# Overview

This guide is intended to provide a reference for performing regularly scheduled maintenance to Datacenter STS Service. From this point on it will be referenced via the acronym DSTS.

Currently the environment consist of the 2 sites Beijing and Shanghai. Each site is configured with 2 DSTS servers in Beijing (BJB) and 2 DSTS servers in the Shanghai (SHA) datacenter (commonly referred to as sites).

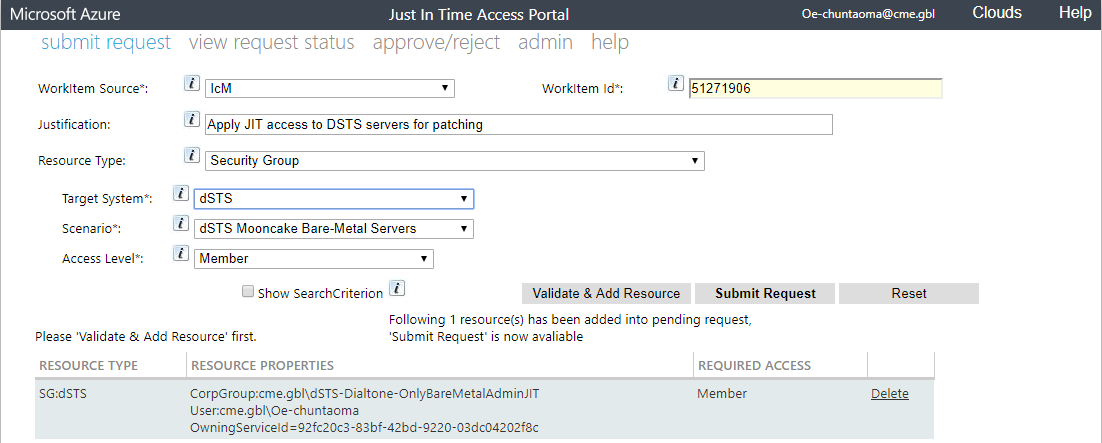
This guide is intended as a reference and may be modified to fit environmental requirements.

## Required Resources

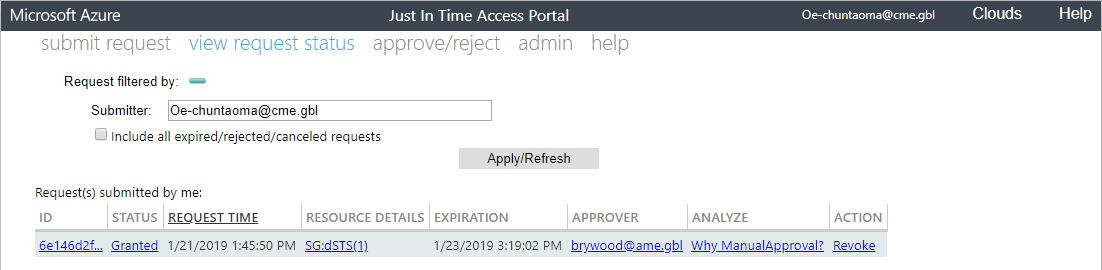
Prior to performing maintenance on DSTS servers, the following prerequisites must be satisfied:

* Users must have the ability to connect to the DSTS servers in each site. To gain the access to Dsts servers, the users need submit JIT request with following steps and get the approval from MSFT dSTS team(AME\AP-dSTS). Due to the time difference, suggest to submit the JIT request in advance so Dsts team has sufficient time to approve it during working hours.
* **Steps of submitting a JIT Access Request against Mooncake dsts servers**

1. Login JIT access portal <https://jitaccess.security.core.chinacloudapi.cn/WorkFlowTempAccess.aspx>
2. Fill out the request form on the main page with referring the following capture



1. Verify the request information in each fields is correct, then click “Validate&Add Resource”, one pending request will be generated at the bottom. Now you can click “Submit Request” button to submit the JIT request. Meanwhile, a JIT notification mail will be delivered to you mailbox and prompts it’s waiting for pending approval from AME\AP-Dsts.
2. To check whether the JIT request is approved or not, you can navigate to “View request status” page of JIT portal. When the request status is “Granted”, you are able to login dsts servers then.



