紙字 	Q O
۲	- Alabama		849	教育	#38VPC	基現VPC用 段	对硝酸间口	NUMPC		損还	1845	
.00.	70		bans8-02#	Exist	Farst	10.05.03.0/20	01413714800054e12164c00	公共			92 20	
Θ	hem		bans8-8282	C Easte	transit	10.86.00.0/20	01413714800054e1284c00	1233			932 884	
\diamond	22803		735-banat	🙂 Eanté	735	10.110.0.020	01413714800054e1284c00	turat			1712 Bile	
۵	神性用令											
٢	0.0221											
4	VPCIDIE											
۲	弹性公司中和带宽											
ස	NATR[37]											
۵	弹性负制均衡											
	VPC INSEED.R											
	0.022345											0
	002858											8
	透灯中用花塔	P										0
	宗寺线	P										
	尔亚根	e .										
	弹性实际系统	P										

图 3-5 创建对等连接 1

图 3-6 创建对等连接 2

					matimating, model, and dell-addr-drap final	unip. Witte			×
	\$***** 🗎 💮 🖽								
≡	网络拉利台		对等连接 ① ※ 5555	• 2000				() (Fin () (Silver)	EA:R
0	838 #110.875				创建对导连接	×	Naitz • 25	• 1562-151022487 Q	C
@ .m	Sistorec		809 transit-요.M	秋念 〇 日禄元	2 対導油研究性物区地均等个VFC用的時期互用。 加減率気管区は2VFC互配、通常用三規規模用。	ARRANC SH	-	1841 1932 1939	
0	分列		tansi-IIE	C#9.	LER年 MVPC	211	-	98 89 62 89	
0	29年後期 19世紀年				* Sit: peering 01e5				
0	动用短期 VPC就日世	*			#36VPCFIE: 10.110.8.029				
0	MELLIN PRIME NATRIX	:			151833MVPC				
۲	WEDRINE VIC INSTAL	÷			• 20872E 01900P1 • ①				
	220391				+ SIMVPC TANK +				0
	202358 204558	e			218W/PC788 10.86.80.020	-			
	云专组 医腹膜	e e			and Role				
	神性宗服苏雄	ď							

4. 配置网络ACL规则

配置红区VPC和公共VPC内部子网之间的网络控制策略,公共VPC的运维接入子网和设计接入子网是唯一开放office访问的网络。

图 3-7 配置网络 ACL 规则 1



图 3-8 配置网络 ACL 规则 2



图 3-9 配置网络 ACL 规则 3

		A4758888509 752238 8084 2228-8897	5089 TERSON 11178	
🎍 \$P\$カ云 ② 11883 •7.18				
E C BERRACE				2 9,461 12 9±61
	1 A46240			
<u>.</u>				
				RB · BRAINSAF Q C
W	12×4983 1E	IPHONES (E	虚阳私用云 近	ian .
3 29827+	10.05 15.0/24		88	TORNER
5				
Ð				
× .				
6				
9				
ascript.void)0);				

图 3-10 配置网络 ACL 规则 4

		SARTERSEN	RP. VERSER, BONDRER	l-lessin-sin dar meses	Bendan, W attill			
□ (12506ACL □ (12506ACL □ (12506ACL □ (12506ACL □ (12506ACL □ (12506ACL □ (12506ACL) (1	医胆子网							2 4 79
C		关联子网 ● 元於7月18. 用BAACLBULSHBFF813	1.7final Ilifinati.		×		at • malaserer Q	C
	10.05.16.	Riturel 聖絵編ACL 書面9番目を行う方用		- 78 × 1	eranover Q	2	BK Rantt	
0		79 a	1P+4988 4E	Prifită (E	498.95.35			
4		ubret2	172.16.95.0119	-	KIE			
•		submitő	172.16.64.019		23 23			
•		Ee42/3+	10.86.17.0/24		28			
		5 • 8982:7 < 1 2 > 8877#	ac I	24				0

