Cisco Success Network - Données de télémétrie

Cisco Success Network – Données de télémétrie

Cisco Success Network est une fonctionnalité permanente de collecte d'informations et de mesures d'utilisation de l'outil de migration de pare-feu sécurisé, qui collecte et transmet des statistiques d'utilisation par l'intermédiaire d'une connexion sécurisée dans le nuage entre l'outil de migration et le nuage de Cisco. Ces statistiques nous aident à fournir une assistance supplémentaire sur les fonctionnalités inutilisées et à améliorer nos produits. Lorsque vous lancez un processus de migration dans l'outil de migration de pare-feu sécurisé, le fichier de données de télémétrie correspondant est généré et stocké dans un emplacement fixe.

Lorsque vous poussez la configuration migrée avec FPSCheck Point vers centre de gestion, le service de transfert lit le fichier de données de télémétrie à partir de l'emplacement et le supprime une fois les données téléchargées avec succès dans le nuage.

L'outil de migration offre deux options au choix pour la diffusion en continu des données de télémétrie : **limitée** et **étendue**.

Lorsque **Cisco Success Network** est défini sur **Limitée**, les points de données de télémétrie suivants sont collectés :

Tableau 1 : Télémétrie limitée

Point de données	Description	Exemple de valeur
Durée	L'heure et la date de collecte des données de télémétrie	2023-04-25 10:39:19
Type de source	Le type de périphérique source	ASA
Numéro de modèle de l'appareil	Numéro de modèle de l'ASA	ASA5585-SSP-10, 5969 Mo de RAM, CPU Xeon série 5500 2000 MHz, 1 CPU (4 cœurs)
Version source	Version d'ASA	9.2 (1)
Version de gestion des cibles	La version cible du centre de gestion	6.5 ou plus récent

Point de données	Description	Exemple de valeur
Type de gestion cible	Le type de périphérique de gestion cible, à savoir le centre de gestion	Centre de gestion
Version du périphérique cible	La version du périphérique cible	75
Modèle de l'appareil cible	Le modèle du périphérique cible	Cisco Secure Firewall Threat Defense pour VMware
Version de l'outil de migration	La version de l'outil de migration	1.1.0.1912
État de la migration	L'état de la migration de la configuration ASA vers le centre de gestion	SUCCÈS

Les tableaux suivants fournissent des informations sur les points de données de télémétrie, leurs descriptions et des exemples de valeurs, lorsque **Cisco Success Network** est défini sur **Étendue** :

Tableau 2 : Télémétrie étendue

Point de données	Description	Exemple de valeur
Système d'exploitation	Système d'exploitation qui exécute l'outil de migration de pare-feu sécurisé. Il peut s'agir de Windows7/Windows10 64 bits/macOS High Sierra	Windows 7 :
Navigateur	Navigateur utilisé pour lancer l'outil de migration de pare-feu sécurisé. Il peut s'agir de Mozilla/5.0, de Chrome/68.0.3440.106 ou de Safari/537.36.	Mozilla/5.0

Tableau 3 : Informations sur le point de vérification source

Point de données	Description	Exemple de valeur
Durée	L'heure et la date de collecte des données de télémétrie	2023-04-25 10:39:19
Type de source	Le type de périphérique source	Check Point
Numéro de série du périphérique source	Numéro de série de Check Point	Numéro de série de l'appareil, s'il existe.
Numéro de modèle du périphérique source	Numéro de modèle de Check Point	
Version du périphérique source	Version de Check Point	R77.30
Nombre de configurations sources	Le nombre total de lignes dans la configuration source	504

