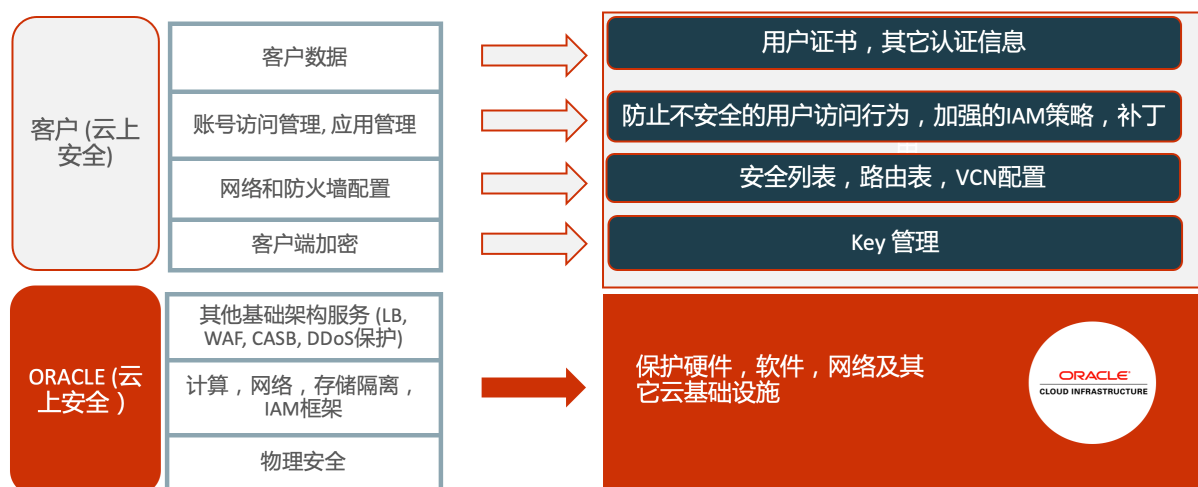


# 利用OCI操作系统管理服务(OS Management)简化操作系统更新和补丁程序

企业应用上云，安全问题是首要考虑的因素之一。Oracle在OCI公有云上提供了全方位、多层次的安全保护机制。但是对于云上的应用安全，企业与Oracle有不同的安全责任范畴，需要企业与Oracle共同承担安全责任。

## OCI上安全责任模型



例如，在OCI上创建的计算实例，如果操作系统不是选择的Oracle自治Linux，则操作系统的更新和补丁需要客户自己来进行维护。但是不少客户会忽略定期更新系统包和补丁，特别是安全漏洞补丁，这将会使实例受到黑客攻击的风险，造成数据泄露，客户端响应变慢，企业应用失效等等不良后果。

没有经验的客户在管理操作系统软件包和补丁程序时，会遇到不少问题，如：更新软件包的查找，安装程序源的配置，安装包之间的依赖等等。

OCI 提供的操作系统管理服务(OS Management)可以让客户在OCI实例上管理操作系统环境的更新和补丁程序，客户可以通过浏览器或者API来管理更新和补丁，简化更新和补丁流程。

## 操作系统管理服务支持的映像

Linux:

- Oracle Linux 6 及以上版本
- Oracle Linux 7 及以上版本
- Oracle Linux 8 及以上版本

Windows:

- Windows Server 2012 R2 Standard, Datacenter
- Windows Server 2016 Standard, Datacenter
- Windows Server 2019 Standard, Datacenter

本文将会以Oracle Linux虚拟机计算实例为例，简述OS管理服务的配置步骤。

## 先决条件


- 计算实例必须是支持的映像。
- 服务网关或公共IP地址：您的实例必须连接到具有以下其中一项的虚拟云网络（VCN）：
  - 具有服务网关的私有子网，该子网使用具有Oracle Services Network CIDR标签的所有区域服务。
  - 具有NAT网关的私有子网。
  - 具有Internet网关的公共子网。
- 安全列表（仅Windows实例）：必须定义安全列表或网络规则，以允许访问Windows更新服务器。
- 获取目标实例和区间的OCID。

## 步骤一：安装Oracle Cloud Agent

默认情况下，在当前Oracle提供的映像上都会安装Oracle Cloud Agent。如果是旧映像需要手动安装Oracle Cloud Agent。

1. 进入你想管理的计算实例详细信息页面，点击**Oracle Cloud Agent**标签页。如果Oracle Cloud Agent没有安装或版本不是最新的，则需要手工进行安装。