5. 配置路由表

路由表由一系列路由规则组成,用于控制虚拟私有云内子网的出流量走向。创建 虚拟私有云时,系统会自动为生成一个默认路由表,同时可以为子网自定义路由 表。

图 3-11 配置路由表 1

				 SARTABABINE REPORT 	ASSAL 0-2011-6443	ለ-ይሳለን ጠበአቀድሳለን.	前在开启							×
*	単方云 ① 11111					Q 78				80% I#				0
Ξ	网络控制台		路由表 ① ****** ******								© #0	9 (69.94	agaes	
6	0.2 855.47							285255A3	• 80	• 10	0.0000000	7 Q	00	
۲	50EVPC		80	成料私有云	黄型				关键子目	1911				
.00.	78		rtb-tip:	22	W-28 世界				4	80. 20	78 2425			
0	25:42		10-510	438	数以加出表				1	800 7.80	7A 2002			
0	对等油槽		rto transit	torsit	W-25 由後				1	89. 90	78 8485			
۵	弹性用中		市公共	公共	脱いしたたち				2	899 (200	7A #488			
۲	00/01212181	-												
Φ	VPCREe													
۲	神性公司的研究	۰.												
8	NATROX													
0	建成的现在													
	VPC HINES:													
	0.022996													0
	212008													8
	通知中用用器	8												
	2010	8												
	元由後	. °												
	律性无限外器	8												

图 3-12 配置路由表 2

		stop. adding actual single	Construction of the constr		
= < m-tgs					Q #0
	添加路由			*	
@ ⁸⁷⁰ migs L	(專品集 rfs-tpo贯以聚由集				
101. ID 47373754-6531-4e31-0018-09159aefcee4 🕼					
□ #d - ∠	H0984 ① 下	0 M-4 ① 28A	551.6		
0	10.05.0.024 73	■ E限 * trans141区(34252950	8552-6479-9 v	÷	
· · ·		(8)(8)(5))			
		M2 8 0			
C NOR STREET VERSE			-		MADERBERGER Q C
C Elevent (2)	下-現業型 ①	¥—₩ ()	東型 ①	SR 26	操作
S ≤ Lease	Local	Local	展開	系统数3. 表示VPC方案的回道	1932 BB
I 10.0.0.08	VINEX	vpngw-5558	Kitt.	d107e172-3271-4626-6270-e76656609102	1922 - BER
10.86.16.0/20	27883838	transit-KEE	国建立		912 BSk
10.06.00.0020	对酸连接	transil-428	目定义		1912 BBB

6. 配置安全组规则

通过安全组规则对弹性云服务器进行防护。

图 3-13 配置安全组规则 1

				BARHEMMENT	in, nanadu, ipesti nadis	-exect-serve	ao Filomatandao.	na÷n							×
Ξ	Riazakio		安全期 ②									@ #0	9 milite	eittea	
0	03		809	创建安全组				×						C	
@ .m	8/254		ALRONHIXEFER	* 2/F	10-5100						50			Q	
•	REACL		apétito	 • €010 	87/0658 +				08-092709	#208.2 17.	REPORT	NUCH I	1.5 ×		
0	PSER VPCRBs		apásta	<u>10.4</u>	通見2006年5日、第以北通22、118 第四第30日595日、道門丁香葵活動 ping37月7月14日5日7日5日5日5日	10, 10, 443 (2017, 524) L					ACE/ICII	REAR I	15 +		
	MESSERVER	•	userane_species_FLESSERSE_388			0255			wa-4803-9373-000	546040121	READ READ	世現2月 世現2月	59 + 58 +		
©	30122.8038	1	stemane_poolert_NETWORK_SSTH	-					x8-48c3-9373-90	54#040121	ACE/ICII	REAN I	NE +		
0	STORES	Ť	semane_tpcdet_MX0TER_7205380 Invators-sp		ni R	5 8			wb-65cb-9373-800	Seabab-121	REALING IN	1000000000000000000000000000000000000	59 + 58 +		
	02208		Dys-Full-com		4		0				122000	REAR I	NE V		
	spanate	ø	Sys-WebServer		10						REAL ROOM	REAR I	NE +		0
	云中战 苏维荣	8 8	<u></u> 858: H → <u></u> 2 →												0
	神性苦肠外毒	ø													

