主机相关 存储配置 **黄磊** 2018-03-19 发表

H3C FlexStorage P5000存储是一款横向扩展存储平台,专为满足虚拟化环境不断变化的需求而设计。 支持iSCSI (Internet Small Computer System Interface 互联网小型计算机系统接口)存储协议,能够 在IP协议上层运行SCSI指令,从而使网络上的主机系统(Initiator端)通过IP网络就能够访问到存储资 源(Target端)。在遇到Windows系统主机挂载FlexStorage P5730存储卷失败时,可以参考本案例完 成初步的问题定位。

1、iSCSI发起程序

iSCSI发起程序是Windows系统下的一款连接iSCIS Target也就是iSCSI存储的客户端软件,现在已经内置于如Windows 2008等系统中,如下图。如果没有请先正确安装iSCSI发起程序。

iSCSI 发起程序 属性	
目标 发现 收藏的目标 卷和设备 RADIUS 配置 快速连接 差更分和目标并使用某术连接器受到目标,请键入该目标	元的 TP +10+11-或 DNS 名
祝 然后单击"快速连接"。	快速连接 (Q)
已发现的目标 (G)	刷新 (8)
名称	状态
】 若要使用高级选项进行连接,请选择目标,然后单击 "连接"。	连接 (M)
若要完全断开某个目标的连接,请选择该目标,然后单 击"断开连接"。	断开连接 (0)
对于目标属性,包括会话的配置,请选择该目标并单击 "属性"。	属性(P)
对于配置与目标关联的设备,请选择该目标,然后单击 "设备"。	设备(V)
有关基本 iSCSI 连接和目标的详细信息	
确定	取消 应用(A)

iSCSI发起程序的运行还需要依赖"Microsoft iSCSI Initiator Service"服务,正确安装iSCSI发起程序后,并检查该服务是否正常启动,如果没有启动,请在Windows"服务"中启动该服务。

服务						
◎ 服务						
Microsoft iSCSI Initiator Service	名称	描述	状态	启动类型	登录为	^
	🔍 KtmRm for Distributed Transaction Co	协调		手动	网络服务	
	🔍 Link-Layer Topology Discovery Mapper	创建		手动	本地服务	
里后动此服务	🔍 Microsoft .NET Framework NGEN v2.0	Micr		禁用	本地系统	
	🔍 Microsoft .NET Framework NGEN v2.0	Micr		禁用	本地系统	
描述:	🔍 Microsoft .NET Framework NGEN v4.0	Micr		自动(延迟…	本地系统	
管理从这台计算机到远程 iSCSI 目标	🔍 Microsoft .NET Framework NGEN v4.0	Micr		自动(延迟	本地系统	
设备的 Internet SCSI (iSCSI)会话。	🔍 Microsoft Fibre Channel Platform Regi	注册		手动	本地服务	
法登录或访问 iSCSI 目标设备。如果	🔍 Microsoft iSCSI Initiator Service	管理	已启动	自动	本地系统	
该服务已禁用,则所有显式依赖于该	🔍 Microsoft Software Shadow Copy Prov	管理…		手动	本地系统	=
服务的服务将不会启动。	🔍 Mozilla Maintenance Service	Moz		手动	本地系统	
	🔍 Multimedia Class Scheduler	基于	已启动	手动	本地系统	
	🔍 Net.Msmq Listener Adapter	Rece		禁用	网络服务	
	🔍 Net.Pipe Listener Adapter	Rece		禁用	本地服务	
	🔍 Net.Tcp Listener Adapter	Rece		禁用	本地服务	
	🔍 Net.Tcp Port Sharing Service	Prov		禁用	本地服务	
	NET_INSPECTION_GBGSrv		已启动	自动	本地系统	
	NET_INSPECTION_LnsSrv		已启动	自动	本地系统	
	NET_INSPECTION_MySQL		已启动	自动	本地系统	
	NET_INSPECTION_Tomcat7	Ара	已启动	自动(延迟	本地系统	
	🔍 Netlogon	为用		手动	本地系统	