计算 - 实例 - 实例详细信息 - 工作请求



osmtest

启动 停止 重新引导 编辑 更多操作

实例信息 **Oracle Cloud Agent** 标记

正在运行

Oracle Cloud Agent 是用于管理实例上运行的插件的轻型进程。插件收集性能度量、安装操作系统更新以及执行其他实例管理任务。

插件名称	状态	消息	上次更新时间	启用插件
Vulnerability Scanning	-	-	-	已禁用
OS Management Service Agent	-	Plugin OS Management Service Agent not present for instance ocid1.instance.oc1.ap-seoul-1.anuwxgfrboghfhqccco2y5agc522jgs5dyfab6zcyct34temp5m6aaz7msq	-	已启用
Custom Logs Monitoring	-	Plugin Custom Logs Monitoring not present for instance ocid1.instance.oc1.ap-seoul-1.anuwxgfrboghfhqccco2y5agc522jgs5dyfab6zcyct34temp5m6aaz7msq	-	已启用
Compute Instance Run Command	-	Plugin Compute Instance Run Command not present for instance ocid1.instance.oc1.ap-seoul-1.anuwxgfrboghfhqccco2y5agc522jgs5dyfab6zcyct34temp5m6aaz7msq	-	已启用
Compute Instance Monitoring	-	Plugin Compute Instance Monitoring not present for instance ocid1.instance.oc1.ap-seoul-1.anuwxgfrboghfhqccco2y5agc522jgs5dyfab6zcyct34temp5m6aaz7msq	-	已启用

显示 5 项 < 1/1 >

2. 以opc用户连接到计算实例，运行下面的命令来判断Oracle Cloud Agent软件是否已经安装。（如果不是新版本，该命令也会自动更新Agent软件。）

```
sudo yum info oracle-cloud-agent
```

3. 如果没有安装或安装的版本不是最新的，可以运行下面的命令来安装。

```
sudo yum install -y oracle-cloud-agent
```

4. 从OCI控制面板，再次进入计算实例详细信息，查看**Oracle Cloud Agent**标签页，可以看到最新版本Agent插件已经启动。这些插件是用来监控计算实例性能，收集日志信息，漏洞扫描等等。本文中我们只用查看OS Management Service Agent插件是否正常启动。你可以切换启用或禁用开关来管理插件。

计算 > 实例 > 实例详细信息

osmtest

启动 停止 重新引导 编辑 更多操作

实例信息 Oracle Cloud Agent 标记

Oracle Cloud Agent 是用于管理实例上运行的插件的轻型进程。插件收集性能度量、安装操作系统更新以及执行其他实例管理任务。

停止插件

插件名称	状态	消息	上次更新时间	启用插件
Vulnerability Scanning ⓘ	-	-	2021年5月11日周二 UTC 08:59:17	<input type="checkbox"/> 已禁用
OS Management Service Agent ⓘ	● 正在运行		2021年5月11日周二 UTC 08:59:17	<input checked="" type="checkbox"/> 已启用
Custom Logs Monitoring ⓘ	● 正在运行	started plugin and agent	2021年5月11日周二 UTC 08:59:17	<input checked="" type="checkbox"/> 已启用
Compute Instance Run Command ⓘ	● 正在运行		2021年5月11日周二 UTC 08:59:17	<input checked="" type="checkbox"/> 已启用
Compute Instance Monitoring ⓘ	● 正在运行		2021年5月11日周二 UTC 08:59:17	<input checked="" type="checkbox"/> 已启用

显示 5 项 < 1/1 >

## 步骤二：为操作系统管理服务设置策略

1. 创建一个动态组，其中包含要由OS Management Service管理的实例集。例如：
- 名称：osm-group
  - 说明：Dynamic group for OS Management
  - 匹配规则：`Any {instance.id = 'ocid1.instance.oc1.iad..exampleuniqueid1', instance.compartment.id = 'ocid1.compartment.oc1..exampleuniqueid2'}`，替换为你的目标实例id和区间id。如果你有更多的实例，你可以增加匹配规则。