图 3-14 配置安全组规则 2



3.1.2 购买云资源

购买云服务器
 用于部署北鲲云管理平台和堡垒机,配置见上面章节。

图 3-15 购买云服务器 1

				• *	ьялавдялая	. 7692500. WORK	22285-0680-8040-	TRAFFORMER NUTR			×
*	\$25 · @ 2000										8 F 8
Ξ	2.5		#性云服务器 ③						⊙ ङशः ्र —खश्माः : d.∰	isz i 9 ellen 🗾	5941 <u>28</u> 98
	神性系统保健		Baseco: SIR-CH (I)								с
۵	TRIBAN NW	8	HA ZA INGE 25 -							0 0 6	8
703	建全国际各部		RUMBER								000
۵	z₩a		88:0 2	202	388 V	WS 7	1218-1218	PRM	iidskit V	63	12/1
0	中間日本の17月後		Coulor Reserve	2	210120	250	1000		松平(松月(目の快勝) 32元后前期	enverse2h_CN_name=h	88.4
۵	00.001275										- 1
۲	神性中間	•									
Φ	#24(0)	e *									
۲	王臣朱操正										
۵	RUMEN NEW	ø									
Φ	BERNE NEW	1									
	286	8									
	2008090	<i>.</i>									0
	2002WD										8
	Sector Day										0
	640										
											-

图 3-16 购买云服务器 2

المالية المالية <t< th=""><th></th><th>■ R##0- 40.0# 140-78445, HE02182, S 17853 ①</th><th>z (188-7#(1) 188-28- ort845x ⊘</th><th>88 Q</th><th>2044 NB 41 72</th><th>A 62 20180 If</th><th>BIDLS (general</th><th> ⊡ ⊙ π</th></t<>		■ R##0- 40.0# 140-78445, HE02182, S 17853 ①	z (188-7#(1) 188-28- ort845x ⊘	88 Q	2044 NB 41 72	A 62 20180 If	BIDLS (general	⊡ ⊙ π
③ 10.0000 ● 10.0000 <t< th=""><th></th><th>5 88 #5- 440.45 160-766415, 864046, 9 17852 ⊙</th><th>а (188-гж.(1) 198-28- отален ()</th><th></th><th></th><th></th><th>803</th><th>⊙ 2.4</th></t<>		5 88 #5- 440.45 160-766415, 864046, 9 17852 ⊙	а (188-гж.(1) 198-28- отален ()				803	⊙ 2.4
() 10000		। स्वाह क्राउ – । अतः त्यह उद्यान्तरकर्मातः, सावजनातः, त रामह्य ः	四 1989-1711(1) 195-128- 07884234 ②					
44444 44444 44744 4774 47743 47745	RATHEN	 11日 長日- 1400-0月 11日 日本 11日 日本 11日 日本 11日 日本 	а (1986-Гж.(1) (1986-1986- 1978-Февралов 1978-Тек					
4-1日 ● ○ 第 約5月前日 中型之間5月回三十回日、前 (5月前) 初月回三日 (5月前) 初月回三日 (5月前) (1月回三日) (1月回三日)	naiste and and a state	THE O	2 98/14(1) 99-28- 018424 ()					
1994) 219120 2018 x201178 ()	रास्ट) इस्टः)	() (2007						
arti starta ())							
ni • Ad	15 4cP0s	• 78 100	• 0885	۹	Independenting Independent			
08820	WCPUS 4E	AM .5	CEA 12	88/8X98 () II	ARREN () ;;	945	HEREAD () 12	
c7.starge.4	4vCPUs	1908	Intel Ice Lake 3.90Hz	最大 8 00.05	86/5PP8		¥524,88/1	
c0.starge.4	4vCPUs	1008	Intel Cascade Lake 3 85Hz	2.4/8 GBB1	8675993		¥499.00/7]	
c3.starge.4	4vCPUs	190.6	Intel SkyLake 6151 3.90Hz	113 0665	selling		¥492.00/9	
55.10rge.4	4vCPUs	1908	INNE Cascade Lake 2.60Hz	0.35/2 0985	285998		¥431,20/7	
s2.siarge.4	4vCPUs	1508	Intel SkyLake 6161 2.2GHz	0.4.11.5 Galls	1575995		¥431.29/9	
s2.starps.4	4vCPUs	1938	Intel E5-2880V4 2-40Hz	0.4/1.5 GBIN	15/5975		R105.5019	
01 c1 64 64 63 64 64 64 64 64 64 64 64 64 64 64 64 64	otarge 4 otarge 4 otarge 4 otarge 4 otarge 4	stage 4 4/CFUs stage 4 4/CFUs		stopp 4 4/07k 1008 Het Concost Line 1.10er stopp 4 4/07k 1008 Het Disclet 1013.00er stopp 4 4/07k 1008 Het Concost Line 1.10er stopp 4 4/07k 1008 Het Concost Line 1.10er stopp 4 4/07k 1008 Het Concost Line 1.10er stopp 4 4/07k 1008 Het Concost Line 1.20er	Appl APpl UBA MacCamanatistics 111 Admin Appl APpl MacCamanatistics 111 Admin 112 Admin Appl APpl MacCamanatistics 111 Admin 112 Admin Appl APpl MacCamanatistics 112 Admin 112 Admin Appl APpl MacCamanatistics 112 Admin 112 Admin Appl APpl MacCamanatistics 112 Admin 112 Admin	At/Dia At/Dia<	Appl APPN VDB MedDamaskak LBg 2.11.028 APPN APPN AppA APDN VDB MedDagAdV11306 1.10.00 50.797 - AppA APDN VDB MedDagAdV11306 0.17.005 57.797 - AppA APDN VDB MedDagAdV1206 0.17.005 10.797 - AppA APDN VDB MedDagDA144 10.100 10.797 -	Appl APDA NAGA NAGADARALALISIA 2.14 (200) 10.0701 APRA Appl APDA NDB MEDBARALALISIA 2.14 (200) 10.0701 ADDA APRA APPA APRA APRA APRA APPA APPA