* Users should be able to access the replicated shared path\\cme.gbl\Services\MSNPlat.

## Optional Resources

It is recommended that these prerequisites exist before performing maintenance:

* Change Management procedures such as Request for Changes (RFC’s) should be submitted and approved prior to scheduled maintenance start.
* If utilizing monitoring tools such as Geneva, DSTS servers should be suppressed prior to initiating any maintenance.
* Familiarity with the tools and commands in Appendix A and referenced throughout this document.

# Maintenance Practices and Procedures

Recommendations provided in this section are advised best practices for performing maintenance and rebooting DSTS servers within a domain(s).

## Change Management Request

Detailed change management tools and procedures are outside the scope of this article and should be addressed at a management level.

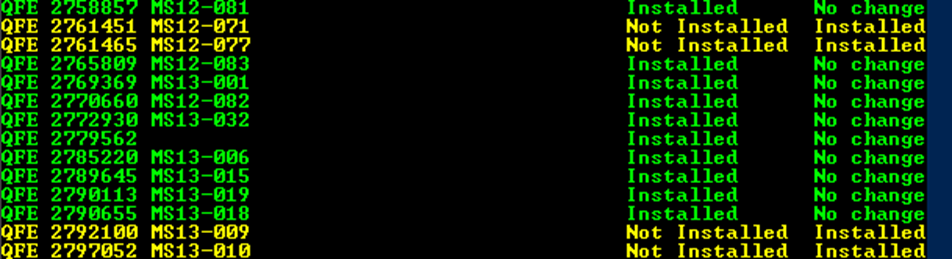
Prior to submitting a change request, the MSNPatch tool can be used to gather a list of items that will be installed. This is useful for detailing what changes that will be committed for change management documentation.

1. To determine what patches will be installed run MSNPatch in **Preview** mode.
2. Right click the **Power Shell** icon, and select **Run as Administrator**. Paste the following command:

\\cme.gbl\services\MSNPLAT\gold\MSNPATCH\MSNPatch.exe /PREVIEW

1. Review the output, any QFE marked not Installed will be installed when MSNPatch is ran utilizing the install parameters.

Output is also logged to: C:\msnipak\MSNPATCH\<date/time>\\_\_ipak\_\_.log



## Patch Groups

It is highly recommended that maintenance and reboots only occur on one patch group at a time. There should be a minimum of 5 days gap between both groups to decrease potential risk.

Example:

|  |  |
| --- | --- |
| Patch Group 1 | Patch Group 2 |
| SHA02DSTSDT01  SHA02DSTSDT02 | BJBDSTSDT01  BJBDSTSDT02 |

## Maintenance Flow

All change management procedures should be submitted and approved before this point. The following is a generic flow of events during the maintenance period. The next section will detail applying patches as an example.

## Maintenance Flow for Group 1

1. Send patching notification to stakeholders prior to initiating maintenance.
2. Put all servers in Group 1 into maintenance mode and/or suppress any monitoring and alert tools for the target DSTS servers.
3. On each DSTS server in Group 1, run the MSNPatch.exe tool:
   1. Right-click the **Power Shell** icon and select **Run as Administrator**. Paste the following command:

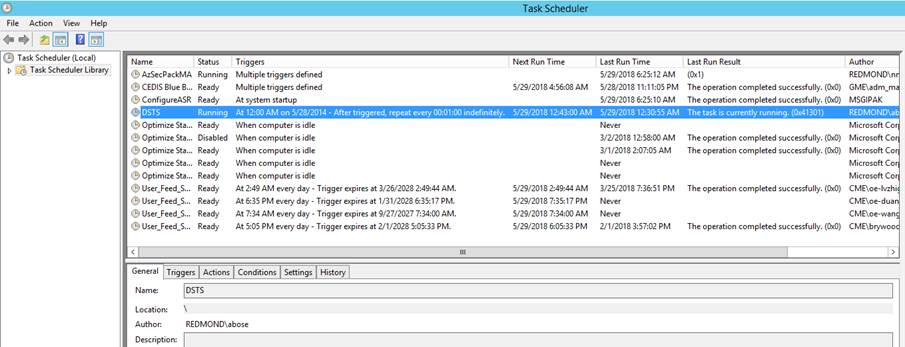
\\cme.gbl\services\MSNPLAT\gold\MSNPATCH\MSNPatch.exe /EnforceTLS12:FALSE