创建动态组 帮助

名称  
osm-group  
不允许使用空格，仅允许使用字母、数字、连字符、句点或下划线。

说明  
Dynamic group for OS Management

匹配规则  
规则定义哪些资源是此动态组的成员。系统会自动添加所有符合标准的实例。  
① 示例：Any {instance.id = 'ocid1.instance.oc1.iad..exampleuniqueid1', instance.compartment.id = 'ocid1.compartment.oc1..exampleuniqueid2'}  
☒ 匹配下面定义的任意规则 ☐ 匹配下面定义的所有规则  
规则 1  
Any {instance.id = 'ocid1.instance.oc1.ap-seoul-1.anuvgljrobogfhqcuymfzcc5d7q', instance.compartment.id = 'ocid1.compartment.oc1..aaaaaaaahnn5imnbuqskultzbeksokn2nm6ar6zcc5d7q'}  
[规则构建器](#)  
+ 其他规则

显示高级选项

创建 取消 ☐ 创建另一个 动态组

2. 创建一个策略，授予实例访问操作系统管理服务的权限，同时授予该动态组权限检索实例详细信息的权限。你可以在当前区间创建，也可以创建在上层或根区间。
- ALLOW dynamic-group <dynamic\_group\_name> to use osms-managed-instances in compartment <compartment\_name>
  - ALLOW dynamic-group <dynamic\_group\_name> to read instance-family in

compartment <compartment\_name>

## 创建策略

名称

osm-policy

不允许使用空格。仅允许使用字母、数字、连字符、句点或下划线。

说明

osm-policy

区间

oraclepartnersas (根) /

oraclepartnersas (根) /

策略构建器

显示手动编辑器



ALLOW dynamic-group osm-group to use osms-managed-instances in compartment osm-compartment  
ALLOW dynamic-group osm-group to read instance-family in compartment osm-compartment

示例：Allow group [group\_name] to [verb] [resource-type] in compartment [compartment\_name] where [condition]

显示高级选项

创建

取消



创建另一个 策略

- 用opc用户ssh连接到虚拟机实例，重新启动Oracle Cloud Agent。

```
sudo systemctl restart oracle-cloud-agent.service
```

- 运行下面的命令来验证您的实例是否可以访问OS Management提取服务(ingestion service)。  
将 <region> 替换为实例所在的区域，如：ap-seoul-1。

```
curl https://ingestion.osms.<region>.oci.oraclecloud.com/
```

下面的结果表明该实例可以成功到达OS Management提取服务。(注：输出中包含403 Forbidden是正常的。)

```
<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx/1.16.1</center>
</body>
</html>
```

## 5. 验证yum配置。

```
$ ls /etc/yum.repos.d
```

确定 `/etc/yum.repos.d` 目录中的 `*.repo` 文件都备份到同一目录中的 `*.repo.osms-backup`。如果没有，等待几分钟后再次查看，直到备份完成。

```
ksplice-ol7.repo.osms-backup      oracle-softwarecollection-ol7.repo.osms-backup
mysql-ol7.repo.osms-backup        oraclelinux-developer-ol7.repo.osms-backup
oci-included-ol7.repo.osms-backup uek-ol7.repo.osms-backup
oracle-epel-ol7.repo.osms-backup  virt-ol7.repo.osms-backup
oracle-linux-ol7.repo.osms-backup
```

## 6. 验证OS Management Service代理插件是否正在实例上运行。

```
$ ps -elf | grep osms | grep -v grep
4 S root      20811 20791  0  80    0 - 62265 -      11:22 ?          00:00:00
/usr/bin/sudo -n /usr/libexec/oracle-cloud-agent/plugins/osms/osms-agent
4 S root      20813 20811  0  80    0 - 2163 -      11:22 ?          00:00:00
/usr/libexec/oracle-cloud-agent/plugins/osms/osms-agent
4 S root      20814 20813  0  80    0 - 322898 -    11:22 ?          00:00:02
/usr/libexec/oracle-cloud-agent/plugins/osms/osms-agent
```

OS Management Service Agent插件正常运行后，您已完成用于设置托管实例的任务。现在，您可以使用OS Management服务来管理实例。

# 步骤三：管理Linux软件包

下面将介绍如何由OS Management Service管理Linux实例的软件包。

1. 从OCI控制台进入计算实例详细信息的页面，在资源下点击操作系统管理。可以看到该实例可用的操作系统更新，其中包含：
  - 安全：解决了在开发、测试期间或用户报告发现的安全漏洞的更新。安全修补程序通常具有一个或多个关联的CVE（常见漏洞和披露）名称，用来标识漏洞。
  - Bug：此更新程序修复了用户报告的问题或在开发或测试过程中发现的问题。
  - 增强：该更新在软件包的软件中引入了新特性，改进的功能或增强的性能。
  - 其他：该更新未归类。