图 3-17 购买云服务器 3

				8847.688	ARANA WEALAN ADALAS	28-9550-5079-71895	880699. RUTR					
*	\$25 C 0 000					RR						
=	< 的复数性素服务	s								201		
0	() BRIER 6) Refer										
0	Re	12E(172 16.0.016) 12E(1800016) 25	• C subset:	(172.19.98.0/19)	• C mecilitrate	• 13186.4cP	BBINOT ()					
NA.	1.85+	(i) #12-041+ SERVIS	20 1 10/10-0-									
0 0 0 0	221	Ever meeterverstählster sta managers statistik i Kongen meter everstählt i Kongen Automatiktik i Kongen Automatiktik i Kongen	00-4603-8438-0077874128681 2016-010-011, 10:7-018748343 1 (Deve 5594828) - 5556880 20	o • C #184241 Intel. (Wedaws208888) force	D. Billiosofiit							
Θ		05029	8.7u%	11.05	1988ALI ()	大型	anu 🔿	No.				
&			1	ALM .	TOP: 1194	1Pv4	0.0.0.00	VPN				
Θ			1	718	TOP. 22	IP14	22					
			1	A3P	25	1946	Sys-WebServer					œ
			1	738	TOP: 443	IPv4	28					0
		CAP-LINE CALVE	1	ni#	IOMP: Add	194	0.1.1.00					
		A 1777 C 4814	0.8797									
	RFR - 1	+ * 100 •	8:884 ¥275.50 9/25/77.887 #34	ene ()					Ŀ	-9	T-9.098	

图 3-18 购买云服务器 4

		CONTRACTOR CONTACTOR	- Weight - Section - / Inviews						^
	◎ 2000 日本 1 ○ 2000								8
Ξ	< NORMEZ NOR	52						ana 🖉 🖬	
۵	() BARE (2	() FINER () INVER							
۲	590460	ect-eee5 2/P#S							
۲		nvenimmer sunemmeridestankomes.							
m	10.2								
0									
0	2074	And Add Cograde							
0	R#8	niot							
4	**	andri medelilasromatici							
0		1000-0000 69							
\$	MAX.0255	2012/2014/2011 49							
e	-								
	289	estecia. Interaction, parametermenter,							0
		20155X (19824) \$2755X (1)							٢
	58976858	vautoelif							
	安徽合作法常容量	- 200 + 06 *							
		27.96还加州上建立市场库空间不小于来台层的建立用。							
	NFB - 1	+ 6 108 • BERNY ¥315.50					2-9	T-P BORD	