2、是否发现Target

Windows已发现的存储Target会显示在iSCSI发起程序的"目标"菜单中,已正常挂载的存储Target状态显示为"已连接"。

	_
iSCSI 发起程序 属性	X
目标 发现 收藏的目标 卷和设备 RADIUS 配罟	
~快速连接	
若要发现目标并使用基本连接登录到目标,请键入该目标	內 IP 地址或 DNS 名
称,然后甲击"快速连接"。	
	「地志」を按い
目标(1):	伏迷连接 (1)
一已发现的目标 (G)	
	刷新(R)
名称	状态
ign. 2003-10. com. lefthandnetworks: group1:172:	已连接
着要使用高级选项进行连接,请选择目标,然后单击 "连按"。	
石安元王町开来个日标的连接,请选择该日标,然后早 击"断开连接"。	断开连接 (D)
对于中兵届州,有任今迁的副罢,违法探读中兵并并主	
"属性"。	馬性 (P)
	反面(9)
有关基本 iSCSI 连接和目标的详细信息	
确定	取消 应用(A)

已发现的Target状态显示为"不活动"时,请选中对应的Target后点击"连接"按钮。

iSCSI 发起程序 属性	۲.
目标 发现 收藏的目标 卷和设备 RADIUS 配置	_
快速连接 若要发现目标并使用基本连接登录到目标,请键入该目标的 IP 地址或 DNS 名 称,然后单击"快速连接"。	
目标(I): 快速连接(Q)	
已发现的目标 (G) 刷新 (B)	
名称	
ign.2003-10.com.lefthandnetworks;group1:172: 不活动	
若要使用高级选项进行连接,请选择目标,然后单击	
若要完全断开某个目标的连接,请选择该目标,然后单 断开连接 (D) 击"断开连接"。	
对于目标属性,包括会话的酒器,请选择该目标并单击	
对于配置与目标关联的设备,请选择该目标,然后单击	
有关基本 iSCSI 连接和目标的详细信息	
确定 取消 应用 (A)	

推荐勾选"将此链接添加到收藏目标列表",便于以后系统启动时自动连接Target。

连接到目标	×
目标名: ign.2003-10.com.lefthandnetworks:group1:172:lun1	
浴此连接添加到收藏目标列表。 该操作会在每次计算机重新启动时使系统自动尝试还原连接。	
□ 启用多路径 (C)	
高级 (ស) 确定 耳	测

3、网络是否可达

由于iSCSI协议承载在IP上层,使用TCP 3260端口,需要确保主机系统到存储提供业务的虚拟IP地址 之间网络可达。可以通过ping等工具测试网络连通性。

存储的虚拟IP地址可以通过CMC (Centralized Management Console) 登陆存储管理组,选中对应的集群后,点击"iSCSI"后查看,如下图。

🚋 HP StoreVirtual Centralized Man	agement Console			
文件(巴▼ 査供(□▼ 任务(□▼ 帮助)	11 - ① 校査升级件 💷 査看通知			
	译细信意 使用摘要 卷使用率 系统使用 点拟 P 为获得希情功能或负钱学贩的 SCSI 访问, 虚拟	8 运程快振 会话 SCSI 医射视图	_	2
- 2 管理 は古	库拟IP	子网推码	存储系统	
○ 量 20000円 一层型 性能系改善 中小局型 作能系改善 中小局型 作能系统(1) ⊕-高 第(4)総技能(0)				

4、排查网络问题

检查网络配置主要包括:

1) 检查存储虚拟IP地址和承载业务的网卡IP地址为同网段。存储节点网卡地址可以在存储节点"网络" 中的"TCP/IP"菜单下查看。

¥(D ● 査供(0) ● 任务(D ● 帮助) GAN 状态页 入口	 10 ・ © 検査判 10 ・ 10 ・ 	+级件 ■ 查看# P TCP 状态	9知 降由 通信						
— [@] Σ ⁺ 配置摘要 → 器 group1									3
中	14	lame I	Description	MAC	Mode	IP Address	Subnet Mask	Gateway	Туре
▲ ▲ 电子邮件	FlexLO	M:Port1 Bro	adcom Corpo	28:80:23:A1:24:AC	static	192.168.149.11	255.255.255.0	0.0.0.0	NIC
SNMP	FlexLO	M:Port2 Bro	adcom Corpo	28:80:23:A1:24:AD	disabled	0.0.0	0.0.0	0.0.0.0	NIC
由一個 服务部(5)	FlexLO	M:Port3 Bro	adcom Corpo	28:80:23:A1:24:AE	disabled	0.0.0.0	0.0.0.0	0.0.0.0	NIC
B.44	FlexLO	M:Port4 Bro	adcom Corpo	28:80:23:A1:24:AF	static	192.168.127.200	255.255.255.0	0.0.0.0	NIC
E- cluster1	NICSId	2:Port1 Emu	ulex Corporati	D0:BF:9C:C0:D1:60	disabled	0.0.0	0.0.0.0	0.0.0.0	NIC
	NICSId	2:Port2 Emu	ulex Corporati	D0:BF:9C:C0:D1:64	disabled	0.0.0.0	0.0.0.0	0.0.0.0	NIC
日本 日本 日本 日 日 日 日 日 日 日 日 日 日 日 日 日	TCP/IP 4	F& -							

2) 检查是否有到主机系统地址的路由信息,并且"设备"为业务网卡。如果路由信息不正确,可以点击"路由任务"编辑路由信息。

💼 HP StoreVirtual Centralized Manag	gement Console					- • ×
文件(巴▼ 査核(□▼ 任务(□▼ 帮助(田)	• ① 检查升级件 🛄 查看通	im .				
	▲ TCP/IP TCP 状态 路由信息(按照序)	路由 通信				2
	设备	网络	网关	网络掩码	标志	
→▲区 电子邮件	FlexLOM:Port1	192.168.149.0	0.0.0.0	255.255.255.0	U	
SNMP	FlexLOM:Port4	192.168.127.0	0.0.0.0	255.255.255.0	U	
□ ■ 取力和(5)	FlexLOM:Port1	169.254.0.0	0.0.0.0	255.255.0.0	U	
	FlexLOM:Port4	169.254.0.0	0.0.0.0	255.255.0.0	U	
	Red free					
	10 0 1 7 7					

3) 检查主机系统到存储之间的网络设备配置,如果有经过安全设备,确保安全策略中放行存储虚拟IP 地址的TCP 3260端口。

5、检查iSCSI接口

H3C FlexStorage P5000存储上有不同的接口角色定义,其中iSCSI接口定义为对外提供iSCSI连接服务的接口角色,需要将对外提供业务网卡配置成iSCSI接口后,存储通过虚拟IP地址才能提供iSCSI连接服务。



6、iSCSI Name配置

iSCSI的识别机制是基于名字的,这个名字一般被称为iSCSI Name。建立连接时, Initiator端发起一个连接请求, Target端收到请求后,确认Initiator端发起的请求中所携带的iSCSI Name是否与Target端绑

定的iSCSI Name一致。如果一致才能建立iSCSI通信连接。iqn规范定义的发起程序名称格式为"iqn.do maindate. reverse.domain.name:optional name",例如: iqn.2017-12.com.h3c:server1。 在iSCSI发起程序的"配置"菜单中检查发起程序名称配置是否规范。

iSCSI 发起程序 雇性
目标 发现 收藏的目标 卷和设备 RADIUS 配置
此处的配置设置是全局设置,会影响以后使用该发起程序进行的任何连接。
任何现有连接都可以继续工作,但如果重新启动系统,或发起程序试图重新连 接到目标,则这些连接可能会失败。
连接到目标时,高级连接功能允许对特定连接进行特别控制。
发起程序名称:
ign. 2017-12. com. h3c:server1
若要修改发起程序名称,请单击"更改"。 更改 00
若要將发起程序 CHAP 机密设置为与相互 CHAP 一起使 CHAP (P) 用,请单击"CHAP"。
若要设置发起程序的 IPsec 隧道模式地址,请单击 IPsec(I) "IPsec"。
若要生成系统中所有已连接的目标和设备的报告,请单据告(R) 报告(C)
有关配需的详细信息
确定 取消 应用 (A)