Point de données	Description	Exemple de valeur
Mode pare-feu	Le mode de pare-feu configuré sur Check Point - routé ou transparent	ROUTAGE
Mode contextuel	Le mode contextuel de Check Point. Il peut s'agir d'un contexte unique ou multiple.	UNIQUE
Statistiques de configuration de point de contrôle :		
Nombre d'ACL	Le nombre d'ACL associées au groupe d'accès	46
Nombre de règles d'accès	Le nombre total de règles d'accès	46
Nombre de règles NAT	Le nombre total de règles NAT	17
Compte d'objets réseau	Le nombre d'objets réseau configurés dans Check Point	34
Nombre de groupes d'objets réseau	Le nombre de groupes d'objets réseau dans Check Point	6
Compte d'objets de port	Le nombre d'objets de port	85
Compte de groupes d'objets de port	Le nombre de groupes d'objets de port	37
Nombre de règles d'accès non prises en charge	Le nombre total de règles d'accès non prises en charge	3
Nombre de règles NAT non prises en charge	Le nombre total de règles d'accès NAT non prises en charge	0
Nombre de règles d'accès basées sur FQDN	Le nombre de règles d'accès basées sur le nom de domaine complet (FQDN)	7
Nombre de règles d'accès basées sur une plage de temps	Le nombre de règles d'accès basées sur une plage de temps	1
Nombre de règles d'accès basées sur SGT	Le nombre de règles d'accès basées sur SGT	0
Résumé des lignes de configuration que l'outil n'est pas en mesure d'analyser		
Nombre de configurations non analysées	Le nombre de lignes de configuration non reconnues par l'analyseur syntaxique	68
Nombre total de règles d'accès non analysées	Le nombre total de règles d'accès non analysées	3

Tableau 4 : Informations sur le périphérique de gestion cible (Centre de gestion)

Point de données	Description	Exemple de valeur
Version de gestion des cibles	La version cible de centre de gestion	6.2.3.3 (build 76)

Point de données	Description	Exemple de valeur
Type de gestion cible	Le type de périphérique de gestion cible, à savoir, centre de gestion	Centre de gestion
Version du périphérique cible	La version du périphérique cible	75
Modèle de l'appareil cible	Le modèle du périphérique cible	Cisco Secure Firewall Threat Defense pour VMware
Version de l'outil de migration	La version de la migration aussi1	1.1.0.1912

Tableau 5 : Résumé de la migration

Point de données	Description	Exemple de valeur
Stratégie de contrôle d'accès		
Nom	Le nom de la stratégie de contrôle d'accès	N'existe pas
Nombre de règles d'accès	Le nombre total de règles d'ACL migrées	0
Nombre de règles d'ACL partiellement migrées	Le nombre total de règles d'ACL partiellement migrées	3
Nombre de règles ACP étendu	Le nombre de règles ACP étendues	0
Fonction NAT		
Titre du champ	Le nom de la politique de NAT	N'existe pas
Nombre de règles NAT	Le nombre total de règles NAT migrées	0
Nombre de règles NAT partiellement migrées	Le nombre total de règles NAT partiellement migrées	0
Plus de détails sur la migration...		
Nombre d'interfaces	Le nombre d'interfaces mises à jour	0
Nombre de sous-interfaces	Le nombre de sous-interfaces mises à jour	0
Nombre de routes statiques	Le nombre de routes statiques	0
Nombre d'objets	Le nombre d'objets créés	34
Nombre de groupes d'objet	Le nombre de groupes d'objets créés	6
Nombre de groupes d'interfaces	Le nombre de groupes d'interfaces créés	0
Nombre de zones de sécurité	Le nombre de zones de sécurité créées	3
Nombre d'objets réseau réutilisés	Le nombre d'objets réutilisés	21
Nombre de renommages d'objets réseau	Le nombre d'objets qui sont renommés	1

Point de données	Description	Exemple de valeur
Nombre d'objets de port réutilisés	Le nombre d'objets de port qui sont réutilisés	0
Nombre d'objets de port renommés	Le nombre d'objets de port qui sont renommés	0

Tableau 6 : Données de performance de l'outil de migration de pare-feu sécurisé

Point de données	Description	Exemple de valeur
Temps de conversation	Le temps nécessaire pour analyser Check Point (en minutes)	14
Temps de la migration	Le temps total nécessaire pour la migration de bout en bout (en minutes)	592
Temps de transfert de la configuration	Le temps nécessaire pour transférer la configuration finale (en minutes)	7
État de la migration	L'état de la migration de la configuration Check Point vers centre de gestion	SUCCÈS
Message d'erreur	Le message d'erreur affiché par l'outil de migration de pare-feu sécurisé	null (nul)
Description de l'erreur	La description de l'étape où l'erreur s'est produite et la cause première possible	null (nul)