2. 购买SFS Turbo存储

用于搭建文件系统,服务于芯片设计环节的仿真业务、软件安装、工艺库、IP库 等数据存储。

图 3-19 购买 SFS Turbo 存储 1



图 3-20 购买 SFS Turbo 存储 2

	华为 云 1 15100			93	Q	8910	928	IØ 2	e finita	92	334686	中党 (昭和)	bkunyun	۲
Ξ		< 创建文件系统 ①												
		 КАКАСНАЙК Ф НИКС 	BE:rs Extended BE:rs • 2010:rs:rs:rs:rs:rs:rs:rs:rs:rs:rs:rs:rs:rs:	ABLIGHANDA CUBARAMA TOTAL TARAS REAL RE	Rectar.	× 4	社販売 1008(0) 1-2034 1-2034 1-2034 1-2034 1-2034 1-2034 1-2034 1-2034 1-2034 1-2034 1-2034 1-2034 1-2034 1-2034 1-2034 () 1-	参加版 5 775 775 775 775 7 7 7 7 7 7 7 7 7 7	4# 22					
		* 記載(69)	500 +	intia, Takassi hokaita.										0 B
		01981 RESH ¥200.00 #95% Religionstyr, 3	NPS *						I	020910				

3. 购买云堡垒机

云堡垒机提供云计算安全管控的系统和组件,包含部门、用户、资源、策略、运 维、审计等功能模块,集单点登录、统一资产管理、多终端访问协议、文件传 输、会话协同等功能于一体。通过统一运维登录入口,基于协议正向代理技术和 远程访问隔离技术,实现对服务器、云主机、数据库、应用系统等云上资源的集 中管理和运维审计。

图 3-21 购买云堡垒机 1

				54+	Л ЕНЦЕНТИ Р. ПЕН228 . 1	adnu oʻrazi qishi shari Taqis	880-80A #01718			×
<u>*</u>	#25 ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆									9 9
=	EXEN.		云望坐机 ①						BERN I NEAD REE	201
	ERINE							采州名称	• 880.7887 Q	C
۲	*24	ø	\$912.0	可能分包	80908	41.81.P1842	985P	计供信式	85	- 1
10 0	9829 03950	e e				<u>_</u>				
۵						服元券修数据				
ø										
4										
۲										
8										
e										
										0
										ļ

图 3-22 购买云堡垒机 2

											() 85	NIT FOR	sisin	នទ. ៧៥	***	1. igen	au ea	1018-10	的小	nan Ai	Dession	nikan.	NG LEFT OF	8							×
	华为云																														
Ξ						19	(.	NURS																							Т
0																															
\odot						R	002			29.91	ISH																				
۲																															
.03						11	100			044	ม	Ø																			
0																															
\odot							1963M			9 SR-7	**																				
٢							14-50																								
\odot										CP-104P	-																				
4							198912			गमर	2	时用 包	59	10	E۶	13	明26		22	RB4EN	NOTION CONTRACT										
©																															
&						*\$	NER			EH-9508																					
٢						85	20.62		身) 見)	(A)(王)(昭和 (法律和天)(122 M 18 3P		2281	787/18																	
						* 12	estas.	[0.0	11日日				100 通知 100 印油酒	£			200	8.* ₽			50 50	200 gene								6
									1	000 HEA	R			2,000 HE	产量			5.00	0 <u>87</u> 4%	ł											8
								C	0	NRRON Sali	928 928	erorritadia E calificati a	0.10175 0.578-0	1907 1904 1904 1904	取 (井38) 毎日)	\$P) 255	1003.00	15 40 90	109												
					E	ini.	¥1,90	00.00		~																	0,235/2				