资源

度量

附加的块存储卷

附加的 VNIC

引导卷

控制台连接

运行命令

工作请求

操作系统管理

定制日志

配置

配置: VM.Standard.E4.Flex

OCPU 计数: 1

网络带宽 (Gbps): 1

内存 (GB): 16

本地磁盘: 仅块存储

固件: UEFI\_64

引导卷类型: PARAVIRTUALIZED

传输中加密: 已禁用

操作系统管理

可使用[操作系统管理服务](#)管理计算实例上的更新和补丁程序。

可用更新:

13 安全

78 Bug

1 增强

5 其他

已调度作业: 0

工作请求: 0

操作系统: oraclelinux-release

内核 : 5.4.17-2036.103.3.1.el7uek.x86\_64

...

2. 点击右边菜单，可以看到有安装安全更新或者安装所有更新选项，你可以在这里进行更新的安装。本例中我们选择查看操作系统管理详细信息。

资源

度量

附加的块存储卷

附加的 VNIC

引导卷

控制台连接

运行命令

工作请求

操作系统管理

定制日志

操作系统管理

可使用[操作系统管理服务](#)管理计算实例上的更新和补丁程序。

可用更新:

13 安全

78 Bug

1 增强

5 其他

已调度作业: 0

工作请求: 0

操作系统: oraclelinux-release

内核 : 5.4.17-2036.103.3.1.el7uek.x86\_64

查看操作系统管理详细信息

安装安全更新

安装所有更新

3. 在详细信息页面可以查看可用的更新包，你可以选择某个或多个更新包，点击安装更新按钮。

MI

osmtest

托管实例信息

区域: oraclepartnersas (根) / [查看可用区域](#)

父软件源: [Oracle Linux 7 Server Latest \(x86\\_64\)](#)

计算实例: osmtest

操作系统: oraclelinux-release

内核 : 5.4.17-2036.103.3.1.el7uek.x86\_64

OCID: ...6aiz7msq [显示](#) [复制](#)

有更新可用: 92

上次引导: 2021年5月11日周二 UTC 08:47:45

资源

可用的程序包更新

可用程序包

安装的程序包

组

软件源

已调度作业

工作请求

安装更新

名称

可用版本

安装的版本

体系结构

类型

通知

CVE

☐

PyYAML

[3.13-1.el7](#)

[3.10-11.el7](#)

x86\_64

其他

-

-

⋮

☒

bcc

[0.10.0-1.0.1.el7](#)

[0.10.0-1.el7](#)

x86\_64

Bug 修复

[ELBA-2021-9061](#)

-

⋮

☐

bcc-tools

[0.10.0-1.0.1.el7](#)

[0.10.0-1.el7](#)

x86\_64

Bug 修复

[ELBA-2021-9061](#)

-

⋮

☐

bpftool

[3.10.0-1160.25.1.el7](#)

[3.10.0-1160.15.2.el7](#)

x86\_64

Bug 修复

[ELBA-2021-1397](#)

-

⋮

4. 你可以选择立即安装，也可以选择定制计划，在未来某个时间点启动安装任务。点击安装程序包更新按钮。

# 安装程序包更新

是否确实要安装 1 个程序包更新？


安装计划

☒ 立即安装 ☐ 定制计划

安装程序包更新 取消

5. 你可以看到正在进行程序包更新的工作请求。点击正在进行的工作链接。

操作系统管理 - 托管实例详细信息



osmtest

托管实例信息

区间: oraclepartnersas (根) /Team/MQWANG/CHXWANG

父软件源: [Oracle Linux 7 Server Latest \(x86\\_64\)](#)

计算实例: [osmtest](#)

操作系统: oraclelinux-release

内核: 5.4.17-2036.103.3.1.el7uek.x86\_64

OCID: ...6alz7msq [显示](#) [复制](#)

有更新可用: 92

上次引导: 2021年5月11日周二 UTC 08:47:45

资源

[可用的程序包更新](#)

[可用程序包](#)