Fichier d'exemple de point de contrôle de télémétrie pour r77

Voici un exemple de fichier de données de télémétrie sur la migration de la configuration de Check Point vers défense contre les menaces :


```
{
  "metadata": {
    "contentType": "application/json",
    "topic": "migrationtool.telemetry"
  },
  "payload": {
    "Check Point_config_stats": {
      "Ipv6_access_rule_counts": 0,
      "Ipv6_bgp_count": 0,
      "Ipv6_nat_rule_count": 0,
      "Ipv6_network_counts": 24,
      "Ipv6_static_route_counts": 6,
      "access_rules_counts": 63,
      "acl_counts": 63,
      "fqdn_based_access_rule_counts": 0,
      "nat_rule_counts": 0,
      "network_object_counts": 143,
      "network_object_group_counts": 31,
      "no_of_fqdn_based_objects": 0,
      "ospfv3_count": 0,
      "port_object_counts": 370,
      "port_object_group_counts": 55,
      "sgt_based_access_rules_count": 0,
```

```
  "timerange_based_access_rule_counts": 0,
  "total_unparsed_access_rule_counts": 0,
  "tunneling_protocol_based_access_rule_counts": 0,
  "unparsed_config_count": 15,
  "unsupported_access_rules_count": 0,
  "unsupported_nat_rule_count": 0
},
"context_mode": "SINGLE",
"error_description": null,
"error_message": null,
"firewall_mode": "ROUTED",
"log_info_acl_count": 0,
"migration_status": "SUCCESS",
"migration_summary": {
  "access_control_policy": [
    [
      {
        "access_rule_counts": 63,
        "apply_file_policy_rule_counts": 0,
        "apply_ips_policy_rule_counts": 0,
        "apply_log_rule_counts": 0,
        "do_not_migrate_rule_counts": 0,
        "enable_Global-ACL-Policy": true,
        "enable_Zone-Specific-ACL-Policy": false,
        "enable_hit_count": false,
        "expanded_acp_rule_counts": 1,
        "name": "FTD-Mig-1566804327",
        "partially_migrated_acl_rule_counts": 0,
        "update_rule_action_counts": 0
      }
    ]
  ],
  "interface_counts": 12,
  "interface_group_counts": 0,
  "interface_group_manually_created_counts": 0,
  "nat_Policy": [
    [
      {
        "NAT_rule_counts": 0,
        "do_not_migrate_rule_counts": 0,
        "name": "Doesn't Exist",
        "partially_migrated_nat_rule_counts": 0
      }
    ]
  ],
  "network_object_rename_counts": 0,
  "network_object_reused_counts": 0,
  "object_group_counts": 15,
  "objects_counts": 54,
  "port_object_rename_counts": 0,
  "port_object_reused_counts": 5,
  "security_zone_counts": 13,
  "security_zone_manually_created_counts": 0,
  "static_routes_counts": 22,
  "sub_interface_counts": 11
},
"migration_tool_version": "2.0.3169",
"rule_change_acl_count": 0,
"source_config_counts": 0,
"source_device_model_number": "Check Point Model Not Exists",
"source_device_serial_number": null,
"source_device_version": "R77.30",
"source_type": "Check Point",
"system_information": {
```

```
      "browser": "Chrome/76.0.3809.100",
      "operating_system": "Windows NT 10.0; Win64; x64"
    },
    "target_device_model": "Cisco Firepower 9000 Series SM-24 Threat Defense",
    "target_device_version": "76",
    "target_management_type": "6.4.0.4 (build 31)",
    "target_management_version": "6.4.0.4 (build 31)",
    "template_version": "1.1",
    "time": "2019-08-26 12:55:40",
    "tool_analytics_data": {
      "objectsplit_100_count": 0
    },
    "tool_performance": {
      "config_push_time": 725,
      "conversion_time": 29,
      "migration_time": 1020
    }
  },
  "version": "1.0"
}
```