4. 购买VPN网关

VPN网关是虚拟私有云中建立的出口网关设备,通过VPN网关可建立虚拟私有云和企业数据中心或其它区域VPC之间的安全可靠的加密通信。

VPN网关需要与用户本地数据中心的对端网关配合使用,一个本地数据中心绑定 一个对端网关,一个虚拟私有云绑定一个VPN网关。VPN支持点到点或点到多点 连接,所以,VPN网关与对端网关为一对一或一对多的关系。

图 3-23 购买 VPN 网关

*	华为云 1988	0.7%					88	Q 8010	958 IQ 24	FRIR RE	79 GBU415	\$ (184) I	skuryun	B	
=	用462464		VPN网关 ①				57 (DE 104)								
60 63	en.		0 2018 414202 1114202 1114202 0 420192011 22019202 201010 1114202											×	
m ©	171082													×	
0	1710528		#52/08											×	
8 6	2.69	•		50000007 55800.00000000			BECONSTRUCTED DUCIDENT MEDIATION CONTENT DUCIDA INTERNAL AND								
Φ	820		・ YMEBH2075編集中台 ・ ・												
0	945570P	1													
			80	板岩	dSEAA	72	RXP	0.011	已的建筑1/21/白绿数	80 H8R4	w	80	Q	C	
			V vprgu-5558	0 E#	an a	Pec	123.60.236.129	atimilia-m 300 Monja	t/	1212 2022/06/01 14:00	k47 (5)	-		9	
														-	
														6	
suppor	the available on	i Anna faoir	hum tonic 0187565705 htm												

3.1.3 部署北鲲云平台服务

步骤1 配置北鲲云平台部署服务器

1. 配置节点域名解析 3台服务器都需要

vi /etc/hosts 172.17.3.11 deploy 172.17.3.12 accountslave 172.17.3.13 authslave

2. 配置部署服务器间免密登录

ssh-keygen -f ~/.ssh/id_rsa -t rsa -N " cat /root/.ssh/id_rsa.pub >> /root/.ssh/authorized_keys cd ~/.ssh ssh-copy-id accountslave scp ~/.ssh/id_rsa accountslave:/root/.ssh

关闭防火墙和selinux #关闭防火墙 需要注意要在安装docker之前就关闭好 否则关闭后要重启docker systemctl disable firewalld --now #禁用selinux 需要重启才能生效 sed -i "s/SELINUX=enforcing/SELINUX=disabled/g" /etc/sysconfig/selinux sed -i "s/SELINUX=enforcing/SELINUX=disabled/g" /etc/selinux/config

4. 安装必备软件例如docker

yum install -y docker-ce-19.03.9-3.el7.x86_64 docker-ce-cli-19.03.9-3.el7.x86_64 containerd.io-1.2.6-3.3.el7.x86_64 systemctl enable docker --now curl -o /usr/local/bin/docker-compose -L https://get.daocloud.io/docker/compose/releases/download/ 1.27.4/docker-compose-`uname -s`-`uname -m` chmod +x /usr/local/bin/docker-compose

5. 部署节点安装gnome桌面和VNC服务方便堡垒机可视化连接 yum install -y tigervnc-server xorg-x11-fonts-Type1 xrdp

yum groupinstall -y "GNOME Desktop" "Graphical Administration Tools" yum install -y mesa-libGL yum install -y fwupdate systemctl enable gdm --now

步骤2 创建docker swarm集群

初始化docker swarm集群 deploy节点执行 初始化swarm集群 deploy docker swarm init

2. 添加节点到docker swarm集群并建立必须目录

以下accountslave节点执行

docker swarm join --token SWMTKN-1-1rmkhkehf6ciu45803kg2ixu48jvbl7rzbdsbyqe3lc4dqxd6d-14d7kfs2ei4lzit4h3hgczuu3 172.17.3.11:2377 mkdir -p /data/db/account /data/logs/nginx /data/zk/zoo/data /data/zk/zoo/datalog /data/logs/zoo / data/logs/kafka chmod -R 777 /data/logs/nginx 以下authslave节点执行 docker swarm join --token SWMTKN-1-1rmkhkehf6ciu45803kg2ixu48jvbl7rzbdsbyqe3lc4dqxd6d-14d7kfs2ei4lzit4h3hgczuu3 172.17.3.11:2377 mkdir -p /data/db/auth /data/logs/nginx /data/logs/openresty /etc/openIdap/cacerts chmod -R 777 /data/logs/nginx