[安装的程序包](#)

[组](#)

[软件源](#)

[已调度作业](#)

[工作请求](#)

工作请求

操作类型	状态	完成百分比	已接受
<a href="#">程序包更新</a>	● 正在进行	0	2021年5月11日周二 UTC 12:41:57
<a href="#">程序包更新</a>	● 成功	100	2021年5月11日周二 UTC 12:25:34
<a href="#">程序包安装</a>	● 成功	100	2021年5月11日周二 UTC 12:12:36

显示 3 项 < 第 1 页 >

6. 你可以查看工作请求的详细信息。

操作系统管理

工作请求

工作请求详细信息

WR

正在进行

Package Install/Upgrade

工作请求信息

类型: 程序包更新

区间: oraclepartnersas (根) /Team/MQWANG/CHXWANG

OCID: ...yg23hvka

显示

复制

关联的托管实例: osmtest

关联的已调度作业: -

接受时间: 2021年5月11日周二 UTC 12:41:57

资源

错误消息数 (0)

关联的资源 (2)

错误消息

消息

错误代码

时间戳

找不到任何项。

显示 0 项 < 1/1 >

7. 等待一段时间，任务完成，图标变绿。

操作系统管理

工作请求

工作请求详细信息

WR

成功

Package Install/Upgrade

工作请求信息

类型: 程序包更新

区间: oraclepartnersas (根) /Team/MQWANG/CHXWANG

OCID: ...yg23hvka

显示

复制

关联的托管实例: osmtest

关联的已调度作业: -

接受时间: 2021年5月11日周二 UTC 12:41:57

资源

错误消息数 (0)

关联的资源 (2)

错误消息

消息

错误代码

时间戳

找不到任何项。

显示 0 项 < 1/1 >

8. 回到查看操作系统管理详细信息的页面，我们用另一种方式来安装更新软件。点击某安装包的链接，如： `bind-export-libs` 的可用版本。

操作系统管理

托管实例详细信息

MI

osmtest

托管实例信息

区间: oraclepartnersas (根) /Team/MQWANG/CHXWANG

父软件源: Oracle Linux 7Server Latest x86\_64

计算实例: osmtest

操作系统: oraclelinux-release

内核: 5.4.17-2036.103.3.1.el7uek.x86\_64

OCID: ...6alz7msq

显示

复制

有更新可用: 97

上次引导: 2021年5月11日周二 UTC 08:47:47

资源

可用的程序包更新

可用程序包

安装的程序包

组

软件源

已调度作业

工作请求

可用的程序包更新

安装更新

名称

可用版本

安装的版本

体系结构

类型

通知

CVE

☐

PyYAML

3.13-1.el7

3.10-11.el7

x86\_64

其他

-

-

:

☐

bcc

0.10.0-1.0.1.el7

0.10.0-1.el7

x86\_64

Bug 修复

ELBA-2021-9061

-

:

☐

bcc-tools

0.10.0-1.0.1.el7

0.10.0-1.el7

x86\_64

Bug 修复

ELBA-2021-9061

-

:

☐

bind-export-libs

32.9.11.4-26.P2.el7\_9.5

32.9.11.4-26.P2.el7\_9.3

x86\_64

安全

ELSA-2021-1469

CVE-2021-25215

:

☐

bind-libs

32.9.11.4-26.P2.el7\_9.5

32.9.11.4-26.P2.el7\_9.3

x86\_64

安全

ELSA-2021-1469

CVE-2021-25215

:

☐

bind-libs-lite

32.9.11.4-26.P2.el7\_9.5

32.9.11.4-26.P2.el7\_9.3

x86\_64

安全

ELSA-2021-1469

CVE-2021-25215

:

☐

bind-license

32.9.11.4-26.P2.el7\_9.5

32.9.11.4-26.P2.el7\_9.3

noarch

安全

ELSA-2021-1469

CVE-2021-25215

:

☐

bind-utils

32.9.11.4-26.P2.el7\_9.5

32.9.11.4-26.P2.el7\_9.3

x86\_64

安全

ELSA-2021-1469

CVE-2021-25215

:

☐

bpftool

3.10.0-1160.25.1.el7

3.10.0-1160.15.2.el7

x86\_64

Bug 修复

ELBA-2021-1397

-

:

9. 你可以查看该程序包的详细信息。点击相关性的页面。



操作系统管理

软件源

软件源详细信息

程序包详细信息

P

bind-export-libs

BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. This package set contains only export version of BIND libraries, that are used for building ISC DHCP.