通过CMC登陆存储管理组后,选择"服务器",对应服务器配置中的"发起程序节点名称"和主机系统ISC SI发起程序中配置的"发起程序名称"需要完全一致。

体(D・ 査氏(0)・ 任务(D・ 帮助) ▲ SAN 状态页 → 2) 入门 → 2) デ 配置病愛 → 2) 雪 group1 由 ▲ (E) 単件	 ◎ 检查升级件 ● 3 详细信息 ● 映射视 视出 服务器和服务	2看通知 图 發群集 ▼										?
	(a) (k) an(J)				1000				1	4.45	05.200	
127.65	夕款	60 N 55	拉油田路	1000	「おしていた」	CHAD 夕谷	6.69	24.15	ww	7Cer:	919 1010	使来
-Lg 127.66	- 127.65	06.99	135/01/06	本部書 CHAR	ion 1993.08 org debias 01 de7e90chde	CHAP 4192	三 山田	和品 木分	****	**	790	14.85
	- 127.66			不定形 CHAP	ion 2017-05 com h3c 01 cuk01		已由用	果分				
Server1	- 180			不需要 CHAP	ion 1993 08 org debias 01 cuknode		已由用	果分				
	- E cvk1		192.16	不需要 CHAP	ign 2015-04.com.h3c:cvk1		已启用	果分				
	- a server1	_		不需要 CHAP	ign.2017-12.com.h3c:server1		已启用	*//			_	_
 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	任务。											

如果不一致,请编辑服务器在"发起程序节点名称"处更改。

🚾 编辑服务器		x
		?
名称:	server1	
说明:		
控制服务器 IP 地址:		
	<u>我使用什么 IP 地址?</u>	
ISCSI 安全性	- 24	
◆お知改またか:	17	_
及延程升中总名	№ [Iqn.2017-12.com.n3c:server] <u>如何查找我的发起程序节点名称?</u>	_
✔ 启用负载平衡	(关于兼容发起程序的信息)	
在不兼容的发起程序_ 要正常运行负载平衡;	上启用负载平衡可能会影响卷的可用性。 · 需要配置群集的虚拟 IP。	
身份验证		
 不需要 CHAP 		
○ 需要 CHAP		
CHAP 名称:		
目标机密:		
发起程序机密	:	
确定	取首	

7、是否启用认证

iSCSI可选配CHAP认证,细分为Initiator认证和Target认证。Initiator 认证要求在Initiator尝试连接到一个Target的时候,Initator需要提供一个密钥给Target供Target进行认证。Target 认证要求在Initiator尝试连接到一个Target的时候,Target需要提供一个密钥给Initiator供Initiator进行认证。

Initiator认证可以在没有Target 认证的时候应用,这种只要求Target验证Initiator的CHAP认证也称为单向认证;Target认证则要求Initiator认证被同时应用才可以,也就是说,Initiator和Target需要相互认证,这种认证被称为相互认证。

存储上是否配置启用认证可以在CMC的"服务器"配置菜单中查看"iSCSI模式"确认。



8、认证方式和密钥

如果启用CHAP认证,需要在存储设备侧和主机系统侧检查是配置单向认证还是双向认证,并且两端对应的认证密钥需要一致。 CHAP认证密钥长度要求必须长于12位。

1) 单向认证

存储设备侧CHAP认证在新建或者编辑服务器菜单中配置,如下图,配置。单向认证需要配置"目标机密"。

🚾 编辑服务器	
	?
名称:	server1
说明:	
控制服务器 IP 地址:	
1	<u> 线使用什么 IP 地址?</u>
- iSCSI 安全性	
✓ 允许通过 iSCSI 访问	1
发起程序节点名称	iqn.2017-12.com.h3c:server1
一点日本地近年	如何查找我的发起程序节点名称?
✓ 后用贝软半衡 在不兼容的发起程序上点	(关于兼容发起程序的信息) 当用负载平衡可能会影响卷的可用性。
要正常运行负载平衡,計	需要配置群集的虚拟 IP。
身份短進	
O 不需要 CHAP	
③ 需要 CHAP	
CHAP 名称:	Auther-server1
目标机密:	
发起程序机密:	
确定	(取) 御