3. 给docker node打上标签

在主节点打标签

docker node ls docker node update --label-add master=true deploy docker node update --label-add account=true accountslave docker node update --label-add auth=true authslave

步骤3 搭建本地docker镜像仓库

- 创建本地仓库目录 部署本地docker registry 并上传cloudam镜像 cd /etc/cloudam docker pull docker.io/library/registry:latest docker tag docker.io/library/registry:latest docker-registry
- 2. 使用yml文件启动docker服务 mkdir -p /etc/cloudam/registry cp ./config/deploy/registry.yml ./ docker-compose -f registry.yml up -d

步骤4 启动docker集群

- 解压docker镜像压缩文件并推送至本地docker镜像仓库 tar -zxvf image_cloud.tar.gz ls ./image/local/*.tar | xargs -n1 docker load -i docker images | grep latest | grep -v deploy | awk '{print "docker tag " \$1 ":latest deploy:5000/" \$1 ":latest;docker push deploy:5000/" \$1 ":latest"}' | xargs -i sh -c '{}'
- 2. 按说明配置.env文件内容 vi /etc/cloudam/.env
- 3. 使用yml文件启动docker服务 env \$(cat /etc/cloudam/.env | grep ^[A-Z] | xargs) docker stack deploy --with-registry-auth --composefile \$cluster_file cloudam

步骤5 验证服务是否正常运行

- 1. 部署后检查是否成功 cd /etc/cloudam cp ./config/deploy/step4_check_post.sh ./ bash step4_check_post.sh
- 2. 登录北鲲云控制台

图 3-24 登录北鲲云控制台



3. 登录北鲲云管理后台

图 3-25 登录北鲲云管理后台



----结束

3.2 配置 LDAP 服务

3.2.1 部署 ldap 服务端

- 配置yml文件ldap用户密码等信息 vi ldap.yml
- 2. 使用yml文件启动ldap docker服务 docker-compose -f ldap.yml up -d

3.2.2 配置 ldap 主从

1. 开启syncprov模块

cat << EOF > mod_syncprov.ldif dn: cn=module{0},cn=config changetype: modify add: olcModuleLoad olcModuleload: syncprov.la EOF DOCKER_LDAP_ID=`docker ps |grep openIdap |awk '{print \$1}'` docker cp mod_syncprov.ldif \${DOCKER_LDAP_ID}:/ docker exec \${DOCKER_LDAP_ID} ldapadd -Y EXTERNAL -H ldapi:/// -f /mod_syncprov.ldif

2. 生成 syncprov 配置

cat << EOF > syncprov.ldif dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config objectClass: olcOverlayConfig olcOverlay: syncprov olcSpCheckpoint: 100 10 olcSpSessionLog: 100 EOF docker cp syncprov.ldif \${DOCKER_LDAP_ID}:/ docker exec \${DOCKER_LDAP_ID} ldapadd -Y EXTERNAL -H ldapi:/// -f /syncprov.ldif

3. 开启同步

cat << EOF > syncrepl.ldif dn: olcDatabase={1}mdb,cn=config changetype: modify add: olcSyncRepl olcSyncRepl: rid=002 provider=ldap://openldap-master bindmethod=simple binddn="cn=admin,dc=xxx,dc=xxx" credentials=xxxx searchbase="dc=xxx,dc=xxx" scope=sub schemachecking=on type=refreshAndPersist retry="5 5 600 +" attrs="*,+" EOF DOCKER_LDAP_ID=`docker ps |grep openldap |awk '{print \$1}'` docker cp syncrepl.ldif \${DOCKER_LDAP_ID}:/ docker exec \${DOCKER_LDAP_ID} ldapadd -Y EXTERNAL -H ldapi:/// -f /syncrepl.ldif