Fichier d'exemple de point de contrôle de télémétrie pour r80

Voici un exemple de fichier de données de télémétrie sur la migration de la configuration de Check Point vers défense contre les menaces :


```
{
"Check Point_config_stats":{
        "Ipv6_access_rule_counts":0,
        "Ipv6_bgp_count":0,
        "Ipv6_nat_rule_count":0,
        "Ipv6_network_counts":3,
        "Ipv6_static_route_counts":0,
        "access_rules_counts":726,
        "acl_category_count":0,
        "acl_counts":726,
        "fqdn_based_access_rule_counts":0,
        "nat_rule_counts":335,
        "network_object_counts":7645,
        "network_object_group_counts":268,
        "no_of_fqdn_based_objects":0,
        "port_object_counts":1051,
        "port_object_group_counts":66,
        "s2s_vpn_tunnel_counts":0,
        "sgt_based_access_rules_count":0,
        "timerange_based_access_rule_counts":0,
        "total_unparsed_access_rule_counts":0,
        "tunneling_protocol_based_access_rule_counts":0,
        "unparsed_config_count":234,
        "unsupported_access_rules_count":0,
        "unsupported_nat_rule_count":0},
        "context_mode":"SINGLE",
        "error_description":"No data.",
        "error_message":"push failed for object network",
        "firewall_mode":"ROUTED",
        "log_info_acl_count":0,
        "migration_status":"FAIL",
        "migration_summary":{
          "access_control_policy":[
           [
           {
               "access_rule_counts":0,
               "apply_file_policy_rule_counts":0,
               "apply_ips_policy_rule_counts":0,
```

```
        "apply_log_rule_counts":0,
        "do_not_migrate_rule_counts":0,
        "enable_Global-ACL-Policy":true,
        "enable_Zone-Specific-ACL-Policy":false,
        "enable_hit_count":false,
        "expanded_acp_rule_counts":1,
        "name":"Doesn't Exist",
        "partially_migrated_acl_rule_counts":0,
        "total_acl_element_counts":389416,
        "update_rule_action_counts":0
    }
]
],
"interface_counts":11,
"interface_group_counts":0,
"interface_group_manually_created_counts":0,
"nat_Policy":[
[
    {
        "NAT_rule_counts":0,
        "do_not_migrate_rule_counts":0,
        "name":"Doesn't Exist",
        "partially_migrated_nat_rule_counts":0
    }
]
],
"network_object_rename_counts":0,
"network_object_reused_counts":0,
"object_group_counts":222,"objects_counts":7148,
"port_object_rename_counts":2,
"port_object_reused_counts":30,
"prefilter_control_policy":[
   [
     {
        "do_not_migrate_rule_counts":0,
        "name":null,
        "partially_migrated_acl_rule_counts":0,
        "prefilter_rule_counts":0
      }
    ]
    ],
"security_zone_counts":11,
"security_zone_manually_created_counts":0,
"static_routes_counts":0,
"sub_interface_counts":8,
"time_out":false},
"migration_tool_version":"2.1.4283",
"mtu_info":{"interface_name":null,
"mtu_value":null},
"rule_change_acl_count":0,
"selective_policy":
        {
        "acl":true,
        "acl_policy":true,
        "application":false,
        "csm":false,
"interface":true,
"interface_groups":true,
"migrate_tunneled_routes":false,
"nat":true,
"network_object":true,
"policy_assignment":true,
"populate_sz":false,
"port_object":true,
```

```
"routes":true,
"security_zones":true,
"unreferenced":true},
"source_config_counts":0,
"source_device_model_number":"Check Point Model Not Exists",
"source_device_serial_number":null,
"source_device_version":"R77.30",
"source_type":"Check Point",
"system_information":
{
"browser":"Chrome/80.0.3987.163","operating_system":
"Macintosh; Intel Mac OS X 10_15_4"},
"target_device_model":"Cisco Firepower 4110 Threat Defense",
"target_device_version":"76",
"target_management_type":"6.5.0 (build 63)",
"target_management_version":"6.5.0 (build 63)",
"template_version":"1.1",
"time":"2020-04-16 04:50:05",
"tool_analytics_data":{"objectsplit_100_count":6},
"tool_performance":
        {
                "config_push_time":1457,
                "conversion_time":279,
                "migration_time":2637
        }
}
```

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.