主机系统侧,需要在iSCSI发起程序中添加目标门户和连到接到目标时,进入"高级"选项下配置。

, 31 <u>/</u> Q	起程序 属性			Σ
目标	发现 收薪	勤目标 卷和设	备 RADIVS 配置	
目标	;门户			
系统	流 将在下列门户	上查找目标(T):		刷新(E)
地址	ht.	端口	适配器	IP 地址
若要	厚添加目标门户	,请单击"发现门	7户"。	发现门户(0)
若	· · · · · · · ·			
ŧ	发现目标门户			
	输入要添加门]户的 IP 地址或	DWS 名称和端口号	•
−iS. iž	芜重面改白标	门白发现的脾镜后	沿罢,诸单去" 三红	3" 坎坷。
4	132321/1410	1 1/ 200404040404040404	«ш'нтч п»	× 1×11 ·
	IP 地址或 D	rs 名称(I):) 第111章	过值为 3260。)(P)
	192.168.149	1	3260	(WIE/5 02000) (1)
Ц		-		
若	[高级(A)	J	确定(0)) 取消(C)
若然	50000 元(130 05年) 日本"删除"	- 加力容/ 阴辺す ∘	キエノコロリル図力 谷り	()))))))))))))))))))))))))))))))))))))
<u>有</u>	<u>关发现和 iSNS</u>	的详细信息		



勾选"启用CHAP登陆",配置"目标机密",和存储设备侧密钥配置一致。

高级	3.设置	? 💌
常	规 IPsec	
	连接方式	
	本地适配器(L):	默认值
	发起程序 IP(I):	默认值
	目标门户 IP(T):	
	- CRC/校验和	
	■ 数据摘要 (0)	□ 标题摘要 (H)
	CHAP 登录信息 通过在目标和发起程序 若要使用,请指定在目 其他名称,否则名称将	之间提供身份验证,CHAP 有助于确保连接安全。 标上为该发起程序配置的相同名称和 CHAP 机密。除非指定 默认为系统的发起程序名称。
	日标机密(S):	••••••
	 □ 执行相互身份验证(若要使用相互 CHAP,) □ 使用 RADIUS 来生成 □ 使用 RADIUS 求目标 	P) 青在"配置"页上指定发起程序机密或使用 RADIUS。 成用户身份验证凭据 (U) 际凭据进行身份验证 (R)
		确定 取消 应用 (A)

2) 双向认证

存储设备侧在新建或者编辑服务器菜单中配置"目标机密"和"发起程序机密"。

🔤 编辑服务器	—
	?
名称:	server1
说明:	
控制服务器 IP 地址:	
	<u>我使用什么 IP 地址?</u>
iSCSI 安全性	
✔ 允许通过 iSCSI 访	й
发起程序节点名称	1991-05.com.microsoft:windows-f2a40tv 如何查找我的发起程序节点名称?
✔ 启用负载平衡 在不兼容的发起程序」 要正常运行负载平衡。	(关于兼容发起程序的信息) 比応用负载平衡可能会影响卷的可用性。 需要配置群集的虚拟 IP。
○ 不需要 CHAP	
● 需要 CHAP	
CHAP 名称:	Auth-server1
目标机密:	
发起程序机密	:
确定	取消