3.2.3 配置 ldap 客户端

1. 在目标主机安装ldap客户端

yum install -y nss-pam-ldapd openldap-clients

2. 配置系统文件

/bin/cp -f /tmp/packer/config/ldap/centos/nslcd.conf /etc/nslcd.conf /bin/cp -f /tmp/packer/config/ldap/centos/nsswitch.conf /etc/nsswitch.conf /bin/cp -f /tmp/packer/config/ldap/centos/authconfig /etc/sysconfig/authconfig /bin/cp -f /tmp/packer/config/ldap/centos/password-auth /etc/pam.d/password-auth /bin/cp -f /tmp/packer/config/ldap/centos/system-auth /etc/pam.d/system-auth

- 3. 配置客户端连接配置nslcd.conf vi /etc/nslcd.conf
- 启动客户端服务 sudo chmod 600 /etc/nslcd.conf sudo systemctl disable nslcd
- 5. 查看部署状态 docker service ls

图 3-26 查看部署状态

[root@deploy ~]	# docker service ls				
ID	NAME	MODE	REPLICAS	IMAGE S	PORTS
qzim3koa2xwk	cloudam_account-mongodb	replicated 8		deploy:5000/mongodb:onprem	
5prw0apmy3wi	<pre>cloudam_account-service</pre>	replicated		deploy:5000/account-service:onprem	
mcrno8iuwk54	cloudam_auth-mongodb	replicated		deploy:5000/mongodb:onprem	
wbw6zocict49	<pre>cloudam_auth-service</pre>	replicated		deploy:5000/auth-service:onprem	
o42czptlca04	<pre>cloudam_c3-ce-app</pre>	replicated		deploy:5000/c3-ce-app:onprem	
3w82nw7bvjya	cloudam_c3-ceadmin-app	replicated		deploy:5000/c3-ceadmin-app:onprem	
m1as3m7pd1r4	cloudam_c3-oc-app	replicated		deploy:5000/c3-oc-app:onprem	
cr75rv393bno	cloudam_cloudam-fileserver	replicated		deploy:5000/fileserver:onprem	*:443->443/tcp, *:108
tcp, *:6677->66	77/tcp, *:8888->8888/tcp, *:9000->	9000/tcp, *:9090->9	090/tcp, *:9975->	9975/tcp	
s9zxdn61z03k	cloudam_cloudam-web	replicated		deploy:5000/intelligroup-frontend:onprem	*:80->80/tcp
z417ve3v82j0	cloudam_cloudam-web-onprem	replicated		deploy:5000/intelligroup-frontend-onprem:onprem	*:10003->10003/tcp
∥o3rbru4pi0j8	cloudam_config	replicated		deploy:5000/config:onprem	
b9qbcgqsfrwf	cloudam_dataset-app	replicated		deploy:5000/dataset-app;onprem	
h2g8452gfb28	cloudam_grafana	replicated		deploy:5000/grafana:onprem	*:3000->3000/tcp
yu7hukh1eyas	cloudam_im-app	replicated 🔬 👌		deploy:5000/im-app:onprem	
vyqzjkivbhyw	cloudam_intelligroup-mongodb	replicated 📈		deploy:5000/mongodb:onprem	
baiau1rq6mak	cloudam_kafka	replicated 🖉 🔗		deploy:5000/kafka:onprem	
uagv3cubieii	cloudam message-service	replicated	2/2	deploy:5000/message-service:onprem	
pg422ajdcgk5	cloudam_openldap-master	replicated		deploy:5000/open1dap:onprem	
z3py90b5rz1p	cloudam_openldap-slave	replicated	1/1	deploy:5000/open1dap:onprem	*:389->389/tcp, *:636
พฤชิกฎดชิงบรสง	<pre>cloudam_phpldapadmin</pre>	replicated		deploy:5000/phpldapadmin:onprem	*:8080->80/tcp
db7unm2buv1w	cloudam_prometheus	replicated		deploy:5000/prometheus:onprem	*:9091->9090/tcp
hyinyhflwe7c	cloudam_registry	replicated		deploy:5000/cloudam-registry:onprem	
ubrogu31zvzd	cloudam_zoo	replicated		deploy:5000/zookeeper:onprem	
[root@deploy ~]	#				



表 4-1 修订记录

发布日期	修订记录
2023-03-03	第一次正式发布。