安装

程序包信息

相关性

版本: 32:9.11.4-26.P2.el7\_9.5

大小: 1.092 MiB

体系结构: x86\_64

软件源: [Oracle Linux 7/Server Latest \(x86\\_64\)](#)

资源

文件列表

名称	上次修改时间	大小 (字节)
/etc/ld.so.conf.d/bind-export-x86_64.conf	2020年12月27日周日 UTC 14:22:06	26
/usr/lib64/bind9-export	2020年12月27日周日 UTC 14:22:09	directory
/usr/lib64/bind9-export/libdns-export.so.1102	2020年12月27日周日 UTC 14:22:06	symlink
/usr/lib64/bind9-export/libdns-export.so.1102.1.2	2020年12月27日周日 UTC 14:22:17	2304080

10. 可以查看该更新包关联的安装包。点击安装。

操作系统管理

软件源

软件源详细信息

程序包详细信息

P

bind-export-libs

BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. This package set contains only export version of BIND libraries, that are used for building ISC DHCP.

安装

程序包信息

相关性

需要

提供

/sbin/ldconfig  
config(bind-export-libs)  
libc.so.6()(64bit)  
libc.so.6(GLIBC\_2.14)(64bit)  
libc.so.6(GLIBC\_2.15)(64bit)  
libc.so.6(GLIBC\_2.17)(64bit)  
libc.so.6(GLIBC\_2.2.5)(64bit)  
libc.so.6(GLIBC\_2.3)(64bit)  
libc.so.6(GLIBC\_2.3.4)(64bit)  
libc.so.6(GLIBC\_2.4)(64bit)  
libcap.so.2()(64bit)  
libcom\_err.so.2()(64bit)  
libcrypto.so.10()(64bit)  
libcrypto.so.10(libcrypto.so.10)(64bit)  
libcrypto.so.10(OPENSSL\_1.0.1\_EC)(64bit)  
libdns-export.so.1102()(64bit)  
libgssapi\_krb5.so.2()(64bit)  
libgssapi\_krb5.so.2(gssapi\_krb5\_2\_MIT)(64bit)  
libisc-export.so.169()(64bit)  
libk5crypto.so.3()(64bit)

bind-export-libs  
bind-export-libs(x86-64)  
config(bind-export-libs)  
libdns-export.so.1102()(64bit)  
libirs-export.so.160()(64bit)  
libisc-export.so.169()(64bit)  
libiscconf-export.so.160()(64bit)

11. 选择要安装的目标实例，点击安装按钮。

## 安装所选程序包

选择要在其上安装所选程序包的实例。

<input type="checkbox"/>	名称
<input checked="" type="checkbox"/>	osmtest
<input type="checkbox"/>	terraformtest

已选择 1 项 显示 2 项

[安装](#) [取消](#)

12. 可以看到程序包安装工作正在进行。

操作系统管理

[已调度作业](#)  
[工作请求](#)  
[托管实例组](#)  
[软件源](#)  
[CVE](#)  
[程序包](#)  
[度量 and 预警](#)

CHXWANG [区间](#) 中的 工作请求

操作类型	状态	完成百分比	已接受
程序包安装	● 正在进行	0	2021年5月11日周二 UTC 12:12:36
程序包安装	● 成功	100	2021年5月11日周二 UTC 03:48:12

显示 2 项 < 第 1 页 >

13. 你可以点击正在安装的工作链接，查看详细信息，直到安装成功。

操作系统管理 » 工作请求 » 工作请求详细信息



成功

Package Install/Upgrade

工作请求信息

类型: 程序包安装

区间: oraclepartnersas (根) /Team/MQWANG/CHXWANG

OCID: ...xyxzw4q [显示](#) [复制](#)

关联的托管实例: [osmtest](#)

关联的已调度作业: -

接受时间: 2021年5月11日周二 UTC 12:12:36

资源

[错误消息数 \(0\)](#)  
[关联的资源 \(2\)](#)

错误消息

消息	错误代码	时间戳
找不到任何项。		

显示 0 项 < 1/1 >

## 参考文档

[OS Management Services](#)

## 备注

---

作者：王敏桥

最新修改日期：2021年5月