1. After the MSNPatch tool completes successfully, reboot the server.
2. After the server is rebooted, login and verify that no other QFE’s need to be installed:

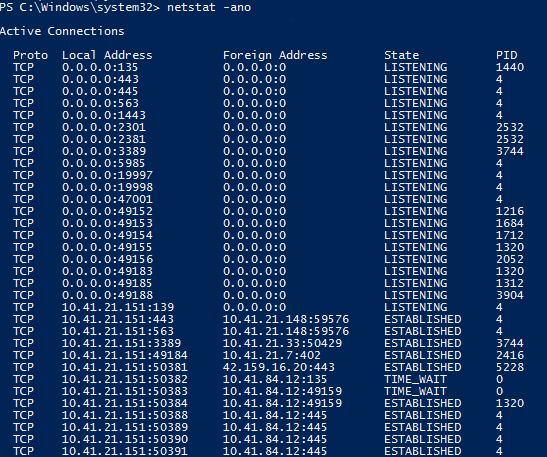
\\cme.gbl\services\MSNPLAT\gold\MSNPATCH\MSNPatch.exe /fcfailonly

* 1. If anything is listed, continue with steps 2 through 4 until no other patches are necessary, otherwise continue to step 6.

1. After all maintenance has been completed verify all necessary services and ports are running:
   1. Get-WmiObject win32\_service | Where {$\_.StartMode -like "Auto" -and $\_.State -notlike "Running"} | select Name, State
   2. Go to Task Scheduler and find the task “DSTS”, check its state and make sure it’s running. If not running, just run it manually.



* 1. Open CMD or Powershell with admin priviledge, run “netstat –ano” to check whether ports 443,563,19997,19998 are **LISTENING** on primary DSTS server SHA02DSTSDT01. (Please refer to the following capture)



1. End maintenance mode and/or any suppression and alerting tools.
2. Send patching end notification and close RFCs.

## Maintenance Flow for Group 2

1. Send patching notification to stakeholders prior to initiating maintenance.
2. Put all servers in Group 2 into maintenance mode and/or suppress any monitoring and alert tools for the target DSTS servers.
3. On each DSTS server in Group 2, run the MSNPatch.exe tool:
   1. Right-click the **Power Shell** icon and select **Run as Administrator**. Paste the following command:

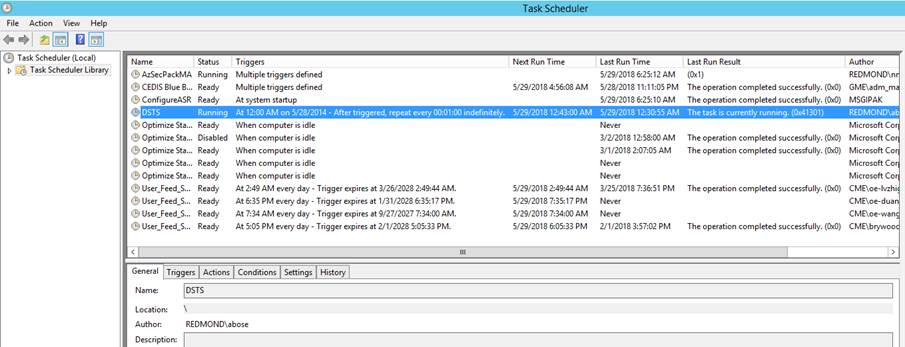
\\cme.gbl\services\MSNPLAT\gold\MSNPATCH\MSNPatch.exe /EnforceTLS12:FALSE

1. After the MSNPatch tool completes successfully, reboot the server.
2. After the server is rebooted, login and verify that no other QFE’s need to be installed:

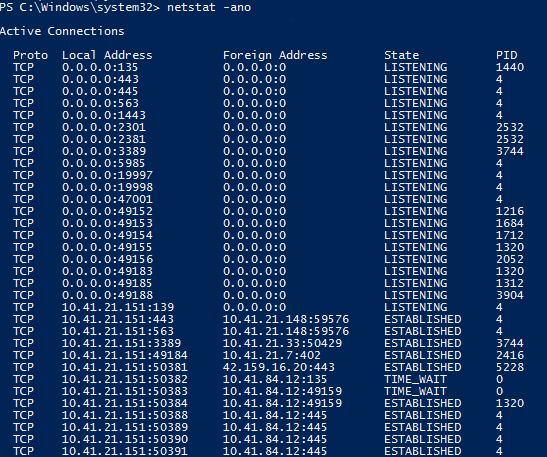
\\cme.gbl\services\MSNPLAT\gold\MSNPATCH\MSNPatch.exe /fcfailonly

* 1. If anything is listed, continue with steps 2 through 4 until no other patches are necessary, otherwise continue to step 6.

1. After all maintenance has been completed verify all necessary services and ports are running:
   1. Get-WmiObject win32\_service | Where {$\_.StartMode -like "Auto" -and $\_.State -notlike "Running"} | select Name, State
   2. Go to Task Scheduler and find the task “DSTS”, check its state and make sure it’s running. If not running, just run it manually.



* 1. Open CMD or Powershell with admin priviledge, run “netstat –ano” to check whether ports 443,563,19997,19998 are **LISTENING** on primary DSTS server BJBDSTSDT01. (Please refer to the following capture)



1. End maintenance mode and/or any suppression and alerting tools.
2. Send patching end notification and close RFCs.

# Appendix A--Patch Schedule

MSNPatch is released every month on Patch Tuesday (2nd Tuesday of every Month).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| January | February | March | April | May | June |
| MSNPATCH | MSNPATCH | MSNPATCH | MSNPATCH | MSNPATCH | MSNPATCH |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| July | August | September | October | November | December |
| MSNPATCH | MSNPATCH | MSNPATCH | MSNPATCH | MSNPATCH | MSNPATCH |

# Appendix B--Tools and Commands used

|  |  |
| --- | --- |
| Description | Commands |
| MSNPATCH  - Preview Mode | [\\CME.gbl\services\MSNPLAT\gold\MSNPATCH\MSNPatch.exe](file://CME.gbl/services/MSNPLAT/gold/MSNPATCH/MSNPatch.exe) /PREVIEW |
| MSNPATCH – Install QFEs | \\CME.gbl\services\MSNPLAT\gold\MSNPATCH\MSNPatch.exe /EnforceTLS12:FALSE |
| MSNPatch – Verify Patches Installed | [\\CME.gbl\services\MSNPLAT\gold\MSNPATCH\msnpatch.exe](file://CME.gbl/services/MSNPLAT/gold/MSNPATCH/msnpatch.exe) /fcfailonly |

# Appendix C--Terms and Definitions

**MSNPatch**–The MSNPatch tool consolidates and automates the installation of regularly released Security Updates.

# Document Revisions

|  |  |  |  |
| --- | --- | --- | --- |
| Rev | Date | Alias | Description |
| 0.1 | 11/8/2017 | Michael Ma PS Team | Initial Draft |
| 0.2 | 11/9/2017 | Michael Ma PS Team | Updated MSNPatch command(removed /CORP) |
| 0.3 | 11/10/2017 | Michael Ma PS Team | Added maintenance flow for group 2 |
| 1.0 | 11/10/2017 | Bryan Woodworth <brywood@microsoft.com> | Reviewed |
| 1.1 | 4/16/2018 | Michael Ma PS Team | Updated MSNPatch command(added /EnforceTLS12:FALSE) |
| 2.0 | 4/17/2018 | Bryan Woodworth <brywood@microsoft.com> | Reviewed |
| 2.1 | 6/6/2018 | Michael Ma PS Team | Added verification steps b,c under step 6 for maintenance flow for group1 and group2 |
| 3.0 | 6/8/2018 | Bryan Woodworth <brywood@microsoft.com> | Reviewed |
| 3.1 | 1/23/2019 | Michael Ma PS Team | Added some description and captures about JIT access request in the part “Required Resources”. |