主机系统侧"发起程序机密"在iSCSI发起程序的"配置"菜单中点"CHAP"按钮后配置。

iSCSI 发起程序 属性	×
目标 发现 收藏的目标 卷和设备 RADIUS 配置	
此处的配置设置是全局设置,会影响以后使用该发起程序进行的任何连接。	
任何现有连接都可以继续工作,但如果重新启动系统,或发起程序试图重新连接到目标,则这些连接可能会失败。	
连接到目标时,高级连接功能允许对特定连接进行特别控制。	
发起程序名称:	
1qn. 1351-03. com. m1crosoft.w1ndows-12840tv	
若要修改发起程序名称,请单击"更改"。 更改(H)	
若要將发起程序 CHAP 机密设置为与相互 CHAP 一起使 用,请单击"CHAP"。	1
若要设置发起程序的 IPsec 隧道模式地址,请单击 "IPsec"。	
若要生成系统中所有已连接的目标和设备的报告,请单报告(&) 去"报告"。	
有关配置的详细信息	
	A)
iSCSI 发起程序相互 CHAP 机密	×
iSCSI 发起程序相互 CHAP 机密用于对目标进行身份验证。必须在要使用相互 CHAP 各个目标上配责在此处输入的机密。	的
相互 CHAP 在向目标建立连接时需要使用发起程序身份验证,当向目标建立连接时, 通过使用高级选项完成此操作。	可
若要清除发起程序中的机密,请单击"清除",然后单击"取消"。	
发起程序 CHAP 机密(I):	

"目标机密"需要在iSCSI发起程序中添加目标门户和连到接到目标时,进入"高级"选项下配置,除了勾选"启用CHAP登陆"、配置"目标机密"外,还需要勾选"执行相互身份验证"。

确定(0) 取消(C)

_____清除(L)_____

高级设置									
常规 IPsec									
本地适配器 (L):	默认值								
发起程序 IP(I):	默认值								
目标门户 IP(T):									
CRC/校验和									
数据摘要(D)	□ 标题摘要 (H)								
☑ 启用 CHAP 登录(E) CHAP 登录信息 通过在目标和发起程序之间提供身份验证,CHAP 有助于确保连接安全。 若要使用,请指定在目标上为该发起程序配置的相同名称和 CHAP 机密。除非指定 其他名称,否则名称将默认为系统的发起程序名称。									
名称(07):	iqn. 1991-05. com. microsoft: windows-f2a40tv								
目标机密 (S):	••••••								
☑ 执行相互身份验证 (P) 若要使用相互 CHAP,请在"配置"页上指定发起程序机密或使用 BADIUS。									
□使用 RADIUS 来生」 □使用 RADIUS 对目和	成用户身份验证凭据(U) 示凭据进行身份验证(B)								
	确定 取消 应用 (A)								

9、集群和卷配置

检查存储集群下正确配置存储卷,并且存储卷分配给服务器。

(i) + = = = =		详细	信息 快照 远程快照 计划 已分配服务器	SCSI 会话 映射视图				
S group1		à	一方面和取消分配服务器				×	
➡ ➡ 爭任 ➡ 服务器(5)		R	选择要分配给卷"lun1"的服务器。				?	作物 秋原
			注意要为任何服务器群集中的每一个服务器分配根卷,请使	刊"分配卷到服务器群集"	•			
🗄 🗮 cluster1			名称	已分配		权限		
一〇〇 性能監視器			127.65		读/写		-	
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □			La 127.66		读户后		-	
			🔓 180		谜 <i>1</i> 7号		-	
	(î		C cvk1		读/7号		-	
(Conjuan1 (0)			erver1	V	读の引			
		N 5						

如果安装以上步骤依旧无法解决,那么建议通过CMC登陆存储管理组后,查看管理组状态和事件告警、收集存储管理组支持套件和存储iLO AHS日志、操作过程相关截图,联系H3C技术支持热线 400-810 -0504进行分析。下面介绍存储管理组支持套件和存储iLO AHS日志收集方法:

1) 存储管理组支持套件信息收集

通过CMC连接存储管理组后,选中管理组右击,选择"导出管理组支持套件"选项。

SAN 状态贝	1.6	送知信息 法积权	1. 651 0 6. 6. 1 . 201 (M	BTIEL DNS	31 H					
2 入门		14-10110-02	Class Rectal Decid	ej jej Dino	65.70					
∑ 配直捕获 Coroupt		11								?
🗕 🔝 group1		名称 🚼	group1							
扩展整个组		状态: 正治	、协调管理器1.p5	730、己配置1个管	管理器1 个常规管理器					
扩展到错误		95件钟即裂·工			已發發用。	At admin				
新建服务器		14 Mt B 25161 75			C. 32. (K/11/	· domin				
新建群集		仲税: 1			本地带宽:	16 MB/sec				
从管理组中删除系统		最佳实践 🧘 (0)	🚫 (1)							
从使理组注销		Ø 网络帧大小一	政性							
关闭管理组										
公務部項相違統		系續(1)								
and the state and state an		名称	IP 地址	机型	连接类型	管理器	特殊管理器	RAID 状态	RAID 症習	1
ATTA B 4240		🙀 1.p5730	192.168.149.11	4730	iSCSI	正常		▼ 正常	RAID 6	1
查看管理组配置										1
查找天妖管理组										
添加虚拟管理器		•							•	1
注册		群集(1)								-
										п
检查升级件										

选择存储管理组支持套件信息保存的路径后点击"保存"按钮。



存储管理组支持套件文件生成生成后,在对应的文件夹中能查看到对应的.zip文件。

				_		×		
③ ● 影 + 計算机 → 本地磁盘(C3 → 用户 → huanglei → 我的文档 →								
文件(F) 编辑(E) 查看(V) 工具(T) 帮助	助(H)							
组织 ▼ 包含到库中 ▼ 共享 ▼	新建文件夹			800 -		0		
- 🚖 收藏实	名称 ^	修改日期	美型	大小				
🚺 下载	2017-12-19T_6_11_01Z()9fcd3d3ae9eebb56eb252c67a72583af.zip	2017/12/19 14:36	WinRAR ZIP 匝缩	4,923 KB				
三 東面								
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>								
- 📜 库								
📑 视频								
回 開片								
▶ 🗟 文档								
2 司 首乐								

2) AHS日志收集

通过WEB方式开的iLO管理界面,输入账号登陆。iLO配置了缺省用户名和密码,缺省用户信息可以在存储设备左上角的贴牌上查看。

293765-001	
iLO Defau	It Network Settings
Serial Number 6CU5108L82	
User Name: Admini	strator
DNS Name: ILO6CU5108L82	
Password: 9864163	38

WEB正常登陆后,在"信息>Active Health System日志"菜单下,设置好收集日志的时间范围,点击"下载"。

Active Health S	ystem 日志的范围,以天为单位	ý.
2017-04-10	到: 2017-04-16	(yyyy-mm-dd)
(范围是过去7 天的日:	志. 将范围重置为联议值.	
加联系人信息		
	联系人信息	
请提供以下聊	美系信息,以帮助我们提供更好	的服务。(可迭的)
+ + + + + + + + + + + + + + + + + + + +		
支持条例号:		
駅系へ迎る:		
电话号码:		
电于即注:		
公司名称:		
注意:联系人信息并	并不被存储在HDM,只会被添加	到被下载的日志文件。
ive Health System 能 、合作伙伴或数据中心	s监测和记录服务器的硬件和系统 L的信息(例如,IP 地址、主机名	流配置的变化。Active I 3、用户名和密码不会社
由下载和发送Active H	Health System 的数据到H3C和H	H3C的合作伙伴,表示约

推荐使用IE浏览器操作,生成的日志文件后缀名以.ahs结尾。

🎧 🕞 🔉 🖡 🕨 huanglei 🕨 下载				 ◆ / / / / / / / / / / / / / / / / / / /		
文件(F) 編輯(E) 查看(V) 工具(T) 帮助	h(H)					
组织 ▼ 包含到库中 ▼ 共享 ▼	新建文件夹				8= • 6	1 (
🚖 乾藏夫	名称	修改日期	类型	大小		
🚺 下戴	HP_6CU5108L82_20171219.ahs	2017/12/19 15:10	AHS 文件	26,399 KB		
🜉 桌面 🔄 最近访问的位置						
□ 库						
₩ 四片						
▶ 文档						